

MASTER UNIVERSITARIO EN INGENIERÍA DE
TELECOMUNICACIÓN

Trabajo Fin De Máster

“CSPay. Nuevo método de pago para la
reducción de fraude y mejora de experiencia de
usuario en soluciones de comercio electrónico.”

Autora: Dña. Carla Solís Carpintero

Tutora: Dña. Ana Jiménez Martín

Director: D. Álvaro Martín García

Universidad de Alcalá
Escuela Politécnica Superior

MASTER UNIVERSITARIO EN INGENIERÍA DE
TELECOMUNICACIÓN

Trabajo Fin De Máster

“CSPay. Nuevo método de pago para la reducción de fraude y mejora de experiencia de usuario en soluciones de comercio electrónico.”

Autora: Dña. Carla Solís Carpintero
Alumna MUIT - UAH | Ingeniera de Calidad Chip y Emisión en Redsys SL

Tutora: Dña. Ana Jiménez Martín
Profesora Titular de Universidad en la Universidad de Alcalá

Director: D. Álvaro Martín García
Ingeniero Informático | Jefe de Dpto. Soluciones Chip y Emisión Redsys SL

TRIBUNAL

Presidente: D. José Manuel Rodríguez Ascariz

Vocal 1º: D. Isaías Martínez Yelmo

Vocal 2º: Dña. Ana Jiménez Martín

Agradecimientos

Quiero agradecer a mi tutora, Ana Jiménez, la dedicación y esfuerzo que ha dedicado para que el presente TFM saliese adelante. No han sido años fáciles, y siempre he contado con su respaldo y seguimiento, adaptándose a mis turnos imposibles y a mis cambios de idea.

Del mismo modo, me gustaría agradecer a Álvaro Martín, por el asesoramiento y guiado que día tras día me ofrece en el trabajo, enseñándome a ser mejor profesional y poder seguir sus pasos. Un recuerdo especial al resto de compañeros de trabajo de Redsys, un placer coincidir con todos vosotros.

Gracias a mi madre. Sin ella, no hubiera conseguido completar con éxito ningún reto. Soy consciente de que no es fácil entender mi ritmo de vida, y quizás lo que más agradezco es precisamente que, aun sin comprenderlo, crea ciegamente que puedo conseguir todo aquello que me proponga.

A mis hermanas, Leticia y Alba, por cederme el puesto de *“la lista de la familia”* cuando realmente son ellas las que me inspiran los valores y la motivación que siempre me hacen seguir adelante y reunir las fuerzas necesarias para seguir luchando tras cada caída.

A Noah, porque no se necesitan las palabras cuando existen tantos sentimientos de por medio.

Gracias a Miguel, por llegar a mi vida cuando más lo necesitaba y darme siempre una razón por la que no merecía la pena abandonar el Máster, pese a que tuviese motivos suficientes para hacerlo.

Como no podía ser de otra manera, mi más sincero agradecimiento a Daniel. Porque siempre fuiste, eres y serás mi mitad. Y contra eso, no se puede luchar.

Por último, me gustaría agradecer el apoyo que he recibido de todos mis amigos, compañeros de universidad y compañeros de trabajo, que me han acompañado en este viaje.

Para papá.

Índice General

I RESUMEN.....	21
RESUMEN	23
ABSTRACT	25
RESUMEN EXTENDIDO	27
II MEMORIA.....	31
1.INTRODUCCIÓN.....	33
1.1 MOTIVACIÓN Y ENTORNO DE TRABAJO	36
1.2 OBJETIVOS	37
1.3 ESTRUCTURA	38
1.4 RESEÑA HISTÓRICA DEL COMERCIO	39
1.4.1 Evolución y despliegue del comercio presencial.....	40
1.4.2 El progreso del comercio electrónico.....	56
2.ESTADO DEL ARTE DEL COMERCIO ELECTRÓNICO	59
2.1 ESTADO DEL ARTE DEL COMERCIO ELECTRÓNICO.	59
2.2 PAGO MEDIANTE INSERCIÓN DE LOS NÚMEROS DE LA TARJETA	63
2.2.1 Pago con tarjeta en comercio electrónico no seguro	63
2.2.2 Pago con tarjeta en comercio electrónico seguro	66
2.3 ELECTRONIC WALLET.....	69
2.3.1 PayPal	69
2.3.2 iupay 71	
2.4 AUTOGESTIÓN DE LOS GRANDES COMERCIOS.....	73
2.5 TARJETAS VIRTUALES.....	75
2.6 EL BITCOIN	76
2.7 OTROS MÉTODOS DE PAGO EN COMERCIO ELECTRÓNICO.....	78
2.7.1 Contra-reembolso	78
2.7.2 Talón bancario	78
2.7.3 Transferencia bancaria.....	78
3.FRAUDE EN E-COMMERCE Y SEGURIDAD DEL PROTOCOLO EMV	79
3.1 FRAUDE EN COMERCIO ELECTRÓNICO	79
3.2 ORIGEN Y TIPOS DE ATAQUES FRAUDULENTOS EN COMERCIO ELECTRÓNICO.....	82
3.2.1 Robo de los datos financieros en el entorno presencial.....	82
3.2.2 Robo de los datos financieros en un entorno no presencial.	83
3.3 PROTOCOLO DE COMUNICACIÓN EMV EN EL ENTORNO PRESENCIAL.....	85

4. ANÁLISIS DE LA SOLUCIÓN Y PROPUESTA CSPAY.	97
4.1 ESTRUCTURA GLOBAL DE LA SOLUCIÓN PROPUESTA.	97
4.2 ANÁLISIS DE LAS POSIBLES ALTERNATIVAS TÉCNICAS.....	101
4.2.1 ETAPA A: Fase de enrolamiento y registro del usuario.....	101
4.2.2 ETAPA B: Obtención del número de teléfono móvil vía web	102
4.2.3 ETAPA C: Comunicación entre el centro procesador y la aplicación móvil	105
4.2.4 ETAPA D: Autenticación del cliente en el dispositivo móvil.....	111
4.2.5 ETAPA E: Protocolo de comunicación entre el móvil y la tarjeta	113
4.2.6 ETAPA F: Operativa transaccional entre Redsys y la entidad financiera	117
5. SOLUCIÓN TECNOLÓGICA PARA EL DEMOSTRADOR CSPAY.....	121
5.1 VISIÓN GENERAL DEL DEMOSTRADOR.	121
5.2 APLICACIÓN PARA EL DISPOSITIVO MÓVIL.....	123
5.2.1 Determinación del sistema operativo: Android vs iOS.	123
5.2.2 Decisión del entorno de desarrollo.....	125
5.2.3 Desarrollo de la aplicación	129
5.3 TARJETAS FINANCIERAS DE PRUEBAS	144
5.4 SERVIDOR PARA EL PROCESAMIENTO Y RESOLUCIÓN DE TRANSACCIONES E-COMMERCE.	147
5.4.1 Elección del lenguaje de programación de la red de pago.....	147
5.4.2 Procesador transaccional alojado en la nube.....	148
5.4.3 Mensajería push: GCM.....	151
5.4.4 Procesamiento y administración de las bases de datos	152
5.4.5 Notificación mediante correo electrónico.....	154
5.5 PÁGINA WEB QUE EMULE COMPORTAMIENTO DE UN COMERCIO ELECTRÓNICO	156
5.5.1 Protocolo de comunicación HTTP	158
6. IMPLEMENTACIÓN DEL DEMOSTRADOR CSPAY.....	163
6.1 FUNCIONAMIENTO DEL SISTEMA.	163
6.2 INTEGRACIÓN Y SECUENCIALIZACIÓN.	165
6.2.1 Proceso de registro de usuario nuevo.	165
6.2.2 Proceso de inicio de sesión.	167
6.2.3 Registro de nueva tarjeta en el servicio.....	168
6.2.4 Operativa de solicitud de baja de una tarjeta en el servicio.....	169
6.2.5 Verificación de disponibilidad de la tarjeta en el servicio.	170
6.2.6 Borrar cuenta de usuario.....	172
6.2.7 Operativa de pago: Transacción Aprobada o Denegada.	173
6.2.8 Operativa de pago: Transacción Cancelada por el usuario.....	175
6.2.9 Operativa de pago: Timeout de usuario vencido.....	176
6.2.10 Operativa de pago: Número de teléfono no dado de alta en el servicio.	177
6.3 EVALUACIÓN DE LA EXPERIENCIA DE USUARIO.....	178
6.3.1 Presentación de los resultados	179
7. CONCLUSIONES Y TRABAJOS FUTUROS.	187
7.1 CONCLUSIONES	187
7.2 DESPLIEGUE DE LA IDEA PROPUESTA EN REDSYS.....	190
7.3 POSIBLES EVOLUCIONES DE LA IDEA PROPUESTA.....	191
7.3.1 E-Wallet: supresión de la tarjeta para la solución e-commerce.....	191
7.3.2 Extrapolación del concepto a otros escenarios	192
7.4 ALTERNATIVAS A ESTUDIAR.	193
7.4.1 Pago por referencia.....	193
7.4.2 Datos de tarjeta válidos para un solo uso (tokenización).....	193
7.4.3 Lectura de tarjeta y generación de CVV2 dinámico.....	194

III PLIEGO DE CONDICIONES	197
PLIEGO DE CONDICIONES.....	199
IV PRESUPUESTO.....	201
PRESUPUESTO.....	203
V MANUAL DE USUARIO	205
MANUAL DE USUARIO	207
VI BIBLIOGRAFÍA	215
BIBLIOGRAFÍA	217

Índice de Figuras

Figura r.1: Flujo teórico de la operativa de pago para la solución CSPay.....	28
Figura 1.1: Diagrama de pago de una transacción presencial en comercio físico con EMV CL.....	34
Figura 1.2: Diagrama de pago de una transacción no presencial en comercio electrónico.....	34
Figura 1.3: Línea de tiempo de la evolución de los medios de pago a nivel mundial.	39
Figura 1.4: Icono representativo de trueque.	40
Figura 1.5: Primera moneda acuñada con carácter oficial, siglo VI a.C., Lidia	41
Figura 1.6: Primera tarjeta de crédito (Nueva York, 1950)	42
Figura 1.7: Bacaladera VISA.....	43
Figura 1.8: Ejemplo de transacción financiera mediante la lectura de la banda magnética en TPV.	43
Figura 1.9: Tarjeta con chip EMV integrado	44
Figura 1.10: Marcas pertenecientes al organismo EMVCo.....	44
Figura 1.11: Esquema tarjeta contactless.	45
Figura 1.12: Ejemplo tarjeta dual.	45
Figura 1.13: Esquema representativo de las competencias y el alcance de EMV	46
Tabla 1.1: Número de tarjetas emitidas en la UE en los últimos años	47
Figura 1.14: Evolución de las tarjetas en circulación en España desde el año 2000	48
Figura 1.15: Esquema red financiera en España.	48
Tabla 1.2: Estadísticas Redsys con respecto a la emisión de tarjetas en España	49
Figura 1.16: Estadísticas tarjetas contactless en España (Mayo2016 a Mayo 2017)	49
Figura 1.17: Ejemplo de wearables con tecnología NFC.....	50
Figura 1.18: Tarjeta biométrica con lector de huella dactilar	50
Figura 1.19: Esquema de pago móvil presencial.....	51
Figura 1.20: Representación del parque de terminales conectados a Redsys	52
Tabla 1.3: Comparativa de las aplicaciones de pago Android Pay, Samsung Pay y Apple Pay.....	53
Figura 1.21: Resumen del uso mensual de los pagos móviles en España	55
Figura 1.22: Imagen característica que representa el comercio electrónico.	56
Figura 2.1: Estudio de eMarketer de la evolución del e-commerce (2016)	59
Figura 2.2: Evolución trimestral número de millones de transacciones de comercio electrónico	60
Figura 2.3: Preferencias de los usuarios de e-commerce encuestados en relación a los dispositivos que utilizan para realizar una compra online	61
Figura 2.4: Métodos de pago más utilizados para llevar a cabo una transacción de e-commerce . . .	61
Figura 2.5: Formulario de pago con tarjeta para comercio electrónico no seguro.....	64
Figura 2.6: Ejemplo de tarjeta inteligente con los datos sensibles destacados.	65
Figura 2.7: Procedimiento de una transacción financiera online de comercio electrónico (CNP).....	65
Figura 2.8: Representación de phishing en transacción de comercio electrónico no segura (CNP)....	66
Figura 2.9: Posibilidad de phishing en comercio electrónico seguro (Primera fase).....	67
Figura 2.10: Uso del dispositivo móvil del cliente en red de pago de e-commerce (Segunda fase)....	67
Figura 2.11: Inserción de nueva tarjeta en Paypal.....	69
Figura 2.12: Inserción de nueva tarjeta en iupay.....	71
Figura 2.13: Conocimiento de los encuestados en métodos de pago en España	72
Figura 2.14: Inserción de los datos sensibles de una tarjeta en Amazon.....	73
Figura 2.15: Representación Bitcoin	76
Figura 2.16: Evolución de la cotización de bitcoin	77
Figura 2.17: Evolución del número de transacciones diarias en bitcoins	77
Figura 3.1 Representación del fraude online en e-commerce.	80

Figura 3.2 Distribución del fraude en función del origen de la venta (%)	80
Figura 3.3. Estudio de la evolución del fraude en CNP y CP extrapolable a nivel mundial	81
Figura 3.4 Manipulación de un cajero mediante técnica de skimming.....	83
Figura 3.5. Porcentaje de transacciones financieras efectuadas mediante protocolo EMV	85
Figura 3.6. Transacción financiera con una tarjeta chip EMV mediante contactos.	87
Figura 3.7: Formato de estructura TLV.	89
Figura 3.8: Diagrama genérico de activación del protocolo e intercambio de comandos EMV CL.	94
Figura 3.9: Diagrama del kernel para el AID de MasterCard.	95
Figura 3.10: Diagrama del kernel para el AID de VISA.	96
Figura 4.1: Estructura global de la solución propuesta.....	99
Figura 4.2. Solicitud de alta de una nueva tarjeta en el servicio desde la aplicación móvil.....	102
Figura 4.3. Solicitud del número de teléfono móvil desde la página web del comercio electrónico.....	103
Figura 4.4: Desplegable de opciones de pago actuales en comercio electrónico.....	103
Figura 4.5: Opciones de pago que proporcionan los comercios electrónicos encuestados España.....	104
Figura 4.6: Solicitud del número de teléfono móvil del cliente desde la librería de Redsys.....	104
Figura 4.7: Mensajería push a través de los servidores proporcionados por Google.	105
Figura 4.8: Problemática de gestión de la mensajería push para más de una aplicación móvil.	106
Figura 4.9: Miembros del Sistema ServiRed.	108
Figura 4.10: Activación de una aplicación móvil propietaria a partir de mensajería push.	109
Figura 4.11: Descripción de los servicios integrados en el SMM.....	110
Figura 4.12: Factores de la autenticación.	111
Figura 4. 13: Protocolo de comunicación entre el móvil y la tarjeta inteligente mediante NFC.	113
Figura 4.14: Esquema NFC pasivo	114
Figura 4.15: Esquema dispositivo NFC Activo	114
Figura 4.16: Tipos de funcionamiento del dispositivo NFC.....	115
Figura 4.17: Comunicación desde el centro procesador de Redsys a la entidad financiera.	117
Figura 4.18. Esquema final de la solución propuesta.	118
Figura 4.19: Propuesta final de la nueva solución de pago para comercio electrónico.....	120
Figura 5.1. Secciones tecnológicas independientes para el desarrollo del sistema CSPay.	122
Figura 5.2: Estudio de los sistemas operativos del mercado móvil en España	124
Figura 5.3: IDE Eclipse.....	125
Figura 5.4: IDE Xamarin.	126
Figura 5.5: IDE AIDE.....	126
Figura 5.6: IDE Python.	127
Figura 5.9: IDE Unity.....	127
Figura 5.8: IDE Android Studio.	128
Figura 5.10: Flujo de trabajo estándar para el desarrollo de aplicaciones Android.....	129
Figura 5.11: Pantalla de selección de versión Android	130
Figura 5.12: Porcentaje de utilización de distintas versiones Android.....	130
Figura 5.13: Árbol de trabajo de CSPay.....	131
Figura 5.14: Permisos de utilización declarados en el manifest.....	131
Figura 5.15: Estructura POST.....	132
Figura 5.16: URL servidor.	132
Figura 5.17: Suscripción número de teléfono a Topic.	133
Figura 5.18: Esquema completo del funcionamiento de la APP.....	135
Figura 5.19: MainActivity en la APP.	136
Figura 5.20: SecondActivity en la APP.....	136
Figura 5.21: ThirdActivity en la APP.	137
Figura 5.22: FourthActivity en la APP.....	137
Figura 5.23: EsperaNFCActivity en la APP.	138
Figura 5.24: NFCActivity en la APP.	138
Figura 5.25: AltaActivity en la APP.	139
Figura 5.26: BajaActivity en la APP.....	139
Figura 5.27: VerifyActivity en la APP.	140
Figura 5.28: BorrarActivity en la APP.	140
Figura 5.29: InfoActivity en la APP.	141

Figura 5.30: Pago1Activity en la APP.....	141
Figura 5.31: Pago2Activity en la APP.....	142
Figura 5.32: Pago3Activity en la APP.....	142
Figura 5.33: Imagen de tarjeta real e impresora utilizada.....	144
Figura 5.34: Estampado tarjeta robada y tarjeta caducada.....	145
Figura 5.35: Esquema de pago con CSPay y pago móvil.....	146
Figura 5.37: Instancia creada en AWS para el servidor de pago del piloto.....	148
Figura 5.38: Definición de puertos.....	149
Figura 5.39: Conversión de claves en PuttyGen.....	149
Figura 5.40: Autenticación con el servidor para la utilización del programa WinSCP.....	150
Figura 5.41: Transferencia de archivos con WinSCP.....	150
Figura 5.42: Script de arranque.....	151
Figura 5.43: Esquema de trabajo de Amazon SNS.....	152
Figura 5.44: Ejemplo Users.txt.....	152
Figura 5.45: Ejemplo de intercambio de información entre PAN_Pendingy PAN_Authorized.....	153
Figura 5.46: Ejemplo PAN_Blacklist.txt.....	153
Figura 5.47: Ejemplo logst.txt.....	154
Figura 5.48: Ejemplo de notificación de alta.....	154
Figura 5.49: Ejemplo de notificación de pago.....	155
Figura 5.50: Barra de tareas de la web.....	156
Figura 5.51: Catálogo de la web.....	157
Figura 5.52: Posibles métodos de pago implementados en la web.....	157
Figura 5.53: Banner secuencial de la web diseñada.....	158
Figura 5.54: Método de pago del prototipo.....	159
Figura 5.55: Notificación de la web tras aprobar una transacción.....	159
Figura 5.56: Notificación de la web al intentar realizar un pago con una tarjeta no dada de alta.....	160
Figura 5.57: Notificación de la web al cancelar manualmente el pago desde el smartphone.....	160
Figura 5.58: Notificación de la web al no realizar ninguna acción desde el smartphone.....	160
Figura 5.59: Notificación de la web al intentar realizar un pago con una tarjeta caducada.....	161
Figura 5.60: Notificación de la web al intentar realizar un pago con una tarjeta que está en una blacklist.....	161
Figura 5.61: Notificación de la web al introducir un número no dado de alta en la aplicación.....	161
Figura 6.2: Flujo teórico del proceso de registro de usuario nuevo.....	165
Figura 6.3: Flujo del proceso en el demostrador para registro de usuario nuevo.....	166
Figura 6.4: Flujo teórico del proceso de inicio de sesión.....	167
Figura 6.5: Flujo del proceso en el demostrador para inicio de sesión.....	167
Figura 6.6: Flujo teórico del proceso para dar de alta una tarjeta.....	168
Figura 6.7: Flujo del proceso en el demostrador para dar de alta de tarjeta.....	169
Figura 6.8: Flujo teórico del proceso para dar de baja una tarjeta.....	169
Figura 6.9: Flujo del proceso en el demostrador para dar de baja una tarjeta.....	170
Figura 6.10: Flujo teórico del proceso para verificar una tarjeta.....	171
Figura 6.11: Flujo del proceso en el demostrador para verificar una tarjeta.....	171
Figura 6.12: Flujo teórico del proceso para borrar cuenta de usuario.....	172
Figura 6.13: Flujo del proceso en el demostrador para borrar cuenta de usuario.....	172
Figura 6.14: Operativa de pago teórica –Transacción aprobada/denegada.....	173
Figura 6.15: Operativa de pago de la demo– Transacción aprobada/denegada.....	174
Figura 6.16: Operativa de pago teórica – Transacción cancelada.....	175
Figura 6.17: Operativa de pago de la demo– Transacción cancelada.....	175
Figura 6.18: Operativa de pago teórica – Timeout usuario.....	176
Figura 6.19: Operativa de pago de la demo – Timeout usuario.....	176
Figura 6.20: Operativa de pago teórica – N° de tlf no dado de alta.....	177
Figura 6.21: Operativa de pago de la demo – N° de tlf no dado de alta.....	177
Figura 6.22: Metodología de captación de encuestados.....	178
Figura 6.23: Porcentaje de encuestados en función del rango de edad.....	179
Figura 6.24: Resultados de la encuesta sobre métodos de pago conocidos por los encuestados.....	179
Figura 6.25: Resultados de la encuesta sobre métodos de pago utilizados en e-commerce.....	180

Figura 6.26: Resultados de la encuesta de la percepción subjetiva de seguridad de los encuestados al utilizar su medio de pago electrónico habitual.....	180
Figura 6.27: Resultados de la encuesta sobre fraude online en su experiencia.....	181
Figura 6.28: Resultados de la encuesta sobre disponibilidad tarjeta contactless y smartphone con NFC.	181
Figura 6.29: Resultados de la encuesta sobre el grado de innovación de CSPay.....	182
Figura 6.30: Resultados de la encuesta sobre la facilidad de la solución.	182
Figura 6.31: Resultados de la encuesta sobre la percepción subjetiva de seguridad de CSPay.....	183
Figura 6.32: Respuesta de los encuestados a si utilizarían la solución propuesta.	183
Figura 6.33: Resultados de la encuesta de rango de edad de los encuestados con tarjeta contactless y NFC en el móvil.	184
Figura 6.34: Resultados de la encuesta sobre intención de uso de los encuestados con tarjeta contactless y NFC en el móvil.	185
Figura 6.35: Resultados de la encuesta sobre rango de edad de personas que han sufrido fraude.....	185
Figura 6.36: Resultados de la encuesta sobre la sensación de seguridad del pago actual para los usuarios que han sufrido fraude.	186
Figura 6.37: Resultados de la encuesta sobre la utilización de usuarios que han sufrido fraude....	186
Figura 7.1: e-Wallet para comercio electrónico.....	191
Figura 7.2: Incorporación de la tarjeta contactless para transferencias entre usuarios.	192
Figura 7.3: Propuesta de Tokenización de información sensible para comercio electrónico.....	194
Figura 7.4: Propuesta de implementación con CVV2 dinámico.	195
Figura m.1: Inicio de aplicación.....	207
Figura m.2: Pantalla de Inicio de Sesión.....	208
Figura m.3: Flujo “crear usuario”	209
Figura m.4: Menú principal.	210
Figura m.5: Flujo “nueva tarjeta”.....	211
Figura m.6: Flujo “eliminar tarjeta”.....	211
Figura m.7: Flujo “verificar tarjeta”.....	212
Figura m.8: Respuesta a la solicitud “verificar tarjeta”.....	212
Figura m.9: Flujo eliminar cuenta.....	213
Figura m.10: Flujo información APP.....	213
Figura m.11: Flujo de la realización del pago.....	214

Índice de Tablas

Tabla 1.1: Número de tarjetas emitidas en la UE en los últimos años.	47
Tabla 1.2: Estadísticas Redsys con respecto a la emisión de tarjetas en España	49
Tabla 1.3: Comparativa de las aplicaciones de pago Android Pay, Samsung Pay y Apple Pay.....	53
Tabla 2.1: Comparativa volumen comercio electrónico seguro y no seguro procesado en Redsys ...	68
Tabla 3.1: Identificadores financieros.	88
Tabla 3.2. Datos correspondientes a la Pista 2 almacenados en el chip integrado.....	89
Tabla 3.3: Posibles decisiones de la tarjeta en función de la decisión del terminal.....	91
Tabla 3.4: Posibles AIDs en función del Kernel	93
Tabla 6.1: Comparativa de la valoración media de los diferentes grupos de usuarios.	186
Tabla p. 1: Presupuesto de ejecución por material (PEM).....	203
Tabla p. 2: Honorarios del trabajador.	204
Tabla p. 3: Presupuesto Total del TFC	204

Glosario

- ADF: Application Definition File.
- AFL: Application File Locator.
- AID: Application IDentifier.
- AIP: Application Interchange Profile.
- AMEX: American Express.
- APP: Aplicación.
- AWS: Amazon Web Services.
- B2C: Bussines to Consumer.
- BCE: Banco Central Europeo.
- C2C: Consumer to Consumer.
- CDA: Combined DDA/Application Cryptogram Generation
- CECA: Confederación Española de Cajas de Ahorro.
- CNMC: Comisión Nacional de los Mercados y Competencia
- CNP: Card Not Present.
- CP: Card Present.
- CSPAY: Customer Self PAYment.
- CVM: Cardholder Verification Method.
- CVV2/CSC/CVC: Card Verification Value/ Card Security Code/ Card Verification Code.
- DDA: Dynamic Data Authentication.
- DES: Data Encryption Standard.
- e-commerce: Electronic Commerce.
- EMV: Europay MasterCard VISA.
- GCM: Google Cloud Messaging.
- GPO: Get Processing Options.
- HCE: Host Card Emulation.
- HTTP: Hypertext Tranfer Protocol.
- HTTPS: Hypertext Tranfer Protocol Secure.
- IC: Integrated Circuit.
- m-Commerce: Mobile Commerce
- NFC: Near Field Communication.
- NSF: National Science Fundation
- OTP: One Time Password.
- P2P: Peer To Peer.
- PAN: Personal Account Number.
- PCI-DSS: Payment Card Industry Data Security Standard.
- PRICE: Protocolo Integrado de Conexión de Establecimientos.
- PSE: Payment System Environment.
- RGPD: Reglamento General de Protección de Datos.

- RSA: Rivest, Shamir y Adleman.
- SDA: Static Data Authentication.
- SHA: Secure Hash Algorithm.
- SMS: Short Message Service.
- SNS: Simple Notification Service.
- SSL: Secure Sockets Layer.
- TFM: Trabajo Fin de Master.
- TLS: Transport Layer Security.
- TLV: Tag Length Value.
- TPV: Terminales Punto Venta.

Parte I

Resumen

Resumen

A pesar de que el e-commerce está en pleno auge, continúa siendo un entorno muy expuesto a fraude, que conlleva importantes pérdidas económicas y genera inseguridad. El objetivo del TFM es la propuesta de una solución tecnológica novedosa para la reducción de fraude y mejora de la experiencia de usuario dentro de los medios de pago. La propuesta, denominada *CSPay*, consiste en hacer análoga la compra online a la presencial, incorporando la presencia de la tarjeta contactless y del protocolo EMV en un contexto financiero donde, hasta la fecha, no se había contemplado, aportado mayor seguridad al pago en Internet.

Palabras clave: e-commerce, fraude, medios de pago, contactless, EMV.

Abstract

Despite the e-commerce is rising at the moment, it is still a highly exposed to fraud environment, which entails major economic losses and a climate of insecurity. The objective of this project is to provide an original technological solution to reduce fraud and improve user experience of payment methods. The proposal, named *CSPay*, consists in mimicking traditional shopping in the online world, incorporating the presence of a contactless card and the EMV protocol in a financial context, which so far has not been contemplated it. This results in an increase of the online payments security level.

Keyword: e-commerce, fraud, payment methods, contactless, EMV.

Resumen extendido

Se define el comercio electrónico o *e-commerce* como la adquisición de bienes o servicios a través de Internet, utilizando como forma de pago los medios electrónicos. En la sociedad actual el comercio online está viviendo una época de máximo esplendor, aumentando de forma exponencial el número de transacciones financieras llevadas a cabo año tras año. Todos los estudios de mercado convergen en las predicciones y estadísticas del futuro de este sector, considerando el comercio electrónico como el foco de atención de la economía mundial por su gran potencial de evolución y crecimiento emergente.

Los medios de pago para operaciones de *e-commerce* adquieren un papel fundamental, ya que son las soluciones tecnológicas que sustentan y permiten establecer las compras y ventas por Internet. Actualmente conviven múltiples soluciones de pago online en el mercado virtual que presentan una finalidad común, que el cliente liquide el valor de su compra de forma rápida y segura. Sin embargo, no parece que por el momento exista el método de pago ideal que haya conseguido los dos propósitos anteriores.

Al igual que el comercio electrónico está en pleno auge, el fraude en este entorno también ha experimentado un crecimiento muy significativo en los últimos años, convirtiéndose en una problemática de interés social a nivel internacional que conlleva importantes pérdidas económicas anuales. Las transacciones de pago en comercios online están muy expuestas a fraude, ya que los ciberatacantes detectan más vulnerabilidades en este entorno respecto a la robustez actual que garantiza el pago presencial con tarjeta.

Cabe destacar que los medios de pago de los comercios físicos sufrieron una importante revolución tras la migración de las tarjetas financieras de banda magnética a las tarjetas inteligentes con chip integrado. La evolución del formato de la tarjeta fue el desencadenante de la aparición del protocolo de comunicación EMV (Europay, MasterCard y Visa) para el intercambio de información segura entre TPV (Terminales Punto de Venta) y las tarjetas inteligentes. A partir de la expansión de la tarjeta chip y de la utilización del protocolo EMV, las tasas de fraude en comercio presencial se minimizaron notablemente, convirtiéndose el comercio electrónico en el nuevo objetivo de los ataques fraudulentos.

Dado este contexto, se propone una idea original para la reducción de fraude y mejora de la experiencia de usuario en un escenario de comercio electrónico, que pueda ser integrada en los sistemas de pago electrónico disponibles en la actualidad. La solución se centra en la incorporación de la tarjeta contactless financiera y del protocolo EMV en el flujo de pago de una transacción e-commerce a través de Internet. El objetivo es hacer análoga la compra online a la presencial, trasladando al medio virtual los beneficios de seguridad y experiencia de usuario que ofrecen las transacciones en los comercios físicos.

Para incorporar la tarjeta contactless en un entorno online, se necesita un dispositivo con NFC que pueda establecer la comunicación pertinente con la tarjeta física, integrando el protocolo de comunicación EMV Contactless. Por este motivo, la utilización del nuevo método de pago implica el uso del dispositivo móvil del cliente, con sistema operativo Android y tecnología NFC, con el fin de llevar a cabo la lectura de la tarjeta contactless. El hecho de que sea el propio cliente quién de forma autosuficiente lleve a cabo el pago en *e-commerce* gracias a su dispositivo móvil y a su tarjeta contactless, otorga el nombre a la nueva solución propuesta, denominada *CSPay*, por sus siglas en inglés, *Customer Self Pay*.

La utilización de este nuevo método de pago requiere que los usuarios instalen la aplicación *CSPay.apk* en su dispositivo móvil y completen el registro en el servicio. Una vez superada la fase de enrolamiento, se describe el flujo de operatividad nominal en una transacción de comercio electrónico empleando la nueva propuesta (ver *Figura r.1*). La solución consiste en la inserción del número de teléfono móvil del cliente, en vez de los datos sensibles asociados a la tarjeta (PAN, fecha de caducidad y CVV2), en el formulario de pago de la página web de un comercio electrónico. Por lo tanto, se considera que esta solución eliminaría los ataques asociados a técnicas como *phishing* y *pharming*, mejorando la seguridad de la transacción financiera. El titular, tras la inserción de su número de teléfono en el formulario de pago web, recibe una notificación push en la aplicación *CSPay* instalada en su dispositivo móvil.

Para completar el pago en el dispositivo móvil, el usuario debe realizar una primera autenticación en la aplicación móvil, a través de su huella dactilar o mediante una contraseña previamente establecida. Tras esta primera autenticación, tiene que aproximar su tarjeta contactless al lector NFC del dispositivo móvil, emulando el gesto que se realiza en una compra con tarjeta contactless en un establecimiento físico. De forma seguida, se notifica al usuario el resultado de la transacción financiera a través de la página web que originó la petición de pago.

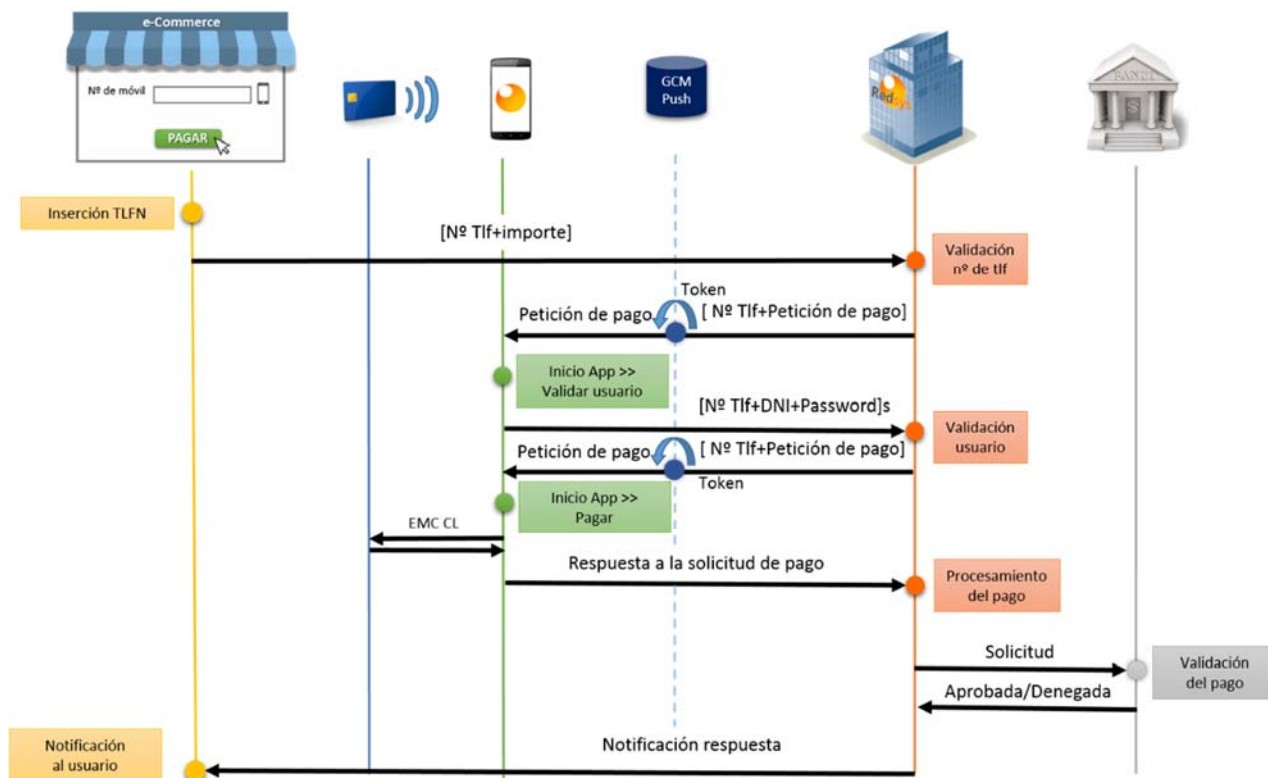


Figura r.1: Flujo teórico de la operativa de pago para la solución *CSPay*.

La definición de la propuesta es el resultado de un profundo estudio del contexto de los medios de pago en el mundo y de un reflexivo análisis de las oportunidades tecnológicas existentes para su implementación, estableciendo una toma de decisión por cada alternativa que podía tener lugar en el desarrollo de la idea.

Con el fin de verificar la viabilidad técnica de la propuesta, se desarrolla un demostrador completo que integra todos los elementos característicos de la solución *CSPay*, como son: la aplicación móvil del cliente, el servidor que emula el procesamiento de transacciones financieras y una página web que realiza las funciones de un comercio electrónico. Además, se utilizan distintos perfiles de tarjetas contactless, con el fin de disponer de diversas casuísticas funcionales (tarjetas caducadas o fraudulentas).

Para conocer la experiencia de usuario que transmite la nueva solución de pago y medir el grado de aceptación que podría presentar *CSPay*, se distribuye una encuesta a cien personas con el fin de que evalúen la innovación, la usabilidad y la sensación de seguridad que ofrece el nuevo método. Los resultados son muy satisfactorios, ya que se obtiene una alta aceptación por parte de la población entrevistada. Este hecho es muy significativo, ya que es tan importante conseguir un método de pago seguro como que la seguridad subjetiva que experimenta el cliente sea la adecuada.

Parte II

Memoria

Capítulo 1

Introducción

El *comercio electrónico* o *e-commerce*, consiste en la adquisición de bienes o servicios a través de Internet, utilizando como forma de pago medios electrónicos. En la sociedad actual el comercio electrónico está en pleno auge, dada la facilidad, comodidad y flexibilidad que ofrecen los pagos por internet. Además, los estudios de mercado revelan que seguirá creciendo vertiginosamente en los próximos años. Sin embargo, todavía es muy vulnerable al fraude, lo que mantiene activa una importante línea de trabajo en la búsqueda de nuevas soluciones en el ámbito de los medios de pagos.

El proyecto presenta una problemática tecnológica y de negocio de interés mundial, con el fin de proponer y desarrollar una idea innovadora que reduzca el fraude y mejore la experiencia de usuario. Se requiere que el nuevo método de pago utilice con acierto la tecnología, sea sencillo y refuerce la seguridad objetiva así como la percepción de la misma, mejorando la experiencia de usuario (no solo debe ser seguro, también ha de transmitir esa sensación). Por estos motivos se propone como solución emular la compra online (ver *Figura 1.1*) con la presencial (ver *Figura 1.2*), incorporando la presencia física de la tarjeta contactless en las transacciones llevadas a cabo mediante comercio electrónico.

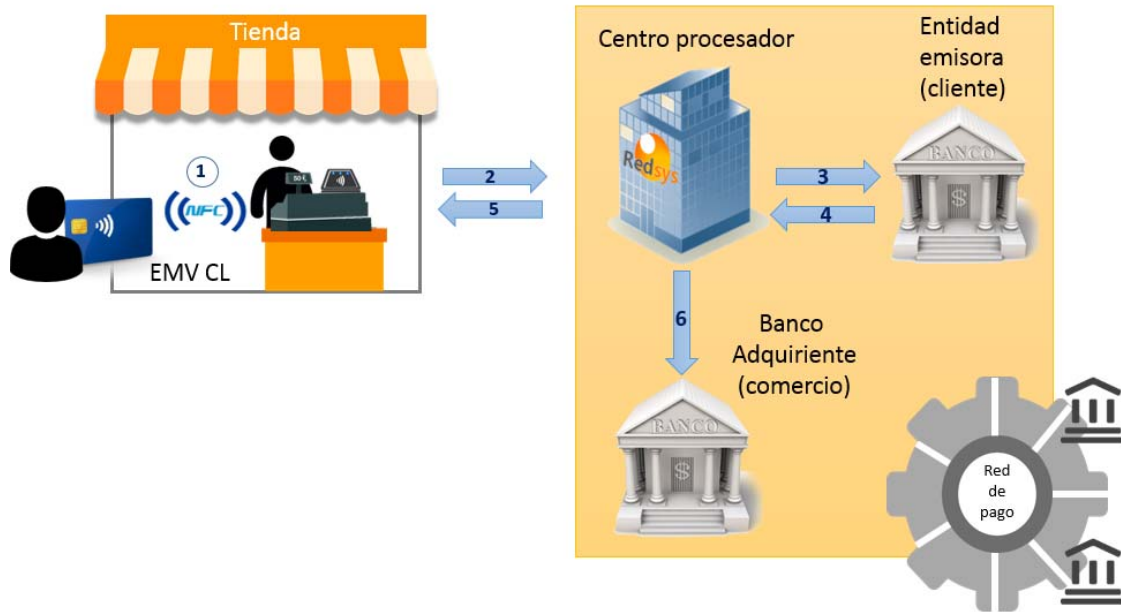


Figura 1.1: Diagrama de pago de una transacción presencial en comercio físico con EMV CL.

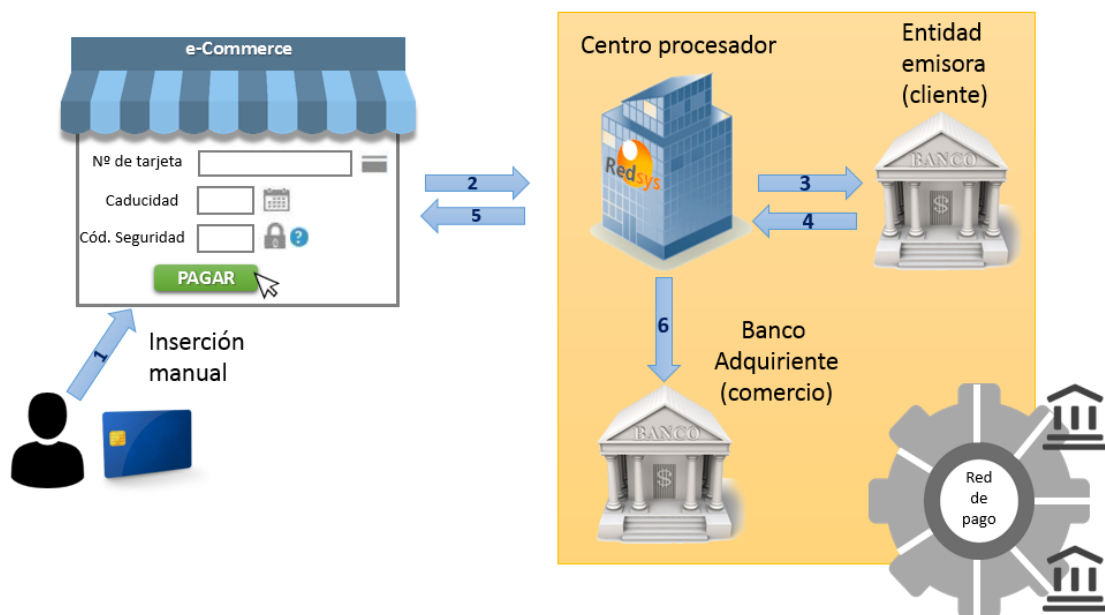


Figura 2.2: Diagrama de pago de una transacción no presencial en comercio electrónico.

Se observa que ambos escenarios los *stakeholders* que participan en el esquema de la red de pago nacional son los mismos:

- **Usuario:** Cliente de una entidad emisora que desea llevar a cabo una transacción financiera a través de su tarjeta en un comercio.
- **Entidad emisora:** Banco que proporciona una tarjeta de pago, ya sea de crédito o débito, a su cliente. Las operaciones efectuadas con dicho instrumento de pago se liquidarán, habitualmente, en la cuenta corriente que el titular de la tarjeta haya designado a tal efecto.

- **Centro procesador de transacciones financieras:** Compañía encargada de gestionar la interconexión entre las distintas entidades financieras que participan en una transacción y conectar en el resto de elementos involucrados en el pago. Tiene la misión de comprobar la fiabilidad de la transacción, la verificación de los datos del cliente y la autorización por parte de la entidad emisora. En España existen las procesadoras de CECA y Redsys (con un volumen transaccional del 91,6% de la adquirencia total en España).
- **Comercio:** Establecimiento que desea vender un artículo a un usuario y contrata a un bando adquirente para disponer de las herramientas necesarias para efectuar una transacción financiera.
- **Entidad adquirente:** Banco que facilita a un comercio el TPV a través del cual tendrá lugar la captación de los datos relevantes de las tarjetas de los clientes a efectos de autorizar la transacción de pago.
- **Red de pago:** Sistema constituido por diferentes entidades y una procesadora de pago que posibilita y favorece la comunicación de las transacciones financieras.

De tal forma que, si se propone incorporar la presencia de la tarjeta física en el flujo transaccional de comercio electrónico, será necesario disponer de una herramienta que permita realizar una lectura segura de los datos de la tarjeta contactless, es decir, que emule en cierto modo el funcionamiento del TPV. El elemento que puede satisfacer estas condiciones y se ha seleccionado en la solución propuesta, es el propio dispositivo móvil del cliente, que deberá disponer de tecnología NFC y sistema operativo Android para poder utilizar este servicio.

En este capítulo se presenta la motivación y el entorno de trabajo, así como los objetivos del proyecto y la estructura del mismo. Por último, se hace una reseña histórica de la evolución del comercio que permita centrar la situación actual del comercio electrónico en el que versa el presente trabajo.

1.1 MOTIVACIÓN Y ENTORNO DE TRABAJO

El presente TFM se enmarca dentro del área tecnológica de los medios de pago, un campo de estudio habitualmente desconocido para las personas ajenas a dicho sector, pero de aplicación diaria y de uso común. La motivación, para llevar a cabo una idea perteneciente a un ámbito tan específico, responde a una experiencia laboral de cuatro años en el sector de los medios de pago. En este tiempo el autor ha participado en importantes proyectos de ingeniería tanto para CECA (Confederación Española de las Cajas de Ahorro) como para Redsys, donde está desarrollando su trayectoria profesional actualmente.

Redsys es la compañía líder en medios de pago a nivel nacional, con 35 años de experiencia como centro procesador y prestación de servicios de pago a las entidades financieras. El estar dentro de este entorno ha permitido identificar pros y contras, así como posibles oportunidades. Dentro del ámbito tecnológico-financiero, el proyecto se centra en la temática del comercio electrónico y se define como el estudio inicial de viabilidad técnica de una nueva solución de pago, acompañada de un demostrador que puede servir como base para el despliegue real de la solución dentro de la compañía. La elección del tema viene motivada por los siguientes condicionantes:

- El comercio electrónico está en plena expansión, con un incremento exponencial del número de transacciones online en los últimos años y con vistas a un continuo crecimiento.
- Las tasas de fraude en e-commerce son muy elevadas en comparación con el comercio presencial, donde a día de hoy la tarjeta inteligente es la protagonista. Cabe destacar que a raíz de la migración de la banda magnética a las tarjetas chip, se produjo un refuerzo muy significativo en la seguridad del comercio presencial y por lo tanto los ataques fraudulentos se focalizaron en el entorno de comercio electrónico.
- Es un negocio sujeto a cambios que se puede ver afectado por dos grandes elementos transversales, la regulación y la seguridad. En el año 2018 entran en vigor nuevas normativas que priorizan la fase de autenticación del cliente a la rapidez de la transacción.

La aceptación de colaboración por parte de Redsys ha sido fundamental en el desarrollo del trabajo puesto que ha permitido utilizar parte de su infraestructura, así como el apoyo directo de D. Álvaro Martín, Jefe del Departamento de Emisión y Chip. Asimismo, el interés mostrado por la solución propuesta respalda la idea original y deja abierta una puerta para su posible materialización.

1.2 OBJETIVOS

El principal objetivo del proyecto es la propuesta y el desarrollo de una nueva solución de pago con carácter innovador que pueda ser integrada en los sistemas de comercio electrónico actuales, con el fin de reducir la elevada tasa de fraude y mejora la experiencia de usuario.

Para lograr la finalidad última del presente trabajo es necesario conseguir una serie de objetivos parciales que se exponen a continuación:

- Análisis del panorama actual de los medios de pago y antecedentes históricos con el fin de evaluar el impacto de la transformación social y económica en la sociedad para determinar el marco del proyecto.
- Definición y comparativa de las vulnerabilidades existentes en las transacciones CNP (Card Not Present) en relación a CP (Card Present), con el fin de justificar la necesidad de implementar una solución alternativa a las actuales para un escenario e-commerce.
- Estudio y desarrollo de una nueva solución de pago robusta para comercio electrónico basada en la utilización del protocolo EMV. Además, deberá ser lo suficientemente atractiva para que sea aceptada por parte de las entidades financieras, los propietarios de los comercios electrónicos y los titulares de las tarjetas financieras. Se debe contemplar que el procedimiento sea sencillo, seguro e innovador para así mejorar la experiencia de usuario.
- Despliegue de un entorno de simulación completo con el fin de entender el funcionamiento de la solución final. Para ello, se implementará una demo explicativa de concepto.

1.3 ESTRUCTURA

Se presenta la memoria del proyecto distribuida en las siguientes secciones, incluyendo una breve descripción del contenido de cada una de ellas.

- **Capítulo 1: *Introducción.***
Se presenta una visión general de la evolución a lo largo del tiempo de los medios de pago a nivel mundial, con el fin de conocer el marco histórico y la transformación social y tecnológica que está sucediendo en la actualidad.
- **Capítulo 2: *Estado del arte del comercio electrónico.***
Se describen las soluciones de pago más recientes y pioneras disponibles en el sector técnico y financiero para llevar a cabo transacciones mediante comercio electrónico, analizando las ventajas y carencias de cada una de ellas.
- **Capítulo 3: *Fraude en e-commerce y seguridad del Protocolo EMV.***
Se estudian los distintos tipos de fraude en comercio electrónico, estableciendo una comparativa con la tasa de fraude en comercio presencial. Se describen las funcionalidades básicas del protocolo EMV justificando su importancia en el sector.
- **Capítulo 4: *Análisis técnico de la solución y propuesta CSPay.***
Se analizan los requerimientos que debe satisfacer la nueva solución de pago, evaluando las diferentes posibilidades existentes de diseño, con la finalidad de tomar la decisión que más se adapte a las expectativas depositadas en la implementación de la idea.
- **Capítulo 5: *Solución tecnológica del demostrador CSPay.***
Se definen en profundidad las cuatro secciones tecnológicas que constituyen la propuesta de pago, detallando los pasos a seguir para la implementación independiente de cada uno de los módulos antes de la integración del sistema.
- **Capítulo 6: *Implementación del demostrador CSPay.***
Se representan los diagramas funcionales con el resultado esperado de la propuesta teórica y la adaptación del comportamiento del piloto ante los mismos escenarios. Se revisa de manera crítica el funcionamiento de la demo y se emite una encuesta para valorar el impacto de la solución en la sociedad.
- **Capítulo 7: *Conclusiones y trabajos futuros.***
Se exponen las deducciones obtenidas en la realización del TFM y se proponen diferentes evoluciones y alternativas tecnológicas de pago, en las cuales, se podría profundizar la investigación enfocando, de este modo, nuevos proyectos.

1.4 RESEÑA HISTÓRICA DEL COMERCIO

Se define el comercio como una práctica natural del ser humano, que consiste en el intercambio de bienes y/o servicios entre varias partes interesadas, independientemente del método y/o la tecnología empleada para este fin [1]. La historia de los medios de pago, está directamente relacionada con el progreso de la actividad económica. De tal forma que se establece un lazo bidireccional: la innovación en los sistemas de pago ha favorecido históricamente el desarrollo económico y viceversa, ya que el avance de la economía y las expectativas de los seres humanos han condicionado la evolución tecnológica de los sistemas de pago, teniendo la ingeniería un rol fundamental en el sector financiero.

A continuación, se muestra una línea de tiempo que engloba las principales innovaciones a lo largo de la historia de los medios de pago en el mundo, tanto para el pago en comercio físico como electrónico. Ver *Figura 1.3*.



Figura 1.3: Línea de tiempo de la evolución de los medios de pago a nivel mundial.

1.4.1 Evolución y despliegue del comercio presencial

El origen de los medios de pago no se puede determinar con exactitud dentro de la historia de la humanidad, ya que el comercio, como actividad socioeconómica, ha estado presente desde que el ser humano comenzó a ser productivo en técnicas de ganadería, agricultura y artesanía.

Fuentes de información históricas determinan que fue en el Neolítico (9000 a.C – 4000 a.C) cuando se abandonó la idea del trabajo ligado únicamente a la subsistencia y se exploró una nueva forma de ingeniería social, iniciando los fundamentos básicos del concepto del comercio y de la política de negocio.

Este desarrollo social surgió gracias a una evolución tecnológica, ya que, la incorporación de nuevas herramientas en el trabajo diario del ser humano, facilitó el crecimiento de la producción de ciertos bienes como, por ejemplo, las cosechas. La sobreproducción de un mismo servicio dentro de una comunidad, denominado excedente, desencadenó que parte de la población se especializara en otros cometidos como la alfarería, la siderurgia, etc.

El excedente de un mismo bien dentro de una comunidad y la aparición de nuevos servicios en otras comunidades, propiciaron el intercambio natural y libre de objetos entre distintos individuos, dando lugar al trueque. Además de dicho intercambio, el trueque desembocó el concepto de la división del trabajo, la propiedad privada y la riqueza, así como las primeras estratificaciones sociales [2]. Ver *Figura 1.4*.



Figura 1.4: Icono representativo de trueque.

Una de las dificultades del trueque fue la ausencia de la unidad de valor exacto como referencia objetiva para la negociación de productos y cantidades asociadas a los mismos en el momento del intercambio. Este hecho provocó que primase el valor simbólico de la necesidad de adquisición de un producto, que el precio y el esfuerzo real que hay detrás del mismo.

El inconveniente más notable del trueque, es que no siempre se encontraba a alguien que accediera a intercambiar el producto deseado por aquel que podría ofrecerse. Este escenario recibe la denominación del problema de la doble conciencia de las necesidades.

Para la resolución de dichas desventajas y fomento del comercio, surgió el intercambio de sal, joyas y piedras preciosas como valor universal para la adquisición de otros bienes. No fue hasta prácticamente siglo VI a.C, coincidiendo con la edad de los metales, cuando las primeras monedas acuñadas con carácter oficial tomaron protagonismo. Ver *Figura 1.5*.



Figura 1.5: Primera moneda acuñada con carácter oficial, siglo VI a.C., Lidia (Turquía en la actualidad)

Durante la primera parte de la historia, la moneda presentaba el valor de su composición, siendo el oro y la plata los metales más cotizados en todas las sociedades. Sin embargo, tras la monumental expansión del uso de la moneda como forma principal de pago, fue necesario remodelar el sistema, debido a la escasez y difícil adquisición de estos materiales.

Dadas estas condiciones, se evolucionó a un sistema monetario denominado Patrón Oro (coexistiendo con el Patrón Plata) que fue empleado en el transcurso del siglo XIX y terminó como consecuencia de la Primera Guerra Mundial. El fundamento de este sistema era que cuando el propietario lo requiriese, podía solicitar la conversión de su divisa a oro y viceversa. De esta manera, los ciudadanos podían intercambiar libremente oro y realizar transacciones en cualquier nación, ya que la equiparación divisa original – oro – divisa final permitía y facilitaba el cambio de moneda.

Sin embargo, era un sistema económico insostenible, ya que los bancos centrales tenían la responsabilidad de mantener y ajustar constantemente sus reservas de oro, que se veía afectada por la variación del precio de dicho metal. Este hecho dificultaba la acción del gobierno por alterar la política económica de cada nación y frenaba el crecimiento tras la guerra.

Finalmente, se optó por la desvinculación del valor de los metales al precio de la moneda, surgiendo de esta forma el dinero fiduciario, modelo de comercio que utilizamos en la actualidad. Se define como un sistema basado en la confianza y creencia de una sociedad en la valoración otorgada a distintas monedas y billetes de forma representativa y no por el material que lo componen.

El dinero fiduciario es emitido y gestionado por los bancos centrales de cada país y supranacionales (como el Fondo Monetario Internacional, el Banco Central Europeo de Inversiones y otras organizaciones similares), que se encargan de velar por la autenticidad y confianza de los usuarios en el sistema de pago definido.

La utilización de la moneda como medio de pago de valor simbólico, propició la creación y/o el uso de otros métodos transaccionales (para la adquisición de bienes) con carácter representativo pero de reconocimiento generalizado. Entre otros, destaca la aparición de las tarjetas, los cheques, los pagarés y demás documentos legales monetarios.

De esta manera, se enmarca a principios del siglo XX el inicio de una revolución sin precedentes en el mundo de los medios de pago, con la tarjeta de crédito como protagonista.

Las primeras tarjetas fueron de papel y estaban destinadas a exclusivos clientes, con alto nivel adquisitivo y social, que se les permitía abonar sus facturas a posteriori, emulando el comportamiento de las tarjetas de crédito que se utilizan en la actualidad. Dichas tarjetas vinculaban a un comercio concreto (en este caso, fueron las empresas petroleras y algunas cadenas de hoteles pioneras en la utilización de este sistema) con un único cliente.

Las guerras y conflictos de la época frenaron la evolución de este método de pago y fue tras la Segunda Guerra Mundial cuando se popularizaron las tarjetas entre las instituciones bancarias de entonces. Se dice que el promotor de la tarjeta de crédito, como herramienta intermediaria entre diferentes comercios y los clientes (concepto novedoso hasta la fecha), fue Frank X. McNamara, fundador de la empresa Diners Club en 1950 [3]. Ver *Figura 1.6*.

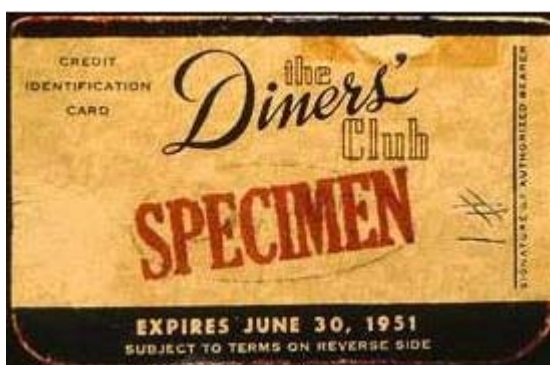


Figura 1.6: Primera tarjeta de crédito (Nueva York, 1950) [4].

Se dice que la idea surgió en una cena en un famoso restaurante de Nueva York, cercano al Empire State Building, en 1949, dónde el Sr. McNamara discutía con dos amigos sobre un problema que tenía con un cliente de la empresa Hamilton Credit Corporation, de la que era el director y el concedente de los créditos.

Al finalizar la cena, el Sr. McNamara se sorprendió al descubrir que no disponía de dinero en efectivo, y tuvo que llamar a su mujer para que se acercase hasta el restaurante y abonase la cuenta. De una situación embarazosa surgió la brillante idea de disponer de una única tarjeta de crédito para su utilización en diferentes establecimientos y comercios.

Las primeras tarjetas de crédito Diners Club fueron entregadas a 200 personas y estaban materializadas en papel, con las condiciones de utilización y el listado de comercios que con contemplaban su aceptación en el reverso. Los beneficios del uso de esta tarjeta se expandieron rápidamente, y a finales de 1950 más de 20.000 personas hacían uso de dicha tarjeta. En el año 1952, Diners se convirtió en marca internacional, y en 1954 se instauró en España.

En los años posteriores aparecieron en el mercado nuevos emisores de tarjetas de crédito que reforzaron la competitividad y eficiencia en el sector de los medios de pago, surgiendo modalidades de pago más interesantes.

Entre los años 60, destacan, entre otros emisores, las marcas que actualmente se conocen como MasterCard (Interbank Card Association y EuroCard, con su primera tarjeta en 1951), VISA (tarjeta BankAmericard del Bank of America con su primera tarjeta emitida en 1958) y American Express (AMEX, 1958).

El primer objetivo que se anhelaba conseguir, y finalmente se logró, fue la aceptación universal de las tarjetas de crédito y débito emitidas, sin presentar limitación geográfica ni contextual.

Para este fin, el primer cambio notable que tuvieron que experimentar las tarjetas fue el material de su fabricación, evolucionando del papel al plástico. Cabe destacar que, las primeras tarjetas de crédito, tenían estampado en relieve los datos sensibles del titular de la tarjeta: número de tarjeta, fecha de efectividad, fecha de caducidad y nombre del titular. Se estableció este diseño porque los establecimientos disponían de un dispositivo sencillo, denominado *bacaladera*, que permitía la captura manual de la información con relieve y generaba un recibo con los datos del cliente y el importe de la operación. Ver *Figura 1.7*.



Figura 1.7: Bacaladera VISA.

El formato de la tarjeta fue ligado a la evolución de nuevos dispositivos electrónicos que permitían la lectura de los datos y evitaban tanto las tareas manuales como la compartición directa de los datos sensibles del titular con un tercero (en este caso, el comerciante).

El almacenamiento de los datos sensibles del titular en la banda magnética de una tarjeta se popularizó en los años 70. Los terminales punto de venta (TPV) disponían únicamente de un lector de banda que permitían obtener la información y habilitaban la comunicación con el centro autorizador para el envío del mensaje de la petición de aprobación online con los datos recuperados del cliente. Ver *Figura 1.8*.

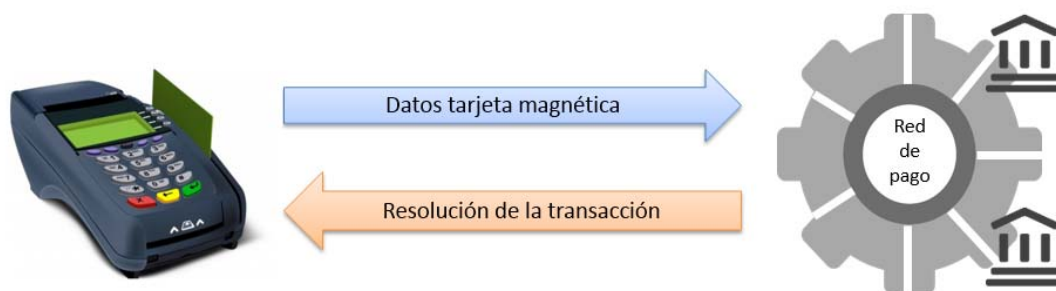


Figura 1.8: Ejemplo de transacción financiera mediante la lectura de la banda magnética en un TPV.

Aunque el escenario anterior fue un gran avance, presentaba carencias en términos de seguridad, integridad y robustez en la gestión de los datos sensibles del titular. De esta manera, surgió la necesidad de rediseñar el formato de la tarjeta financiera, con el fin de reducir el fraude resultante de la falsificación, clonación, pérdida y robo de las tarjetas de banda magnética pura.

Dado el planteamiento anterior, se identifica la revolución real de las tarjetas y, por consiguiente, de los medios de pago, con la integración del microprocesador en las tarjetas financieras, que pasarían a denominarse *Smart Card*. Ver *Figura 1.9*.

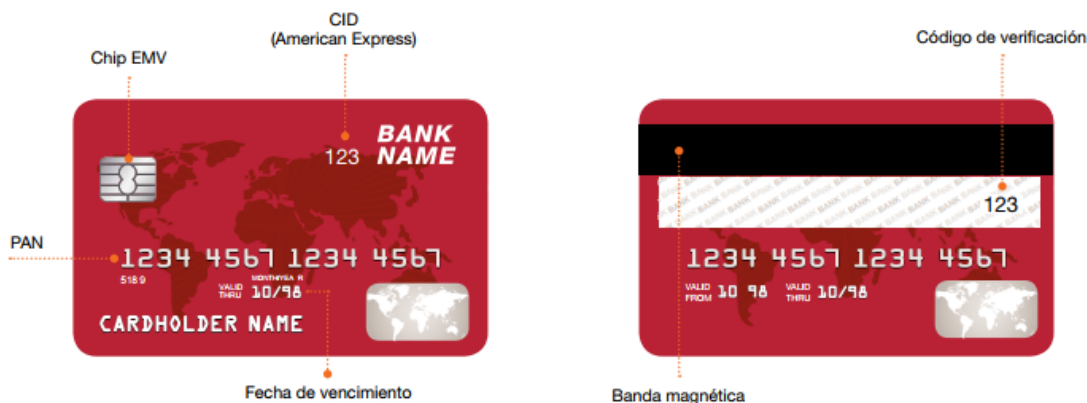


Figura 1.9: Tarjeta con chip EMV integrado [5].

Las especificaciones que definen el protocolo de comunicación entre las tarjetas con chip y los TPV, se bautizaron con el acrónimo de EMV, publicando la primera normativa en 1996. Esta denominación tiene su origen en las iniciales de las potentes marcas financieras que definieron el estándar de interoperabilidad segura a nivel mundial entre las tarjetas inteligentes y los terminales punto de venta: Europay (que fue absorbida posteriormente por MasterCard), MasterCard y Visa [6].

Las tres compañías crearon de forma conjunta el organismo conocido como EMVCo, fundado en 1999, que desde entonces ha ido creciendo y evolucionando con el objetivo de velar por la generación, mantenimiento, actualización y cumplimiento de las normativas EMV. En la actualidad, EMV presenta una adaptación mundial y el organismo EMVCo está formado por: American Express, Discover, JCB, Mastercard, UnionPay y VISA. Ver *Figura 1.10*.



Figura 1.10: Marcas pertenecientes al organismo EMVCo.

En España, la popularidad actual de dichas marcas financieras se establece en función del volumen de tarjetas emitidas y acorde con la utilización de las mismas, siendo por orden de importancia, VISA, MasterCard y American Express, las pioneras en el ámbito nacional.

EMVCo también cuenta con el respaldo de otros *stakeholders* como, por ejemplo, numerosos bancos, procesadores de pago, laboratorios de certificación y fabricantes de TPV y tarjetas inteligentes, que participan como *EMVCo Associates*. Entre otros socios, destaca la participación en España de EURO6000 y Redsys.

Con la evolución de la tecnología y la transformación de los intereses sociales de los ciudadanos, las entidades y las marcas financieras focalizaron sus esfuerzos en la mejora de la tarjeta inteligente a un nuevo servicio de pago que primase la comodidad, rapidez y experiencia de usuario, sin renunciar a las ventajas y prestaciones que garantiza EMV, como la robustez y seguridad. De esta forma, tuvo lugar la tarjeta contactless aplicada al mundo financiero. Ver *Figura 1.11*.

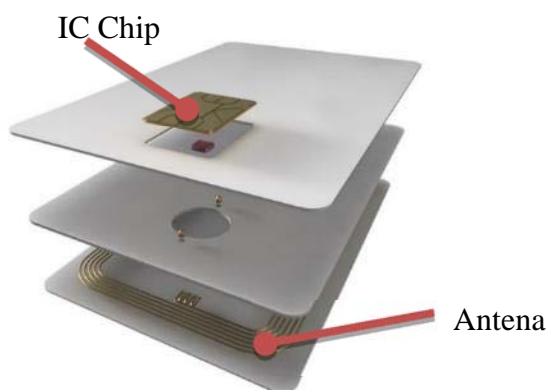


Figura 1.11: Esquema tarjeta contactless.

Las tarjetas sin contactos, por lo general, son duales. Esta afirmación indica que dichas tarjetas pueden ser utilizadas mediante su inserción en el lector de chip del terminal de pago, o bien mediante la aproximación de la misma al lector NFC del terminal. Ver *Figura 1.12*.



Figura 1.123: Ejemplo tarjeta dual.

Aunque la primera tarjeta con tecnología sin contactos fue en el año 1996 (para la venta de billetes electrónicos en Corea del Sur), no se adaptó de forma globalizada y en el ámbito puramente financiero hasta estos últimos años atrás. EMVCo publicó el primer borrador que contenía información sobre la tecnología contactless en el año 2007 y de forma progresiva fue describiendo el comportamiento del terminal adaptado a los diferentes requerimientos de cada una de las marcas financieras.

Dado que los diferentes organismos no llegaron a un acuerdo en lo que se refiere a la operativa sin contactos de las tarjetas financieras, EMVCo acabó publicando siete especificaciones independientes (en función del kernel de la tarjeta) con el fin de describir el comportamiento del terminal ante la captación de una tarjeta u otra en su campo de radiofrecuencia. En la *Figura 1.13* se puede observar el alcance de EMV y en el *Capítulo 3* se amplía información al respecto.

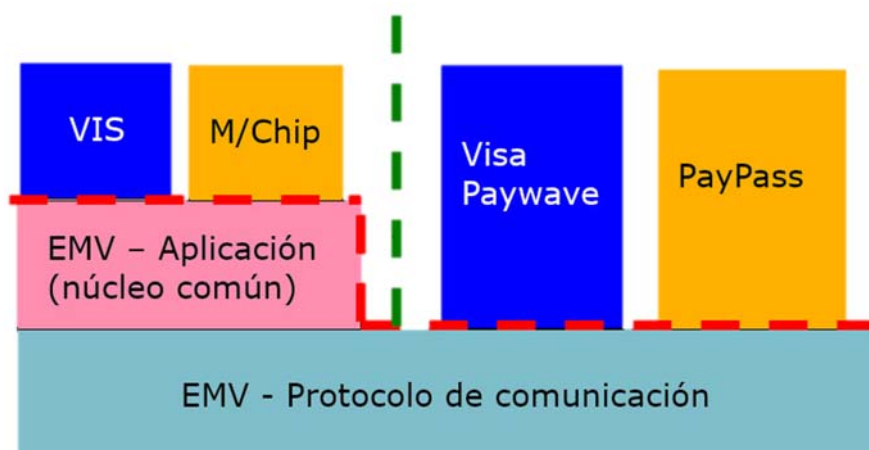


Figura 1.13: Esquema representativo de las competencias y el alcance de EMV.

Cabe destacar que, en el mercado tradicional español, no fue hasta 2012 cuando se inició el primer despliegue de esta nueva tecnología sin contacto en el campo de los medios de pago. Desde entonces, la expansión de las tarjetas contactless ha crecido a un ritmo exponencial, afianzándose en el sector financiero como un método cómodo, rápido y seguro para completar una transacción y compatible con la interfaz con contactos.

La División de Medios de Pago e Infraestructura de Mercado del Banco de España permite consultar de forma pública, en su página web [7], los informes que describen el balance de la situación anual y el progreso de la actividad trimestral de los sistemas de pago en España y en Europa.

En la *Tabla 1.1* se puede observar el número de tarjetas financieras (sin hacer diferencia a la interfaz soportada) emitidas en los últimos años en cada uno de los países que conforman la Unión Europea.

10.1 Number of cards issued by resident payment service providers (cont'd)

(thousands; end of period)

	Cards with a payment function (except cards with an e-money function only)				
	2011	2012	2013	2014	2015
Belgium	20,005.19	20,647.08	20,041.34	21,949.24	22,587.89
Bulgaria	7,985.70	8,259.63	7,736.46	7,227.08	7,152.64
Czech Republic	9,814.91	10,166.59	10,391.88	10,989.13	11,840.72
Denmark	8,111.46	8,275.45	8,449.68	8,926.15	9,776.21
Germany	130,096.63	133,188.18	133,852.03	135,444.66	138,851.82
Estonia	1,778.06	1,787.33	1,790.79	1,814.44	1,829.35
Ireland	5,907.21	6,044.44	6,238.04	6,164.05	6,220.05
Greece	13,836.55	13,367.31	13,859.27	12,516.75	13,567.57
Spain	68,969.51	68,799.65	69,749.37	67,993.67	70,252.17
France	83,005.30	82,313.04	82,222.68	81,040.21	77,406.43
Croatia	-	-	8,687.69	8,472.65	8,554.33
Italy	67,355.24	68,180.10	71,786.32	73,642.12	77,154.03
Cyprus	1,313.82	1,271.57	1,120.06	976.44	1,095.36
Latvia	2,322.86	2,380.86	2,378.17	2,326.46	2,373.10
Lithuania	3,886.10	3,632.63	3,588.45	3,520.13	3,490.97
Luxembourg	1,693.51	1,953.74	2,009.91	2,119.81	2,151.72
Hungary	8,887.85	8,908.45	8,932.24	8,869.56	8,952.84
Malta	729.16	786.55	811.13	837.56	861.22
Netherlands	30,455.79	30,510.47	30,453.66	31,966.49	32,374.61
Austria	11,014.16	11,413.78	11,840.46	12,162.13	12,354.90
Poland	32,044.95	33,100.06	34,658.65	36,068.82	35,209.04
Portugal	20,119.63	20,317.11	18,691.84	18,623.66	18,343.39
Romania	13,348.53	13,705.01	14,147.05	14,446.18	14,874.55
Slovenia	3,284.97	3,294.11	3,266.38	3,155.33	3,365.30
Slovakia	5,337.23	4,603.65	4,782.24	5,259.73	5,456.94
Finland	7,824.71	7,862.36	7,788.70	8,957.65	9,392.76
Sweden	21,107.00	21,336.00	21,969.00	22,100.00	21,728.92
United Kingdom	147,235.00	151,600.00	157,339.00	159,013.00	163,470.00
Euro area total	472,726.65	476,340.46	480,304.20	486,950.38	499,129.56
EU total	727,471.01	737,705.14	758,582.48	766,583.08	780,688.81

Tabla 1.1: Número de tarjetas emitidas en la UE en los últimos años [7].

El Banco de España centra su estudio en el sistema bancario español y, por tanto, se disponen estadísticas desglosadas del último trimestre del 2016, cerrando dicho año con la cifra de 74,51 millones de tarjetas en circulación emitidas en España entre las tres redes españolas de tarjetas.

En la *Figura 1.14* se puede observar la evolución del número de tarjetas en circulación emitidas en España desde el año 2000 hasta la actualidad.

TARJETAS EN CIRCULACIÓN
EMITIDAS EN ESPAÑA

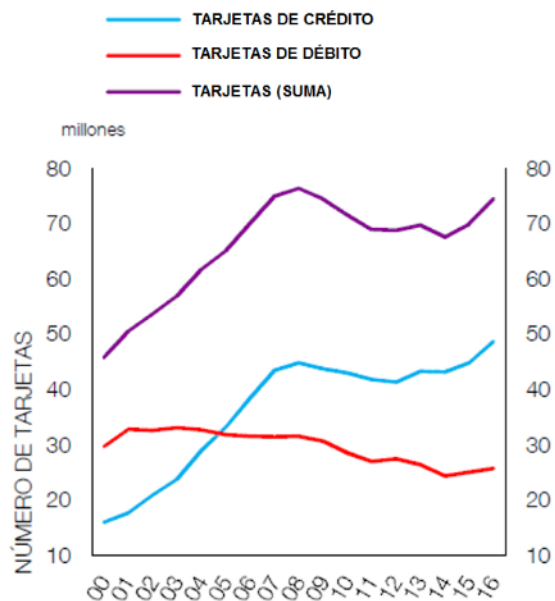


Figura 1.14: Evolución de las tarjetas en circulación en España desde el año 2000 [7].

El total de las tarjetas de España, se obtiene de la suma de las tarjetas emitidas por cada una de las tres redes de pago: ServiRed, 4B y EURO6000. Actualmente, ServiRed y 4B dependen del centro procesador de Redsys, mientras que EURO6000 dispone como procesador a Cecabank. En junio del 2017, los consejeros de las administraciones de las tres redes de pago aprobaron el proyecto de fusión para dar lugar a un único esquema nacional que, por el momento, continuaría utilizando las dos procesadoras transaccionales. Este acuerdo se definió para que entrase en vigor a finales del año en curso, y se intuye que el siguiente paso, a medio plazo, consistirá en la fusión de las dos pasarelas de pago. Sin embargo, a septiembre del 2017, la estructura del procesamiento de la banca española, queda representado en la Figura 1.15.

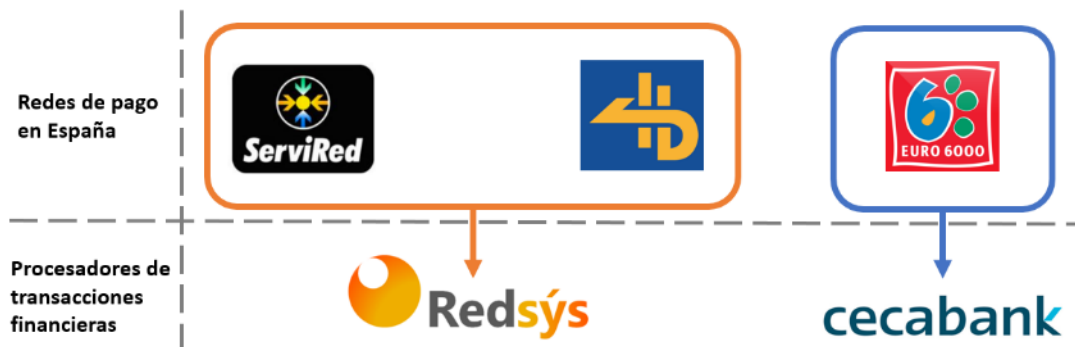


Figura 1.15. Esquema red financiera en España.

Dado que el trabajo fin de máster se realiza con la colaboración de Redsys, se dispone de las estadísticas correspondientes a este organismo respecto a la emisión de tarjetas en España. Se recogen en la siguiente tabla adjunta ciertos datos de interés, actualizados en mayo 2017.

Tarjetas en circulación (Mill.)	Año 2016
Tarjetas emitidas en España 4T 2016	74,51
	A Mayo 2017
Tarjetas emitidas Redsys	68.07
Tarjetas activas Redsys	30.60
Contactless	14.6
Ratio activas/emitidas	45%
Ratio contactless/activas	47.6%

Tabla 1.2: Estadísticas Redsys con respecto a la emisión de tarjetas en España [8].

Se calcula el porcentaje de tarjetas que soportan interfaz sin contactos respecto al total de tarjetas activas emitidas en Redsys (14,6 millones sobre 30,6 millones) obteniendo un ratio de proporcionalidad del 47,6%.

En la *Figura 1.16* se muestra la evolución de tarjetas activas contactless y del número de operaciones llevadas a cabo de forma presencial mediante esta tecnología a lo largo de los meses desde mayo 2016.



Figura 1.16: Estadísticas tarjetas contactless en España (Mayo2016 a Mayo 2017) [8].

A la vista de estos datos se puede afirmar que el despliegue de las tarjetas que soportan interfaz sin contactos es muy significativo, ya que determina un punto de inflexión en el mercado actual, dónde la tendencia es la continua búsqueda de evolución y desarrollo, creciendo a una velocidad vertiginosa y abriendo nuevas posibilidades al mundo financiero.

Esta transformación en el sector de los medios de pago habilita y condiciona la inserción de nuevos productos con carácter innovador al mercado financiero como, por ejemplo, los wearables. Estos dispositivos permiten la adaptación del formato clásico y tradicional de la tarjeta de plástico a nuevas soluciones, cubriendo la misma funcionalidad transaccional (protocolo de comunicación EMV Contactless) y aportando innovación y flexibilidad a los clientes.

La previsión de crecimiento de los wearables, durante el año 2017, es de 322 millones a nivel mundial, de los cuales 44 millones adquirirían el formato de pulsera [8]. En la *Figura 1.17* se presenta una solución basada en MiniTag, donde una pequeña antena que opera con tecnología sin contactos está integrada en una tarjeta de tamaño reducido que permite ser insertada en cualquier otro dispositivo como pulseras, llaveros o pulseras de reloj, etc.



Figura 1.17: Ejemplo de wearables con tecnología NFC.

Otro revolucionario campo de estudio es la autenticación del usuario mediante técnicas biométricas. Existen prototipos de lector de huella dactilar incorporado en el plástico de las tarjetas financieras, con el fin de que el cliente en el momento de efectuar un pago valide la operación mediante el reconocimiento de su dedo y no mediante un número secreto o PIN.



Figura 1.18: Tarjeta biométrica con lector de huella dactilar [9].

El hándicap que frena el despliegue de productos de este tipo, es el aumento del coste que supone para una entidad financiera emisora de las tarjetas. El precio que conlleva la puesta en marcha de una tarjeta con lector de huella hardware incorporado, puede ir asociado a un gasto ocho veces mayor que una de las tarjetas que actualmente esté en circulación. Por este motivo, la validación de la huella dactilar es más propensa en los dispositivos móviles de los clientes que tengan esta funcionalidad habilitada.

Por lo tanto, se puede afirmar que la transformación digital es exponencial y no presenta límites preestablecidos, dado que el 2016 también vino marcado por el inicio de la era del pago móvil.

Este concepto hace referencia al conjunto de servicios que permiten realizar transacciones financieras a través de teléfonos móviles. Tras la definición genérica se puede establecer la distinción de tres tipos de operaciones diferentes:

- **Transferencia de dinero** (entre distintos usuarios de telefonía móvil): Por ejemplo, Bizum o Twyp de ING Direct. Esta operativa queda fuera del ámbito de estudio del TFM, ya que el proyecto se enmarca en el análisis de soluciones de comercio entre un cliente y un establecimiento y no entre usuarios.
- **Compras** (comercio electrónico móvil o m-Commerce): Punto de interés que se desarrolla en el *Capítulo 2*.
- **Pago móvil en el comercio de forma presencial**: A continuación, se describen las diferentes opciones que actualmente existen en el mercado para realizar pagos en establecimientos físicos a través del dispositivo móvil.

Pago móvil en comercio presencial

La integración del pago móvil (*Figura 1.19*) como medio o recurso para llevar a cabo una operación financiera en un comercio físico se ha visto impulsada por el alto índice de smartphones que incorporan chips NFC, así como por la expansión de los TPV que soportan tecnología contactless (siendo el despliegue de los terminales de pago contactless consecuencia directa de la evolución de las tarjetas inteligentes).



Figura 1.19: Esquema de pago móvil presencial.

En la *Figura 1.20* se puede apreciar que el número de TPV activos en España es de 1.659.000. Actualmente el 90% de los 1.259.000 terminales punto venta gestionados por Redsys, soportan interfaz sin contactos. Sobre estos dispositivos se podrían llevar a cabo transacciones financieras con tarjetas inteligentes o con pago móvil indistintamente.



Figura 1.20: Representación del parque de terminales conectados a Redsys [8].

Existen múltiples compañías proveedoras del pago móvil en comercio físico, aunque la filosofía y el procedimiento de uso son prácticamente similares entre todas ellas, con la salvedad de alguna peculiaridad funcional que queda descrita en la definición de cada una de las soluciones.

A grandes rasgos, la metodología es que el usuario, en una primera fase de registro, almacena de forma manual la información de las tarjetas físicas financieras que desea vincular a la cartera virtual de la aplicación móvil del servicio. La finalidad es sustituir la tarjeta física por el dispositivo móvil en el momento de realizar el pago, pero como las comunicaciones inalámbricas no son seguras, los móviles necesitan protegerse de la posible captura de datos, por lo que emplean tecnología HCE (Host Card Emulation) a nivel de protección software o bien *secure element* a nivel de hardware (elemento seguro que se integra en la tarjeta SIM del teléfono). El dispositivo móvil se aproxima al TPV, emulando el comportamiento de la tarjeta, de tal forma que se establecen las comunicaciones pertinentes mediante tecnología NFC.

Las soluciones de pago móvil que han salido al mercado son muy numerosas y parecidas, por lo que ninguna ha destacado de forma notable respecto del resto. Para llevar a cabo el estudio se realiza una división entre las aplicaciones proporcionadas por los fabricantes de dispositivos móviles, aquellas que desarrollan las entidades financieras y las que ofrecen las operadoras móviles, siendo las prestaciones de todas ellas muy parecidas [10] [11].

- **Soluciones de los fabricantes de dispositivos móviles:** La *Tabla 1.3* muestra una breve comparativa entre las diferentes características que aportan las tres aplicaciones de pago más destacables: Android Pay, Samsung Pay y Apple Pay.



Android 4.4 o superior

Conectividad NFC

No debe estar rooteado

Dispositivos compatibles

Galaxy S8/S8+
Galaxy S7/ S7 edge
Galaxy S6/ S6 edge/ S6 edge+
Galaxy A5 (2016-2017)

Dispositivos compatibles

iPhone 7 / 7 Plus
iPhone 6/ 6Plus
iPhone 6s/6s plus
iPhone SE
Apple Watch
iPad mini 3 e iPad Air 2
Mac enlazado a iPhone / Apple Watch
MacBook Pro con TouchID

Entidades asociadas

BBVA

Tarjetas VISA y MasterCard

Servicios financieros El Corte Inglés

Banco Santander
CaixaBank
ImaginBank
Abanca
Banco Sabadell

Tarjetas VISA de CaixaBank
Tarjetas VISA de Abanca
(próximamente MasterCard)
Tarjetas VISA de Banco Sabadell

Banco Santander

BOON

Servicios financieros Carrefour

American Express
Tarjetas MasterCard del Banco Santander
Tarjeta BOON
Endenred(Tarjetas Ticket Restaurant)
Tarjetas PASS de Carrefour

Seguridad

Número de tarjeta virtual

Samsung KNOX

Touch ID

Tabla 1.3: Comparativa de las aplicaciones de pago Android Pay, Samsung Pay y Apple Pay.

- **Soluciones de las entidades financieras:** Son numerosos los bancos que se han querido reinventar tecnológicamente y han apostado por el móvil como método de pago, creando sus propias aplicaciones. Algunos ejemplos son: Bankia, Bankinter, BBVA, CaixaBank, Imaginbank, ING Direct, Sabadell, Santander, Evo, etc.

Todas estas aplicaciones presentan funcionalidades similares, que incluyen la posibilidad de establecer pagos presenciales en establecimientos físicos, sin la necesidad de utilizar la tarjeta inteligente.

Grosso modo, la mayoría de aplicaciones móviles utilizan la tecnología NFC para establecer las comunicaciones entre el móvil y el terminal de pago. Algunas aplicaciones almacenan los números de las tarjetas físicas del cliente en la cartera virtual, con el fin de emular el pago cómo si la operación se desencadenase con dicha tarjeta. Otras aplicaciones permiten disponer de una tarjeta únicamente virtual, que no presenta relación aparente con los datos sensibles de la tarjeta física del titular, con la finalidad de aportar robustez a la transacción.

El caso de la aplicación Twyp Cash de ING se diferencia fundamentalmente del resto de aplicaciones en que no utiliza NFC para efectuar el pago presencial, si no que genera un código que debe ser escaneado o introducido por el dependiente del establecimiento en su servidor.

Por lo general, las aplicaciones móviles financieras pueden permitir realizar otras gestiones, proporcionando servicios de valor añadido al cliente, como la consulta de movimientos, dar de baja tarjetas, modificar el valor del PIN, o realizar transferencias de móvil a móvil de forma inmediata (algunas de ellas, como Bankia, Sabadell, BBVA, Bankinter, EVO e Imaginbank, incluyen Bizum, mientras que ING Direct dispone del servicio Twyp). Pero, como se ha comentado, estos servicios quedan fuera del ámbito de estudio del TFM.

- **Soluciones de las operadoras:** Las tres principales operadoras de nuestro país también disponen de aplicaciones de pago móvil:

- Orange Cash

Los clientes de esta operadora podrán utilizar el servicio de pago móvil integrado en esta aplicación si disponen de tarjeta SIM con NFC (que la compañía ofrece de manera gratuita) y un smartphone compatible (con sistema operativo Android). En la aplicación es necesario introducir manualmente los datos sensibles de las tarjetas físicas que se deseen asociar al servicio para operar con TPV contactless.

- Vodafone Wallet

La compañía se unió a la revolución de los pagos móviles en 2014. Esta aplicación sólo está disponible para Android y funciona vía NFC, pudiendo añadir tarjetas o una cuenta de PayPal.

- Movistar

Movistar permite el pago móvil vía NFC o bien como Orange, a través de tarjetas SIM NFC, que también oferta en los distribuidores, pero únicamente para los transportes públicos de Valencia y Málaga. De momento, no ofrecen una solución para pagos en general como los anteriores.

Como se puede percibir, han sido muchos los proyectos que se han lanzado en paralelo y con diferente grado de interoperabilidad para llevar a cabo el pago, ya que no todas las aplicaciones funcionan en todos los dispositivos móviles, ni en todos los comercios, ni con todas las tarjetas de todos los bancos. Este hecho ha supuesto una barrera para la adopción global del nuevo método de pago, siendo un hándicap para el despliegue masivo de los dispositivos móviles como medio transaccional. Como ninguno de ellos ha cuajado de forma sustancial, ha sido imposible avanzar en el proceso de convergencia.

Los pagos con móviles en España, han alcanzado la cifra de 670 mil operaciones en el mes de mayo 2017, como muestra la *Figura 1.21* representando el 0,2% del total de las operaciones de compra realizadas de forma presencial en un comercio físico. Sin embargo, se estima que, a medio plazo, las prestaciones que aportan las plataformas de pago acabarán solventando las adversidades en función del tiempo, experimentando un crecimiento abrupto de la usabilidad y confianza de los clientes.

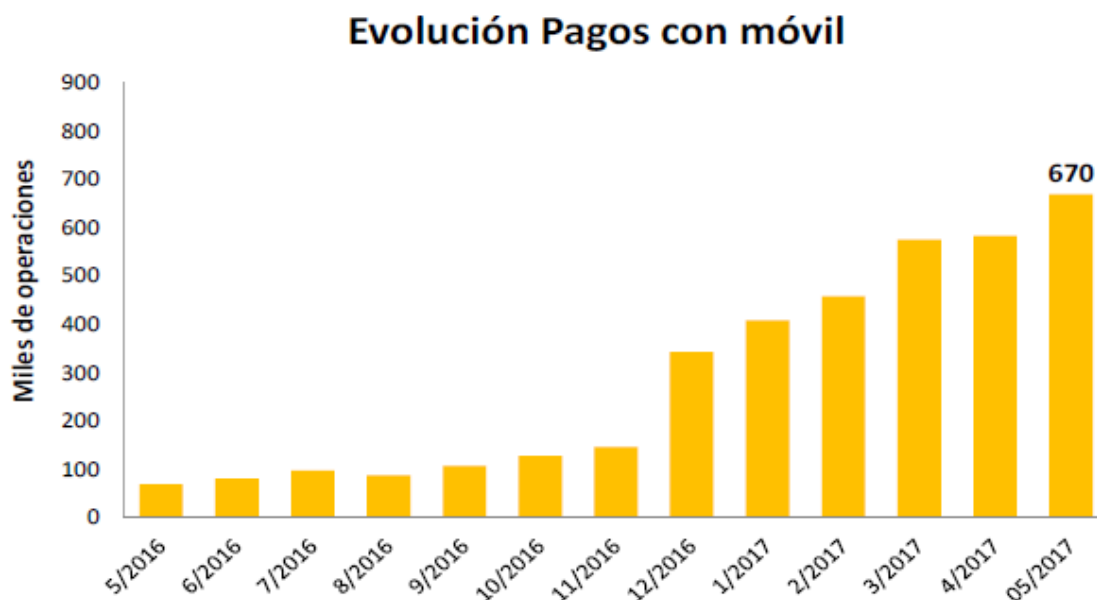


Figura 1.21: Resumen del uso mensual de los pagos móviles en España [8].

Aunque es innegable que la aparición del teléfono móvil como nuevo sistema de pago ha provocado una revolución en el sector financiero, a nivel global los estudios y estadísticas de mercado no revelan que desencadene, al menos a medio plazo, la desaparición de la tarjeta de plástico. En los últimos años se han publicado numerosos informes que se pronosticaba la desaparición de la tarjeta en favor del dispositivo móvil [12]. Sin embargo, algunas de estas publicaciones establecían que la fecha de extinción de la misma se produciría en el año 2016, y en la actualidad, continúa siendo el medio de pago utilizado por excelencia en los comercios y el sello de identidad de las entidades financieras.

La tarjeta inteligente aporta una serie de propiedades especiales que suponen una diferenciación destacable con el resto de productos emergentes en el pago móvil, lo que justifica su hegemonía hasta la fecha. Entre otras, cabe destacar las siguientes apreciaciones:

- Las tarjetas físicas son elementos seguros que permiten la autenticación de la tarjeta (validez de la misma) y del cliente (la propia tarjeta comprueba si el usuario es el titular asociado).
- Disponen de un procesador criptográfico que contribuye a la robustez de la transacción.

- Cuentan con tecnología sofisticada que hace que las posibilidades de manipulación física se reduzcan de forma significativa, siendo prácticamente una probabilidad inexistente.
- Incorporan gestión de riesgos y son partícipes de la decisión de autorización o denegación de la transacción financiera.
- No tienen baterías, la energía para la comunicación es suministrada por los lectores o por los datáfonos.
- Son baratas y están extendidas en la sociedad.

De esta forma, por el momento, se puede desmentir el infundio generalizado de que el dispositivo móvil supone una amenaza real a la coexistencia de ambos dispositivos. Por el contrario, puede marcar una era de enriquecimiento y complementación mutua, dando lugar a sistemas de pago combinados como el que tiene cabida en el presente trabajo final de máster.

Además, existen diferentes escenarios de pago, sujetos a cambios y con posibilidad de mejora en factores fundamentales como la seguridad y la experiencia de usuario, dónde se pueden explotar los recursos disponibles y obtener soluciones a problemas trascendentes. Entre otros, el comercio electrónico, por lo que es importante evaluar el entorno y explotar las posibilidades que las nuevas tecnologías ofrecen. La propuesta del TFM se basa precisamente en la presencia de los dos dispositivos, móvil y tarjeta, para desencadenar una transacción en comercio electrónico.

1.4.2 El progreso del comercio electrónico

El *comercio electrónico* o *e-commerce* (electronic commerce), consiste en la adquisición de bienes o servicios a través de Internet, utilizando como forma de pago medios electrónicos [13]. Ver *Figura 1.22*.



Figura 1.22: Imagen característica que representa el comercio electrónico.

La historia del comercio electrónico es más extensa de lo que comúnmente cabe esperar, ya que aun siendo un negocio pionero y emergente en la sociedad actualidad, se enmarca como una invención que nació con el inicio de Internet, hace casi cuarenta años.

Por consenso general, se atribuye el mérito del comercio electrónico al inventor y empresario británico Michael Aldrich, quien en 1979 descubrió la forma de conectar un ordenador para el procesamiento de pedidos en tiempo real a un televisor especialmente modificado mediante el uso de una línea telefónica, con el fin de vender productos de supermercados. El experimento no funcionó, pero fue un suceso clave para el inicio de una amplia línea de investigación con un desarrollo exponencial año tras año.

La primera venta online B2B (Business to Business, es decir, entre empresas y no directamente al consumidor final) ocurrió en el año 1981, cuando Thomson Holidays promovió la conexión entre sus agentes de viajes. De esta forma se favoreció que los empleados pudiesen intercambiar de manera inmediata la disponibilidad de los catálogos de viajes y ofertar a los clientes un servicio más completo.

Diez años después, en 1991, tuvo lugar un acontecimiento fundamental para el crecimiento del comercio electrónico, ya que la NSF (National Science Foundation) permitió la utilización de Internet para fines comerciales.

En el año 1992, nació la primera librería online, denominada “Stacks Unlimited”, ya que fue creada por Charles Stack. Esta iniciativa empezó como un tablón de anuncios y posteriormente se trasladó a *Books.com*.

En 1994, acontece el segundo punto de inflexión de la evolución del e-commerce, gracias a SSL (Secure Socket Layer). Este protocolo de seguridad sirve para proporcionar información al cliente de que el sitio web es auténtico, real y confiable, permitiendo la compartición de información sensible de manera íntegra y segura, es decir, la transmisión de datos es totalmente cifrada o encriptada. A día de hoy, cuando en una página web se visualiza HTTPS en la URL, implica que está protegido por el certificado SSL.

Ese mismo año, aparece el primer banco en línea, se fundó la compañía que hoy en día conocemos como Amazon (un comercio electrónico de alta repercusión y muy conocido en la actualidad), surgió el navegador Netscape Navigator y se llevó a cabo la primera venta online registrada. Esta primera compra online entre un usuario y un comercio no se trató de la reserva de un viaje o la adquisición de un libro como fueron los sucesos significativos hasta la fecha, sino de una pizza. El establecimiento de Pizza Hut supo aprovechar la nueva oportunidad de negocio que empezaba a surgir con fuerza y comenzó a ofertar pedidos online desde su página web.

En 1995, se fundó Ebay, otro gigante del comercio electrónico. Tres años después, en 1998, se instauró Paypal, una de las mayores compañías de pago por Internet del mundo. Ebay en el año 2002 compró a Paypal, aunque finalmente se desvincularon en el 2015, siendo, a día de hoy, dos potencias independientes y eminentes en el sector comercial y financiero online.

Durante los últimos años, la popularidad y la expansión del comercio electrónico se han intensificado notablemente. Cuando emergió el boom de Internet existía desconfianza en las compras online, y el sentimiento de temor a los estafadores y, por tanto, al robo de la información comprometida, estaba muy presente. En la época actual la tendencia ha ido cambiando, siendo las compras vía web una práctica ampliamente adaptada por los usuarios, pero continúan las preocupaciones fundadas y respaldadas por los casos de fraude en las transacciones llevadas a cabo mediante comercio electrónico.

Capítulo 2

Estado del arte del comercio electrónico

2.1 ESTADO DEL ARTE DEL COMERCIO ELECTRÓNICO

En la sociedad actual, el comercio electrónico está en pleno auge, dada la facilidad, comodidad y flexibilidad que ofrecen los pagos por internet. Además, los estudios de mercado revelan que seguirá creciendo vertiginosamente en los próximos años. Ver *Figura 2.1*.

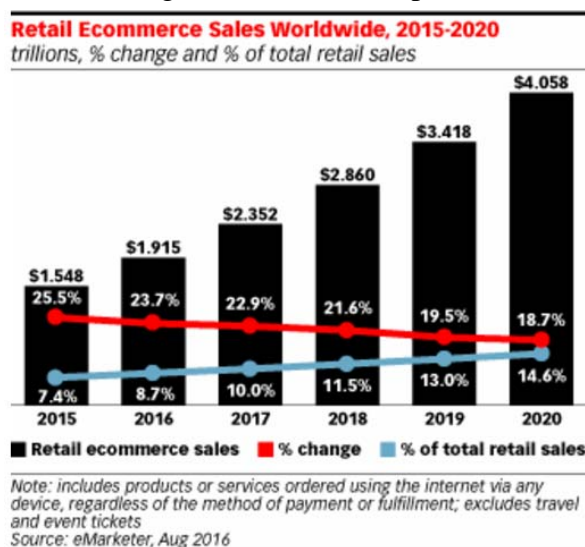


Figura 2.1: Estudio de eMarketer de la evolución del e-commerce (2016) [14]

En España, la evolución del comercio electrónico ha sido muy significativa, superando en el transcurso del año 2016 la cifra de 24 mil millones de euros facturados, lo que supone un incremento total del 20,8% respecto a las anotaciones del 2015. Los datos publicados por la Comisión Nacional de los Mercados y Competencia (CNMC) relativos al desarrollo del ejercicio trimestral desde el año 2011 hasta el cuarto trimestre del 2016, acreditan este progreso. En la *Figura 2.2* se puede visualizar el número de transacciones realizadas por internet mediante tarjeta de crédito o débito. Se registraron casi 400 millones de operaciones de comercio electrónico en España durante el año 2016, de los cuales más de 117 millones se llevaron a cabo únicamente en el último cuatrimestre, hecho que conlleva un 35,7% de valor interanual.

EVOLUCIÓN TRIMESTRAL DEL NÚMERO DE TRANSACCIONES DEL COMERCIO ELECTRÓNICO Y VARIACIÓN INTERANUAL (millones de transacciones y porcentaje)

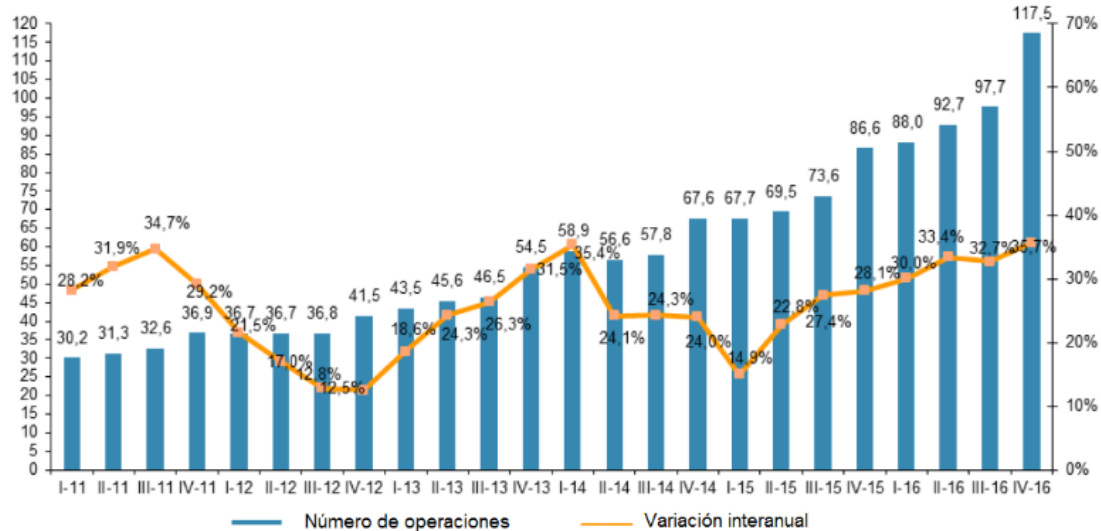


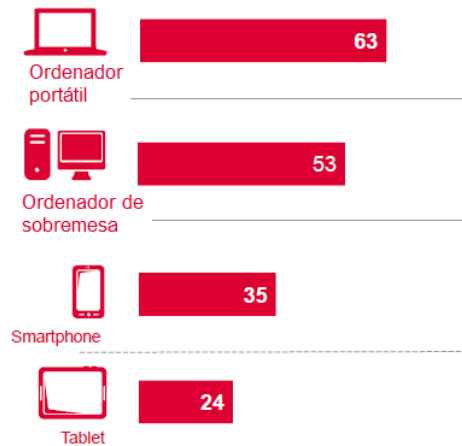
Figura 2.2: Evolución trimestral del número de millones de transacciones de comercio electrónico [15].

Dado que las transacciones mediante comercio electrónico están experimentando un incremento abismal, resulta de especial interés conocer las preferencias actuales y las expectativas de los usuarios para la obtención de estadísticas representativas de la sociedad. Dichas encuestas, entre otras prestaciones, sirven para que los agentes del sector comercial online puedan adaptar sus proyectos a los criterios de los clientes, ofreciendo soluciones más afines a las nuevas necesidades demandadas.

La empresa *dpd group* hizo público en febrero del 2017 un informe completo sobre usuarios de comercio electrónico a través de 21 países de la Unión Europea. Para llevar a cabo el estudio, se realizaron 23450 entrevistas, siendo la participación de los ciudadanos españoles de 1519 respecto del total [16]. Los resultados afirmaron que tres de cuatro personas, utiliza más de un dispositivo diferente para realizar compras online. Además, el dispositivo de pago más utilizado es el ordenador portátil, seguido del ordenador de sobremesa (ver Figura 2.3). Esta información se tendrá en cuenta en la demostración de la nueva solución de pago propuesta, con el fin de emular una compra online lo más afín posible a un escenario convencional. Ver *Capítulo 5*.

Aunque el uso de smartphone para la compraventa de bienes y servicios adquiere la tercera posición en el ranking, es importante recalcar que su utilización está creciendo de manera significativa. Las transacciones de comercio electrónico llevadas a cabo desde un móvil o una tablet, se denominan m-Commerce (Mobile Commerce) y pueden efectuarse mediante un navegador web (como aquellas que se desencadenan desde un ordenador) o una aplicación en el móvil [17].

Dispositivos utilizados para la compra online %



*1.75 dispositivos por persona de media

Figura 2.3: Preferencias de los usuarios de e-commerce encuestados en relación a los dispositivos que utilizan para realizar una compra online [16].

Para los diferentes agentes que intervienen en el método de pago es esencial tener evidencias de la predilección de los usuarios por la utilización de un medio sobre otro y de esta forma poder retroalimentar el diseño de las nuevas soluciones o evaluar las posibles campañas de su producto. El resultado del informe converge en que el medio de pago más extendido en Europa son las carteras digitales, siendo PayPal el procedimiento de liquidación favorito. Sin embargo, se puede observar en la *Figura 2.4* que la investigación realiza una división en cuanto a las tarjetas de las marcas internacionales (Visa y MasterCard) y las tarjetas de bancos nacionales. Si ambos ramales computasen bajo la denominación común de “*pago con los datos de la tarjeta*”, esta opción alcanzaría la posición número uno de la lista.

Métodos de pago más utilizados %

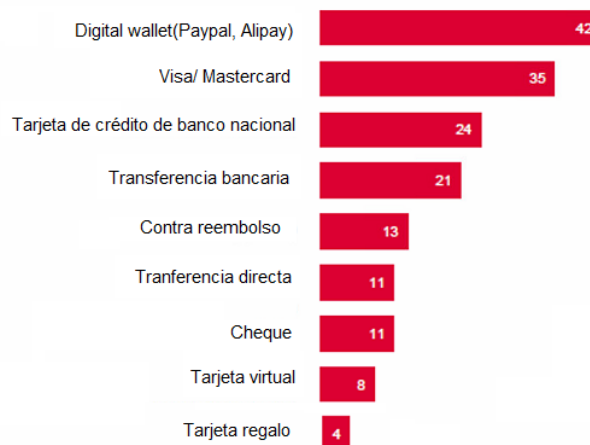


Figura 2.4: Métodos de pago más utilizados para llevar a cabo una transacción de e-commerce [16].

En los apartados subsiguientes se recogen los procesos típicos para llevar a cabo una operación financiera mediante comercio electrónico, evaluando las ventajas y las carencias que presentan cada uno de ellos. En líneas generales, cabe destacar que, todas las opciones actualmente disponibles en el sector para efectuar una operación financiera online de e-commerce, se corresponden con transacciones CNP (Card Not Present) [18]. Esto es debido, a que no existe la necesidad de que la tarjeta inteligente esté presente en el momento de efectuar la transacción, ya que no interviene en el esquema de la red de pago de comercio electrónico. Para resolver este tipo de operaciones, independientemente del método a utilizar, únicamente se requieren los datos que figuran estampados en la tarjeta, por lo que no se realiza una lectura de la información segura almacenada en el chip de la misma, a diferencia de las operaciones dónde la tarjeta está presente en un establecimiento físico.

2.2 PAGO MEDIANTE INSERCIÓN DE LOS NÚMEROS DE LA TARJETA

En este apartado se van a describir las diferentes casuísticas que existen a la hora de realizar pagos en comercio electrónico mediante la inserción de los datos de la tarjeta, en función de su nivel de seguridad.

2.2.1 Pago con tarjeta en comercio electrónico no seguro

Se define la operativa de comercio electrónico no seguro, como aquellas transacciones que se resuelven únicamente con la inserción de los datos sensibles de la tarjeta (PAN, fecha de caducidad y CVV2) en un entorno online. Entre otras instituciones, Redsys y CECA proporcionan los medios y los recursos tecnológicos para realizar pagos electrónicos mediante el uso de tarjetas asociadas a las cuentas bancarias. Este método se conoce como TPV Virtual.

El proceso consiste en que las páginas o servicios web de los comercios comunican mediante una redirección o llamada con la pasarela de pago elegida, transmitiendo el importe, la identificación del comercio (FUC) y la firma de seguridad, por lo que se realiza una autenticación del sitio web antes de la solicitud de los datos del cliente. La librería de pago adquiere el control de la comunicación con el cliente, con el fin de que el comercio no pueda recibir los datos de carácter comprometido y reforzar la seguridad. El TPV virtual contacta con la entidad emisora de la tarjeta, recibiendo la respuesta correspondiente (aceptada o rechazada, y la justificación pertinente). Una vez completada la transacción, se notifica al servicio que utiliza la pasarela de pago y al cliente de la resolución de la misma.

La herramienta de TPV Virtual conlleva una serie de gastos asociados para los comercios electrónicos, como la contratación de este servicio y una comisión por transacción, en función del sector, del tipo de producto, del volumen de las ventas y en general, de las condiciones previamente acordadas y negociadas con la entidad.

En la *Figura 2.5* se observa la típica estructura de un formulario de pago, dónde se solicita la inserción de los datos que se exponen a continuación:

- **Nombre del titular.**
- **PAN** (Personal Account Number): La longitud del número de la tarjeta es variable, pudiendo oscilar entre 13 y 18 dígitos, aunque el valor típico es 16. Cada uno de los números que aparece en las tarjetas financieras presenta un significado (tipo de tarjeta, emisor, país de la emisión, dígito de control que cumple el algoritmo de Luhn, código interno de la entidad, etc.), aunque existen valores privados para garantizar mayor seguridad. Las matemáticas y las finanzas están estrechamente relacionadas, dado que cualquier relación financiera se basa en medios de transmisión de datos a través de las redes y el soporte numérico es requerido en la codificación para una correcta estructuración de la información. Las numeraciones de todas las tarjetas de crédito o débito en circulación deben cumplir la normativa ISO/IEC 7812 [19].
- **Fecha de caducidad:** Presenta en el formato MM/YY, que corresponde con el mes y el año de expiración de la tarjeta financiera.

- **CVV2:** Las siglas CVV2 son el acrónimo de *Card Verification Value* (en español, Valor de Verificación de la tarjeta) y hace referencia a los 3 o 4 dígitos que aparecen estampados en el reverso de este elemento. También recibe otros denominativos, como CSC (Card Security Code) o CVC (Card Verification Code). Este dato es el único campo que no es almacenado ni en la banda magnética ni el chip de la tarjeta, tal solo aparece en la estampación de las tarjetas físicas. Se incorporó esta medida para reforzar la seguridad, ya que se consideraba que reduciría el fraude de forma significativa en las transacciones llevadas a cabo por comercio electrónico dónde se solicitase la inserción de este número.

El razonamiento teórico era correcto, ya que se partía de la suposición de que la única forma de disponer de este valor era con la posesión de la tarjeta en sí, por lo que ante la copia o clonación de la misma, no se podrían efectuar transacciones de este tipo. Sin embargo, en la práctica, a los atacantes no les supuso esta medida ninguna barrera, ya que ante el robo, pérdida, copiado o fotografiado de los valores estampados en la tarjeta, podrían continuar con sus prácticas ilegales. Sin considerar las técnicas de robo de datos online, muy extendidas en la actualidad, explicadas en el *Capítulo 3*. De esta manera, el fraude continuó aumentando a pesar de la aparición del CVV2.

El formulario muestra un título "Pagar con tarjeta u otras formas de pago" con un icono de tarjeta. Hay una pestaña "Tarjeta" seleccionada y un enlace "Otras formas de pago ...". Debajo, se listan las marcas de tarjetas soportadas: VISA, Mastercard, American Express, UnionPay y MIP. El campo "Número de tarjeta" está vacío y tiene un mensaje de error: "Introduce el número de tu tarjeta.". Los campos "Fecha de caducidad" (MM/AA) y "Código de seguridad" están vacíos. El campo "Nombre del titular" está dividido en "Nombre" y "Apellidos". Un botón naranja "Pagar Ahora" está ubicado debajo del formulario.

Figura 2.5: Formulario de pago con tarjeta para comercio electrónico no seguro.

Todos los datos solicitados en el formulario de pago anterior se pueden encontrar estampados en la tarjeta física (*Figura 2.6*). Estos campos se consideran información sensible debido a las acciones que puede desencadenar un uso inapropiado de los mismos.



Figura 2.6: Ejemplo de tarjeta inteligente con los datos sensibles destacados.

Una vez que dichos datos sensibles son insertados por el titular de la tarjeta en el formulario de pago redireccionado desde la página web del comercio electrónico, se establece una comunicación con la red de pago. Esta información viaja online hacia el centro procesador que enruta la petición a la entidad bancaria emisora de la tarjeta (en función del número PAN recibido) para que resuelva esta operación. En la *Figura 2.7* se puede observar la representación simplificada del esquema transaccional de una operación de comercio electrónico tradicional.



Figura 2.7: Procedimiento de una transacción financiera online de comercio electrónico (CNP).

Dado el escenario planteado, se cuestiona la seguridad en la gestión de la información sensible del titular de la tarjeta financiera y de la operativa actual de comercio electrónico. A parte de los factores externos como la pérdida, robo, copia o fotografía de los datos de la tarjeta, también surgen vulnerabilidades en el entorno online que requiere el uso de internet. Existen técnicas fraudulentas para la adquisición de información confidencial, tales como *phishing*, *pharming*, *snooping*, *spoofing* o *spyware* (ver *Capítulo 3*) que generan inseguridad en el pago pese a las recomendaciones generales que las entidades financieras proporcionan a los clientes (verificar que la página web es segura, no proporcionar los datos de las tarjetas a un tercero, revisar periódicamente los movimientos de la tarjeta, etc.). En la *Figura 2.8* se representa un ataque fraudulento, mediante *phishing*, dónde el estafador obtiene la información sensible del titular de la tarjeta.

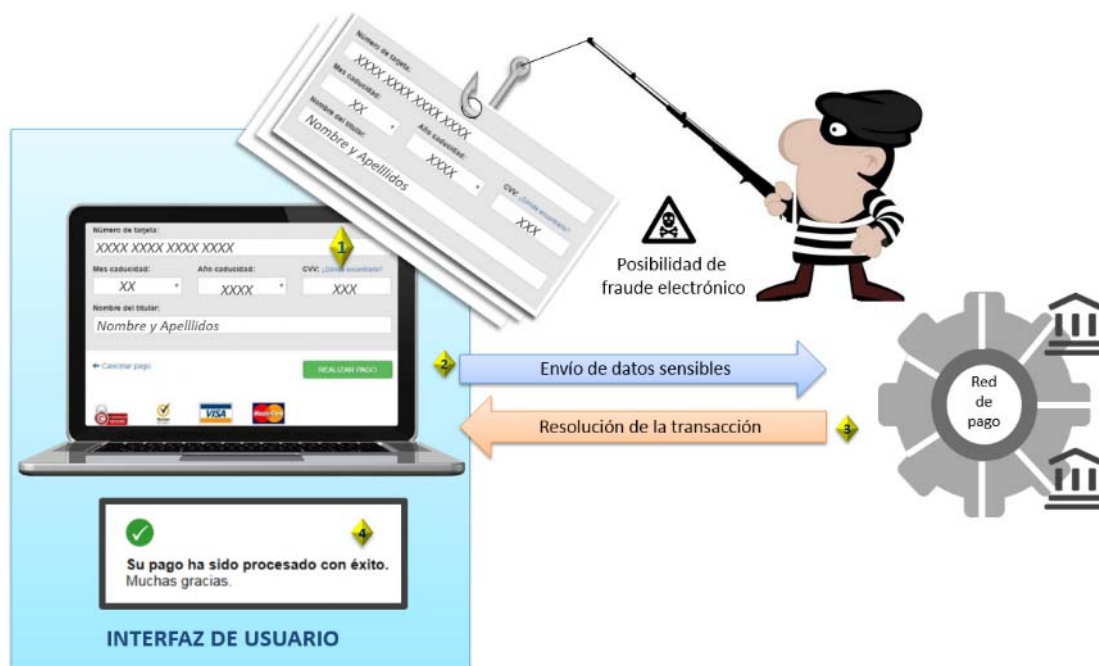


Figura 2.8: Representación de phishing en una transacción de comercio electrónico no segura (CNP).

Por lo tanto, en líneas generales, el pago mediante la inserción de los datos de la tarjeta en el escenario de comercio electrónico no seguro, presenta carencias en la protección de la información sensible y está expuesto a un elevado índice de riesgo. De esta forma, surgen otras alternativas en el ámbito de los medios transaccionales, como el pago con tarjeta en un contexto de comercio electrónico seguro.

2.2.2 Pago con tarjeta en comercio electrónico seguro

Se parte del escenario de comercio electrónico no seguro, dónde el titular de la tarjeta inserta los datos sensibles en el formulario de pago. Una vez que la petición de autorización llega a la entidad financiera, el titular recibe un mensaje de texto (SMS) en su dispositivo móvil con el código de seguridad que debe insertar en una segunda etapa en la página web. Gracias al mensaje recibido, se produce una autenticación en el móvil del usuario durante el proceso de finalización del pago.

Sin embargo, dicha solución, no elimina el *phishing*, ya que los datos sensibles son introducidos por el titular de la tarjeta, tal y como sucedía en la operativa general de comercio electrónico no seguro. En las Figuras 2.9 y 2.10 se representa esta solución de pago conocida como “operativa de comercio electrónico segura”, ya que incorpora el uso del dispositivo móvil del cliente en el esquema general de la red de pago de e-commerce. De forma conceptual, se puede apreciar la persistencia de vulnerabilidades en la primera etapa, ya que el usuario sigue introduciendo datos sensibles en el portal web, y este puede ser objeto de fraude.

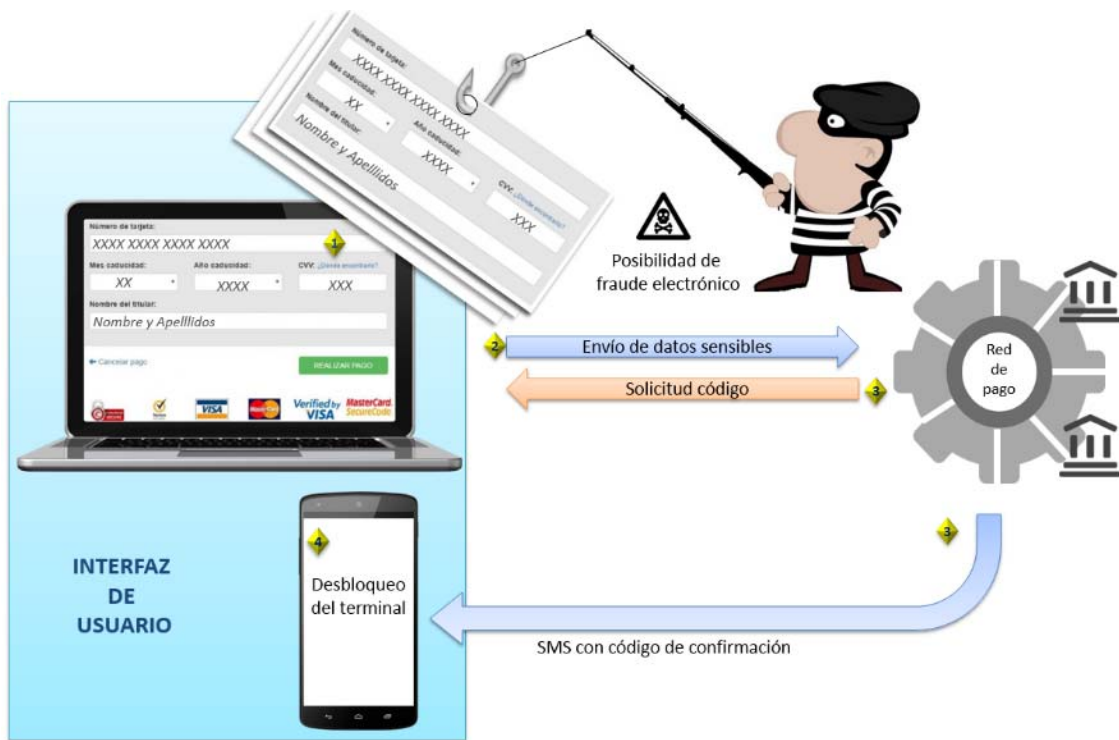


Figura 2.9: Posibilidad de phishing en comercio electrónico seguro (Primera fase)

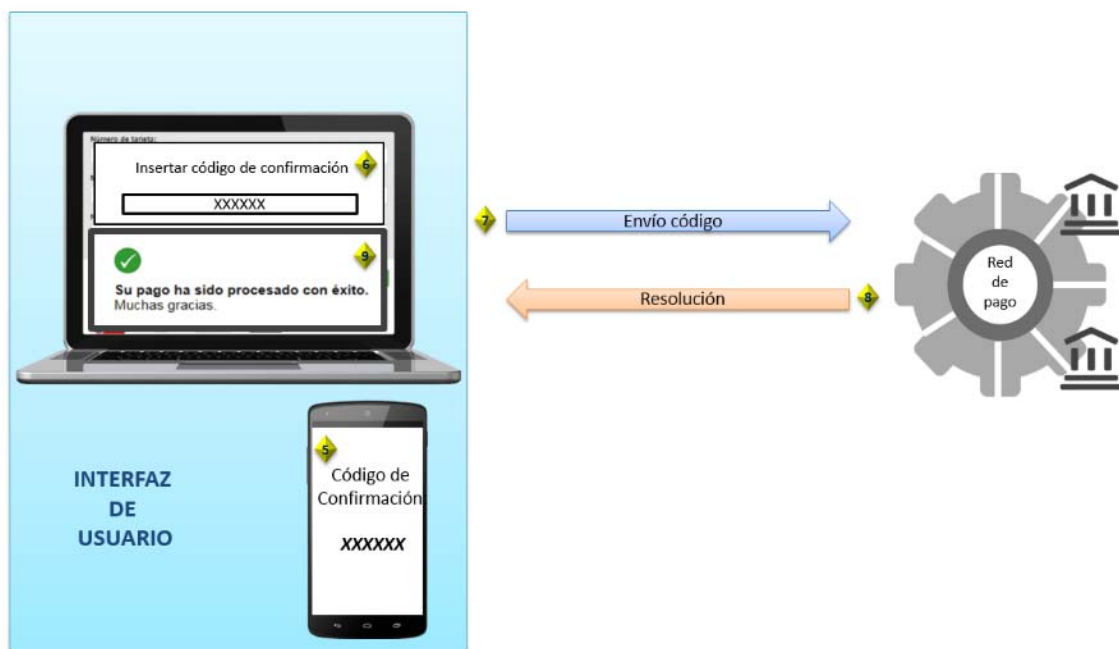


Figura 2.10: Uso del dispositivo móvil del cliente en la red de pago de e-commerce (Segunda fase).

Cabe destacar, que esta alternativa no fue acogida por los gigantes del comercio electrónico, como, por ejemplo, Amazon y Aliexpress, ni por diversos comercios minoristas. El motivo principal por el cual, los comercios online más populares no decidieron incorporar esta operativa, fue porque requería cambios en la infraestructura de la red de pago, así como un incremento de las tasas asociadas al empleo de este método. El SMS que envía la entidad financiera al cliente, conlleva un gasto adicional por parte del banco, que se factura al comercio que habilita este procedimiento (y no al cliente). Además, los grandes comercios no presentían que fuese la solución definitiva al problema del fraude electrónico, por lo que consideraron que salía más rentable continuar asumiendo, por el momento, el riesgo de fraude.

La *Tabla 2.1* pertenece al informe de gestión de Redsys, a Mayo de 2017, y muestra el porcentaje de transacciones procesadas de comercio seguro en comparación con no seguro, representando únicamente un 15% sobre el total. Por lo tanto, se deduce que este método no está tan extendido frente a lo que a priori se podría esperar.

CE Seguro Vs No seguro (Acumulado)					
Millones de operaciones	No Seguro	% Var. Inter.	Seguro	% Var. Inter.	% Seguro
Procesamiento	221,9	38,4%	39,2	26,8%	15,0%

Tabla 2.1: Comparativa del volumen de comercio electrónico seguro y no seguro procesado en Redsys [8].

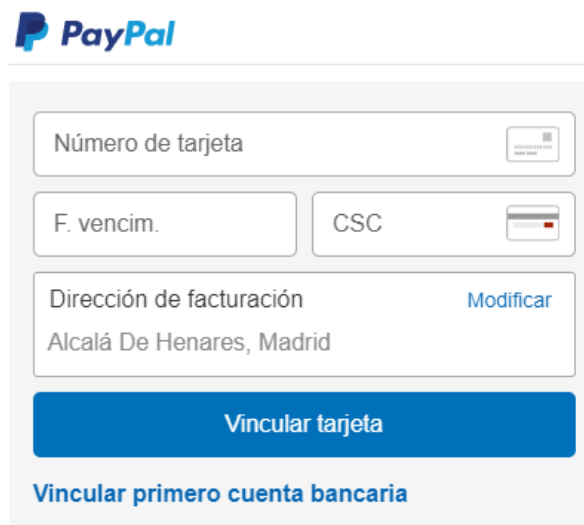
2.3 ELECTRONIC WALLET

Los wallets son monederos virtuales dónde se almacena la información de las tarjetas de pago, cuentas bancarias y otras herramientas personales con el fin de permitir al cliente realizar transacciones financieras electrónicas sin la presencia de la tarjeta física, recreando los datos de los que dispone el titular en su cartera.

Este concepto tuvo su origen en el comercio electrónico, ya que esta solución nació para satisfacer ciertos requerimientos de los pagos en línea, como la demanda de facilidad y de comodidad por parte de los usuarios. Sin embargo, la fuerte inclinación del consumidor a utilizar su dispositivo móvil en diversas actividades, provocó la expansión de los wallets como aplicación móvil para realizar compras desde los smartphones.

2.3.1 PayPal

PayPal es el proveedor de servicios de pago referente en la industria del comercio electrónico que permite realizar transacciones y transferencias por internet, sin la necesidad de insertar en cada movimiento financiero el número de tarjeta. El procedimiento de registro consiste en introducir un correo electrónico con una contraseña y vincular una tarjeta o una cuenta bancaria a la cuenta de PayPal creada.



The image shows a screenshot of the PayPal website's interface for linking a new card. At the top left is the PayPal logo. Below it, there are several input fields: 'Número de tarjeta' (Card number), 'F. vencim.' (Expiration date), and 'CSC' (Security Code). To the right of the 'Número de tarjeta' field is a small icon of a card. Below these fields is a section for 'Dirección de facturación' (Billing address), which currently shows 'Alcalá De Henares, Madrid' and a 'Modificar' (Modify) link. At the bottom of the form is a large blue button labeled 'Vincular tarjeta' (Link card). Below the button is a link that says 'Vincular primero cuenta bancaria' (Link bank account first).

Figura 2.11: Inserción de nueva tarjeta en Paypal.

Para pagar con PayPal, basta con que el comercio electrónico tenga incorporado este método en sus opciones de pago y el usuario inicie sesión con el correo y contraseña establecida. PayPal incorpora además la función opcional de *One Touch*, que mantiene la sesión abierta para que el usuario complete la compra con mayor rapidez.

Se enumeran a continuación las ventajas más significativas que presenta esta plataforma:

- Comodidad y rapidez para el usuario: El cliente asocia su tarjeta o cuenta bancaria a PayPal la primera vez. Una vez establecida esta relación, no es necesario volver a introducir de nuevo los datos sensibles.
- Servicio gratuito para el cliente y con garantía de entrega.
- Seguridad: En el momento de efectuar el pago mediante esta vía, el sitio web del comercio electrónico redirige la comunicación al servicio de pago de PayPal, de tal forma que el vendedor no tiene acceso a las claves de sesión ni a la información sensible del consumidor.

Todo es muy fácil y aparentemente seguro pero, como cualquier otra solución, también presenta una serie de inconvenientes que resulta fundamental destacar. Dichas desventajas se estudian para disponer de un referente que englobe las dificultades que las nuevas soluciones emergentes de pago deben solventar si realmente pretenden impactar en el sector. Entre otros hándicap, destacan:

- PayPal tiene que llegar a acuerdos, uno a uno, con cada comercio online. Dado que el servicio es gratuito para los usuarios, PayPal se beneficia de las desmesuradas comisiones de venta que aplica a los comerciantes. De esta forma, los grandes comercios, como Amazon, huyen de esta solución [20].
- No es un sistema global, ya que no se puede utilizar en todos los comercios electrónicos, ni para cualquier importe. Existe una restricción de cantidad máxima anual fijada en 2.500 euros. Si se excede este importe, es necesario aportar una serie de datos adicionales a los gestores de PayPal, por lo que resulta tedioso.
- Problema colateral en la seguridad del usuario: La rapidez del sistema de pago posibilita que los hackers se encuentren a una única clave personal (inicio de sesión en PayPal) de poder realizar pagos y transferencias fraudulentas. Existe una alta probabilidad de fraude, ya que hay riesgo de sufrir spam fraudulento, phishing, pharming, spoofing y spooning, entre otras técnicas asociadas al robo de información sensible [21].
- Cabe destacar que, si se produce pérdida o robo de la tarjeta física, o bien un estafador consigue los datos estampados en la misma (por ejemplo, mediante *skimming*), podría dar de alta una nueva cuenta de usuario en PayPal y asociar la información substraída a un usuario falso.
- Objetivo claro de los ciberatacantes. El fraude cada vez está más enfocado a conseguir burlar la seguridad de los servidores de almacenamiento de una plataforma que alberga más de doscientos millones de cuentas de usuarios. PayPal indica que dispone de un avanzado sistema de encriptación automática de la información, pero no se puede tener la certeza de que sea inmune a un futuro ataque masivo, exponiendo todos los datos sensibles de los usuarios.

2.3.2 iupay

La cartera digital iupay es una plataforma creada en España que almacena las tarjetas físicas del usuario en un monedero virtual y le permite realizar compras por internet sin tener que aportar datos sensibles en cada comercio electrónico [22]. El comportamiento de este sistema es similar a PayPal, pero respaldado por la banca española. Esta solución, propiedad de Redsys, vino impulsada por las principales entidades financieras de España, entre otras, Bankia, BBVA, CaixaBank, ING Direct, Banco Popular, Banco Sabadell y Banco Santander.

Respecto a PayPal, muestra la ventaja de que no es necesario introducir el número completo de las tarjetas financieras que se desee registrar, con proporcionar el valor de las primeras seis posiciones y las cuatro últimas del PAN en el momento de efectuar el alta en el servicio es suficiente. La fecha de caducidad de la tarjeta continúa siendo un dato obligatorio, mientras que el CVV no es solicitado. Al no revelar en su totalidad los datos bancarios, se reduce considerablemente el fraude ante un ciberataque o mediante el empleo de las técnicas de phishing o pharming.



Figura 2.12: Inserción de nueva tarjeta en iupay.

Otra ventaja en el ámbito de la seguridad, es que siempre que se añade una tarjeta a la cartera de iupay, se autentica al titular de la misma. Para ello, el usuario debe insertar el código de verificación que reciba vía SMS. Además, este método de pago es compatible con la operativa de comercio electrónico seguro, pudiendo recibir el usuario el OTP correspondiente y de este modo, proceder a completar la compra.

Se deduce, por tanto, que es un método fácil, cómodo e inspira más seguridad que PayPal. Sin embargo, no tuvo el éxito esperado en el sector. La desventaja fundamental es que, al igual que PayPal, no es una solución global, ya que no todos los bancos están adheridos a esta forma de pago, ni todos los comercios brindan la posibilidad de emplear este medio.

Otro factor relevante vino marcado porque esta solución se puso en funcionamiento en el año 2014, cuando PayPal ya tenía una alta reputación y millones de usuarios activos. En cierta manera, las expectativas de los clientes no fueron completamente satisfechas, y a nivel global no se supo considerar el valor añadido que ofrecía iuPay respecto del resto de formas de pago que ya se disponían.

El Instituto de Empresa Business School realizó una encuesta en el año 2015, en España, con el propósito de investigar el grado de conocimiento sobre distintos medios de pago y analizar las tendencias para el futuro. En los resultados destacó la familiaridad que los distintos participantes tenían con Paypal, ya que un 88% de los entrevistados conocía este método de pago, frente a un 20,2% que conocía iuPay.

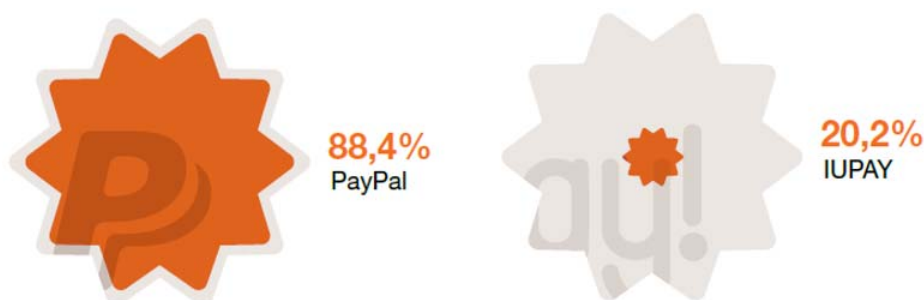


Figura 2.13: Conocimiento de los encuestados en métodos de pago en España [5].

Se observa que, independientemente de la seguridad real o de las prestaciones de una solución, la decisión final del éxito de la misma viene predefinida por la sentencia del cliente. Por lo tanto, la experiencia de usuario es determinante en el análisis de los requerimientos de un nuevo producto.

2.4 AUTOGESTIÓN DE LOS GRANDES COMERCIOS

Se extiende, cada vez más, la práctica de que el propio comercio electrónico solicite o almacene los datos sensibles del usuario para aumentar la comodidad, usabilidad y facilidad en el pago de las siguientes compras.

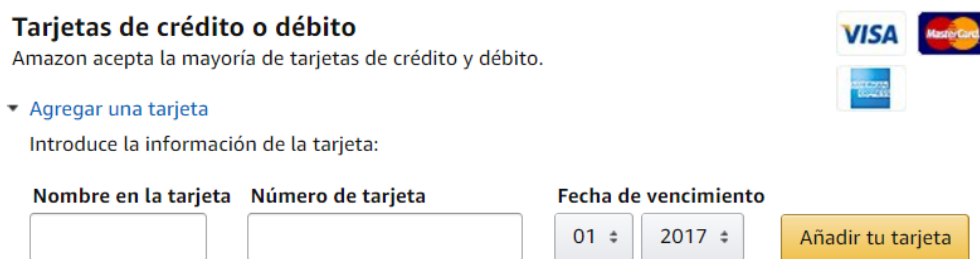
De esta forma, consiguen que para el cliente sea transparente abonar el importe de su factura, ya que el usuario únicamente se limita a seleccionar los productos que desea adquirir y ordenar su pedido. Es importante recalcar que el cliente lo que busca, es comprar y no pagar, por dicho motivo estas soluciones tienen cierto éxito garantizado a pesar de la incertidumbre e inseguridad que refleja el pago.

El problema fundamental de la autogestión de cada comercio, es que los datos comprometidos del titular acaban siendo almacenados en servidores o equipos informáticos que despiertan el interés de los hackers. En este aspecto, la historia de la seguridad cibernética está salpicada de incidentes y robo de datos masivos, que comprometen la imagen de la industria de los medios de pago.

A continuación se detalla la gestión de los medios de pago que utiliza Amazon, una de las empresas más importantes en el mundo del e-commerce a nivel mundial en este momento.

El medio de pago que utiliza Amazon es mediante tarjeta de crédito o débito, siendo las marcas aceptadas: Visa, Visa Electron 4B, Euro6000, MasterCard, American Express y Maestro Internacional.

Amazon brinda la posibilidad de insertar los datos de la tarjeta durante la confirmación del pedido, pero por excelencia se utiliza la propia cuenta para el almacenamiento de dicha información.



The image shows a web form titled "Tarjetas de crédito o débito" with the text "Amazon acepta la mayoría de tarjetas de crédito y débito." To the right are logos for VISA, MasterCard, and American Express. Below the title is a link "Agregar una tarjeta" and the instruction "Introduce la información de la tarjeta:". The form contains three input fields: "Nombre en la tarjeta", "Número de tarjeta", and "Fecha de vencimiento". The date field is split into two boxes for "01" and "2017". A yellow button labeled "Añadir tu tarjeta" is positioned to the right of the date field.

Figura 2.14: Inserción de los datos sensibles de una tarjeta en Amazon [23].

El sitio web de este admirable y exitoso comercio electrónico, notifica explícitamente que los datos sensibles del titular están protegidos en todo momento gracias a sus servidores seguros y que las transacciones que se procesan utilizan el protocolo TLS (Transport Layer Security, anteriormente conocido como SSL).

Sin embargo, el escenario real, es que los piratas informáticos pueden acceder a los números de varias tarjetas que un cliente tenga guardadas en su cuenta, con tal solo conseguir la contraseña de acceso a la misma y sin necesidad de atacar en el transcurso de una operación financiera (eludir el protocolo TLS). Además, la limitada capacidad del ser humano para recordar múltiples contraseñas, provoca que éstas sean fáciles, predecibles y se reutilicen en varios canales, facilitando oportunidades a los hackers.

Cabe destacar que los equipos informáticos que albergan la información masiva de carácter sensible de los usuarios son también un blanco para los estafadores. Hay que tener en cuenta que pueden ser clientes activos o no, es decir, aquellos que en un momento determinado decidieron dar de alta una tarjeta, aunque no llegasen a realizar ninguna compra.

El contexto práctico se reduce a que, los hackers, se encuentran a una única clave que permite el acceso a la información financiera de un usuario, y a un ataque victorioso de conseguir los datos sensibles de miles de ellos, resultando ser este último punto su objetivo prioritario.

Amazon también informa en su página web de todos aquellos medios de pago que no aceptan:

- PayPal: El propio vicepresidente de Amazon Payments, Patrick Gauthier, declaró que, si sus clientes necesitasen o propusiesen la integración de Paypal en la plataforma, ya estaría incluido, pero, a priori, no entendían por qué deberían hacer la experiencia del pago más complicada de lo que debería ser.
- Cheques o giros postales
- Pagos en efectivo en cualquier divisa
- Pagarés
- Domiciliaciones bancarias
- Pagos contra reembolso
- Transferencias bancarias

Es importante recalcar que Amazon presenta ciertas limitaciones al pagar con tarjeta virtual o con una tarjeta de prepago, ya que se factura el producto cuando se produce el envío. De esta forma se trata de evitar que la tarjeta de pago pueda caducar en el periodo comprendido entre la compra y el envío, reduciendo considerablemente la experiencia de usuario.

2.5 TARJETAS VIRTUALES

Una tarjeta virtual se caracteriza por no disponer de soporte físico de plástico, ya que suelen ser de papel o directamente no estar materializada [24]. Este dispositivo no puede ser utilizado en comercios físicos, ya que su campo de operatividad está destinado al comercio electrónico.

Para que un usuario pueda disponer de una tarjeta virtual, es necesario que sea cliente de la entidad financiera que oferte esta plataforma. Normalmente, se requiere, además, que el cliente disponga de una tarjeta de crédito o débito física de dicho banco, siendo la tarjeta virtual únicamente un complemento que aporta valor añadido a este servicio.

Existen diferentes modalidades de negocio dentro del marco de las tarjetas virtuales:

- **Tarjeta pre-pago:** Disponen de un número de tarjeta (PAN), una fecha de caducidad y un CVV, con valores fijos e independientes de los datos sensibles que figuran en la tarjeta física del titular. Suelen tener un límite de saldo máximo para la prevención del fraude, y es combinable con otras formas de pago, como Paypal, dónde se puede registrar esta tarjeta en vez de la física.

La forma de proceder es realizando, previamente a la venta online deseada, la carga de la tarjeta (siendo encarecidamente recomendado que el importe a precargar sea del precio exacto a utilizar en el pago). Dicha recarga está habilitada vía online y desde las oficinas físicas o cajeros, pero esta práctica reduce considerablemente la experiencia de usuario, ya que obliga al interesado a realizar un paso adicional sin una orientación externa (es el propio cliente, quién, por iniciativa propia, debe ingresar en la página web de su banco para realizar la recarga, o asistir presencialmente al cajero, cuando su objetivo final es llevar a cabo una venta online de manera sencilla y rápida, generalmente desde su casa). Esta solución, aunque es interesante, no supone un gran impacto en el contexto de los medios de pago actuales. Actualmente disponer de una tarjeta pre-pago para comercio electrónico, no aporta ninguna ventaja adicional a la conocida decisión de muchos usuarios que, siendo titulares o autorizados de diferentes tarjetas (del mismo o de diferentes bancos), deciden destinar una de ellas exclusivamente a las compras online, limitando el saldo de la cuenta asociada para evitar riesgos.

- **Tarjeta virtual tokenizada:** La tokenización (es un anglicismo derivado de vocablo token, cuya traducción literal sería señal o código) es una de las tendencias que auguran mayor proyección en el futuro de los medios de pago. Esta técnica permite sustituir un dato sensible, en este caso, el número de la tarjeta (PAN), por otro denominado token que de ser filtrado no comprometa la seguridad del pago en el proceso transaccional. A partir del token no es posible establecer una conexión con el valor que representa (PAN). El vínculo que asocia estos dos campos reside en una cámara de datos que presenta una validez determinada, ya sea temporal (minutos, horas, días, etc.) o en función del número de usos (por ejemplo, un token por cada operación financiera, tres transacciones máximas, etc.).

Esta solución presenta estrictas limitaciones en las compras mediante comercio electrónico, ya que no puede ser utilizada en la contratación de aquellos servicios que requieran suscripciones, pagos periódicos o fraccionarios, y en definitiva, que se utilicen para varios cargos en la tarjeta. También surgen incompatibilidades con la política del sistema de PayPal, iTunes, Amazon, etc., que solicitan uno o varios cargos en la misma tarjeta según la preparación del envío de cada producto.

2.6 EL BITCOIN

El bitcoin es una moneda virtual que tuvo su origen en el año 2008, siendo la que más impacto ha causado, de los casi 500 tipos de monedas virtuales existentes según el Banco Central Europeo (BCE).



Figura 2.15: Representación Bitcoin

La tecnología que utiliza el bitcoin es el blockchain [25]. La metodología de funcionamiento se basa en una red descentralizada, sin que intervenga ninguna autoridad central monetaria, que permite todo tipo de transacciones de cualquier parte del mundo vía peer-to-peer (P2P).

Para ello, existe la figura de los *miners* (mineros, en castellano) que prestan su poder de computación para facilitar y verificar las transacciones a través de un software sofisticado de código abierto. Se comprueba que las operaciones son legales en función de los registros de bloques válidos que se llevan a cabo. En el año 2015, se ofrecían 25 bitcoins (6000 dólares) por cada bloque válido completado, a repartir entre los miners intervinientes.

Las transacciones llevadas a cabo mediante el intercambio de bitcoin, no necesitan proporcionar ningún tipo de información personal, son fáciles, presentan alcance global y se realizan prácticamente de forma inmediata. Por este motivo, se conoce como la nueva solución más parecida al dinero en metálico sin fronteras.

El bitcoin se puede utilizar en determinadas tiendas online, y aunque en general no es un medio de pago muy extendido, también es aceptado en más de 200 tiendas físicas en España, de los casi 7000 establecimientos que utilizan este medio de pago en el mundo. Entre otros comercios, se encuentra la participación de Dell y Microsoft.

Cabe destacar que no es un método de pago exento de polémicas, ya que ha sido objeto de hackers en numerosas ocasiones. La muestra más significativa tuvo lugar en el año 2014, cuando Mt.Gox, un mercado importante japonés de bitcoins, quebró tras el saqueo que los piratas informáticos provocaron en los monederos digitales de la compañía, robando medio millón de dólares.

Debido a las consecuencias de los riesgos que comporta, continúa siendo una opción muy limitada. Como desventajas, destaca la falta de transparencia y claridad, el anonimato de los agentes implicados, el fraude y la elevada volatilidad de su cotización, que hace que los usuarios no sepan exactamente cuánto están pagando.



Figura 2.16: Evolución de la cotización de bitcoin [5].

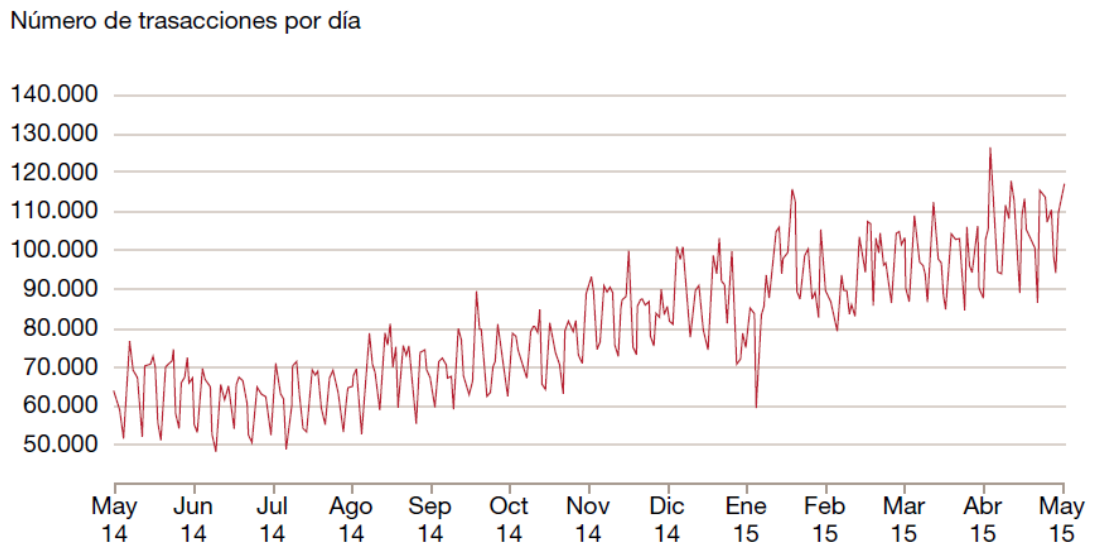


Figura 2.17: Evolución del número de transacciones diarias en bitcoins [5].

Los expertos consideran que, si se lograsen solventar los problemas indicados, podría llegar a consolidarse como un medio de pago electrónico de uso frecuente, debido a la buena adaptación que presenta el bitcoin a la interoperabilidad del ecosistema de internet. Sin embargo, por el momento, continúa siendo una alternativa con severas restricciones añadidas.

2.7 OTROS MÉTODOS DE PAGO EN COMERCIO ELECTRÓNICO

Como se ha explicado en los apartados anteriores, los medios de pago más extendidos para el comercio electrónico son utilizando los datos de la tarjeta de crédito o débito del usuario. Sin embargo, existen otras formas de pago más tradicionales. A continuación se definen los sistemas de pago clásicos para comercio electrónico [26].

2.7.1 Contra-reembolso

El funcionamiento de este sistema de pago es sencillo, ya que el cliente realiza el pago del producto en el momento en el que lo recibe. El abono del importe puede ser entregado directamente al mensajero o en la oficina de mensajería correspondiente. Se trata de una forma de pago segura para el cliente, pero no deseada para los comerciantes, entre otros motivos porque no disponen del dinero hasta semanas después de preparar el envío y puede suponer un gasto adicional si finalmente el cliente no recoge o rechaza el producto por cualquier factor.

2.7.2 Talón bancario

Se trata de un sistema que utiliza como medio de pago un talonario, que previamente el banco ha entregado al titular de una cuenta. Los talones o cheques bancarios se rellenan con la cuantía de la transacción acordada, y el vendedor lo puede cobrar en la misma entidad bancaria a la que pertenece el comprador de manera gratuita o bien en otras entidades si abona los gastos de gestión.

Cada vez es menos utilizado, debido a que supone un riesgo perder el propio talón. Además, no se tiene la certeza en el momento de la recepción del cheque de que la cuenta comprometida disponga de fondos para hacerlo efectivo.

2.7.3 Transferencia bancaria

Es el método de intercambio de dinero más utilizado entre dos usuarios, pero en escenarios de pago entre un cliente y un establecimiento no suele tener tanta aceptación. Este sistema consiste en una transferencia de dinero con origen la cuenta bancaria del comprador y destino la cuenta del vendedor. En el caso de que la entidad bancaria entre ambos sea la misma, la transferencia tarda en hacerse efectiva 1 o 2 días laborales. Sin embargo, si se trata de entidades distintas, este proceso puede llevar incluso 3 días, por lo que supone un inconveniente para el consumidor y el comerciante. Además, ciertos bancos, cobran gastos de gestión por realizar este tipo de movimientos financieros, por lo que los clientes priorizan otros medios de pago previamente analizados (digital wallet o tarjeta).

Capítulo 3

Fraude en e-commerce y seguridad del Protocolo EMV

3.1 FRAUDE EN COMERCIO ELECTRÓNICO

En la actualidad el comercio electrónico se ha convertido en el foco de los ataques fraudulentos, creciendo precipitadamente a pesar de las diferentes alternativas existentes para llevar a cabo una transacción online (ver *Capítulo 2*). Esta realidad viene enmarcada principalmente por los siguientes factores destacables:

- **Incremento del volúmen de operaciones:** El aumento de las transacciones llevadas a cabo mediante comercio electrónico en los últimos años ha sido abismal, creciendo a un ritmo desenfrenado.
- **Escenario difícil de controlar** y/o proteger, dónde todo usuario que tenga una tarjeta financiera operativa está expuesto a fraude, siendo afectados diferentes países con sus propias normativas y regulaciones particulares. Por ejemplo, un usuario desde España puede realizar una compra en un comercio electrónico cuyos servidores físicos residen en el extranjero y, durante la transacción, la comunicación es interceptada por un ciberatacante que ocasiona fraude desde un tercer país, como se representa el *Figura 3.1*. Este hecho complica la identificación de los estafadores, por lo que no se puede erradicar el problema de la elevada tasa de pérdidas si no es con la definición de un método de pago seguro que evite la inserción y distribución online de los datos sensibles en un entorno internacional.

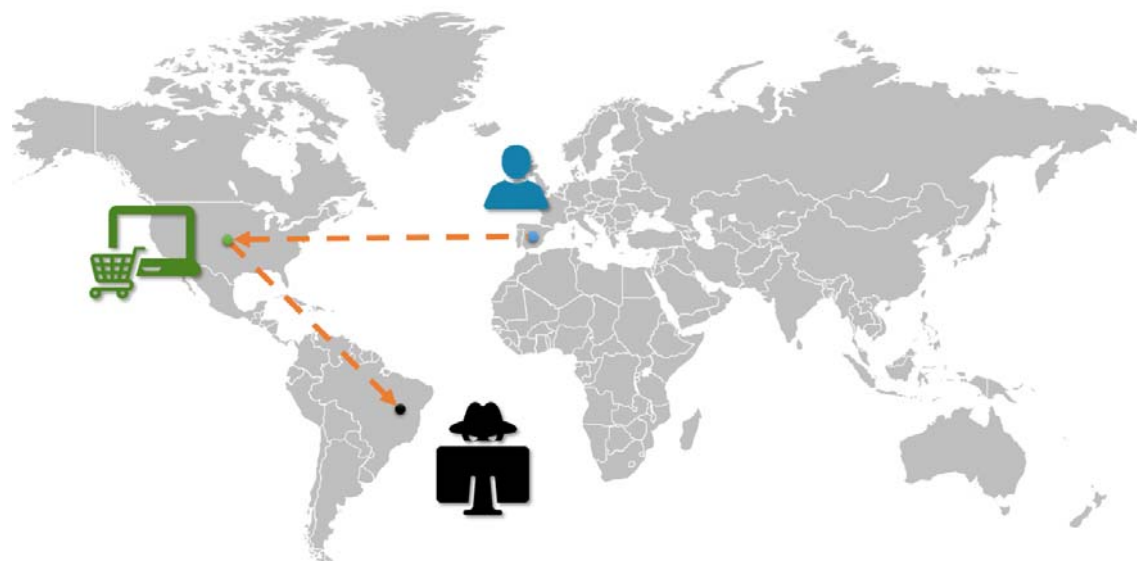


Figura 3.1 Representación del fraude online en e-commerce.

- **Robustez en transacciones con la tarjeta presente:** Aumento de la seguridad y robustez en transacciones que resuelven con la tarjeta presente, escenario donde la expansión del protocolo EMV representa un papel fundamental. El informe que recoge la actividad anual de Redsys durante el año 2016 muestra gráficamente (ver Figura 3.2), en tanto por ciento, la distribución del fraude en función del tipo de la transacción. En la imagen se muestra la comparativa del índice de fraude para cuatro operaciones diferentes: compras en comercio electrónico, compras en TPV insertando mediante tecleo manual los datos sensibles que figuran estampados en la tarjeta, pagos mediante el uso de la banda magnética de la tarjeta, y transacciones mediante protocolo EMV (llevadas a cabo mediante la presencia de la tarjeta inteligente, ya sea con interfaz de contactos o contactless). A partir de estos datos se desprende que en España el 60% del fraude se produce en comercio electrónico, siendo la principal causa de las pérdidas económicas en el sector de los medios de pago.

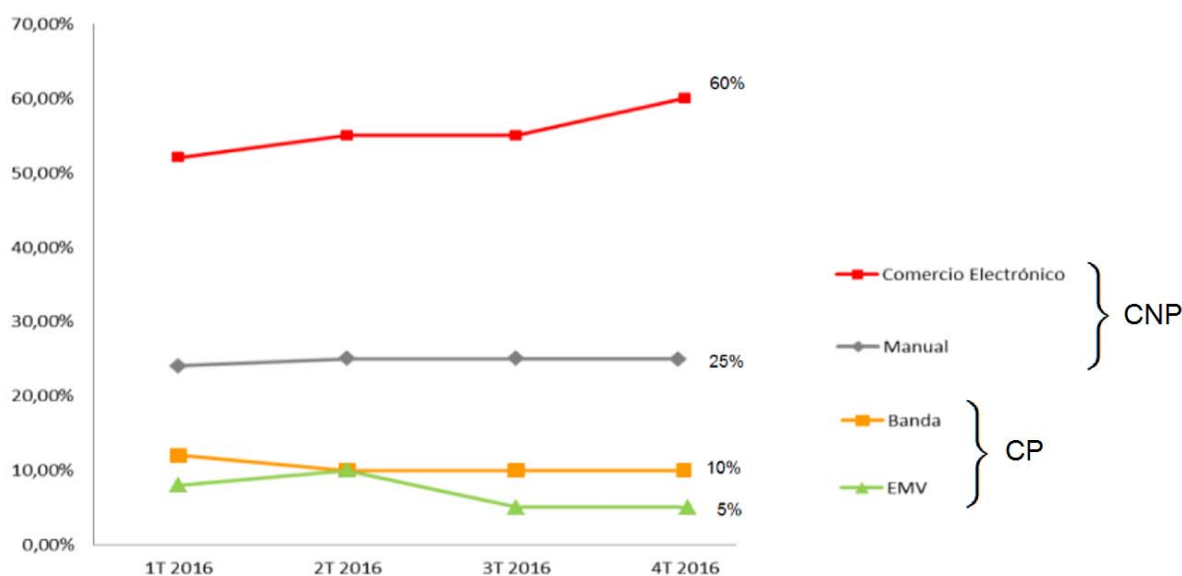


Figura 3.2 Distribución del fraude en función del origen de la venta (%) [8].

En el mundo de los medios de pago, se puede realizar una amplia diferenciación entre dos tipos de transacciones. Por un lado, en las que tanto el titular como la tarjeta deben estar presentes en el momento del cobro, por lo que se denominan transacciones CP (Card Present), siendo la operación típica que se realiza en los establecimientos físicos. En segundo lugar, existen las transacciones CNP (Card Not Present), que son las que se utilizan en comercio electrónico, previamente estudiadas en el *Capítulo 2*.

Hace unos años las transacciones CP no impedían que las tarjetas fueran copiadas o clonadas. Fue a partir del año 2002 cuando la seguridad en este tipo de operaciones se vio realmente reforzada. Este hecho surge gracias a la migración de la banda magnética al chip integrado y, por tanto, a la implantación del protocolo de comunicación EMV para el intercambio de comunicación entre la tarjeta inteligente y el terminal de pago, ofreciendo una alta protección contra el fraude [27]. Aunque la problemática de la seguridad en transacciones CNP lleva presente desde la aparición del comercio electrónico, fue a raíz de que se reforzase la seguridad en las operaciones CP, cuando los estafadores observaron que las posibilidades de éxito de los ataques fraudulentos residían en CNP.

Un estudio realizado por la prestigiosa empresa *Javelin Strategy&Research* en Reino Unido y Canadá, en el año 2014, comprobó que las pérdidas por fraude en transacciones CNP, eran muy superiores a CP y previó que esta brecha continuaría creciendo a lo largo de los años de forma significativa, lo que se ha ido cumpliendo.

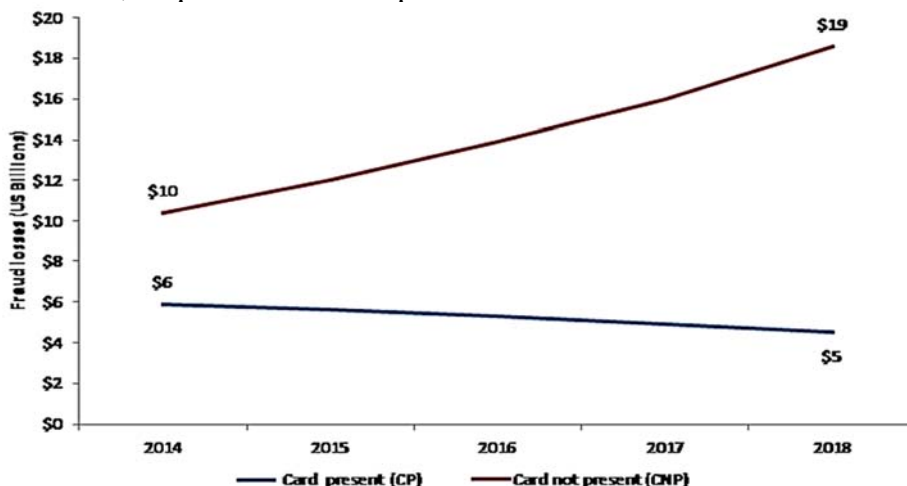


Figura 3.3. Estudio de la evolución del fraude en CNP y CP extrapolable a nivel mundial [28].

En Europa, en el año 2016, las pérdidas por fraude en transacciones CNP representaron más del 60% de las pérdidas totales de fraude financiero, valores coincidentes con el estudio de mercado de Redsys de la situación en España. Este problema presenta impacto a nivel mundial, ya que se estima que el fraude en e-commerce supondrá el 65% del fraude total en 2020 [29].

De tal forma que surge, más que nunca, la necesidad de estudiar nuevas soluciones de pago para comercio electrónico, que eviten estos riesgos y aporten robustez y fiabilidad en las transacciones financieras, siendo la principal motivación para la propuesta del presente TFM. Dado que el protocolo EMV supuso toda una revolución en los medios de pago, la idea es extrapolar su utilización en el comercio electrónico, incluyendo la presencia de la tarjeta en el flujo transaccional. Por este motivo, es imprescindible conocer los riesgos actuales del entorno online que la nueva solución debería evitar y estudiar las particularidades del protocolo de comunicación EMV a implementar.

3.2 ORIGEN Y TIPOS DE ATAQUES FRAUDULENTOS EN COMERCIO ELECTRÓNICO

Se define el concepto de estafa en comercio electrónico a la acción de utilizar los datos de una tarjeta financiera ajena, en un entorno online, sin estar autorizado a su uso por el titular de la misma, en beneficio propio y ocasionando daño patrimonial al propietario o a la entidad bancaria que cubra este tipo de operación delictiva. La Ley de Comercio Electrónico (LSSI, LSSICE o Ley 34/2002, del 11 de julio, sobre los Servicios de la Sociedad de la Información y de Comercio Electrónico) recoge parcialmente la Directiva comunitaria sobre obligaciones de los prestadores de servicios en comercio electrónico, estableciendo un régimen de responsabilidad específico según la causa y el entorno del fraude o de fuga de los datos [30].

En función del origen del fraude para la obtención de los datos sensibles financieros a utilizar en comercio electrónico, se puede establecer la diferenciación entre la actividad de robo o captura de datos en un escenario físico, o bien a través del uso exclusivo de internet.

3.2.1 Robo de los datos financieros en el entorno presencial

Los estafadores consiguen tener en su posesión la información sensible de la tarjeta, a partir de las siguientes técnicas ajenas al uso de Internet, aunque la finalidad de dicho fraude sea la obtención de bienes y servicios en el medio online.

- **Captura de la información estampada en la tarjeta:** La información sensible viene grafiada en la propia tarjeta, tal y cómo se expone en el Capítulo 1 y 2. De tal forma que a través de una fotografía, una grabación o una copia manual de los datos que aparecen en la misma, se podrían adquirir los campos necesarios (con el PAN y la fecha de caducidad es suficiente) para emprender una transacción financiera en un comercio electrónico.
- **Captura de la información almacenada en la banda magnética:** Las tarjetas chip continúan siendo emitidas con banda magnética. Este hecho se debe a dos factores claves, siendo el primero de ellos el uso de una tecnología de backup en el caso de que se produzca un daño en el chip (se prioriza siempre la posibilidad de pago, asumiendo el riesgo) y el segundo motivo, es porque la mayoría de cajeros dispone de un sistema de rodillos en el lector empotrado, con el fin de identificar que se trate de una tarjeta financiera y no permitir la inserción de otro tipo de acreditación, papel u objeto en el interior del hardware. De tal forma que, una técnica extendida, es el *skimming* [31]. Consiste en un lector de banda magnética fraudulento, que se coloca sobre la ranura de otro tipo de lectores, resultando muy difíciles de identificar, como puede ser en el interior de un cajero (ver *Figura 3.4*). La manipulación de este sistema permite a los delincuentes clonar y duplicar las tarjetas, obteniendo, por consiguiente, la información precisa para el pago en comercio electrónico. Cabe destacar que la banda magnética presenta un dato almacenado, correspondiente al código de servicio, que es diferente en función de si la tarjeta dispone de chip integrado o no. Ya que, si existe chip, la lectura del mismo debe ser el primer método que se debe utilizar en una transacción presencial. De esta forma, tras deslizar una tarjeta con chip y banda por el lector de banda magnética, el terminal notifica en su pantalla que se debe insertar la tarjeta, reduciendo la posibilidad de fraude en comercio presencial, por lo que los estafadores invierten más sus esfuerzos en el mundo online.



Figura 3.4 Manipulación de un cajero mediante técnica de skimming [31].

3.2.2 Robo de los datos financieros en un entorno no presencial

El robo de datos en un entorno no presencial o virtual, contempla el fraude logrado por el estafador mediante engaños vía telefónica, así como a través de un entorno online, escenario en el que se centra el estudio del TFM. Los timos por Internet son cada vez más frecuentes, produciéndose tanto para el robo de contraseñas con el fin de acceder a la información financiera de forma indirecta (contenida dentro de las aplicaciones e-wallet, el correo, los sistemas de almacenamiento o las redes sociales), así como para la obtención directa de los datos comprometidos de la tarjeta en el momento en el que el titular de la misma efectúa un pago online. A continuación, se exponen las principales técnicas fraudulentas utilizadas a través de Internet [32] [33] [34].

- **Snooping:** Está basado en la monitorización de las redes digitales para encontrar contraseñas u otros datos de origen personal. Este tipo de fraude puede utilizar, a su vez, otras técnicas, como la disposición del escritorio compartido del usuario o la monitorización de su pantalla (viendo en directo los datos que inserta en una compra online), la búsqueda en archivos basura para encontrar contraseñas u otra información sensible, etc. Es muy molesto y peligroso, y no todos los proveedores de internet (ISP, Internet Service Provider) protegen la privacidad de los clientes.
- **Spoofing:** En líneas generales, consiste en la sustitución de la dirección IP origen de un paquete, por otra dirección IP, a la cual se desea suplantar. Este tipo de fraude se consigue, generalmente, gracias a programas existentes destinados a tal fin y puede ser usado para cualquier comunicación dentro del protocolo TCP/IP.
- **Phishing:** Este método basa su fundamento en la suplantación de instituciones en las que, a priori, el usuario deposita su confianza, como puede ser entidades, bancos, sucursales de correo o seguros contratados. Normalmente el fraude se produce a través de un correo electrónico, que presenta adjunto un enlace dónde se solicita al usuario que actualice sus datos bancarios, o complete un pago pendiente. Una vez que los estafadores obtienen los datos, estos pueden ser utilizarlos para todo tipo de actividades delictivas. Los principales servicios afectados son las redes sociales, servicios de banca en línea de las entidades financieras más importantes y las aplicaciones de correo electrónico y mensajería.

Cada día, se produce la falsificación de unas 57.000 páginas web en el mundo. El ranking de los ocho sitios web más falsificados de la historia son: Ebay (23,21%), Western Union (21,15%), VISA (9,51%), United Services Automobile Association (6,85%), HSBC (5,98%), Amazon (2,42%), Bank of America (2,29%), y PayPal (1,77%).

- **Pharming:** Se trata de páginas web falsas, de cualquier tipo, en las que destacan aquellas destinadas a las descargas y a la compra online, en las que existe software maligno. Para evitar el fraude vinculado al pharming, se recomienda encarecidamente que los usuarios presenten atención a la URL del sitio web, verificando la cabecera *https* (HyperText Transfer Protocol Secure), que es, por excelencia, el protocolo destinado a la transferencia segura de datos.
- **Cookies:** HTTP cookie, web cookie o simplemente cookie, son series de texto que se envían de los servidores a los navegadores web, y de forma posterior se retransmiten desde dicho navegador. Son utilizadas para autenticar o mantener información específica del usuario como, por ejemplo, objetos en el carro de la compra de una tienda online, cuando el usuario accede a un sitio web que ya ha frecuentado con anterioridad. La utilidad principal es acceso inmediato a aquellos sitios en los que el usuario ya ha entrado, con el fin de facilitar su visita y su compra, si es el caso. El aspecto negativo, es que estas cookies ocupan espacio en el disco duro y son vulnerables al spyware, técnica que se detalla en el siguiente apartado. Otra problemática adicional, es el uso de un ordenador compartido en sitios públicos, ya distintos usuarios podrán acceder a las cuentas dónde otros tengan guardadas sus credenciales en las cookies, sin haber sido conscientes de este hecho.
- **Spyware:** Este software monitoriza el uso del usuario en la web y, posteriormente, muestra anuncios atractivos en función de las búsquedas que el usuario había realizado. También se le conoce como Adware y, en principio, únicamente se utiliza para enviar datos a las empresas de marketing. Sin embargo, se desconoce el potencial y el alcance de los espionajes derivados de esta técnica legal.
- **Smishing:** El concepto es similar al *phishing*, pero en este caso, los ciberdelincuentes envían los enlaces falsos a través de mensajes de texto (SMS). Los mensajes utilizados tienen la apariencia de SMS oficiales de las compañías reales y disponen de la opción de aceptar o cancelar sin dar mucha más información al respecto. Si el usuario acepta, es redirigido a un sitio web falso o bien a una aplicación sospechosa, dónde se solicita vía online la inserción de datos sensibles.
- **Malware:** Estas técnicas dirigen sus ataques a servidores críticos que almacenan información sensible, con el fin de bloquear, secuestrar o cifrar datos del disco duro (ransomware) o, por el contrario, realizar fugas masivas de datos de forma pública, comprometiendo la imagen de la industria y ocasionando pérdidas desmesuradas del capital.

3.3 PROTOCOLO DE COMUNICACIÓN EMV EN EL ENTORNO PRESENCIAL

El protocolo de comunicación EMV (Europay, Visa y MasterCard) [27] es un estándar de interoperabilidad segura que permite el intercambio de información entre una tarjeta inteligente con microprocesador (IC) y un terminal de pago (TPV), con el fin de autenticar transacciones financieras mediante tarjetas de crédito y débito. El fundamento de dicho protocolo está basado en la ISO 7816 [35], que define las características físicas (las dimensiones y localización de los chip), las señales electrónicas y los comandos de intercambio APDU (Unidades de Datos del Procolo de Aplicación) para tarjetas inteligentes con contactos, sean financieras o de identificación.

Este tipo de comunicación se ha ido introduciendo de forma escalonada en el mercado mundial de las transacciones presenciales como consecuencia de la rápida evolución y del extenso crecimiento de diferentes dispositivos tecnológicos compatibles con EMV (tarjetas inteligentes, wearables, etc.), al servicio de un negocio imperecedero, dada la necesidad de emisión de pagos seguros entre particulares y comercios en la sociedad actual. En la *Figura 3.5* se puede observar la comparativa, entre el año 2015 y el 2016, del porcentaje de transacciones que se resuelven mediante EMV respecto del total de operaciones llevadas a cabo con la tarjeta presente a nivel internacional.

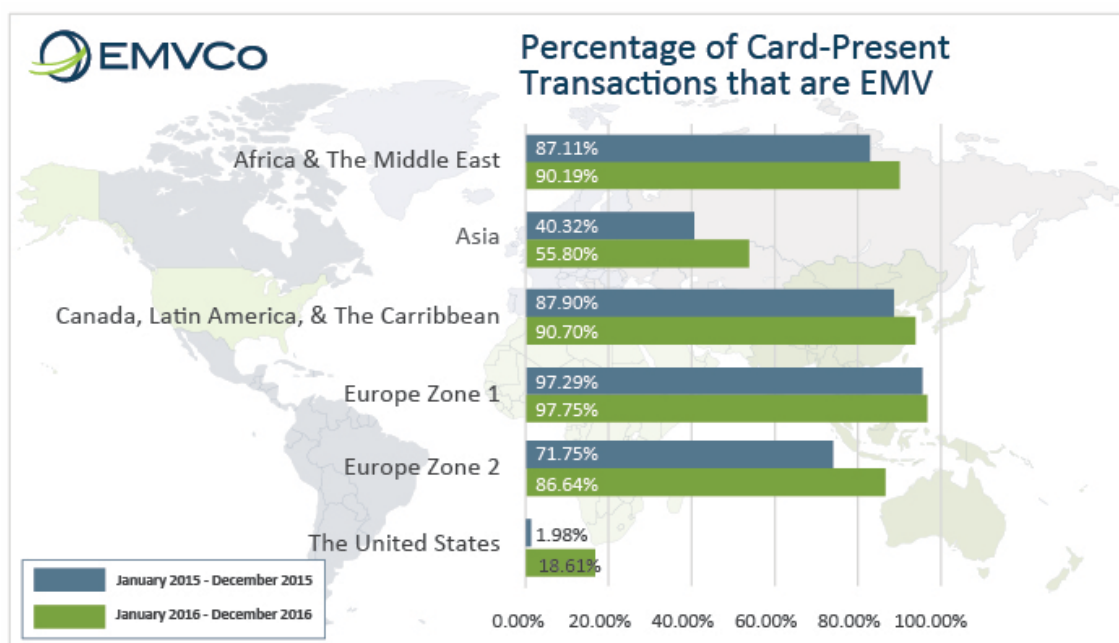


Figura 3.5. Porcentaje de transacciones financieras efectuadas mediante protocolo EMV [6].

Se verifica que el porcentaje de transacciones EMV continua creciendo de forma global. Europa es pionera en la utilización de tarjetas inteligentes con chip integrado, presentando una tasa de fraude en comercio presencial hasta tres veces menor que en EEUU, donde a pesar del abrupto crecimiento de expansión del protocolo EMV en los dos últimos años (incremento de nueve veces más), continúan siendo mayoritariamente fiel a la banda magnética. La inseguridad de la banda magnética reside en que los datos se almacenan en texto plano y con carácter estático, de tal forma que resulta sencillo y barato utilizar técnicas como *skimming* para la obtención de la información sensible necesaria para clonar la tarjeta y ocasionar fraude.

Las tarjetas chip, sin embargo, incorporan criptografía que permite el cifrado de los datos, haciendo uso de algoritmos como DES, Triple DES, RSA y SHA, además de autenticación dinámica y gestión de riesgos, por lo que garantizan integridad, autenticidad, seguridad y fiabilidad en las transacciones financieras.

El estándar EMV, para comunicaciones entre tarjetas inteligentes y TPV mediante interfaz con contactos, define la interacción a nivel físico, eléctrico y de aplicación. Sin embargo, para interfaz sin contactos, solo establece el marco común del protocolo de comunicación, sin describir detalles de aplicación compartidos. En este caso, cada una de las diferentes marcas utiliza su propia operativa, que EMVCo incorpora en especificaciones totalmente independientes en función del kernel, tal y cómo se indicó en el *Capítulo 1*. En la *Figura 3.6*, se muestra el diagrama que ofrece el escenario básico de una operación EMV estándar con tecnología con contactos, que viaja online a la red de pago, siendo la base comparativa para el resto de casuísticas y a continuación se describe brevemente cada una de las fases definidas en el proceso.

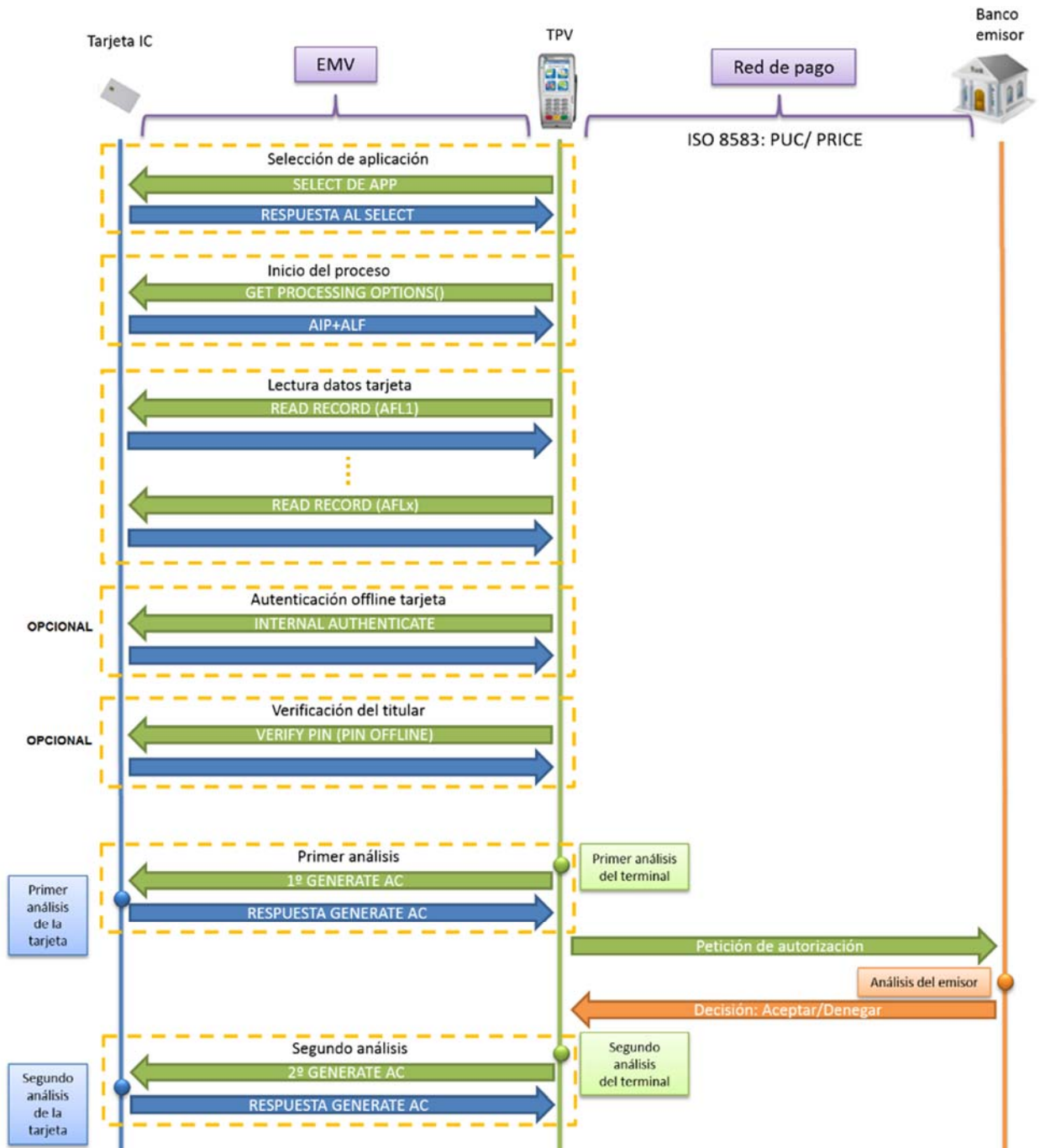


Figura 3.6. Transacción financiera con una tarjeta chip EMV mediante contactos.

Se exponen, de forma resumida, las diferentes fases y los comandos EMV [27] que participan en el proceso de comunicación entre el TPV y la tarjeta inteligente.

- **Selección de la aplicación:** El terminal dispone de una lista de aplicaciones financieras (AID, Application IDentifier) con las que muestra compatibilidad para realizar una transacción financiera, siendo certificado para ese fin. Las aplicaciones disponibles están definidas en la ISO/IEC 7816-5 [35] y en la *Tabla 3.1* se puede observar una muestra de las comunes. En este proceso se genera un listado de aquellas aplicaciones que son comunes entre el terminal y la tarjeta, pudiéndose obtener tres escenarios distintos:

- 1) **No existen aplicaciones comunes:** La transacción finaliza de forma inmediata, siendo imposible establecer una operación EMV. Esta justificación es uno de los motivos por lo que no todas las tarjetas son aceptadas en cualquier comercio.
- 2) **Solo existe una aplicación común:** El terminal de pago selecciona automáticamente la aplicación de la tarjeta, siendo este procedimiento transparente para el usuario. En el plano técnico, se traduce al envío de una sucesión de comandos SELECT por parte del terminal, donde únicamente se recibe respuesta satisfactoria a uno de ellos por parte de la tarjeta.
- 3) **Existen varias aplicaciones comunes:** El TPV muestra al titular de la tarjeta las diferentes aplicaciones disponibles, llevando a cabo el usuario una selección manual de aquella con la que desea operar. Este escenario es común para los portadores de una tarjeta inteligente donde, de forma simultánea, conviven una aplicación de crédito y débito, pudiendo notificar al personal del establecimiento en cuál de ellas desea recibir el cargo. En esta fase, se envían sucesivos SELECT por parte del terminal, donde a más de uno la tarjeta inteligente responde con éxito.

AID	APLICACIÓN
A000000003 1010	VISA DEB/CRED
A000000003 2010	ELECTRON
A000000003 2020	V PAY
A000000003 3010	INTERLINK
A000000003 8010	VISA PLUS
A000000004 1010	MASTERCARD
A000000004 6000	CIRRUS
A000000004 3060	MAESTRO
A000000004 6000	EUROCHEQUE

Tabla 3.1: Identificadores financieros.

Otro modo de funcionamiento relativo a la selección de aplicación, es la utilización del PSE (Payment System Environment). El terminal de pago manda un único SELECT con el valor del PSE, siendo '1PAY.SYS.DDF01' como se define en las especificaciones EMV [27]. La respuesta a este comando por parte de la tarjeta, contiene todos los datos necesarios para desencadenar la transacción. Sin embargo, la existencia del PSE en la tarjeta es opcional, de tal forma que no siempre está disponible una aplicación PSE que sirva de acceso o nexo al contenido de la información de las restantes.

- **Inicio de la aplicación:** Después de la selección de la aplicación EMV, el terminal obtiene de la tarjeta las opciones de procesamiento, derivando de este concepto la denominación que recibe el comando GET PROCESSING OPTIONS (GPO). Si la ejecución se realiza de forma correcta, la tarjeta inteligente devuelve en la respuesta al terminal los campos AIP (Application Interchange Profile, traducido como perfil de intercambio con la aplicación) y AFL (Application File Locator, que puede ser transcrito como la localización de los archivos de la aplicación).

El AIP se utiliza para describir las características que soporta la tarjeta, como es el tipo de autenticación de datos offline (estática, dinámica o combinada) o el método de verificación del titular (firma, pin online, pin offline en claro o cifrado, etc.). El terminal, en función de las mismas, desencadena un proceso, dando paso en fases posteriores a los comandos opcionales INTERNAL AUTHENTICATE y VERIFY PIN, si las condiciones lo permiten.

Gracias al campo AFL, el terminal puede determinar en qué registros de la tarjeta inteligente reside la información disponible para su lectura y recuperación de los datos de interés. Para su obtención, el terminal utiliza sucesivos comandos denominados READ RECORD en la fase posterior.

- **Lectura de los registros:** El terminal envía un comando READ RECORD por cada registro de la tarjeta, almacenado dentro de un fichero, del que desea adquirir los datos. La información se almacena en formato de estructuras TLV (Tag – etiqueta del campo, Length – longitud del valor en bytes, Value – valor de la etiqueta), y las tramas que se transmiten son en codificación hexadecimal.



Figura 3.7: Formato de estructura TLV.

En esta fase se recupera, entre otros campos, los datos de la pista 2 (como el PAN y la fecha de caducidad, ver *Tabla 3.2*), el código de país del emisor, la lista de prioridades en el método de verificación del titular (CVM, *Cardholder Verification Method*), los certificados, firmas y claves públicas y los datos de la aplicación seleccionada.

Name	Description	Source	Format	Template	Tag	Length
Track 2 Equivalent Data	Contains the data elements of track 2 according to ISO/IEC 7813, excluding start sentinel, end sentinel, and Longitudinal Redundancy Check (LRC), as follows: Primary Account Number Field Separator (Hex 'D') Expiration Date (YYMM) Service Code Discretionary Data (defined by individual payment systems) Pad with one Hex 'F' if needed to ensure whole bytes	ICC	b n, var. up to 19 b n 4 n 3 n, var. b	'70' or '77'	'57'	var. up to 19

Tabla 3.2. Datos correspondientes a la Pista 2 almacenados en el chip integrado.

- **Autenticación offline de los datos:** En función del AIP recibido por parte de la tarjeta en la respuesta al SELECT, el terminal está en disposición de realizar uno de estos tres métodos de autenticación:
 - 1) **SDA (Static Data Authentication):** El terminal verifica una firma digital estática almacenada en un registro de la tarjeta, y por lo tanto, recuperada en la respuesta del comando READ RECORD. Esta técnica permite garantizar la integridad de la información leída, pero no la autenticidad de la tarjeta, por lo que ya no se utiliza en el mercado europeo.

- 2) **DDA (Dynamic Data Authentication):** El procedimiento consiste en el envío del comando INTERNAL AUTHENTICATE, que contiene un dato aleatorio, para que la tarjeta calcule en función del mismo una firma digital con el fin de que el terminal pueda verificar la autenticidad de la tarjeta. De esta forma, se detecta si una tarjeta ha sido copiada, previniendo el fraude debido al empleo de técnicas como skimming.
 - 3) **CDA (Combined DDA/Application Cryptogram Generation):** Esta autenticación offline combina las funcionalidades de DDA con la generación del criptograma de la aplicación contenida dentro del comando GENERATE AC, permitiendo al terminal comprobar la autenticidad de la tarjeta.
- **Verificación del titular:** Para la constatación de que el usuario que desea realizar un pago es el titular de la tarjeta, se tiene que llevar a cabo uno de los métodos de verificación que estén disponibles, en función de las capacidades de la tarjeta (AIP y CVM) y del tipo de terminal. Se exponen a continuación los típicos modos de autenticar al titular:
- 1) **Pin cifrado offline:** El terminal envía a la tarjeta el número secreto introducido por el usuario mediante el comando VERIFY PIN, y es la propia tarjeta quién verifica al titular. La comunicación del valor PIN desde el TPV a la tarjeta se transmite cifrada.
 - 2) **Pin en claro offline:** Igual que el escenario previo, pero con la salvedad de que la información no se envía cifrada.
 - 3) **Pin cifrado online:** El valor del PIN insertado por el titular de la tarjeta se envía al centro de resolución de transacciones financieras, siendo el emisor quién verifica este campo y tiene en cuenta el resultado de dicha comprobación para la resolución de la operación.
 - 4) **Firma:** El titular debe firmar el ticket de compra suministrado por el personal del establecimiento, quién tiene la obligación de solicitar el DNI del cliente para la revisión manual de las firmas coincidentes. Si una vez que la compra ha sido finalizada con éxito, el trabajador del establecimiento detecta que el cliente no es el titular de la tarjeta, tiene la posibilidad de anular la venta previa.
 - 5) **Métodos combinados:** Se solicita al titular la inserción del PIN y la firma para completar una misma transacción. Este escenario suele ser común en un entorno internacional, dónde la tarjeta tiene un país de emisión distinto al país configurado por el terminal de pago.

- **Primer análisis del terminal:** El función de las condiciones producidas en el transcurso de la transacción, el terminal toma una primera decisión, que es comunicada a la tarjeta en el comando GENERATE AC. Las características que intervienen en la decisión son configuradas en el terminal, pudiéndose establecer múltiples parametrizaciones y combinaciones posibles, en función de los requerimientos del comercio físico o de la entidad que proporciona el terminal de pago. Para este primer análisis, se puede tener en cuenta, entre otros parámetros, si la autenticación offline de los datos ha fallado o no se ha realizado correctamente, si la inserción del PIN offline ha sido correcta o fallida, si la tarjeta es nueva o está caducada, etc. En función del resultado de este estudio, se pueden producir tres desenlaces diferentes:
 - 1) **Transacción denegada offline:** El terminal considera que tiene motivos suficientes para abortar la transacción, sin llegar a solicitar al emisor una petición de autorización.
 - 2) **Transacción aprobada offline:** El terminal, por su parte, aprobaría directamente la transacción, siempre y cuando la tarjeta está conforme. Este escenario no es común en España, aunque para operaciones requieren cierta rapidez, como por ejemplo los peajes, sí se utiliza.
 - 3) **Solicitud de autorización online:** Es el entorno típico, donde el terminal indica a la tarjeta que desea solicitar la aprobación del centro de resolución. Si la tarjeta está de acuerdo, la transacción viaja online. Dicha operación solo será denegada si la tarjeta dispone de motivos suficientes para ello y no desea consultar al centro de resolución.

- **Primer análisis de la tarjeta:** La tarjeta recibe en el comando PRIMER GENERATE AC la decisión determinada por el terminal de pago. En función y condicionada a la misma, la tarjeta también tiene la posibilidad de intervenir en el desenlace de la operación, respondiendo siempre con la misma decisión del terminal o con una determinación más restrictiva. Ver *Tabla 3.3*.

Decisión del terminal	Posibles decisiones de la tarjeta
Transacción denegada	Transacción denegada
Petición online	Petición Online/Denegada
Transacción aprobada	Online/Aprobada/Denegada

Tabla 3.3: Posibles decisiones de la tarjeta en función de la decisión del terminal.

La tarjeta respalda y fundamenta su determinación en función de la actual transacción y de las operaciones previas. Puede tener en cuenta, entre otras comprobaciones, si la tarjeta es nueva, si el número de intentos de PIN ha sido excedido, si se han superado ciertos límites de acumuladores y contadores internos, si la transacción anterior no fue completada, etc. Finalmente, la decisión es transmitida desde la tarjeta al TPV en la respuesta al comando PRIMER GENERATE AC, pudiendo concluir la transacción mediante dos modos distintos de conexión:

- 1) **Transacción offline:** Si la tarjeta notifica con un criptograma la aprobación o denegación, el terminal muestra en la pantalla la resolución al titular de la tarjeta y finaliza la transacción.

- 2) **Transacción online:** Si la tarjeta envía una solicitud de petición online, el terminal establece las comunicaciones pertinentes con el centro de resolución de transacciones financieras. Tras la recepción de la respuesta de la red de pago, tiene lugar el segundo análisis del terminal.
- **Segundo análisis del terminal:** En función del éxito en la comunicación entre el terminal de pago y el centro de resolución, se puede decretar la siguiente clasificación:
- 1) **La transacción no puede llevarse a cabo online:** Si se produce un problema de conectividad, y tras sucesivos reintentos automáticos de llamada no se solventa, el terminal debe realizar una segunda decisión. Si detecta algún tipo de inconveniente para la aprobación de la transacción, el terminal comunicará la denegación a la tarjeta en el comando SEGUNDO GENERATE AC. Si por el contrario, el terminal está parametrizado para que en circunstancias específicas, como un fallo en la comunicación, la operación sea aceptada, notificará en dicho comando su deseo de aprobar la transacción. En esta fase, bajo ningún concepto, se enviará una nueva solicitud de ir online.
 - 2) **La transacción se resuelve online y se recibe la respuesta del centro autorizador:** El terminal comunica la respuesta del emisor a la tarjeta (operación aceptada o denegada) y presenta el criptograma del emisor en el SEGUNDO GENERATE AC, para que la tarjeta lo valide y tome la última decisión de la operación.
- **Segundo análisis de la tarjeta:** La tarjeta recibe la respuesta del emisor a través del terminal de pago. Si la transacción ha sido denegada, la tarjeta únicamente puede contestar del mismo modo. Si por el contrario, ha sido aprobada, se debe validar la autenticación del emisor para determinar la última decisión del flujo transaccional, pudiéndose producir uno de los siguientes escenarios:
- 1) **Autenticación del emisor satisfactoria:** La tarjeta valida los datos recibidos del centro de resolución correctamente y envía un criptograma de autorización al terminal de pago, reseteando todos los contadores internos offline. En este caso, se dice que la operación ha sido aprobada online.
 - 2) **Autenticación del emisor errónea:** Si la tarjeta al realizar la verificación de los datos recibidos desde el centro autorizador detecta alguna anomalía y considera que la respuesta procede de un origen fraudulento, envía un criptograma de denegación al terminal, que a su vez solicita una anulación al centro de resolución oficial.

Existen más comandos pertenecientes a EMV que dotan de mayor flexibilidad operacional al protocolo de comunicación, pero que quedan fuera del flujograma básico y no son de interés o relevancia en el estudio en curso.

Para las comunicaciones sin contactos, grosso modo, se pueden destacar las siguientes diferencias significativas respecto a la operativa básica definida para la tecnología con contactos.

- **Última decisión del desenlace de la transacción:** En la operativa básica con contactos, tras la aceptación por parte del centro autorizador, la tarjeta toma la última decisión sobre el resultado de la operación. Sin embargo, en los dispositivos contactless, la tarjeta no participa en la decisión del resultado de la transacción una vez que ya ha sido aprobada por la entidad autorizadora. El motivo de esta evolución viene dado por la prevalencia de la velocidad antes que la seguridad, ya que el escenario ideal es que sea el propio cliente quién aproxime su tarjeta al terminal de pago, una única vez y sin cedérsela a un tercero.
- **Verificación del titular:** Cuando una transacción se resuelve mediante interfaz con contactos, se aplica uno de los métodos disponibles de verificación de titular. Los casos, plenamente excepcionales, dónde esto no ocurre son en máquinas de vending y en algunos parking o peajes, asumiendo el riesgo de que el cliente no sea el titular de la tarjeta. En el caso de la operativa sin contactos, se define a nivel europeo, que no se verifique a titular a no ser que el importe de la transacción sea mayor o igual a 20.00€ en el caso de tarjetas Visa, y mayor a 20.00€ (desde 20.01€) para MasterCard. Esta medida se justifica por la importancia que se concede a la velocidad transaccional en operaciones donde el riesgo no es elevado (importes pequeños) y además el tráfico es monitorizado, pudiendo detectar fraude ante movimientos repetitivos o poco comunes. Un ejemplo podría ser un surtidor de gasolina que no es atendido por ningún operario; una persona que se encuentra una tarjeta contactless podría suministrarse 19.99€ con concepto “gasolina”. Sin embargo, si esta operación fraudulenta se repitiera de forma consecutiva, saltarían las alarmas del equipo de detección de fraude de los centros procesadores.
- **Flujograma de trabajo de la aplicación:** Las comercializadoras de tarjetas no llegaron a un acuerdo para tener un diagrama funcional de aplicación común, de tal forma que EMVCo define hasta siete especificaciones distintas en función del kernel, como recoge la *Tabla 3.4*.

Identificador del Kernel	AID de la aplicación
Kernel 1	JCB AIDs (algunas de Visa)
Kernel 2	MasterCard AIDs
Kernel 3	Visa AIDs
Kernel 4	American Express AIDs
Kernel 5	JCB AIDs
Kernel 6	Discover AIDs
Kernel 7	UnionPay AIDs

Tabla 3.4: Posibles AIDs en función del Kernel [36].

En la *Figura 3.8* se representan las fases comunes de activación del protocolo de comunicación sin contactos y el intercambio de los comandos EMV Contactless que son similares para todos los kernel, siendo la etapa común a nivel de aplicación, la correspondiente a la selección.

- **Selección de la aplicación:** El terminal envía un comando SELECT del PPSE (Proximity Payment System Environment), siendo de valor '2PAY.SYS.DDF01' [37]. La filosofía de funcionamiento es análoga al método de contactos para la selección del PSE, con la salvedad de que en contactless este campo y su uso es de carácter obligatorio. La tarjeta devuelve en la respuesta el ADF Name (Application Definition File), que es similar al AID, y opcionalmente comunica el identificador del kernel con el que el terminal debe trabajar. La mayoría de tarjetas en circulación no tienen el campo correspondiente al kernel, ya que la definición de este concepto ha sido incorporada recientemente en las especificaciones. El terminal, por lo tanto, debe determinar el modo de proseguir en función del AID de la tarjeta inteligente, estableciendo la relación que se muestra en la tabla anterior.

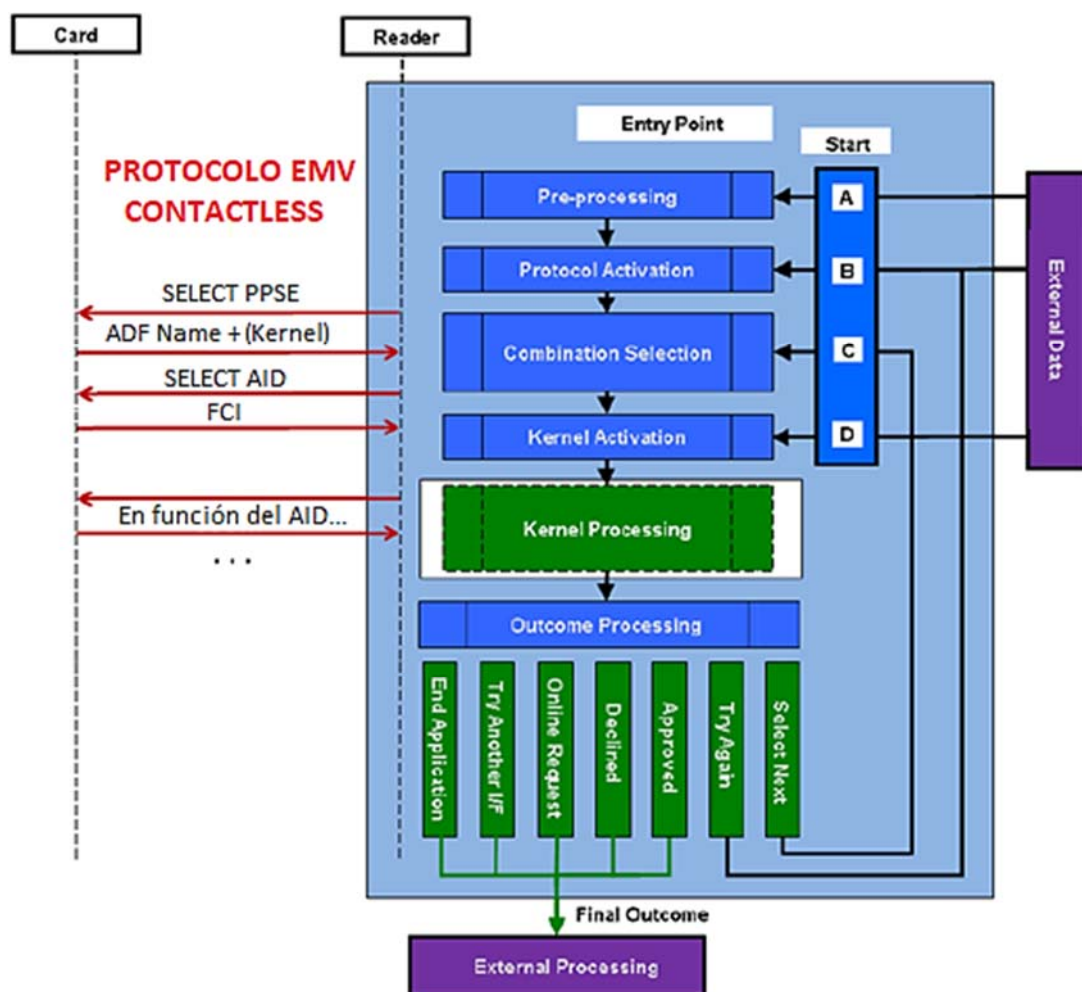


Figura 3.8: Diagrama genérico de activación del protocolo e intercambio de comandos EMV Contactless.

El proyecto se centra en las tarjetas Visa y MasterCard, que son aquellas que presentan mayor volumen de tarjetas en España, tal y cómo se describe en el *Capítulo 1*.

Por lo tanto, los kernel a estudiar, son:

- **Kernel 2:** AID de MasterCard [38]

La definición del modo funcional de aplicación para las tarjetas MasterCard en relación al interfaz sin contactos es muy similar a la operativa de contactos, manteniéndose fiel, en la medida de lo posible, al flujograma de trabajo inicial. Como en el uso de la tecnología sin contactos prima la velocidad de transacción, la tarjeta se retira antes de conocer la respuesta del centro de resolución y, por lo tanto, el último comando EMV transmitido es análogo al PRIMER GENERATE AC de contactos. En la *Figura 3.9* se detalla el diagrama específico correspondiente a este kernel, siendo los comandos que aparecen similares a los explicados con anterioridad.

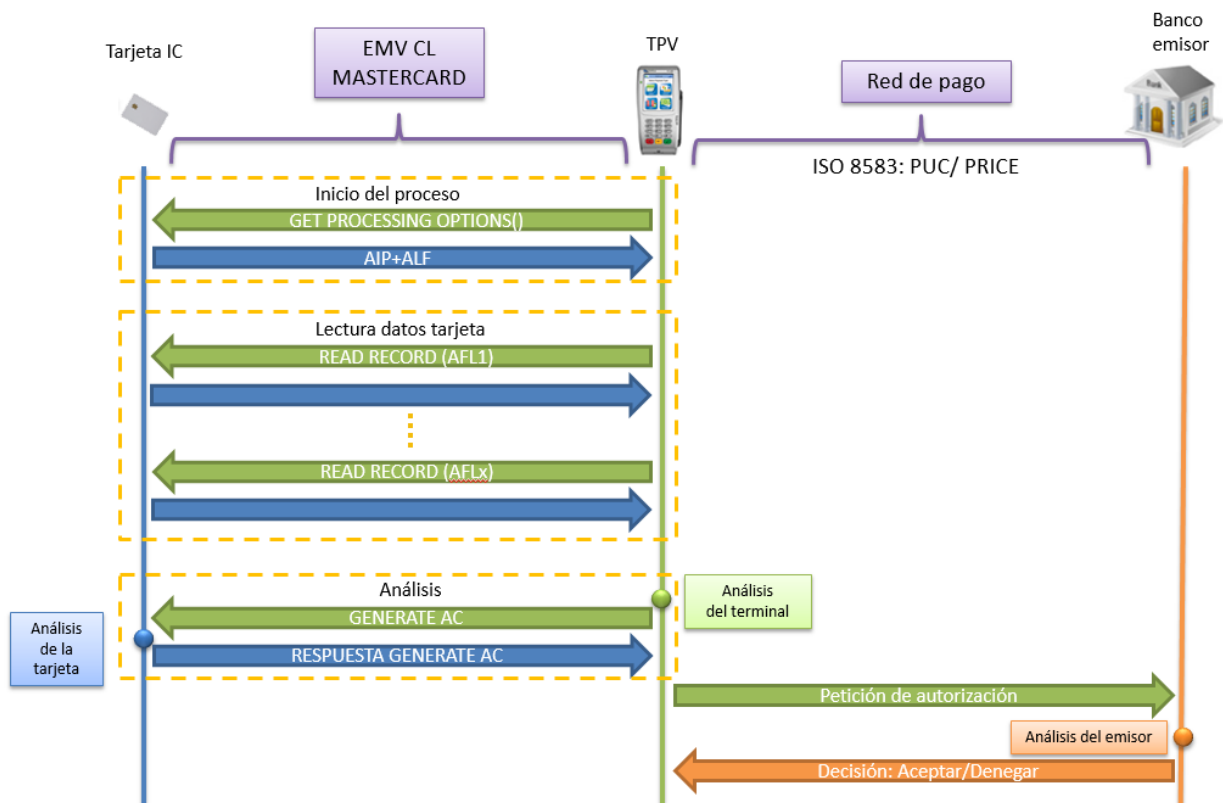


Figura 3.9: Diagrama del kernel para el AID de MasterCard.

- **Kernel 3:** AID de VISA [39]

La definición que se establece en el kernel 3 rompe con el sistema estudiado hasta el momento, ya que se produce un rediseño de los comandos que intervienen en la comunicación. Tras la fase de selección de la aplicación, el único comando de carácter obligatorio necesario se denomina GET PROCESSING OPTIONS, pero no es similar al estudiado para las transacciones con contactos ni para las operaciones contactless de tarjetas MasterCard. En este caso, el GPO adquiere un rol mucho más importante, transmitiendo la tarjeta VISA Contactless, en su respuesta, toda la información necesaria para la operación. La fase de lectura de registros (READ RECORD) no es obligatoria, ya que como se observa en la *Tabla 3.5*, ciertos campos de interés, como son los datos de la pista 2 (PAN y fecha de caducidad), se pueden adquirir tanto del comando GPO como de los READ RECORD para el caso del AID de VISA.

Name (Format; Tag; Length; Source; Path)	Requirement	Description	Retrieval
Track 2 Equivalent Data F: b T: '57' L: var. up to 19 S: Card	Mandatory	Contains the data elements of the Track 2 according to the [ISO 7813], excluding start sentinel, end sentinel, and LRC	GPO, READ RECORD

Tabla 3.5: Datos de la pista 2 para el AID VISA.

En la respuesta a los comandos READ RECORD, la tarjeta proporciona los certificados RSA y la información necesaria para que el terminal pueda validar el hash de los datos estáticos. En el caso de la implementación del prototipo de la solución propuesta, se programan únicamente los comandos que son de carácter obligatorio.

En la *Figura 3.10* se representa el flujo transaccional específico para el kernel 3.

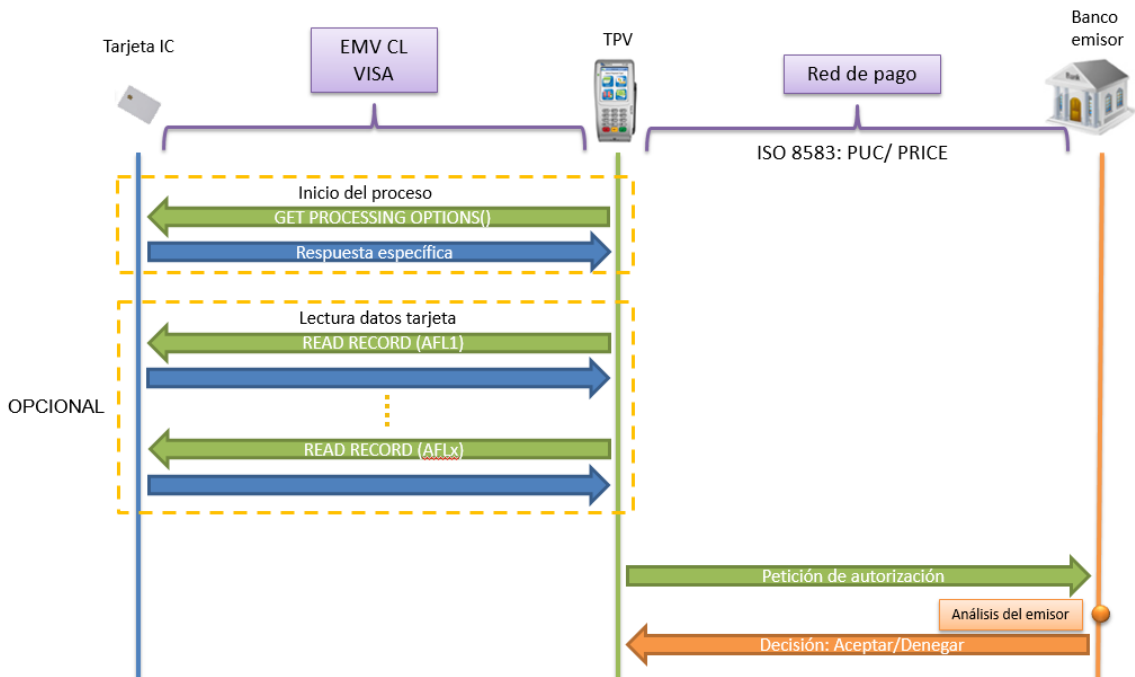


Figura 3.10: Diagrama del kernel para el AID de VISA.

Capítulo 4

Análisis de la solución y propuesta CSPay

4.1 ESTRUCTURA GLOBAL DE LA SOLUCIÓN PROPUESTA

Existen múltiples opciones de pago en comercios virtuales como se detalla en el *Capítulo 2*, pero ninguna de ellas, hasta la fecha, ha conseguido disminuir la elevada tasa de fraude como se muestra en el *Capítulo 3*. Actualmente los ataques fraudulentos se centran en las transacciones llevadas a cabo mediante comercio electrónico, siendo un entorno más expuesto a fraude que el pago con tarjeta inteligente en los comercios físicos. Dado que se producen altas pérdidas por fraude online y la presencia de la tarjeta aporta seguridad, surge la idea de integrar la operativa conceptual y técnica del mundo presencial al entorno virtual.

Se resume el fundamento básico de la propuesta del TFM como la incorporación de la presencia física de las tarjetas contactless financieras en los sistemas de comercio electrónicos actuales. Para poder integrar la tarjeta en un escenario e-commerce, se necesita un dispositivo con tecnología NFC que establezca la lectura de la misma. Por lo tanto, se requiere en el diseño la incorporación del teléfono móvil del titular de la tarjeta como herramienta para la comunicación con la tarjeta contactless. La definición de esta nueva solución de pago surge con la motivación de satisfacer los siguientes propósitos:

- **Reducir la elevada tasa de fraude actual en e-commerce e inspirar seguridad a los usuarios:** La presencia de la tarjeta física y del protocolo de comunicación EMV en una transacción financiera garantiza la robustez, integridad y autenticidad de los datos sensibles en el entorno transaccional. En el presente TFM se utiliza el protocolo de comunicación EMV Contactless entre el dispositivo móvil con tecnología NFC del usuario y la tarjeta inteligente contactless.

- **Mejorar la experiencia de usuario.** La tendencia de otras soluciones competidoras en el mercado es la simplificación al máximo del proceso de pago, aun sacrificando la seguridad (como por ejemplo, *OneClick*). En la solución propuesta se desea llegar a un equilibrio entre la usabilidad y la seguridad. La incorporación de la tarjeta en el contexto online, requiere que el usuario realice la acción de aproximar la tarjeta contactless al lector NFC de su dispositivo móvil, emulando el movimiento que realizaría para el pago con tarjeta contactless en un TPV en un comercio físico.

El nuevo método de pago propuesto, se denomina *CSPay*, por sus siglas en inglés de *Customer Self Pay*. La elección de este nombre viene dada porque es el propio cliente quién de forma autosuficiente lleva a cabo el pago a través de dos elementos seguros de los que ya dispone, como son su propio dispositivo móvil y su tarjeta física. La propuesta consiste en la inserción del número de teléfono móvil del cliente, en vez de los datos sensibles asociados a la tarjeta (PAN, fecha de caducidad y CVV2), en el formulario de pago de la página web de un comercio electrónico. Por lo tanto, se considera que esta solución eliminaría los ataques asociados a técnicas como *phishing* y *pharming*, mejorando la seguridad de la transacción financiera.

Otra ventaja añadida que presenta esta alternativa, es que los comercios electrónicos dejarían de manejar datos sensibles de las tarjetas (PAN, fecha de caducidad, CVV2). De esta forma, no tendrían que cumplir y renovar las auditorías relacionadas con las certificaciones PCI DSS (*Payment Card Industry Data Security Standard*). Dicho estándar de seguridad de datos para las tarjetas de pago surge tras la fusión de los programas de protección de datos de Visa, MasterCard, American Express, Discover y JCB, obligando a todos los participantes en el proceso de pago que acepten, guarden o transmitan datos de tarjeta, a cumplir estrictas normas de seguridad, que implican un desembolso importante, y no garantizan la inexistencia de fraude. Además, el incumplimiento de esta normativa conlleva sanciones económicas de gran envergadura [40]. Por lo tanto, esta nueva solución podría suponer gran aceptación por parte de los comercios electrónicos.

Respecto a la figura del cliente, se han analizado estudios del mercado de los últimos meses que reúnen las impresiones de los usuarios ante un escenario *e-commerce*. Los datos revelan que los clientes priorizan la seguridad frente a la rapidez en sus compras online, y algunos participantes señalan explícitamente que están preocupados por la seguridad en sus compras en Internet [41]. El marco social hace pensar que la nueva solución podría llegar en un momento idóneo para su expansión.

Para el diseño y definición técnica de la idea, se ha llevado a cabo un estudio de las diferentes alternativas funcionales y tecnológicas existentes para cada una de las etapas que constituyen la solución (ver *Figura 4.1*). Se examina la viabilidad y usabilidad de cada una de las etapas indicadas, con el fin de seleccionar aquella opción que más se adecúe a los objetivos planteados.

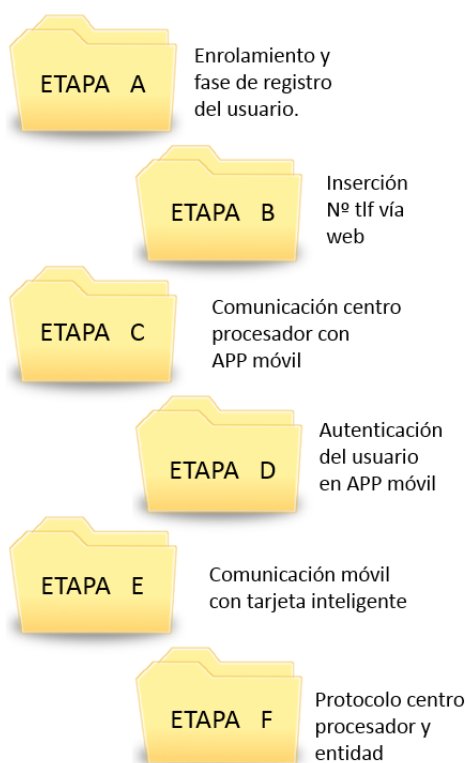


Figura 4.1.:Estructura global de la solución propuesta.

Se describe brevemente el alcance de cada una de las etapas y las funcionalidades básicas que deben satisfacer para el posterior análisis de la estructura final de la solución *CSPay* (ver Apartado 4.2).

- **Etapa A:** Corresponde a la fase de enrolamiento y registro del usuario. El cliente que decida darse de alta en el servicio, debe registrar un único dispositivo móvil (con sistema operativo Android y tecnología NFC soportada) con el que desee realizar las compras mediante comercio electrónico. El sistema permite asociar diferentes tarjetas financieras a un mismo dispositivo móvil, ya sea a través de la aplicación móvil o desde la entidad financiera.
- **Etapa B:** Consiste en la inserción del número de teléfono por parte del usuario en el formulario web. En el proceso de una transacción e-commerce utilizando el método de pago *CSPay*, el propio comercio o la librería de Redsys solicita el número de teléfono móvil en vez de los datos sensibles asociados a la tarjeta (PAN, fecha de caducidad y CVV2).
- **Etapa C:** Atañe a la transmisión de información entre el centro procesador (Redsys) y la aplicación móvil del cliente. Se deben estudiar diferentes escenarios para la implementación de dicha comunicación, como son las distintas opciones que ofrece la mensajería push o el Servicio Móvil Multipago (SMM).

- **Etapa D:** Afecta a la primera autenticación del usuario a través de la aplicación móvil. Tras la recepción de una notificación en relación a una solicitud de pago, el usuario debe desbloquear su dispositivo móvil y proceder con la autenticación.
- **Etapa E:** Concierno a la conexión entre el teléfono móvil y la tarjeta inteligente, con el fin de realizar la segunda autenticación. El usuario deberá aproximar su tarjeta contactless financiera al dispositivo móvil NFC, obteniendo una experiencia muy parecida al pago presencial.
- **Etapa F:** Impacta en el protocolo de comunicación entre el centro procesador (Redsys) y la entidad financiera emisora de la tarjeta con la que se ha llevado a cabo la transacción.

4.2 ANÁLISIS DE LAS POSIBLES ALTERNATIVAS TÉCNICAS

Dados la estructura global de la solución propuesta y los objetivos a satisfacer en el diseño final, se realiza un estudio tecnológico de las diferentes alternativas existentes para abordar cada una de las etapas que constituyen el proyecto.

4.2.1 ETAPA A: Fase de enrolamiento y registro del usuario

Se analizan dos alternativas diferentes para determinar qué organismo va a llevar a cabo la inscripción de los usuarios en el nuevo método de pago. Dada la experiencia de Redsys en el almacenamiento centralizado de información sensible (un ejemplo destacable sería Bizum, que está respaldado por Redsys), se establece para ambos escenarios que sea el centro procesador quién albergue en un directorio los datos necesarios del cliente para la implementación del proyecto. Se recogen a continuación los datos mínimos requeridos:

- Número de teléfono del titular de la(s) tarjeta(s) o de la persona autorizada.
- PANes de las tarjetas con las que se desee llevar a cabo transacciones financieras mediante comercio electrónico.

A1 – Las entidades financieras proporciona la información de los usuarios a Redsys

Los bancos que deseen ser partícipes de esta nueva solución de pago ofertarán a sus clientes la posibilidad de dar de alta o baja sus tarjetas financieras en el servicio (por ejemplo, vía web o presencial en sus oficinas) y comunicarán a Redsys dicha información según sea planificado. Una posible alternativa, sería definir una comunicación diaria (cierre del día) entre las diferentes entidades financieras y Redsys, dónde se proporcione la información de altas y bajas de los clientes o cualquier tipo de modificación en el servicio (alta y baja de tarjetas financieras del directorio).

A2 - Método combinado para dar de alta o baja un nuevo usuario en el servicio

Se complementa la opción anterior con la posibilidad de que el usuario desde la propia aplicación móvil pueda enviar la solicitud de alta o baja de su(s) tarjeta(s) física(s) financiera(s) en el servicio. Existirá una opción en el menú de la aplicación móvil destinada para este fin, y el cliente podrá aproximar la tarjeta que desee utilizar. El centro procesador de Redsys gestionará la petición y enviará la solicitud de alta a la entidad emisora de la tarjeta aproximada por el cliente.

Si la entidad confirma que la tarjeta del cliente está operativa, desde Redsys se enviará un código de seguridad (vía SMS) al teléfono móvil que el titular de la tarjeta haya proporcionado a su banco. De esta forma, se podrá autenticar al cliente, sobre todo en aquellos casos en los que el número móvil que se desee registrar para el pago mediante CSPay sea distinto al que posee la entidad financiera.

La aplicación móvil solicitará al cliente la inserción del código de seguridad con el fin de completar el proceso de alta para cada una de las tarjetas nuevas. En la *Figura 4.2* se adjunta el esquema resultante.



Figura 4.2. Solicitud de alta de una nueva tarjeta en el servicio desde la aplicación móvil.

4.2.2 ETAPA B: Obtención del número de teléfono móvil vía web

Para iniciar una transacción en un escenario de comercio electrónico mediante el método de pago *CSPay*, se requiere la obtención del número de teléfono móvil del cliente. Se establece una diferenciación en función del organismo que facilite el formulario al cliente y recupere el valor de este campo.

B1 - El comercio electrónico solicita el número de teléfono al cliente

Las páginas web de los comercios electrónicos tendrían que incluir un formulario para brindar la oportunidad al titular de la tarjeta de insertar el número de teléfono móvil del dispositivo con el que desea efectuar el pago. A continuación, el comercio electrónico que necesitase llevar a cabo la venta, transmitiría dicho número de teléfono al centro procesador de transacciones de Redsys.

De forma global se descarta esta opción porque implicaría un alto impacto en la modificación de todas las páginas web de los comercios electrónicos que quisieran acogerse a esta nueva solución de pago. Cabe destacar que el Reglamento General de Protección de Datos de la UE (RGPD) unificará la ley de protección de datos en toda la UE a partir del 25 de mayo de 2018, sustituyendo automáticamente a las leyes nacionales. Dicho Reglamento introduce una serie de cambios clave que afecta a todas las organizaciones que procesan datos personales de los residentes de la UE (ya sea de tarjeta financiera o personales), por lo que los comercios no estarían a priori interesados en añadir complejidad a su sistema actual. Incluso se prevé que ciertos establecimientos online deleguen sus sistemas de pago actuales en librerías de pago de Redsys, con el fin de evitar satisfacer todos los criterios que reúne PCI DSS y RGPD.

El flujograma de esta solución, que ha sido descartada, se puede observar en la *Figura 4.3*

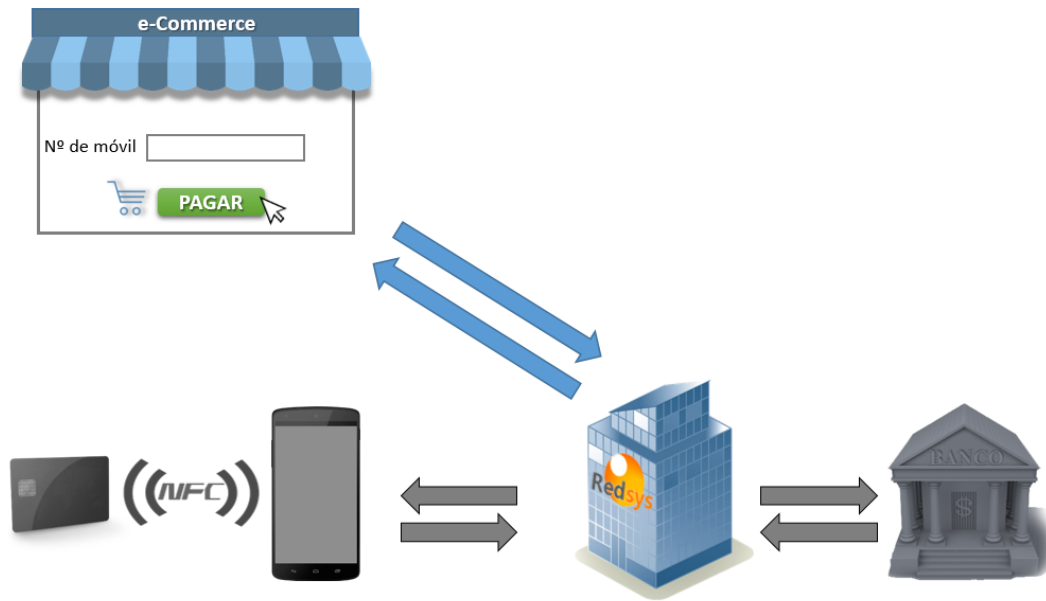


Figura 4.3. Solicitud del número de teléfono móvil desde la página web del comercio electrónico.

B2 - Se añade en la librería de Redsys el nuevo método de pago

La propuesta por excelencia es la incorporación de un nuevo método de pago en el desplegable de opciones de la librería de Redsys (*Figura 4.4*), añadiendo la posibilidad de “Pagar con CSPay” dentro del formulario, permitiendo al cliente insertar su número de teléfono móvil en vez de los datos sensibles de la tarjeta.

Pagar con Tarjeta

Nº Tarjeta:

Caducidad: mm aa

Cód. Seguridad: ?

Figura 4.4: Desplegable de opciones de pago actuales en comercio electrónico.

Este cambio sería prácticamente transparente para los comercios electrónicos que actualmente integran en sus sitios web el módulo de la pasarela de pago (TPV virtual) que proporciona Redsys, ya que únicamente tendrían que reemplazar la librería anterior por la nueva que se les facilitase.

Un informe de *Adigital* en base a una encuesta realizada a más de 2000 empresas de comercio electrónico en España [42], determina que el método de pago con mayor integración en los sitios web *e-commerce* es el TPV Virtual (ver *Figura 4.5*). De tal forma que la incorporación de un nuevo método de pago en dicho formulario, podría suponer una alta aceptación por parte de todos los establecimientos virtuales que ya utilizan este sistema.

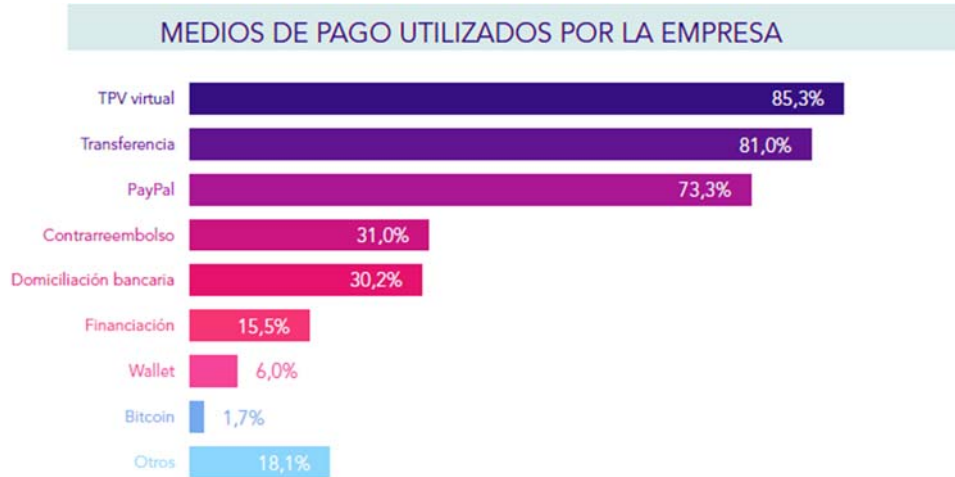


Figura 4.5: Opciones de pago que proporcionan los comercios electrónicos encuestados de España [42].

Se muestra el flujograma resultante de la alternativa seleccionada en la *Figura 4.6*. Para el resto de diagramas de flujo que aparecen en el presente capítulo se tendrá en cuenta esta primera decisión.

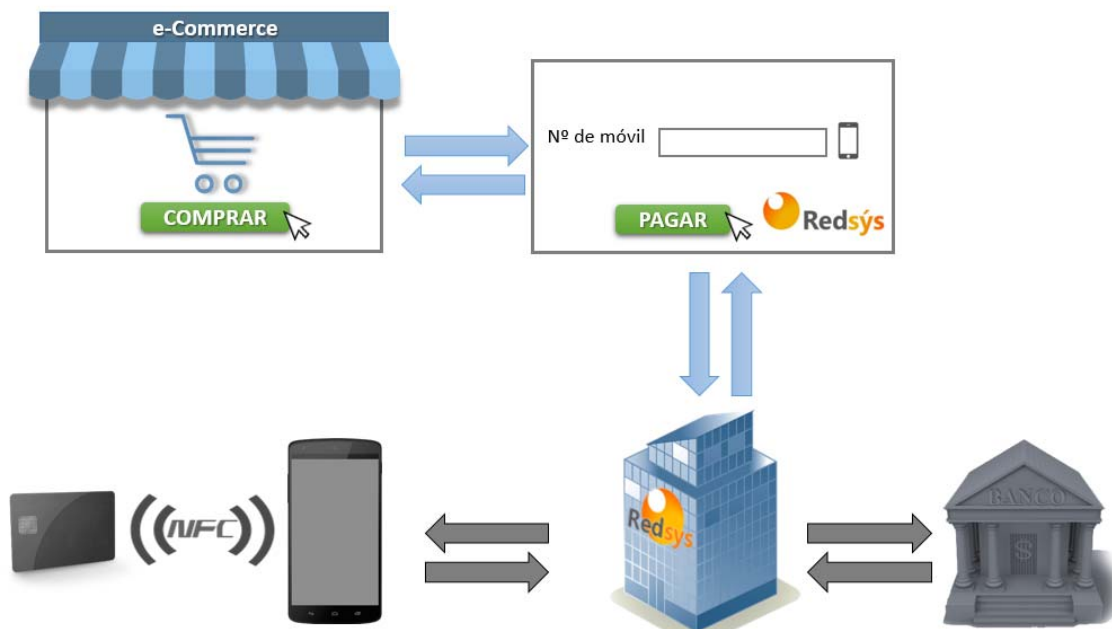


Figura 4.6: Solicitud del número de teléfono móvil del cliente desde la librería de Redsys.

4.2.3 ETAPA C: Comunicación entre el centro procesador y la aplicación móvil

Se desea que el nuevo método de pago presente una buena experiencia de usuario, por lo que se establece como objetivo que el proceso sea fácil e intuitivo. Con el fin de satisfacer dicho requerimiento, se determina que una vez que el titular de la tarjeta ha insertado su número de teléfono en la página web, la aplicación del dispositivo móvil se inicialice automáticamente, solicitando la contraseña de acceso al cliente. Se descarta, por tanto, en esta fase inicial, que sea el propio usuario quién tras la inserción del número de teléfono móvil en la página web, inicie manualmente la aplicación móvil desde su dispositivo. Se estudian distintos escenarios técnicos con el fin de hallar la solución óptima.

C1 - Mensajería push

Para el desarrollo del proyecto se propone el envío de un mensaje push directo desde el centro procesador de Redsys a la aplicación instalada en el dispositivo móvil del cliente. Se descarta el envío de un mensaje push indirecto, dado que no se ajusta a la filosofía del escenario que se quiere abordar. La mensajería push indirecta requiere de la integración de librerías complejas en la aplicación móvil, metodología que por experiencias previas se rechaza dada la complejidad observada en proyectos anteriores.

Para llevar a cabo el envío de un mensaje push directo a un dispositivo móvil, Redsys utiliza la funcionalidad que ofrecen los servidores de Google conocidos como GCM, de sus siglas en inglés, *Google Cloud Messaging*. En la *Figura 4.7* se puede observar el flujo que representa la comunicación definida.

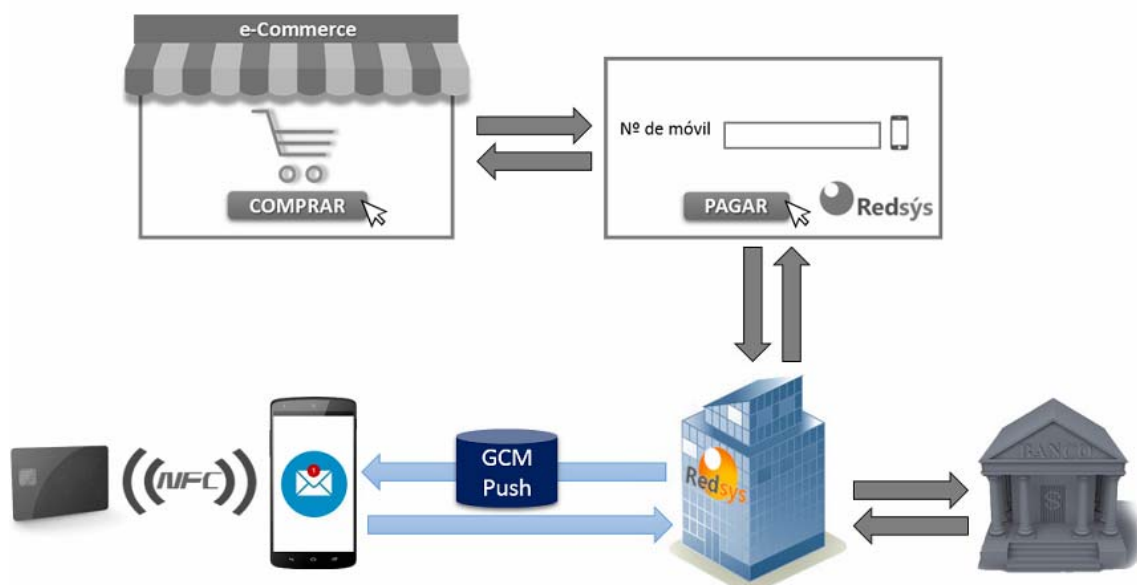


Figura 4.7: Mensajería push a través de los servidores proporcionados por Google.

Haciendo uso de los servidores de GCM, y en función de las características de la aplicación móvil que se desee ‘despertar’ mediante la mensajería push, se definen tres alternativas distintas de diseño.

C1.a - Homebanking: Elección en el dispositivo móvil

En este caso de estudio, cada entidad financiera incorpora el nuevo método de pago en su propia aplicación móvil. Este escenario resulta de interés para ciertos bancos, ya que, dentro de su propia aplicación, introducen un nuevo servicio de valor añadido a sus clientes.

Sin embargo, existe un inconveniente fundamental en la gestión del mensaje push para los dispositivos móviles que presentan más de una aplicación financiera instalada. A priori se desconoce con qué emisor de tarjeta desea el usuario efectuar el pago, de tal forma que, si es cliente de más de una entidad y tiene sus correspondientes aplicaciones móviles instaladas, el mensaje push iría dirigido a todas ellas. Se representa esta problemática en la *Figura 4.8*.

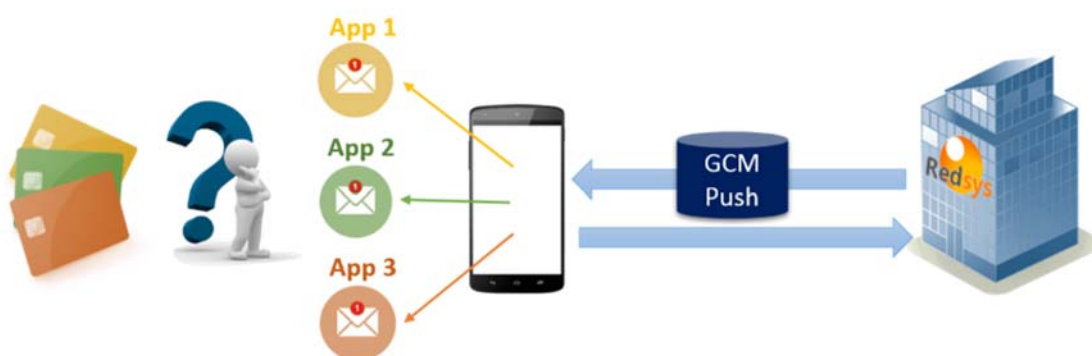


Figura 4.8: Problemática de gestión de la mensajería push para más de una aplicación móvil.

Dado este escenario, el titular de dichas tarjetas elegiría con cuál de ellas quiere llevar a cabo la compra y, por lo tanto, tendría que seleccionar manualmente con qué aplicación financiera (asociada a la tarjeta) desea desencadenar la transacción. Este sistema podría ser confuso para los clientes, disminuyendo las expectativas depositadas en una solución que garantizase una alta experiencia de usuario. Como mejora, se podría habilitar una opción para que el usuario asignase una aplicación de pago por defecto, o bien se almacenase la información relativa a la última aplicación financiera que fue utilizada para tal fin y de este modo establecerla como favorita. Sin embargo, no termina de ser una solución eficiente.

Cabe destacar otra desventaja asociada a este procedimiento, relacionada con las restricciones que establecen ciertas entidades ante la recepción de un mensaje push en sus aplicaciones móviles. Por ejemplo, BBVA no permite que su aplicación móvil propietaria ‘despierte’ ante un mensaje push, de tal forma que no podría incorporar esta solución. Dados estos inconvenientes, se rechaza esta alternativa.

C1.b - Homebanking: Elección en la página web

Se contempla la posibilidad de insertar en la página web, junto con el campo de inserción del teléfono móvil, un desplegable que contenga un listado de las entidades financieras disponibles. Este método presentaría la ventaja de conocer qué aplicación bancaria es la receptora del mensaje push antes de su envío.

Sin embargo, se descarta esta posibilidad, debido a que la enumeración de todos los bancos existentes para que el titular de la tarjeta seleccione a cuál pertenece, no resulta práctica. Se adjunta un listado de los bancos miembros del sistema ServiRed en la *Figura 4.9* para verificar la imposibilidad de abordar esta alternativa.

Este método empeoraría la experiencia de usuario, además de ser propenso a errores y estar sujeto a actualizaciones del listado frecuentes (por ejemplo, una fusión entre entidades). Una forma de representar la no viabilidad de la solución, podría ser estableciendo como ejemplo una tarjeta IBERIACARD, que puede haber sido emitida a través del banco Santander, Bankia o BBVA, sin que el titular de la misma sea consciente de este hecho en el momento de efectuar la compra mediante comercio electrónico.

NRBE	
Número de registro del Banco de España	
0019	DEUTSCHE BANK, S.A.E
0057	BANCO DEPOSITARIO BBVA, S.A.
0078	BANCA PUEYO, S.A.
0081	BANCO DE SABADELL, S.A.
0125	BANCOFAR, S.A.
0128	BANKINTER, S.A.
0130	BANCO CAIXA GERAL, S.A.
0131	NOVO BANCO, S.A, SUCURSAL EN ESPAÑA
0138	BANKOIA, S.A.
0182	BANCO BILBAO VIZCAYA ARGENTARIA, S.A.
0186	BANCO MEDIOLANUM, S.A.
0188	BANCO ALCALÁ, S.A.
0198	BANCO COOPERATIVO ESPAÑOL, S.A.
0220	BANCO FINANTIA SOFINLOC, S.A.
0227	UNOE BANK, S.A.
0229	WIZINK BANK, S.A.
0234	BANCO CAMINOS, S.A.
0240	BANCO DE CRÉDITO SOCIAL COOPERATIVO, S.A.
2038	BANKIA, S.A.
2080	ABANCA CORPORACIÓN BANCARIA, S.A.
2108	BANCO DE CAJA ESPAÑA DE INVERSIONES, SALAMANCA Y SORIA, S.A.
3001	CAJA RURAL DE ALMENDRALEJO, SOCIEDAD COOPERATIVA DE CREDITO
3005	CAJA RURAL CENTRAL, SOCIEDAD COOPERATIVA DE CREDITO
3007	CAJA RURAL DE GIJÓN, COOPERATIVA DE CRÉDITO
3008	CAJA RURAL DE NAVARRA, SOCIEDAD COOPERATIVA DE CREDITO
3009	CAJA RURAL DE EXTREMADURA, SOCIEDAD COOPERATIVA DE CREDITO
3016	CAJA RURAL DE SALAMANCA, SOCIEDAD COOPERATIVA DE CREDITO
3017	CAJA RURAL DE SORIA, SOCIEDAD COOPERATIVA DE CREDITO
3020	CAJA RURAL DE UTRERA, SOCIEDAD COOPERATIVA ANDALUZA DE CREDITO
3023	CAJA RURAL DE GRANADA, SOCIEDAD COOPERATIVA DE CREDITO
3025	CAJA DE CRÉDITO DE LOS INGENIEROS, SOCIEDAD COOPERATIVA DE CREDITO
3035	CAJA LABORAL POPULAR, SOCIEDAD COOPERATIVA DE CREDITO
3058	CAJAMAR CAJA RURAL, SOCIEDAD COOPERATIVA DE CREDITO
3059	CAJA RURAL DE ASTURIAS, SOCIEDAD COOPERATIVA DE CREDITO
3060	CAJA RURAL DE BURGOS, FUENTEPELAYO, SEGOVIA Y CASTELLDANS, SOCIEDAD COOPERATIVA DE CRÉDITO
3067	CAJA RURAL DE JAEN, BARCELONA Y MADRID, SOCIEDAD COOPERATIVA DE CREDITO
3070	CAIXA RURAL GALEGA, SOCIEDAD COOPERATIVA DE CREDITO LIMITADA GALLEGA
3076	CAJASIETE, CAJA RURAL, SOCIEDAD COOPERATIVA DE CREDITO
3080	CAJA RURAL DE TERUEL, SOCIEDAD COOPERATIVA DE CREDITO
3081	CAJA RURAL DE CASTILLA-LA MANCHA, SOCIEDAD COOPERATIVA DE CREDITO
3085	CAJA RURAL DE ZAMORA, SOCIEDAD COOPERATIVA DE CREDITO
3096	CAIXA RURAL DE L'ALCUDIA, SOCIEDAD COOPERATIVA VALENCIANA DE CREDITO
3098	CAJA RURAL NUESTRA SEÑORA DEL ROSARIO, S. COOP. ANDALUZA DE CRÉDITO
3111	CAIXA RURAL LA VALL "SAN ISIDRO", S. COOP. DE CREDITO VALENCIANA
3117	CAJA RURAL D'ALGEMESÍ, SOCIEDAD COOPERATIVA VALENCIANA DE CREDITO
3127	CAJA RURAL DE CASAS IBAÑEZ, S. COOP. DE CREDITO DE CASTILLA LA MANCHA
3130	CAJA RURAL SAN JOSE DE ALMASSORA. S. COOP. DE CRÉDITO VALENCIANA
3140	CAJA RURAL DE GUISSONA, SOCIEDAD COOPERATIVA DE CREDITO
3159	CAIXA POPULAR-CAIXA RURAL, S. COOP. DE CRÉDITO VALENCIANA
3183	CAJA DE ARQUITECTOS, SOCIEDAD COOPERATIVA DE CREDITO
3187	CAJA RURAL DEL SUR, SOCIEDAD COOPERATIVA DE CREDITO
3190	CAJA RURAL DE ALBACETE, CIUDAD REAL Y CUENCA, S. COOP. DE CRÉDITO
3191	CAJA RURAL DE ARAGÓN, SOCIEDAD COOPERATIVA DE CREDITO
8321	ENTRE2 SERVICIOS FINANCIEROS, E.F.C., S.A.
8788	CAIXABANK PAYMENTS, E.F.C. E.P., S.A.U.
8816	SOCIEDAD CONJUNTA PARA LA EMISIÓN Y GESTIÓN DE MEDIOS DE PAGO, E.F.C., S.A.
8834	EVOFINANCE, ESTABLECIMIENTO FINANCIERO DE CRÉDITO, S.A.U.
--	GLOBAL NORWALK, S.L.U.

Figura 4.9: Miembros del Sistema ServiRed.

C1.c - Aplicación móvil propietaria de Redsys

Con el fin de conseguir una solución eficiente que presente fácil interoperabilidad y globalidad, se propone el desarrollo de una aplicación propietaria de Redsys que permita obtener la lectura de los datos de cualquier tarjeta inteligente financiera, independientemente de la entidad a la que pertenezca. Ver *Figura 4.10*.



Figura 4.10: Activación de una aplicación móvil propietaria a partir de mensajería push.

Este escenario presenta una fácil integración con la mensajería push, ya que únicamente existiría una aplicación financiera como receptora de dicho mensaje, favoreciendo significativamente la experiencia de usuario. Esta opción destaca tecnológicamente respecto del resto de alternativas, aunque presenta el inconveniente de que el usuario debe descargarse una nueva aplicación, hasta el momento desconocida, si desea utilizar el nuevo método de pago planteado. Se asume esta circunstancia, seleccionado esta opción para la propuesta del nuevo método de pago y la implementación del demostrador.

C2 - Servicio Móvil Multipago (SMM)

El Servicio Móvil Mutipago (SMM) utiliza un canal push específico asociado, pero con ciertas particularidades que se mencionan a continuación. La ventaja fundamental que presenta el SMM es que el usuario únicamente tiene que descargarse una aplicación (que actualmente ya está disponible) en el dispositivo móvil, que permite además la convivencia con múltiples servicios que proporciona Redsys (ver *Figura 4.11*). De esta forma, la solución garantiza una alta aceptación por parte de los titulares de las tarjetas financieras que actualmente ya son usuarios del SMM, pudiéndoles ofertar a partir de una actualización, otro servicio de valor añadido, como es el nuevo método de pago propuesto.



Figura 4.11: Descripción de los servicios integrados en el SMM.

El principal inconveniente es que en la aplicación del SMM incluye de forma conjunta todas las aplicaciones de aquellas entidades que desee configurar el cliente, pudiendo coexistir más de una. De esta forma, se enviaría un tipo de mensaje push a la librería común de Redsys en el SMM, pero no se podría distinguir cual es la aplicación bancaria que se desea ‘despertar’. Se podría plantear como plan de contingencia que el usuario realizase una elección previa de la aplicación financiera que quisiera utilizar por defecto, o bien activar todas ellas y establecer una selección manual en el momento del pago (pudiendo almacenar la información de la aplicación financiera seleccionada, como la favorita para la venta siguiente). En definitiva, esta opción presenta ciertas desventajas del planteamiento definido como ‘homebanking’, por lo que se descarta esta alternativa.

4.2.4 ETAPA D: Autenticación del cliente en el dispositivo móvil

La propuesta de solución que se presenta, tiene como fundamento una robusta autenticación del cliente, con el fin de satisfacer los objetivos planteados. Para que el proceso de autenticación se considere robusto, debe incluir al menos dos de los tres factores de autenticación existentes (ver *Figura 4.12*)

- “YO SÉ”: Sería la necesidad de conocer una contraseña para la utilización de la aplicación del móvil.
- “YO SOY”: Otra alternativa es poder desbloquear la aplicación móvil financiera a partir del reconocimiento de la huella dactilar.
- “YO TENGO”: En este escenario sería la presencia física de la tarjeta inteligente en el esquema de pago. También se depende del dispositivo móvil, porque lo que es una solución con doble “YO TENGO”.

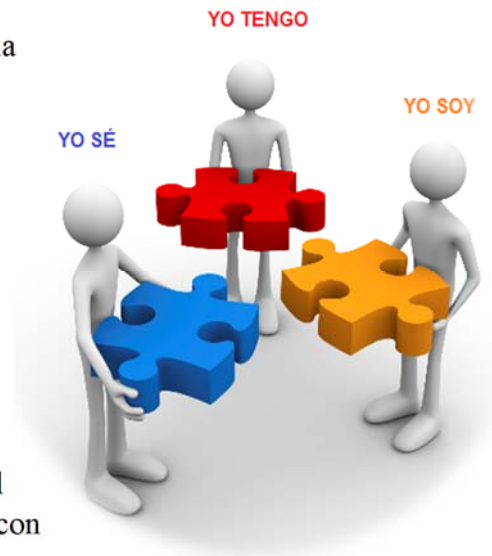


Figura 4.12: Factores de la autenticación.

Por lo tanto, el sistema planteado se podría definir con la fórmula “YO SÉ” + “YO TENGO” + “YO TENGO” o bien, “YO SOY” + “YO TENGO” + “YO TENGO”, siendo la presencia de la tarjeta inteligente y el dispositivo móvil (elementos familiares para todos los usuarios), muy relevantes en el nuevo método de pago de comercio electrónico.

D1 - Implementación de la autenticación del titular de la tarjeta

Una vez que el titular de la tarjeta ha insertado su número de teléfono móvil en la página web, recibe una notificación push a la aplicación propietaria instalada en su dispositivo móvil. El usuario deberá desbloquear el teléfono móvil si así lo tiene predefinido y proceder a la autenticación en la aplicación financiera a través de la huella dactilar o una contraseña.

Si la contraseña es correcta, el teléfono móvil solicitará al usuario que aproxime su tarjeta inteligente al móvil para realizar la lectura de los datos, procediéndose de esta forma la segunda autenticación. Si, por el contrario, la contraseña es incorrecta, se notificará al usuario de este hecho para que nuevamente lo intente. Esta alternativa ha sido seleccionada para la propuesta *CSPay* y por lo tanto, se implementa en el demostrador.

D2 - Doble factor de autenticación: Normativa PSD2

En el año 2007 tuvo origen la normativa PSD (por sus siglas en inglés, Payment Services Providers, que corresponde a la Directiva de Servicios de Pago), con el objetivo de crear un mercado único de pagos en la Unión Europea que fomentase la innovación, competencia y eficiencia en el sector. En el año 2013, la Comisión Europea propuso una revisión (PSD2) con la pretensión de determinar cómo conseguir dichos objetivos, destacando entre otros hitos, el doble factor de autenticación [43].

Hasta finales del año 2018 no entrarán en vigor la obligación de cumplimiento de la nueva normativa, pero se contempla la posibilidad de que este reglamento presente impacto en la definición del doble factor de autenticación. El nuevo concepto podría determinar que para considerarse robusta una autenticación de doble factor, las dos vías de autenticación (en el esquema que aplica, la inserción de la contraseña en la aplicación móvil y la lectura de la tarjeta inteligente) se tendrían que realizar de forma concatenada sin que el usuario recibiese información del resultado parcial de cada una de ellas.

Es decir, según el escenario planteado, ante la inserción incorrecta de la contraseña en la aplicación móvil, se solicitaría de igual forma al usuario que aproximase la tarjeta inteligente al dispositivo móvil para proceder a la lectura de los datos, aunque la transacción ya esté destinada a denegarse.

Este cambio no presenta alto impacto en el desarrollo de la aplicación móvil, pero sí preocupa la experiencia de usuario, ya que, ante un error en la inserción de la contraseña, el titular de la tarjeta tendría que finalizar el procedimiento completo para finalmente descubrir que la autenticación no se ha llevado a cabo de forma correcta, siendo desconocedor de dónde se ha producido el problema (en la inserción de la contraseña o con la tarjeta con la que se ha intentado operar). Por el momento, se deja esta opción como consideración de estudio a futuro si las normativas lo consideran necesario.

4.2.5 ETAPA E: Protocolo de comunicación entre el móvil y la tarjeta

El fundamento de la nueva propuesta se basa en la incorporación de la tarjeta inteligente (Card Present) en un esquema de pago donde las transacciones financieras se realizaban sin la presencia de la misma (CNP) hasta la fecha actual. De forma general, la inclusión de dicho elemento mejora la experiencia de usuario y proporciona mayor seguridad, aunque en función del grado de interacción de la tarjeta se podrán establecer dos vías de desarrollo (lectura de tarjeta o transacción completa EMV Contactless) con diferentes ventajas asociadas. La tecnología que se utiliza para establecer la comunicación entre el dispositivo móvil y la tarjeta, es NFC. El pago se realiza al aproximar la tarjeta contactless al dispositivo móvil, como si el cliente estuviera efectuando un pago presencial en un TPV de un comercio físico. Ver *Figura 4.13*.

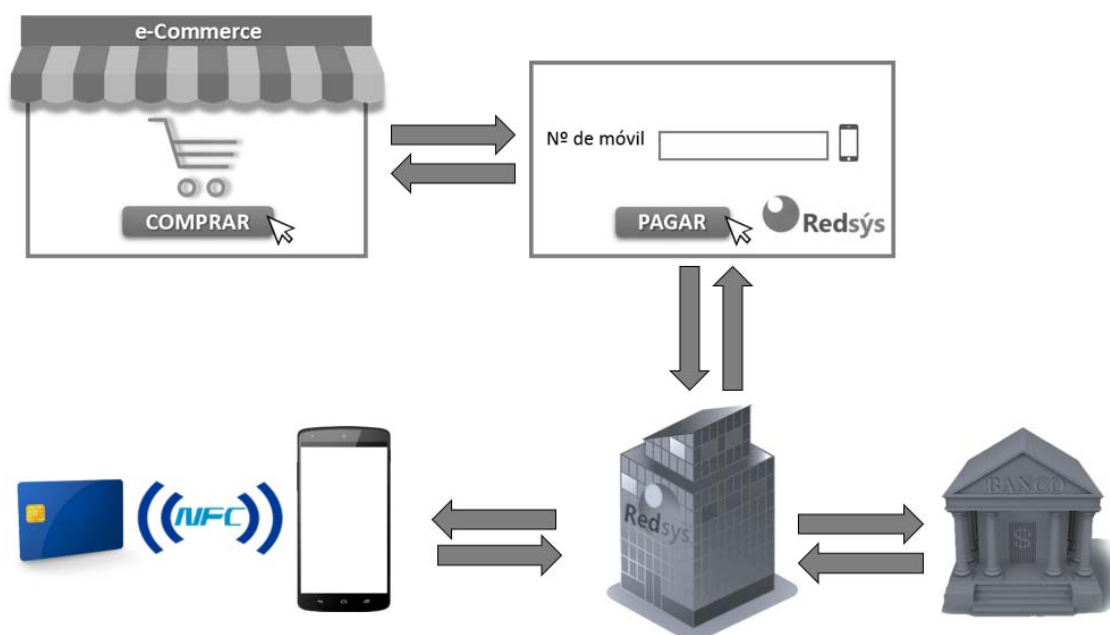


Figura 4. 13: Protocolo de comunicación entre el móvil y la tarjeta inteligente mediante NFC.

NFC es el acrónimo de *Near Field Communication* y está basado en la técnica de RFID (*Radio Frequency Identification*), con ISO 14443 [44]. Esta tecnología inalámbrica de corto alcance y alta frecuencia (13,56 MHz, banda en la que no es necesario disponer de licencia), presenta ventajas en cuanto a la velocidad de comunicación, el coste, la robustez, la provisión de servicios y la convergencia de su uso, en comparación con el resto de conexiones existentes disponibles en un teléfono móvil. Por este motivo, cada vez son más los dispositivos que integran esta funcionalidad sin limitar su uso, permitiendo explorar a los desarrolladores el potencial que ofrece esta plataforma abierta para la creación de nuevas aplicaciones.

Es importante mencionar los modelos de funcionamiento que presenta NFC, ya que existen dos técnicas de operatividad, que se rigen en función de la fuente que suministra la energía para el intercambio de información entre dos dispositivos.

- **Pasivo:** En este modo de funcionamiento, uno de los dispositivos no utiliza suministro interno de energía, sino que, cuando se aproxima lo suficiente al otro elemento (activo), se aprovecha de su campo electromagnético gracias al acoplamiento inducido (ver *Figura 4.14*). De esta forma, el elemento pasivo puede obtener la energía de la modulación de la carga y transferir su respuesta. Este es el modo de funcionamiento por excelencia que utilizan las tarjetas inteligentes. Cabe destacar que los dispositivos móviles cuando emulan el comportamiento de una tarjeta (HCE) para llevar a cabo un pago móvil en un TPV, también utilizan este método.

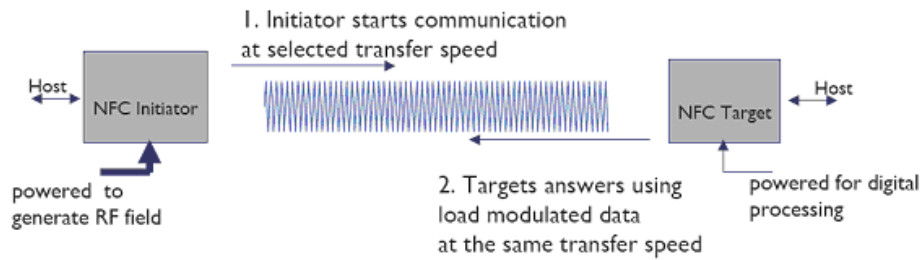


Figura 4.14: Esquema NFC pasivo [44].

- **Activo:** En este caso, ambos dispositivos obtienen la energía de forma interna, generando cada uno de ellos su propio cambio electromagnético para la transmisión de los datos (ver *Figura 4.15*). Este modo de funcionamiento queda fuera del ámbito de estudio del proyecto.

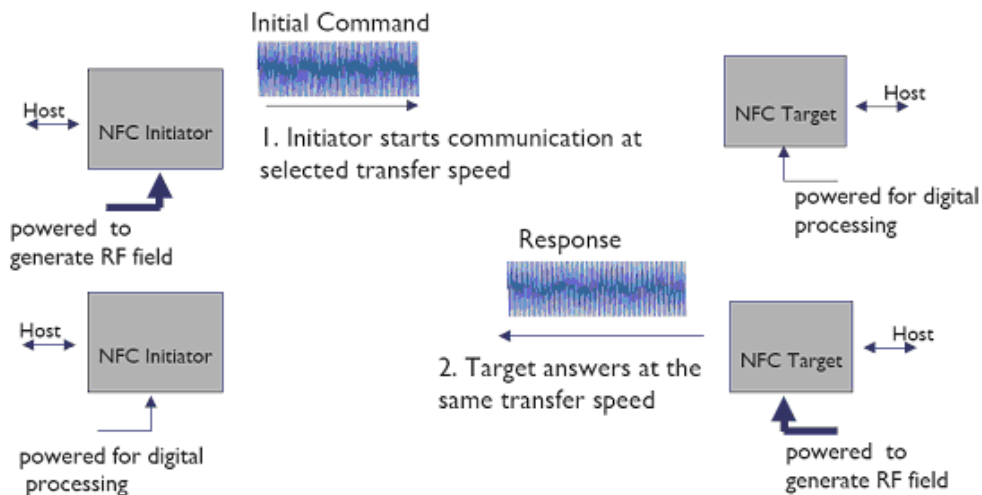


Figura 4.15: Esquema dispositivo NFC Activo [44].

El comportamiento operativo de los dispositivos NFC, viene determinado por el modelo de funcionamiento descrito. La tecnología NFC destaca por ser flexible y eficiente, presentando hasta tres configuraciones distintas de trabajo, según el rol que desempeñan los dos actores partícipes en la comunicación. A continuación, se detallan las tres vertientes existentes (ver *Figura 4.16*), definidas y particularizadas desde la perspectiva de un dispositivo móvil que incorpora la funcionalidad NFC.

- **Emulación de la tarjeta inteligente:** En este modo de funcionamiento, el dispositivo NFC se comporta y actúa como si se tratase de una tarjeta inteligente sin contactos, siendo de cara a un lector o a un TPV, como un elemento pasivo del que se puede extraer la información de interés mediante comandos de lectura. Esta configuración es compatible con características de seguridad avanzadas, y por lo tanto es utilizado para transacciones financieras, control de acceso y gestión de entradas. El ejemplo por excelencia de la empleabilidad de este comportamiento, es el pago móvil en un TPV en soluciones de comercio presencial (escenario estudiado en el *Capítulo 1*).
- **Peer-to-Peer:** Esta arquitectura posibilita la sincronización instantánea y el intercambio de información entre dos dispositivos activos que utilicen NFC. Por ejemplo, dos teléfonos móviles podrían establecer este tipo de comunicación con el fin de intercambiar archivos, contenido digital o configurar el enlace para otra tecnología inalámbrica. La tecnología NFC no tiene como fin la transferencia masiva de datos, pero sí que presenta alta velocidad para la gestión del enlace (o emparejamiento) entre dos dispositivos que se deseen conectar a través de redes inalámbricas de mayor ancho de banda, como Bluetooth o WiFi.
- **Modo Lectura/Escritura:** Esta configuración permite que el dispositivo NFC activo sea capaz de transmitir información y leer el contenido de las tarjetas sin contacto y de las etiquetas NFC. El conjunto de las tarjetas que muestran interoperabilidad con los dispositivos NFC, se definen en las especificaciones publicadas por NFC Forum. Este organismo se encarga de emitir especificaciones para asegurar la estandarización entre dispositivos y servicios, formando al mercado (fabricantes, desarrolladores de aplicaciones, instituciones financieras, consorcios de transporte, etc.) sobre la tecnología NFC. En relación a las tarjetas compatibles, se definen, entre otros formatos, las especificaciones basadas en ISO 14443 Tipo A y B (correspondientes a los estándares internacionales de tarjetas inteligentes sin contacto) que resulta de interés en el presente TFM. El ejemplo del uso de este modo de funcionamiento es la utilización del protocolo EMV Contactless para emprender la comunicación entre el dispositivo móvil y la tarjeta inteligente sin contactos.



Figura 4.16: Tipos de funcionamiento del dispositivo NFC.

Cabe destacar, que existen cinco etapas presentes en toda comunicación NFC, independientemente del modo de comportamiento establecido.

- **Descubrimiento:** En esta fase los dispositivos implicados inician la fase de rastreo, con su posterior reconocimiento.

- **Autenticación:** Los dispositivos se verifican entre ellos, para comprobar si están autorizados o si deben establecer algún tipo de cifrado adicional en la comunicación.
- **Negociación:** En esta etapa se definen parámetros comunes para entablar la comunicación, como la velocidad de transmisión, la identificación del dispositivo, el tipo de aplicación, el tamaño de los datos, y si procede, también definen la acción a desencadenar.
- **Transferencia:** Una vez negociados y adaptados los parámetros para la comunicación, se procede a realizar el intercambio o la lectura de los datos.
- **Confirmación:** El dispositivo receptor confirma el estado de la comunicación y de la transferencia de la información.

E1 - Autenticación del titular mediante la lectura de la tarjeta

Una vez que el usuario aproxima la tarjeta inteligente contactless al dispositivo móvil, se puede obtener el número de tarjeta (PAN) y la fecha de caducidad sin que exista la necesidad de teclear dicha información. La lectura de los datos se puede llevar a cabo mediante tecnología NFC o escaneo de los mismos mediante la cámara del dispositivo móvil.

Sin embargo, el CVV2, dato necesario para efectuar la transacción financiera, no se puede recuperar mediante la lectura de la tarjeta, y es necesario que el titular de la misma inserte manualmente los tres dígitos que lo componen. Este procedimiento mejora la experiencia de usuario y elimina la aplicabilidad de las técnicas de *phishing* para la captura de datos sensibles y posterior fraude.

Se dice que mediante este proceso se “autentica” al titular de la tarjeta inteligente, ya que, para llevar a cabo la transacción financiera completa, se necesita que el usuario haya desbloqueado previamente la aplicación bancaria de su móvil (“yo sé”) y disponga de la tarjeta física (“yo tengo”).

Ante el robo o extravío, copia o clonación de una tarjeta, el estafador no estaría en condiciones de poder efectuar un pago mediante comercio electrónico utilizando este método al no disponer de la aplicación financiera y del móvil dado de alta. Si además, el estafador también tiene en su poder el dispositivo móvil, debería conocer la contraseña de la aplicación para poder realizar el fraude. Por otro lado, se establece en la toma de requisitos que, tras la instalación y registro de la aplicación financiera en un nuevo dispositivo móvil, se desactive del anterior, de tal forma que quedaría inhabilitada la funcionalidad del terminal móvil sustraído.

E2 - Autenticación y autorización mediante una transacción EMV Contactless

Se propone efectuar una transacción completa EMV Contactless para dotar al sistema de pago de la seguridad que ofrecen los procesos criptográficos que realizan las tarjetas inteligentes en el transcurso de una operación financiera.

Para el desarrollo de esta alternativa, se debe enviar desde el centro procesador de Redsys un número aleatorio (“desafío”) que el teléfono móvil enviará a la tarjeta para obtener la respuesta de la misma. A continuación, el dispositivo móvil enviará a Redsys la información proporcionada por la tarjeta para que ésta intervenga en el proceso de autorización. De esta manera, se conoce a este método como “autenticación y autorización”, siendo un escenario más robusto y seguro. Se selecciona esta opción para la definición de la solución de pago CSPay.

4.2.6 ETAPA F: Operativa transaccional entre Redsys y la entidad financiera

La implantación del número método de pago presenta impacto en el protocolo de comunicación entre el centro procesador y las entidades financieras, conocido como PRICE (Protocolo Integrado de Conexión de Establecimientos). Ver *Figura 4.17*. Se deben establecer nuevas definiciones para los campos existentes de este protocolo, ya que existen mensajes dónde se requiere proporcionar información sobre el escenario de cómo se ha llevado a cabo la transacción. En este caso, se deberá comunicar a la entidad de que la operación se ha realizado mediante comercio electrónico y con la tarjeta física del titular presente, siendo una casuística desconocida hasta la fecha actual.

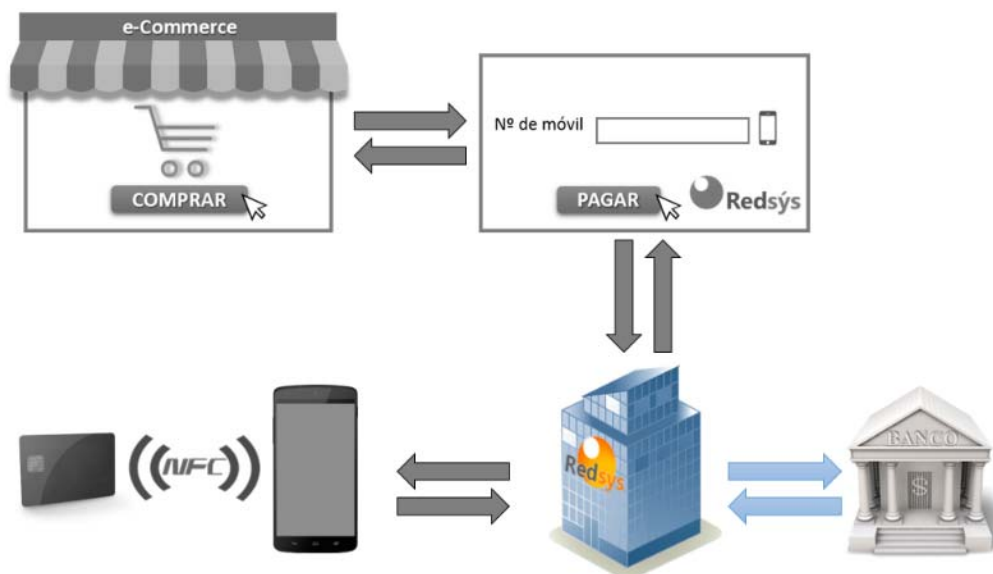


Figura 4.17: Comunicación desde el centro procesador de Redsys a la entidad financiera.

4.4 DEFINICIÓN FINAL DE LA PROPUESTA CSPAY

Tras el estudio de viabilidad técnica realizado, se propone el desarrollo del método de pago *CSPay*. Se resumen las opciones que se ha decidido implementar en función de las diversas alternativas propuestas para cada una de las etapas (ver *Figura 4.18*).

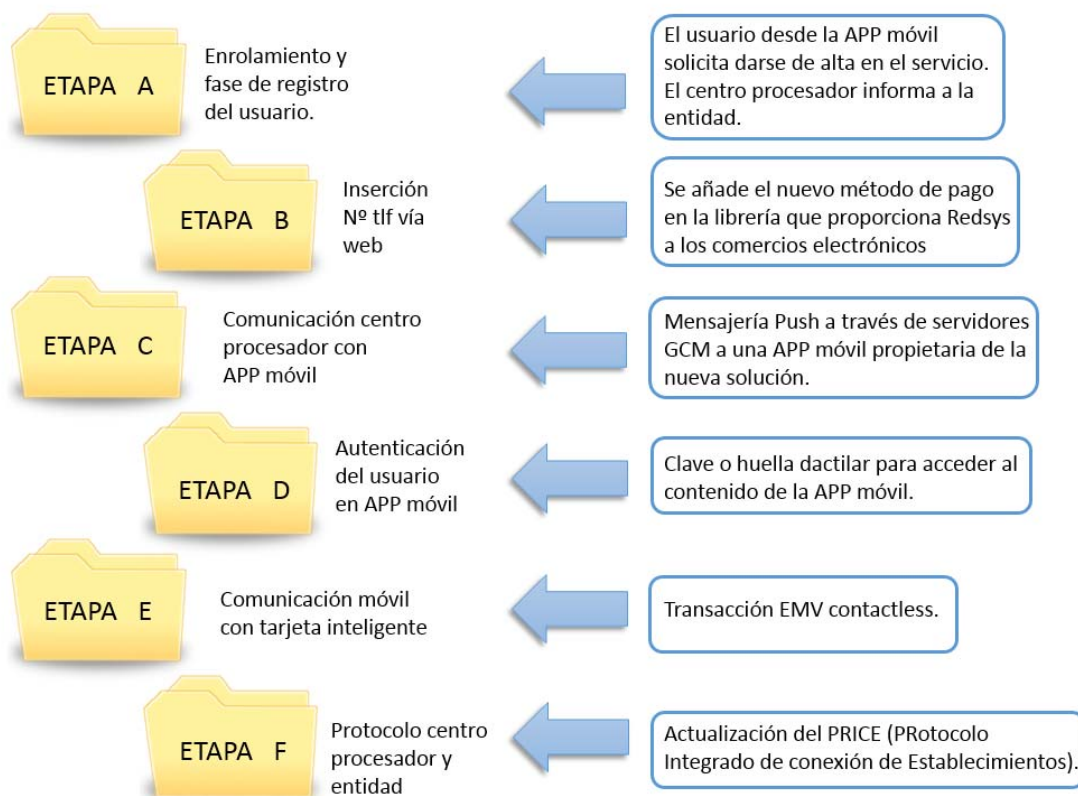


Figura 4.18. Esquema final de la solución propuesta.

- **Etapa A:** El enrolamiento se llevará a cabo de forma combinada, teniendo el usuario la opción de darse de alta en el servicio *CSPay* a través de la entidad financiera que desee promocionar este servicio o directamente desde la aplicación móvil. El estudio se centra en habilitar esta opción desde la propia aplicación móvil, ya que es Redsys el responsable de este cometido.
- **Etapa B:** En el momento de efectuar el pago, el comercio electrónico redirecciona el sitio web a la librería de Redsys, que posibilita la inserción del número de teléfono móvil en el formulario de pago para completar la transacción mediante la solución *CSPay*.
- **Etapa C:** La transmisión de la información entre el centro procesador y la aplicación móvil del cliente se llevará a cabo mediante mensajería de push directo, a través de los servidores de Google. La aplicación móvil receptora de dicho mensaje, será propietaria de Redsys.
- **Etapa D:** El cliente se autentica en el dispositivo móvil (mediante clave de acceso o huella dactilar) y se valida la contraseña de la aplicación financiera antes de proceder a la lectura de la tarjeta inteligente.

- **Etapa E:** El usuario aproxima su tarjeta al dispositivo móvil y se realiza una transacción EMV Contactless mediante tecnología NFC.
- **Etapa F:** Se incorpora una nueva definición en el protocolo de comunicación PRICE entre el centro procesador de Redsys y la entidad financiera con el fin de que se pueda notificar que la transacción se ha llevado a cabo en comercio electrónico y con la presencia física de tarjeta.

El diagrama de flujo de la propuesta final se representa en la *Figura 4.19*. La numeración de las flechas secuencia las comunicaciones que tienen lugar en el transcurso de una transacción financiera e-commerce utilizando el método de pago *CSPay*.

1: La página web del comercio electrónico integrará la librería proporcionada por Redsys. En el momento en el que el cliente desee abonar el pago se producirá la redirección de la página del comercio al sitio web de selección de pago de Redsys.

2: El cliente teclea su número de teléfono móvil en la página web, y esta información viaja al procesador de transacciones financieras de Redsys.

3: El procesador transaccional realiza una primera comprobación, verificando que el número de teléfono introducido corresponde a un cliente dado de alta en el servicio. A continuación, despierta la aplicación del móvil mediante mensajería push (se utilizan los servidores de Google Cloud Messaging).

4: El usuario introduce su contraseña en la aplicación y sigue las indicaciones que aparecen en la pantalla del dispositivo móvil, dónde se solicita que aproxime la tarjeta (que es leída mediante tecnología NFC).

5: La aplicación del móvil transmite los datos recuperados de la tarjeta y la información de la operación cifrada al centro procesador de transacciones.

6: El centro procesador analiza el PAN recibido y envía la operación a la entidad emisora correspondiente.

7: La entidad financiera verifica los datos de la transacción y aplica la lógica de negocio pertinente (comprobando la disponibilidad de fondos disponibles en la cuenta del titular de la tarjeta, que no aparezca el número de tarjeta en la lista negra, etc.) A continuación, proporciona una respuesta a Redsys con la resolución de la operación.

8: Redsys registra la operación para el posterior cierre de sesión con los adquirentes y notifica la resolución al cliente.

9: Una vez que se informa al cliente de la respuesta a la operación llevada a cabo, se devuelve el control a la página web del comercio, por si el cliente deseara continuar navegando por la misma.

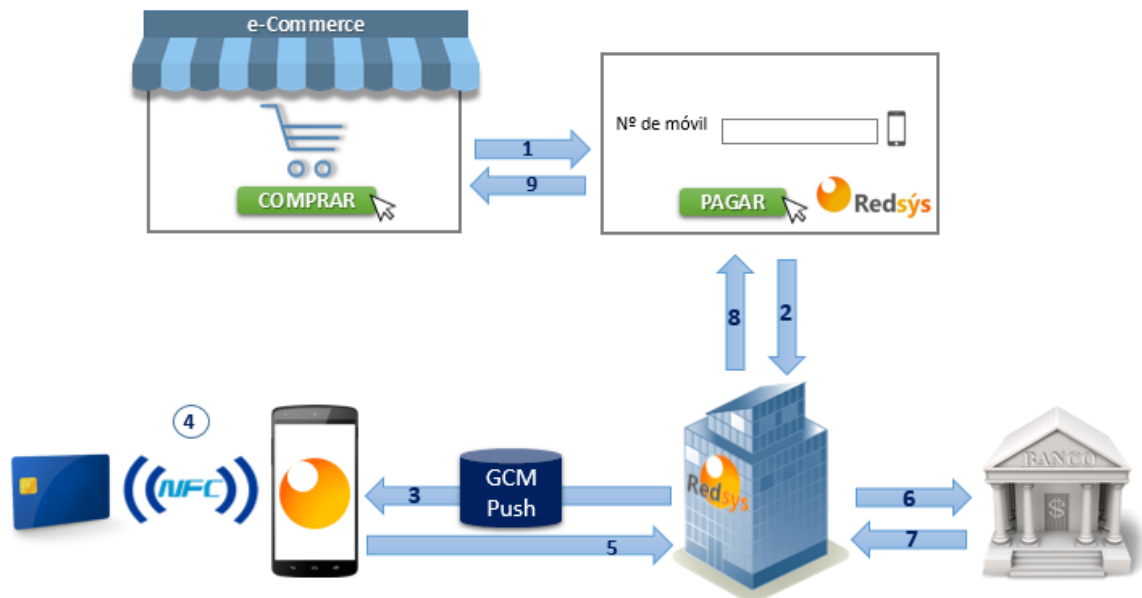


Figura 4.19: Propuesta final de la nueva solución de pago para comercio electrónico.

Capítulo 5

Solución tecnológica para el demostrador CSPay

5.1 VISIÓN GENERAL DEL DEMOSTRADOR.

El principal objetivo del proyecto es presentar un nuevo método de pago para comercio electrónico y, por lo tanto, se requiere implementar un demostrador que permita analizar la viabilidad de la solución técnica de la propuesta. La implementación funcional como prueba de concepto, surge para cubrir la necesidad de orientar un proyecto de gran envergadura de manera simplificada, de tal forma que sirva de base sólida para el enfoque de la solución real. El demostrador permite emular el modo de funcionamiento y secuencialización del sistema final, permitiendo a los usuarios experimentar la sensación de ser clientes de este servicio.

En este capítulo se aborda la solución técnica del demostrador, con la finalidad de escenificar conceptual y funcionalmente cada una de las cuatro secciones tecnológicas que constituyen la nueva propuesta de pago para un escenario de comercio electrónico (ver *Figura 5.1*). De esta forma, resulta más sencillo entender y analizar el comportamiento que adopta cada una de estas áreas diferenciadas que se exponen a continuación, necesarias para el correcto funcionamiento del sistema conjunto. Desde el punto de vista de la transacción online hay que emular el entorno de la misma, lo que implica un comercio electrónico y un centro procesador y de resolución del pago. Por otro lado, la solución propuesta requiere del uso del teléfono móvil, lo que implica desarrollar la aplicación correspondiente para formalizar el pago. Por último, será necesario disponer de diferentes tarjetas para poder validar el sistema.



Figura 5.1. Secciones tecnológicas independientes para el desarrollo del sistema CSPay.

Cabe destacar que la implementación del demostrador ha sido integral, habiendo desarrollado dentro del presente proyecto cada uno de los módulos implicados en el proceso y, por lo tanto, no se ha utilizado código privado sujeto a restricciones de confidencialidad. En los apartados subsiguientes se muestran los requerimientos y el proceso detallado de cómo se ha implementado cada uno de los bloques de forma independiente. En el *Capítulo 6*, se lleva a cabo la definición de la integración total del sistema y se muestra el funcionamiento completo de la solución CSPay propuesta.

5.2 APLICACIÓN PARA EL DISPOSITIVO MÓVIL

Para el desarrollo de la aplicación móvil ha sido necesario evaluar, en primera instancia, las necesidades teóricas que presenta la definición de la solución. En el *Capítulo 4*, se indica que la aplicación móvil presenta dos cometidos diferenciados:

- **Fase de enrolamiento:** El usuario desde su dispositivo móvil tiene la oportunidad de registrarse (realizar un alta nueva) en el sistema, así como de vincular o desvincular las tarjetas con las que desee pagar mediante comercio electrónico.
- **Medio de pago:** El móvil recibe un mensaje push que activa la aplicación, solicitando al usuario que, tras la autenticación, aproxime la tarjeta inteligente al dispositivo móvil.

Los objetivos funcionales clave para satisfacer los requisitos globales previamente establecidos, son los dos siguientes:

- Tecnología **NFC** para la lectura de la tarjeta inteligente con el fin de recuperar los datos almacenados en el chip (ya sea en la fase de vinculación/desvinculación de una tarjeta nueva, así como en el propio pago). Esta funcionalidad determina el sistema operativo y la versión de los dispositivos móviles que pueden ser compatibles con la solución y, por lo tanto, condiciona el enfoque del desarrollo de la aplicación (programación para Android, iOS, Blackberry o Windows).
- Comunicación bidireccional con el servidor, dónde los envíos desde el dispositivo móvil se lleven a cabo a través de un POST al servidor, y la recepción se realice a través de una notificación **push** que provoque que “se despierte” la aplicación móvil. Es importante que el sistema operativo y la herramienta de desarrollo sean compatibles con esta funcionalidad.

En los apartados subsiguientes se procede a estudiar detalladamente el modo de implementación.

5.2.1 Determinación del sistema operativo: Android vs iOS.

Se lleva a cabo una investigación del panorama actual de los diferentes sistemas operativos que albergan en los dispositivos móviles de los usuarios, con el propósito de precisar la plataforma de la aplicación. En España, por excelencia, predomina Android (plataforma de Google), siendo el rey de los sistemas operativos para los smartphones. Se adjunta, en la *Figura 5.1*, una recopilación de los datos de interés en relación a la cuota de mercado nacional.

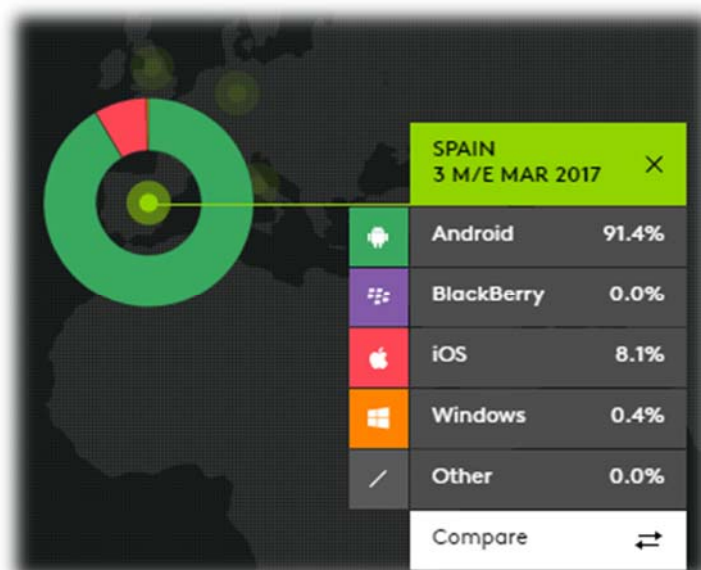


Figura 5.2: Estudio de los sistemas operativos del mercado móvil en España [45]

Android simboliza más del 90% de la contribución de dispositivos móviles en circulación en España, y junto con iOS (perteneciente a Apple) forman un tándem que cubre prácticamente la totalidad del mercado móvil nacional. Esta coyuntura es fundamental, ya que la creación de una aplicación móvil implica la elección de la(s) plataforma(s) de desarrollo, implicando coste y tiempo asociado la programación para cada uno de los diferentes entornos. La adaptación por parte de los usuarios de una nueva solución tecnológica únicamente puede ser analizada mediante estadísticas y sondeos, pero se parte de la premisa de que el público objetivo al que va dirigida son aquellos usuarios que disponen de las condiciones de partida necesarias. Por este motivo, la elección del sistema operativo decreta el alcance del proyecto, limitando el número máximo de usuarios que tendrán la oportunidad de disfrutar las prestaciones que se ofertan.

A nivel mundial, la distribución adquiere un baremo equiparable, siendo la cuota de Android preeminente en el sector de los sistemas operativos para móviles. Diferentes empresas de consultoría e investigación de las tecnologías de información determinaron, en el censo del año 2016, que Android engloba el 87,5% del total, seguido de iOS con el 12,1%. Este binomio de sistemas operativos alcanza la solemne cifra de 99,6% [46].

Una vez contextualizado el marco comercial, se requiere revisar si las alternativas estudiadas posibilitan el cumplimiento de la demanda técnica. El requerimiento crítico y restringente es que el dispositivo móvil soporte la activación del NFC. En relación a esta consideración, el equipo de Android es rotundo, si el modelo del móvil tiene integrado este módulo, el usuario es libre de utilizar esta funcionalidad y, por lo tanto, el desarrollador puede explorar nuevos fines asociados a esta tecnología. En el caso de iOS el escenario es muy diferente, ya que los productos de Apple tienden a ser partidarios de la utilización exclusiva de sus soluciones propietarias, impidiendo la inconclusión a terceros. La ejemplificación de este concepto viene dada por la integración del chip NFC en el iPhone 6, pero limitada única y exclusivamente al funcionamiento de Apple Pay, prohibiendo el acceso a cualquier otra aplicación que desee hacer uso de esta tecnología. Contra todo pronóstico, Apple ha reconsiderado esta tesitura, entreabriendo al nuevo modelo *iOS 11* al estándar NFC [47]. Las nuevas funcionalidades a soportar, se ciñen en la lectura de etiquetas y tarjetas contactless (no presenta el abanico de posibilidades de Android, aunque para el presente objeto de estudio es suficiente).

Dado que Android es firmemente predominante y no impone restricciones en la utilización de todos los módulos integrados, se selecciona este sistema operativo para llevar a cabo la demo del proyecto *CSPay*. Si la aceptación de la nueva solución es positiva y aumenta la demanda de iOS posibilitando el uso de NFC, no se descarta migrar la aplicación a esta otra plataforma.

5.2.2 Decisión del entorno de desarrollo.

La utilización del entorno de desarrollo integrado (IDE) adecuado es una de las elecciones más importantes a la hora de implementar una aplicación para Android. Esto puede repercutir en la calidad del producto, y en la facilidad y versatilidad a la hora de desarrollarlo. A continuación, se describen las herramientas más populares en el mundo del desarrollo de aplicaciones Android [48].

- Eclipse

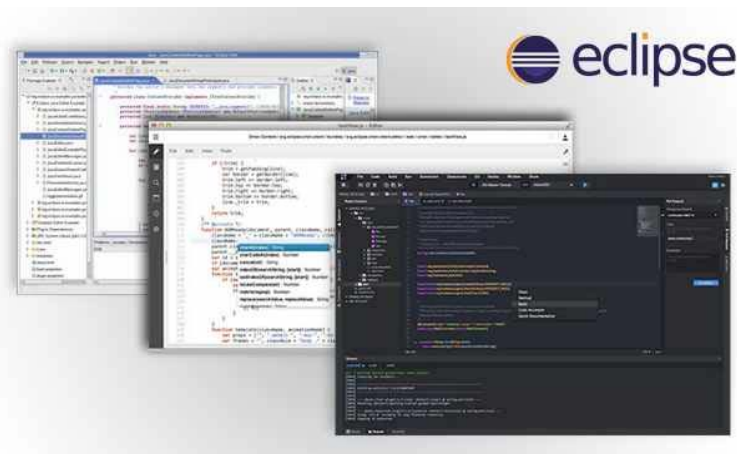


Figura 5.3: IDE Eclipse.

Hasta hace poco era el entorno por excelencia para el desarrollo de aplicaciones Android. Desde que apareció este sistema operativo, era el entorno de desarrollo integrado (IDE) oficial de Google para crear aplicaciones. Este hecho cambió con la aparición de la primera versión oficial de Android Studio en Diciembre de 2014, tal y como se explica en el apartado correspondiente.

Es una herramienta creada por IBM, pero actualmente es de código libre y es desarrollada por la *Fundación Eclipse*. En cuanto a la configuración y al flujo de trabajo, el hecho de que Eclipse se utilice para desarrollar en otras plataformas e idiomas, hace que la experiencia de usuario sea más complicada y que surjan incompatibilidades.

- Xamarin



Figura 5.4: IDE Xamarin.

Se trata de una herramienta gratuita creada por Microsoft, y que viene incluida en el famoso Visual Studio. La principal ventaja es que es un sistema multiplataforma, es decir, se parte del mismo código para obtener una aplicación funcional tanto en IOS como en Windows pone. El lenguaje de programación es C#, por lo que es útil si no se quiere utilizar Java, pero a la vez se aleja del sistema Android.

Una característica interesante y única es que se dispone de pruebas automatizadas a través de dispositivos reales conectados a la nube, aunque para este proyecto concreto carece de interés.

- AIDE



Figura 5.5: IDE AIDE.

AIDE, o Android IDE, se diferencia del resto de entornos en que es posible desarrollar las aplicaciones desde el propio dispositivo móvil. No es un IDE pensado para realizar grandes proyectos, por lo que carece de funcionalidades avanzadas, además de las limitaciones que ofrece el programar en pantallas pequeñas.

Por otra parte, su funcionamiento es bastante similar al de Android Studio y Eclipse, por lo que es una buena opción para aprender las nociones básicas sobre el desarrollo de aplicaciones móviles de forma cómoda, ya que se puede probar en cualquier lugar.

- **Python**



Figura 5.6: IDE Python.

Se trata de un lenguaje de programación muy utilizado para desarrollar todo tipo de proyectos. En cuanto a las aplicaciones, hay varias opciones, como PyMob o la librería pgs4a (Pygame Subset for Android). Es un lenguaje fácil y accesible por lo que puede ser útil para aplicaciones sencillas, pero para proyectos complejos para aplicaciones móviles, pierde muchas funcionalidades con respecto a Android Studio. Hay que considerar que el objetivo es un prototipo de la solución propuesta y, por lo tanto, es una aplicación sencilla, lo que no justifica utilizar entornos más complejos o potentes. En el apartado 5.4.1 se justifica la utilización de este lenguaje para la programación del servidor.

- **Unity**

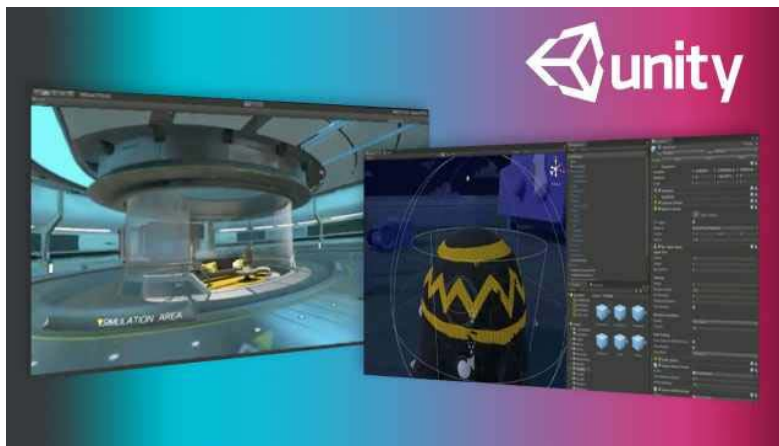


Figura 5.9: IDE Unity.

Este entorno está especializado en el desarrollo de los juegos. Es tanto un motor como un entorno de desarrollo que permite realizar juegos multiplataforma de todo tipo. Sus posibilidades son muy diversas, ya que permite crear desde aplicaciones muy simples hasta proyectos con física realista y gráficos 3D.

Adicionalmente, se puede añadir código en C# o Java, por lo que las opciones son casi ilimitadas. Unity se ha convertido en uno de los referentes en cuanto a desarrollo de juegos

móviles, ya que evita la necesidad de crear un motor desde cero, lo que ahorra mucho tiempo y esfuerzo.

En cuanto al desarrollo de aplicaciones que no sean juegos, es bastante complejo, por lo que no es una opción viable para el presente proyecto.

- Android Studio



Figura 5.8: IDE Android Studio.

Desde la aparición de este IDE en Diciembre de 2014, es el entorno de programación oficial de Google para el desarrollo de las aplicaciones Android.

Una de sus principales ventajas con respecto es que se ha creado exclusivamente para programar en Android, por lo que es más intuitivo y fácil de usar que el resto de entornos comentados anteriormente. Además la compatibilidad es total con un rendimiento óptimo. De esta forma se consigue que la compilación sea más rápida que en Eclipse, que era el anterior IDE de referencia para Android.

En líneas generales, todas las acciones se realizan de forma mejorada con respecto al resto de entornos: Mejor interfaz, los emuladores consumen pocos recursos, sencillez para crear diversas versiones de una misma aplicación, mejores plantillas para empezar los proyectos, exportación de archivos .apk de forma sencilla, facilidad de trabajo en equipo por la favorable distribución de código, entre otras.

Estas prestaciones se consiguen, en gran parte, gracias al compilador que utiliza Android Studio, llamado *Gradle*. Es un plugin (lo que facilita su actualización), que reúne las mejores prestaciones de otros sistemas de compilación. Está basado en JVM (Java Virtual Machine), lo que significa que entiende cualquier script programado en Java.

Debido a estas ventajas, se ha seleccionado la herramienta de Android Studio para el desarrollo de la aplicación *CSPay.apk*, ya que es el mejor entorno para la creación de la mayoría de aplicaciones Android.

5.2.3 Desarrollo de la aplicación

El flujo de trabajo que se ha utilizado para el desarrollo de la aplicación Android de *CSPay* es el recomendado en la guía de usuario de la herramienta *Android Studio*, dado que es el entorno elegido para la implementación (ver *Figura 5.10*).



Figura 5.10: Flujo de trabajo estándar para el desarrollo de aplicaciones Android [49].

- **Setup:** En la sección de setup se configura el contexto del desarrollo y se crea un proyecto nuevo para la programación de la aplicación móvil. Una decisión importante que condiciona el resto del proyecto y se determina en esta etapa, es la parametrización del SDK (Software Development Kit) mínimo sobre el que se desea programar. Los niveles más bajos de las APIs disponibles presentan compatibilidad con mayor número de dispositivos, por lo tanto conviene seleccionar el menor nivel que permita satisfacer al menos las mínimas funcionalidades necesarias para llevar a cabo el proyecto. En la Figura 5.9 se puede apreciar la pantalla de configuración de Android Studio, con la versión Android 5.0 (Lollipop) seleccionada.

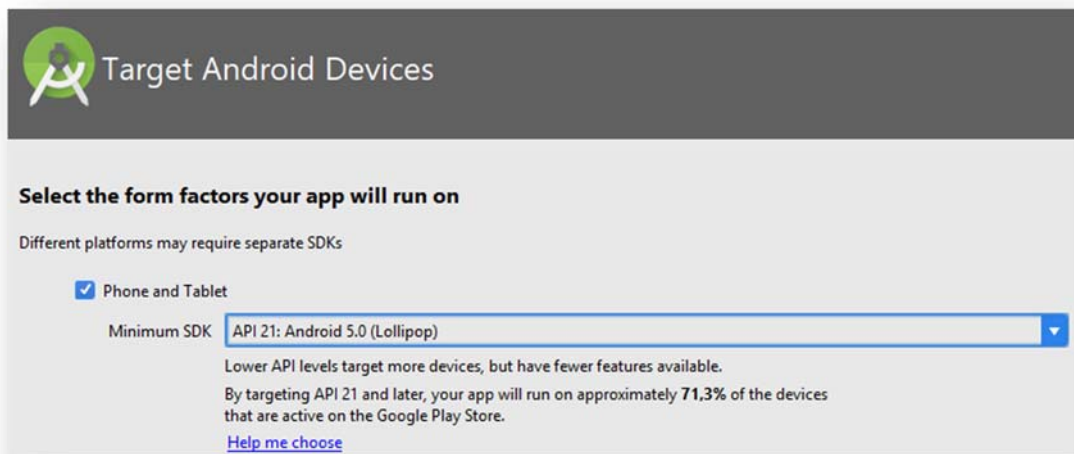


Figura 5.11: Pantalla de selección de versión Android.

Para la toma de la decisión, ha sido necesario analizar la tabla de ayuda que contiene la tasa de mercado contemplada para cada versión de Android y las funcionalidades básicas. Ver Figura 5.10.

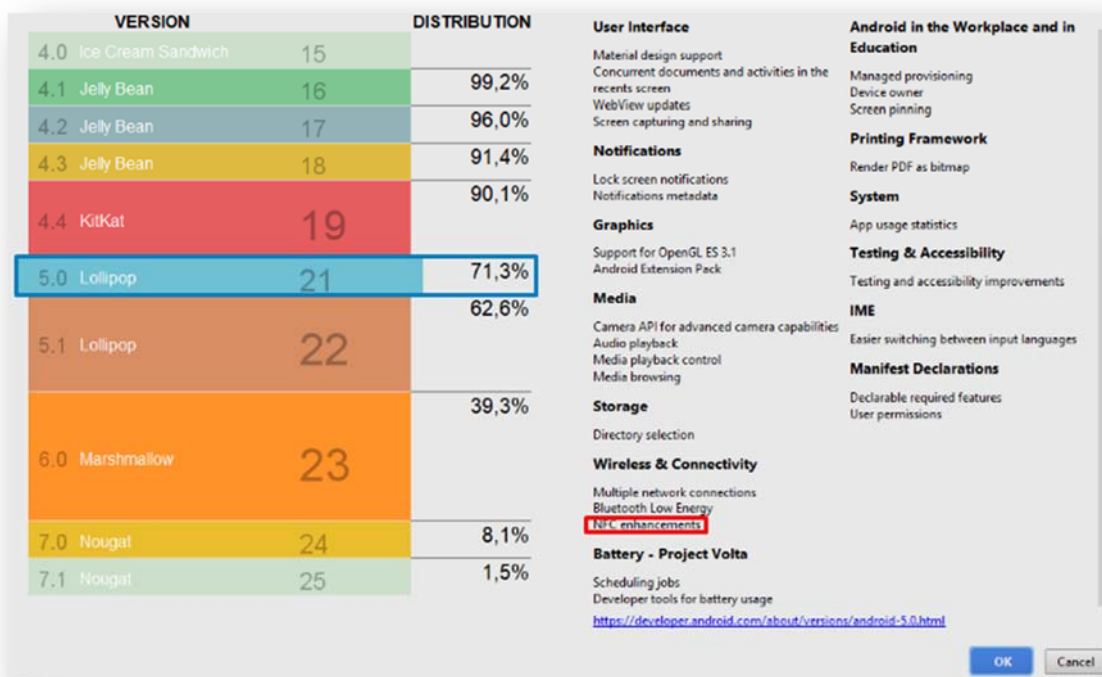


Figura 5.12: Porcentaje de utilización de distintas versiones Android

En la descripción de la versión de *Android 5.0 Lollipop* se notifica que a partir de esta versión (inclusive) existen mejoras en el NFC, en cuanto a un uso más amplio y flexible, por lo que en este aspecto resulta de especial interés programar en sistemas operativos que sean compatibles con las últimas funcionalidades disponibles en relación a esta tecnología. Además, presenta una cuota del 71,3% de compatibilidad con el mercado móvil Android de carácter mundial, por lo que la demo adquiere carácter representativo.

- **Write:** Esta sección alberga la programación íntegra de la aplicación. Antes de dar inicio al desarrollo del código ha sido necesario reflexionar detenidamente sobre el alcance y las funcionalidades teóricas de este servicio. Se puede observar, en la *Figura 5.11* el árbol de trabajo que define la estructura de la programación del proyecto *CSPay*. A continuación se exponen las secciones contenidas para el desarrollo de la solución.

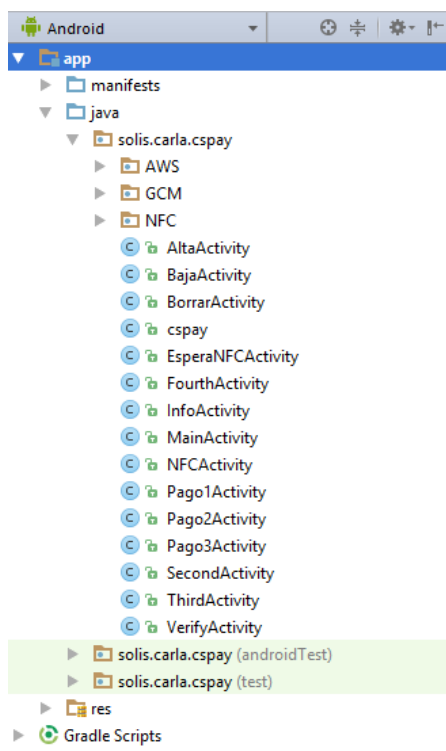


Figura 5.13: Árbol de trabajo de CSPay.

- **Manifests:** En esta sección se declaran los permisos de utilización para hacer uso de diferentes funcionalidades del dispositivo móvil desde la aplicación. Una vez que una aplicación es publicada y un usuario procede a su descarga desde Play Store, debe aceptar los permisos que han sido declarados para el correcto funcionamiento del servicio. Para el TFM, ha sido de vital importancia incluir los permisos de Internet (para establecer la comunicación desde el dispositivo móvil al servidor que procesa la transacción), GCM (con el fin de habilitar la recepción de mensajería push por parte del servidor) y NFC (para la lectura de las tarjetas contactless), como se muestra con el pseudocódigo en la *Figura 5.14*.

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="solis.carla.cspay.permission.C2D_MESSAGE" />
<uses-permission android:name="android.permission.NFC" />
```

Figura 5.14: Permisos de utilización declarados en el manifest.

En el manifests también es necesario emprender las configuraciones adicionales que requieren determinadas librerías (como la configuración del dispositivo en modo receptor para los mensajes push de la librería GCM), y la declaración de las actividades con sus connotaciones especiales (por ejemplo, qué *activity* tiene acceso a NFC).

- **Java:** Como ya se ha analizado, *Android Studio* es altamente utilizado debido a las ventajas que ofrece, ya que permite escribir fácilmente código de calidad, diseñar interfaces de usuario de forma sencilla y crear recursos para diferentes tipos de dispositivos. Por este motivo, existe una gran comunidad de desarrolladores activos que de forma pública comparten en la red librerías de interés común. Para la programación de la aplicación móvil del TFM, se han utilizado como referencia los siguientes tres proyectos con diferentes funcionalidades. En la fase de desarrollo, cada uno de los pilares que conforman el proyecto de Android fue particularizado y depurado de forma totalmente independiente, para su posterior integración en la aplicación móvil final:
 - **AWS:** Esta librería permite el envío de POST al servidor de pago. Se ha dominado AWS (Amazon Web Services) debido a que el destinatario de dicho POST está alojado en un servicio que ofrece Amazon en la nube (Apartado 5.2.3). Se ha personalizado la librería de referencia [50], creando la clase `SendPost` que simplifica la funcionalidad general, ya que permite el envío de un POST desde cualquier actividad o fase que desee desencadenarlo. La estructura que se ha definido para el envío de todos los POST al servidor, contiene los campos que se muestran en la *Figura 5.15*.

```
public String OP = "";
public String NOMBRE = "";
public String CORREO = "";
public String TLFN = "";
public String DNI = "";
public String PASS = "";
public String PAN = "";
public String DATE = "";
```

Figura 5.15: Estructura POST.

No es obligatorio completar la información de todos los campos en cada petición (pueden viajar vacíos), la necesidad de recuperar los valores en el servidor, dependerá del tipo de solicitud que se envíe en cada fase.

Se adjunta la dirección destino del POST utilizada durante gran parte del desarrollo del proyecto. La URL del servidor está sujeta a cambios mensualmente por restricciones de licencias (detallado en el *Apartado 5.2.3*).

```
BASE_URL = "http://cspayprocess.ddns.net";
```

Figura 5.16: URL servidor.

- *GCM*: La utilización del servicio *Google Cloud Messaging* permite la recepción de push en la aplicación, por lo que su implementación es fundamental [51]. El primer paso es registrar la aplicación en el sitio web de GCM [52] y obtener las claves para la fase de autenticación de las futuras comunicaciones. El gran dilema en la definición del servicio desde la perspectiva del dispositivo móvil, fue si se llevaba a cabo o no, la suscripción de un número de teléfono al registro de TOKEN mediante un TOPIC. Esta decisión, en líneas generales, condiciona el diagrama completo del diseño. De no suscribir el teléfono móvil a un TOPIC, se hacía necesario transmitir el TOKEN asignado (y las actualizaciones del mismo, ya que caduca periódicamente) al servidor de pago alojado en AWS, para que almacenase y restaurase este valor en una base de datos, que permitiese identificar al dispositivo mediante la vinculación:

Número de teléfono → TOKEN asociado

Con el fin de disminuir la complejidad del servidor, para la obtención de los mismos servicios, se decidió suscribir el número de teléfono a un TOPIC. De esta forma, es Google quién dispone de la vinculación del número de teléfono del usuario con el TOKEN necesario para establecer la comunicación. Dado este escenario, el servidor únicamente tiene que transmitir el número de teléfono que recibe de la página web del comercio electrónico (si está dado de alta en el servicio de *CSPay*) y transmitírselo a *Google*. Este flujo permite, a su vez, que el dispositivo móvil no tenga que enviar el TOKEN que recibe de Google al servidor de pago alojado en AWS.

La suscripción del número de teléfono a un TOPIC, se realiza en la tarea de *RegistrationService* contenida dentro de GCM, como se describe en la *Figura 5.17*:

```
subscription.subscribe(registrationToken, "/topics/" + TLFN, null);
```

Figura 5.17: Suscripción número de teléfono a Topic.

La clase *GcmIntentService* gestiona los eventos de recepción de mensajes push:

- Activa el flag de push recibido.
- Completa el motivo del desencadenante del push para liberar una acción u otra en el dispositivo móvil.

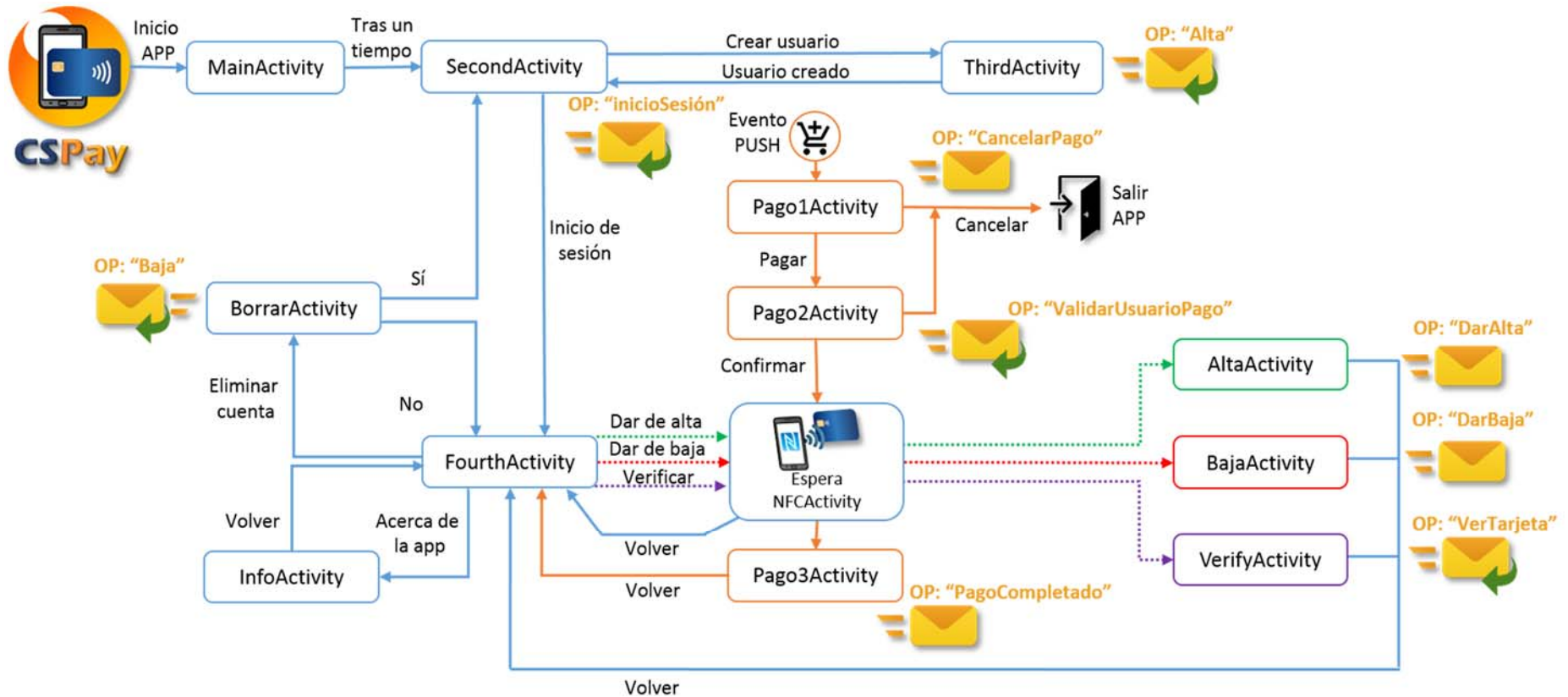
En el caso especial de recibir un push de pago, se guarda la información contenida en el mensaje (identificador del comercio electrónico, importe de la transacción y moneda). En este escenario, aparece una notificación de *Android* en la parte superior izquierda del dispositivo, personalizada con un carrito de la compra. Una vez que el usuario pulsa en la notificación, se recuperan los datos y se muestran por pantalla, además de ser utilizados de forma interna en el transcurso de la operación.

- *NFC*: Se utiliza una librería NFC para la lectura de las tarjetas inteligentes mediante comandos EMV Contactless (ver *Capítulo 3*) disponible de forma libre internet [53]. Se personaliza el código básico disponible para la obtención de los campos de interés (PAN y fecha de caducidad) almacenados en el chip de la tarjeta y con carácter necesario para desencadenar una solicitud o una transacción de pago. Tal y cómo fue estudiado, en tecnología sin contactos, los flujogramas son distintos en función del AID de la aplicación. Para el TFM se ha desarrollado la secuencia de comandos básicos para la implementación de una transacción EMV Contactless para tarjetas Visa (kernel 3) y MasterCard (kernel 2).

Las *Activities* aparecen también en el directorio raíz de java (junto con AWS, GCM y NFC), y representan cada una de diferentes etapas programadas para establecer la funcionalidad completa del sistema. Con el fin de satisfacer las necesidades expuestas en el *Apartado 5.2.1*, se organiza la aplicación desde dos puntos de vista diferentes en función de la solicitud de acceso a la aplicación:

- Interactuación manual por parte del usuario.
- Recepción de una notificación push de pago.

En la *Figura 5.18* se muestra el esqueleto de todas las actividades que se pueden desencadenar en función de los dos puntos de entrada. Este diagrama representa visualmente la conexión entre todas las actividades programadas y los mensajes POST y push que son intercambiados con el servidor. Se observa que, en el flujo nominal, existe la actividad *EsperaNFCActivity* compartida entre ambas vías. A continuación se definen cada una de las actividades partícipes en la solución:



* = Se envía POST al servidor ->post.send()

= Se envía POST al servidor y se recibe un PUSH como respuesta.

Figura 5.18: Esquema completo del funcionamiento de la APP-

- **MainActivity:** Visualiza por pantalla el logotipo diseñado para la aplicación durante un breve periodo de tiempo. Si existe información de usuario, se recupera en esta fase (nombre, teléfono y DNI) y se manda una actualización del TOKEN a Google (solicitud de actualización de la suscripción al TOPIC\TLFN). Posteriormente, da paso a la ventana de SecondActivity. Ver *Figura 5.19*.

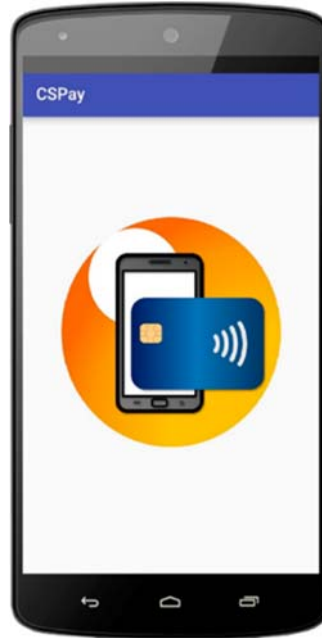


Figura 5.19: MainActivity en la APP.

- **SecondActivity:** Fase de inicio de sesión o de creación de nueva alta en el servicio. Si se pulsa el botón de INICIO DE SESIÓN, se envía un POST con las credenciales del usuario introducidas al servidor de pago. Si se realiza correctamente la validación, se recibe un push que habilita el acceso a *FourthActivity*. De lo contrario, se solicita volverlo a intentar. Si se pulsa CREAR USUARIO, la aplicación móvil redirige a *ThirdActivity* para mostrar el formulario de una nueva cuenta de usuario. Ver *Figura 5.20*.



Figura 5.20: SecondActivity en la APP.

- **ThirdActivity:** Se solicita al usuario que complete los campos que aparecen en la lista para la creación de un nuevo cliente del servicio *CSPay*. En caso de existir una cuenta para ese dispositivo móvil, no se permite una nueva creación por motivos de seguridad. Ver *Figura 5.21*.



Figura 5.21: ThirdActivity en la APP.

- **FourthActivity:** Una vez que se ha autenticado correctamente el usuario (proviene de la fase *SecondActivity*) se muestra un menú con las opciones disponibles en la aplicación. En función del botón que pulse el usuario, se desencadenará una sucesión de eventos u otra. Ver *Figura 5.22*.



Figura 5.22: FourthActivity en la APP

- **EsperaNFCActivity:** El objetivo de esta etapa es mostrar un mensaje por pantalla para que el usuario aproxime su tarjeta contactless y pueda intentar leer la tarjeta. Si se produce una lectura correcta, salta a la ventana siguiente. De lo contrario, se solicita una sucesión de reintentos por parte del usuario. Ver *Figura 5.23*.



Figura 5.23: EsperaNFCActivity en la APP.

- **NFCActivity:** Esta etapa se activa siempre que se aproxime una tarjeta contactless al dispositivo móvil con la aplicación preparada. Si la tarjeta se aproxima cuando *EsperaNFCActivity* está en ejecución, se realiza una lectura del PAN y de la fecha de caducidad que se utilizará para el evento que haya desencadenado la fase de *EsperaNFCActivity*. En función de la petición de lectura de la tarjeta (alta, baja, verificación o pago) se desencadena una actividad u otra, siendo este flujo transparente para el usuario. Si, por el contrario, el usuario aproxima la tarjeta en una pantalla dónde esta actuación no procede, se notifica en una nueva ventana. Ver *Figura 5.24*.



Figura 5.24: NFCActivity en la APP.

- **AltaActivity:** La finalidad es esta etapa es dar de alta una tarjeta en la base de datos del servidor de pago, por lo que se envía un POST con los datos leídos de la tarjeta en la etapa *NFCActivity* y se presenta en la pantalla el contenido de los mismos. Ver *Figura 5.25*.



Figura 5.25: AltaActivity en la APP.

- **BajaActivity:** El proceso de esta fase es similar al caso anterior, pero con la salvedad de que el fin es dar de baja la tarjeta en la base de datos del servidor. El POST contiene los mismos datos pero con un identificador OP distinto. Ver *Figura 5.26*.



Figura 5.26: BajaActivity en la APP.

- **VerifyActivity:** El objetivo de esta etapa es que el usuario pueda comprobar si una tarjeta está dada de alta o no en el servicio. De esta forma, se envía un POST con los datos de la tarjeta leídos y se espera respuesta a la petición por parte del servidor (push). En función de la respuesta que proporcione el servidor, se muestra en la pantalla si la tarjeta está o no operativa para el servicio de *CSPay*. Ver *Figura 5.27*.



Figura 5.27: VerifyActivity en la APP.

- **BorrarActivity:** Esta sección se encarga de dar de baja a un usuario en la aplicación. Se envía un POST con los datos del usuario, para eliminar del servidor la información vinculada al titular, y tras la confirmación del servidor (push) de que la solicitud ha sido procesada correctamente, se eliminarán los datos almacenados en el teléfono. Ver *Figura 5.28*.



Figura 5.28: BorrarActivity en la APP.

- **InfoActivity:** Se muestra el logo de la Universidad de Alcalá e información de la desarrolladora de la aplicación. Ver *Figura 2.29*.



Figura 5.29: InfoActivity en la APP.

- **Pago1Activity:** Esta ventana únicamente aparece tras recibir un push de pago y pulsar en dicha notificación. Se muestran los datos relevantes de la solicitud de pago originada en la página web de la compra online (identificador del comercio, importe y moneda). Si se cancela, se envía POST al servidor con la definición de la acción. Si se acepta el pago, la aplicación continua a la ventana de Pago2Activity. Ver *Figura 5.30*.

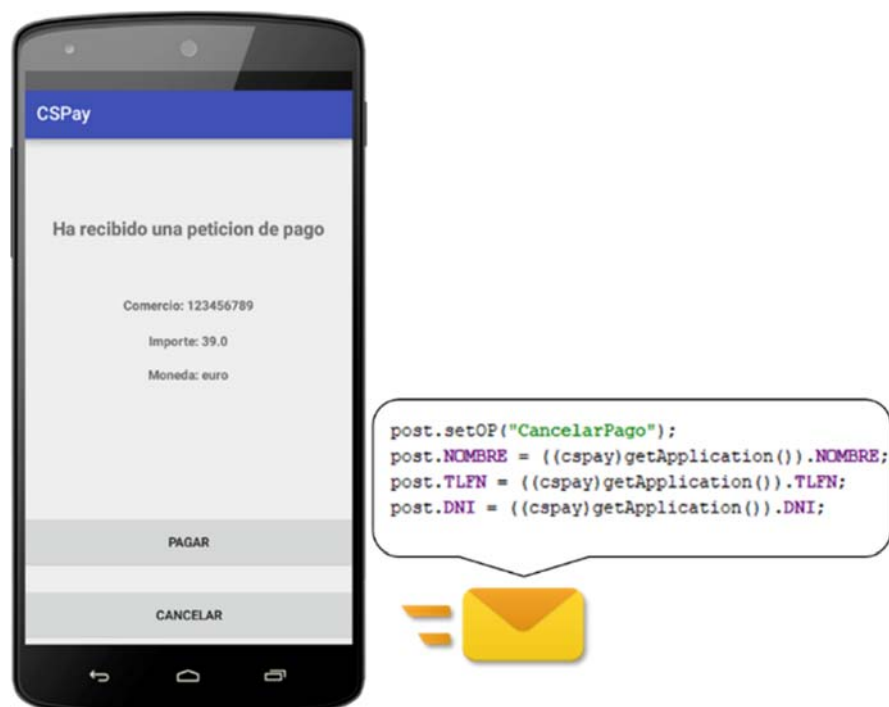


Figura 5.30: Pago1Activity en la APP.

- **Pago2Activity:** Se solicita al usuario que se autentique. Esta ventana difiere de *SecondActivity*, debido a que en esta fase no existe la posibilidad de crear un usuario nuevo. Si se cancela en esta fase, se envía el mismo POST que desde la cancelación de *Pago1Activity*. Si se introducen los datos de usuario, se envía un POST con esta información. Si la autenticación es correcta, se recibe del servidor un push que permite acceder a la pantalla de *EsperaNFCActivity*. Ver *Figura 5.31*.

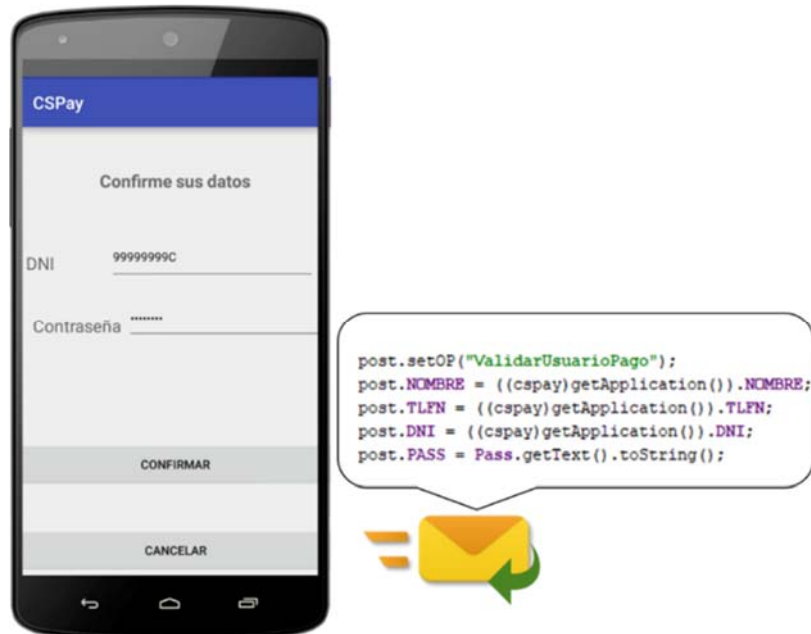


Figura 5.31: Pago2Activity en la APP.

- **Pago3Activity:** Se envía un POST con los datos leídos de la tarjeta y se informa al usuario que la solicitud de pago ha sido procesada. El resultado de la operación dependerá del servidor y será mostrada en la página web del comercio electrónico. Ver *Figura 5.32*.



Figura 5.32: Pago3Activity en la APP.

- **cspay:** Es una actividad en la que se almacena información compartida entre las diversas actividades. Por ejemplo, se registra si se ha recibido un push, y de qué tipo, así como los datos del cliente a guardar en la aplicación, como son el número de teléfono, el nombre de usuario y el DNI.

- **Build & Run:** En esta etapa se construye el proyecto en un paquete de APK de debug (*CSPay.apk*), con el fin de que pueda ser ejecutado en el emulador o en un dispositivo con Android. Para la elaboración de la demo del TFM se ha utilizado la funcionalidad de descarga en el teléfono con los siguientes dispositivos: Samsung 5, Samsung 7 y BluBoo. De esta forma, se realiza la verificación del funcionamiento correcto sobre el dispositivo final a tiempo real y tras cada modificación (rápida revisión de cambios y ajustes o calibraciones en las pantallas).

- **Iterate:** Este paso se denominada iteración por la sucesión de etapas de depuración, perfiles y pruebas, con el enfoque de eliminar los errores y optimizar el rendimiento de la aplicación.

- **Publish:** El último hito es la publicación de la aplicación móvil para la descarga pública y masiva por parte los usuarios. Dado que no es una versión real, se omite el paso de la puesta en producción. Los dispositivos móviles que quieran hacer uso de la demo serán configurados en modo programador y se llevará a cabo la instalación de la aplicación en modo debug.

5.3 TARJETAS FINANCIERAS DE PRUEBAS

Se diseñan y personalizan tarjetas de pruebas específicas para llevar a cabo la demo del sistema transaccional completo. Las tarjetas inteligentes utilizadas contienen sistemas operativos certificados y satisfacen los criterios establecidos por Visa o MasterCard. En definitiva, presentan un comportamiento similar a las tarjetas financieras en circulación, con la salvedad que las claves almacenadas en el chip no corresponden con el valor esperado en un entorno real. De lo contrario, se podría considerar que se están emitiendo nuevas tarjetas en la calle de forma irregular.

Durante el desarrollo y las pruebas del proyecto, se han utilizado los siguientes dispositivos:

- Tarjeta inteligente física

Se crean nuevas tarjetas inteligentes a partir de distintos fabricantes de chip, con diferente sistema operativo cargado e imagen de personalización dispar, con el fin de realizar lecturas correctas y verificar el funcionamiento adecuado a nivel global. Cada una de las muestras ha sido personalizada con valores (número de tarjeta y fecha de caducidad) exclusivos.

Para la estampación de las tarjetas, se ha utilizado la herramienta *Datacard Financial ID Card Printer* haciendo uso del software *ID Works Design & Production*, ya que se dispone de este material en las instalaciones del edificio de Redsys. Para las tarjetas cuyo fin son pruebas nominales, se ha utilizado el logo diseñado para la aplicación *CSPay* y el escudo de la Universidad de Alcalá. Ver *Figura 5.33*.



Figura 5.33: Imagen de tarjeta real e impresora utilizada.

Para los ensayos particulares, que requieren que la operación sea denegada por estar sujeta a condiciones características, se han esbozado dos diseños más. El resultado es que la transacción se rechaza, ya sea porque desde el servidor de pago se detecte que esté relacionada con movimientos fraudulentos (seguimiento de las últimas transacciones con carácter sospechoso o por notificación de robo) o bien, porque esté caducada y el usuario no la haya dado de baja en el sistema. Ver *Figura 5.34*.



Figura 5.34: Estampado tarjeta robada y tarjeta caducada

- **MiniTag en weareables**

Los estudios efectuados con dispositivos weareables, preparados para el entorno de pruebas como las tarjetas físicas descritas con anterioridad, también han obtenido un resultado exitoso. Tal y cómo se indica en el *Capítulo 1*, un MiniTag es una tarjeta convencional pero de tamaño reducido, por lo que la única discrepancia reside en las dimensiones de la antena y, por lo tanto, se necesita mayor proximidad física entre los elementos (móvil y MiniTag) para obtener un valor de campo suficiente para la transmisión de la información.

- **Tarjetas físicas reales**

El piloto también ha sido probado con una gran variedad de tarjetas reales (de diferentes bancos), llevando a cabo lecturas correctas de dichos soportes físicos personales, que están actualmente vigentes y en circulación. Se llevó a cabo esta práctica para garantizar el funcionamiento correcto de la aplicación actual y preparar el sistema por si en un futuro se deseara adaptarlo a un entorno de pre-producción/producción. Sin embargo, no se recomienda una batería de pruebas extensa hasta que la información no se almacene cifrada en el servidor, ya que actualmente las bases de datos residen en texto plano en AWS, y no es una buena práctica almacenar información sensible aunque el entorno sea controlado.

- **Tarjetas virtuales (tokenizadas) generadas con la opción de pago móvil**

Se ha verificado que también es viable emprender la lectura de una tarjeta virtual generada y almacenada en un dispositivo móvil. Para ello es necesario que el móvil esté configurado como elemento pasivo (emulando el comportamiento de una tarjeta financiera) sobre el móvil que tiene instalada la aplicación CS Pay (elemento activo). Dicha actividad se representa en la *Figura 5.35*.



Figura 5.35: Esquema de pago con CSPay y pago móvil.

Se aprecia que la solución es flexible y presenta alta compatibilidad con las diferentes opciones financieras emergentes en el sector de los medios de pago. Este hecho es muy significativo, ya que a priori no establece barreras tecnológicas que frenen la adaptación del proyecto, más allá de los requerimientos teóricos establecidos en la definición de la idea.

5.4 SERVIDOR PARA EL PROCESAMIENTO Y RESOLUCIÓN DE TRANSACCIONES E-COMMERCE

Se desea programar un servidor que emule el comportamiento de un centro procesador y de resolución de transacciones financieras. Se requiere que dicho servidor esté disponible en la nube e interactúe de forma particular con los distintos elementos que participan en el sistema y envían peticiones para su procesado, como los que se introducen a continuación:

- **Páginas web de comercios electrónicos:** Desde el sitio web se envía una solicitud de tipo POST al servidor con el número de teléfono del cliente, el importe de la transacción, el identificativo del comercio y el código de moneda, entre otros datos de interés. Esta petición es gestionada por el servidor y desencadena una serie de acciones. Una vez completado el proceso, el servidor notifica la resolución de la transacción financiera mediante un *Status Code* específico (particularizado y definido para la comunicación entre el servidor y la web del comercio electrónico), vinculado a la solicitud POST previamente recibida.
- **Dispositivos móviles:** Las solicitudes que atiende el servidor generadas en el dispositivo móvil son tipo POST y se realiza un filtrado en la recepción según el campo "OP" definido y contenido en el mensaje, con el fin de ejecutar una funcionalidad u otra. Para establecer la comunicación desde el servidor a un teléfono móvil, es necesario utilizar mensajería push y, por lo tanto, el dispositivo debe tener la aplicación instalada y haber dado de alta un usuario en el sistema.

El servidor también presenta la funcionalidad extra de enviar correos electrónicos a la cuenta personal del usuario de la aplicación móvil, remitiendo un mensaje de bienvenida tras una alta nueva en el sistema, así como el resultado de cada una de las operaciones financieras que se lleven a cabo utilizando el nuevo medio de pago.

5.4.1 Elección del lenguaje de programación de la red de pago

Se implementa el servidor que contiene la lógica del procesamiento de las peticiones y la capacidad de resolución de dichas operaciones, sirviendo como nexo entre el sitio web del comercio electrónico y el dispositivo móvil del cliente. Se ha realizado en lenguaje de programación Python, y a continuación se enumeran los principales motivos para ello.

- Es un lenguaje de programación interpretado, cuya filosofía hace hincapié en una sintaxis que favorezca un código legible y, por lo tanto, resulta más sencilla, simplificada y rápida la programación de alto nivel.
- Es elegante, flexible y portable, con módulos diferenciados y ordenados, por lo que presenta alta compatibilidad y escalabilidad.
- Tiene un estilo productivo, de tal forma que en menos líneas se consiguen las mismas prestaciones que con otros lenguajes de alto nivel, sin ser necesario prestar tanta atención a los detalles, como la declaración y definición de todos los datos.

- Una comunidad de desarrolladores respalda este lenguaje. Este aspecto es muy importante, ya que permite la puesta en común de nuevos planteamientos en foros, la consulta de problemáticas, la disposición de código abierto de uso público y manuales compartidos con funcionalidades auto-contenidas, permitiendo al desarrollador tener herramientas enriquecedoras para el desarrollo de su cometido.
- Conocimiento de programación Python.

Dadas las ventajas expuestas, se codifica la operativa del servidor en el lenguaje de programación Python, a partir de un editor de texto común pero que disponga de prestaciones interesantes. Se ha seleccionado como medio de trabajo Notepad++, por ser un editor altamente funcional y gratuito, que permite resaltar la sintaxis de la codificación en Python, además de agrupar secciones de código, proporcionando plegables que puedan ocultar o mostrar las funciones, y hacer la lectura más legible. Además, Notepad++ proporciona guías de ajuste de sangría, particularmente útil para la definición de los bloques de código funcional de Python. Para guardar un script en Python, a partir de un editor de texto, se modifica manualmente la extensión de *.txt* a *.py*. La ejecución del script *.py*, siempre se llevará a cabo a través del servidor alojado en la nube, ya que requiere de la recepción, procesamiento y el envío de peticiones POST.

5.4.2 Procesador transaccional alojado en la nube

Se desea crear un servidor web, con el fin de disponer en la nube del bloque que emula el funcionamiento de la red de pago, de tal forma que pueda ser visible y alcanzable vía HTTP por los dispositivos móviles y las páginas webs de los comercios electrónicos. Se ha elegido Amazon Web Services (AWS) para la creación de la máquina virtual, con el fin de que albergue el código Python previamente programado con el objetivo de ejecutarlo de forma eficiente y autónoma.

La decisión acerca de la utilización de AWS ha sido determinada en función de la experiencia en la creación de instancias en Internet. El servicio que se ha utilizado, contenido en la oferta de AWS, es Amazon Elastic Compute Cloud (EC2), que está diseñado para proporcionar a los desarrolladores capacidad informática en la nube de forma segura, con control del entorno y de tamaño variable y escalable, siendo muy resistente a errores [54]. Además, el servicio web de Amazon EC2 permite activar y desactivar de forma rápida instancias en el servidor, por lo que únicamente se factura en función de las capacidades utilizadas para cubrir las necesidades de cada proyecto. Para el caso del servidor del TFM, se ha utilizado la capa gratuita de Amazon EC2, creando una instancia denominada *CSPay* (ver Figura 5.37), que permite una disposición máxima de funcionamiento operativo de 750h al mes, siempre y cuando el volumen de tráfico no denote carga relativa a servicios en producción.

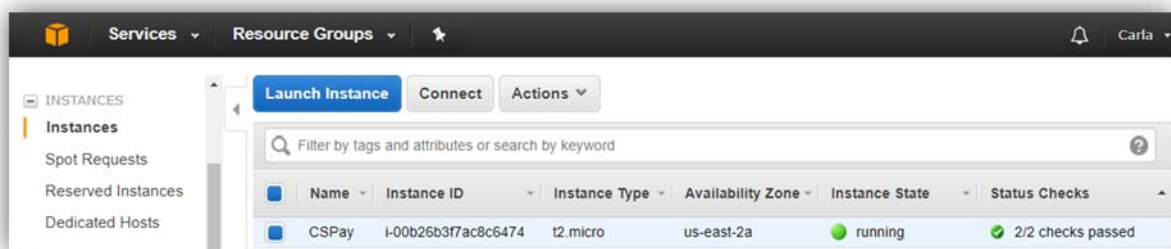


Figura 5.37. Instancia creada en AWS para el servidor de pago del piloto.

Tras la creación de la instancia, se genera automáticamente la clave de autenticación necesaria para establecer la conexión de forma remota a la máquina virtual de Amazon. Dicha clave presenta un formato *.pem*, no soportado por las herramientas que se desean utilizar, como Putty y WinSCP, para el acceso desde el ordenador personal al servidor, por lo que, tras la descarga, debe ser transformada a un formato conocido. Antes de emprender la conversión de la clave, es necesario definir los puertos en la instancia de AWS para habilitar las comunicaciones pertinentes. La configuración por defecto de EC2 incluye el tipo de conexión SSH (Secure Shell) en el puerto 22, que es la forma de establecer la comunicación entre el equipo personal y la instancia creada. En este listado es necesario añadir la conexión HTTP con puerto 80, para la emisión y recepción de peticiones POST. Ver Figura 5.38.



Figura 5.38: Definición de puertos.

Tras la configuración de los puertos, se retoma la fase de transformación del formato de la clave de autenticación (*.pem*), obtenido de AWS, para su uso en herramientas de acceso remoto a la instancia, que necesitan disponer de la extensión *.ppk*. La herramienta que permite establecer la conversión de la claves es PuTTY Key Generator (PuttyGen) [55]. Se adjunta la captura de pantalla correspondiente a esta fase en la Figura 5.39.

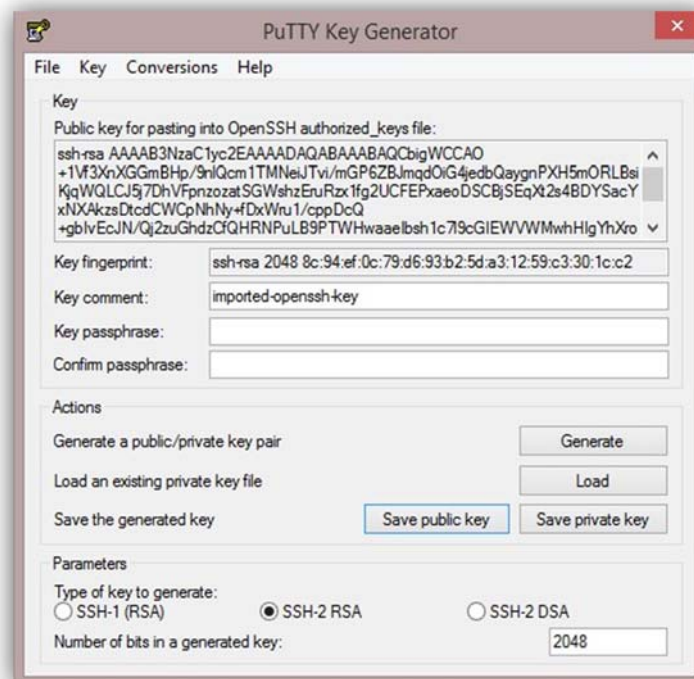


Figura 5.39: Conversión de claves en PuttyGen.

Una vez que se obtiene la clave *.ppk* y se verifica que el puerto 22 correspondiente a SSH está correctamente configurado en la instancia de AWS, se puede hacer uso del programa WinSCP. Esta herramienta permite la transferencia bidireccional de datos entre el ordenador personal y la instancia, con el código del servidor de pago, alojada en la nube. Para su apropiada configuración, se debe insertar la ruta de la clave de autenticación (el repositorio dónde reside el archivo *.ppk*), el usuario (*Ubuntu*, debido a los parámetros seleccionados en la creación de la instancia) y la IP pública dinámica que la instancia toma en el arranque, como muestra la *Figura 5.40*.

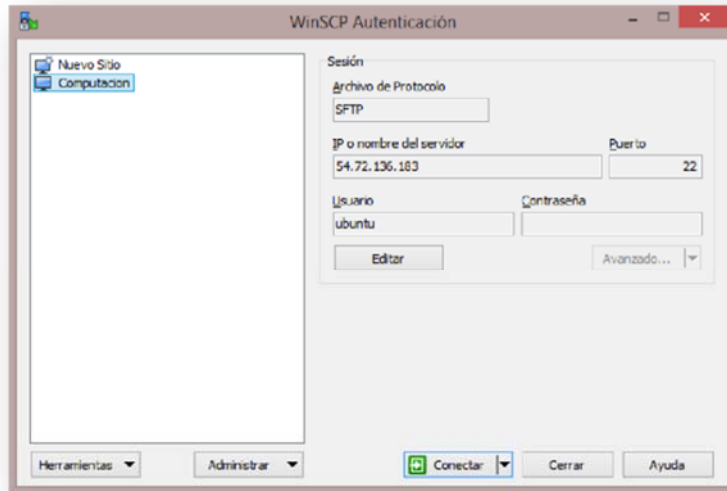


Figura 5.40: Autenticación con el servidor para la utilización del programa WinSCP.

Una vez establecida la comunicación entre el ordenador personal y la máquina de AWS, se puede realizar la transferencia de archivos de forma sencilla, arrastrando archivos o carpetas, además de abrir, editar o borrar la información, directorios o códigos almacenados en la nube, como muestra la *Figura 5.41*.

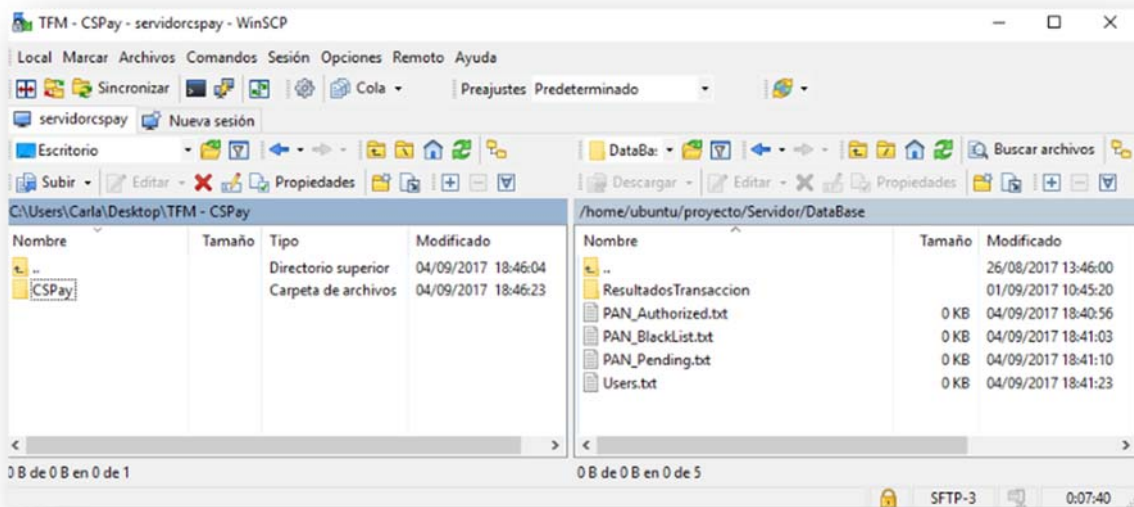


Figura 5.41: Transferencia de archivos con WinSCP.

Con el fin de evitar costes adicionales, la IP pública no es fija sino dinámica, de tal forma que cada vez que se produce el arranque de la instancia, se ve modificada. Esta situación es conflictiva y requiere ser solventada, ya que, de lo contrario, habría que modificar el código de la página web y de la aplicación Android cada vez que se enciende la instancia. Cabe recordar que, dicha instancia, no se puede dejar encendida, dado que es una versión gratuita de prueba con la restricción de 750h mensuales de uso. Por lo tanto, se busca una alternativa funcional y económica para la problemática establecida.

La página web de No-IP [56], ofrece un servicio dinámico de DNS (Domain Name System) que permite asociar una URL estática a cada IP pública dinámica que vaya adquiriendo la máquina de AWS. Para completar este proceso, es necesario crear una cuenta de usuario en No-IP y registrar un dominio de uso, que presenta una validez de 30 días. Dado que el piloto tiene una fecha de inicio de desarrollo del proyecto superior a tres meses, cabe destacar que ha sido necesaria la activación de tres dominios diferentes (con sus consecuentes cambios en el bloque de la aplicación móvil y de la página web), siendo los siguientes:

- *cspayprocess.ddns.net*
- *cspayserver.ddns.net*
- *cspay.ddns.net*

Para la vinculación de la activación de la máquina de AWS (momento en el que se asigna una dirección IP pública), con la resolución del dominio (cuenta No-IP), se ha creado un script de ejecución automático en el arranque del sistema. De esta forma, cuando se enciende la instancia CSPay a través de la página web de AWS, se resuelve la IP dinámica a la URL previamente definida, y se inicializa el código Python del servidor de pago desarrollado. En la *Figura 5.42* se adjunta el script de arranque, fundamental para la resolución de la problemática expuesta.

```
#!/bin/bash
cd /usr/local/src/noip-2.1.9-1
./noip2
cd /home/ubuntu/proyecto/Servidor
sudo python Server.py
```

Figura 5.42: Script de arranque.

5.4.3 Mensajería push: GCM

Se plantea el uso de la mensajería push, como recurso necesario para el envío de notificaciones desde el servidor de procesamiento y resolución del pago, a los diferentes dispositivos móviles suscritos al servicio CSPay. El funcionamiento de la mensajería push consiste en la identificación del dispositivo móvil a partir de un token que generalmente proporciona APNS (Apple Push Notification Service) para los móviles Apple y GCM (Google Cloud Messaging) para aquellos que pertenecen a Google. Dado que el desarrollo de la aplicación móvil ha sido destinado a Android, será necesario hacer uso del sistema GCM [52]. Además, Redsys tiene experiencia con Google en este tipo de mensajería, por lo que añadir funcionalidades a un canal existente resulta más sencillo que entablar una nueva comunicación desde su fase inicial.

Aun así, se ha hecho un estudio del mercado, identificando otros proveedores que ofertan el servicio de mensajería push. Entre otros, destaca Amazon SNS (Simple Notification Service), que se publicita como un sistema de envío de mensajería push, de forma sencilla y rentable [57]. Tras analizar su esquema de trabajo, se pudo deducir que desde Amazon SNS emiten una petición a GCM, para sea este quién localice el dispositivo móvil (ver *Figura 5.43*).

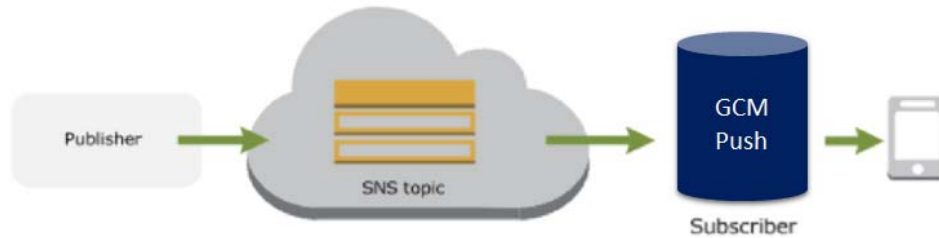


Figura 5.43: Esquema de trabajo de Amazon SNS.

De tal forma que existe la necesidad de operar a través de Google, por lo que se considera más óptimo trabajar sin intermediarios y comunicar directamente desde el servidor de pago (AWS) al servicio GCM.

5.4.4 Procesamiento y administración de las bases de datos

Se ha definido una serie de bases de datos en el servidor para satisfacer los requerimientos funcionales, así como para la correcta administración y gestión de la información. Estos archivos residen en la nube, por lo que se necesita establecer comunicación mediante WinSCP para la recuperación de los mismos.

- Directorio **users.txt**: El servidor escribe en esta base de datos la información que recibe del POST cuyo origen es el dispositivo móvil con la identificación de OP = 'Alta', siempre y cuando no existan datos asociados a ese dispositivo móvil. En el caso de recibir un POST con OP = 'Baja' elimina todos los datos correspondientes al número de teléfono que emitió dicha solicitud. Ante la recepción de OP = 'InicioSesion' o bien, OP = 'ValidarUsuarioPago', se consulta el directorio para verificar si la contraseña es correcta. Si el origen de la petición es la página web de un comercio electrónico, se comprueba si el número de teléfono con el que se desea llevar a cabo el pago corresponde a un usuario dado de alta en el servicio. Ver *Figura 5.44*.

```

    1 Carla carla.solis@edu.uah.es 612345678 99999999C proyecto
  
```

Normal text file length: 59 lines: 1 Ln: 1 Col: 60 Sel: 0 | 0 Dos\Windows ANSI INS

Figura 5.44: Ejemplo Users.txt.

- Directorio **PAN_Pending.txt** y **PAN_Authorized**: El registro PAN_Pending almacena la información recibida en el POST que procede de un dispositivo móvil con OP = 'DarAlta'. Si, por el contrario, la OP = 'DarBaja' o 'Baja', se eliminan todos los datos correspondientes al número de teléfono que emitió dicha solicitud de ambas bases de datos. Para que una solicitud de tarjeta pendiente, pase a ser autorizada, el administrador del sistema debe realizar un traslado manual de la información de una base de datos a otra, emulando que se ha recibido el consentimiento de la entidad bancaria emisora de la tarjeta financiera a la solicitud de tarjeta nueva en el servicio (ver *Figura 5.45*). El directorio de PAN_Authorized se consulta ante la recepción de una petición OP = 'PagoCompletado' desde el dispositivo móvil. Si existe coincidencia de la tarjeta aproximada con los datos almacenados en dicha base de datos, siempre y cuando no esté caducada ni aparezca en el directorio PAN_BlackList.txt, la operación será aprobada.

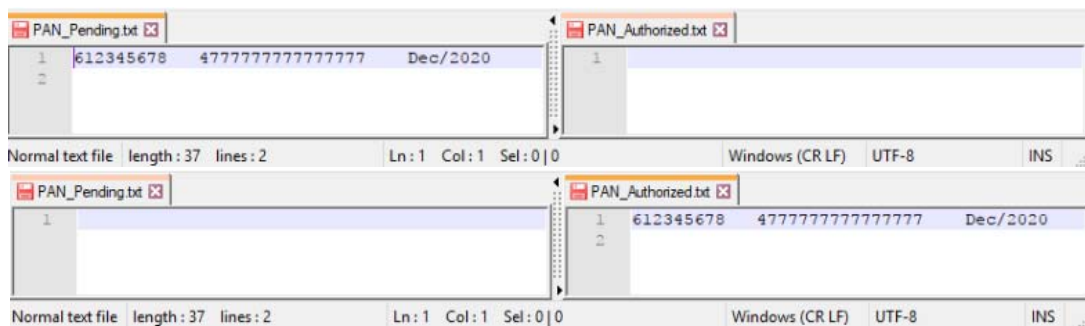


Figura 5.45: Ejemplo de intercambio de información entre PAN_Pending.txt y PAN_Authorized.txt.

- Directorio **PAN_BlackList.txt**: Este registro almacena la información de las tarjetas que están sujetas a connotaciones fraudulentas. Se inserta de forma manual los datos que aparecen en la *Figura 5.46*, emulando la notificación de la entidad emisora al centro procesador, con el fin de que el servidor deniegue toda transacción financiera que se intente realizar con dicha tarjeta. Este directorio se consulta ante la recepción de OP = 'ValidarPago' desde el dispositivo móvil. Si existe coincidencia de los datos recibidos con los que figuran en la lista, la transacción financiera será denegada ante la sospecha de que la tarjeta ha sido copiada, clonada o robada.

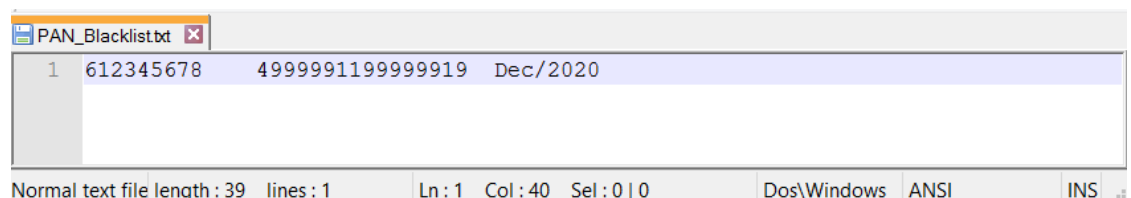


Figura 5.46: Ejemplo PAN_Blacklist.txt.

- Directorio **logs.txt**: Esta base de datos permite la monitorización y revisión de todas las peticiones que entran al sistema, independientemente del origen de las mismas (páginas webs de los comercios electrónicos o solicitudes de los teléfonos móviles), con el fin de controlar el entorno de procesamiento transaccional. Ver *Figura 5.47*.

```

1 POST (12/9 14:40:52): {'TLFN': '612345678', 'DNI': '99999999C', 'CORREO': 'carla.solis@edu.uah.es', 'PASS': 'demo',
2 'DATE': '', 'NOMBRE': 'Carla', 'PAN': '', 'OP': 'Alta'}
3
4 POST (12/9 14:41:17): {'TLFN': '612345678', 'DNI': '99999999C', 'CORREO': '', 'PASS': 'aa',
5 'DATE': '', 'NOMBRE': 'carla', 'PAN': '', 'OP': 'InicioSession'}
6
7 POST (12/9 14:45:30): {'TLFN': '612345678', 'DNI': '99999999C', 'CORREO': '', 'PASS': '',
8 'DATE': 'Dec%2F2020', 'NOMBRE': 'carla', 'PAN': '4777777777777777', 'OP': 'DarAlta'}
9
10 POST (12/9 14:55:16): {'TLFN': '612345678', 'DNI': '99999999C', 'CORREO': '', 'PASS': '',
11 'DATE': 'Mar%2F2019', 'NOMBRE': 'carla', 'PAN': '4777777777777777', 'OP': 'VerTarjeta'}
12
13 POST (12/9 15:10:22): {'origen': 'cspay', 'fuc': '123456789', 'moneda': 'euro', 'idioma': 'Spa',
14 'telefono': '612345678', 'importe': '1150'}
15
16 POST (12/9 15:11:20): {'TLFN': '612345678', 'DNI': '99999999C', 'CORREO': '', 'PASS': 'aa',
17 'DATE': '', 'NOMBRE': 'carla', 'PAN': '', 'OP': 'ValidarUsuarioPago'}
18
19 POST (12/9 15:11:37): {'TLFN': '612345678', 'DNI': '99999999C', 'CORREO': '', 'PASS': '',
20 'DATE': 'Dec%2F2020', 'NOMBRE': 'carla', 'PAN': '4777777777777777', 'OP': 'PagoCompletado'}
21

```

Figura 5.47: Ejemplo logst.txt.

5.4.5 Notificación mediante correo electrónico.

Dado que en la fase de creación de un usuario, se solicita al cliente la inserción de su correo electrónico, se ha creado en paralelo la cuenta de correo cspayproject@gmail.com, con el fin de informar y notificar a los usuarios de la aplicación *CSPay* de las diferentes situaciones de carácter especial que puedan acontecer. Actualmente, el servidor envía un e-mail con un mensaje de bienvenida al cliente que acaba de crear correctamente una nueva cuenta en el sistema, recordándole la contraseña de acceso a la aplicación (ver *Figura 5.48*).



Figura 5.48: Ejemplo de notificación de alta.

También se envía un correo electrónico al cliente con el resultado de cada intento de transacción financiera empleando este nuevo método de pago, sea cual sea el desenlace de la misma (aprobada, denegada, cancelada, timeout, etc.). En la *Figura 5.49* se observa un ejemplo de correo electrónico recibido ante una compra llevada a cabo con éxito.

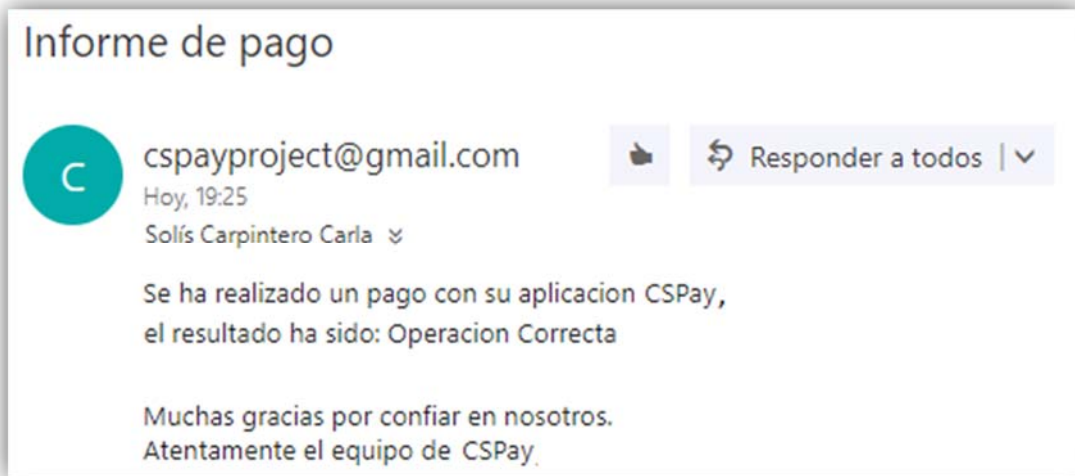


Figura 5.49: Ejemplo de notificación de pago.

5.5 PÁGINA WEB QUE EMULE EL COMPORTAMIENTO DE UN COMERCIO ELECTRÓNICO

Se lleva a cabo el diseño de una web básica de comercio electrónico que permita la simulación de un pago online. En el formulario de pago, no se solicitará la inserción de los datos sensibles del titular de la tarjeta (PAN, fecha de caducidad, CVV), tan solo será necesario el teléfono móvil del cliente.

Para el desarrollo de la página web del presente proyecto, se ha utilizado bootstrap [58]. La herramienta dispone de un conjunto de elementos web personalizables, incluidos en una sola plataforma de código abierto. Este servicio contiene plantillas de diseño con tipografía, formularios, botones, cuadros, menús de navegación y otros elementos de diseño basados en **HTML** y **CSS**, así como, extensiones de JavaScript adicionales.

Esta herramienta fue creada por Mark Otto y Jacob Thornton de Twitter para fomentar la consistencia en la implementación de su red social, ya que debido a los múltiples desarrolladores que trabajaban en paralelo para mejorar y mantener la página, con frecuencia surgían inconsistencias e incompatibilidades. En Agosto de 2011, tras comprobar el asombroso potencial que inspiraba esta herramienta de forma globalizada, decidieron lanzarlo como proyecto de código libre (Open source) en GitHub, siendo en febrero de 2012 el proyecto de desarrollo público más popular. Desde entonces, Bootstrap ha servido para unificar entornos de trabajo en el mundo del desarrollo web, y con ello, la obtención de páginas con un código estructurado y sencillo para facilitar su posterior modificación y/o mantenimiento.

Se ha decidido utilizar esta plataforma para la implementación de la página web del comercio electrónico del prototipo, debido a la gran versatilidad y sencillez que presenta, además de ser compatible con la gran mayoría de navegadores y dispositivos. Además, presenta una ventaja decisiva respecto a otras opciones que han sido analizadas antes de emprender el desarrollo web (como por ejemplo, Prestashop o Joomla), que es la inexistencia de código y archivos fuente a modo de residuos, inutilizados, desconocidos o sobrantes, en los directorios donde reside la lógica de la aplicación web.

El diseño final de la página web en desarrollo, consta de una barra de tareas constituida por tres pestañas (Catálogo, Pagar y Acerca del TFM) y un botón para vaciar los artículos añadidos a la cesta virtual de la compra (Ver *Figura 5.50*).



Figura 5.50: Barra de tareas de la web.

La primera pestaña, correspondiente al *Catálogo de productos* (ver *Figura 5.51*), muestra una sucesión de diferentes artículos disponibles con distintos importes para su compra, donde el usuario puede seleccionar los que sean de su interés para efectuar la compra. A medida que un artículo es añadido a la cesta de la compra, se suman los importes asociados a los productos, con el fin de disponer del valor total en el módulo de pago.



Figura 5.51: Catálogo de la web.

En la segunda pestaña tiene lugar el método de pago, dónde se brinda al usuario la oportunidad de seleccionar aquel medio que más se ajuste a sus necesidades para el abono del importe de los productos previamente añadidos a la cesta de la compra en la pestaña anterior. Cabe destacar que en la implementación de la demo, únicamente está programada la funcionalidad del pago mediante la inserción del teléfono móvil, ya que es la iniciativa de interés del proyecto. La lógica funcional viene detallada en *Apartado 5.4.1*. Las opciones de pago mediante la inserción del número de la tarjeta, así como a través de la cuenta de PayPal, solo incluyen la parte de diseño gráfico, sin desencadenar ningún evento o acción el hecho de que el usuario pulse en botón “Pagar”. En la *Figura 5.52* se pueden observar todas las opciones disponibles desplegadas para su revisión.

Figura 5.52: Posibles métodos de pago implementados en la web.

Por último, para mejorar el diseño y mostrar el potencial de bootstrap, se ha implementado un carrusel de tres imágenes en la parte superior de la web, las cuales van sucediendo de forma automática transcurrido un tiempo determinado. Ver *Figura 5.53*.

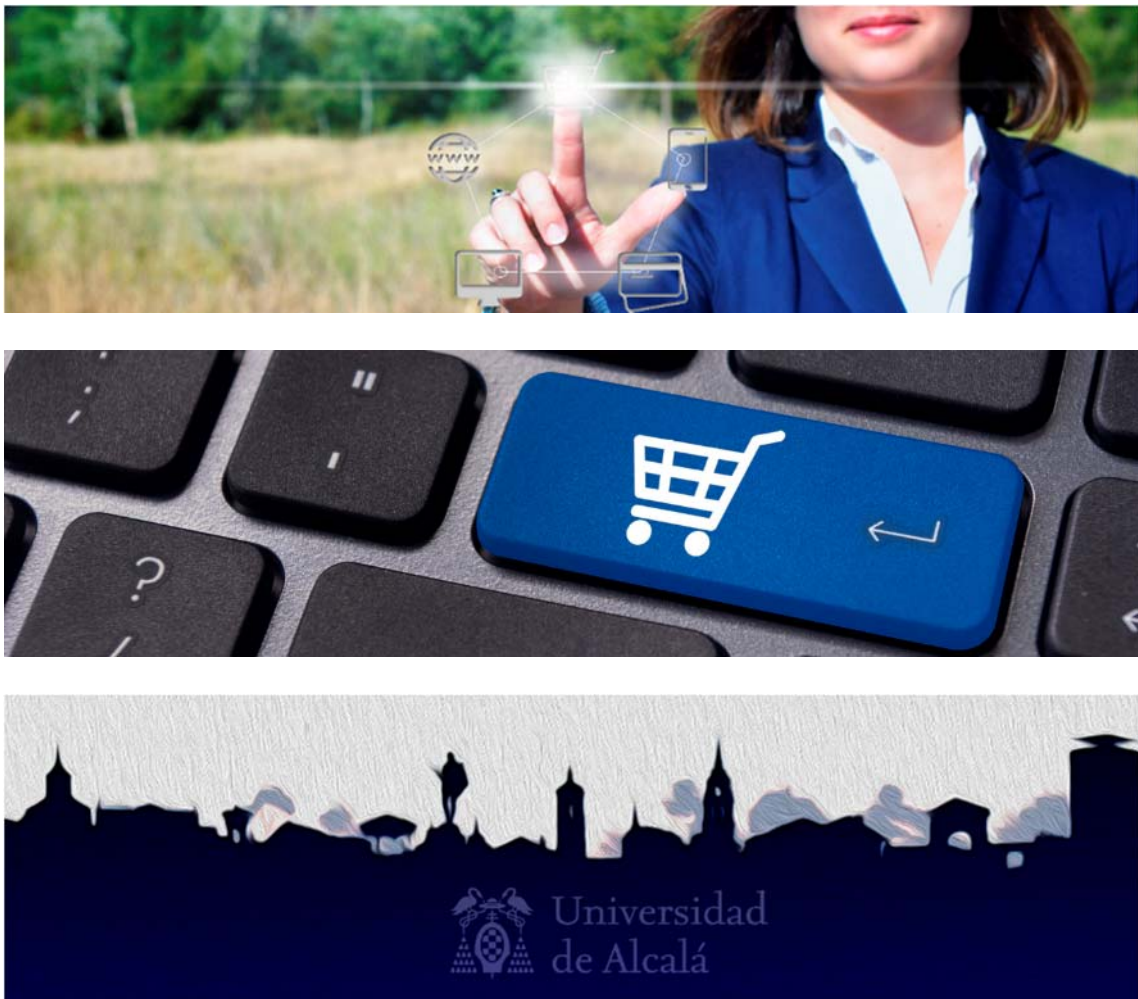


Figura 5.53: Banner secuencial de la web diseñada.

5.5.1 Protocolo de comunicación HTTP

Para la transferencia de información entre ciertos elementos interesados que constituyen el sistema, se utiliza el protocolo de comunicación Hypertext Transfer Protocol (HTTP) que habilita las transmisiones en Word Wide Web. HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores y proxies) para comunicarse [59]. Gracias a esta utilidad, es factible establecer las comunicaciones pertinentes entre la página web del comercio electrónico y el servidor de pago, así como aquellas conexiones iniciadas en el dispositivo móvil que también van dirigidas al mismo servidor en cuestión.

En dicho protocolo existe una serie predefinida de métodos de petición para su utilización y además presenta la flexibilidad de poder ir adoptando nuevos recursos para añadir nuevas funcionalidades compatibles con las anteriores. Cada método indica la acción que se desea desencadenar sobre un componente del destinatario identificado. Para satisfacer las necesidades de la demo, se ha hecho uso del mensaje de solicitud POST.

Por definición, el método POST (RFC 2616) realiza una petición a un servidor web con el fin de que éste procese y acepte los datos incluidos en el cuerpo del mensaje (se suele utilizar para el envío de formularios) [60]. Los POST llevados a cabo desde la página web del comercio y desde la aplicación móvil, utilizan la URL del servidor de pago web (obtenida a partir del servicio dinámico de DNS, No-IP) para establecer la comunicación.

Para desencadenar un POST desde la página web del comercio electrónico implementada, es necesario añadir previamente algún artículo del catálogo a la cesta, y seleccionar el método de pago correspondiente a la inserción del número de teléfono del titular de la tarjeta. Una vez que se inserta el número de teléfono, siempre y cuando éste sea de nueve cifras, y se pulsa el botón PAGAR, se envía un POST con la información necesaria para que el servidor identifique correctamente el tipo de transacción, y se pueda proceder al pago, tal y como se muestra en la *Figura 5.54*:

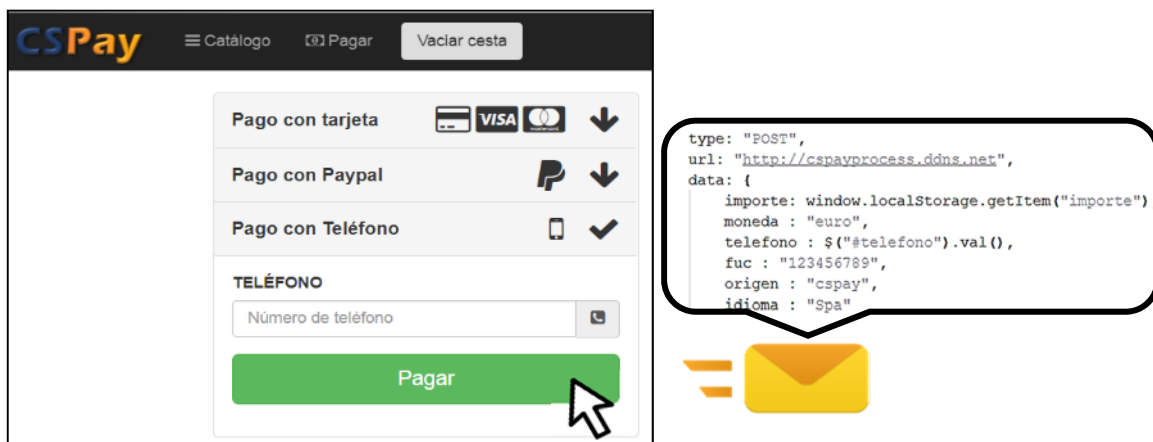


Figura 5.54: Método de pago del prototipo.

Los posible Status Code de HTTP que envía el servidor de pago como respuesta al procesamiento de la solicitud POST, han sido definidos y utilizados para notificar las diferentes acciones que han acontecido en el transcurso de la emulación de la operación financiera [61]. A continuación, se analizan los posibles valores que contempla el piloto para la identificación de los diferentes escenarios de las pruebas. (*Figuras 5.55 – 5.61*)

- **Status Code = 200:** Transacción aprobada



Figura 5.55: Notificación de la web tras aprobar una transacción.

- **Status code = 401:** Transacción denegada porque la tarjeta que el usuario ha aproximado en el dispositivo móvil no ha sido previamente dada de alta en el servicio y, por lo tanto, no aparece en la base de datos del servidor como que pertenezca a la lista de PAN autorizados.



Figura 5.56: Notificación de la web al intentar realizar un pago con una tarjeta no dada de alta.

- **Status code = 406:** Transacción denegada porque el usuario ha cancelado la operación en el dispositivo móvil, en la fase previa a la lectura de la tarjeta contactless.



Figura 5.57: Notificación de la web al cancelar manualmente el pago desde el smartphone.

- **Status code = 408:** Transacción denegada porque el usuario ha dejado vencer el tiempo máximo que proporciona el servicio para la finalización del pago, sin haber realizado ninguna acción en el dispositivo móvil.



Figura 5.58: Notificación de la web al no realizar ninguna acción desde el smartphone.

- **Status code = 416:** Transacción denegada porque el usuario ha utilizado una tarjeta cuya fecha de caducidad ha expirado.



Figura 5.59: Notificación de la web al intentar realizar un pago con una tarjeta caducada.

- **Status code = 423:** Transacción denegada porque el servidor de pago tiene indicios de que la tarjeta contactless, que ha sido aproximada al dispositivo móvil para efectuar el pago, puede estar sujeta a fraude.



Figura 5.60: Notificación de la web al intentar realizar un pago con una tarjeta que está en una blacklist.

- **Status code = 425:** Transacción cancelada, debido a que el número de nueve dígitos insertado no corresponde con ningún cliente del servicio CSPay.



Figura 5.61: Notificación de la web al introducir un número no dado de alta en la aplicación.

Capítulo 6

Implementación del demostrador CSPay.

6.1 FUNCIONAMIENTO DEL SISTEMA.

Una vez estudiados de forma independiente los cuatro módulos tecnológicos que constituyen la propuesta definida, se lleva a cabo la integración total del sistema *CSPay*. La propuesta tiene como objeto la definición de un nuevo método de pago para la reducción de fraude y la mejora de la experiencia de usuario, de tal forma que la implementación del demostrador satisface la necesidad de analizar y valorar estos dos cometidos:

- **Evaluación de la viabilidad técnica de la solución:** Para la reducción de fraude se ha definido de forma teórica la incorporación de la tarjeta presente en el flujo transaccional de una solución de comercio electrónico. Al añadir la tarjeta inteligente contactless en un nuevo contexto, se necesitaba disponer de otro dispositivo adicional para la lectura de los datos del chip, como es el teléfono móvil del cliente. La incorporación de ambos elementos en la operativa de pago e-commerce implica la definición de nuevas casuísticas y flujos de trabajo. Para ello, en el *Apartado 6.2* se detalla el comportamiento completo esperado de la solución, definiendo los distintos escenarios con las diversas posibilidades de operatividad que se pueden ofrecer, tanto en la descripción teórica como en la adaptación funcional para la puesta en marcha del piloto. La finalidad es establecer los diagramas de conexión entre los distintos bloques del sistema, con el fin de relacionar el comportamiento individual de cada uno de ellos dentro del marco común de la solución de pago (ver *Figura 6.1*), verificando que efectivamente existe viabilidad en la solución tecnológica propuesta.

- **Medición de la experiencia de usuario:** Se define experiencia de usuario (UX, User eXperience) al conjunto de factores y elementos relativos a la interacción del usuario con un entorno o dispositivo concreto, cuyo resultado es el grado de satisfacción y la percepción positiva o negativa de dicho servicio, producto o dispositivo. Para obtener una referencia de las sensaciones que experimentan los usuarios ante este nuevo método de pago, se distribuye un video explicativo con el funcionamiento del demostrador y se facilita una encuesta a cien personas para abstraer los resultados pertinentes, recogidos en el *Apartado 6.3*.



Figura 6.1: Diagrama de bloques del sistema.

6.2 INTEGRACIÓN Y SECUENCIALIZACIÓN.

Se definen las diferentes casuísticas que se han tenido en cuenta para el diseño e implementación de la solución *CSPay*, secuencializando las actividades pertinentes dentro de los flujos funcionales con el fin de transmitir una visión de sincronismo y operatividad del sistema. En los esquemas correspondientes al demostrador se ha utilizado la misma nomenclatura que en el *Capítulo 5* para la mención de las diferentes actividades de la aplicación móvil, así como de los registros del servidor y los Status Code de la página web del comercio electrónico, con el fin de disponer de una visión completa de cada proceso.

6.2.1 Proceso de registro de usuario nuevo.

Un nuevo usuario se descarga la aplicación de pago *CSPay*, y tras la instalación de la misma, debe registrarse en el servicio a través de la APP si desea disfrutar de las prestaciones que el nuevo método de pago ofrece en escenarios de comercio electrónico.

- **Flujo teórico del proceso.**

Se define el diagrama de flujo que tendría lugar en la fase de creación de usuario por parte del propietario del dispositivo móvil Android. Una vez que el cliente introduce los datos requeridos para una nueva alta en el sistema, se manda de forma automática una petición desde el dispositivo móvil a los servidores GCM. El objetivo es que el dispositivo móvil del cliente sea suscrito al servicio de la aplicación, y Google establezca una vinculación entre el número de teléfono y un token localizador, que permita identificar el dispositivo (a través del número de teléfono) en las futuras comunicaciones push originadas en el centro procesador. De forma prácticamente simultánea, el dispositivo móvil envía la información del cliente necesaria para la solicitud de una alta nueva al centro procesador. Dicho procesador almacena los datos recibidos en un directorio seguro destinado a tal fin, y responde a la aplicación del dispositivo móvil (haciendo uso de los servidores de Google), indicando si el usuario ha sido o no creado. La *Figura 6.2* muestra el diagrama de flujo del proceso y la participación de cada uno de los stakeholders en él.

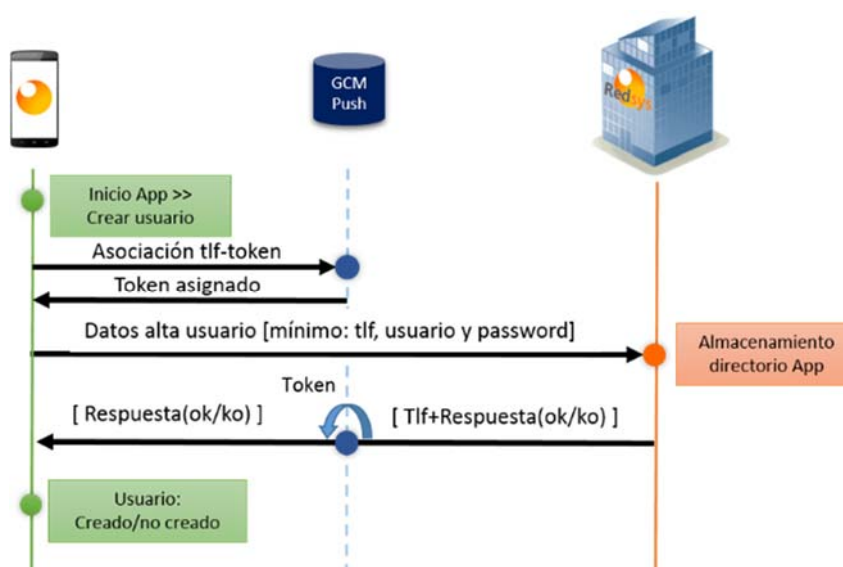


Figura 6.2: Flujo teórico del proceso de registro de usuario nuevo.

- **Flujo del proceso en el demostrador.**

Se implementa en la práctica un escenario similar al teórico, dónde el usuario navega por las opciones de la aplicación móvil detalladas en la *Figura 6.3*, hasta la fase de creación de un nuevo usuario. A continuación se envía de forma automática una solicitud de vinculación de token a los servidores de Google y un POST al servidor de la aplicación de pago, con la información que se define en la misma figura. El servidor de AWS almacena los datos en el fichero *user.txt* y responde a la aplicación del dispositivo móvil a través del servicio GCM con el resultado del proceso. Si el usuario ha sido creado con éxito, se envía además un correo electrónico de bienvenida al titular de la cuenta, recordándole la contraseña que ha elegido para la utilización de este servicio.

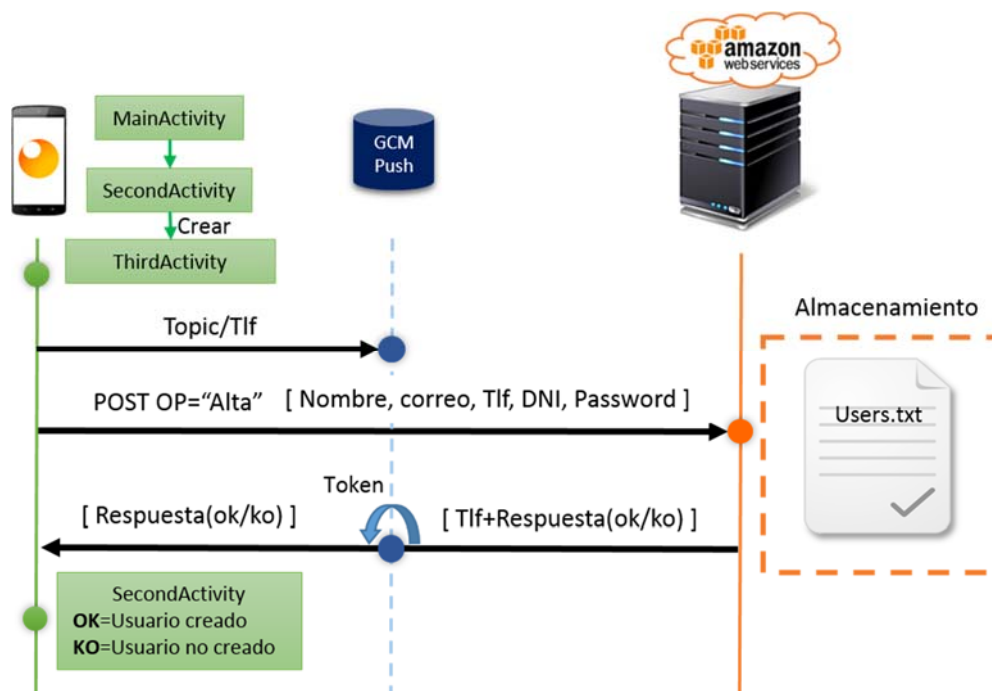


Figura 6.3: Flujo del proceso en el demostrador para registro de usuario nuevo.

6.2.2 Proceso de inicio de sesión.

- **Flujo teórico del proceso.**

Una vez que el usuario ha sido creado, el inicio de sesión consiste en la inserción del DNI y de la password (establecida previamente por el cliente) en la aplicación móvil. El centro procesador valida la contraseña mediante la comparación del campo recibido y los datos almacenados en su directorio. Si la clave introducida por el cliente es correcta, se permite al usuario acceso a los servicios de la aplicación. Si por el contrario, es incorrecta, se deniega la petición y no se permite al usuario ingresar en la aplicación. Se representa el diagrama funcional en la *Figura 6.4*.

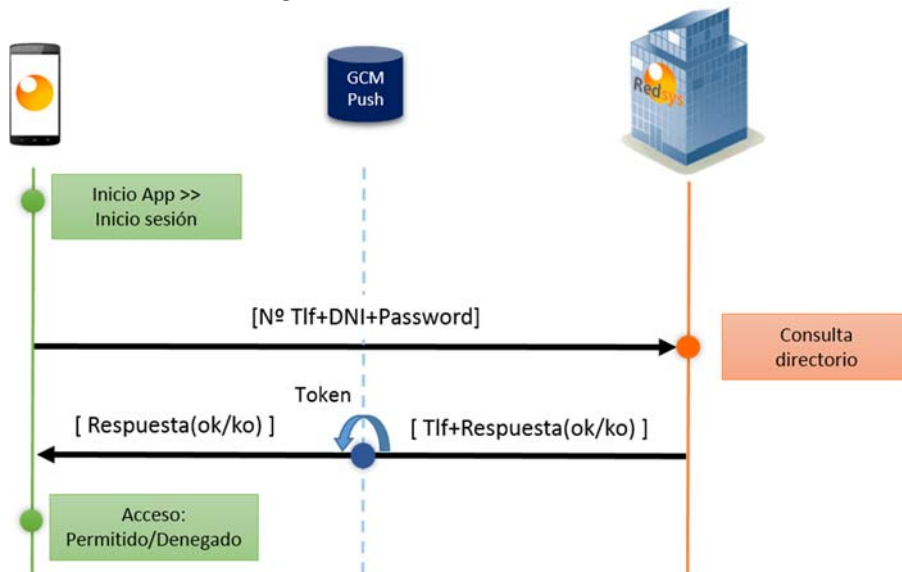


Figura 6.4: Flujo teórico del proceso de inicio de sesión

- **Flujo del proceso en el demostrador.**

En la práctica se ha mantenido fiel el fundamento de la idea teórica, detallando las pantallas de la aplicación móvil, los campos que viajan en las comunicaciones y el nombre del directorio de consulta del servidor en la *Figura 6.5*.

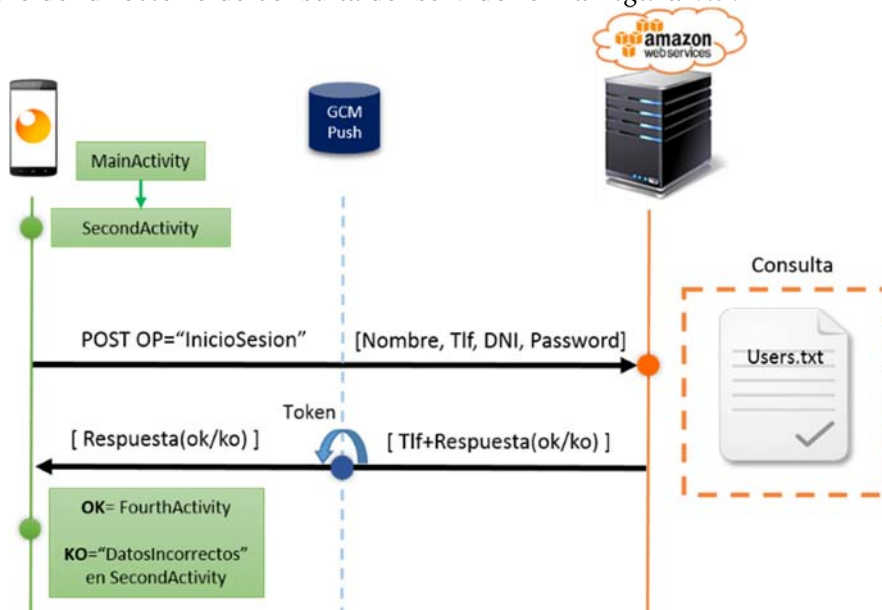


Figura 6.5: Flujo del proceso en el demostrador para inicio de sesión.

6.2.3 Registro de nueva tarjeta en el servicio.

- **Flujo teórico del proceso.**

El usuario desde la aplicación del móvil puede asociar o vincular diversas tarjetas de diferentes bancos a este servicio, con el fin de que en la operativa de comercio electrónico pueda completar con éxito el pago mediante el uso de las mismas. Esta opción está disponible en las opciones de menú, y tras la selección de nueva tarjeta, el usuario debe aproximar su tarjeta contactless al lector NFC del dispositivo móvil. De forma automática se envía una solicitud de tarjeta nueva al centro procesador, que tras un primer procesamiento interno, redirecciona la petición a la entidad emisora de la tarjeta. El banco comprueba la veracidad de los datos (la tarjeta aproximada pertenece a uno de sus clientes y está operativa) y puede autenticar al usuario para corroborar que efectivamente desea utilizar este servicio. Cada entidad financiera puede llevar a cabo la metodología de autenticación que prefiera según la política de empresa como, por ejemplo, llamar directamente al titular o bien delegar esta responsabilidad al centro procesador. Se propone que la entidad financiera tras la validación del estado de la tarjeta, remita al centro procesador el número de teléfono móvil del titular de la cuenta corriente. Dicho procesador envía un SMS con un código de validación de tarjeta al número de teléfono indicado por el banco, que puede coincidir o no con el número del dispositivo móvil desde el cual el usuario desea utilizar la aplicación. El cliente inserta la contraseña recibida en la aplicación, y el centro procesador valida el código de seguridad, actualizando el directorio de tarjetas dadas de alta en el servicio si el proceso ha finalizado con éxito. Ver *Figura 6.6*.

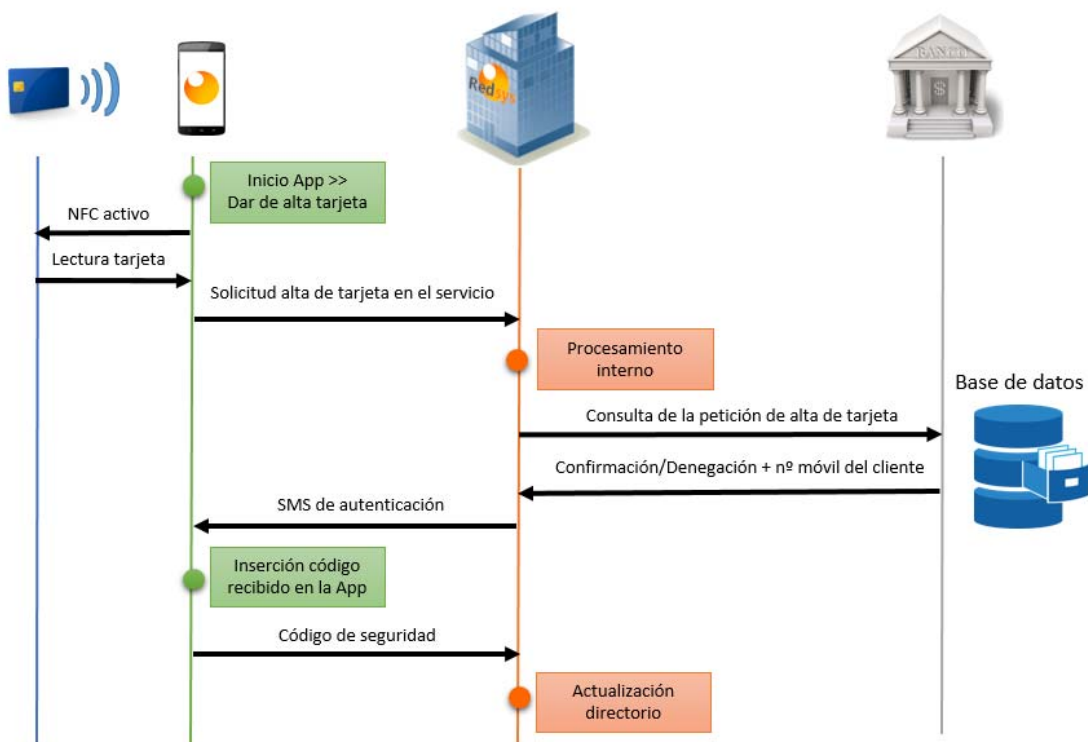


Figura 6.6: Flujo teórico del proceso para dar de alta una tarjeta.

- **Flujo del proceso en el demostrador.**

Para llevar a cabo la prueba de concepto con el demostrador, se ha emulado que el administrador de la base de datos alojada en el servidor pueda ejercer las funciones de la entidad financiera emisora de cada una de las tarjetas. De esta forma, ante la solicitud de una nueva tarjeta en el servicio, se actualiza automáticamente la base de datos *PAN_Pending.txt* del servidor y se puede gestionar manualmente si se desea que pertenezca al listado de números de tarjetas autorizados (*PAN_Authorized.txt*) o si por el contrario no se quiere incluir en el servicio (emulando que, por ejemplo, la tarjeta no dispone de fondos). Ver *Figura 6.7*.

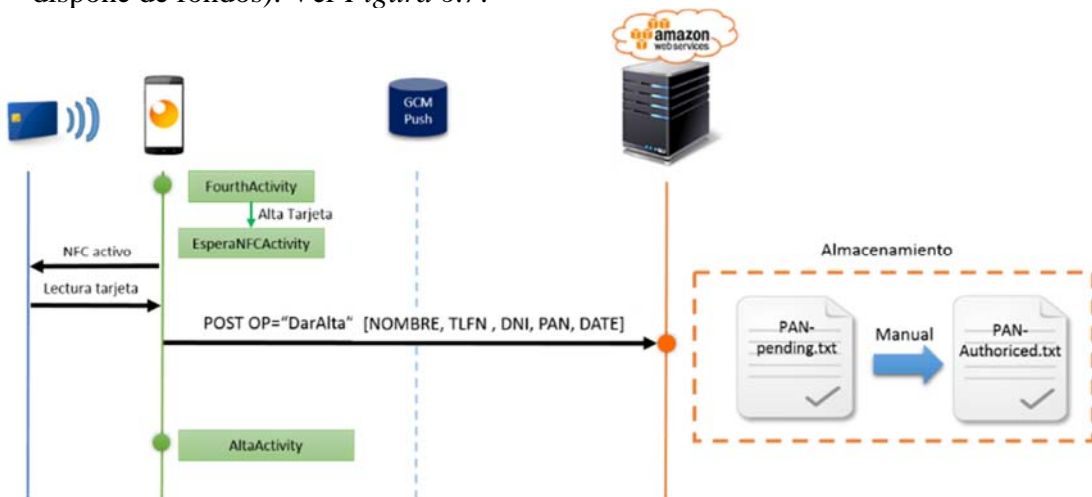


Figura 6.7: Flujo del proceso en el demostrador para dar de alta de tarjeta.

6.2.4 Operativa de solicitud de baja de una tarjeta en el servicio.

- **Flujo teórico del proceso.**

Se define en los requerimientos teóricos la posibilidad de dar de baja una tarjeta en el servicio desde las opciones de menú de la aplicación móvil. Esta posibilidad está destinada a aquellos usuarios que decidan dar de baja una tarjeta tras una vinculación previa temporal. El centro procesador ante la recepción de esta solicitud, elimina todo registro de tarjeta de su base de datos (ver *Figura 6.8*). Para los casos de extravío o robo de la misma, se habilitan otros canales de notificación de baja, como es la propia comunicación por parte del titular a su entidad financiera, que denegará todas las transacciones efectuadas con dicha tarjeta de forma análoga a la operativa presencial.

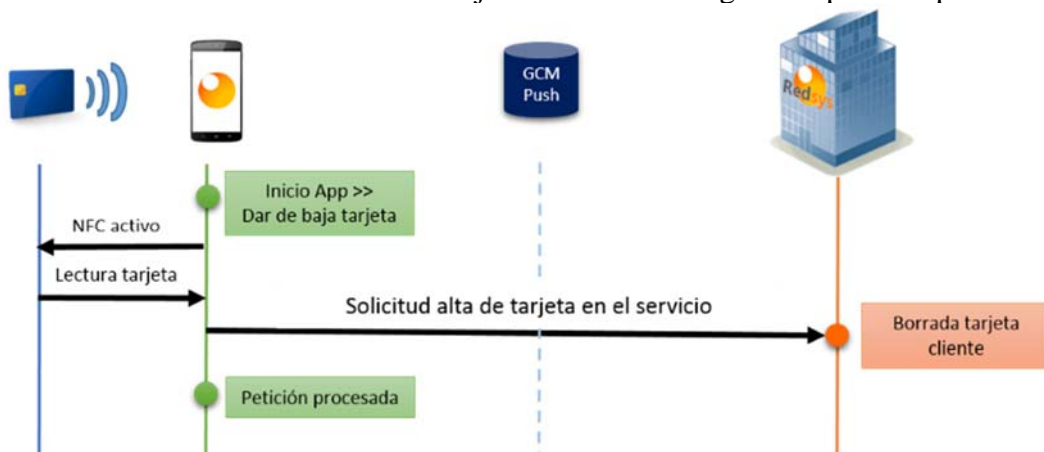


Figura 6.8: Flujo teórico del proceso para dar de baja una tarjeta.

- **Flujo del proceso en el demostrador.**

El flujo de trabajo que se ha implementado para esta operativa sobre el emulador es similar a la descripción teórica. En la *Figura 6.9* se pueden observar las diferentes actividades que intervienen en la aplicación del dispositivo móvil y los registros del servidor sujetos a modificaciones, ya que ante una solicitud de baja de tarjeta, se elimina toda referencia a la misma de los ficheros *PAN_Authoriced.txt* y *PAN_Pending.txt*.

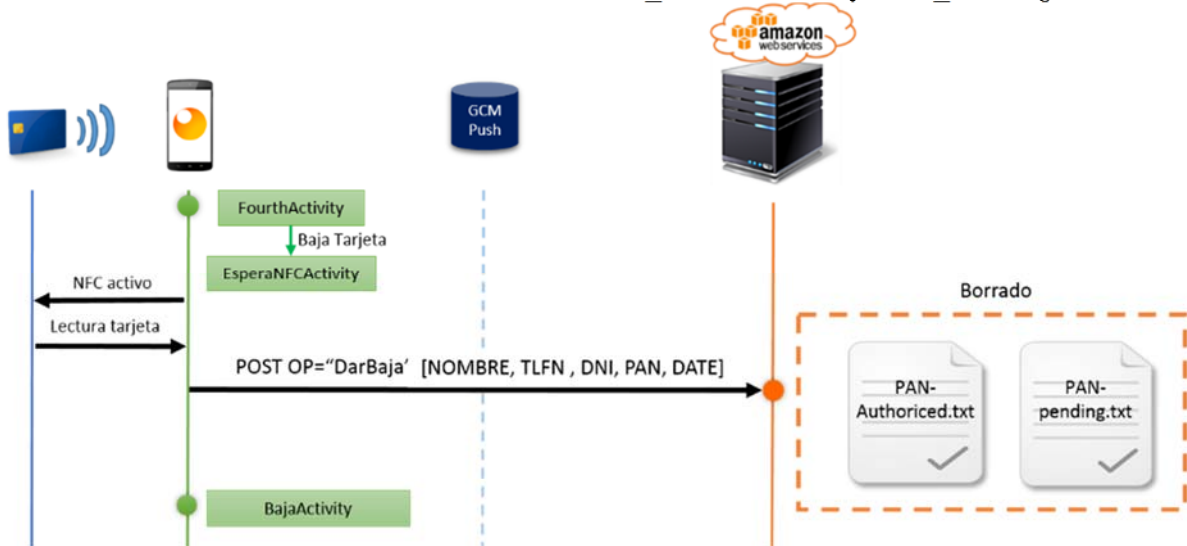


Figura 6.9: Flujo del proceso en el demostrador para dar de baja una tarjeta.

6.2.5 Verificación de disponibilidad de la tarjeta en el servicio.

- **Flujo teórico del proceso.**

Desde las opciones de menú de la aplicación móvil se permite al usuario consultar si la tarjeta con la que desea llevar a cabo operaciones de comercio electrónico, empleando el método *CSPay*, está dada de alta y disponible en el sistema. Para ello, el usuario aproxima la tarjeta deseada al lector NFC del dispositivo móvil, que envía automáticamente la petición. El centro procesador consulta su base de datos y responde al usuario con la información solicitada (ver *Figura 6.10*). La indicación de que la tarjeta está registrada es meramente informativa, por lo que no garantiza ni implica de ningún modo que la transacción financiera llevada a cabo mediante comercio electrónico tenga que ser aprobada.

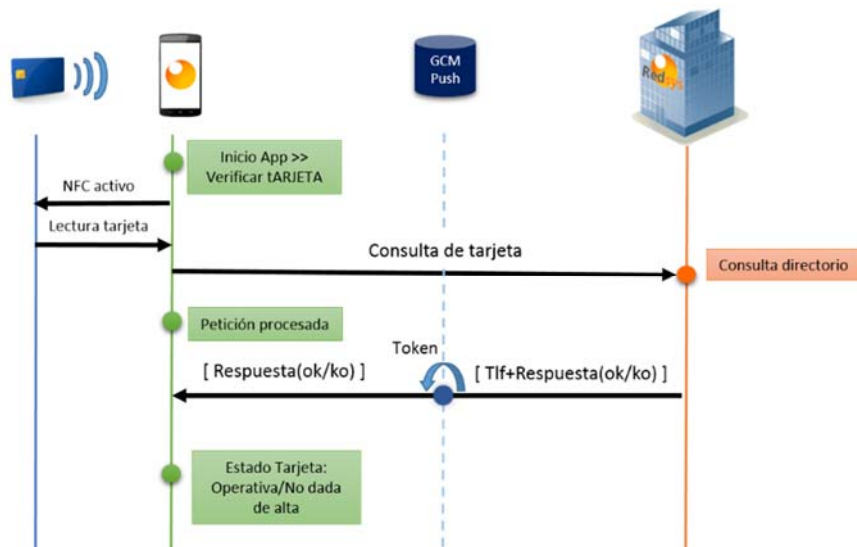


Figura 6.10: Flujo teórico del proceso para verificar una tarjeta.

- **Flujo del proceso en el demostrador.**

Para el caso concreto de la implementación del demostrador, el servidor realiza la consulta en el archivo de *PAN_Authorized.txt* para determinar si la tarjeta está dada de alta correctamente en el servicio. En esta fase no se tiene en cuenta si la tarjeta está caducada o si existe indicio de fraude, únicamente se corrobora que aparece en la base de datos previamente indicada y se proporciona esta información al titular de la misma.

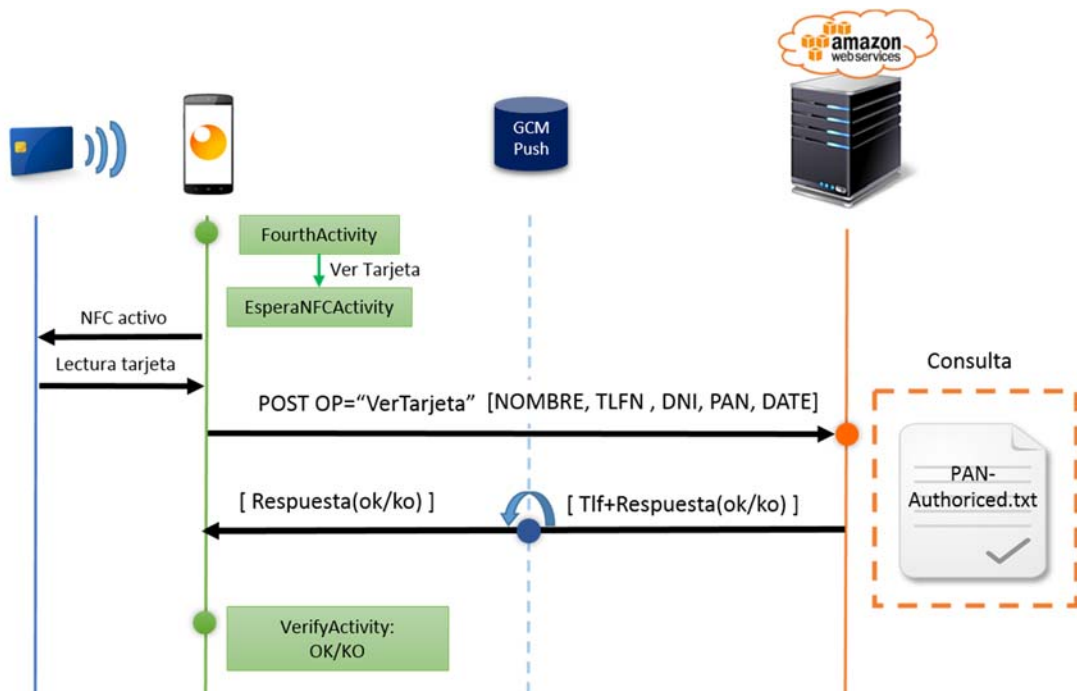


Figura 6.11: Flujo del proceso en el demostrador para verificar una tarjeta.

6.2.6 Borrar cuenta de usuario

- **Flujo teórico del proceso.**

Desde el menú de la aplicación móvil se posibilita que el usuario tenga la opción de eliminar su cuenta y todos los datos vinculados a la misma. Una vez completada con éxito la operativa representada en la *Figura 6.12*, el cliente queda totalmente desvinculado de este servicio.

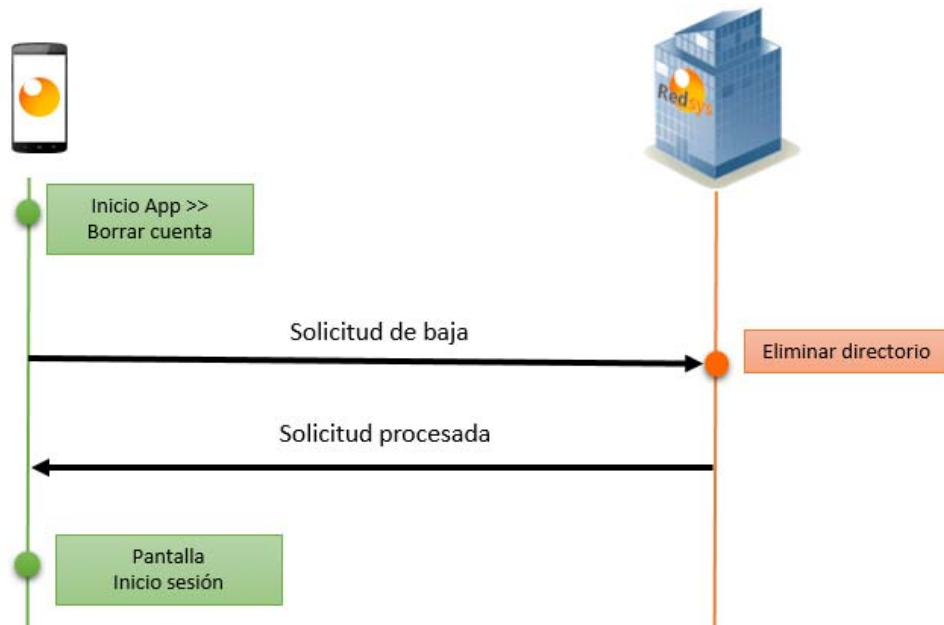


Figura 6.12: Flujo teórico del proceso para borrar cuenta de usuario.

- **Flujo del proceso en el demostrador.**

Para la eliminación de una cuenta de usuario, el servidor del demostrador borra automáticamente toda entrada vinculada al número de teléfono del cliente de los archivos *User.txt*, *PAN_Authorized.txt*, y *PAN_Pending.txt* (ver *Figura 6.13*). La base de datos *PAN_Blacklist.txt* solo puede ser gestionada manualmente por el administrador del servidor, y únicamente se actualizará una entrada de dicho registro si se desea emular una nueva instrucción por parte de la entidad financiera.

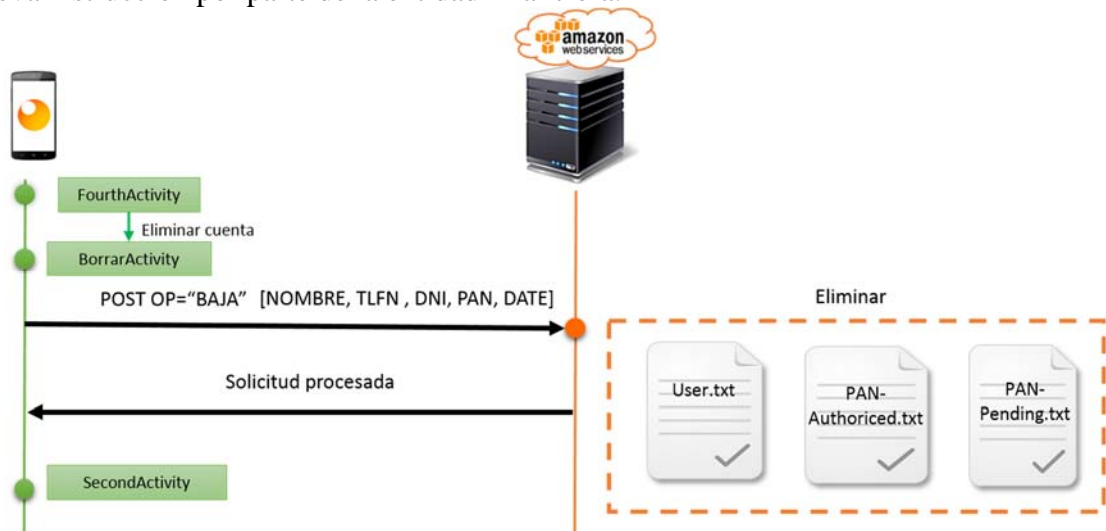


Figura 6.13: Flujo del proceso en el demostrador para borrar cuenta de usuario.

6.2.7 Operativa de pago: Transacción Aprobada o Denegada.

- **Flujo teórico del proceso.**

El usuario inicia una compra mediante comercio electrónico con el nuevo método de pago planteado, de tal forma que inserta su número de teléfono móvil en el formulario habilitado para tal fin. El centro procesador recibe la petición de pago y lleva a cabo una primera validación (autentica el sitio web del comercio electrónico y comprueba que el número de teléfono insertado por el usuario corresponde a un cliente del servicio). De forma seguida envía un mensaje push a la aplicación móvil del cliente a través de los servidores de GCM. El usuario recibe la notificación en su dispositivo móvil y lleva a cabo el procedimiento para completar el pago (autenticación y aproximación de la tarjeta contactless). El centro procesador obtiene la información de la tarjeta y procesa el pago, redireccionando a la entidad financiera correspondiente la solicitud de autorización. La entidad aprueba o deniega la petición en función de las condiciones de la cuenta corriente del cliente, tal y cómo sería el escenario de comercio presencial o electrónico actual, notificando la resolución al centro procesador, que a su vez comunica la decisión al comercio y al usuario a través de la página web. El diagrama completo teórico y funcional se muestra en la *Figura 6.14*.

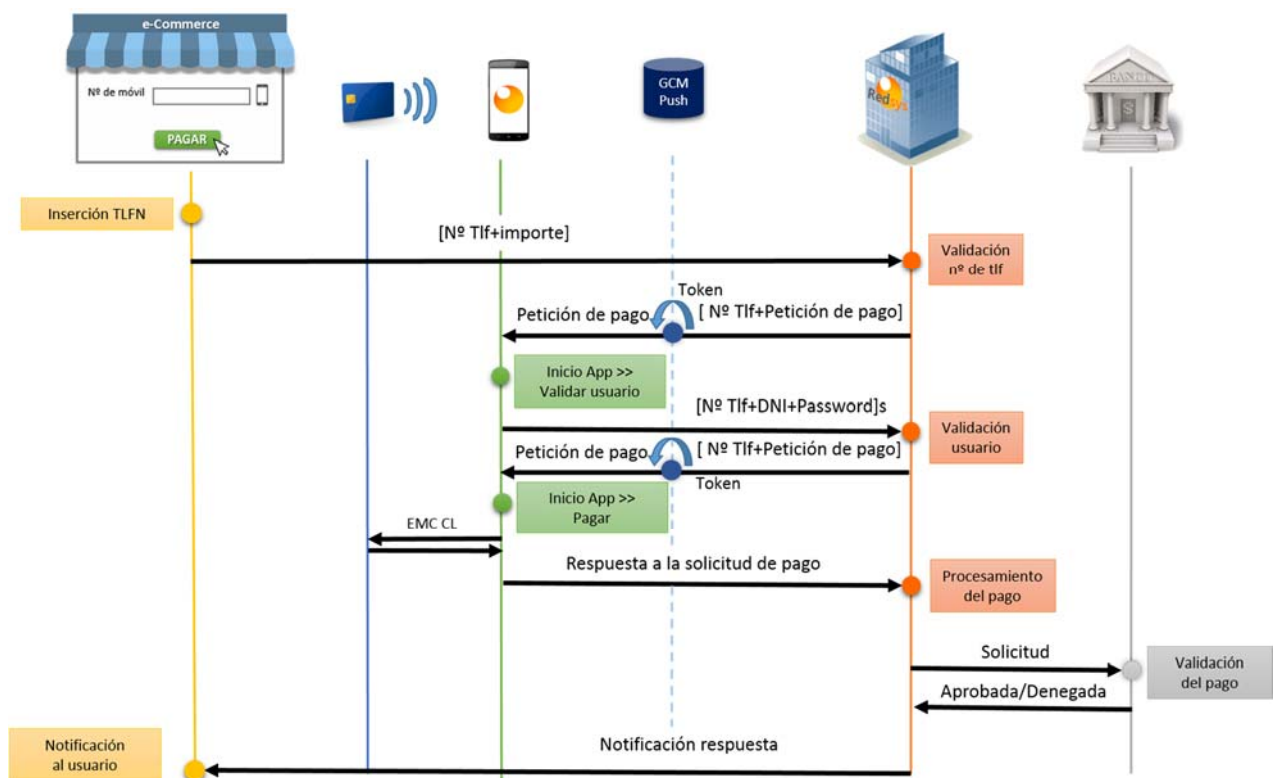


Figura 6.14: Operativa de pago teórica –Transacción aprobada/denegada.

- **Flujo del proceso en el demostrador.**

Para la implementación de este escenario en la solución piloto se ha seguido la filosofía teórica. En la *Figura 6.15* se observa el diagrama de trabajo y las distintas etapas, comunicaciones y registros que intervienen. Cabe destacar que, para que una transacción sea aprobada en el demostrador, la tarjeta utilizada para completar la operación debe estar dada de alta en la lista *PAN_Authorized.txt*, no aparecer en el registro *PAN_Blacklist.txt* y no disponer de una fecha de expiración vencida (tarjeta caducada), ya que estas comprobaciones han sido programadas en el servidor para la autorización o denegación de la petición de pago.

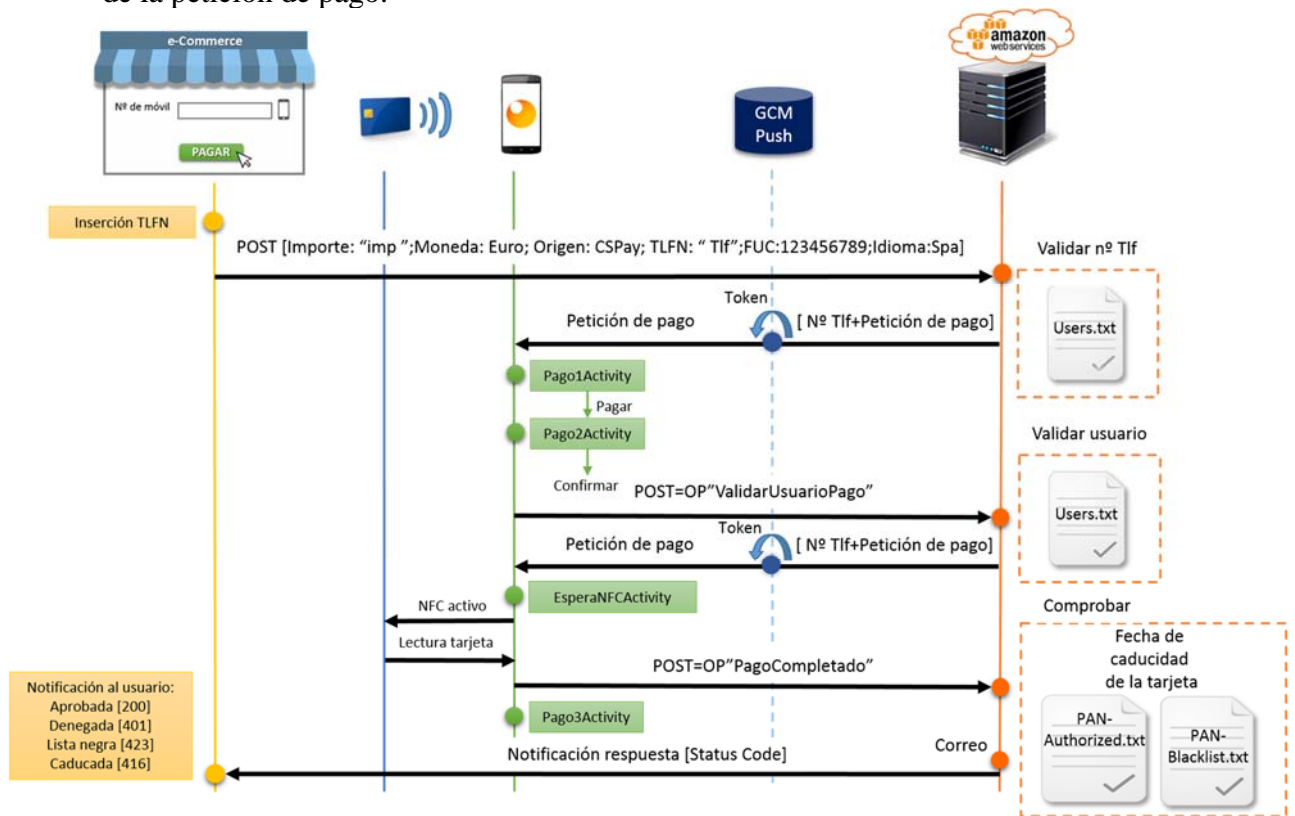


Figura 6.15: Operativa de pago de la demo– Transacción aprobada/denegada.

6.2.8 Operativa de pago: Transacción Cancelada por el usuario

- **Flujo teórico del proceso.**

Se define como requerimiento que el usuario tenga la oportunidad de cancelar la operación una vez que ha recibido la notificación de pago en su dispositivo móvil. Si este escenario acontece, la tarjeta física y la entidad emisora no intervienen en la comunicación. En la *Figura 6.16* se puede observar el diagrama de flujo del proceso.

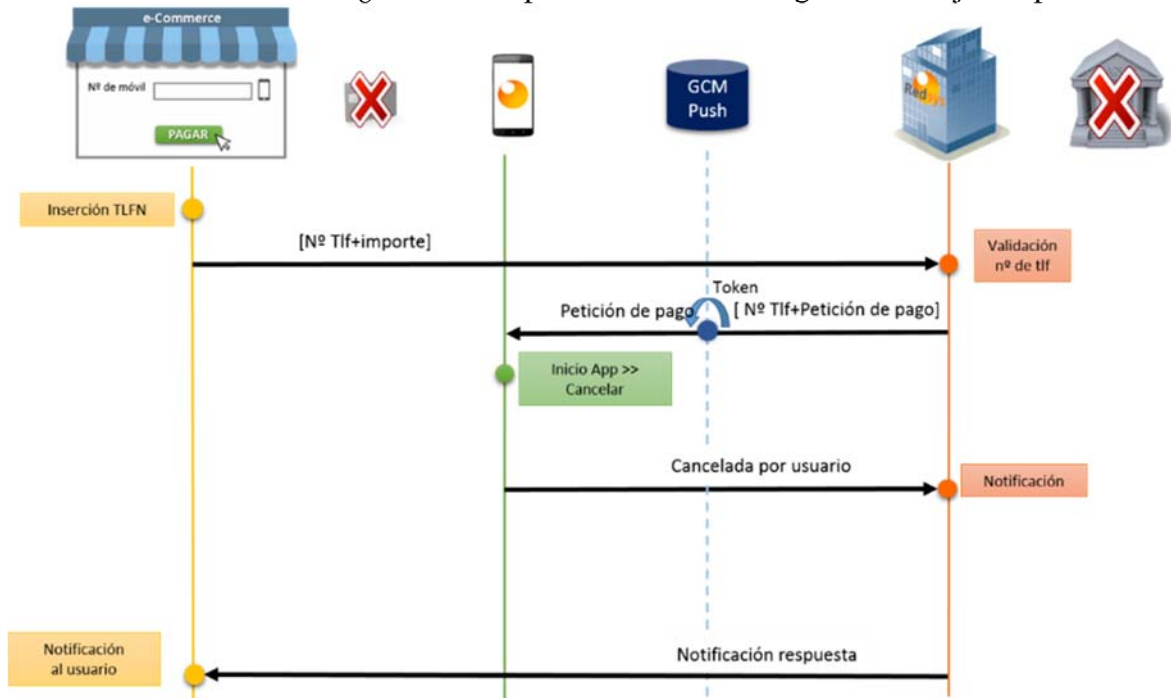


Figura 6.16: Operativa de pago teórica – Transacción cancelada.

- **Flujo del proceso en el demostrador.**

La cancelación de la transacción por parte del usuario se programa según la descripción teórica descrita en el epígrafe anterior. En la *Figura 6.17* se puede consultar el proceso completo que se lleva a cabo.

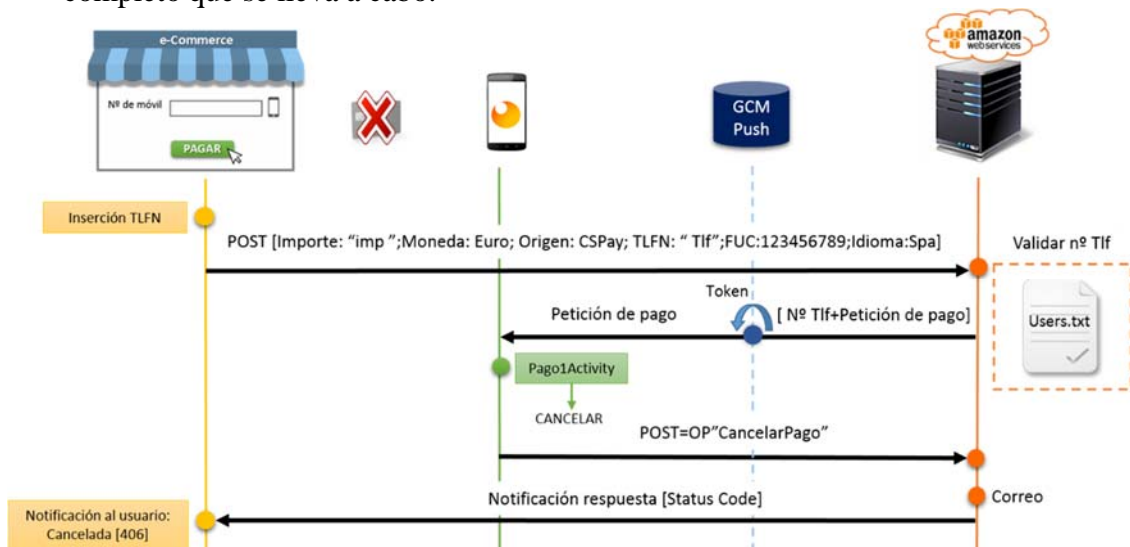


Figura 6.17: Operativa de pago de la demo – Transacción cancelada.

6.2.9 Operativa de pago: Timeout de usuario vencido.

- **Flujo teórico del proceso.**

Si tras la recepción de la notificación push el usuario no desencadena ninguna acción (no cancela ni continua el pago), transcurrido un tiempo vence el *timeout* que el servidor asigna al usuario para completar el proceso. Si esto ocurre, el centro procesador cancela la transacción en curso y notifica al comercio electrónico de esta circunstancia. En esta operativa no interviene la tarjeta física ni la entidad financiera. Ver *Figura 6.18*.

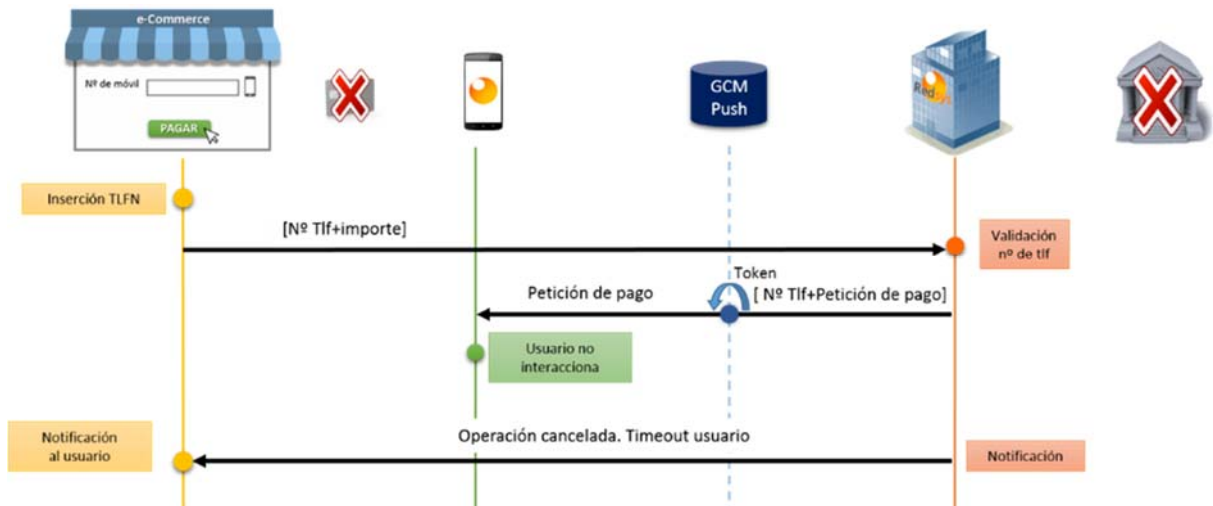


Figura 6.18: Operativa de pago teórica – Timeout usuario

- **Flujo del proceso en el demostrador.**

Acorde con la definición teórica descrita previamente, se representa la implementación en el demostrador del vencimiento del *timeout* que el servidor asigna al usuario en la *Figura 6.19*.

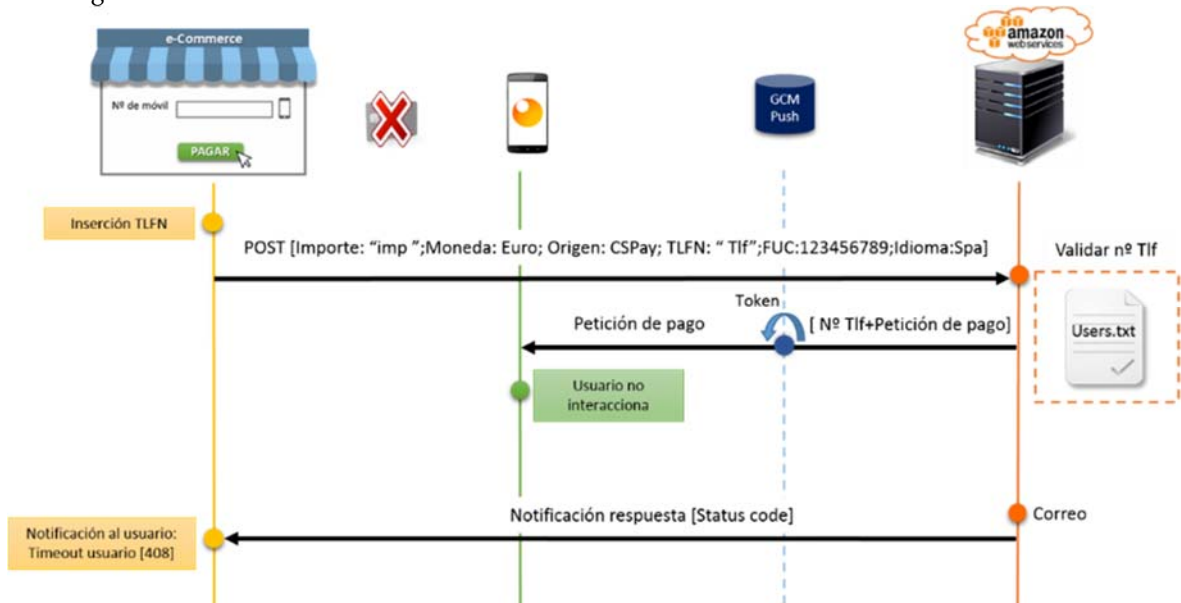


Figura 6.19: Operativa de pago de la demo – Timeout usuario

6.2.10 Operativa de pago: Número de teléfono no dado de alta en el servicio.

- **Flujo teórico del proceso.**

La página web del comercio electrónico comprueba que el número de teléfono que inserta el cliente presenta una estructura válida (9 caracteres numéricos), y de ser así, transmite la petición al siguiente elemento de la cadena. El centro procesador recibe la petición y valida el número de teléfono recibido. Si dicho número corresponde a un cliente del servicio *CSPay*, continua con el pago (*Apartado 6.2.7*). Si por el contrario, no encuentra coincidencias en su base de datos de la aplicación, aborta directamente la transacción en curso. Ver *Figura 6.20*.



Figura 6.20: Operativa de pago teórica – N° de tlf no dado de alta.

- **Flujo del proceso en el demostrador.**

Se programa la validación del número de teléfono en el servidor del demostrador, comprobando la existencia del número de teléfono recibido desde la página web del comercio electrónico en el registro *user.txt*. Ver *Figura 6.21*.



Figura 6.21: Operativa de pago de la demo – N° de tlf no dado de alta.

6.3 EVALUACIÓN DE LA EXPERIENCIA DE USUARIO

Se necesita estimar la experiencia de usuario de la nueva solución propuesta en el presente TFM porque el éxito y continuidad de la misma depende del grado de aceptación de los usuarios. No se puede considerar a los clientes como parte del negocio, si no que deben ser el centro del mismo, por lo que conseguir la confianza y enriquecer su experiencia han sido objetivos claro para el desarrollo técnico de la elaboración del TFM. Para evaluar la solución y extraer mediciones y estadísticas de la opinión que tienen los usuarios sobre *CSPay*, se ha elaborado una encuesta. La herramienta que se ha utilizado ha sido Google Forms [62] y el estudio se ha realizado entre los días 8 y 11 de septiembre de 2017.

Se define el *target* como el conjunto de personas a las que va específicamente dirigido un producto, y podrán ser los futuros usuarios de este servicio. En el caso de la propuesta *CSPay*, se considera el *target* a la parte de la población que desee realizar compras en comercio electrónico utilizando este nuevo método de pago y disponga de tarjeta contactless y móvil NFC para poder llevarlo a cabo.

El *universo* consiste en la población objeto del estudio y de la medición. En este caso, se ha considerado una muestra de 100 personas de diferentes edades residentes en España, que no tuvieran línea directa con el interesado y que fuesen ajenas al sector de los medios de pago, con el fin de que los resultados no estuviesen sujetos a condicionantes y fueran objetivos. En la *Figura 6.22* se representa que los encuestados pertenecen a salto uno y dos respecto del encuestado, con una relación 3:10 respectivamente.

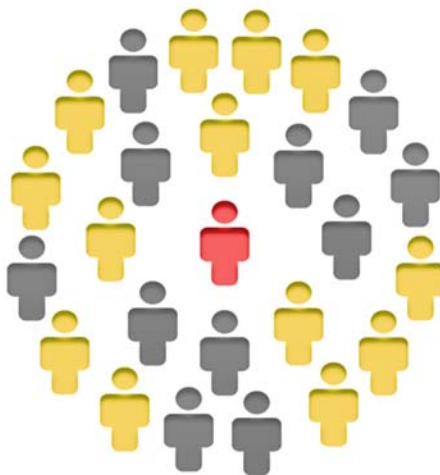


Figura 6.22: Metodología de captación de encuestados.

Las respuestas se utilizan con el fin de identificar las necesidades y mejorar la eficiencia de la propuesta, sin ánimo de conservar ningún dato propiamente personal o identificador de las personas que han respondido. Dado que la encuesta se ha difundido por un medio online, se conserva el correo electrónico de los encuestados, con la finalidad de controlar que las respuestas corresponden a personas físicas reales. Tras la defensa del TFM todos los formularios serán destruidos, cumpliendo con la ley del secreto estadístico y de protección de datos.

6.3.1 Presentación de los resultados

En este apartado se muestran las conclusiones generales obtenidas tras el análisis de los resultados de la encuesta. El formulario ha sido completado por 25 personas de cada uno de los cuatro rangos de edad definidos en la *Figura 6.23*, de tal forma que se han estudiado 100 respuestas. El interés de conseguir la opinión de personas de diferentes rangos de edad viene dada por la motivación de adquirir una visión más amplia de la sociedad.

Rango de edad

100 respuestas

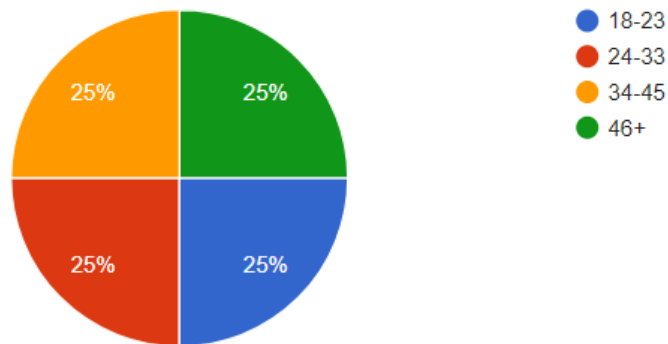


Figura 6.23: Porcentaje de encuestados en función del rango de edad.

Tras la identificación de la edad por parte del encuestado, se inicia una sucesión de cuatro preguntas cortas de carácter general para conocer el grado de conocimiento, preferencias e impresiones que tiene la muestra de la población respecto a los distintos medios de pago que conviven en el mercado. De esta forma, se puede entrever el grado de adaptación y aceptación por parte de los usuarios de los métodos de pago más recientes y analizar cuáles son los fuertes competidores en el sector.

El conocimiento de los usuarios respecto al mundo de los medios de pago viene recogido en la *Figura 6.24*. De los resultados obtenidos se refleja que el 91% de los encuestados conoce el pago mediante inserción de los datos de la tarjeta, seguido de cerca con el 82% de Paypal. Las tarjetas virtuales son las menos conocidas como cabía esperar.

¿Qué medios de pago conoces?

100 respuestas

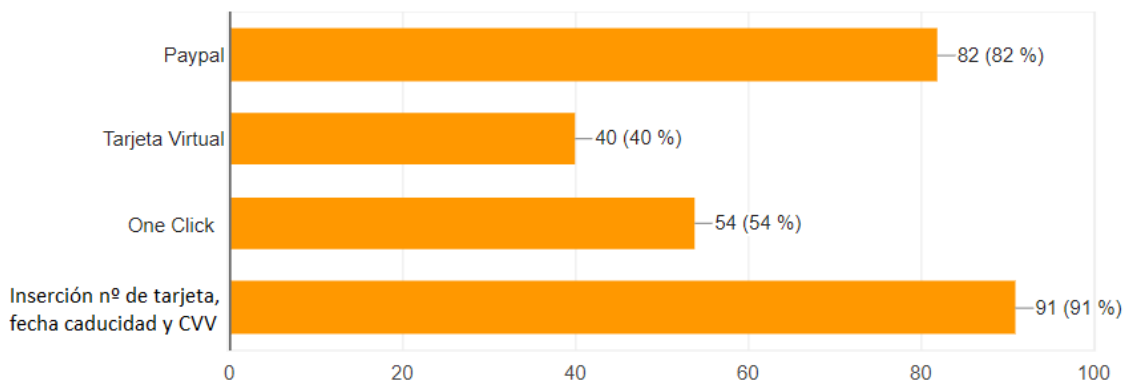


Figura 6.24: Resultados de la encuesta sobre métodos de pago conocidos por los encuestados.

En cuanto a la utilización de estos métodos a la hora de pagar en comercio electrónico se observa un claro dominante en el mercado, siendo la inserción de los datos de la tarjeta el método más utilizado, con el 35% de diferencia respecto de PayPal que es el segundo, tal y como se puede observar en la *Figura 6.25*.

¿Qué métodos de pago utilizas cuando compras por Internet?

100 respuestas

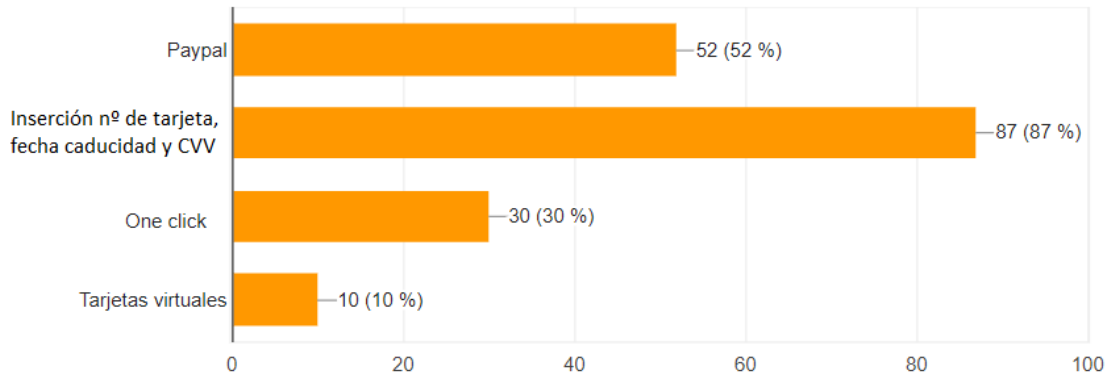


Figura 6.25: Resultados de la encuesta sobre métodos de pago utilizados en e-commerce.

A continuación se pregunta a los usuarios por la sensación de seguridad que inspira el método de pago que habitualmente utilizan. En la *Figura 6.26* se ve reflejado que solo un 38% de los encuestados considera que realizar compras online es realmente seguro. Por este motivo es tan importante el factor de la seguridad subjetiva. El método de pago propuesto no solo debe ser seguro, si no que se debe ganar la confianza de los usuarios y transmitir la impresión de tranquilidad.

¿Te parece seguro el pago actual mediante comercio electrónico?

100 respuestas

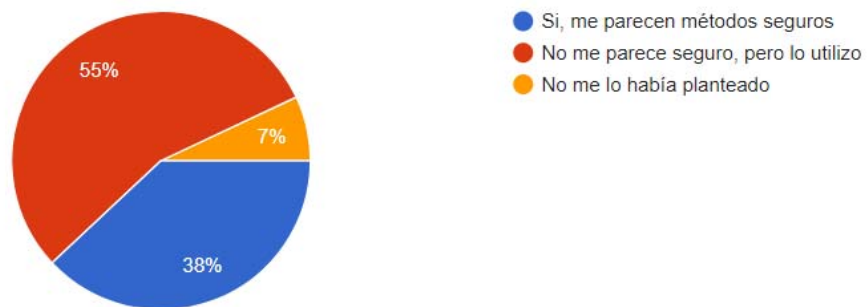


Figura 6.26: Resultados de la encuesta de la percepción subjetiva de seguridad de los encuestados al utilizar su medio de pago electrónico habitual.

Con el fin de conocer si la sensación de inseguridad es fundada o no, se pregunta a los encuestados de forma seguida si alguna vez han sufrido fraude. El 12% reconoce haber sufrido fraude en primera persona y un 56% indica que alguien de su entorno lo ha experimentado (ver *Figura 6.27*). Se tratan de cifras importantes y, por lo tanto, se refuerza la motivación de llevar la propuesta del presente TFM, tal y como se indicó en el *Capítulo 1*.

¿Has sufrido fraude online?

100 respuestas

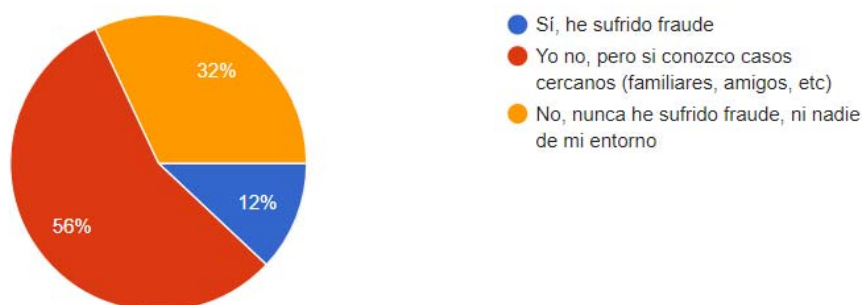


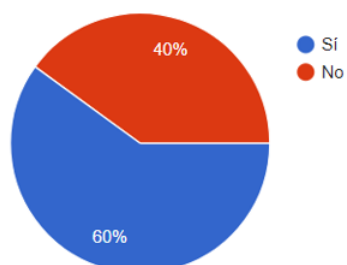
Figura 6.27: Resultados de la encuesta sobre fraude online en su experiencia.

Tras las cuatro preguntas introductorias en la materia de los medios de pago, se analizan los medios físicos que disponen los encuestados en cuanto a la posibilidad de utilizar la nueva solución de forma inmediata. Para este fin, es necesario que la población disponga de tarjeta contactless y smartphone Android con tecnología NFC. Se puede observar, en la *Figura 6.28*, que el 60% de los encuestados dispone de tarjetas inteligentes sin contactos. Esta cifra es menor que el resultado esperado, ya que este factor restringe la utilización del servicio en el marco actual. Sin embargo, esta circunstancia está en periodo de cambio, ya que Visa y MasterCard han acordado que en Europa será obligatoria la emisión de tarjetas con interfaz contactless a partir del año 2020. De esta forma, las tarjetas que únicamente soportan interfaz con contactos disponen de una fecha de caducidad próxima, y los bancos emitirán nuevos productos duales que reemplacen los anteriores.

En cuanto al sistema operativo Android con tecnología NFC, se concluye que el 67% de los encuestados dispone de un smartphone compatible con los requerimientos de la solución *CSPay*. En los últimos años, la mayoría de los dispositivos móviles salen al mercado con esta tecnología, independientemente de la gama. Además, parece que iOS también se introduce en el estándar NFC (ver *Capítulo 5*) por lo que se prevé que las cifras aumentarán de forma significativa en los próximos años.

¿Dispones de tarjeta contactless?

100 respuestas



¿Dispone tu móvil android de tecnología NFC?

100 respuestas

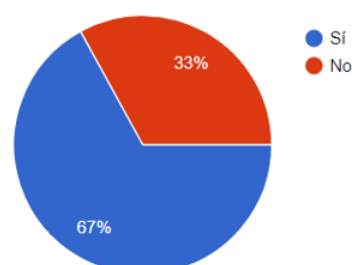


Figura 6.28: Resultados de la encuesta sobre disponibilidad tarjeta contactless y smartphone con NFC.

Tras completar la primera parte del estudio se mostró a los encuestados el funcionamiento del demostrador *CSPay* y se solicitó que evaluaran la innovación, usabilidad y sensación de seguridad que el nuevo método de pago les transmitía. Estos parámetros podían ser clasificados de 1 a 5, siendo 5 la máxima puntuación.

El primer aspecto a analizar es el factor de innovación que ofrece la nueva solución. La totalidad de los encuestados (ver *Figura 6.29*) calificó la idea de innovadora. Además, un 65% puntuó la propuesta con una valoración de cinco sobre cinco puntos.

¿Te parece una solución innovadora?

100 respuestas

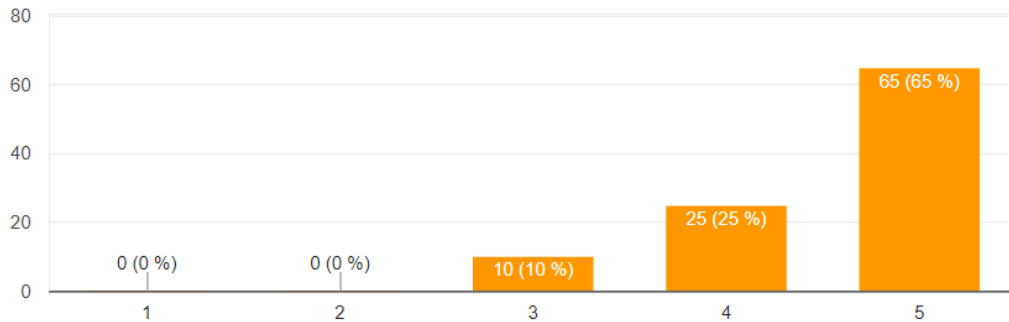


Figura 6.29: Resultados de la encuesta sobre el grado de innovación de CSPay.

El segundo factor a estudiar, es la usabilidad. Uno de los requerimientos para la implantación del nuevo método de pago, es que los usuarios dispongan de una herramienta que sea segura pero a la vez sencilla y cómoda para completar los pagos en comercio electrónico. La compra online mediante el uso de las tarjetas de coordenadas reducía significativamente la experiencia de usuario, así como la inserción manual de todos los dígitos que constituyen el número PAN de la tarjeta. En este caso, *CSPay* requiere del uso de la tarjeta y del dispositivo móvil, que son elementos de fácil acceso por parte del titular y aportan seguridad. De tal forma que no se requiere la inserción de largas contraseñas o copiado de números, por lo que se considera un medio práctico. En la *Figura 6.30* se puede observar que el 99% de los encuestados aprueban la sencillez del nuevo método, frente a un 1% que lo suspende. El 70% del número de usuarios puntúan con la máxima valoración la facilidad del diseño.

¿Te parece fácil de usar?

100 respuestas

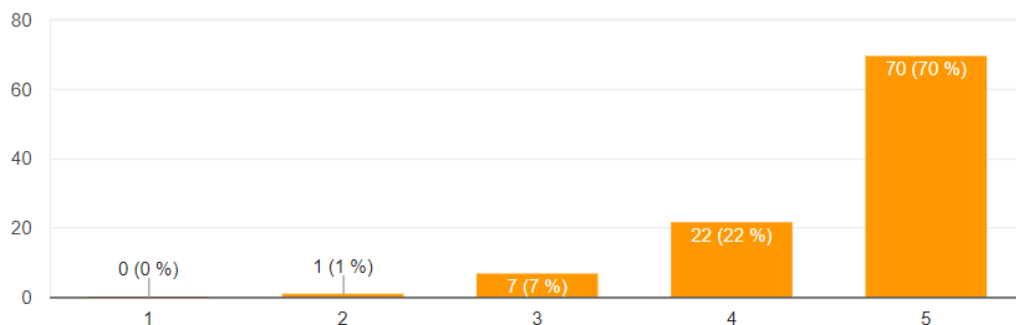


Figura 6.30: Resultados de la encuesta sobre la facilidad de la solución.

Por último, se ha analizado un factor clave que tenía que reunir el nuevo método de pago, la percepción subjetiva de seguridad. En el *Capítulo 4* se definió que para que un proceso se considerase robusto, tenía que reunir al menos dos de los tres factores de autenticación existentes: “YO SOY”, “YO SÉ” y “YO TENGO”. CSPay dispone de tres de ellas, por lo que el nivel de seguridad objetiva es muy alto. Sin embargo, es fundamental conocer qué sensación genera en los encuestados. En la *Figura 6.31* se observa que el 97% de los encuestados aprueba la robustez de la solución, frente al 3% que no lo considera seguro. El 64% ofrece una valoración de cinco sobre cinco en seguridad.

¿Consideras que es un método de pago seguro?

100 respuestas

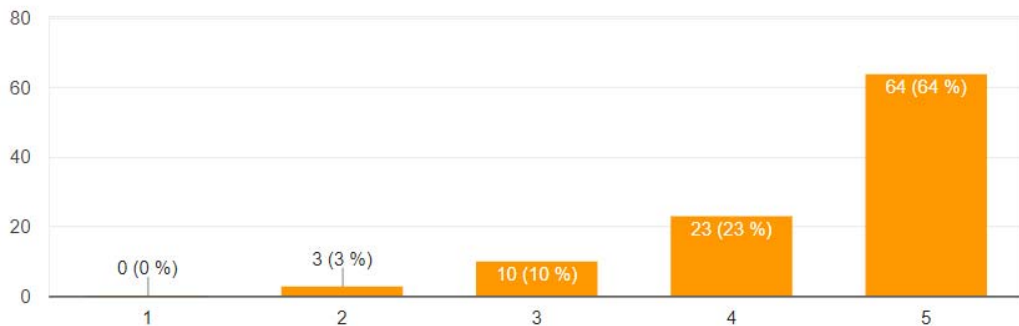


Figura 6.31: Resultados de la encuesta sobre la percepción subjetiva de seguridad de CSPay.

Finalmente, se analiza el porcentaje de participantes que se sienten atraídos y muestran interés por utilizar el nuevo método de pago si estuviera disponible en el mercado y contasen con los medios necesarios para poder llevar a cabo la transacción (tarjeta contactless y móvil NFC). Se observa en la *Figura 6.32* que el 76% de los usuarios indican abiertamente su conformidad en utilizar el nuevo método de pago en sus compras de e-commerce, y el 24% restante se muestra indeciso respondiendo con un “tal vez”. Resulta muy interesante que el *universo* de la encuesta se muestre receptivo a la adopción de un nuevo medio de pago y no se obtenga ninguna negativa rotunda entre los encuestados.

¿Lo utilizarías?

100 respuestas

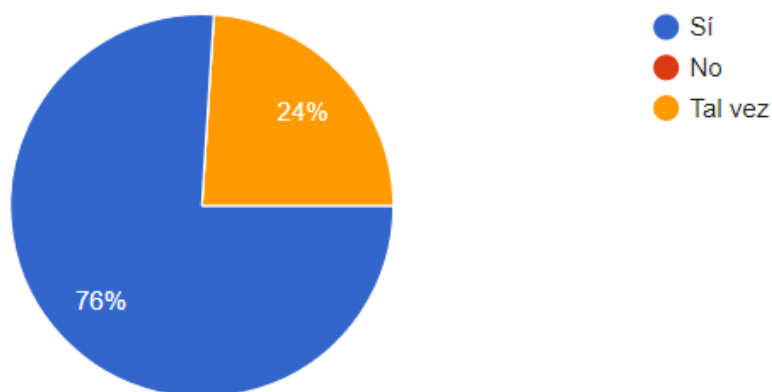


Figura 6.32: Respuesta de los encuestados a si utilizarían la solución propuesta.

A continuación, se han analizado los resultados obtenidos al filtrar las respuestas de los encuestados en algunos campos específicos.

- **Encuestados que disponen de la tecnología necesaria para utilizar CSPay.**

Para que un usuario pueda disfrutar de los servicios que ofrece el nuevo método de pago definido en el presente TFM, debe disponer de una tarjeta contactless y de un dispositivo móvil que soporte tecnología NFC. El 49% de los encuestados reunía ambas condiciones, de tal forma que se toman estadísticas parciales respecto de este nuevo *universo*. Entre el 100% de los encuestados que disponen de la tecnología suficiente para poder utilizar CSPay, destaca la baja presencia del rango de edad comprendido entre los 18 y los 23 años (ver *Figura 6.33*). Esto se debe a que muchos de ellos aún no disponen de su primera tarjeta financiera (contactos ni contactless), por lo que podría cambiar a corto plazo. El acceso a estas tecnologías aumentará de forma masiva en un futuro cercano, ya que actualmente los bancos están proporcionando a sus nuevos clientes tarjetas contactless, y la mayoría de nuevos smartphones que salen al mercado ya incorporan tecnología NFC.

Rango de edad

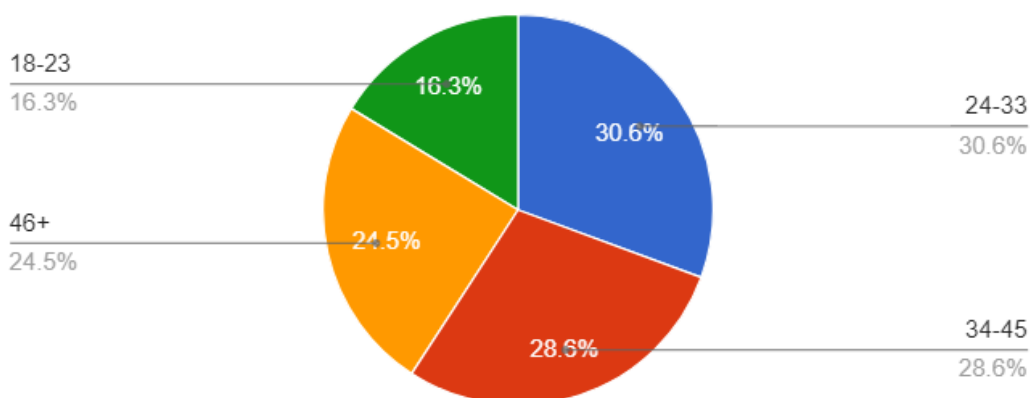


Figura 6.33: Resultados de la encuesta de rango de edad de los encuestados con tarjeta contactless y NFC en el móvil.

En cuanto a la utilización de CSPay, se puede observar en la *Figura 6.34*, que el porcentaje de usuarios que están dispuestos a utilizar este método de pago aumenta al 87,8% % si se limita la población de estudio a aquellos que disponen de los medios necesarios. Se deduce por tanto que cuando las circunstancias o condiciones son más favorables para la incorporación de un cambio, más receptivos se muestran los usuarios.

¿Lo utilizarías?

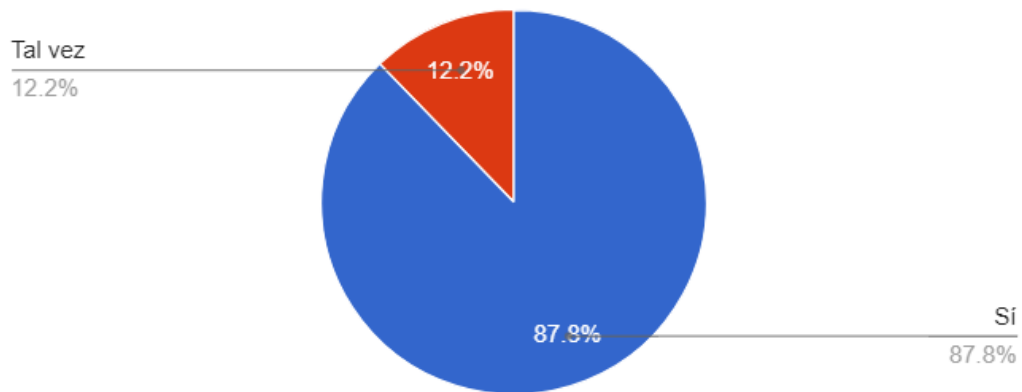


Figura 6.34: Resultados de la encuesta sobre intención de uso de los encuestados con tarjeta contactless y NFC en el móvil.

- Usuarios que han sufrido fraude.

En la *Figura 6.35* se recogen las estadísticas de los encuestados que han sufrido fraude. Se puede comprobar que el rango de edad que más ha experimentado esta problemática es el correspondiente al grupo de 24 a 33 años. Se puede intuir que también se trata de un rango de edad que presenta una alta actividad de transacciones llevadas a cabo mediante comercio electrónico y, por lo tanto, está más expuesto a este riesgo.

Rango de edad

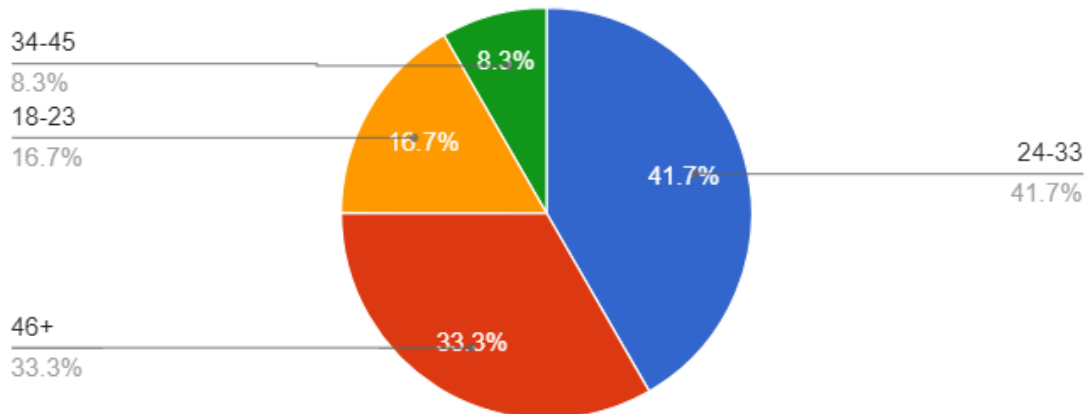


Figura 6.35: Resultados de la encuesta sobre el rango de edad de personas que han sufrido fraude.

La mayoría de encuestados que ha sufrido fraude, como es lógico, considera que los métodos de pago actuales no son seguros. Ver *Figura 6.36*.

¿Te parece seguro el pago actual mediante comercio electrónico?

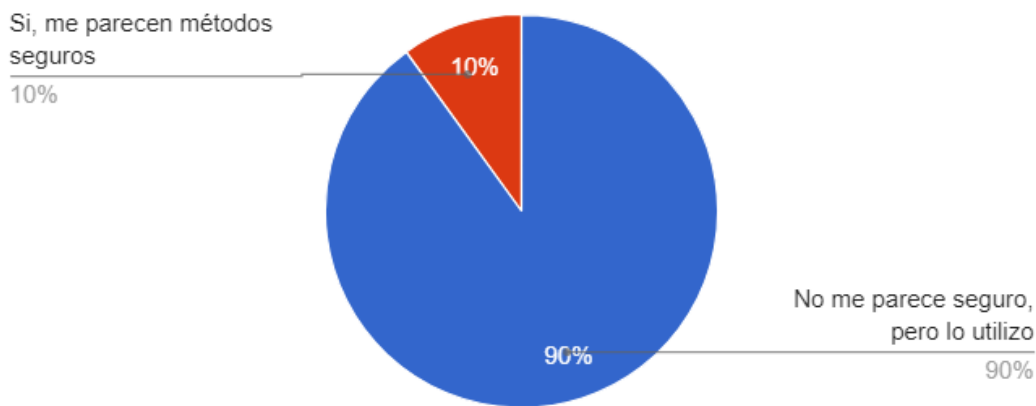


Figura 6.36: Resultados de la encuesta sobre la sensación de seguridad del pago actual para los usuarios que han sufrido fraude.

Por lo tanto, resulta muy interesante obtener la confianza de este *universo* y poder proporcionar soluciones seguras a los usuarios que presentan este perfil. En cuanto a la utilización de CSPay, aumenta hasta el 83,3% el porcentaje de encuestados que se acogería a este servicio, con respecto al 76% de los resultados generales. Ver Figura 6.37.

¿Lo utilizarías?

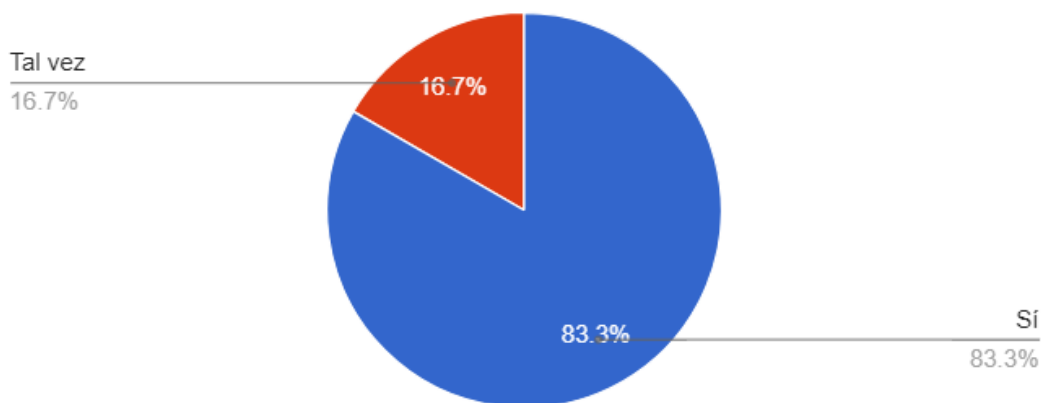


Figura 6.37: Resultados de la encuesta sobre la utilización de los usuarios que han sufrido fraude.

Para finalizar el apartado, se recogen en la *Tabla 6.1*, los resultados de las casuísticas estudiadas, en cuanto a la sensación de innovación, facilidad de uso y seguridad que transmite la solución CSPay a distintos *universos* entre los 100 encuestados.

Puntuación	Totalidad de encuestados	Disponen de tarjeta contactless y NFC	Han sufrido fraude
Innovación	4.55	4.73	4.67
Usabilidad	4.61	4.67	4.67
Seguridad	4.48	4.69	4.58

* Puntuación máxima 5 puntos.

Tabla 6.1: Comparativa de la valoración media de los diferentes grupos de usuarios.

Tras el análisis de los resultados, se puede concluir que el nuevo método de pago presenta una alta aceptación por parte de población entrevistada. Los métodos actuales siguen comprometiendo la seguridad de los usuarios, y CSPay aún a las características que los usuarios necesitan: Innovación, usabilidad y, sobre todo, seguridad.

Capítulo 7

Conclusiones y trabajos futuros.

7.1 CONCLUSIONES

En este TFM se ha desarrollado una idea original para reducir el fraude y mejorar la experiencia del usuario en transacciones de e-commerce. La propuesta se centra en incorporar la tarjeta contactless y el protocolo EMV, característico de las transacciones presenciales, a la compra online, para así aportar a este medio de pago mayor seguridad y transmitir dicha sensación al cliente. Para justificar la propuesta y demostrar su viabilidad se ha desarrollado un demostrador que integra todos los elementos característicos de la solución *CSPay*, como son: la aplicación móvil, un servidor para el procesamiento de transacciones financieras y una página web que emula las funcionalidades de un comercio electrónico. Además se han personalizado distintos perfiles de tarjetas de prueba, con el fin de disponer de más casuísticas funcionales (tarjetas caducadas o fraudulentas).

Se exponen las contribuciones más relevantes aportadas en el presente proyecto, en función de los resultados obtenidos en el transcurso y desarrollo del mismo.

- Se ha realizado un profundo análisis teórico del mundo de los medios de pago, tanto en un entorno presencial como no presencial, con el fin de enmarcar el proyecto en un contexto de interés tecnológico y social, fundamentado por el rápido crecimiento del comercio electrónico en la actualidad.

Este estudio ha permitido entender el proceso de transformación que está sufriendo el sector, adecuándose las nuevas soluciones presenciales que están en auge al uso del teléfono móvil como herramienta de pago. El conocimiento de esta realidad, permite diseñar nuevas soluciones adaptadas al ecosistema de la movilidad, sin tener que renunciar a las prestaciones que ofrece la presencia de la tarjeta física financiera, ni fijar o establecer límites del marco de aplicación.

- Se ha llevado a cabo una comparativa objetiva entre las tasas de fraude de las transacciones CNP y CP, destacando que el entorno más vulnerable corresponde a las compras online efectuadas en las páginas web de los comercios electrónicos, justificando de este modo la necesidad de diseñar una nueva solución de pago robusta para escenarios e-commerce a pesar de las múltiples opciones existentes.

A partir de los datos expuestos se ha demostrado que en CP las transacciones son mucho más seguras desde la aparición del chip integrado en las tarjetas inteligentes y del protocolo de comunicación EMV, convirtiéndose el comercio electrónico en el foco de los ataques fraudulentos. Dado que, el mero hecho de que la tarjeta esté presente aporta robustez a la operación, se concluye que la mejor solución para la reducción de fraude en comercio electrónico es aquella que incorpore la presencia de la tarjeta inteligente en el pago.
- Dadas las reflexiones de los puntos anteriores, se ha propuesto una solución técnica donde el dispositivo móvil y la tarjeta representan un papel fundamental. Se han analizado diferentes alternativas tecnológicas para la definición teórica de la idea, tomando decisiones de cómo implementar cada una de las partes que componen el sistema global en función del impacto y de las características de todas ellas. Se ha deducido la importancia que presenta el contexto y los aspectos externos en la elaboración de una propuesta técnica, ya que las normativas, la seguridad, el negocio y los diferentes intereses de los diferentes stakeholders en el sistema, juegan un papel fundamental y pueden condicionar el plan funcional tecnológico.
- Se ha definido, implementado y desplegado un demostrador piloto que muestra el concepto de la idea que se desea transmitir. Para llevar a cabo este proceso, ha sido necesario desenvolverse en diferentes lenguajes de programación e integrar los distintos módulos independientes con el fin de crear un sistema global completo. La experiencia acumulada da prueba de lo difícil que resulta conocer qué tecnología, herramienta o servicio es el más adecuado para generar una solución flexible, barata, elegante y productiva.
- Se han evaluado una serie de características de la idea presentada a través de una encuesta realizada a cien personas, de diferentes edades, grado de estudios y sexo, con el fin de obtener una noción básica del conocimiento sobre distintos medios de pago que dispone la sociedad actual y del posible grado de adaptación de la nueva propuesta. Los usuarios tienen una gran influencia en el sector de los servicios financieros, la opinión que tengan sobre el medio de pago (conveniencia, facilidad y seguridad) repercutirá de forma directa en el despliegue o no de una nueva solución. Por este motivo, se han centrado los esfuerzos del proyecto en conseguir una solución segura, a la par que conlleve una experiencia de usuario satisfactoria. Los resultados de la encuesta resultan favorables y motivan la continuidad de seguir trabajando en esta línea.

Tras el análisis de las deducciones anteriores, se puede concluir que los objetivos parciales, definidos en la etapa inicial del proyecto, han sido superados con éxito y, por consiguiente, el propósito final del TFM también ha sido alcanzado.

La idea principal giraba en torno a la propuesta de una solución de pago, de carácter innovador, que pudiera ser aceptada e integrada en los sistemas de pago electrónico disponibles en la actualidad. Cabe destacar que el planteamiento de la propuesta, así como el piloto que acompaña los fundamentos teóricos de la misma, han sido presentados para su valoración a la compañía de Redsys. La empresa ha mostrado interés real en el proyecto, identificando la solución como una oportunidad viable, puntera y diferenciadora en el mercado online, apostando por el potencial de la misma para su posible implementación en el negocio actual de los medios de pago.

7.2 DESPLIEGUE DE LA IDEA PROPUESTA EN REDSYS

Dado que existe cierto interés por parte de la compañía de Redsys en la propuesta definida en el presente TFM, se establecen los siguientes hitos que muestran continuidad del proyecto en un entorno profesional.

- Integración del piloto (desarrollado para el TFM) en el entorno de desarrollo de Redsys, realizando los siguientes pasos adicionales:
 - Utilización de las librerías oficiales que proporciona Redsys a los comercios electrónicos suscritos al servicio TPV Virtual, añadiendo en el formulario de pago la posibilidad de inserción del número de teléfono móvil.
 - Migración de las funcionales del servidor de pago alojado en la nube para la demo, a la lógica del servidor transaccional de Redsys. Se puede reutilizar gran parte de la infraestructura existente, por lo que únicamente sería necesario incorporar la base de datos de usuarios activos en la aplicación, y añadir la vinculación del nuevo número de teléfono móvil registrado al número de tarjeta financiera ya almacenado en Redsys.
 - Conexión interna entre el servidor transaccional y el centro de mensajería de push directo de Redsys, que ya dispone de un canal habilitado para la comunicación con GCM, debido a otras soluciones de pago móvil presencial que están siendo desarrolladas.
 - Cifrado de todas las comunicaciones existentes. En la demostración actual, los datos son transmitidos en texto plano.
- Reunión corporativa con los representantes del departamento de negocio para asegurar factibilidad del plan económico y financiero que respalde la propuesta.
- Junta con el equipo comercial y de ventas, para el análisis de la aceptación del servicio por parte de las entidades financieras españolas.

7.3 POSIBLES EVOLUCIONES DE LA IDEA PROPUESTA

A partir de la filosofía y las líneas generales definidas para la solución de pago presentada en el TFM, surgen dos evoluciones diferenciadas de la propuesta.

7.3.1 E-Wallet: supresión de la tarjeta para la solución e-commerce

El origen del fraude en e-commerce viene dado, mayoritariamente, por la captura de la información sensible de la tarjeta (PAN, fecha de caducidad y CVV2), ya sea a través del entorno online o bien mediante la obtención de los datos estampados en la tarjeta física. Se puede pensar que la problemática tiene su origen en los campos que constituyen el formulario de pago, al ser la única información necesaria para efectuar una transacción financiera. Por este motivo, resulta de interés añadir un nuevo método de pago que solicite la inserción del número de teléfono móvil del cliente, y de esta forma se necesite de un nuevo elemento (en este caso, el dispositivo móvil) en el diagrama transaccional actual. Para llevarlo a cabo, la aplicación móvil del cliente podría tener almacenadas virtualmente las tarjetas financieras, de esta forma, no sería necesario aproximar la tarjeta física. El flujo de trabajo que cabría esperar, se puede observar en la *Figura 7.1*.

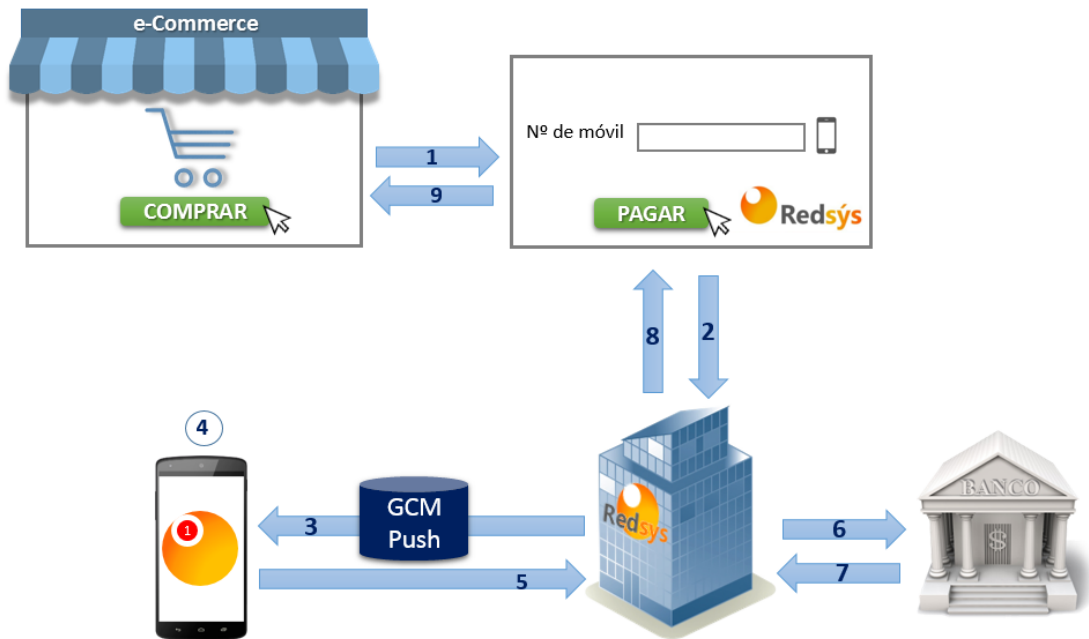


Figura 7.1: e-Wallet para comercio electrónico

Respecto a la propuesta original, esta evolución presenta las siguientes ventajas:

- Permite llegar a un público más amplio, ya que no sería necesario disponer de una tarjeta contactless ni de un móvil NFC (si, por ejemplo, se habilita la opción de inserción manual de las tarjetas físicas en el sistema virtual e-wallet).
- Las transacciones serían más rápidas, ya que se elimina la fase de aproximar la tarjeta en el transcurso de una operación. Cumpliría con la tendencia de facilitar y simplificar al máximo el proceso del pago.

Sin embargo, también refiere ciertas desventajas, ya que el método de pago ideal no existe:

- La aplicación móvil almacena información sensible, de tal forma que los dispositivos móviles podrían convertirse en un nuevo objetivo de ataque.
- La transacción no sería CP, por lo que las ventajas que incorpora la presencia de una tarjeta física inteligente no podrían aplicarse.
- La seguridad disminuye, ya que se suprime un factor “YO TENGO” del diagrama de pago.

7.3.2 Extrapolación del concepto a otros escenarios

El TFM se centra en las transacciones financieras llevadas a cabo entre usuarios y comercios electrónicos, conocidas en el sector de los medios de pago como B2C (Business to Consumer). El concepto básico de la propuesta del proyecto, como ya se ha visto, gira en torno a hacer análoga la compra presencial a la online, aproximando la tarjeta contactless al móvil vía NFC y haciendo uso del protocolo de comunicación EMV.

Una posible evolución, es la extrapolación de la idea a otros escenarios, como en sitios web C2C (Consumer to Consumer) como, por ejemplo, Ebay, o bien para los pagos de persona a persona a través de transferencias entre usuarios, como es el caso de Bizum o Twyp de ING Direct. Cabe destacar que BBVA ha sacado al mercado su producto Cashup, que permite realizar pagos móviles instantáneos a través de Bizum a cualquier contacto y se integra dentro de WhatsApp, Telegram, Hangouts y Facebook Messenger. Este sistema consiste en enviar dinero a través del chat, con la misma sencillez que se adjunta una foto, un vídeo o un emoji.

Se propone como futuro trabajo, la inserción de la tarjeta presente, como refuerzo de seguridad, en transacciones entre en dos usuarios a través de un chat o aplicación móvil destinada a tal fin. En la *Figura 7.2* se propone incluir la tarjeta contactless para autenticar a un cliente que desea realizar una operación mediante Bizum.



Figura 7.2: Incorporación de la tarjeta contactless para transferencias entre usuarios.

7.4 ALTERNATIVAS A ESTUDIAR.

A raíz de la solución de pago propuesta, surgen otras opciones que podrían ser válidas para la obtención del mismo fin, reforzar la seguridad en las transacciones de comercio electrónico gracias a la presencia de la tarjeta inteligente.

7.4.1 Pago por referencia.

Se plantea una nueva solución de pago que consiste en la inserción de un número de referencia para la autorización de una transacción en la página web de un comercio electrónico, en vez de los datos sensibles (PAN, fecha de caducidad y CVV2).

En este caso, el usuario debe iniciar sesión, por motivación propia, en la aplicación móvil de la entidad financiera de su tarjeta. Una vez que el usuario se autentica en la aplicación, aproxima su tarjeta para que el centro procesador genere un código de referencia a partir de los datos enviados y en función de la fecha y hora. Por último, el usuario introduce en la página web del comercio electrónico la referencia recibida y espera la resolución de la transacción.

Respecto a la propuesta original, esta alternativa no presenta ventajas aparentes. Este método presenta impacto similar en el formulario a rellenar y en el protocolo de comunicación entre Redsys y la entidad financiera (se debe definir e implementar una nueva casuística para la notificación de este tipo de operación).

Como desventaja, se podría atribuir que es poco intuitiva para el cliente, ya que debe iniciar sesión en la aplicación móvil sin haber recibido ninguna notificación, disminuyendo de esta forma la experiencia de usuario.

7.4.2 Datos de tarjeta válidos para un solo uso (tokenización).

Se propone un nuevo método de pago para escenarios de comercio electrónico que no presenta impacto en los formularios web existentes. Se brinda la oportunidad de que el titular de la tarjeta inserte los datos de un PAN de un solo uso o tokenizado.

Para obtener la tokenización de los datos reales y convertirlos en virtuales, el titular de la tarjeta debe iniciar sesión en la aplicación móvil y aproximar su tarjeta al lector NFC (de esta forma, se obtiene el número PAN y la fecha de caducidad real). A continuación, el centro procesador genera los datos sensibles virtuales (PAN, fecha de caducidad y CVV2) a partir de la información real recibida, y se los hace llegar al dispositivo móvil del cliente. El titular de la tarjeta inserta en la página web estos nuevos valores, válidos únicamente para un uso y con limitación temporal, reduciendo de esta forma el fraude asociado a phishing y pharming. Ver *Figura 7.3*.

Esta solución, respecto de la original, presenta la ventaja de compatibilidad con los formularios de pago actuales. El inconveniente principal es que es el propio usuario quién debe iniciar el flujo de comunicación en el dispositivo móvil (disminuyendo en cierto grado la mejora en la experiencia de usuario) y además, no todos los comercios electrónicos funcionan de forma adecuada con los datos virtuales como, por ejemplo, Amazon (ver Capítulo 2).

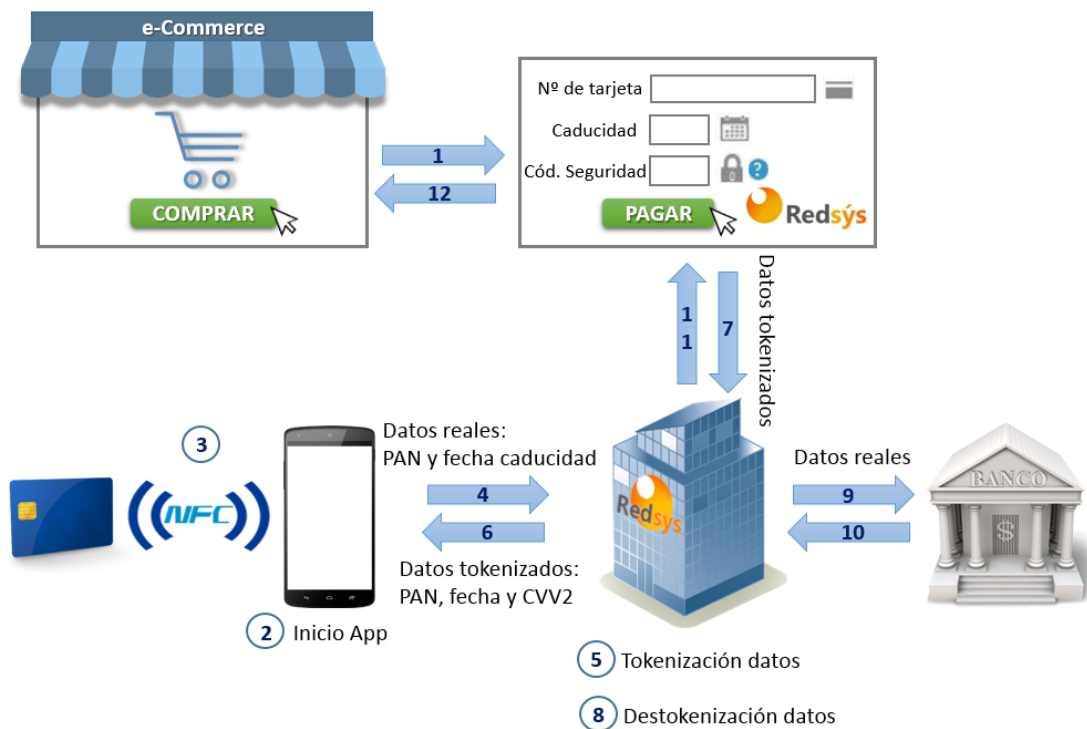


Figura 7.3: Propuesta de Tokenización de información sensible para comercio electrónico.

7.4.3 Lectura de tarjeta y generación de CVV2 dinámico.

Se propone un diagrama de pago que combina la presencia de la tarjeta inteligente con la generación de CVV2 dinámico para transacciones de comercio electrónico. Esta solución no presenta impacto en los formularios web existentes y elimina cierto fraude por phishing y pharming al no introducir el código CVV2 real. Tampoco ocasiona modificaciones en el protocolo de comunicación entre el centro procesador de Redsys y las entidades financieras.

El inconveniente frente a la idea original es que es el propio usuario quién debe iniciar el flujo de comunicación en el dispositivo móvil (disminuyendo en cierto grado la mejora en la experiencia de usuario). A continuación, aproxima su tarjeta física al móvil (produciéndose una lectura de la misma) y recibe del centro procesador un CVV2 diferente al que tiene estampado en el reverso de su tarjeta. En este escenario, el código de seguridad puede ser calculado en función del PAN y la fecha de caducidad real y de algún dato más obtenido de la tarjeta, como por ejemplo, el ATC (Application Transaction Counter). De esta forma, es más impredecible el resultado del algoritmo generador de CVV2.

Esta solución puede convivir con comercio electrónico seguro y no seguro. Se tendría que estudiar el factor añadido de seguridad, ya que al ser el PAN y la fecha de caducidad datos reales, la probabilidad de fraude aumenta respecto a la propuesta original, aunque su puesta en marcha sería prácticamente inmediata.

En la *Figura 7.4* se puede visualizar el flujograma del diseño y la secuenciación del mismo.

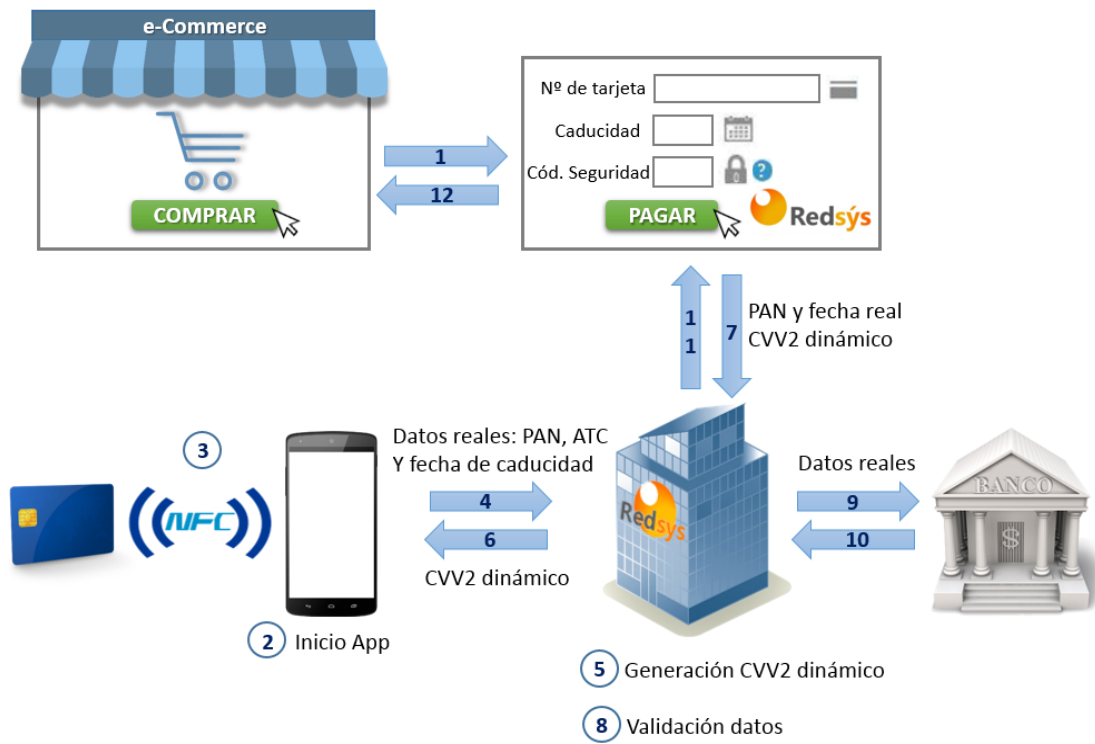


Figura 7.4: Propuesta de implementación con CVV2 dinámico.

Parte III

Pliego de condiciones

Pliego de condiciones

Para la realización del presente proyecto se planifica la dedicación de 300 horas de un Ingeniero de Telecomunicaciones, el cual debe contar con experiencia previa en el sector tecnológico de los medios de pago y conocimiento financiero del negocio transaccional.

Se enumeran a continuación los medios necesarios para el correcto desarrollo de dicho Trabajo Final de Máster. Cabe recordar que en el transcurso del proyecto se lleva cabo un estudio teórico detallado, así como la definición y puesta en marcha de un piloto que emule el funcionamiento real de la nueva solución definida.

Hardware

- Ordenador personal: Intel Core i7, velocidad de 3,40 GHz y memoria RAM de 8 GB (o superior).
- Tres dispositivos móviles con sistema operativo Android (con versión 5.0 o superior) y tecnología NFC.
- Conjunto de tarjetas inteligentes financieras con funcionalidad contactless.
- Maquinaria de estampación de tarjetas DataCard

Software

- Microsoft Office 2013 (o superior).
- Bootstrap, para el entorno de desarrollo de páginas web de código abierto, que permita emular la adquisición de un producto y la selección del pago, mediante la operativa de comercio electrónico.
- Notepad++, como editor de texto para la programación en Python del servidor que emula el comportamiento de la red de pago.
- Amazon Web Service (AWS), como recurso tecnológico para la representación del centro de procesador y de resolución de transacciones financieras alojado en la nube.
- WinSCP y PuTTY (PuTTYgen), para el control remoto desde el ordenador personal a la máquina virtual del servidor de pago residente en AWS.
- Cuenta de usuario en No-IP, para la obtención de un servicio dinámico de DNS.

- Google Service Messaging (GCM), para el envío de notificaciones push desde el servidor de pago a los diferentes dispositivos móviles.
- Software Development Kit (SDK), de Android Studio, para el desarrollo de la aplicación propietaria financiera en el dispositivo móvil.
- Acceso a herramientas disponibles en el entorno laboral de la empresa de Redsys, para la carga del sistema operativo en las tarjetas inteligentes de pruebas (Smart Card Manager) y la personalización de las mismas (Advantis Perso Builder).
- ID Works Design&Production, para el diseño e impresión de los logotipos esbozados.

Parte IV

Presupuesto

Presupuesto

El coste del presente TFM se debe principalmente a la cuantía de los materiales utilizados y a los honorarios del trabajador partícipe en el proyecto. En primer lugar se obtiene el *Presupuesto de ejecución por material* (PEM), el cual es debido a los equipos informáticos y programas software que han sido utilizados. En la tabla p. 1 se muestra el cálculo realizado para obtener el PEM correspondiente.

Presupuesto de ejecución por material (PEM)			
Concepto	Cantidad	Precio Unidad	Coste Total
Material			
Ordenador personal	1	799,00 €	799,00 €
Tarjetas inteligentes	10	1,15 €	11,50 €
Smartphone Android con NFC	3	160,00 €	480,00 €
Material Oficina	1	120,00 €	120,00 €
Material Software			
Windows 10 Professional	1	50,00 €	50,00 €
Office 2013	1	75,00 €	75,00 €
Advantis Perso Builder	1	No disponible*	No disponible*
Flash Loader Application	1	No disponible*	No disponible*
DataCard ID Works Design&Production	1	No disponible*	No disponible*
Notepad++	1	Open Source	0,00 €
Android Studio 2.3.3	1	Open Source	0,00 €
Bootstrap	1	Open Source	0,00 €
Amazon Web Service (AWS)	1	Open Source**	0,00 €
Usuario de No-IP, resolución DNS	1	Open Source**	0,00 €
Google Cloud Messaging (GCM)	1	Open Source**	0,00 €
WinSCP	1	Open Source	0,00 €
Putty/PuttyGen	1	Open Source	0,00 €
Total PEM			1.535,50 €

*Acuerdos bilaterales comerciales entre proveedores y empresas certificadas en medios de pago, restringido al uso público.

**Utilización del software de la capa gratuita que proporciona cada herramienta.

Tabla p. 1: Presupuesto de ejecución por material (PEM).

Los honorarios del empleado se establecen a una cuantía de 50€ por cada hora de servicio de ingeniería proporcionado al proyecto. La duración del TFM es de 300 horas trabajadas, de tal

forma que los gastos totales debidos al personal contratado se pueden consultar en la Tabla p. 2.

Honorarios				
Concepto	Nº personas	Duración (horas)	Precio Unidad	Coste Total
Ingeniería	1	300	50,00 €	15.000,00 €
Total				15.000,00 €

Tabla p. 2: Honorarios del trabajador.

El presupuesto total del proyecto será, por tanto, la suma del valor del material (PEM) y el resultado del salario del trabajador. Es necesario aplicar el Impuesto de Valor Añadido (IVA) sobre el valor resultante de la suma anterior. En la p. 3 se detallan los gastos que proporcionan el coste total del proyecto.

Presupuesto	
Concepto	Coste Total
PEC	1.535,50 €
Honorarios	15.000,00 €
Subtotal	16.535,50 €
IVA (21%)	3.472,45 €
Total	20.007,95 €

Tabla p. 3: Presupuesto Total del TFC

El presupuesto total del proyecto, de carácter interno, asciende a la cifra de 20.007,95 €

Madrid, Septiembre de 2017
El Ingeniero Jefe de Proyecto

Fdo.: Carla Solís Carpintero
Ingeniera de Telecomunicaciones

Parte V

Manual de usuario

Manual de usuario

El usuario que desee utilizar el medio de pago descrito para soluciones de comercio electrónico, se debe instalar el archivo *CSPay.apk* en su dispositivo móvil Android, con una versión de aplicación 5.0 o superior, que disponga de tecnología NFC para la lectura de las tarjetas contactless financieras. A continuación, se describen las diferentes operativas existentes en la aplicación desarrollada.

1) Inicio de la aplicación.

En el momento de la apertura de la aplicación, aparece una pantalla de bienvenida con el logo representativo de la solución de pago durante un periodo de tiempo determinando, hasta dar paso a la pantalla de inicio de sesión.

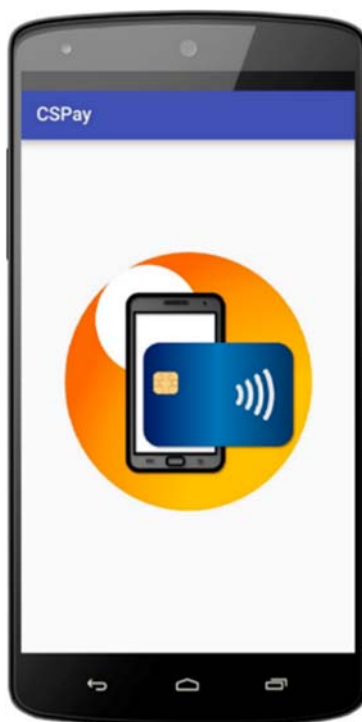


Figura m.1: Inicio de aplicación

2) Inicio de sesión

Para iniciar sesión se debe introducir el DNI y la contraseña de la aplicación. Si el usuario es nuevo en la aplicación, debe pulsar el botón de crear cuenta y proceder con el registro en el servicio.



Figura m.2: Pantalla de Inicio de Sesión.

3) Creación de usuario

Se deben rellenar todos los campos solicitados: Nombre, DNI, teléfono, correo electrónico y contraseña de la aplicación (con su correspondiente repetición de la misma, por si hubiese algún problema en el mecanografiado). Se limita la utilización de un dispositivo móvil por usuario, de tal forma que solo puede existir un DNI asociado a un número de teléfono en la base de datos del servidor de la aplicación. Es necesario que el usuario marque la casilla para aceptar las condiciones del uso de la aplicación (se permite a la aplicación móvil que disponga de acceso a NFC para la lectura de las tarjetas y procese la mensajería push enviada desde el servidor).

El número de teléfono móvil registrado será el que se utilice para efectuar el pago en las páginas web de los comercios electrónicos. El correo electrónico que el usuario proporcione será utilizado como otra vía de comunicación desde el servidor para contactar con el cliente, por ejemplo, para el envío del recibo tras una transacción aprobada o la notificación del motivo por el cuál ha sido denegada. También se envía un correo electrónico de bienvenida a la aplicación tras completar con éxito la fase de registro.

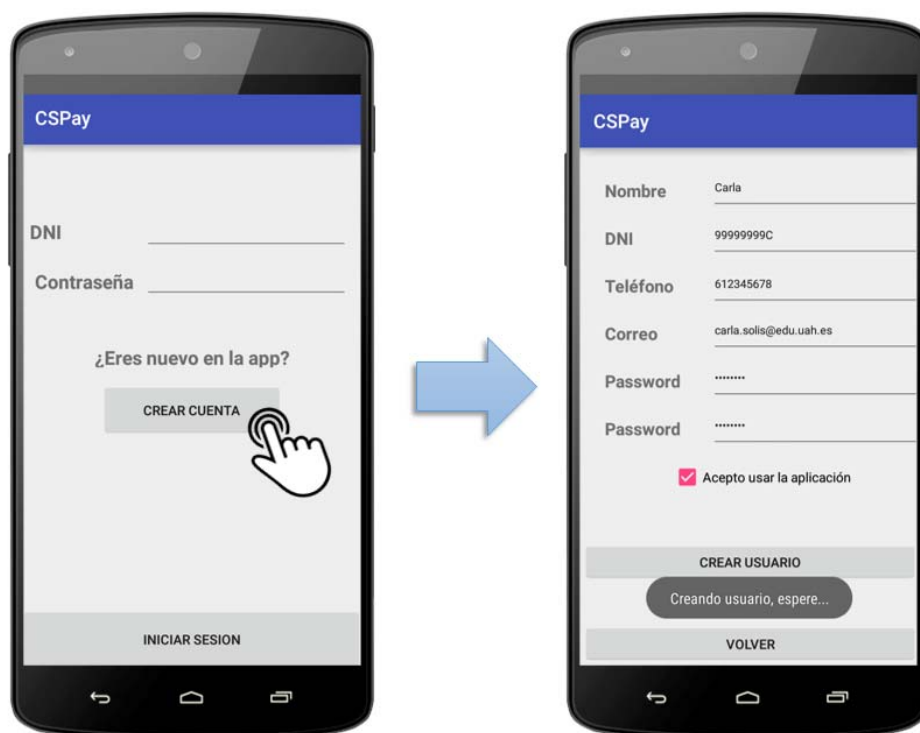


Figura m.3: Flujo “crear usuario”

4) Opciones del menú principal

En el menú principal de la aplicación existen cinco posibilidades de actuación:

- **Nueva tarjeta:** Permite dar de alta una nueva tarjeta en la aplicación de pago *CSPay*.
- **Eliminar tarjeta:** Permite dar de baja una tarjeta en la aplicación, si previamente ha sido dada de alta en el servicio.
- **Verificar tarjeta:** Comprueba si la tarjeta aproximada está dada de alta o no en el servicio y, por tanto, si puede ser utilizada para realizar una compra en comercio electrónico utilizando este método de pago.
- **Eliminar cuenta:** Permite dar de baja un usuario de la aplicación. Se eliminan todos los datos vinculados a este usuario (registro del número de teléfono móvil, contraseña, números de tarjetas, etc.).
- **Acerca de la App:** Muestra información relativa a la aplicación.



Figura m.4: Menú principal.

En los siguientes apartados se detallan las diferentes opciones disponibles.

5) Solicitud de alta nueva de tarjeta en el sistema

La opción de “nueva tarjeta” del menú principal permite dar de alta una nueva tarjeta para la utilización de *CSPay* como método de pago en los comercios electrónicos. Tras seleccionar dicha opción, se debe aproximar la tarjeta contactless deseada al sensor NFC del dispositivo móvil. Aparece una notificación por pantalla, que indica que el banco verificará los datos.



Figura m.5: Flujo “nueva tarjeta”.

6) Solicitud de baja de tarjeta en el sistema

La opción de “eliminar tarjeta” del menú principal permite dar de baja una tarjeta que previamente ha sido dada de alta en el servicio. Tras seleccionar dicha opción, se debe aproximar la tarjeta contactless al sensor NFC, de igual forma que en el proceso anterior.

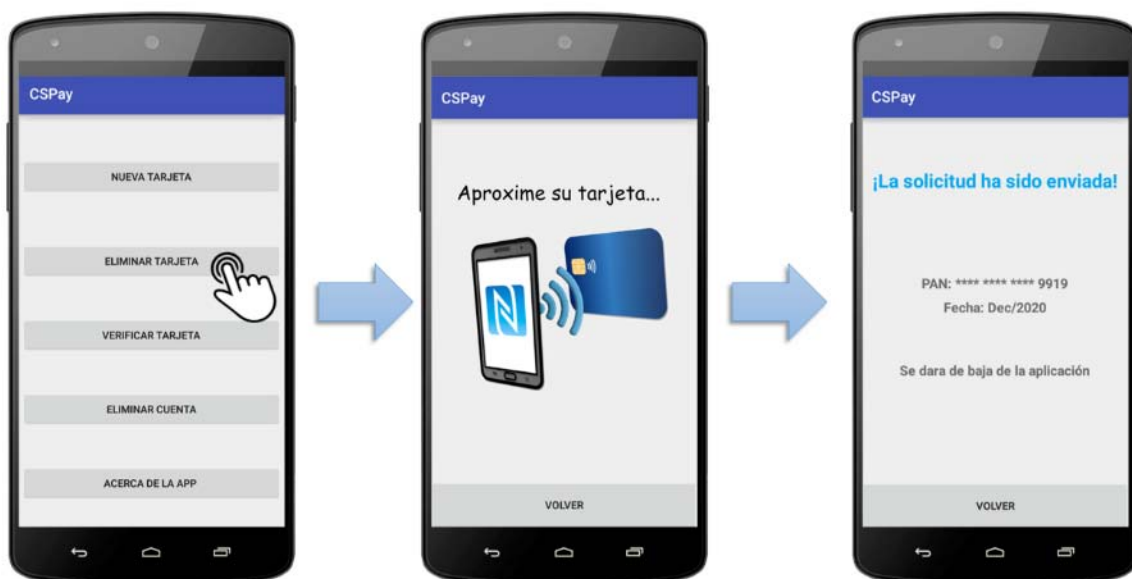


Figura m.6: Flujo “eliminar tarjeta”.

7) Verificación de tarjeta dada o no de alta en el sistema de pago

La opción de “verificar tarjeta” del menú principal permite comprobar si la tarjeta aproximada al dispositivo móvil está disponible para su uso en el método de pago *CSPay*.

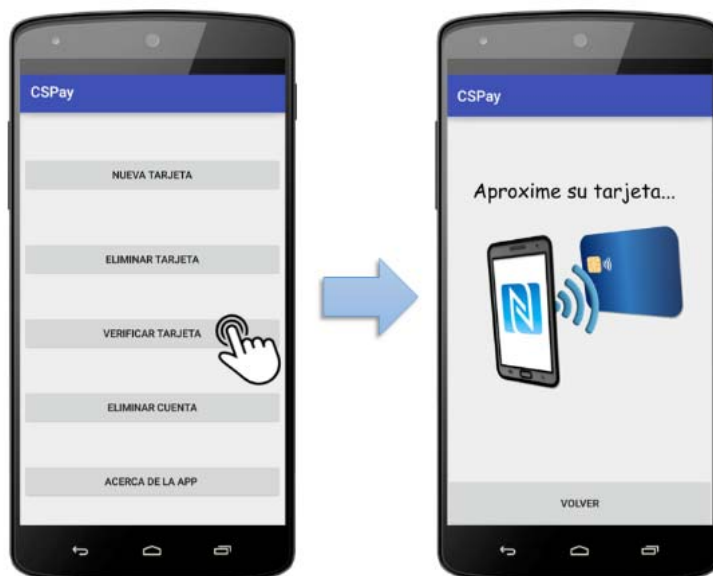


Figura m.7: Flujo “verificar tarjeta”.

En función de la respuesta recibida por el centro procesador, existen estas dos posibilidades:

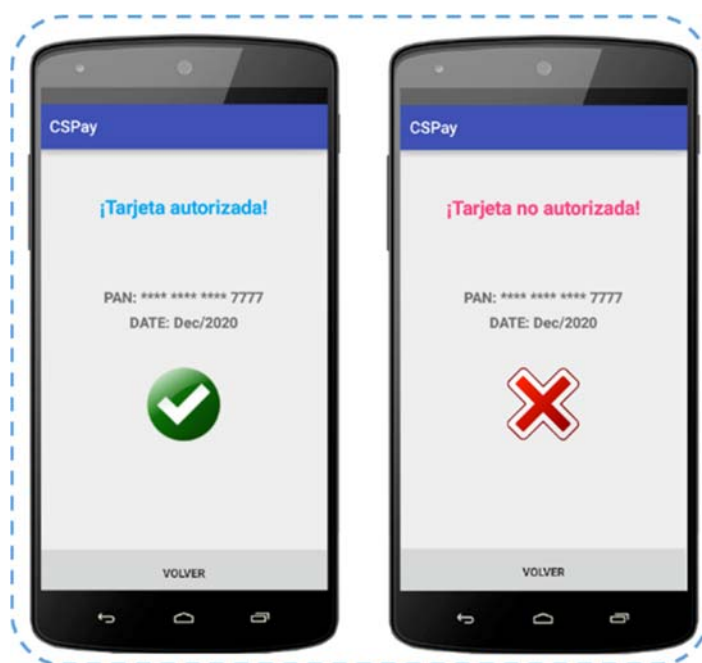


Figura m.8: Respuesta a la solicitud “verificar tarjeta”.

8) Eliminación de la cuenta creada

La opción de “eliminar cuenta” del menú principal permite dar de baja la cuenta creada. Tras seleccionar dicha opción se debe confirmar que se quiere dar de baja el usuario. El servidor ante esta petición, elimina todos los datos vinculantes a la cuenta (usuario, número de teléfono registrado, tarjetas operativas, etc.).

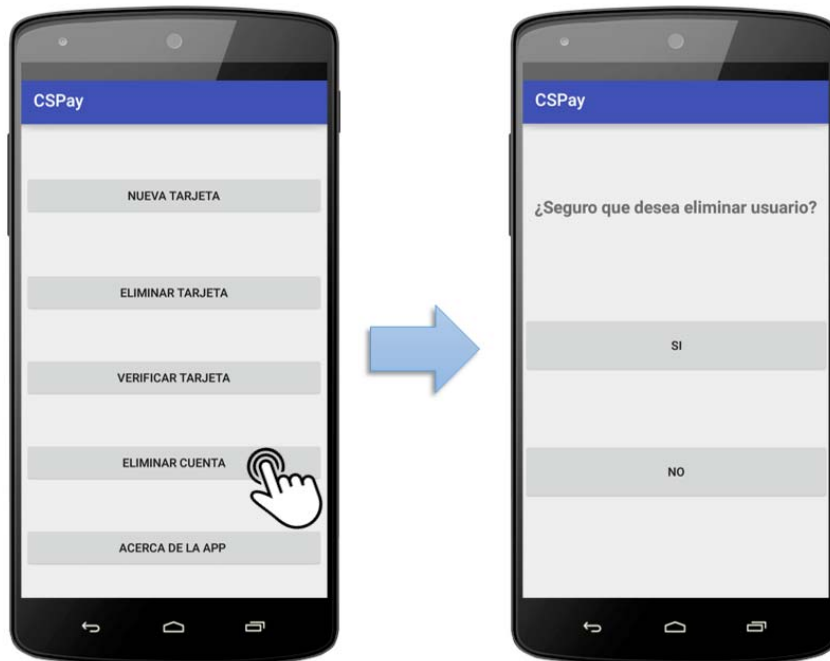


Figura m.9: Flujo eliminar cuenta.

9) Información sobre la APP

La última opción del menú principal denominada “acerca de la APP” permite obtener información sobre la aplicación. Para volver al menú principal se debe presionar el botón volver.



Figura m.10: Flujo información APP.

10) Realización del pago mediante CSPay.

El usuario debe insertar el número de teléfono móvil en la página web del comercio electrónico que soporte el pago mediante CSPay. A continuación, recibirá una notificación en el dispositivo móvil para completar el pago con los datos relacionados con la solicitud (identificador del comercio, importe y código de moneda). En esta etapa, el cliente puede cancelar o pagar la compra. Si se pulsa el botón “pagar”, aparece una ventada de iniciar sesión para autenticar al titular, por lo que debe introducir la contraseña (el DNI se guarda por defecto), y aproximar la tarjeta contactless (con la que desee efectuar el pago y que previamente esté data de alta en el servicio) al lector NFC del dispositivo móvil. El resultado de la operación se comunica en la página web del comercio electrónico y vía email.



Figura m.11: Flujo de la realización del pago.

Parte VI

Bibliografía

Bibliografía

- [1] *Economipedia*. Diccionario electrónico de economía, finanzas y marketing.
Disponible en: <http://economipedia.com/diccionario-economico/>
- [2] E. Alcaraz, *Diccionario de términos económicos, financieros y comerciales*. 2008.
Editorial: ARIEL
- [3] *Historia de las tarjetas de crédito*. Marzo 2015.
Disponible en: <https://www.bbva.com/es/historia-de-las-tarjetas-de-credito/>
- [4] *Bancos y Finanzas. Las tarjetas de crédito*.
Disponible en: <https://bancosyfinanzas.wordpress.com/la-cuenta-corriente/tarjetas-de-credito/un-poco-de-historia/>
- [5] *Los medios de pago, un paisaje en movimiento*. Año 2016.
Disponible en: <http://www.pwc.es/es/financiero/publicaciones-financiero.html>
- [6] *EMVCo* Disponible en: <https://www.emvco.com/>
- [7] *Estadísticas del Banco de España. Departamento de Sistemas de Pago*.
Disponible en: <https://www.bde.es/f/webbde/SPA/sispago/ficheros/es/estadisticas.pdf>
- [8] *Estadísticas de Redsys. Informes de gestión de la comisión delegada 2017 y balance anual 2016*.
- [9] *Omicrono. Tarjetas con lector de huella. P. Moya. Abril 2017*.
Disponible en: <http://omicrono.elespanol.com/2017/04/tarjetas-con-lector-de-huellas-mastercard/>
- [10] A. Martí Xataka. Diciembre 2016.
Disponible en: <https://www.xataka.com/moviles/quiero-pagar-con-el-movil-en-espana-que-son-las-opciones-disponibles>
- [11] *Xataka Android. Cosmos. Junio 2016*.
Disponible en: <https://www.xatakandroid.com/aplicaciones-android/como-puedes-pagar-hoy-en-dia-con-tu-smartphone-android-en-espana>
- [12] *Blastingnews*. Junio 2016
Disponible en: <http://es.blastingnews.com/economia/2016/06/cuando-el-movil-acabo-con-la-tarjeta-00968825.html>

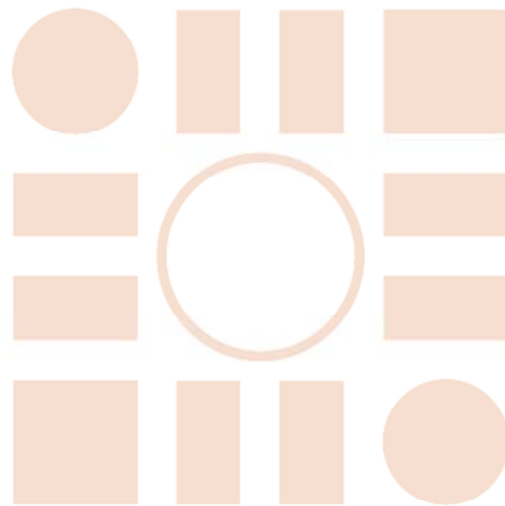
- [13] K. Laudon; C. Guercio. *E-commerce: Negocios, tecnología, sociedad*. (Editorial Prentice Hall, 4º Edición).
- [14] eMarketer. "Worldwide Retail e-commerce Sales: The eMarketer Forecast for 2016". Agosto 2016. Retail & Ecommerce.
- [15] Comisión Nacional de los Mercados y Competencia (CNMC). Julio 2017.
Disponible en: <https://www.cnmc.es/node/363937>
- [16] DPD Full Report e-shopper barometer.
Disponible en: https://www.dpd.com/home/insights/e_shopper_barometer
- [17] m-commerce.
Disponible en: <https://wiboomeia.com/que-es-el-m-commerce/>
- [18] CNP. Card Not Present. The independent source for original CNP news.
Disponible en: <https://cardnotpresent.com/>
- [19] ISO/IEC 7812
Part 1: Numbering system. 2017.
Part 2: Application and registration procedures. 2017.
- [20] B. Soto, *Amazon no acepta pago con PayPal*. Enero 2016
Disponible en: <https://marketing4ecommerce.net/amazon-pago-con-paypal/>
- [21] I. Barbero. *PayPal, objetivo de hackers*. 7 de Septiembre de 2016.
Disponible en:
https://cincodias.elpais.com/cincodias/2016/09/07/lifestyle/1473243045_514028.html
- [22] M. Monforte. *HelpMyCash*.
Disponible en: <https://www.helpmycash.com/banco/iupay/>
- [23] Amazon. *Métodos de pago*.
Disponible en:
https://www.amazon.es/gp/help/customer/display.html/ref=footer_payment?nodeId=201262600
- [24] YaSeHacerlo. *Categoría de Métodos de pago por Internet*. Mayo 2016.
Disponible en: <https://yasehacerlo.com/tarjeta-virtual/>
- [25] Bitcoin
Disponible en: <https://bitcoin.org/es/como-funciona>
- [26] IngenioVirtual | *Proyectos Web, Comercio electrónico y negocios online*
Disponible en: <http://www.ingeniovirtual.com/formas-de-pago-en-el-comercio-electronico/>

- [27] *EMV Integrated Circuit Card Specifications for Payment Systems: Version 4.3*
Book 3 - Application Specification
Disponible en: <https://www.emvco.com/specifications.aspx?id=223>
- [28] *Data Breach Fraud Impact Report. Javelin Strategy&Research. November 2014.*
Disponible en: <https://www.javelinstrategy.com/>
- [29] *Online Payment Motion Code webinar Online. Sept 2016. Oberthur Technologies.*
Shopping: How to secure e-transactions with new payment solutions
- [30] *Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)*
Disponible en: <http://www.lssi.gob.es/paginas/Index.aspx>
- [31] *BBVA Francés. Septiembre 2016.*
Disponible en: <https://blog.bbvafrances.com.ar/articulo/Phishing/que-es-el-skimming-y-como-evitar-que-copien-tus-tarjetas/43>
- [32] B. Ryland. *GiveMeCredit*. Diciembre 2014.
Disponible en: <https://www.givemecredit.com/articles/1/identity-theft/skimming,-phishing,-pharming-and-other-frauds.htm>
- [33] A. Crespo. *RedesZone*. Diciembre 2014.
Disponible en: <https://www.redeszone.net/2014/11/14/el-60-de-los-sitios-web-phishing-consiguen-robar-datos-de-los-usuarios/>
- [34] R. Rozalén. *SILICON*. Enero 2017.
Disponible en: http://www.silicon.es/72-las-brechas-datos-las-empresas-se-al-hacking-skimming-phishing-2327631?inf_by=59909512681db844018b4903
- [35] *Estándar ISO/IEC 7816.*
Part 3: Card with contacts - Electronic Interface and Transmission Protocols.2006.
Part 4: Organization, security and commands for interchange. 2013
- [36] *EMV Contactless Specifications for Payment Systems. Book A.*
Architecture and General Requirements. March 2016, v2.6.
- [37] *EMV Contactless Specifications for Payment Systems. Book B.*
Entry Point Specification. March 2015, v2.5.
- [38] *EMV Contactless Specifications for Payment Systems. Book C-2.*
Kernel 2 Specification. February 2016, v2.6.
- [39] *EMV Contactless Specifications for Payment Systems. Book C-3.*
Kernel 3 Specification. February 2016, v2.6.
- [40] *PCI – DSS. Security Standards Council.*
Disponible en: <https://es.pcisecuritystandards.org/minisite/env2/>
- [41] J. Domenech *SILICON*. Julio 2017.

- Disponible en: http://www.silicon.es/los-usuarios-e-commerce-priorizan-la-seguridad-frente-la-velocidad-2345816?inf_by=59909512681db844018b4903
- [42] Asociación Española de Economía Digital. Informe de empresas.
Disponible en: www.adigital.org
- [43] M. K. Pedersen. *Normativa PSD2*. Marzo 2016.
Disponible en: <http://www.clubecommerce.com/es/actualidades/m/news/nueva-directiva-europea-de-pagos-psd2-unos-de-los-impactos-mas-importantes-para-retailers-en-europa-24110>
- [44] G. Serna *Near Field Communication. Parte I pp16-18*.
Disponible en: <https://es.slideshare.net/GabrielSerna/tutorial-near-field-communication-nfc>
- [45] *Kantar Worldpanel*. Mayo 2017.
Disponible en: <https://www.kantarworldpanel.com/es/Noticias/Cuota-de-mercado-de-smartphones-en-Espana>
- [46] L. Sui. *StrategyAnalytics*. Nov 2016
Disponible en: <https://goo.gl/FEtOtt>
- [47] S. Fernández. Junio 2017.
Disponible en: <https://www.xatakamovil.com/apple/contra-todo-pronostico-apple-entreabrira-ios-11-al-estandar-nfc>
- [48] I. Lasso *Tekzup*. Abril 2017.
Disponible en: <https://tekzup.com/7-plataformas-diferentes-desarrollar-android-apps/>
- [49] *Manual de Usuario de Android Studio*.
Disponible en: <https://developer.android.com/studio/intro/index.html>
- [50] C. Mgbemena. Diciembre 2016.
Disponible en: <https://code.tutsplus.com/es/tutorials/sending-data-with-retrofit-2-http-client-for-android--cms-27845>
- [51] A. Hathibelagal. Febrero 2016.
Disponible en: <https://code.tutsplus.com/es/tutorials/how-to-get-started-with-push-notifications-on-android--cms-25870>
- [52] *GCM*
Disponible en: <https://developers.google.com/cloud-messaging/>
- [53] *Librería EMV*
Disponible en: <https://github.com/devnied/EMV-NFC-Paycard-Enrollment>
- [54] *AMAZON WEB SERVICE*
Disponible en: <https://aws.amazon.com/es/free/>

- [55] *PuTTYGen*
Disponible en: <https://www.ssh.com/ssh/putty/windows/puttygen>
- [56] *No-IP*
Disponible en: <https://www.noip.com/>
- [57] *SNS*
Disponible en: https://aws.amazon.com/es/sns/?nc2=h_m1
- [58] *Bootstrap*
Disponible en: <http://getbootstrap.com/>
- [59] *HTTP*
Disponible en: <https://www.w3.org/Protocols/>
- [60] *POST*
Disponible en: <https://tools.ietf.org/html/rfc2616>
- [61] *Stack Overflow*
Disponible en:
<https://stackoverflow.com/documentation/jquery/316/ajax#t=201708260948479026476>
- [62] *Google Form*
Disponible en: <https://www.google.es/intl/es/forms/about/>

Universidad de Alcalá
Escuela Politécnica Superior



ESCUELA POLITECNICA
SUPERIOR



Universidad
de Alcalá