Memoria de la acción AYUDAS DE LA UNIVERSIDAD DE SALAMANCA PARA LA INNOVACIÓN DOCENTE

Llaves FIDO (Fast IDentify Online) como segundo factor de autenticación en la gestión on-line de los procesos de enseñanza y aprendizaje

Código del Proyecto: ID2017/030

Existen dos tipos de tecnología de autenticación. La de factores universales de autenticación (Universal Authentication Factors o UAF) utiliza datos biométricos, dispositivos físicos (mochila) y contraseñas. La segunda se conoce como Universal Second Factor Authentication (U2F) o autenticación en dos pasos. Todos los métodos de autenticación tienen desventajas: las contraseñas se pueden adivinar, las tarjetas inteligentes se pueden robar y la biométrica se puede fingir en determinadas condiciones. Pero si se combinan, como se hace en la U2F, el nivel de seguridad es mayor.

El segundo factor de autenticación es pues un método de validación adicional de datos que, sumado a los métodos habituales, permite intensificar los niveles de seguridad; por poner un ejemplo a nivel bancario es muy frecuente utilizar *una tarjeta plástica* que tiene en el dorso una matriz de 9 filas y 9 columnas; cada celda contiene pares de datos (números), los cuales le serán solicitados al momento de la firma de cualquier operación monetaria o bien *el uso de una clave móvil*, que es una aplicación que puede ser instalada en cualquier dispositivo smartphone y que funciona como método de validación de datos, intensificando los niveles de seguridad y evitando el fraude electrónico, permitiendo generar claves de autenticación dinámica para la firma de operaciones.

Una llave FIDO nos sirve para acompañar a nuestro usuario y contraseña de cuenta de acceso con un segundo factor de autentificación, siendo una llave de este tipo más segura que un SMS o incluso un código de autenticador móvil, por el sencillo hecho de no estar conectado ni ser alterable.

La llave FIDO U2F (Universal 2 Factor Authentication) lleva grabada una clave privada que no es modificable y será cotejada con la clave pública en nuestros servicios online, cada vez que iniciemos sesión en nuestra cuenta por ejemplo que nos identifiquemos en el id_USAL por ejemplo para acceder a la plataforma de formación studium.usal.es, a la calificación de actas, en la cuenta Google, DropBox, etc.

Al formar parte de FIDO empresas como Microsoft, Google, Samsung, PayPal, Visa, Lenovo y Nok Nok, entre otros, es seguro que lo apoyarán de una forma u otra en sus productos. Existe mucha información en internet, en concreto en esta web https://www.slideshare.net/FIDOAlliance/presentations encontramos múltiples presentaciones que avalan el peso de este método como segundo factor de autenticación.

Objetivo principal del proyecto:

> Ventajas e inconvenientes del uso de llaves FIDO (Fast IDentify Online) como segundo factor de autenticación en la gestión on-line de los procesos de enseñanza y aprendizaje.

Sin duda todo proceso de enseñanza-aprendizaje on-line comienza con el acceso on-line a diferentes plataformas y servicios y se clausura con las calificaciones de las actas, pero no por ello es menos importante la fase intermedia en la que el deseo es tener identificado al estudiante, por lo que lo interesante sería abordar todos y a cada uno de ellos.

Hemos buceado en la red para ver si alguna universidad española lo ha implementado y no hemos encontrado ninguna y por ello nos lanzamos a hacer esta experiencia piloto para conseguir en el octavo Centenario de la Universidad de Salamanca ser la pionera en innovación mediante la implantación del sistema FIDO en el inicio de sesión seguro en el proceso de enseñanza aprendizaje on-line o complementaria de la formación presencial con Llave de seguridad USB NFC y JavaCard.

Todo el estudio previo a la presentación de este proyecto indica que obtendremos muy buenos resultados, pero como supone mucho cambio, primero consideramos que hay que hacer experiencia piloto con un grupo reducido de profesores, alumnos, materias y centros y que las conclusiones a las que lleguemos nos permita implantar el proyecto con éxito en toda la universidad, por ello hemos hecho la experiencia piloto para acceder a campus-bisite.usal.es.

Los **objetivos detallados planteados** en este proyecto han sido:

- Formar a los estudiantes que participan en este proyecto en temas de seguridad en el acceso on-line.
- Analizar ventajas e inconvenientes del uso de las llaves FIDO frente a las alternativas de:
  - Crear certificados propios para instalar en el navegador.
  - Validación por código enviado por un segundo canal, que sería canal telefónico vía sms.
  - Uso del DNI electrónico y el teléfono.
  - NFC en combinación con lectores conectados a ordenadores de sobremesa o vía teléfonos móviles.
- Estudiar qué procesos de la gestión on-line del proceso de enseñanza/aprendizaje se deben considerar de nivel máximo de seguridad y plantear la viabilidad de hacer obligatorio el uso de las llaves FIDO.
- Personalizar el software del servidor de control de llaves FIDO para las necesidades de la Universidad de Salamanca y hacer estudio de posible desarrollo en el CPD (Centro de Proceso de Datos) de la USAL.
- Estudiar el coste de la gestión del propio software de control.
- Analizar las ventajas que ofrecen las llaves FIDO usb con NFC y JavaCard frente a otras llaves FIDO simples.
- Estudiar el nivel de dificultad activación y desactivación de las llaves, así como su funcionamiento.

- Poner en prueba, como segundo factor de autenticación, las llaves FIDO buscando todas las posibles funcionalidades de las mismas para la gestión on-line del proceso de Enseñanza-Aprendizaje.
- Estimar el coste de implantación del sistema FIDO en toda la Universidad.

Impacto sobre la docencia

El proyecto que presentamos mejora el proceso docente, fundamentalmente en el inicio (identificación del estudiante y del profesor) y en el final (calificación de actas) de cualquier titulación y centro, pues es transversal a todos por ello hemos elegido materias de diferentes titulaciones y centros.

En la actualidad la mayoría de la formación Oficial en la USAL es presencial entendiendo que la mayor dificultad en la formación on-line es la acreditación del estudiante sobretodo en el momento de realizar la evaluación on-line. En la enseñanza presencial para la evaluación continua nos da miedo dar más peso a los cuestionarios o tareas realizadas por la plataforma de formación on-line por la inseguridad de quien lo ha realizado. Por ello, si aumentamos el grado de certeza de quién es quién se está formando podremos apostar más por la formación virtual, por la semipresencial o presencial con mayor formación complementaria on-line.

Evitaremos que los mensajes que nos enviamos por correo electrónico, por ejemplo, exámenes que estamos preparando entre profesores, o los mismos exámenes que tengamos en dropbox, caigan en manos de los estudiantes que se vayan a evaluar si alguien consigue nuestro usuario y contraseña ya que le faltaría la llave.

En el proceso final de enseñanza aprendizaje, la evaluación, podemos evitar que las actas sufran ataques, por lo que los resultados del aprendizaje serán fiables y no nos vuelva a pasar que tengamos que sospechar que nuestros propios estudiantes modifican las actas.

Beneficios obtenidos

- Reflexionar sobre la inseguridad de utilizar un identificador y una contraseña.
- Concienciar de la necesidad de utilizar otros métodos de autenticación más seguros como es el segundo factor de autenticación.
- Encontrar una manera cómoda y segura, haciendo uso de un segundo factor de autenticación, de identificarnos on-line en todos los servicios de la Universidad.
- Utilizar la misma tecnología que otros servicios de los cuales normalmente hacemos uso como google, Dropbox, etc.
- Identificar al estudiante on-line y por lo tanto resolver la mayor barrera que la Junta de Castilla y León encuentra a la hora de la formación on-line.
- Conseguir que los profesores valoremos más la actividad que realiza el estudiante en studium, pues tendremos la certeza de quien está conectado.
- Finalizar el proceso de docencia confirmando que las calificaciones del alumno no han sido alteradas.

Metodología de trabajo

La metodología de trabajo que hemos llevado a cabo en resumen ha sido:

- Realizar reunión inicial presencial los profesores implicados en el proyecto.
- Crear debate entre los participantes sobre el método de autenticación que están utilizado en los diferentes accesos que hagan on-line, dentro y fuera de la Universidad. Posteriormente seleccionar a tres alumnos de cada asignatura basándonos en la actividad en studium, en el espíritu innovador y en la preocupación que sientan por la seguridad.
- Presentar FIDO y otros métodos de autenticación a los alumnos y proporcionarles por medio de un seminario la formación necesaria para el uso de la llave FIDO.
- Proporcionar a cada miembro participante una llave FIDO e impartir la formación necesaria para el adecuado uso y dar a conocer todas sus funcionalidades.
- Mantener reuniones presenciales y on-line todos los miembros del equipo de trabajo de forma periódica.
- Realizar experiencia piloto con el sistema de autenticación propuesto.
- Analizar ventajas e inconvenientes del método de autenticación y hacer estudio comparativo en base a la seguridad y comodidad respecto de los métodos de autenticación disponibles en la universidad y que anteriormente usara cada uno.
- Obtener listado de los servicios que ha utilizado cada uno, tanto servicio interno a la universidad como externo.
- Reunión final de los miembros del equipo para hacer estudio y propuesta sobre la viabilidad de implantar este método de autenticación como posible método para determinados servicios universitarios, como puede ser el acceso a la intranet de la Universidad.

Recursos empleados

Para poder llevar a cabo el proyecto hemos necesitado contar con los siguientes recursos materiales y de software específico:

- **Llaves FIDO usb con NFC y NFC y JavaCard**. Llave de seguridad USB + NFC y JavaCard (FIDO U2F Security Key) para PC, Mac y dispositivos móviles Android con NFC. Proponemos estas llaves FIDO porque al incorporar tecnología JavaCard permite ejecutar de forma segura pequeñas aplicaciones java (applets) en dicha llave.
- **Software servidor control llaves FIDO**. Se trata del software de activación de las llaves FIDO, que ahora para probar lo hemos externalizarlo pero que si se llegara a implantar en nuestra universidad sin duda la propuesta sería desarrollarlo en el CPD.

Resultados:

Todos los participantes para probar el acceso a la web mediante la llave FIDO hemos registrado las llaves en la web demo https://shttps://u2f.cloudentify.com/u2fdemo/

En concreto hemos elegido un usuario y contraseña y a continuación hemos registrado la llave y hemos probado el acceso a la web con dicha llave.

Cada participante ha elegido el servicio dónde ha querido probar el segundo factor de autenticación y en este caso cada uno nos hemos encontrado con una serie de dificultades. En particular nos hemos encontrado que las llaves sólo son compatibles oficialmente con Google Chrome. En Mozilla Firefox sólo es compatible mediante un plugin, aunque están trabajando para implementar el Universal 2 Factor en Firefox de forma nativa.

A modo de resumen estas son las páginas de instrucciones para registrar la llave en distintos servicios:

- Google

https://support.google.com/accounts/answer/6103523?co=GENIE.Platform%3DAndroid&hl=es

- Facebook

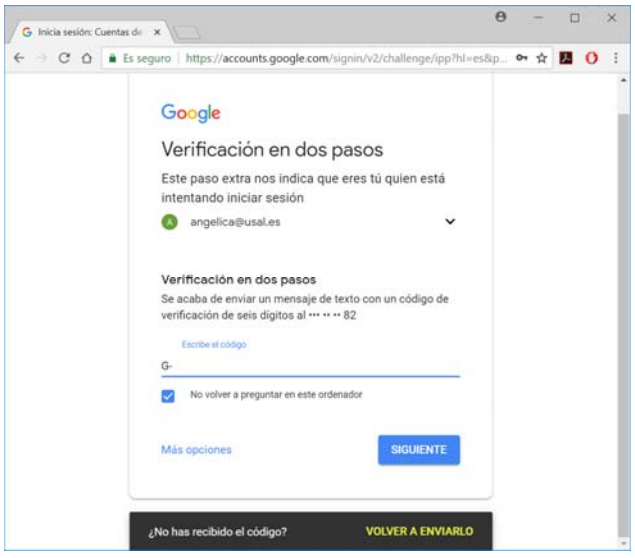
https://es-la.facebook.com/help/401566786855239

- DropBox

https://www.dropbox.com/es_ES/help/security/enable-two-step-verification#2falsecurity-keys

Otra de las dificultades es que para acceder a servicios como google drive para activar las llaves tenemos que hacer uso de un teléfono móvil, pero bueno, como la Universidad de Salamanca cuenta con el número de móvil de cada despacho no sería mucho problema, salvo que dos usuarios compartan el mismo número de teléfono.

Hemos probado el acceso a los diferentes servicios y no hemos tenido dificultad después de detectar que no era compatible con todos los navegadores.



Hemos iniciado el desarrollo web para usar las llaves FIDO en campus-bisite.usal.es

Conclusiones

Los resultados, por parte de los profesores y de los alumnos, se resumen en los siguientes ítems:

- La mayoría de los usuarios desconocen el segundo factor de autenticación que ofrece la universidad, en concreto la existencia de latch y quien lo conoce no lo tiene activado y muchos de los que lo tienen activado lo dejan abierto.
- Es una necesitad trabajar con un segundo factor de autenticación para acceder a servicios como las actas y a la formación on-line.
- El manejo de las llaves FIDO es muy sencillo como hemos podido probar en diferentes servicios.
- El segundo factor de autenticación es mediante el uso de un dispositivo hardware por lo que aumenta el nivel de seguridad frente a otros métodos de autenticación.
- Proponemos utilizar como primer factor de autenticación usuario y contraseña y segundo las llaves FIDO.
- Para acceder a determinados servicios propondríamos obligatorio el uso de las llaves FIDO. Sin duda para acceder a las actas. Actualmente se puede acceder con certificado digital pero también con usuario y contraseña.
- La inversión entendemos que es asequible; en concreto hay que proporcionar una llave **FIDO** a cada profesor, hacer el desarrollo web de acceso a los diferentes servicios y desarrollar el software de control de las llaves.

Salamanca, 6 julio 2018

Fdo.: Angélica González Arrieta