NFC Mobile Payment with Citizen Digital Certificate

Wei-Dar Chen, Keith E. Mayes
Smart Card Centre
Information Security Group
Royal Holloway, University of London
UK

Yuan-Hung Lien
Department of Innovations in Digital Living
Lan Yang Institute of Technology
Yilan, Taiwan

Jung-Hui Chiu
Department of Electrical Engineering
Chang Gung University
Tao-Yuan, Taiwan

***Abstract*—With the increasing availability of smart handsets, the mobile phone is likely to become the device of choice for accessing sophisticated services and applications in a convenient yet secure manner. This is especially true with the introduction of Near Field Communication (NFC), which provides the phone with an interface allowing it to act as a smart card reader or to emulate smart cards. However the user registration process is relatively weak for access to mobile communication services and some third party application providers have concerns when security certification is totally reliant on the trust and processes of the mobile network operator. In contrast, the Citizen Digital Certificate (CDC) is a PKI based citizen identification card issued to a user by the government, following a rigorous user registration process. In our investigation we explore the combined use of NFC phones and the CDC card, by using the government card to endorse the security of credentials held within the NFC Security Element that is hosted within the phone's Subscriber Identity Module (SIM). In this paper, we propose and describe a secure mobile payment system solution for use in a traditional in-store environment, which combines the CDC PKI, the NFC secure element within the SIM and a 3G mobile network. Moreover, the solution provides a convenient user experience, which leverages from the wide-scale 3G network and the short-range contactless communication of NFC, and could replace the use of payment or service specific smart cards.**

I. Introduction

A very common way of allowing users to make non cash payments is to issue them with a smart card. The number of issued physical cards has been steadily increasing in recent years and many people have multiple debit, credit cards and transport cards. To address this, some bank cards are already issuing multi-purpose cards, e.g. the Oyster card and payWave variant of credit cards issued by Barclay in the UK. Combining banking and transport functionality in a secure manner has some notable advantages, e.g. a user can have the e-cash functionality of a transport card and use the bank credentials for top-up whenever the credit runs low. [1]

The above example serves to illustrate that an alternative to simply issuing more and more smart cards is desirable and that a solution may benefit from combination of multiple technologies and legacy systems. In this paper the combination of the multiple technologies: Near Field Communication (NFC), Secure Element-SIM (SE-SIM) and Public Key Infrastructure (PKI), are used with mobile communication and CDC legacy systems to construct an m-payment system.

NFC in addition with SE-SIM provides strong cryptographic calculation power and proximity communication between compatible devices. It offers good security, yet an easy intuitive user experience and ubiquitous mobile access to users' payment accounts and credit. The functionality may also be securely managed via the mature and well standardised telecommunication infrastructure of the mobile network operator (MNO). PKI, apart from its slow speed of calculation on limited resource devices, offers strong security and verifiable digital signatures without the key distribution problems of symmetric solutions. How to combine the best features of these existing technologies (and associated legacy systems) and construct a secure and easy to use in-store payment system, is the main goal of this work.

A number of m-payment studies have been published in recent years. Most of them utilise technologies such as GPRS [18], SMS [19], bluetooth [21] [22], WAP [23] [24] and so on, to interact with mobile phones for m-payment transactions. However, most of the aforementioned approaches are designed for online web payment transaction [4], and have security and ease-of-use restrictions that limit user acceptance. Other weaknesses relate to Internet connection speed or SMS latency, which result in lengthy set-up and transaction times. There is less literature related to conventional (shop based) payment transaction scenarios [2] [3], which will be the focus for this work.

Two phases are defined in the proposed payment transaction; the user registration (endorsed registration) phase and the actual payment execution phase. Registration is only performed once and relies on a prior trust relationship of both the MNO and the user with a third party Certification Authority (CA). In particular, the CA is the government entity that issued the user's CDC card. The MNO trust relationship with the CA permits a mobile enabled transaction to be associated with the strong user identity registration of the CDC card.

II. Background

A. Near Field Communication (NFC)

NFC is specified in ISO/IEC 18092 [5] and is a short-range wireless interface with data exchange rates up to 424Kbps and an operating frequency of 13.56 MHz. NFC offers three main operation modes for various types of applications: card

(smart card/RFID) emulation mode, card reader mode and peer-to-peer mode. NFC is an extension of the ISO/IEC 14443 Type A [6] and Felica [7] specifications and NFC is therefore compatible with these systems. ISO/IEC 21481 describes extended services for NFC, which includes the possible use of existing ISO 14443 Type B and ISO/IEC 15693 [8] products. The main application areas are payment/transaction, ticketing, access control, connectivity, information download and loyalty [9]. The application types could be roughly classified into four groups: touch-and-go, touch-and-confirm, touch-and-connect and touch-and-explore [10]. The NFC secure element (SE), which contains secure program memory and key material, could be a device embedded into the mobile phone or be integrated into the UICC (platform that hosts the SIM). The Single Wire Protocol (SWP) supports SIM-centric solutions and allows for connections between the UICC card and an NFC wireless modem chip in the handset [9] [11]. For detailed NFC security analysis please refer to [12] and [13].

B. Citizen Digital Certificate (CDC)

The Citizen Digital Certificate is a natural person certificate based on Public Key Infrastructure (PKI), mainly for assisting the government in solving problems associated with offering electronic services on the Internet. These problems are difficulty of verifying the online user identity and ensuring the security of online data transmission. The main purposes of having this government PKI (GPKI) are offering a good government information security on the Internet, providing integrity and non-repudiation features on each transaction, simplifying government administrative processes (physically and electronically), and upgrading services to be more efficient for both the government agencies and citizens.

Functions of the CDC include: (1) *Identification Verification*: During any kind of online process when identity verification is needed, CDC IC card can be used instead of inserting user name and password. (2) *Encryption*: Information is encrypted; the information being transmitted is protected from the danger of interception and disclosure. (3) *Signature*: According to E-Signature law no. 9, and with the agreement of the signer, his/her signature can be transformed into an E-Signature. When an electronic file is combined with an electronic signature, it is viewed as a legal document and has the same authority as a paper document with governmental seal. Therefore, the original paper document can be legally replaced by the electronic document. (4) *Electronic Certificate*: Paper certificates from different agencies can be changed into electronic form by using the Citizen Digital Certificate.

Some use cases of CDC include: Internet tax return filing, health insurance personal data and fine inquiry, electronic motor vehicle and driver licence information management, digital household registration and ID loss reporting. For more information please refer to [14] [15] [16] [17].

III. NFC M-PAYMENT SYSTEM WITH CDC

We assume that a customer wishes to perform a mobile payment transaction while shopping within a conventional in-store environment (with a fixed line POS) and that the customer is already registered for CDC i.e. CDC is a government issued certificate that works as a digital ID card. The uniqueness of the CDC card card, the private-key and public-key secure functionality, and the nation-wide acceptance and validation are complimentary features for NFC phone (SE-SIM) enabled mobile payment services. Please note that all phone-based cryptographic calculations and confidential data in the proposed solution are carried out and stored in the SE-SIM.

TABLE I
ABBREVIATIONS AND NOTATIONS

AuC	Authentication Centre
CDC	Citizen Digital Certificate
Cer	Certificate
$D()$	Decryption
DT	Date and Time
$E()$	Encryption
EC	Endorsed Credential
ED	Expiry Date
GEN	Self Key Generation Command from MNO
GCA	Government Certificate Authority
ID	Identity/serial number of the smart card
$IMSI$	International Mobile Subscriber Identity
K_{APP}	Application Key between SE-SIM and CDC
MAC	Message Authentication Code
MNO	Mobile Network Operator
MP	Mobile Payment
$MSISDN$	Mobile Subscriber ISDN Number (phone number)
MSK	Shared key between MNO and SE-SIM
NFC	Near Field Communication
OI	Ordering Information
ON	Ordering Number
PI	Payment Information
PI_{REQ}	Payment Information Request
PK	Public Key
POS	Point of Sale
PR	Payment Result
R	Random Number
SE	Secure Element
$Sig_A(B)$	Signature of B which is signed by key A
SK	Private Key
SN	Serial Number
TC	Transaction Counter
TL	Transaction Limit
$TMSI$	Temporary Mobile Subscriber Identity
TP	Total Price
TSN	Transaction Number
$USIM$	Universal Subscriber Identity Module

In this section, a step-by-step description is given of the combined CDC and NFC mobile payment system solution. The m-payment transaction service is separated into two phases: Endorsed Registration phase and the Payment Transaction phase. Assumptions and requirements are presented before each phase description. All the notations and abbreviations used within the descriptions are provided in Table 1.

A. Phase 1: Endorsed Registration

Endorsed registration is the process of binding the mobile transactional credentials with customer credentials certified by a trusted third party. As Figure 1 depicts, three entities are used in this phase: MNO/AuC, the customer's NFC phone/SE-SIM

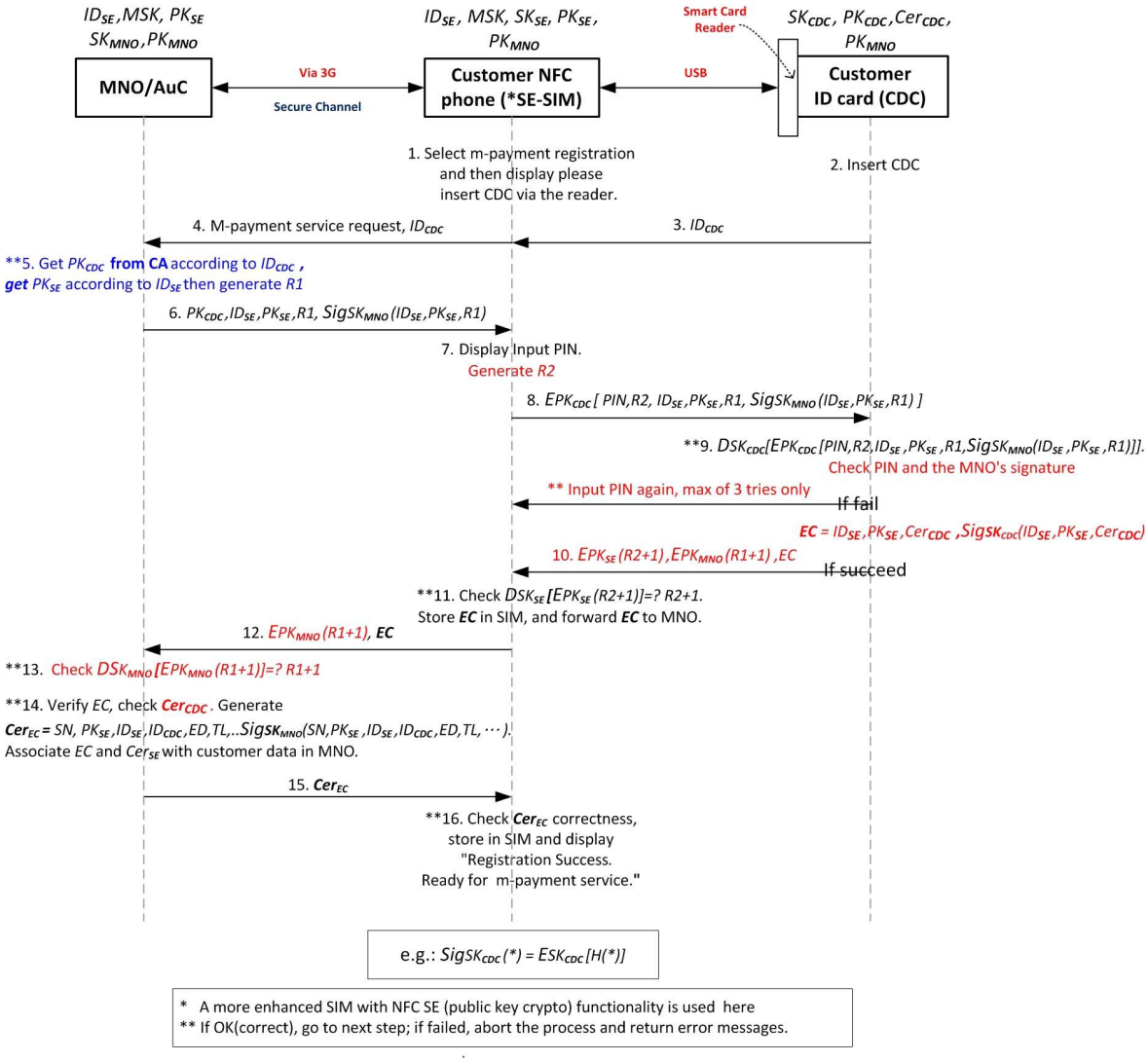

Fig. 1. NFC m-Payment with CDC – Endorsed Registration Phase

and the customer's ID card, e.g. CDC. Here we use CDC as an example in the system and assume both MNO and customer's CDC are under the same CA, i.e. the Government CA (GCA). The GCA (which represents the trusted third party) is used to verify the customer's CDC, so that it can be used to endorse the customer's SE-SIM. The MNO works as a domain entity to verify the mobile user's phone and associated CDC. Because it recognises the GCA it can check the authenticity of the CDC provided by the customer and verify the Endorsed Credential (EC) to generate a certificate for the SE-SIM (Cer_{SE}) for later use in mobile payment transactions.

The customer NFC phone is a bridge for the MNO to authenticate the CDC ID card and prove that transaction information is backed by the CDC. The main job of the CDC here is to generate the EC as a valid endorsement for the customer phone when performing subsequent m-payment transactions.

Some additional *assumptions* are necessary: (1) The MNO has already cooperated with the GCA, which means the CDC card would contain the public key of the MNO (PK_{MNO}) when it is issued to the user. (2) The MNO has pre-stored its public key (PK_{MNO}) and a "personalised" shared key (MSK) on the SE-SIM. (3) The SE-SIM already has a personalised secret key (SK_{SE}) and public key (PK_{SE}) stored securely in non-volatile memory. (4) The mobile communication channel between the MNO/AuC and the customer NFC phone is secure. (5) The customer NFC phone has an external smart card reader (or cradle) connected in order to communicate with the customer's ID card (CDC). (6) The MNO can obtain the public key of the CDC via a channel to the GCA. Note that assumption (5) is only required for registration and would become unnecessary if future CDC cards follow the market trend and also offer a contactless interface.

The first step of endorsed registration is to forge a strong legal binding between the "customer's CDC" and "SE-SIM"

cards. In order to achieve this we use the customers's CDC private key (SK_{CDC}) to sign the public key of the SE (PK_{SE}). An Endorsed Credential (EC) and a certificate of the SE (Cer_{SE}) will be generated and utilised in the payment transaction phase. For further detail on the binding generation processes between the CDC and the SE-SIM please see the protocol step descriptions.

Step 1 – 2: The customer first selects "register" from the m-payment application on his mobile phone which triggers generation of a random number, $R1$, and prompts the user to insert the CDC into the reader.

Step 3: Here the ID number of the CDC card (ID_{CDC}) is sent to the customer's phone.

Step 4 – 5: The customer's NFC phone makes an m-payment service request to the MNO. We assume there is a secure channel between the MNO and the customer phone, using the identity and security credentials that are pre-stored in the SIM and known by the MNO. Furthermore, the MNO has records of the phone's ID_{SE} and associated PK_{SE}. By sending the ID_{CDC} to the MNO it is possible for the MNO to check the validity of the CDC via the GCA and obtain the associated public key (PK_{CDC}).

Step 6: A random number, $R1$, is generated when the check of step 5 is successful. The MNO produces a packet of information including PK_{CDC}, ID_{SE}, PK_{SE}, $R1$. A signature is added using the MNO's private key (SK_{MNO}).

Step 7 –8: After the pack of information is received, the NFC phone prompts the user to enter a PIN for the purpose of user identification of the CDC card. The SE-SIM then forwards a new pack of information to the CDC including the original information ID_{SE}, PK_{SE}, $R1$, MNO's signature in addition with the PIN and another random number, $R2$, using the public key of CDC sent from MNO and encrypted under it.

Step 9: The government issued ID card, CDC, decrypts the received packet of information ($PIN, R2, ID_{SE}, PK_{SE}, R1$) from the MNO. If the PIN check fails then the phone may repeat step 8 allowing the customer to try again. If the PIN try limit is reached (typically three attempts) then the transaction terminates with an error message and customer guidance is displayed via the phone. The significance is that the CDC card may no longer be in possession of the legitimate holder.

If the PIN and signature are valid the CDC card increments both $R1$ and $R2$, to reduce the risk of replay attack when the values are used again. An Endorsed Credential (EC) is generated here, which is a binding of NFC phone and CDC information (ID_{SE}, Cer_{CDC}, PK_{SE}), that is signed by the CDC. ID_{SE} and PK_{SE} are the two critical components for identifying the SE-SIM. Cer_{CDC} and the signature of the CDC provide a proof that these components are backed and guaranteed by a legitimate government issued ID card. $EC = ID_{SE}, PK_{SE}, Cer_{CDC}, SigSK_{CDC}(ID_{SE}, PK_{SE}, Cer_{CDC})$.

Step 10 – 11: The random numbers $R1 + 1$ and $R2 + 1$ are used by the MNO and SE-SIM respectively as tests of freshness. $R1 + 1$ and $R2 + 1$ are encrypted by PK_{MNO} and PK_{SE} respectively to provide confidentiality. The encrypted random values and the EC are sent to the NFC phone. Providing $R2 + 1$, is correct, the EC is stored in the SE-SIM.

Step 12 – 14: The encryption of $R1 + 1$ by PK_{MNO} and the EC are forwarded to the MNO for further authentication. The MNO can decrypt $R1 + 1$. If the check on the returned $R1 + 1$ is correct, it implies that the correct CDC card is being used for registration this is still true as the value of R1 is correct. Furthermore, by checking the certificate of the CDC (Cer_{CDC}) via the GCA's Certificate Revocation List (CRL) the MNO can determine if the CDC is still valid. After the check of Cer_{CDC} and EC, a new certificate is created for subsequent use in m-payment transactions. This certificate is called the certificate of EC i.e. (Cer_{EC}) and it includes extra customer account information and payment details associated to this service, such as the certificate's serial number (SN), expiry date (ED), transaction limits (TL) as well as PK_{SE}, ID_{SE} and ID_{CDC}. All this information is signed by the MNO's private key (SK_{MNO}).

Step 15 – 16: Finally the certificate of EC is sent back to the NFC phone. If the signature is correct the information is stored in the SE-SIM for use in the m-payment transactions.

B. Phase 2: NFC m-Payment Transaction

Given a successful endorsed registration from the previous phase, the customer phone/SIM is now ready to perform in-store m-payment transactions, in which a customer tries to perform an in-store m-payment through the authentication/verification of the MNO (that is endorsed by the CDC). On first entering the payment application, the phone shall automatically display the expiry date of certificate EC to the user, and payment actions will be restricted if Cer_{EC} is out of date. The general payment process is that a customer presents his phone close to the shop NFC POS, so the phone can present Cer_{EC} for an ID authentication of its SE-SIM, and if the check passes then EC is sent in addition with the payment information.

The MNO should already have EC and Cer_{EC} from the registration phase, and a personalised/unique secret key (MSK) for the customer SE-SIM. There is no secret key shared between the shop POS terminal and the customer SE-SIM, thus the shop POS relies on the MNO to verify the authenticity of the customer SE-SIM. The shop POS is able to verify the MNO signatures as it has access to the public key of the MNO (PK_{MNO}).

Step 1 – 2: The shop NFC POS first scans barcodes/RFID tags of the items to be purchased. The shop POS has a display of the total price of this purchase. The customer holds his phone close to the shop POS as the preferred method of payment and receives ordering information (OI) from the POS. The information includes the order number (ON), total price (TP) and date/time of OI (DT_{OI}). A given date/time of purchase is essential in any kind of payment transaction record.

Step 3: In this step there is a design option, as the user can be prompted for manual input e.g. a PIN, or alternatively

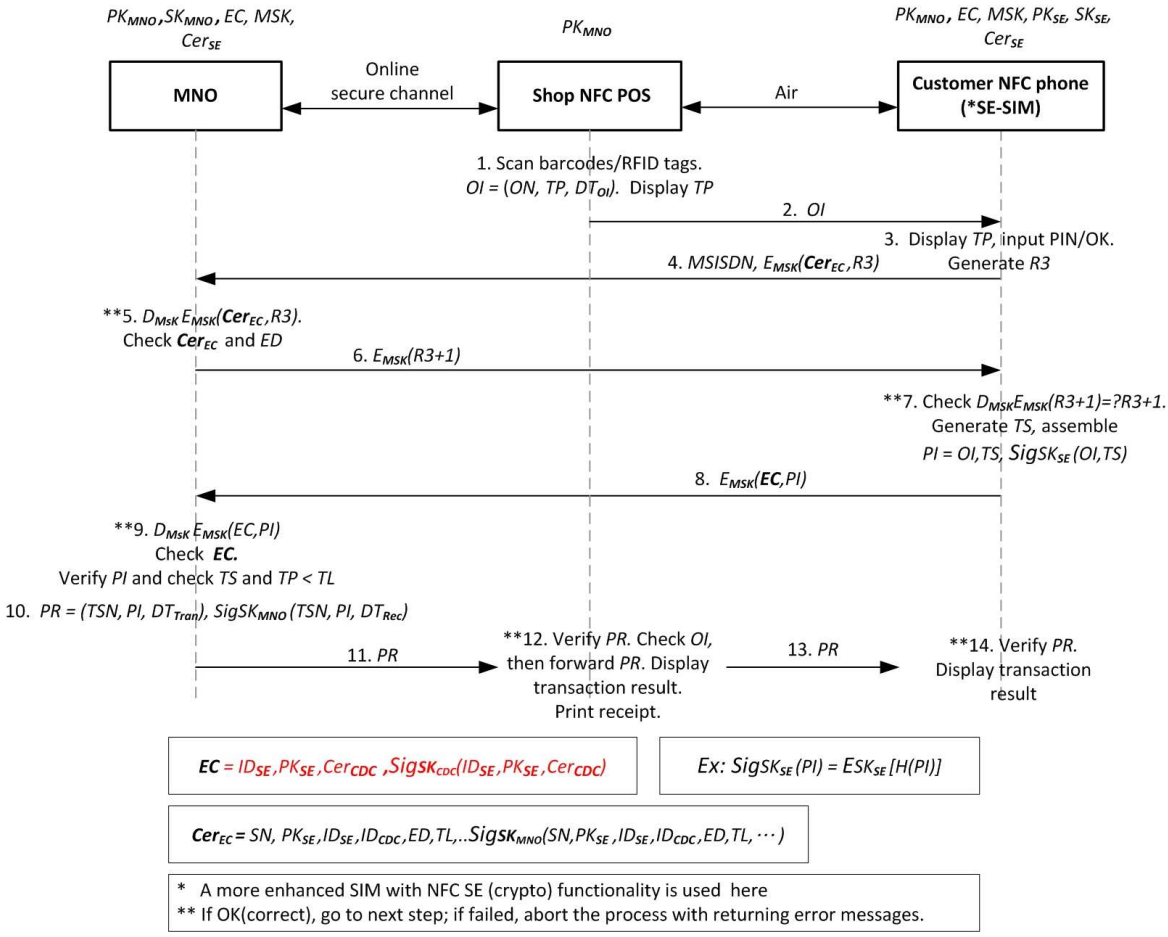

Fig. 2. NFC m-Payment with CDC – Payment Transaction Phase

the process could continue automatically for a faster/smoother transaction. The manual check prevents misuse of lost or stolen phones; whereas an automatic process can be faster and more convenient for customers. By displaying total price, the customer can be sure that the amount of money he would pay is correct. The SE-SIM then generates a random number ($R3$) that is used in subsequent authentication.

Step 4 – 5: The Cer_{EC} and $R3$ are encrypted under the personalised key (MSK) between the MNO and the SE-SIM and sent along with the Mobile Subscriber ISDN Number ($MSISDN$) (phone number) to the MNO, using the POS as a simple pipe. Using $IMSI$ instead of $MSISDN$ for added privacy is an option, however $MSISDN$ is perhaps more relevant to customers i.e. clearly indicates purchases made with the phone. In any case, the account details can be linked to the $IMSI$ or $MSISDN$ by the MNO, which means the MNO should know the SE-SIM's identity and the associated certificate created during endorsed registration. The MNO compares the received Cer_{EC} with the registration version and checks for expiry before continuing with the process.

Step 6: The incremented $R3$ is encrypted under MSK and sent back to the customer SE-SIM, using the POS and phone as a simple pipe.

Step 7 – 8: If the check of the incremented random number is correct, the SE-SIM can confirm that it is dealing with messages from the genuine MNO. The SE-SIM then generates payment information, $PI = OI, TS, SigSK_{SE}(OI, TS)$. The time stamp ($TS$) is embedded here to keep the freshness of the system. The customer SE-SIM signs OI and TS, to prove that this binding data is authorised and legally issued from the SE-SIM. In step 8, the PI and EC are encrypted under MSK (to preserve privacy) and sent to the MNO.

Step 9: EC is checked first after the decryption of the binding data from step 8. The MNO uses PK_{SE} from within EC for verifying the signature of the SE-SIM on the payment information. At this stage, the MNO has confirmed the identity of the customer and its signed PI. A check of time stamp (TS) is necessary to ensure payment messages are sent within an expected time, and a further check is made to ensure that the total price (TP) does not exceed the transaction limit (TL).

Step 10 – 11: After the verification of PI, the money is deducted from the customer's account. The MNO creates a payment result PR for this transaction. The PR includes the transaction number (TN), payment information and date/time of completed transaction, plus the MNO signature.

Step 12 – 14: The shop POS verifies the signature on

PR using its pre-stored MNO public key (PK_{MNO}). It then checks for the correct payment amount within OI. The POS then displays the transaction result on its screen and prints an itemised billing receipt (on paper). The customer phone also receives PR and then independently verifies and displays the transaction result. The same PR are expected to be shown on the shop POS and the customer phone as the final step in the transaction.

IV. PRELIMINARY ANALYSIS

A. Attack Scenarios

The protocol has been considered with respect to a number of attack scenarios which are outlined in this section. Note that RP and PP are used to indicate registration phase and payment phase respectively.

1) (RP) The customer could present a stolen CDC card during registration however the user PIN challenge would prevent this from being useful. An invalidated or expired CDC would also be detected by the MNO.
2) (RP) The use of the phone as a PIN entry device could create a vulnerability if the code could be tampered with, however the integrity of the phone application could be secured via the cryptographic functionality of the SIM card.
3) (RP) If the CDC to phone link could be eavesdropped during a normal registration then an attacker may attempt to discover the CDC PIN from the exchanged messages. Registration is intended to happen in a trusted environment although this cannot be completely guaranteed and the likelihood of attack increases if the CDC evolves to a contactless interface. Therefore, the protocol protects the transmitted PIN via encryption with (PK_{CDC}).
4) (RP) A dishonest customer could take a copy of the legitimate EC and Cer_{EC} and store in a second phone, however this should be of limited use as the original phone's SE (rather than that of the second phone) is bound within the credentials.
5) (PP) A dishonest customer or shop-keeper might attempt to send captured transaction credentials to try and charge purchases to another account, however the signature on new payment information will not be correct and the timestamp will be invalid on an old payment signature.
6) (PP) During an m-payment transaction a customer or shop-keeper might attempt to change the order information and correct payment, however this information is checked visually as well as within the transaction protocol.
7) (PP) It is unlikely that the MNO would attempt fraud due to the existing trust relationship with its customers; however customers would have some protection as legitimate transactions are required to be associated with signed payment information. This assumes that the SK_{SE} only exists within the SIM-SE.

B. Advantages and Disadvantages of the CDC Mobile Payment Scheme

Advantages: The benefits of the proposed protocol/system are listed below.

1) The customer NFC phone has an endorsed transaction credential (i.e. EC) stored in the SE-SIM, which is backed by the strong registration processes of the government ID card that has national recognition.
2) It is unnecessary for shops to be fitted with multiple proprietary MNO systems as the proposed solution offers flexible multi-MNOs service to customers.
3) Pre-storage of secret keys within the SE-SIM and the use of public key infrastructure minimise key distribution worries, and customer signatures ensure the authenticity and consent of purchase (i.e. non-repudiation).
4) Payment information (PI) is protected from being manipulated by the shop POS.
5) Customers do not need to bring additional ID or payment cards as the endorsed registration means that the handset can prove its authenticity and also that of the customer (if the transaction PIN option is used).
6) In general the solution offers a more reliant and widely recognised user registration process for mobile phone access to services.

Disadvantages: As well as the advantages mentioned above, there are also potential weaknesses that need further discussion.

1) With the current style of CDC card, an external contact smart card reader or a cradle is needed during endorsed registration. This is likely to limit registration to a trusted environment such as an MNO shop or government office, although it is probable that a contactless CDC interface will eventually be supported.
2) The payment process has been presented as on-line, although it is known that there are arguments for off-line support [3]. The endorsed credentials (which are at the core of the proposal) are considered equally valid for off-line use although there would be greater reliance on the attack resistance and integrity of the POS units. The credentials could also be used in a different kind of on-line transaction in which the customer scans his own purchases and transacts directly with the MNO over the cellular network.
3) A customer's MSISDN (phone number) is sent back in clear to the MNO for customer identification via the shop POS during a payment transaction. Although, phone numbers are not regarded as the most confidential of information when compared to secret keys for example, there is still a privacy concern that phone numbers could be linked with customer purchasing habits.
4) The speed and ease-of-use of a transaction system will determine whether it is successful. The proposed solution requires a number of cryptographic processes including PKI functions, which may stretch the capabili-

ties of limited resource devices such as security elements and mobile phones. A detailed performance analysis is planned as follow-on work.

5) The protocol uses PKI key-pairs for both encryption and signing purposes. Strictly speaking this does not follow best practice advice of using a key-pair for one purpose only, however this is also true of other major and widespread solutions such as credit card EMV chip and PIN transactions. Further key-pairs could be added, although this may have a practical impact on key storage and management.

V. Conclusion

In this paper, we proposed the binding of NFC mobile phone security technologies with the user identity security of the CDC card that is backed by a strong user registration process. The binding is achieved by an endorsed registration phase that cryptographically binds the PKI credentials of the CDC card and NFC phone in a way that is then nationally recognised. The credentials can then be used for in-store payment transactions to provide authentication, integrity and non repudiation, and without the user needing to carry any payment or ID cards. The solution, which is applicable to multiple MNOs, has a number of interesting features, although the implementation performance requires further investigation and this is currently the subject of a follow-on study.

References

[1] "Barclay Credit Card + Oyster Card" http://www.barclaycard-onepulse.co.uk/oysterCard.html

[2] W.D. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, J.H. Chiu, "NFC Mobile Transactions and Authentication Based on GSM Network," nfc, *2nd International Workshop on Near Field Communication*, pp.83-89, 2010

[3] W.D. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, J.H. Chiu, "Using 3G Network Components to Enable NFC Mobile Transactions and Authentication," *Progress in Informatics and Computing (PIC-2010)*, 2010.

[4] M. Massoth, T. Bingel, "Performance of Different Mobile Payment Service Concepts Compared with a NFC-Based Solution," iciw, *2009 Fourth International Conference on Internet and Web Applications and Services*, pp.205-210, 2009

[5] ISO/IEC 18092 (ECMA-340), "Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)".

[6] ISO/IEC 14443, "Identification cards - Contactless integrated circuit cards - Proximity cards".

[7] FeliCa www.sony.net/Products/felica/.

[8] ISO/IEC 15693, "Identification cards - Contactless integrated circuit cards - Vicinity cards".

[9] Stolpan, "Near Field Communication", 16th IST Mobile Summit 2007, Budapest, Hungary http://www.stolpan.com/uploadfiles/1_Mobilesummit2007_workshop.pdf

[10] Philips Semiconductors, "Near Field Communication RFID Workshop", 2006 http://www.rfidconsultation.eu/docs/ficheiros/Graber.pdf

[11] GSMA, "Requirements for Single Wire Protocol NFC Handsets", 2008 http://www.gsmworld.com/documents/reqs_swp_nfc_handsets_v2.pdf

[12] G. Madlmayr, J. Langer, C. Kantner and J. Scharinger, "NFC Devices: Security and Privacy", *Proceedings of 3rd International Conference on Availability, Reliability and Security (ARES '08)*, 2008.

[13] E. Haselsteiner and K. Breitfus "Security in Near Field Communication (NFC)". *Proceedings of Workshop on RFID Security(RFIDSec)*, 2006.

[14] Taiwan government public key infrastructure with CDC http://moica.nat.gov.tw/

[15] What is Citizen Digital Certificate http://moica.nat.gov.tw/html/en/what.htm

[16] M. Sonntag, "Electronic Signatures for Legal Persons" http://www.fim.uni-linz.ac.at/research/telework/ElSigLegalPersons.pdf

[17] S. Magnus and M. Maron, "A Public Key Infrastructure in Ambient Information and Transaction Systems" http://www.uni-koblenz.de/~maruhn/publications/gmr_2_09.pdf

[18] W. LIU, C. ZHAO and W. ZHONG, "The GPRS Mobile Payment System Based on RFID", *ICCT International Conference*, pp. 1-4, Nov 2006.

[19] H. Harb, H. Farahat, and M. Ezz, "Secure SMS Mobile Payment Model. Anti-counterfeiting", *The 2nd ASID International Conference*, PP. 1-17, 2008.

[20] S.L. Ghiron, S. Sposato, C.M. Medaglia, A. Moroni, "NFC Ticketing: A Prototype and Usability Test of an NFC-Based Virtual Ticketing Application," nfc, pp.45-50, *2009 First International Workshop on Near Field Communication*, 2009.

[21] S. Pradhan, E. Lawrence, A. Zmijewska, "Bluetooth as an Enabling Technology in Mobile Transactions," itcc, vol. 2, pp.53-58, *International Conference on Information Technology: Coding and Computing* (ITCC'05) - Volume II, 2005

[22] L.B. Bhajantri, S.S. Manvi, M.A. Vijayakumar, "Secure Mobile Payment System in Wireless Environment", *Proceedings of International Conference on Future Computer and Communication*, pp. 31-35, 2008.

[23] J. Meng and L. Ye, "Secure Mobile Payment Model Based on WAP", *Proceedings of 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM apos '08)*, pp.1-4, 2008.

[24] Y. Xu, X. Liu, R. Yao, "A Payment Model of Mobile Phone Based on Third-Party Security," Management of e-Commerce and e-Government, 2009. ICMECG '09. International Conference on , vol., no., pp.400-403, 2009