Distributed Identity for Secure Service Interaction

Mohammad M. R. Chowdhury, Josef Noll
UniK
N-2027, Kjeller, Norway.
mohammad@unik.no, josef@unik.no

***Abstract*—People rely on physical identities and computers to access today's numerous services. It requires having various identity cards and typing of a good number of usernames and passwords daily to prove one's identity to the remote services. These create inconvenience in use and significant security vulnerability. In this paper, we present a concept of digital identity and thereby accessing services to solve this problem. It uses the mobile phone as identifier to one's digital identity. An individual is expected to exercise the similar real world roles in digital world through the proposed identity mechanism. Our goal is to develop a system that is both secure and usable.**

Keywords-role; identity; authentication; service interaction.

I. INTRODUCTION

Identification is necessary to access various value added services from service providers. Interactions of these services are required to play certain roles of human being in life. Physical identities cannot be used while accessing services in the digital world. Moreover, different types of services require different types and forms of identifications. People increasingly use computers to do business over the Internet. But accessing today's web-based email, online value added services, or banking sites invariably requires typing various usernames and passwords for identification. These passwords can be captured and reused by hostile parties. To make the service access simple, hassle-free and above all secure, a unique identity entity is required from where user can retrieve the appropriate type of identifications.

Mobile phone penetration is expected to reach 100% in many of the European countries [1]. It has become a foremost electronic device for communication worldwide because of its mobility, seamless and secure access provision to networks. In addition to this, mobile phone has *always online* functionality. Day by day, more and more PC capabilities are integrated with mobile phones. Therefore, we focus on accessing the proposed identity and hence, services through Mobile Phone/SIM card authentication. The proposed identity mechanism has the potential to replace the present physical identities, usernames and passwords.

The paper will first postulate the need for a role based identity and illustrate its proposed generic architecture. It will then address the security aspect of this identity and justify why mobile phone has the potential to serve as an identifier. By introducing some service examples, it will discuss how service interactions through role based identity can be realized. The paper will provide a critical analysis on different aspects of proposed and other identity solutions. Finally, it concludes with the review of main points of this paper and comments on future research.

II. DIGITAL IDENTITY

A. *Human roles in life*

Every human being plays numerous roles in life to live. As a student, we are attending an education institute; as a researcher or engineer, we are working in a company; as a consumer, we are buying things with cash or credits; we are maintaining social relationships with family, relatives, neighbors and colleagues. While exercising these roles in life, we are interacting with many service providers to receive different types of services. Analyzing these scenarios, it can be said that every human being plays roles basically in three different areas, personal, professional and social areas. Therefore in reality, leading everyday life is nothing but playing some personal roles, professional roles and social roles.

B. *Real world to digital world*

To carry out these personal, professional and social roles, an individual needs to interact with many other people and many interfaces of numerous service points in the real world. During these interactions, we need to present our identifications to others that represent our identity in this world. Now-a-days, people are carrying a good number of physical identities, for example, passport/personal ID, credit cards, bank cards, student card, office ID, driving license etc. with them. In addition to these, a bunch of usernames and passwords are used everyday for identification to access many web sites and other electronic services which is very troublesome. Passwords are becoming increasingly unusable as organizations try to stay ahead of the hackers by making them more complex and increasing the frequency of changes. According to the predictions made by Gartner in its annual IT security summit 2005, 80% of organizations will reach a password breaking point [2]. Everyday, more and more real life services are available digitally. So, we are heading into an extremely worrisome world of identification. A unique identity mechanism needs to be developed in the digital realm where individuals would be able to control and manage their various digital profiles, assigning the appropriate attributes to each according to their context. In real world, it is difficult to selectively verify or reveal portions of one's identity: most forms of identification contain more information than is needed for any transaction. The identity system must disclose the least

identifying information possible, as it ensures the least possible damage in the event of a breach. It needs to be addressed while designing a unique identity mechanism. We are now thinking of such a system where every real life services are available digitally and can be accessed from anywhere by using digital identifications. Individuals need to practice the similar roles in the digital world that they are currently practicing in the real world. Therefore, a role based digital identity is proposed in this contribution.

C. Generic architecture of role based identity

Human roles already have been divided into three different areas, such as, personal, professional and social roles. In this article, we are proposing a concept of "My digital identity" that can be divided into 'My personal identity (PID)', 'My corporate identity (CID)' and 'My social identity (SID)' that would represent ourselves and our relevant real life roles to the digital world. 'My personal identity' can be used to identify ourselves in our personal and commercial interactions. Similarly, 'My corporate identity' and 'My social identity' can be used in our professional and interpersonal interactions respectively. Each of these three identities will have several identifiers. Each identifier will be used to access several relevant services and a number of attributes will characterize an identifier (see fig.1).

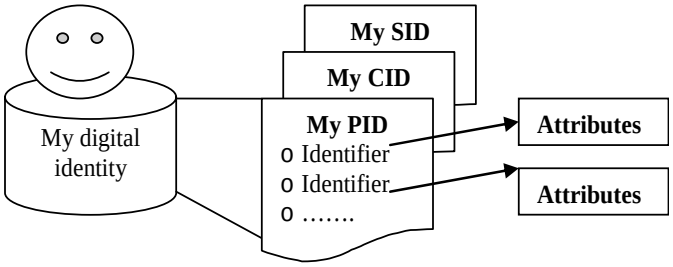

Figure 1. Architecture of "My digital identity".

Attributes are those set of characteristics of an identifier that are required by the service providers during service interactions. For example, passport can be one of the identifiers and name, date of birth, date of issue, date of expiry, the country that issued the passport, passport number etc. can be its attributes. The passport that is in fact a personal identity will be used to deal with governments electronically. Similarly, another identifier will be used to get access to financial services, like, buying something through credit cards. Attributes of such identifiers are name of the person who holds the credit card (may be optional), number of the card, pin code, date of expiry etc. My PID might have some more identifiers to access our home premises, home network or VPN etc. In the same way, My CID and My SID will have several such identifiers and attributes. My CID might hold the identifiers to access our office premises, office LAN/VPN etc. According to Dick Hardt, individual's interests, fondness, preferences or tastes are also part of his/her identity [3]. In the proposed identity model, these features will also be dealt with by My SID. It will also include my calendar, my address book, and identifiers for accessing my email, messenger, IP telephony etc.

Each identifier will contain only the required identifying information that a service provider needs to know. Each identifier will be used to access one or several relevant services. "My digital identity" thus, ensures the *minimum disclosure* of identifying information. This is how; an identity repository ("My digital identity") that will be placed partly in the network environment and partly in mobile phone SIM card, will possess our proposed identity. To enhance the security for service interactions, like, financial transactions, SIM card will hold some of the identifiers that require stringent security requirements. Therefore, SIM card is also a part of "My digital identity" only to interact some specific services. We are proposing that "My digital identity" can be accessed either by our very personal mobile phone (priority) or by our PC through fixed internet connection (optional). SIM card of the mobile phone will automatically identify us as the owner of "My digital identity".

D. Service interaction

Services have to be accessed through either of the IDs (PID, CID or SID) and their identifiers proposed. Identifiers and attributes can be added according to the user's service requirements. Owner of "My digital identity" can also include his/her own interests, fondness, preferences, address book, calendar in My SID. Therefore, personalization is an essential feature in such identity mechanism. User can control which of the attributes he/she wants to reveal while interacting services. These can make "My digital identity" a very much user centric. The data always flows from/through the identity with user's consent. There are mutual trust relationships between this identity repository and the service provider's websites or contents [4]. Therefore, disclosure of identifying relationship is limited to parties having trust relationships with "My digital identity". User can even downloaded the identifier with required attributes from "My digital identity" and stored temporarily at the memory of SIM to transfer users' credentials through Bluetooth or from NFC enabled phone to other NFC enabled devices [5], [6].

III. SECURITY INFRASTRUCTURE

Ensuring security to these identities (especially while doing financial transactions) is a burning issue, considering the fact that we are proposing to place part of this identity repository in the network that is vulnerable to electronic attack. It has been proposed in this paper that our mobile phone will act as the primary device to access "My digital identity". In addition to this, a part of the identity will be stored in mobile phone SIM card. Here, it is assumed that the user has the provision for 'always-on' functionality in his/her mobile phone. Fig.2 illustrates different levels of security against their security requirements.

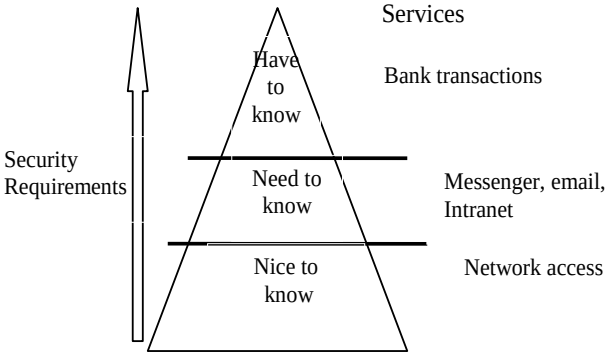

Figure 2. Security infrastructure based on security requirements.

Through a *nice to know* [5] authentication mechanism, user can access "My digital identity" and, through a *need to know* [5] authentication mechanism, user can access most other services, such as, accessing messenger (msn or yahoo), my address book, IP telephone (skype, voipstunt, telenor etc.), e-mail account; accessing home or office premises etc. using appropriate identifiers of My PID, My CID or My SID. *Nice to know* services are network access, where knowledge about usage is only required. *Need to Know* services have higher security requirements. Highest security requirements are required for *have to know* [5] services. Users have to be authenticated through a *have to know* authentication mechanism to use the identifiers that are required to access financial services, such as, bank, credit card etc. Here, we are proposing to deploy the *have to know* authentication mechanism in SIM card. Thus SIM card will be a part of "My digital identity". This will significantly minimize the possibility of disclosure of identities for financial services, in case there are electronic attacks on network contents of "My digital identity". To further enhance the privacy of attribute entries of the legitimate owner, identifiers of the above mentioned IDs will be visible to the owner but the attribute entries will not be. Owner can edit and add or delete the contents in the edit mode.

IV. MOBILE PHONE AS IDENTIFIER

A. *Acceptibility*

Now-a-days mobility of people increases due to dynamic life style and working nature. The mobile phone has become a foremost electronic device not only for communication but also for managing different other activities, such as, banking, collecting information from web, checking emails etc. Mobile phone penetration is expected to reach 100% in most of the developed countries. So, the basic infrastructure to use the mobile phone as identifier is already in place. Currently, different types of access systems can be found in wireless networks. Services are expected to be interoperable in different wireless communication systems. A SIM is a temper resistant device in a wireless system holding subscriber identity and authentication information. The SIM card in the mobile phone has the capability to provide all levels of authentication, and support mechanisms for revocation of credentials stored in the SIM card [7]. It is only active if authenticated by the network operator. If it gets stolen, the operator can disable the card. SIM card opens for authentication and encryption in every wireless network (Bluetooth, WLAN, WiMAX) in addition to GSM and UMTS [7]. So, SIM card enables authentication mechanism to interact different services will certainly give a technological edge to the development of future wireless technologies and services. By placing the identity repository in the network, we are reducing the volume of data transfer from mobile phone to network. In consequence, the additional data transfer due to the use of such system will leave a very little effect on the capacity of air interface. Therefore, the acceptability of mobile phone as identifier is expected to be very high.

B. *Extended SIM card authentication*

Currently, the SIM card provides the *nice to know* access to network. We propose that the SIM card authentication will also be enough to enter "My digital identity". The higher security requirements that *need to know* services may require might also be satisfied through SIM card authentication [5].

As proposed, the *have to know* authentication mechanisms will be realized in SIM card. Hence, we are introducing an *extended SIM card* (ESIM) that has the capability to hold multiple credentials. One will be responsible to provide the *nice to know* and *need to know* authentications and another one will store the *have to know* authentication mechanisms. Fig.3 shows the scenario of extended SIM (*ESIM*) card authentication in "My digital identity".

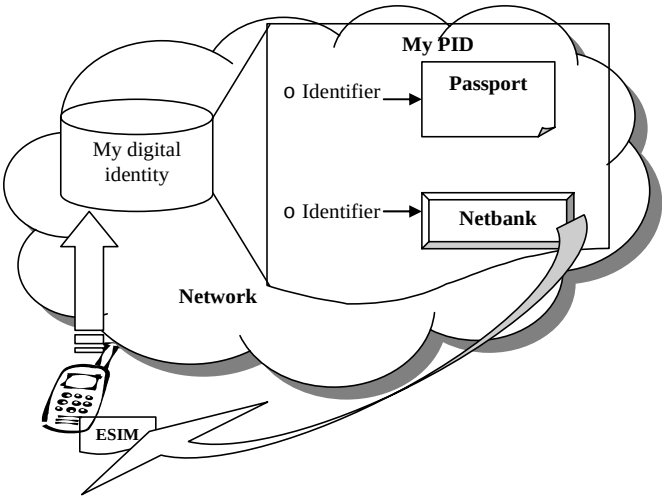

Figure 3. SIM card holds the *have to know* authentication mechanism.

Thus, *ESIM* will also be a part of "My digital identity" which will not be placed in network.

The *have to know* authentication mechanism in SIM card can be realized by implementing Public Key Infrastructure (PKI) [8]. In mobile networks, there exists a formal relationship between users/subscribers on one hand and the network operator of the other. Therefore, network operator can naturally play the role of Certification Authority (CA). The user's private key as well as the root CA public key can be distributed in a secure way in the form of SIM card. The formal relationship, which the operators already have through roaming agreement, could be extended to cross-certification of each other public keys. Mobile network operators therefore are in a very strong position to establish themselves as CAs, and the

mobile device naturally lends itself to become a secure storage medium for these cryptographic keys [9].

C. Service examples

A model service interaction scenario can be established through "My digital identity". Somebody wants to buy air ticket using his/her credit card from Lufthansa. The action is performed through the following steps (see fig.4):

1) "My digital identity" is accessed from mobile phone.
2) Lufthansa.de is accessed and request is made to buy an air ticket.

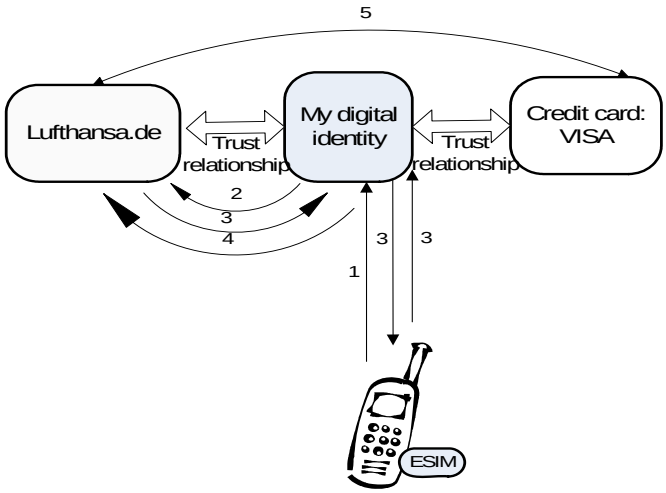

Figure 4. Purchase of air ticket by "My digital identity".

3) Lufthansa.de asks for credit card identity from "My digital identity" for payment. At this point, the payment requires the use of *have to know* authentication mechanism from owner's mobile phone SIM card (*ESIM*). SIM card performs the necessary authentication that results a payment receipt.
4) "My digital identity" sends the receipt to Lufthansa.de.
5) Lufthansa.de checks this receipt of payment with credit card authority, for example, VISA for validation.

This is how; a person can buy air ticket from airlines websites using his/her digital identity repository.

Fig.5 illustrates another service example. Here, somebody wants to access bank account using NetBank while on the way. He/she wishes to check account balance or see the last several transaction records or transfer some money to other account or to "Mobile purse" [10]. User can log into "My digital identity" using *nice to know* authentication mechanism (SIM), thereby MyBank in My PID using *need to know* authentication (SIM) and can transfer money to a different account using *have to know* authentication (SIM+PKI). This is how; ESIM plays its role during authentication. User may even check account balance or last transaction records with *need to know* authentication. Somebody even wants to load electronic cash to mobile phone while he/she is on the move. Funds can be transferred from bank account into his/her mobile purse with *have to know* authentication.

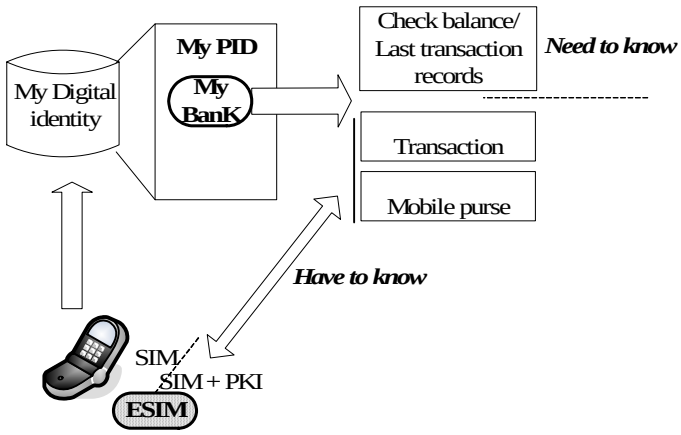

Figure 5. Access of MyBank through "My digital identity" using mobile phone authentications.

Funds can be transferred from bank account into his/her mobile purse with *have to know* authentication. The money in mobile purse corresponds to cash. A SMS message will be sent to the service number given by the merchant with the key word of the product or service user wish to buy from mobile phone. The payment is debited to the purse instantly, and the merchant can verify the payment immediately as well.

V. ANALYSIS

In the "Laws of Identity", Kim Cameron states that any sustainable and universally adopted identity architecture must only reveal the least identifying information possible with the user's consent [11]. In the proposed identity mechanism, user controls how much identifying information it would reveal to the service providers. As the services are accessed through relevant identity (PID, CID or SID) and their relevant identifiers, minimal disclosure of only necessary identifying information with user's consent is ensured. Accessing this identity through mobile phone provides the major advantage over the other available identity mechanisms. Mobile phone acts as a primary identifier to "My digital identity". It is available 24 h/7 days a week, as compared to about 4 h average usage of a PC. Thus, it provides the always online functionality with availability. As, SIM card may also provide *need to know* authentication, some services that require minimum security can be available to the users as soon as they enter the proposed identity repository by mobile phone. Deployment of *have to know* authentication mechanism in SIM (*ESIM*) not only enhances the security to access financial services but also increases the acceptability of this identity to users. Another very useful feature of such identity concept is portability of identifier from one device to another, especially to the devices that has no direct connectivity to "My digital identity". Thus, this identity can be accessed from anywhere and service continuity is possible in heterogeneous wireless environment. In case of losing or theft of SIM, we can use our PC to access "My digital identity" which is an optional access possibility to "My digital identity". It obviously requires some security modification or enhancement.

The proposed identity mechanism will certainly create values for the users, network operators and service providers.

User can use a unique identity mechanism that is simple, easy to use, digital in nature but available anywhere and portable to any device. It has the potential to replace all the physical identities in the real world. Network operators can also earn revenues by providing space for the repository and through the additional data transfer requirements. Users can access service readily. As there are trust relationships among the parties involved in transactions here, the possibilities for fake transactions will be reduced significantly. Once "My digital identity" repositories are known to the service providers, new offers can even be posted directly to these repositories.

SXIP [12] and Windows CardSpace [13] are two identity solutions developed by Sxip identity and Microsoft Corporation. In SXIP, membersites are typical websites that consume identity data by sending SXIP requests for user data to homesites, also websites that store user identity data. Homesites authenticate and identify users. It uses two-factor authentication solution to access services, like, online banking that requires strong authentication mechanism. SXIP 2.0 can use a third party credentials which is an interesting way to hide the use of PKI behind a software layer. Windows CardSpace uses a variety of virtual cards, each retrieving security token from the identity providers for authentication and identification to services. For greater security, user protects cards with personal identification number (PIN). To provide further assurance of secure communication, Microsoft together with other partners in industry is expected to create a new level of certificate that might contain more information than a traditional Secure Sockets Layer (SSL) certificate. These two identity solutions provide the movement of identity data over the internet. In addition to effortless movement of identity over the internet, the proposed mechanism supports the portability of identity data among the devices. Authentication and identification provided by the SIM card is the principle distinctive feature of it. To reduce the security vulnerability *have to know* authentication mechanism has been moved to SIM card. The web PKI suffers from insecure distribution and storage of cryptographic keys and therefore does not provide a complete chain of trust [9]. By combining the roles of CA, mobile network operators would make it easier to have a complete chain of trust around PKI because there already exists a trust relationship between mobile network operators and their customers. Gemalto, one of the leading digital security providers, is using high capacity SIM card for storing digital certificates or rights [14]. The identity repository can be used instead to store these rights that can be accessed through mobile phone. Thus, some overheads during data transfer can be avoided. The mechanism also ensures the portability of rights. There are many identities based on chip cards, like, memory cards and smart cards [15]. There are multiple chip cards, provided by multiple entities and single chip card, shared by few entities. If the proposed identity repository is available in the network which can be accessed anytime and from anywhere through an *always online* mobile phone, such various identity based chip cards might not be necessary at all. User just needs only one smart card, *ESIM* card.

VI. CONCLUSION

The paper introduced a new concept of a digital identity, its security infrastructures and service interaction mechanisms. Part of the identity is placed in the mobile phone SIM card instead of putting it in the identity repository in network to meet the highest security requirements. Authentication to this identity and thereby service access using mobile phone is one of the main features of this concept. The paper also explains several service examples using the proposed identity mechanism. The concept of a unique identity repository in the network will obviously enhance the user experience in seamless service interaction in heterogeneous wireless networks. In our future work, we will focus on establishing a use case on seamless user experience in heterogeneous wireless networks.

ACKNOWLEDGMENT

The contribution is a part of an ongoing research in WP2 of SWACOM project, funded by The Research Council of Norway. The authors would like to acknowledge the contributions and supports provided by their colleagues from UniK, Kjeller and Telenor R&D, Fornebu, Norway.

REFERENCES

[1] Telecommunication Statistics, "OECD key ICT indicator", http://www.oecd.org/

[2] Gartner, www.gartner.com

[3] D. Hardt, "Identity 2.0", OSCON 2005, http://www.identity20.com/media/OSCON2005/

[4] RSA Security, http://www.rsasecurity.com/

[5] J. Noll, J.C. Lopez Calvet, K. Myksvoll, "Admittance services through mobile phone short messages", Proceedings of the International Conference on Wireless and Mobile Communications ICWMC'06, July 29-31, 2006, Bucharest.

[6] J. Noll, U. Carlsen, G. Kalman, "License transfer mechanisms through seamless SIM authentication", International Conference on Wireless Information Systems, Winsys 2006, 7.-10. August 2006, Setubal, Portugal.

[7] J. Noll, "Services and applications in future wireless networks", in press, *Telektronikk*, Q4/2006.

[8] J. Markovski, M. Gusev, "Application level security of mobile communications", Proceeding of the 1st International Conference on Mathematics and Informatics for Industry MII 2003, Thessaloniki, Greece, April 2003, pp. 309-317.

[9] A. Jøsang and G. Sanderud, "Security in Mobile Communications: Challenges and Opportunities", In the proceedings of the Australasian Information Security Workshop, Adelaide, Australia, February 2003.

[10] Nordea Bank PLC, Finland, www.nordea.fi.

[11] K. Cameron, "The Laws of Identity", http://www.identityblog.com/

[12] The Simple eXtensible Identity Protocol, Sxip, http://sxip.net/

[13] Windows CardSpace, http://cardspace.netfx3.com/

[14] Gemalto, a leading digital security provider, http://www.gemalto.com/

[15] Senthil Sengodan, "On secure mobile identity provisioning", Wireless World Research Forum Meeting 15, 08-09 December 2005, Paris, France.