Strong authentication with mobile phones

Janne Kaavi
Helsinki University of Technology
jkaavi@gmail.com

Abstract

Many of the services that we use daily, for example banking, have transformed from traditional customer services into Internet services. In important services, such as the banking, a strong authentication is needed to protect both the users of the services and the service providers.

Due very rapid techinical progress mobile web browsing has become possible. Modern phones with big and sharp touch screens have made it also usable. Therefore, all our daily internet services could be accessed with mobile devices from wherever we are. Because of this strong authentication methods that can be used with mobile phones are needed.

At the moment strong authentication in Finland relies on TUPAS -authentication. It is a good method but has also some drawbacks like dependency on the banks and the difficulty of using with mobile devices. In this paper I describe four promising methods for acheiving strong authentication with mobile devices. The methods are SMS-OTP, Mobile certificate, NFC and On-board Credentials. The approaches of the methods differ greatly from each other, nevertheless all of those can be used for achieving the goal of usable strong mobile authenticaion. Methods are compared to each other from both service providers and users point of view.

Keywords: Strong authentication, Mobile authentication, SMS-OTP, Mobile certificate, NFC, ObC, On-board Credentials

1 Introduction

The majority of our daily business has moved to the internet: banking, insurances, government systems etc. Online shopping is growing rapidly and even grocery stores are launching internet services which offer home delivery. At the same time traditional customer service points are being shut down. In 1980, there were over 3500 bank offices in Finland, now the number is a little over 1600 [9]. Dispite the fact that the rapid decrease has ended, still long distances, long queuing times and short opening hours of the customer service points are driving people into using internet services. When services that contain sensitive data are moved to internet, strong authentication is required to protect both the service provider and user of the service. In Finland, the most commonly used strong authentication method is TUPAS. It was created by Federation of Finnish Financial Services and it is *"a common way to authenticate web customers for third party services with the same IDs that are used to authenticate customers in the web bank service"* [26].

There are three basic types of authentications. The most common one is authentications based on something that one *knows*, usually a password. The second category is authentications that are based on something that one *has*, like a smart card. And the third category is based on something that a person *is*, an immutable personal characteristic for example a fingerprint. There is no standardized or official definition for term *strong authentication*, but often, also in this paper, it is defined as an authentication that uses two out of those three mechanisms [21]. An example of strong authentication in use is withdrawing money from an ATM, which requires you to *have* your ATM card and to *know* your pin code. The other example is the above mentioned TUPAS. It requires you to *know* your customer number and to *have* a list of one time passwords provided by your bank.

It is possible to use mobile devices for strong authentication of users in similar situations to those in which TUPAS is now used. The authentication can technically be implemented in many different ways using a mobile device and the SIM card within it. In this paper, I study different methods that could be used for achieving similar strong authentication to that which TUPAS provides but by using mobile devices. I will describe how the methods generally operate and are used. The focus is on studying those methods from service provider's and end-user'spoint of view: difficulty and costs of the deployment and usage, and the usability of the system.

At the end of this paper I compare those different methods to each other and also to TUPAS. The comparison concentrates mainly on non-technical aspects such as costs of using and experiences of the usage. TUPAS is good base for the comparison, even though it is not a mobile authentication method, because it is currently in use. Mobile authentication is not going to replace TUPAS any time soon, nevertheless any new system should be better than its predecessor.

2 Background

Finland has been forerunner in mobile communications. In the early days of mobile communications in mid 90s there was nearly 50% yearly growth in mobile subscribers. In the year 2005, the number of subscribers exceeded the number of people in Finland and nowadays there is about 115 subscriptions per 100 persons [25]. A report from Ericsson in summer 2010 states that worldwide mobile subscriptions had reached 5 billion and that the growth is 2 million new subscribers per day. They estimate that there will be 50 billion connected devices by year 2020 [7]. Now almost everyone has one mobile device that is connected to the network. Ten years from now everyone has more than five such devices.

Mobile devices are here to stay.

In addition to the huge growth in number of subscribers, another rapid change has been going on in the area of mobile communications. Mobile phones have transformed into something much more. Modern mobile devices are much closer to a computer than to a phone; the main functionality is not making phone calls. These devices are typically called smart phones or mobile computers. This technical development has created many new opportunities for what can be done with mobile devices. People can use their email, browse web pages, use social media services, take photos, record videos and so forth. Web browsers have been in smart phones for years, but using those has been really difficult. Modern phones with big and sharp touch screens have made mobile web browsing not only possible, but also usable. Because of all this, there really is a growing need for good mobile authentication methods.

Mobile authentication methods already exists and are employed in many European countries, for example in Sweden, Norway, Slovakia and Italy [2]. In Finland, the area of mobile authentication has been studied and developed for several years, but still mobile authentication is not available here. Finland is no longer forerunner.

It is possible to use TUPAS with mobile devices, but that is difficult from the users point of view. Using mobile devices directly for authentication would have many benefits:

- Because everyone already has a phone, there is no need for additional devices like smart cards.
- Practically all Finns have a mobile phone and they carry it with them almost all the time. Therefore authentication could be used whenever and where ever it is needed. This is not the case for example with TUPAS password lists, which are often stored at home.
- The mobile network allows connection only to authenticated phones which offers some basic security, for example using copied SIM cards is hard.
- Roaming and interoperability in mobile communications are in use in all over the world. Same mobile authentication methods could be spread around the world to allow using the same methods also abroad.
- These kinds of systems are already in use, thus those are proven to work.

In addition to strong authentication, many other kinds of useful functionalities could be added to mobile devices. For example there is lot of research in combining the functionalities of a wallet and a mobile phone: incorporating for example travelling cards, bonus cards, gift tokens and even credit cards to a mobile device. Then the paying could be done by keeping the mobile device near of a reader. In some countries, for example Japan, these kinds of systems are already in wide use. [2]

These different types of mobile services could be beneficial to each other, because many people do not realize that mobile phones are not just for making phone calls anymore. New different kinds of applications will widen the space of things that people think that can be done with these mobile devices.

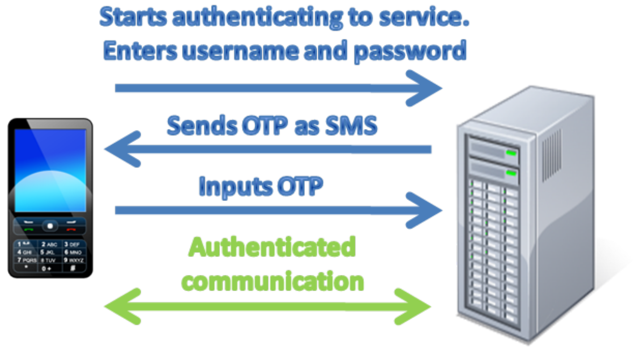

Starts authenticating to service.
Enters username and password
Sends OTP as SMS
Inputs OTP
Authenticated communication

Figure 1: SMS-OTP authentication with a smart phone

3 Methods for strong mobile authentication

3.1 Sim card based

One viable approach for strong mobile authentication is to use the SIM card that is found within every mobile phone. SIM (Subscriber Identity Module) is a removable small smart card that contains the International Mobile Subscriber Identity (IMSI) and small pieces of software. IMSI is a 15 character code that mobile networks use for identifying subscribers. Also other information, for example user's phonebook, can be stored to a SIM card. [15]

Most important and obvious benefit in this approach is that there is no need for any additional hardware, like a card reader, and some cases no need for addition software either. If software or data is required, it can be distributed within the SIM card and thus users do not need to install any additional software into their devices. This makes things much easier from the user's point of view.

SIM cards also have some features that improve security. Mobile network authenticates every connected device using the IMSI code. Even though cloning a SIM card is possible, using a copied SIM is much harder because the network does not allow multiple devices to connect with the same IMSI. In addition, information stored on SIM card is protected by four characters long PIN codes. The four character code is definitely too short to protect from brute force attack, but still an simple brute force attack is infeasible because data will be locked after few wrong attempts and thus cannot be used after that.

3.1.1 One time password using SMS

The SMS one time password (SMS-OTP) is a simple idea that can be used for two factor authentication. It is based on password that is generated by the service provider and transmitted to user using the SMS service. The password is fairly short and is valid only once and only for a short period of time. This kind of system is being used in many services, for example some ebanks [5] [12].

Usage

The service provider sends SMS messages to the user, and therefore the service provider must know the user's mobile phone number. The number is typically entered when the user registers to the service. Figure 1 illustrates one scenario how SMS-OTP can be used. First phase of the authentication happens by entering the typical credentials like a username/password pair. With those credentials the service provider recognizes the user, generates the OTP and sends it to user as SMS message. Finally the user enters the code to the service and then the user is strongly authenticated. [23]

This is not the only way to use SMS for authentication. For example a Finnish bank called Nordea uses SMS for confirming transactions that are detected to be *unusual* by sending a confirmation request SMS message to the user. The transaction will not be carried out before the user has answered to that message with letter "A". [18]

Service providers that would like to start using SMS-OTP can either buy it as a product or a service from a company offering it, for example, VISUALtron MobileKey [4] or TeleSign's Two-Factor Authentication. TeleSign's Two-Factor Authentication also provides possibility of using a voice call for delivering the OTP [24]. Other possibility is implementing it by themselves since it is fairly simple because all it needs is a device that is capable of sending SMS messages.

Advantages

There are many good things in SMS-OTP. The most important one is that it can reach practically everyone. Using it does not require any additional hardware or software or even any changes to the SIM card. Therefore everyone who has a mobile device capable of receiving SMS messages could straight away start using SMS-OTP as authentication method.

The costs of the system for the service provider are fairly low because SMS messages are very cheap and SMS-OTP system is simple to implement. For the users SMS-OTP is typically free since receiving SMS messages does not cost anything.

In addition from the user's point of view SMS-OTP is very simple and easy to understand. Even totally non-technical users can understand why it adds security because SMS messages are typically considered to be private.

Problems

There are also problems in the SMS-OTP approach. Many mobile phones (Nokia S40 phones, old iphones etc.) do not support multitasking, i.e. they cannot run multiple applications at the same time. Therefore, if the user is authenticating to a service using mobile devices web browser and the service sends an SMS message, the user might not be able to read it without closing the browser. After the browser is closed, the SMS is useless. Even if the phone supports multitasking, using SMS-OTP might be difficult in some devices. User has to open another application to read the message and then memorize (or write down) the password and then switch back to browser and enter it. [2]

One possible solution for the above-mentioned problem is Flash SMS, which is a SMS that is displayed directly on the phone's screen [28], but it is also problematic because displaying of Flash SMS is not guaranteed in all phones. The message is not always automatically stored to phone so it could work poorly also in phones that do support multitasking. [2]

There are also potential security issues with the SMS-OTP. Firstly, all the mobile phone operators between the service provider and user become part of the trust chain and thus need to be trusted. In case of roaming there are multiple operators. Secondly, SMS encryption can be decrypted by an attacker and therefore SMS-OTP cannot be totally trusted [17].

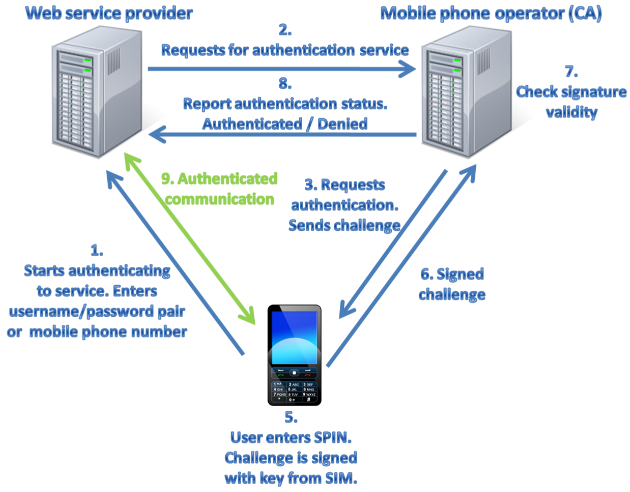

Web service provider
Mobile phone operator (CA)
2. Requests for authentication service
8. Report authentication status. Authenticated / Denied
7. Check signature validity
9. Authenticated communication
3. Requests authentication. Sends challenge
1. Starts authenticating to service. Enters username/password pair or mobile phone number
6. Signed challenge
5. User enters SPIN. Challenge is signed with key from SIM.

Figure 2: Mobile certificate authentication with a smart phone

3.1.2 Mobile certificate

Mobile certificate is an add-on service to a mobile subscription which purpose is to make mobile authentication not only possible but usable. Both service providers and users will have to pay for the service. It is based on Public Key Infrastructure (PKI) and the keys and certificate are stored to user's personal SIM card. The certificate contains a unique personal identifier, for example social security number and permanent personal details: name, birth date, gender and nationality. The mobile phone operators function as PKI Certification Authorities (CA). [2]

Conceptually Mobile certificate is close to the electronic identity card which is one of the previous failed attempts for achieving widespread use for an e-authentication method in Finland. In summer 2008, only 180 000 Finns had a electronic identity card. The goal was to have 1.7 million users at that time.[6] One of the possible reasons for the previous failures might have the difficulty of taking the method into use. For example, the electronic identity card must be personally applied and retrieved from the police. In the other hand, Mobile certificate has taken this into account. Even though almost everyone has a SIM card, from Mobile certificates point of view it is not sufficient because by default SIM cards do not contain the needed information. The new SIM card must be requested from the mobile phone operator, but that can be easily done via the operator's web service. [27]

Usage

As with the SMS-OTP, when a user is authenticating to a service that offers Mobile certificate as authentication method, the service provider needs to know the user's mobile phone number. This can be given either once when the user registers to the service, or every time the user authenticates to the service.

Figure 2 illustrates the whole authentication process. When user is authenticating, the web service provider requests authentication service from a Certification Authority, which is the user's mobile service provider. Based on the user's cell phone number, the request is sent to a correct CA. After receiving such request the CA sends authentication request containing a challenge to the user's mobile phone. Then user enters a PIN number, called SPIN, which unlocks the secret key stored within the user's SIM card. Next the challenge is signed with the user's secret key and sent back to the CA. After receiving the challenge back, the CA can check whether the challenge was signed with the right key or not. Then the CA sends information about the authentication to the web service provider and if the key was OK the user is now authenticated. The SPIN is not the same PIN as is used for locking the phone and for security reasons it is not preset to be 0000 or 1234 [1].

Mobile certificate can also be used for authenticating customer during a phone call. In addition to that, authenticating is not restricted to situations when user is using the mobile device for accessing the service. Separate computer can also be used, which is in fact the more typical use case. In that situation the communication between the user and the web service provider go through user's computer and communication between the user and the CA go through user's mobile phone. Everything else is identical to the situation in figure 2.

Advantages

As mentioned earlier, SIM based approaches are easy from the users point of view. With Mobile certificate, all that the users need to do is to acquire new SIM card from their mobile phone operator and after that the Mobile certificate can be used. Using the system is also simple, just enter the SPIN when requested.

Event though Mobile certificate was designed and developed by the biggest Finnish mobile phone operators: DNA, Elisa and TeliaSonera Finland, also the needs of Finnish banks were specially taken into account. The banks could easily start using mobile transaction certificate side by side with the current TUPAS system.[10]

The opportunity for using Mobile certificate during a phone call is also important benefit. This could be a very useful feature for example in customer services of banks and insurance companies where sensitive data might need to be exchanged over phone.

Problems

As mentioned above, Mobile certificate will be non-free service for the users and the service providers. Because the service is not yet deployed there is no information about the prices, except that the prices will be determined by the mobile phone operators who are offering the service. The pricing will have big impact on the rapidity of the deployment.

In addition it is possible that when the service is used entirely with mobile phone like in figure 2, Mobile certificate method suffers from similar problems in non-multitasking environments as the SMS-OTP.

It was announced that the first consumers should be able to get the SIM cards supporting the certificate during year 2010. But in the last quarter 2010, release date or any details has not yet been published. [1] Therefore it seems that consumers will not get their certificates during this year, and no service can use Mobile certificate as authentication method.

3.2 Near Field Communication

Near Field Communication (NFC) is a wireless short-range communication technology which is based on *Radio Frequency Identification (RFID)* technology. RFID is the technology that is used for example in Finnish public transportation system travelling cards. NFC technology can be, and has successfully been, integrated to mobile phones. In 2005 Vodafone sold the world's first NFC phone. [11] From the field of modern smart phones Nokia C7 is an example of a device containing NFC chip [16].

Mobile phones with NFC open many very interesting opportunities. Such devices can be used to replace for example physical keys and bonus cards. Nevertheless, from the mobile authentication point of view the most interesting possibility is that NFC allows the mobile phones to function as smart card readers. Some of the current credit cards are so called contactless credit cards, which can be read remotely with a RFID reader. With NFC chip mobile phones can act as such readers, and thus credit cards can be read by using a mobile phone.

> *Mobile phones are about to become the biggest RFID reader infrastructure in the world [11].*

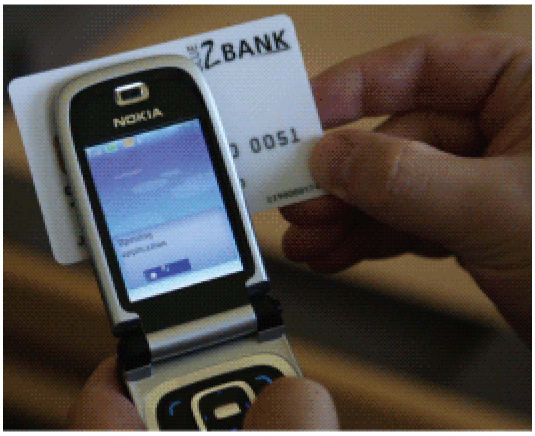


Figure 3: Mobile phones can act as credit card reader [13].

Usage

The opportunity to use mobile phone as smart card reader makes it also possible to use NFC as an authentication method. Procedure for authenticating to an ebank using mobile phone with NFC and contactless credit card is as following [19][13]:

1. User visits web site of the ebank and request a challenge number from the bank by entering a personal customer ID.

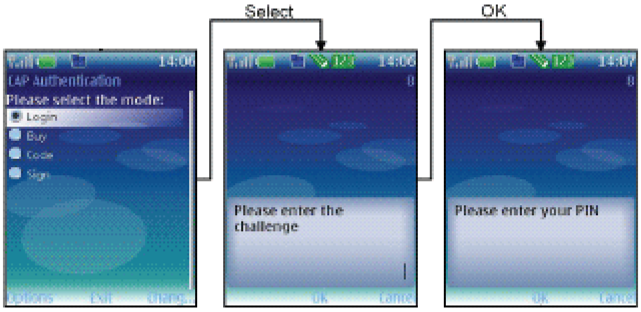
2. User starts reading a credit card with a mobile phone by touching the back of the phone with the card. *See figure 3.*

3. NFC can be used for many other things in addition to authentication. Therefore the user must then select which function to use. *Left box in figure 4.*

4. Enters the challenge received from bank. *Middle box in figure 4.*

5. Enters the PIN code of the credit card. *Right box in figure 4.*

6. Receives a code as response. That code can be used for authenticating to a web service.



CAP Authentication

Please select the mode:

Please enter the challenge

Please enter your PIN

Figure 4: Authentication using a credit card and a mobile phone with NFC. [13].

Advantages

The main idea of the NFC is not authentication; it is just a side product. The real strength of the NFC technology is the huge variety of different things that can be achieved with it, which improves the chance of getting NFC widely deployed.

Problems

There are at least three notable issues in using NFC for authentication. Firstly, the usability of this method is fairly poor. It contains multiple steps including visiting the service provider site, entering customer number, challenge and PIN code and holding a credit card near the phone.

Second issue is the availability. Only some of the current mobile phones contain a NFC chip. It will take many years before majority of devices contain the chip, and therefore NFC based solutions cannot be taken into wide use before that. The lack of RFID cards also prevents using NFC. In 2006 about 20 million consumers in the United States had a contactless credit card [20]. I could not find any Finnish bank offering such cards to Finnish customers.

And the third is security and privacy from the end-users point of view. There has been discussion about issues of RFID credit cards. Because of the fact that the cards can be read remotely, also criminals can read those remotely. Attacker with RFID reader can harvest information from the cards just by wandering in a crowd of people. The harvested data can be used for at least compromising the privacy of the people, but potentially also for more serious attacks.[20].

3.3 On-board Credentials

On-board Credentials (ObC) is an architecture that utilizes general purpose hardware to achieve inexpensive, open and secure way of storing and using credentials. An ObC credential consists of some secret data, most typically keys, and an algorithm that operates the data [8]. An application that implements ObC can be installed to a mobile device that meets the requirements *(see section 3.3.2 System requirements)* of ObC. Service providers can independently define and share new credential secrets to users' devices. The ObC application protects the credentials that are stored to the device and the users can use the credentials to authenticate themselves to service providers services.

3.3.1 Challenges in software based approaches

Approach based on an application within a mobile device is not trouble free either. First of all, many of the modern mobile devices are multitasking environments. This means that multiple applications can be running at the same time and share the resources provided by the hardware. Because the applications are running at the same time, it is sometimes possible for a application to read memory areas that are allocated to an another application. For secure applications, this is naturally a serious problem. For example, consider an application that stores some secret data, like passwords, as encrypted. When the application is being used, the data must be decrypted and it must exist somewhere within the memory of the device as decrypted. If some other application can read the data from the memory while it is decrypted, then the security has failed and the secret is lost.

Someone might ask why and how there could be a malicious application that tries to steal data on my mobile phone. As stated before, mobile phones are not just mobile phones anymore. The users can install all kinds of applications from many different sources to their mobile devices. And not all of those can be trusted. Recent study about Android application stated following:

> About 20 percent of the 48,000 apps in the Android marketplace allow a third-party application access to sensitive or private information [3].

The worst part of that is that Android marketplace is an official application source that most people consider a trusted source.

It is also likely that someday automatically spreading malware, similar to computer viruses, becomes a problem also in mobile devices. For these reasons ObC has minimum requirements for the mobile devices.

Secondly, there are a lot of different mobile devices. Making an application that works properly on all mobile devices is practically impossible. Therefore, all devices cannot be supported and the application must be designed to some specific group of devices.

3.3.2 System requirements

The initial goal of ObC was to *"minimize the cost of implementing and deploying the ObC system"* [8]. Naturally, the goal of security is something that could not be bargained for. Therefore, ObC requires that the device contains a proper secure execution environment. The goals of security and low costs could both be reached by relying on general purpose secure hardware that is already widely deployed in mobile devices. The disadvantage is that ObC cannot be used if the device does not provide such execution environment. ObC architecture states three requirements for an secure execution environment [14]:

- ***Isolated secure execution environment**: It must be possible to execute trusted code isolated from the untrusted code executing on the same device.*
- ***Secure storage**: It must be possible to store persistent data so that confidentiality and integrity of the data can be assured.*
- ***Integrity of secure environment**: It must be possible to ensure the integrity of the secure environment.*

Such secure environments do exists and therefore it was not neither necessary nor cost efficient to design new one[14]. An example of such environment is Texas Instruments' M-Shield, a mobile security technology solution that is available for the OMAP platform that is used in mobile devices. Many Nokia high-end phones have built-in M-Shield. It provides for example cryptographic accelerators, a random number generator and secure on-chip keys and thus many cryptography related applications can utilize it and receive improved performance and security.[22] ObC can also be implemented on top of other secure environments than the M-Shield [14].

3.3.3 Architecture

After inexpensiveness and security, openness was the third important goal of ObC. Openness in ObC means that any service provider is allowed to create and to provision new secrets and credential algorithms without having to obtain permission from any third party. Naturally, this must be possible without compromising the security of the system. Therefore the ObC system had to be designed so that malicious or erroneous credential algorithm cannot cause serious harm to the system. This raised two requirements which had to be taken into account in the architecture design of the ObC [14]:

- Secret data must be isolated from the credential programs.
- System resource, like CPU time and memory, consumed by credential programs must be monitored and controlled.

Figure 5 represents a simplified architecture of the ObC. A mobile device which meets the above mentioned requirements can be split into two different environments: Normal execution environment where all normal applications are running, And secure execution environment which is used only for some specific security demanding tasks. Both environments have their own CPU and memory. Typically the resources provided by secure execution environments are very limited. For this reason all of the main elements of ObC cannot be within the secure environment.

In fact only small part of ObC operates within the secure environment: ObC provisioning subsystem and ObC Interpreter. In addition very small amount of data is being stored within the secure environment memory. Most important piece of that data is a device specific master key called *ObC platform key (OPK)*. *ObC Interpreter* is the key element for achieving the required isolation between credential programs and the secret data. It provides a virtualized environment where the programs can be run. The OPK key is used by the ObC Interpreter and it will never leave the secure environment. *ObC provisioning subsystem* handles the credential provisioning functionality. It is separated from the interpreter for achieving smaller memory requirement for the interpreter and thereby leaving more space for ObC programs. The rest of ObC, including majority of all data, is stored within the normal environment. Client applications use the ObC via the *ObC Credentials Manager*. The Credentials Manager manages the *ObC Database*, which contains all the credential secrets and programs in encrypted form. In addition it provides a *"secure user interface"* for accessing the ObC. Only the Credentials Manager is allowed to communicate with the ObC interpreter. Service providers can define their own credentials and provision those to devices through client applications. [14]

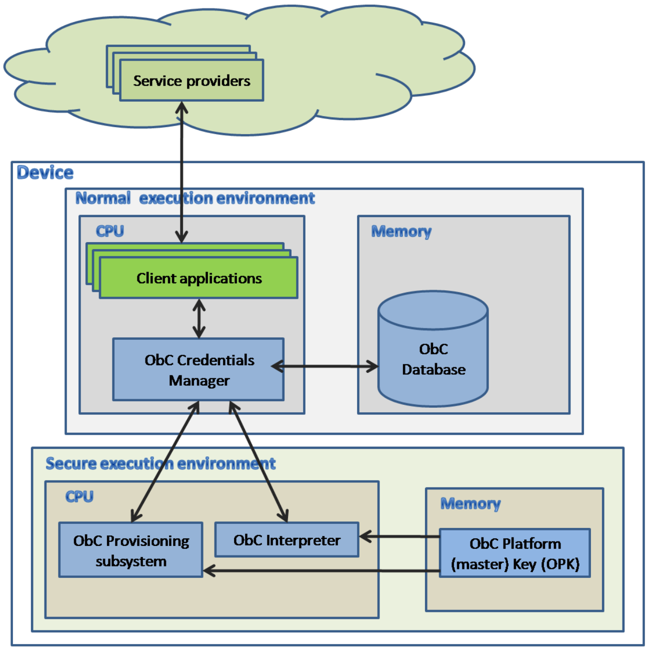

Service providers
Device
Normal execution environment
CPU
Client applications
ObC Credentials Manager
Memory
ObC Database
Secure execution environment
CPU
ObC Provisioning subsystem
ObC Interpreter
Memory
ObC Platform (master) Key (OPK)

Figure 5: Simplified overview of the ObC architecture

3.3.4 Advantages

Maybe the biggest advantage, especially for small-scale service providers, is the open provisioning. Service providers can develop their secure services totally independently from device manufacturers and other stakeholders. This will probably mean that ObC will be free for both the service providers and the users.

The utilization of general purpose secure execution environments is also an advantage. It greatly improves the security of the system by ensuring secure handling of secret data.

3.3.5 Problems

The most obvious disadvantage is that because of the requirements ObC can not be used in old devices, it cannot even be used in all of the new devices. However, secure execution environments are becoming more and more common in mobile devices and therefore this should not prevent the deployment of ObC.

Second and probably more serious issue is that ObC is designed by Nokia. This is a problem because typically different vendors are not keen to implement systems that are not their own. Even though Nokia has a huge market share in Finland, it is not 100%. Using ObC must not be restricted to Nokia phones or ObC cannot become heavily deployed, because service providers cannot exclude huge amount of pontetial customers. Therefore it would be important to get ObC standardized or to find some other way to get other mobile device vendors to create compatible implementations of ObC to their devices.

3.3.6 Situation

The idea and the architecture of ObC seem promising. However, there is a lot of work to be done for getting ObC deployed. I could not find any official information about deployment status of ObC. At the moment it still seems to be at research state and cannot be taken into use.

Couple of complete implementations of ObC systems exists for different platforms. As an example an implementations which runs on phones with Symbian operating system and M-Shield secure environment. [8] These implementations are mainly created for testing purposes and seem to be more like prototypes than complete products.

4 Comparision

4.1 Requirements

SMS-OTP does not require anything else than a device that is capable of receiving SMS messages. The only requirement for using Mobile certificate is a new SIM card that contains the required credentials. The both NFC and ObC require a physical chip to be added to the device. Some of current mobile devices contain the NFC chip that is required for using the NFC based method and some of the devices contain the secure environment that the ObC requires. It is difficult to say which of those gets deployed into majority of the mobile devices faster.

In addition with NFC method, it is not enough to have a mobile device that contains the NFC chip, a contactless card is also needed. It seems that at the moment in Finland all the credit cards are traditional cards and do not contain RFID chip. Therefore before the NFC authentication can be used, banks need to start offering contactless cards.

From the requirements point of view SMS-OTP is clearly the best since all the other methods require something to be added to most of the current mobile devices. The second best in this category is Mobile certificate where the only requirement is a new SIM card.

4.2 Deployment status

As mentioned earlier, all of the methods are not deployed at the moment and therefore cannot be used yet. In fact only the SMS-OTP could immediately be taken into use in Finland by a service provider.

Mobile certificate should have been released by now, but for some reason this has not happened yet. ObC, seems to be still at research state and therefore it is very difficult to say that when, if ever, it gets widely deployed. The NFC technology is ready, but the lack of mobile phones with NFC and contactless cards prevents using it.

Therefore, from the deployment status point of view the best of these options is the SMS-OTP. Second best is probably Mobile certificate, because it should have been published already and therefore it should become available soon.

4.3 Pricing

Pricing is naturally a very significant factor in all commercial systems. This is important from both users and service providers' point of view. If the costs for the users are too high, the users will very likely keep on using the old system. If the costs for the service providers are too high, they will not invest on the new system.

Depending on how the SMS-OTP is used the price for the users is either free or very low. The costs are also fairly low for the service provider. I could not find any other information about pricing of Mobile certificate, except that the price is determined by the mobile phone operators. Therefore the pricing information will become available after mobile phone operators start to offer it. Pricing of NFC will depend on the issuers of the contactless cards. As the ObC is still at research state, there is no official information about the pricing. Nevertheless, due the openness of the ObC, it will likely be free for both users and service providers. However, designing the needed credentials might create some costs for the service providers.

From the user's point of view, the costs of NFC and ObC are increased by the need for purchasing new mobile phone. As a conclusion, there is not enough data for making a comprehensive analysis about the pricings. Nevertheless, the costs of SMS-OTP are very low and the costs of ObC are also very likely going to be low.

4.4 Usability

Usability is also a very important factor in applications that would potentially be widely deployed and get a huge amount of users. In mobile applications achieving good usability is especially challenging because of the small size of the devices. The huge amount of different mobile devices, which all operate a bit differently, makes this even more challenging.

Because most of the methods cannot be used at the moment, analyzing the usability is very difficult. This is especially difficult with ObC, since there is not much information about how it is really going to be used.

Using the NFC for authentication contains multiple steps and requires entering three codes therefore the usability of that method is poor. In addition it has similar requirement

	Requirements	Deployment status	Pricing	Usability
TUPAS	Need to be a customer of a Finnish bank. Also need to have the password list available when using the service.	Is in use in Finland by all major banks. Also many other services offer TUPAS authentication.	Prices depend on the contract with the bank. For end-users fairly cheap (e.g. Nordea 2e/month), expensier for service providers (start payment and monthly fee).	Usable and easy to understand, but requires having the passwordlist available.
Mobile certificate	New SIM card containing credentials. Easy to get from a mobile phone operator.	Cannot be used yet. Was supposed to become available during 2010, but seems to be delayed for unknown reason.	Not free. Costs depend on the contract between user and mobile phone operator. Prices not yet published.	Presumably easy to use. In addition to normal authentication requires only entering SPIN number.
SMS-OTP	None.	Used in many services, for example in some ebanks.	Some fairly small costs for the service providers from sending the OTP messages. Typically none for the users.	Simple to understand. Easy when using with separate computer, a bit more difficult when using with just a mobile device.
ObC	Mobile device containing a proper secure execution environment, e.g. M-Shield. Many modern devices contain such environment.	Cannot be used yet. Seems to be still in research stage.	No information available. Will probably be free because of the openness.	No information about how it will be used.
NFC	Mobile device containing NFC chip and a contactless card.	Not available in Finland. The lack of NFC phones and contactless cards prevents from using.	Prices depend on the contract with the bank.	Poor. Using requires going through many steps and entering multiple codes.

Figure 6: Comparision of the authentication methods

than TUPAS: users are required to have their contactless card available when they want to use the authentication. As mentioned, SMS-OTP has problems considering usability when the mobile device is used for both authenticating and using the service: it requires memorizing or writing down the one time password. Authenticating with Mobile certificate requires, in addition to normal username/password authentication, only entering the SPIN number. Therefore from the usability point of view the best is Mobile certificate.

Probably all of the methods, except TUPAS, will have problems with non-multitasking mobile devices because the application that is used for accessing the service is not the same application that handles the authentication. Non-multitasking devices cannot run multiple applications simultaneously, and therefore one of the applications needs to be closed before the other one can be started. Nevertheless, the authentication methods can still be used with such devices if the service is used for example with separate computer and the non-multitasking mobile device handles only the authentication.

5 Conclusion

Even though the goals of the described methods are similar, the approaches differ much from each other. All of the methods have their strengths and weaknesses. Unfortunately, most of the methods are not yet deployed and thus cannot be used. Therefore, if a service provider intends to right away start offering a mobile authentication, solutions based on the SMS-OTP seem to be the only option.

In fact SMS-OTP is overall fairly good mobile authentication method, at least for services that do not require very heavy protection. It is cheap and light and very easy to understand and use when service is accessed with separate computer. The only real disadvantage is the usability issues when mobile device is used for both authenticating and using the service.

Mobile certificate is probably a good method at least from the end-users point of view because, it will be easy to both start to use and to use. It should become available during this year, but it seems that the release has been delayed for some reason. I still think that it will become available soon because the Finnish mobile phone operators will want to get a share of the money that moves in authentication business. At the moment because of TUPAS that money goes to banks.

The pricing of Mobile certificate is still a big question. If it is too expensive, users will stay with the old system.

The openness and the general architecture makes ObC very promising method, but it might be very challenging to get it in to use. Nevertheless, it is interesting to follow the development of it. NFC is also very interesting idea and I presume that sooner or later the technology will get deployed worldwide. However, due the difficulty of using NFC as authentication method, the strength of it is in other situations than authentication, like in different kinds of payments and advertising.

References

[1] Mobiilivarmenne.fi. http://www.mobiilivarmenne.fi/fi/. accessed date: 18.10.2010.

[2] Mobiilitunnistamismenetelmät, November 2008. http://www.arjentietoyhteiskunta.fi/files/185/mobiilitunnistamismenetelmat.pdf.

[3] cnet - Elinor Mills. Report says be aware of what your Android app does. http://news.cnet.com/8301-27080_3-20008518-245.html. accessed date: 16.10.2010.

[4] V. S. Corporation. MobileKey (Mobile Authentication Server). http://www.visualtron.com/products_mobilekey.htm. accessed date: 18.10.2010.

[5] DenizBank. SMS Verification. http://www.denizbank.com/EN/Acikdeniz/internetBranch/SMSDogrulama.htm. accessed date: 5.10.2010.

[6] Digitoday - Jukka Lehtinen. Sähköinen tunnistusfloppi on käynyt kalliiksi. http://www.digitoday.fi/tietoturva/2008/04/21/sahkoinen-tunnistusfloppi-on-kaynyt-kalliiksi/200811104/66. accessed date: 14.10.2010.

[7] Ericsson. Mobile subscriptions hit 5 billion mark. http://www.ericsson.com/thecompany/press/releases/2010/07/1430616, July 2010. accessed date: 24.9.2010.

[8] J. erik Ekberg, N. Asokan, K. Kostiainen, P. Eronen, A. Rantala, and A. Sharma. NRC-TR-2008-001 On-Board Credentials Platform Design and Implementation, 2008.

[9] Etelä-Saimaa artikkelitietokanta - Anssi Kemppinen. Etelä-Karjalasta katoaa viimeinen kyläkonttori. http://www2.lappeenranta.fi/lehtitietokanta/artikkeli.php?id=10874, 2009. accessed date: 18.10.2010.

[10] FiCom - Nora Elers. Mobiili asiointivarmenne yksinkertaistaa tunnistautumista. http://www.ficom.fi/tietoa/tietoa_5_3.html. accessed date: 14.10.2010.

[11] Flexible Services - Antero Juntunen. Mobile Ticketing Business Model Analysis. http://www.flexibleservices.fi/files/file/Liitteet/P04-EDEN_WP2_D2.2_Mobile_Ticketing_Business_Model_Analysis_v1.pdf. accessed date: 2.11.2010.

[12] Garanti. Help & Advice. What is verification via SMS? http://www.garanti.com.tr/en/help_advice/faqs.page?faqName=internet_banking_verification_via_sms#calcContent=UID4955498. accessed date: 5.10.2010.

[13] IBM Zurich Research Lab - Diego A. Ortiz-Yepes. Enhancing Authentication in eBanking with NFC-Enabled Mobile Phones. http://ercim-news.ercim.eu/en76/rd/enhancing-authentication-in-ebanking-with-nfc-enabled-mobile-phones. accessed date: 2.11.2010.

[14] K. Kostiainen, J.-E. Ekberg, N. Asokan, and A. Rantala. On-board credentials with open provisioning. In *ASIACCS '09: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, pages 104–115, New York, NY, USA, 2009. ACM.

[15] Network System Architects, Inc. What is a Subscriber Identity Module (SIM)? . http://www.gsm-security.net/faq/subscriber-identity-module-sim.shtml. accessed date: 13.10.2010.

[16] NFC Times - Dan Balaban. Nokia Begins Shipping C7 Smartphone with NFC Chip Inside. http://www.nfctimes.com/news/nokia-prepares-introduce-first-nfc-smartphone. accessed date: 2.11.2010.

[17] K. Nohl and C. Paget. GSM: SRSLY? http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html. accessed date: 16.11.2010.

[18] Nordea. Näin toimii maksun lisävahvistus. http://www.nordea.fi/Henkil%C3%B6asiakkaat/Internet+ja+puhelin/Mobiilipalvelut/N%C3%A4in+toimii+maksun+lis%C3%A4vahvistus/1294702.html. accessed date: 6.11.2010.

[19] Nordea. Strong End-user Authentication for Online Banking with NFC Handsets. http://www.mobilemondayoulu.com/wp-content/uploads/Strong_End-user_Authentication_for_Online_Banking_

with_NFC_310809.pdf. accessed date: 2.11.2010.

[20] RFID - Consortium for Security and Privacy. Vulnerabilities in First-Generation RFID-Enabled Credit Cards. http://www.rfid-cusp.org/blog/blog-23-10-2006.html. accessed date: 18.11.2010.

[21] RSA. Security Information Security Glossary - Strong authentication. http://www.rsa.com/glossary/default.asp?id=1080.

[22] J. Srage and J. Azema. M-Shield mobile security technology. http://focus.ti.com/pdfs/wtbu/ti_mshield_whitepaper.pdf, 2005.

[23] TeleSign. TeleSign's SMS Identification Stops Phishing and Online Fraud! http://www.prlog.org/10626763-telesigns-sms-identification-stops-phishing-and-online-fraud.html. accessed date: 5.10.2010.

[24] TeleSign. Two-Factor Authentication. http://www.telesign.com/solutions_twofactor_auth.php. accessed date: 18.10.2010.

[25] Tilastokeskus. Matkapuhelinliittymien määrä sekä liittymät 100 asukasta kohti vuosina 1980, 1985 ja 1990-2007. http://www.stat.fi/til/tvie/2007/tvie_2007_2008-06-05_tau_006_fi.html, 2008. accessed date: 24.9.2010.

[26] M. Virtanen. Mobile Electronic IDl. Master's thesis, Aalto University School of Science and Technology, May 2010.

[27] Väestörekisterikeskus. Mikä on kansalaisvarmenne? http://www.sahkoinenhenkilokortti.fi/vrk/fineid/home.nsf/pages/4DC96862A6BFA292C2256FFF00379DE9. accessed date: 14.10.2010.

[28] Yahoo. What is Flash SMS. http://in.content.mobile.yahoo.com/new/flash/. accessed date: 5.10.2010.