

Aldata



NORTH East South West
INTERREG III C

 PROJECT PART-FINANCED
BY THE EUROPEAN UNION

Dual Interface smart card test in Tampere

ECitizen project
20 June, 2005

Content

1. Background	3
2. Applications to be tested	3
3. Smart card technology	3
4. Structure of testing	4
5. First phase results.....	5
5.1 Trûb as card provider	5
5.2. Sonera	6
5.3. Public transport	7
5.4. PKI (electronic) authentication	7
6. Notifications from the second test round of the first phase	9
7. Certificates provided by the Finnish Population Register Centre.....	14
7.1 Applying and issuing the card.....	14
7.2 Card related issues	15
8. Summary	16

1. Background

City of Tampere piloted during years 2003 – 2004 a smart card based eTampere card with close 5500 users. The card which is planned to be taken in use in the final production phase is so called dual interface card which was not yet tested in environment of city of Tampere. Due to the lack of user experience city of Tampere has decided to set up a test with 40 cards to be used in the former pilot applications to test the functionalities of the dual interface card.

Aldata Smart Card Oy acted as a coordinator in testing. Aldata Smart Card Oy is 100 % owned subsidiary of Aldata Solution Oy.

2. Applications to be tested

The applications to be tested have been public transport access control system, library usage with penalty payments, PKI usage in TAMK environment and payments in the TAMK restaurant. (TAMK=Tampere Polytechnic)

For the test 40 users were nominated to get full coverage of results from all the tested functionalities.

Aldata Industries Oy, now Aldata Smart Card Oy has coordinated the testing, gathered the test results and provided the smart cards and physical access control readers for the test.

3. Smart card technology

The cards that were tested were based on the following technologies:

Chip:	Philips MifareProX
Operating system	IBM JCOP 30
PKI-applet1:	MyEID (Finnish Eletronic ID card compliant)
PKI-applet2:	SafeSign
EEPROM:	16 kBytes
Mifare emulation:	1 kBytes

This card type enables the compliance with existing Tampere City Transport bus cards and eTampere pilot cards. So, the new card can

be taken in use parallel with the existing cards without the pressure of changing the existing infrastructure (readers, ticketing validators, software).

The target of the testing has been to use the new dual interface card in all existing usage points and write down a report of the findings during the tests. After the tests conclusions can be made about the new card functionality making the basis for the future planning.

4. Structure of testing

In the first test phase all basic tests regarding the card usage were done with a small card amount (9 cards). Test users in this phase were using two different card types. The difference was in PKI applet, on some of the cards the applet was a Finnish MyEid applet, on the others a Dutch SafeSign applet.

After these basic tests the test was enlarged to cover the whole test user group. Following testing was done in two phases.

The items to be tested were also the card and card user unique identification numbers, card supply logistics and in physical access control system side the availability and supply and installation logistics of the so called sector readers. These findings were gathered to help to create a full picture of the issues related to the card and the card holder identification. These results also help to identify the questions which might come up when starting the potential production usage phase of Dual Interface cards.

In second phase the focus was on issues related to physical access control system side and the functionality of the new cards in electronic applications and forms.

5. First phase results

The main goal for the City of Tampere is to use the new Dual Interface cards in all of the existing applications in the same way as with the existing cards set all the participating companies in front of a challenging situation:

This new card type was also new to Aldata (previously internal tests in physical access control and in PKI usage with SafeSign applet)

The card type was new to Fujitsu, whose DigiSign software was enabled to support it. At the same time MyEID applet was further developed to be usable with this new chip and operating system.

The card type was also new to Intermarketing and Pusatec (ticketing validator providers)

The card type was new to Sonera (CA = certificate Authority services)

All the companies involved have made remarkable efforts to enable the start the test phase of Tampere city card project.

5.1 Trüb as card provider

The first issue which was tested was the flexibility of the card provider. In this phase the target was to find out and clarify the order / delivery processes and service willingness of Trüb.

The card delivery was splitted in many small batches. The batches were clearly from different production batches, probably also done by using different production procedures. A part of the cards were ordered with operating system and PKI applet, another part with only operating system loaded. Essential issues with Dual Interface cards are key management (Mifare emulation – factory keys – customer specific keys, applet loading – Visa test keys or customer specific keys) and Mifare emulation and operating system versions.

In first phase of the testing it was noticed that card provider had not taken into account importance of factory keys in Mifare emulation -> two of those nine cards for the first phase were loaded with other than the factory keys. This caused problems in card usage with public

transport application, because the initialization software requires factory keys on card. So, two of those nine cards were not able to initialize at all.

This was fixed in second test phase when card holders were equipped with cards test keys on them.

5.2. Sonera

A second issue which was tested was the certificate issuing process of Sonera. This was done together with Sonera CA personnel. In the set up phase a missing file in the certification authority (CA) system caused a failure situation in WEB-RA function, but this was corrected during the initialization process of the first cards.

The second challenge that rose up was the card itself. Sonera has previously used Setec's Instant EID cards in their WEB-RA process. On these cards there already exists a generated key pair to enable to certificate generation. Normally the WEB RA process is able to generate a key pair on the card during the certificate request process but this functionality was missing in the Sonera WEB RA process developed specifically to the eTampere project.

On test cards there were no keys generated by the manufacturer so the certification request process stopped and generated a failure report. Just to test another possibility the certificate request was done through SSH internet service. With that certificates could be loaded on the cards.

As a result and conclusion of the first phase the cards to be used in the second phase were equipped with pre generated key pairs. An essential improvement would also be if Sonera could develop its WEB RA process to be able to function without key pairs which are generated and loaded on the card by the card provider.

5.3. Public transport

The third test environment was public transport. Loading of Tampere City Transport applications succeeded well except with two cards. In tests the payment usage of the card with the ticketing validators went well, card reading speed was the same as with ordinary bus cards. With one card problems in reading the card history were found.

Also a very important finding was that loading the public transport application on the cards with test keys succeeded well. In the initialization process the card number which is loaded on the card is the one printed on the card, it is not connected to the unique Mifare serial number.

The own card number used in public transport application can be managed also by the public transport organization of the city, the card numbers used are just from an ordinary number slot. Thinking about the logistics of the cards the card manufacturer can take care of card number printing and storing on the chip as a service. During that process also a connection between public transport serial number and Mifare number can be created. This means that there is no need to send the cards to the ticketing validator providers before taking them in use.

Those two totally "dead" cards were tested by Aldata before they were sent to Trüb for further tests. In Aldata's tests it was noticed that the Mifare keys on the cards were not the factory keys but they had been changed. Also on the contact chip some problems were found in the PKI applet key management. Those cards were sent to Trüb for their tests. Output of the tests was the same.

5.4. PKI (electronic) authentication

The fourth test place was TAMK and PKI. The test case was to load a certificate generated by Microsoft CA onto the cards. The certificate was to enable smart card logon to a Windows based local area network.

There were two applets and two client software (CSP) available. The first one tested was Fujitsu's DigiSign software together with MyEID applet. One advantage this software has is that it already has a support for the eTampere cards. In Windows 2000 pc platform there will be

errors in functions if there are more than one PKI software installed at the same time.

In Windows XP platform several parallel software can function parallel (based on Aldata tests and experiments).

The card use of TAMK test users succeeded well after finding out the problems several CSPs in same pc caused. The smart card based Domain login functioned as expected. The functionality of SafeSign software was not yet verified in this phase.

In this first phase testing it was already verified that the basic concept is working properly – in principal and in action the dual interface cards were compliant with the bus cards already in use, and with a minor extra development work also with PKI usage.

6. Notifications from the second test round of the first phase

In the second phase the tests included:

- Swimming hall usage
- Payments in student restaurant
- PKI usage in TAMK
- Penalty payments in library

6.1. *Swimming hall*

Swimming hall usage. In swimming hall the functionality tested was the entrance through the gates. This meant an automatic credit from the card and automatic opening of the gate after the credit. The cards as well as the credit were functioning properly.

At the same time also the reading of the card history by the gate reader was tested. The software used in service point supports this functionality. Reading the card history was working properly and no faulty test cases were found in swimming hall tests.

6.2. *Student restaurant*

Restaurant payments in TAMK student restaurant. In the tests the so called student lunch (special price) was paid and the payments were successful. Also other payments were tested with the cards and everything worked as expected.

This test had a special importance because the validator is provided by another manufacturer than the validators used in busses. With this test it could be verified that the new dual interface card is functioning properly in both validator types in spite of different manufacturers. The test also showed that an application loaded in one environment is working in another environment as well.

Regarding the student restaurant payments the option of adding new products in the product portfolio and taking them into use in addition to the very limited selection at the time of the test was also discussed. It was noted that from the technology point of view there is nothing preventing that.

6.3 Electronic authentication

PKI usage in TAMK. This time several cards were initialized with Microsoft certificates. In the specification of the certificate system some issues in certificate request process needing a further development were noticed.

DigiSign software was installed in an ordinary pc in a study class to replace Smart Trust Personal CSP software.

As a result of this test it was noticed that both the new dual interface cards and the eTampere cards were working properly with DigiSign software in the smart card logon process.

Another test finding was that if there are older versions of CSP software installed in same pc as the newer ones, technical problems might appear. Also removing older versions of CSP software can cause some challenges because old registry values might remain when the main software is deleted.

6.4. Library

Library usage. In the library penalty fees for testing were generated manually and the fees were paid by using the new dual interface card. The transactions succeeded well and this was also the second time to verify that different validators are compliant and that the card is working properly with them both.

In library usage more advantages can be reached if the Mifare card number is connected to the library application to be used as library card ID. The readers best for this purpose need to be further investigated to find out a solution where a cost effective combined reader for Mifare card reading and bar code reading could be found.

6.5 Physical access control system testing

The dual interface card has already been tested in Aldata FlexWin physical access control system where the card is functioning in the same way as an ordinary Mifare card. Aldata is using a unique Mifare serial number in its system.

The physical access control system mainly used in the city of Tampere is Timecon system. In Timecon system a specific number as well as the data transmission protocol used (Wiegand) are stored in a defined sector. The method Timecon is using is confidential information so Aldata was not able to provide the cards or the readers direct to the city of Tampere.

In the physical access control system testing the first remark was that Timecon had big challenges in installing the new reader, supporting Mifare technologies.

The first challenge was the personalization of the cards for physical access control usage. The system provider was not willing to tell to its customer (the city of Tampere) what is needed to take the new cards into use. It seems that their strong presence in the process is needed to enable the new card usage. In practice this doesn't give the city of Tampere a real opportunity to purchase the cards and take them in use in the way it wants.

The second challenge was to purchase the reader and get delivered to the city of Tampere, a good procedure for this was difficult to find. Finally the new reader was installed as a part of the system the city of Tampere owns.

Installation instructions from the system provider to the customer have been quite insufficient, it is obvious that the provider is not willing to allow this to be done either by the customer or a partner named by the customer. Their target seems to be that they want the customer to buy that service from them and use their service personal for installation.

In this case a special attention must be paid on the key management also with the test cards to enable enough information to the city of Tampere. Key management should be taken care of by the customer, not the system provider, to make it easier to change the provider in future if necessary.

As a result of testing the physical access control system was that the cards can be used as physical access control cards. It was not possible to verify if both physical access control application and public transport application can be stored on the same card.

Testing is also important in the future to find out possible conflicts between different applications (key management for Mifare sectors).

It is possible that both physical access control application and public transport application close all the sector on Mifare card not depending on the capacity the application requires.

Below shortly listed the actions and results of physical access control system test:

- installing the reader in the network
- adding the terminal controller (ttc 2650)
- connecting the reader to the terminal controller
- configuration of the terminal controller
- adding a new channel in the central unit
- the terminal controllers chain channel reprogramming (needed when channels are added to the chain, if this is not taken into account earlier)
- the functionality of the reader and the card has been verified.

As a result and a recommendation for future actions the city of Tampere should clarify its contract with the physical access control system provider to enable an open and competitive situation for all actors.

6.6 Testing the electronic forms

Testing the electronic processes was started after succeeding in loading Sonera certificates on MyEID applet.

In the beginning of the test session problems with signing the electronic forms were found.

When the cards were tested in Aldata's environment they were working properly in different electronic form services (eTampere test site, Avain Technologies test site). The result was that the problems were caused by the pc used in the city of Tampere.

In the pc there was SmartTrust Personal CSP software installed which was removed before installing DigiSign CSP.

The card was sent back to Tampere and DigiSign was installed to a pc where no CSP software was installed before. The card was then working properly.

As a result was noticed that with those places where there are previous CSP software (SmartTrust, SSH Accession) installations there might be similar situations. To prevent this kind of problems it must be found out what kind of traces will remain in pc registries when software is removed.

When using the electronic services and forms a specific attention must be paid on the certificates being used. It is worth to evaluate also other certificate service providers and their services.

7. Certificates provided by the Finnish Population Register Centre

The city of Tampere asked later in September a clarification of other certificate service providers. In testing phase Sonera CA certificates and Microsoft CA certificates were tested. The new clarification was about the possibility to use the certificates issued by the Finnish Population Register Centre on eTampere card.

To find out the possibilities representatives of PRC were interviewed.

In the interview the following issues were discussed:

- applying and issuing the card
- registration
 - o Organizations
 - o Connections needed
 - o Other procedures
- card related issues
 - o card type (dual interface card)
 - o evaluations needed
 - o card personalization organisation
- certificate issuing system
 - o prices of the certificates
 - o connections between the personalization organization and the certificate issuing system
 - o order sizes
 - o contract period

7.1 Applying and issuing the card

Any organization fulfilling the requirements described in qualified certificate issuing organization actions can act as a registration authority.

In practice the registration authority could be an own organization of the city or as with mobile certificates the local police office.

The network connections needed are related to checking the personal data accuracy from the Population Information System which is in use in the registration offices. The city of Tampere has access rights to the Population Information System so this won't cause any challenges.

The training of the registration organization is taken care of PRC and the training of city personal can be performed as their duty.

7.2 Card related issues

The card type chosen (dual interface card) is technically suitable to be an Electronic ID card platform. The evaluations needed were discussed and the conclusion was that no card has passed the evaluations based on new SSSC specification.

Further discussions regarding the technology shall be done with the persons of the technical department in certificate unit during the contract negotiations.

Visa International uses Mifare ProX card in their dual interface EMV credit card solutions in Asia.

The requirements set to card personalization organization were discussed when discussing the issues relating to card personalization process. Now the card having FINEID certificates are personalized by Setec. Using the same personalization organization would significantly ease the progress of the process because Setec has the required Baltimore ARM software to make the certificate requests. On the other hand this model doesn't enable the competition of different personalization service providers.

If some other company than Setec will be used, the minimum requirement is to purchase the ARM license and a leased line between the new personalization organization and the Population Register Centre.

8. Summary

Based on the testing it can be said that the new Mifare ProX dual interface card can be taken into use in parallel with the existing bus cards and eTampere pilot cards without making any changes to the applications.

Also the reading / writing speed on the contact less side is on the same level as on the bus cards , so the usability is good also when the speed is taken into account.

The PKI functionality can be a feature available to those users who want to use the certificates. The capacity of the card (16kb – 1kb for Mifare emulation) sets some limits to the amount of certificates which can be loaded onto the card. The certificate types used in the test enable two (2) user certificates on the card at the same time.

The Java Card operating system (IBM JCOP) offers open platform for developing software for new applets, for example for public transport application a possibility to load tickets or money in a wallet over the internet has already been evaluated.

The card key management issues should be paid extra attention to in the future to ensure an open and independent system, which is not tied to a specific provider and which enable a situation where the standards are open and a real competition is possible.

The possible lack of capacity with the new eTampere cards can be solved by using a new card provided by Philips. SmartMX card emulates the Mifare card in a same way as the tested ProX card. The capacity of the new card is 72kb and porting the IBM JCOP operating system on the card has been finalized after the testing period. The applications will work on both chip platforms.

When developing the applications on the card the best solution is the globally unique Mifare ID number stored on the chip so the card is identified by that serial number. The user information can be and is good to connect to that serial number either in the application or in the back end system.

There are several certificate issuing systems available, also Sonera has renewed its model at the same time when they took a new CA system in use. In this document there is also a short description of the certificate model which the Population Register Centre is offering. There are also other service providers available and the TAMK model using Microsoft certificates for the smart card logon or in electronic signatures is a well working model for internal usage.