FEIDHE (a project)
Electronic Identification in Finnish Higher Education

Mikael Linden, Janne Kanner, and Mika Kivilompolo

FEIDHE project

1 Introduction

In Finnish universities and polytechnics students and staff members have access to several information systems and services requiring user authentication. Traditionally authentication is based on username-passwords pairs. In the information systems the passwords or alternatively, some one-way hash values deriving from them are stored in a user database. When the user is to be authenticated to the system, one is prompted to enter one's username and password, which are then compared to the data stored in the database. If the username-password pair correspond to ones in the user database, access is granted to the resources that are available for the user.

In the username-password pair authentication, the identification of the user is based on the knowledge that the user has. Using encrypted connections provides protection against attackers who listen to the communication channel in order to capture passwords. However, from the security point of view, the username-password authentication has some distinct vulnerablies, which are mostly due to the 'human factor': the user may use a password that is too short or it can be easily guessed, or the same username-password pair is used in several systems at the same time. Some countermeasures can be implemented for example, by rejecting passwords that are too weak or force the user to change passwords frequently. Furthermore, there is no administrative tools available for preventing the user from storing the passwords on different media than one's memory (i.e. the user may write down the passwords on a small piece of paper just next to the workstation).

An alternative approach to user authentication is to use public key cryptography (aka asymmetric cryptography) in which there are two distinct keys, one for encryption and the other for decryption. The encryption key (the public key) is made available for everyone willing to send an encrypted message to the user. Only the user has the private key that is needed for decrypting the encrypted message.

In order to authenticate a user the computer system sends to the user a challenge, which is basically a sequence of random bits encrypted with the user's public key. If the user has the corresponding private key, one is able to decrypt the challenge and send the decrypted bit sequence back to prove one's identity.

The private key can be stored in a cryptographic token, e.g. a smart card, that will never reveal the key, but instead uses it for decryption when user authentication is needed. Now, when the information system encrypts a challenge with the user's public key, it can be responded to only if the corresponding private key in the token is available. The cryptographic token, further, is generally protected with a four digit personal identify number

(PIN) and other protection functions that prevents unauthorised users to misuse the token. Hence, the public key authentication is based on something the user knows (PIN code) and something the user unique has (a cryptographic token).

2 PKI and its national Implementation in Finland

The generation of a private-public key pair is not enough for the comprehensive use of public key cryptography in authentication. A system called Public Key Infrastructure (PKI) is needed for managing the keys. This chapter introduces some principles of the PKI and its national implementation in Finland.

2.1 PKI fundamentals

From the system point of view, a user in the PKI is the owner of the private key. The PKI is needed to define how to distribute the public key to the authenticating information system and how to pair the public key to a particular user, possessing the private key. In order to implement a large scale PKI, a trusted third party, called Certificate Authority (CA), is needed. The CA is exclusively responsible to ensure the identity of the private key's holder.

The CA defines its policy in a public document called Certificate Policy (CP). The Certificate Practice Statement (CPS) is a document that states specifications on the CP. Typically, the CPS defines for instance how the identity of the user is verified and who is authorised to do that.

As a proof of the identity of the private key's holder the CA issues a certificate. It is a statement that by the virtue of digital signature of the CA binds the identity of the user in a real world to the particular public key in the network. A certificate contains, typically, name of the user, the public key of the user, serial number for the certificate, the public key of the CA, and validity of the certificate. In order to make the certificate available for everyone in the network, it is stored in a public directory server.

In PKI authentication, the identity of the user can be verified as follows: the authenticating system fetches user's certificate from the public directory and then gives to the user a challenge that can be correctly responded to, only if the user has the private key.

The certificate has a finite validity, also the user can loose or destroy the private key, or the key might be stolen. Due to these reasons, the CA maintains a public list of invalid certificates. This list is called in the literature as the Certificate Revocation List (CRL). Therefore, in the PKI authentication process also the validity of the certificate must ascertain from the CRL.

The market is gradually getting ready for large scale deployment of PKI. The standards are becoming stabile, and commercial PKI products are entering markets.

2.2 National PKI in Finland

In Finland the public sector has been the driving force in PKI implementation. In 1996 a common working group of three ministries issued a report[1] stating that the electronic

identification of a citizen belongs to the infrastructure of the information society. According to the report it is necessary to develop and maintain information systems needed. A project called Finnish Electronic Identity (FINEID) was launched to specify a national PKI and to make other necessary preparations. The Population Register Center was nominated as CA. Related modifications in the legislation were made in the parliament.

From the beginning of December 1999 the citizens of Finland have been entitled to apply for an electronic ID card (FINEID card)[2]. The application procedure is similar to the practice for the conventional ID documents (e.g. passport); the citizen files an application at the local police office, where the officer identifies the applicant and checks the validity of the application. Electronic ID cards with the embedded chip are manufactured by Setec, a Finnish smart card vendor, and the certificate, is issued by Population Register Center. The price for the electronic ID card is 27 euros (card is valid for three years), whereas the conventional ID card costs 22 euros.

The FINEID card contains two private keys (and two certificates). One of the keys is used only for authentication and the other only for decrypting messages and for digital signatures.

Until September 25th, 2000 (6045) FINEID cards had been issued[3]. The bottleneck for the rapid increase in the number of FINEID cards has been the lack of services relying on the FINEID card and PKI. Only one bank has launched a FINEID based authentication to its web services, and few public sector services, mostly utilising digital signatures, have been introduced. The private service providers seem to hesitate as long as the number of potential customers having the FINEID card is so small. Another barrier delaying the growth of the user number is the cost of equipment i.e. the smart card reader and the software necessary for utilising the reader in applications.

3 FEIDHE - Electronic Identification in Finnish Higher Education

Reliable user authentication has been an issue in Finnish universities and polytechnics as well. The national FINEID project accelerated the related discussion in universities among the people responsible for network security.

Students in Finland have national student plastic ID card, which is a requirement e.g. in student prices in public transportation or other student discounts. The student cards are issued by the student unions, which have strong position in Finnish universities. For students embedding a chip to the student card is considered to be a natural step in expanding the current range of the services to the PKI based services. For staff members it would be the responsibility of the university to provide the EID cards needed. Because all the universities in Finland are owned by the state, the FINEID project formed a natural starting point for building up PKI in the universities.

A FEIDHE (Electronic identification in Finnish higher education) project was chartered in May 2000 as a common project of all the Finnish universities, the national union of the Finnish student unions and CSC - Scientific Computing Ltd., which is a non-profit company owned by the ministry of education and the maintainer of the national research and education network in Finland. Polytechnics and their student unions joined the project

in October 2000. Altogether there are 50 project members and they cover approximately 250 000 potential users (including students and staff members), which is about 5% of the population in Finland.

The goal of the project is to develop a smart card based authentication system for the needs of the Finnish higher education. The project aims at enabling an introduction of an EID smart card for higher education (FEIDHE card) during year 2002.

To reach the goal the project evaluates solutions available in the markets and makes specifications and recommendations needed. Furthermore, the project estimates the costs and funding needed to build the necessary infrastructure. The project also collects and distributes information to the project members on PKI and how to build services on it.

The main interest of the project is the introduction of stronger user authentication methods in the universities and polytechnics. However, digital signatures are also a subject of interest because of the increase in service level and cost-reduction in the administration that they would imply. There has also been interest in using the FEIDHE card for various payments in the campus.

4 Technical Aspects

From the technical point of view the project field can be divided into four layers (1). The security of each layer is based on the underlying layers. Basically all the security is based on cryptography, especially on the RSA algorithm and SHA-1 hash function, that are used in FINEID PKI and cards. Network protocols, such as Secure Sockets Layer (SSL)[4], utilise PKI in user authentication. End user services are built on top of the network protocols, such as WWW services, which are run on SSL. This chapter examines the PKI layer, Network protocol layer and Service layer in more detail.

4.1 PKI planned in FEIDHE

The FEIDHE PKI will be based on interoperability with as many services as possible in the public and commercial sectors in Finland. To that end the PKI will lean heavily on compatibility with the existing governmental PKI and Finnish legislation on electronic identification.

The project proposes that a commonly trusted commercial certificate authority should be selected for issuing the certificates for the users. CA signs the certificates with its own private key to bind the person's identity to the public key. CA is also responsible for maintaining a public directory for the certificates and the certificate revocation list.

CA does not necessarily do everything by itself. It is usual that the task of identifying the applicants and distributing the issued cards is given to a separate body that is called Registration Authority (RA). In FEIDHE the duty of RA is to be performed by the student administration of higher education institutes. Each applicant will be identified with a valid visual identity card such as a driving licence or a passport according to the CA's certificate policy. Then the applicant will fill an application form and give a photograph.

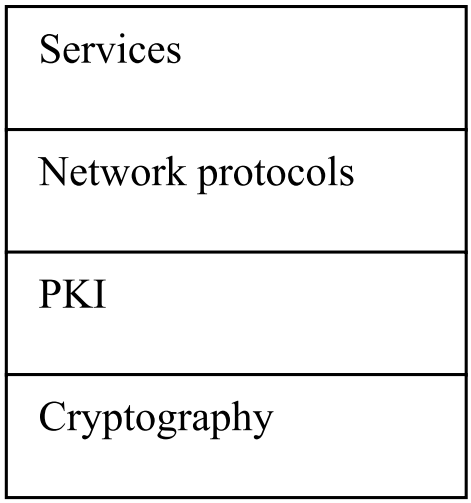

Figure 1. Technical layers in FEIDHE.

The project will use standard X.509 certificates[5]. No additional information is included with the possible exception of email addresses. This is to avoid constantly updating the certificates to reflect changes e.g. in person's role or position. The certificates will be placed both in the smart card and in the public directory that supports Light-weight Directory Access Protocol (LDAP)[6].

Components needed in the client and server side are illustrated in Figure 2. In the client side a smart card reader and some extra software is needed to enable the workstation to use smart cards. PC/SC working group, which is a consortium of the major computer operating system and smart card vendors, has published a de facto standard[7] for client side software architecture. Microsoft has released the base components of the architecture for Windows operating system, and the corresponding software for Linux environment is implemented in a project called MUSCLE (Movement For The Use Of Smart Cards In A Linux Environment) [8].

The PC/SC architecture as such is generic. The component specific to EID cards is called PKI client, and it is built on top of the PC/SC base components. The PKI client provides a standard interface to client applications, such as web browser and mail client, to access the services in the EID smart card.

To make user authentication PKI-enabled some extra functionality needs to be implemented in the server side as well. The signature and the validity dates of the user's certificate need to be verified. Furthermore, the server needs to check that the certificate is not in the certificate revocation list. Each institute will integrate this functionality in their centralised authentication server or set up a separate PKI server to handle it.

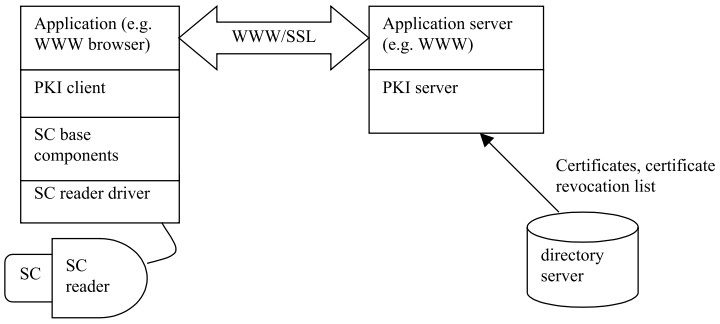

Figure 2. Client and server components in a smart card (SC) enabled PKI.

4.2 Network protocols utilising PKI

From the network protocol point of view the operation, in which the user is authenticated using her private key, is called client authentication. Fortunately most existing network protocols have support for client authentication implemented or at least specified.

Maybe the most important network protocol supporting client authentication is Secure Sockets Layer (SSL), securing transactions on World Wide Web. Client authentication is a feature of SSL handshake protocol and the most popular WWW browsers have a built-in support for it. During SSL handshake the server can optionally request the client to send its certificate. To ensure that the client has also control of the corresponding private key, the server uses the public key of the certificate to encrypt a challenge to the client. The client implementation of SSL uses the underlying PKI client to utilise the attached smart card to get a proper response to the challenge.

Another protocol for secure transport is Secure Shell (SSH) [9], that is commonly used in remote shells in Unix environments. SSH supports client authentication based on certificates. However, no commercial products using the feature have entered the markets. In FEIDHE project the extensions needed in SSH client and server are investigated.

Kerberos is a well-known, complex protocol used in authentication and session key distribution. Kerberos is traditionally based on symmetric cryptography. It is included in Windows 2000 operating system as the primary authentication method, but Microsoft has replaced the first Kerberos transaction with public key operation called PKINIT[10]. This enables the use of a smart card in Windows 2000 login.

Several commercial Virtual Private Network (VPN) products based on IP Security Protocol (IPSec)[11] have been launched, some of them supporting public key client authentication as well. IPSec is commonly used in establishing remote connections to corporate networks over insecure public networks such as the Internet. FEIDHE project evaluates existing VPN solutions to test their smart card support.

4.3 End user services in FEIDHE

End user service is a complex concept in FEIDHE. Logging on to the Windows network using Kerberos, establishing a remote shell using SSH and setting up a remote connection using IPSec can be considered grass-root level services in the project. More specific services can be implemented on WWW.

Because there are much more students than staff members, the large volume services are those used by students. Enrolments to periods, courses and exams are examples of administrative services for students. Educational services for students would cover the large variety of e-learning environments that have been discussed a lot in public. The FEIDHE card would replace the use of passwords in these services.

Using smart card authentication instead of passwords may increase convenience for the user, but it does not cause significant cost reduction for the institute. More savings can be obtained by introduction of the digital signature. Routine work can be reduced if documents requiring traditional print-and-sign can be converted to the paperless format with digital signature. This concerns especially the administration of the institutes, e.g. travel expense reports, bookkeeping etc.

The FEIDHE project is not going to implement end-user services in a large scale. Only some single services are implemented to test the technology and to get some user experience. Instead the project should be considered as an initiative to build up the infrastructure on top of which services can be implemented. It is the responsibility of the institutes to develop the services when the infrastructure is fully implemented and tested.

5 Further Prospects

Large scale deployment of PKI and services relying on it is not possible without piloting. To get technical experience and early user experiences on the services to be implemented, a set of pilots is to be launched during 2001 in universities and polytechnics.

Pilots vary with respect to the target group and service, number of users and the network protocols used. In most pilots the environment is WWW, taking advantage of the security provided by SSL. Another important pilot environment is Windows, because high education institutes are gradually upgrading their network environments into Windows 2000 that has built in support for smart cards.

To make the maintenance of large amount of certificates as easy as possible, the PKI has to be integrated tightly to the user administration in the institutes. In practice the user databases have to be centralised so that adding a new user has to be done only once. In the pilots the centralised user management is a topic which is not clearly related to smart cards.

6 Conclusions

Public key infrastructure based on smart cards makes it possible to replace authentication based on passwords with public key authentication. To implement smart card based PKI,

smart card readers need to be installed in workstations, extra software is needed both in the client and server side to make use of the client authentication built in most network security protocols. Furthermore, procedures for issuing and distributing smart cards to network users have to be implemented.

FEIDHE is a project in Finnish universities and polytechnics whose goal is to develop smart card based authentication system for the needs of the Finnish higher education. The project aims at enabling an introduction of electronic identity smart card during year 2002. In the project a PKI and network protocols relying on it are piloted to establish a secure environment on top of which services requiring high security can be implemented.

References

[1] Electronic identity and Identity card. Ministry of Finance, Ministry of Transport and Communications, Ministry of the Interior, 16 September, 1996. http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/sidrap10.htm(in Finnish)

[2] The Police of Finland, Licence services. http://www.poliisi.fi/english/pi274en.htm

[3] Population Register Center, The Electronic ID card. http://www.fineid.fi/default.asp?path=1%2CGeneral%2FNews\amp{}template=

[4] A. Frier, P. Karlton, P. Kocher. The SSL 3.0 Protocol, Netscape communications, 18 November 1996. http://home.netscape.com/eng/ssl3/ssl-toc.html

[5] R. Housley, W.Ford, W. Polk, D. Solo. Internet X.509 Public Key Infrastructure Certificate and CLR Profile, Internet Engineering Task Force, RFC 2459, January 1999. http://www.ietf.org/rfc/rfc2459.txt

[6] M. Wahl, T. Howes, S. Kille. Lightweight Directory Access Protocol (v3), Internet Engineering Task Force, RFC 2251, December 1997. http://www.ietf.org/rfc/rfc2251.txt

[7] PC/SC Working Group. http://www.pcscworkgroup.com/

[8] Movement For The Use Of Smart Cards In A Linux Environement.http://www.linuxnet.com/

[9] Internet Engineering Task Force, Secure shell working group. http://www.ietf.org/html.charters/secsh-charter.html

[10] Internet Engineering Task Force, Kerberos working group. http://www.ietf.org/html.charters/krb-wg-charter.html

[11] Internet Engineering Task Force, IP Security Protocol working group. http://www.ietf.org/html.charters/ipsec-charter.html