

Fujitsu mPollux

MobiSign Security Option

White Paper

Fujitsu mPollux Version 1.9

October 2005



The programs described in this document may only be used in accordance with the conditions under which Fujitsu Services Oy supplies them.

This document is provided to your organization on the understanding that its content is and remains the intellectual property of Fujitsu Services Oy. The document is provided on the understanding that its use is confined to the people in your organization who are responsible for evaluating its content and that there is an obligation on your organization and such people within your organization to keep its content in confidence. This document may not, without the prior written authority of Fujitsu Services Oy, be copied or shown in whole or in part to any third party. When no longer required for the agreed purpose, the document is to be returned to Fujitsu Services Oy.

Fujitsu Services Oy endeavors to ensure that the information in this document is correct and fairly stated but does not accept liability for any error or omission.

The development of Fujitsu Services Oy products and services is continuous and published information may not be up to date. It is important to check the current position with Fujitsu Services Oy. This document is not part of a contract or license save insofar as may be expressly agreed.

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited. The Possibilities are Infinite is a trademark of Fujitsu Limited. mCastor, mProcess, mPollux, mPollux security options are trademarks or registered trademarks of Fujitsu Services Oy and Fujitsu Limited. Other product and company names mentioned herein may be trademarks or tradenames of their respective owners.

Table of Contents

| | | |
|-----|--|----|
| 1 | INTRODUCTION | 4 |
| 2 | SPECIFICS OF PKI BASED SECURITY | 4 |
| 3 | WHO WILL BENEFIT FROM THE MOBISIGN SECURITY OPTION?..... | 6 |
| 4 | MPOLLUX MOBISIGN™ USE SCENARIOS..... | 7 |
| 4.1 | General | 7 |
| 4.2 | MobiSign for Mobile Users | 8 |
| 4.3 | MobiSign for Web Users..... | 10 |
| 5 | OVERVIEW OF THE MPOLLUX MOBISIGN™ SERVER ARCHITECTURE..... | 11 |
| 5.1 | mPollux™ Base Functionality | 11 |
| 5.2 | Components of the mPollux MobiSign™ Security Option | 12 |

1 INTRODUCTION

The mPollux™ Security Server is Fujitsu Services' multifunction security solution, which can be easily adapted for the diverse needs and security level requirements of user organizations. This is made possible by the modular architecture of mPollux™ Security Server: the Server offers a number of Security Options and the user organization chooses the Option(s) that best suit(s) its needs.

This white paper describes the functionality of the **MobiSign Security Option** that is designed to support strong authentication and digital signature by mobile phone.

The mPollux™ Security Server with MobiSign Security Option consists of:¹

- The mandatory **mPollux™ Base** component, which implements the application interfaces through which mPollux™ is used, and common services like logging and an interface to a user database or directory.
- The Security Option, which can be utilized using **SIM Toolkit** technology and mobile operators' **mobile PKI** services.

2 SPECIFICS OF PKI BASED SECURITY

The MobiSign functionality is based on the application of cryptographic techniques, more exactly on **Public Key technology**. Public Key cryptography is based on the use of **key pairs**, one of which is private and the other public, hence the name of the technology. The **Public Key Infrastructure (PKI)** concept means the set of functions, components, and arrangements needed to use PKI based security in practice.

Setting up a Public Key Infrastructure requires the following actions:

- Defining a policy or principle of how the Public Key Infrastructure is organized and implemented in association with the service in question.
- Choosing Trusted Third Party/-ies used as Certification Authority/-ies (CA) in the environment.
- Organizing certificate issuing and revocation procedures with the chosen CA(s).
- Choosing and connecting to public or private directory /-ies that keep the users' certificates.
- Implementing the retrieval of user certificates and checking revocation lists with the directory service(s).
- Handling of encryption and signing operations and tamper-proof storing of service provider private keys.

¹ See the chapter "Overview of the mPollux MobiSign Server Architecture" for a more detailed description of the server architecture.

The implementation of the PKI can be based on standards (X.509 and PKCS#1-15) and standard tools offered by Certificate Authority (CA) and other vendors. PKI technology enables strong authentication, non-repudiation, confidentiality and integrity.

Implementation Assumptions

Certificates Users have existing certificates issued to them. The issuer can be corporate/private or public authority/party. Issued certificates are stored in a directory.

MobiSign / SIM Toolkit

The SIM Toolkit based implementation of mPollux MobiSign™ must always be done in co-operation with a mobile operator who is the issuer of the SIM and the owner of the SIM Toolkit application on the SIM. User private keys and certified public keys are normally generated and stored on the SIM card during the pre-personalization of the card. The key pairs could as well be generated on the card during its activation; the method chosen depends of the card issuer's policy and available public key infrastructure. A standard X.509 type certificate is used for both the user's certificate and the service provider's certificate (the certificate for the public key of the service provider). The certificates (or references to them) are stored on the SIM card.

SIM Toolkit is an ETSI/SMG standard for Value Added Services and e-commerce using GSM phones to do the transactions. It is widely supported by basically all GSM mobile phones introduced during 1999 and after.

SIM Toolkit programmed into the special GSM SIM card essentially enables the SIM card to drive the GSM handset interface, build up an interactive exchange between a network application and the end user and access or control access to the network.

3 WHO WILL BENEFIT FROM THE MOBISIGN SECURITY OPTION?

Mobile Users

mPollux MobiSign™ Security Option provides PKI based application level authentication and digital signatures for the mobile application environments.

Web Users

PKI based security is normally supposed to require that Web users have workstations with smart card readers and special PKI client software. These are, however, not in common use today. This has kept PKI based security from becoming popular, even though there is strong need in e-business for the kind of high-level security that one can achieve with PKI.

The mPollux MobiSign™ Security Option offers a different solution. The penetration percentage of GSM mobile phones is growing very quickly all over the world; already covering practically all households in several countries. It is also quite widely recognized that mobile phones are becoming trusted personal devices for their owners. These facts are the motivation for also using mPollux MobiSign™ for Web users. Instead of using specially equipped workstations, mPollux MobiSign™ allows the use of standard Web workstations. The smart card functions needed for high-security PKI are implemented in the SIM (Subscriber Identification Module, which actually is a smart card in itself) of the user's GSM phone. With mPollux MobiSign™, all authentication and digital signing functions needed when using a Web service are performed between the user's GSM phone and the mPollux™ Security Server. The actual application communication takes place on the Web connection in a normal manner.

4 MPOLLUX MOBISIGN™ USE SCENARIOS

4.1 GENERAL

The fundamental operation principles of mPollux MobiSign™ are the use of a GSM mobile phone as a user's "personal, portable smart card reader", and (with the exception of MobiSign mobile application users) the idea of performing security related communication (authentication and signature interchanges) on a separate, independent signaling channel, between the GSM phone and mPollux™ Security Server. This makes it possible to attach MobiSign Security functions to any kind of service capable of using the mPollux™ Security Server API. From a user's point of view, this means that one common method and security token (the phone and its SIM card) can be used to access different services; e.g., a mobile service and a Web service. From a service provider's point of view, this means that with one common solution, the mPollux MobiSign™ Security Server, strong PKI based security can be offered to users in a uniform manner regardless of the service they use.

The security services that mPollux MobiSign™ provides are user authentication and use of digital signatures for transaction non-repudiation and/or authentication of documents. Communication security for mPollux MobiSign™ users is achieved employing SSL/TLS on Web application.

4.2 MOBISIGN FOR MOBILE USERS

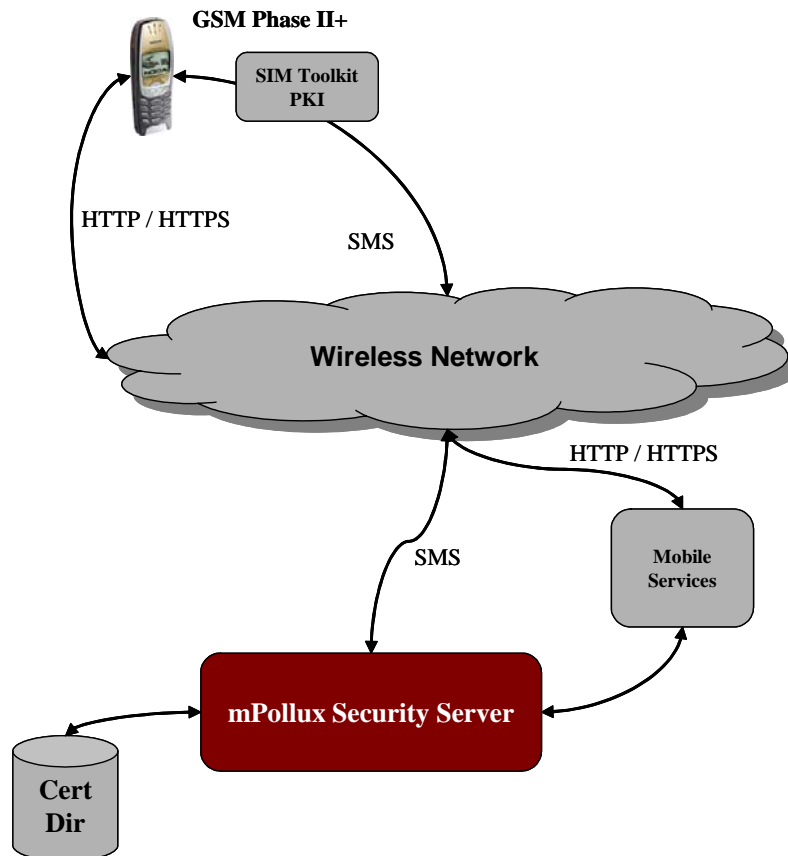


Figure 1 MobiSign for Mobile users

Figure 1 presents the scenario where mPollux MobiSign™ is used with mobile services. The user has a mobile phone that he/she employs for both application communication and security interchanges. Application communications take place over a standard mobile connection. The security interchanges take place over an encrypted SMS connection.

The only special requirement for the mobile service is the ability to use the mPollux™ API to invoke the required security operations.

The application level authentication of the user is based on a challenge message sent by mPollux MobiSign™ to the user's mobile device. The user has to sign it digitally by using his/her PKI certificate stored in the PKI application on the SIM. **Figure 2** shows the steps for mPollux MobiSign™ authentication. A similar sequence of steps takes place when mPollux MobiSign™ is used to digitally sign a transaction.

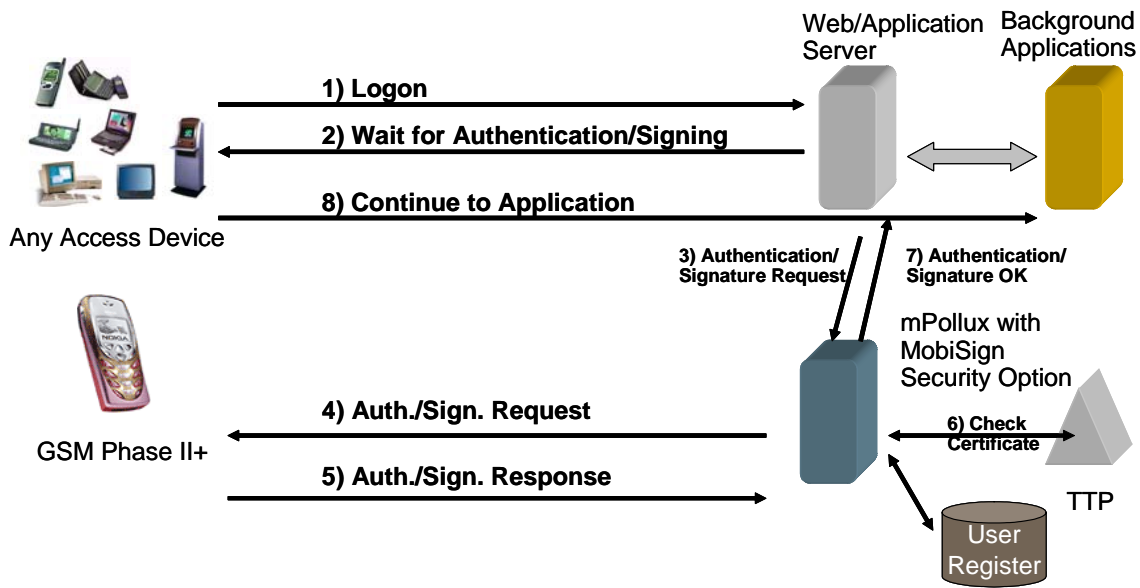


Figure 2 Authentication and Signing with mPollux MobiSign™

4.3 MOBISIGN FOR WEB USERS

Figure 3 presents the scenario where mPollux MobiSign™ is used with Web services. The user communicates with the Web service with a Web browser using a standard HTTP or HTTPS connection. Any device (PC, PDA, digital TV, ...) running a Web browser can be used as an application workstation. The only special requirement for the Web service is the ability to use the mPollux™ API. The user also needs a GSM mobile phone with a SIM containing the PKI application.

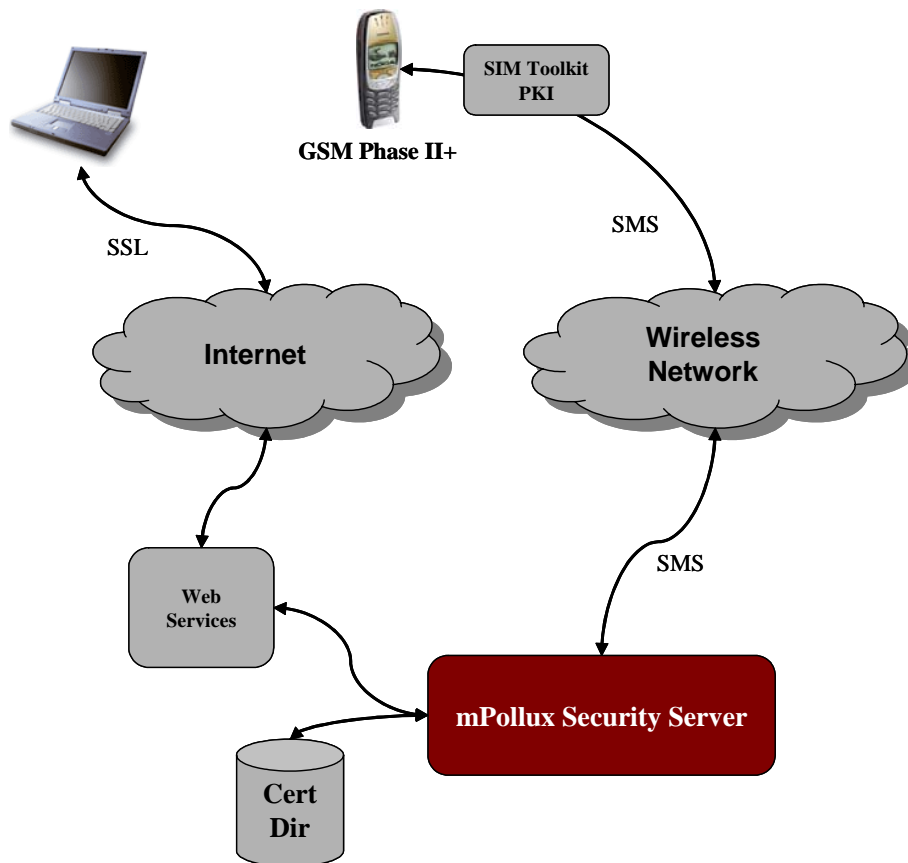


Figure 3 MobiSign for Web users

The authentication and possible digital signing operations take place between the mobile device and the mPollux MobiSign™ Server. SMS messages are the means of communication between the phone and mPollux MobiSign™. The flow of events and security protocols used are the same as described above for the mobile service case. The only difference is now that the application device and the authentication/signing device are not the same.

5 OVERVIEW OF THE MPOLLUX MOBISIGN™ SERVER ARCHITECTURE

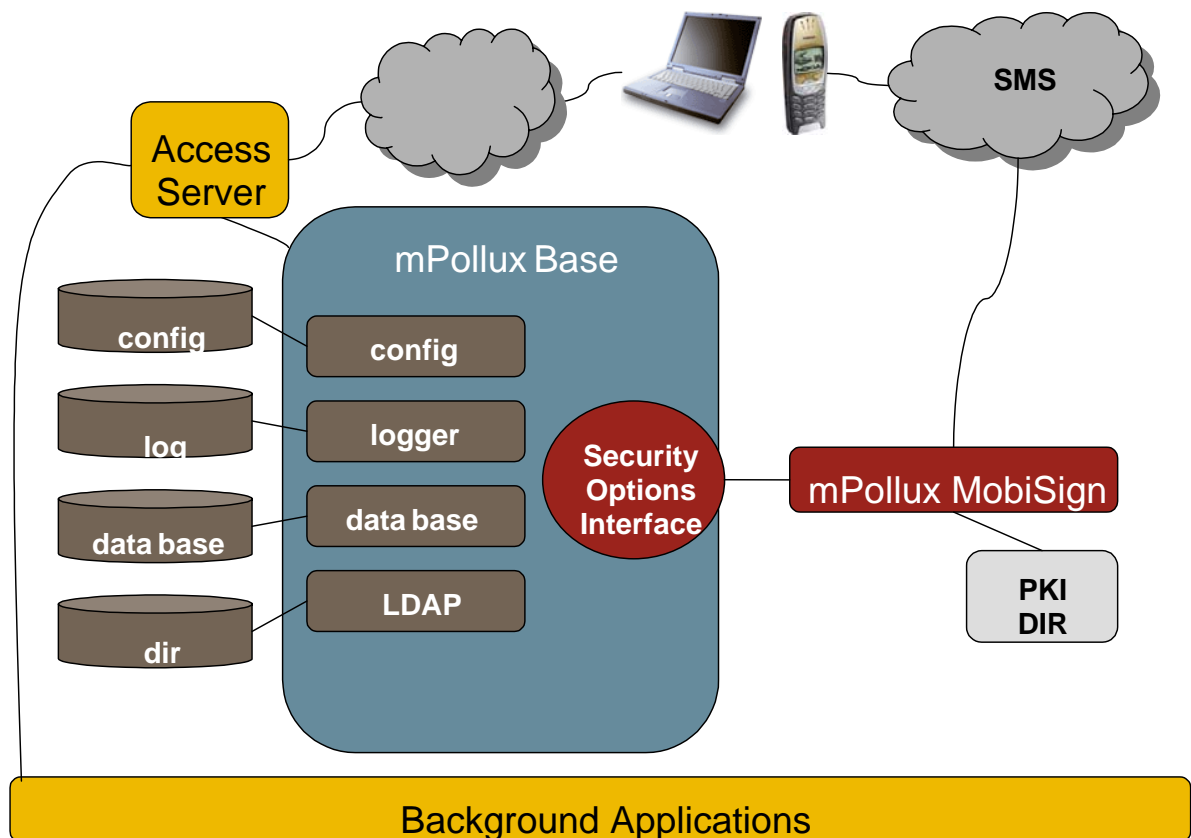


Figure 4 mPollux™ with the MobiSign Security Option Server Architecture

Figure 4 illustrates the general architecture of the mPollux™ Security Server with the MobiSign Security Option.

5.1 MPOLLUX™ BASE FUNCTIONALITY

Application Interfaces to mPollux MobiSign™

The Application Programming Interfaces to the mPollux MobiSign™ Security Option are implemented by the common mPollux™ Base component. Microsoft **.NET** and **Java** environments are supported.

Logging

The logging functions of mPollux™ Base are used to log all security related operations of the mPollux MobiSign™ Security Option.

Access to User Register

A user register is needed to store the information of mPollux MobiSign™ users. It can be a local database or a private or public **LDAP** directory. Access to this user database/directory is implemented as an mPollux™ Base function.

5.2 COMPONENTS OF THE MPOLLUX MOBISIGN™ SECURITY OPTION

PKI Interface (PKI IF)

The PKI Interface component takes care of the interfaces needed for **Certification Authority/-ies (CA)** and **Directory/-ies** containing user certificates and CRLs (**Certificate Revocation Lists**), and uses these to validate certificates used in authentication and digital signing operations. Certificate validation can be done for full **X.509 certificates**. Validation can be based on certificates received from user devices or **certificate URLs** as recommended by mobile PKI standards. The component also takes care PKCS#7 signature verifications. More than one PKI can be connected to an mPollux™ Security Server installation.

mPollux MobiSign™ Server

The mPollux MobiSign™ Server is the server side peer of the PKI client of the phone. It manages all the PKI operations and takes care of needed encryption/decryption operations on the server using the Java software components. The mPollux MobiSign™ Server communicates with the PKI client in the mobile device using SMS messages in the end-to-end security interchanges (authentication and digital signing protocols).

Mobile Devices

mPollux MobiSign™ sets some requirements on the mobile device. These requirements depend on the solution. SIM Toolkit based MobiSign requires a GSM phase II+ phone.