

Fujitsu mPollux

DigiSign 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 DIGISIGN SECURITY OPTION?.....	5
4	MPOLLUX DIGISIGN™ USE SCENARIOS.....	6
	4.1 General	6
	4.2 DigiSign for Web Users.....	7
5	OVERVIEW OF THE MPOLLUX DIGISIGN™ SERVER ARCHITECTURE.....	8
	5.1 mPollux™ Base Functionality	8
	5.2 Components of the mPollux DigiSign™ Security Option.....	9

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 **DigiSign Security Option** that is designed to support strong authentication and digital signatures by smart cards or software certificates.

The mPollux™ Security Server with DigiSign 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 implemented using standard x.509 certificate technology.

2 SPECIFICS OF PKI BASED SECURITY

The DigiSign 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 the certificate issuing and revocation procedures with the chosen CA(s).
- Choosing and connecting with the 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 DigiSign Server Architecture" for a more detailed description of the server architecture.

The implementation of the PKI can be based on standard tools offered by many vendors.

Implementation Assumptions

mPollux DigiSign™ is a pure server solution. Still, some client side components are needed for the full security functionality to be achieved.

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.
Smart Cards	A tamper-proof device for holding securely - among other things - user's private key and his certificate.
Client software	Software that communicates with the smart card reader, the software certificate and the browser are not currently part of mPollux DigiSign™. The implementation of these is based on standards like Microsoft Crypto API and PKCS#11 and offered by many vendors. mPollux DigiSign Client™ will be this kind of product later on.
Client hardware	When the client side PKI implementation is smart card based, smart card readers are needed at the client device. mPollux DigiSign™ does not include these hardware components.

3 WHO WILL BENEFIT FROM THE DIGISIGN SECURITY OPTION?

Web Users	PKI based security normally requires that Web users have workstations with smart card readers and special PKI client software. These are more and more commonly used today. This means that PKI based security is coming more popular. This is urged also by the requirement of e-business for higher-level security, which can be best achieved with PKI.
PKI Applications	Applications that need two basic PKI functions: X.509 certificate checking towards CRL and PKCS#7 signature verification.

4 MPOLLUX DIGISIGN™ USE SCENARIOS

4.1 GENERAL

The fundamental operation principles of mPollux DigiSign™ are the use of a smart card and smart card reader and the idea of performing security related communication (authentication and signature interchanges) on the same channel as application communication. It is possible to attach mPollux DigiSign™ 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 standard methods and security software and devices (card readers and smart cards) can be used to access different services. From a service provider's point of view, this means that with one common solution, the mPollux DigiSign™ 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 DigiSign™ provides are user authentication and the use of digital signatures for transaction non-repudiation and/or authentication of documents. Communication security for mPollux DigiSign™ users is achieved employing SSL/TLS on Web application connections.

4.2 DIGISIGN FOR WEB USERS

Figure 1 presents the scenario where mPollux DigiSign™ is used with Web applications. The user communicates with a Web application using a Web browser that employs a standard HTTPS connection. Any device (PC, PDA, digital TV, etc.) running a SSL/TLS enabled Web browser can be used as an application workstation. The only special requirement for the Web application is the ability to get a client certificate from the SSL/TLS session and to use the mPollux™ API. The user also needs a smart card or software certificate on the client side.

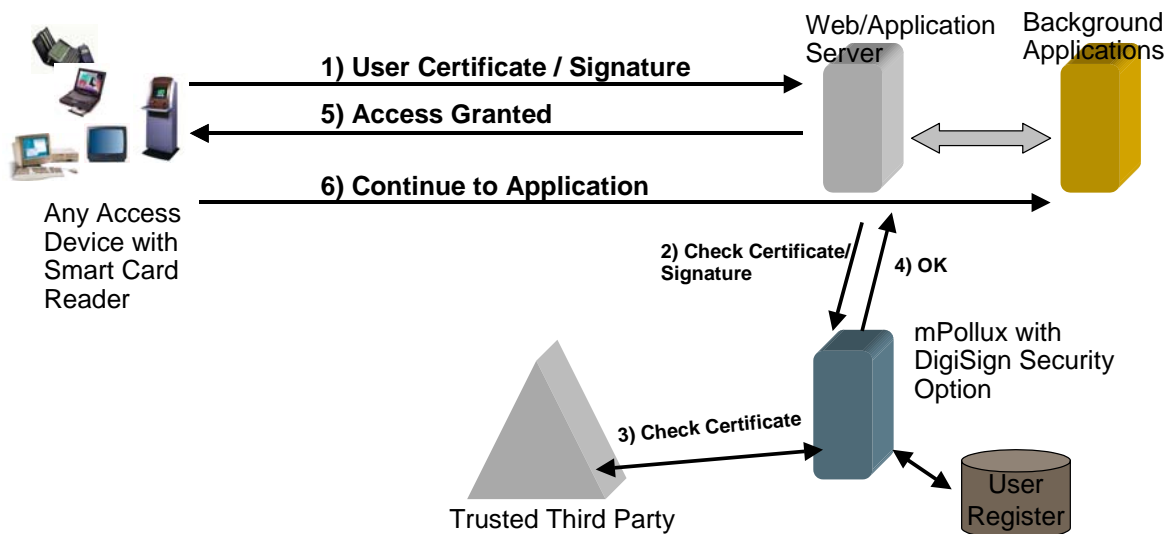


Figure 1 DigiSign for Web users

5 OVERVIEW OF THE MPOLLUX DIGISIGN™ SERVER ARCHITECTURE

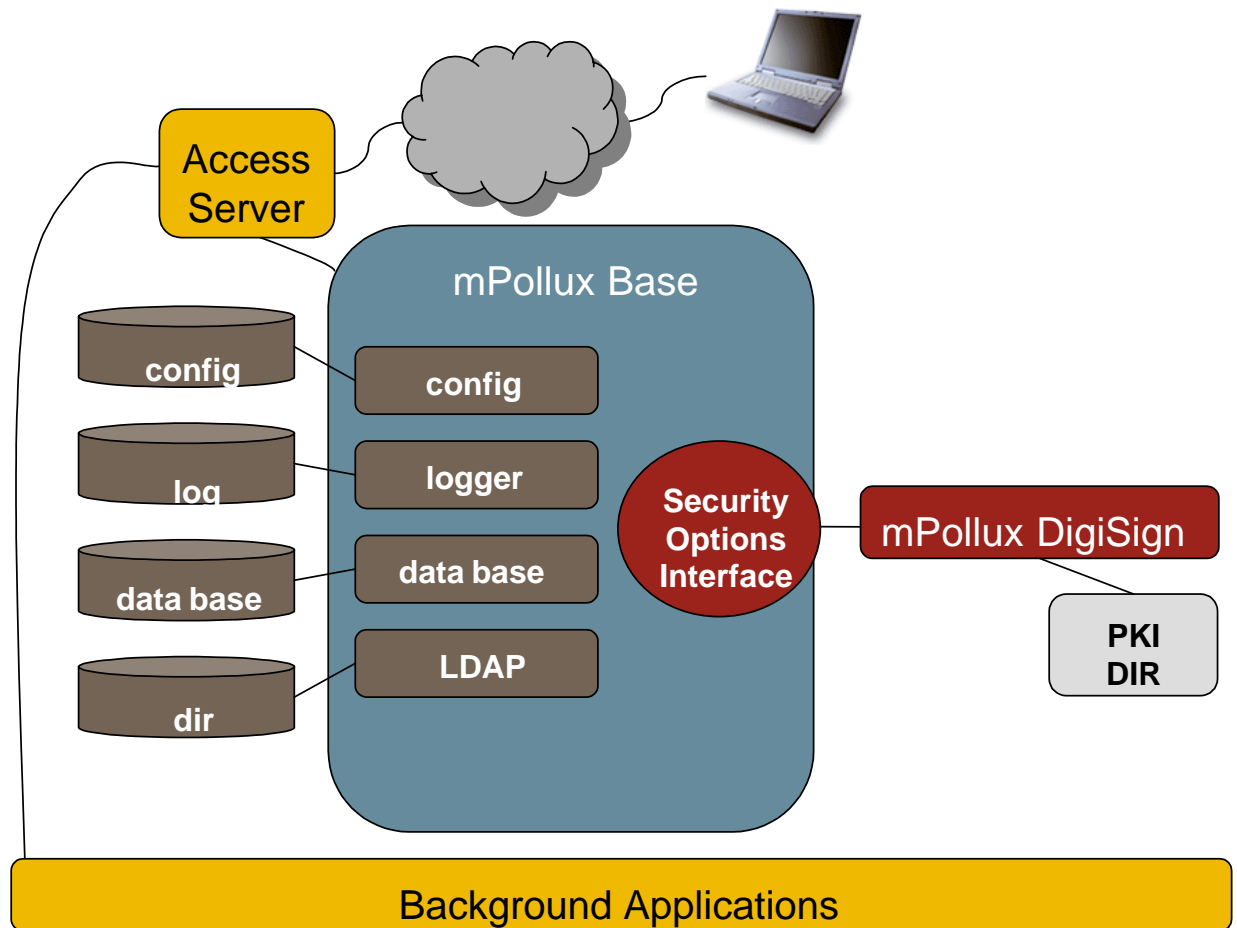


Figure 2 mPollux™ with the DigiSign Security Option Server Architecture

Figure 2 illustrates the general architecture of the mPollux™ Security Server with the DigiSign Security Option.

5.1 MPOLLUX™ BASE FUNCTIONALITY

Application Interfaces to mPollux DigiSign™

The Application Programming Interfaces to the mPollux DigiSign™ 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 DigiSign™ Security Option.

Access to User Register

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

5.2 COMPONENTS OF THE MPOLLUX DIGISIGN™ 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 **X.509 certificates**. Validation can be based on certificates received from user devices like smart card or so called software certificates. The component also takes care of PKCS#7 signature verifications. More than one PKI system can be connected with an mPollux™ Security Server installation.

mPollux DigiSign™ Server

The mPollux DigiSign™ Server is the server side peer of the smart card or software PKI client. It manages all the PKI operations and takes care of needed encryption/decryption operations on the Java software components.