



Fujitsu mPollux – *Security Server*

In the context of e-business, the security of communications is of ever growing importance. Several different schemes exist for the **authentication** of the involved parties and communicated messages, or for the insurance of transaction **confidentiality and non-repudiation**. Some of these schemes share common features and implementation level components and some don't.

Fujitsu mPollux empowers the e-business operator run a security service that allows **the choice of the most suitable security scheme** for each purpose; hides the differences of various security schemes; and **enables usage through one unified interface**.

mPollux is a modular, multi-function, multi-technology system that provides a state-of-the-art solution to the requirements of quickly changing business needs and operating environments. When the requirements evolve over time, the functionality can be maintained and enhances with the addition of relevant new options.

mPollux means new, more efficient and user-friendly ways to use services - in other words independently of time and device. It outsources enterprise's customer service process so that the end-customer manages the process by itself and uses the best suitable way and device while doing it. No matter what the service, device or service value, the service can be offered to the requested security level.

Security services are implemented as "common services" for all applications and services.

mPollux security services provide answer to **all levels of identifying, authenticating, signing, encrypting** etc. requirements. Security level can be of high standard when needed – or the user of the service may choose the easiest way he/she is used to.

mPollux is designed to secure primarily web and wireless applications. **It provides authentication and authorization services that can be used to control access to a single application, or to implement a Single Sign-On access control system for various applications.** Several different authentication methods are supported. Authorization functions can be implemented combining the use of mPollux services and the access features of the Web Server product in use. The service can also generate and check digital signatures and it is also able to provide a link to time stamping services as well.

mPollux provides a good foundation to develop and implement new customer operation models for all services and products in different security scenarios. It allows a **flexible way to proceed to using new technologies and utilizing existing solutions to enhance and improve services.**

mPollux Security Server Products

The **mPollux Security Server** is a set of security products that can handle applications' security requirements in multi-channel environments.

The API provided by mPollux Security Server includes functions for authentication, digital signature, encryption, and time stamping.

Authentication function varies from a simple verification of stored user information to a more complex sequence where the user device, the application server, and the mPollux Security Server select and verify PKI (Public Key Infrastructure) certificates. mPollux Security Server also support biometric authentication methods, such as Fujitsu Palm Vein.

mPollux Security Server consists of **mPollux Base** and at least one **Security Option**. Additional Security Options may be added as needed. The mPollux Base is a mandatory component, which implements the application interface, basic User Register access and logging. The system uses a database or an LDAP directory as the user register.

mPollux WebFront can be used to implement access control for web and non-web applications. It functions as a firewall and/or as a HTTP reverse proxy.

Selected set of mPollux Security Options work together with mPollux Base to implement the security functionality required.

Security Options:

- **mPollux CallSign, a multi-factor authentication and authorization facility for easy entry to mobile security.** Any (mobile) phone can act as the user terminal and it is not tied to any specific application area. In practice CallSign implements a challenge-response protocol over normal voice call link.
- **mPollux PalmSign is biometric authentication mechanism which is based on Fujitsu Palm Vein technology and sensor hardware.**
- **mPollux DigiSign** supports authentication and digital signatures based on **PKI smart cards and standard X.509 certificates.**
- **mPollux MobiSign** provides **wireless PKI** solution for current mobile phones. It makes the mobile phone your personal trusted device. With mPollux MobiSign, mobile phone is a smart card and smart card reader in your pocket.
- **mPollux SMS** provides **challenge-response** type of authentication over mobile short message channel.
- **mPollux Classic** is traditional **username and password based authentication mechanism** which can re-use existing user registers like LDAP, SQL DB and Kerberos V5.

