White Paper
mPollux™ DigiSign

Fujitsu's Identity and Access Management product family for secure use of e-business services.

Contents

Authentication Options

mPollux™ Authentication services provide a suite of security options for authenticating users, each with the authentication scheme of its own.

- By definition, strong authentication means authentication that is based on at least two of the following factors:
  - Something that the user knows (for example, password or PIN code)
  - Something that the user possesses (for example, a smart card)
  - Something that the user is (biometrics, for example palm vein diagram)
- mPollux™ offers several options for strong authentication. DigiSign implements smart card based authentication services.
- Genuine PKI-based digital signatures implemented with DigiSign enable integrity of signed data (any changes to the data make the signature invalid) as well as authentication and non-repudiation (the certified identity of the signer is associated with the signature in a way that it can't be forged). User signatures are enabled by the PKI based security options. In addition, mPollux™ provides a security option that enables applications to make system signatures of their own.
- All the PKI based security options include certificate validation. Certificates are validated both when signing documents and when verifying signatures. Validation checks that the certificate is syntactically valid, not forged, not out of date and not on the revocation list of the Certificate Authority that issued it. Validation of a given certificate is included in all the PKI based security options also as a distinct function. mPollux™ supports LDAP in access to certificate revocation lists.
- DigiSign authentication service needs information about users. Either a directory or database pointed out by the customer, or a separate user register dedicated for DigiSign can be used.

1 mPollux™ DigiSign

Authentication and digital signatures using a smartcard

The mPollux™ DigiSign option provides authentication that is based on PKI-empowered smart cards. The chip of such a smart card contains

- a standard X.509 certificate that gives the certified identity of the user,
- a private key associated with the identity on the certificate, and
- a PIN code that the user must give when responding with her private key to the cryptographic authentication challenge.

The DigiSign option uses SSL/TLS client authentication technique to verify the user's identity. The user's access device must support that, and must have a smart card reader with appropriate reader software (for example, mPollux™ DigiSign Client). DigiSign option also validates the user's certificate in conjunction with authentication. A part of that is checking against the Certificate Revocation Lists of the issuer of the certificate. For that purpose DigiSign supports the LDAP protocol.

DigiSign provides strong authentication, because it is based on the following two factors:

- Something that the user possesses: the smart card that contains certificates for different purposes and associated private keys of the user.
- Something that the user knows: the PIN code that enables the user to use the smart card for authentication and electronic signatures.

In the future also USB tokens are planned to be supported by DigiSign in addition to smart cards.

2 mPollux™ DigiSign services

DigiSign support many optional mechanisms to authenticate a user or to sign documents. It also incorporates several self-service features for end-user.

2.1 Authentication

DigiSign authentication operates with certificates securely stored on the PKI card and a PIN number that user enters from keyboard. Once the Client Authentication sequence has been conducted between the workstation and server, the server can retrieve user information from the CA related to the user's authentication certificate. A Certificate Revocation List can be consulted to check if the certificate is still valid.

2.2 Digital signatures

DigiSign client can be used to create digital signatures by using operating system's standard interfaces or with the help of web interface.

DigiSign also enables an application to ask its user to sign an electronic document with her smart card.

If the DigiSign Client is used in the workstation as card reader software, it allows the user to see the text before signing it.

2.3 PIN change

With DigiSign the administrator can force a PIN change to a user. This means that the user is authenticated with existing PIN and chooses a new pin that is written to the card.

2.4 Enrolling and managing smart card content

DigiSign user can personalize or upgrade smart card content with number of different methods.

3 Optional mPollux™ DigiSign applications

3.1 mPollux™ DigiSign Server Application

DigiSign Server Application can be used to handle PKI based authentication of users and pass user credentials to customer's business applications. This requires an interface to customer's user registry (for example MS AD, a SQL database or a LDAP directory). DigiSign can also manage a Card Revocation List and download it periodically from related CAs.

DigiSign Server is client's server side counterpart providing centralized access point for many PKI & certificate management related tasks. DigiSign Server can be used for retrieving certificates from CAs, initializing smart card and handling smart cards' contents, making digital signatures and managing certificate and smart card life cycle and other PKI and certificate related tasks. DigiSign Server supports scripting language, which can be used for easy and efficient creation of PKI, cryptography and certificate handling related web applications and services.

3.2 Card production management

DigiSign contains a card management application that can be used to personalize new PKI cards.

4 Supported standards

DigiSign supports following standards. Note that this list is evolving with new supported standards, so please check the real-time situation with Fujitsu Finland Oy.

Supported general digital certificate related standards
- X.509
- PKCS#5, PKCS#7, PKCS#10, PKCS#12
- CMP, CMC

Supported signature related standards
- PKCS#1, PKCS#7, XML-DSIG

Supported reader driver interfaces
- PC/SC

Supported smart card operating systems
- Aventra MyEID applet for JCOP
- Oberthur IAS-ECC v1.0.1
- Oberthur FINEID applet
- Gemalto EID2048 applet
- SetCOS Java EID applet
- SetCOS 4.3.1, 4.3.2 and 4.4.1
- MIOCOS v1.1 or newer (Atmel)
- MIOCOS v2.3 (Fujitsu FRAM)

Supported standard Cryptographic interfaces
- Cryptography API: Next Generation (CNG)
- CryptoAPI v2.0
- PKCS#11 v2.01
- OS X Tokend

Supported cryptographic algorithms
- MD4, MD5, SHA (different variants)
- RC-2, DES, 3-DES, AES, RSA, ECDSA, ECDH

Supported cryptographic protocols
- SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2

Other Supported interfaces
- DigiSign Toolkit (DLL)
- WebSigner and WebToolkit
- SCS

5 Supported platforms

DigiSign is supported on the following platforms. Note that this list is evolving with new platform versions, so please check availability of current supported versions from Fujitsu Finland Oy.

- Microsoft supported Windows versions for desktop and server use
- Linux SUSE Enterprise Desktop
- Red Hat Enterprise Linux
- Linux Ubuntu
- CentOS Linux
- Mac OS X and iOS

For more information, please contact:

Fujitsu Finland Oy
mPollux-Sales@fi.fujitsu.com