Fujitsu mPollux DigiSign Client
Technical References

This reference document contains technical information necessary for system administrators, who are installing Fujitsu mPollux DigiSign Client in their IT system.

Contents

1	DigiSign Client smart card reader software	3
1.1	Supported operating systems and standards	3
1.2	References	3
2	Installation	4
2.1	Installation in Windows operating systems	4
2.2	Notes for Cryptoki application users	4
2.3	Notes for Cryptoki developers	4
2.4	Notes for Citrix users	4
2.5	Notes for Oracle SSO users	4
3	DigiSign Client and mPollux Service Manager settings	4
4	DigiSign Toolkit	6
5	Smart Card Minidriver	7

1 DigiSign Client smart card reader software

Fujitsu mPollux DigiSign Client software can be used with a smart card for secure access to electronic services or organization networks or for signing documents or email messages electronically.

1.1 Supported operating systems and standards

DigiSign Client supports the following operating systems and standards.

Supported operating systems and standards	
Computing operating systems	Microsoft Windows 8 32/64 bits Microsoft Windows 7 32/64 bits Microsoft Windows Vista 32/64 bits Microsoft Windows XP Microsoft Windows Server 2012 Microsoft Windows Server 2008 and 2008R2 Microsoft Windows Server 2003 32/64 bits Linux SUSE Enterprise Desktop Red Hat Enterprise Linux Linux Ubuntu Mac OS X v10.7
Reader driver interfaces	PC/SC
Smart card operating systems	MIOCOS v1.1 or newer (Atmel) MIOCOS v2.3 (Fujitsu FRAM) SetCOS 4.3.1, 4.3.2 and 4.4.1 SetCOS Java EID applet Gemalto EID2048 applet Aventra MyEID applet for JCOP Oberthur FINEID applet Oberthur IAS-ECC v1.0.1
Cryptographic interfaces	Cryptography API: Next Generation (CNG) CryptoAPI v2.0 PKCS#11 v2.01
Other interface standards	DigiSign Toolkit (DLL) HTTP interface for the signature component HTTP interface for personalizing smart cards
Cryptographic algorithms	MD5, SHA (different variants) RC-2, DES, 3-DES, AES, RSA

1.2 References

The following documentation is provided with the software:

- *Fujitsu mPollux DigiSign Client Technical References* (this guide)
- *Fujitsu mPollux DigiSign Client Installation and User Guide – Windows*
- *Fujitsu mPollux DigiSign Client Installation and User Guide – Linux*
- *Fujitsu mPollux DigiSign Client Installation and User Guide – Mac OS*

2 Installation

2.1 Installation in Windows operating systems

In the Windows operating system, you can install the DigiSign Client by using the installation wizard (see *Fujitsu mPollux DigiSign Client Installation and User Guide – Windows*) or silently.

The following command installs DigiSign Client silently without the wizard or the background image. Only installation progress is shown.

```
# <DigiSign installation package> /SILENT
```

The following command installs DigiSign Client silently without even the installation progress.

```
# <DigiSign installation package> /VERYSILENT
```

2.2 Notes for Cryptoki application users

You can find Cryptoki, the PKCS#11 module named `cryptoki.dll`, in the installation directory. The installation directory has changed from `Program Files\Fujitsu Services` to `Program Files\Fujitsu`.

2.3 Notes for Cryptoki developers

By default, the secondary authentication mechanism (auto-login) is enabled. If auto-login causes logical application errors, you can disable it by setting the value of the `disableCryptokiAutoLogin` registry key or environment variable to `1`.

2.4 Notes for Citrix users

The following settings are recommended:

- Disable the smart card cache (`doNotUseSmartCardCache=1`)
- Enable the smart card serial number cache (`SmartCardSNCache=1`)
- Define the path to the smart card cached and set full rights to all users (`SmartCardCachePath`=<set path>)

For more details, see Chapter 3, DigiSign Client and mPollux Service Manager settings.

2.5 Notes for Oracle SSO users

If you are using a smart card provider, set the value of `cspGetKeyParamCompatibilityMode` registry key to `1`. This changes the behaviour of the `GetKeyParam()` function so that the smart card authenticator of Oracle SSO can locate the correct key container and certificate.

Setting `cspGetKeyParamCompatibilityMode` registry key to `1` causes the WS2008 certificate enrolment to fail.

3 DigiSign Client and mPollux Service Manager settings

This section describes the settings that can be used to change the behavior of DigiSign Client and mPollux Service Manager. The settings can be found in the following locations:

- Windows registry settings:
  - Registry keys in Windows 32-bit operating systems:
    - `HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\DigiSign Client`
    - `HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\mPollux Service Manager`
  - Registry keys in Windows 64-bit operating systems:
    - 64-bit applications:
      - `HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\DigiSign Client`
    - 32-bit applications:
      - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\DigiSign Client`
      - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\mPollux Service Manager`
- File in Linux: `DigiSign.conf`

■ File in Mac OS: com.fujitsu.DigiSign.conf

DigiSign Client and mPollux Service Manager settings

Key	Default value	Description
aboutDialogBitmap	Empty	Default path to the image in the About dialog and tab.
acceptEmptyPIN	0	If set to 1, users can log in without providing a PIN code.
addCertFriendlyName	0	If set to 1, DigiSign shows friendly names for certificates if available. Note that all VPN programs do not accept friendly names.
addAllCspKeyContainers	0	If set to 1, DigiSign generates key containers that do not contain certificates. Some programs only work with containers that contain a certificate. In that case, set the value to 0.
buildReaderListTimer	5	The interval in seconds in which DigiSign polls the smart card. If you are using DigiSign through a slow remote connection or a thin client, increase the value to reduce the polling frequency.
certExpirationWarningDays	30	The number of days prior to certificate expiration when DigiSign displays a warning about the expiration.
disableNonRepPurpose	0	Windows only: If set, the use of PIN2 is disabled.
closeBrowsersConfirm	0	If closeBrowsers is set, ask confirmation form the user before closing the browsers
closeBrowsers	0/1	Depending version; Tries to close web browser when card is removed from the reader
closeBrowsersExcludeReader		Do not close browsers if received event comes from this reader. Same wildcards are allowed than in 'excludeReader'
cryptoProvider	mPolluxCSP.dll	Internal use only.
cspGetKeyParamCompatibilityMode	0	If set to 1, some applications might work better.
DataPath	Depends on the operating system	Linux and Mac only: The pipe path.
doNotUseSmartCardCache	1	If set to 1, DigiSign reads the smart card instead of the cached card information. Setting this on slows down the usage.
dropAuthentication	0	If set to 1, the user must re-authenticate after each RSA operation.
disableAuthTab	0	If set to 1, the Authentication tab in DigiSign Manager is hidden.
disableCryptokiAutoLogin	0	If set to 1, the DigiSign PIN dialog is disabled. The user is shown the program's own dialog with the program's own functionality.
disableCryptokiBufferCheck	0	If set to 1, the set buffer size for cryptoki may be exceeded.
disableCryptokiPIN2Slot	0	By default, cryptoki creates to slots for PIN codes, one for Pin 1 and another for PIN2. If set to 1, PIN 2 is disabled.
excludeReader	Empty	A list of those PC/SC (Personal Computer/Smart Card) readers that DigiSign should ignore. This list enables DigiSign to be used in computers that have several card readers. In the list, wild cards are allowed; for example, *O2*||*CCID* ignores all readers that contain the substring O2 or CCID.
forceSelectApplet	0	If set to 1, DigiSign always selects the EID applet at startup.

forceGUI_ModeLocal	0	If set, the graphical user interface (GUI) is always loaded into a local process instead of the mPollux Service Manager.
HTTPToolkitEnabled	0	If set to 1, enables the httpToolkit interface that can be used for creating spare cards on work stations.
HTTPSignerDisabled	0	Some anti-virus programs consider the HTTP signer service as malware. Setting this value to 1 disables the HTTP signer service.
keyGenCheatMode	0	Windows only: By default, a new key is generated for the card when logging in to the organization domain, thus disabling the use of write-protected smart cards. If set to 1, existing keys are used, allowing the use of write-protected smart cards.
Language	Empty	Sets the language for the user interface. The possible values are `fi` (Finnish), `en` (English), and `sv` (Swedish).
managerBannerBitmap	Empty	The path to the default banner image in mPollux Service Manager.
modulePath	Depends on the operating system	The path to the dynamic libraries.
onlyDigiSignCertificates	0	If set to 1, the DigiSign Toolkit only returns certificates that are assigned against DigiSign.
pinDialogBitmap	Empty	The path to the default image in the PIN dialog.
pkcs15crt	1	If set to 1, DigiSign writes the CRT components of the RSA key to the key file in the smart card. All smart cards do not work with CRT components. In that case, set this value to 0.
SmartCardCachePath	Depends on the operating system	The path to the temporary directory for the smart card cache files.
SmartCardSNCache	0	If set to 1, the contents of the smart card is stored based on the card's serial number. This may speed up the card usage, but if the contents are changed, the changes are not shown on other work stations.
safeMode	0	When a smart card is removed from the card reader, the program may not always notice it immediately. If usage of the program must only be possible when the card is inserted (for example, banking applications) set this value to 1. The program will work slower, but the usage will be interrupted immediately when the card is removed.
SmartCardCacheKeep	0	If set to 1, the smart card cache file is not removed when the card is removed. This is useful when it must be possible to use the card with slow remote connections. This requires special implementation for the program.
showAsn1CertInWindows	0	If the operating system supports showing the contents of the certificate, the contents are shown in the format set by the operating system. If this value is set to 1, the certificates are always shown in ASN.1 format, regardless of the operating system capabilities.
userLevel	0	If set to 1, the graphical user interface (GUI) is shown in advanced mode where you can delete keys or certificates.

4 DigiSign Toolkit

The DigiSign Toolkit is a C interface that is included in the DigiSign Client Windows installation package. The Toolkit allows you to program your own system to use DigiSign Client. The Toolkit provides functions such as the following:

- Searching for user certificates
- Computing and verifying digital signatures

- Authenticating against the mPollux Server
- Transmitting Certificate Management Protocol (CMP) messages to different Certificate Authority (CA) systems

After default installation in Windows environment, you can find the Toolkit in the following directory:

```
C:\Program Files\Fujitsu\mPollux DigiSign Client\Toolkit
```

For more information on the Toolkit, see the `DigiSign_Toolkit.h` file in that directory.

5 Smart Card Minidriver

Beginning from version 3.5, mPollux DigiSign Client includes a Windows Smart Card Minidriver for CryptoAPI and Microsoft Cryptography API: Next Generation (CNG). In the minidriver model, common interface for all smart cards is provided by Microsoft Base Smart Card Crypto Provider and Microsoft Smart Card Key Storage Provider, and minidriver provides the card specific functionality. Card related user interfaces are in most cases provided by Windows. In the current version read only functionality of Windows Smart Card Minidriver Specification is supported up to version 6.

mPolluxCSP is still installed and can be used by acquiring a CryptoAPI context explicitly or by setting it as the default provider for the supported smart cards in registry.

Contact
FUJITSU FINLAND OY
Address: PL 100, 00012 FUJITSU
Phone: +358 29 302 302
Website: www.fujitsu.com/fi