Release Notes

Date: 9th July 2012

Document Reference: D1265346A

This document presents information about Classic Client 6.2 – Patch 2 – 001.
It shows what has changed since Classic Client 6.2 – Patch 1 – 001.

What's New?

Corrected Problems

The following problems have been corrected in this version:

- The ATR for the "Other Optelio Card (Santander MPCOS)" has been corrected.
- A shortcut name has been corrected (secutity to security).
- When the user automatically registers Classic Client as a security module in Firefox, Firefox displays a warning to say "A script from "file://" is requesting enhanced abilities that are UNSAFE and could be used to compromise your machine or data". This is normal, but could alarm the user. Consequently, a note has been added to the HTML page that displays during the registration, telling the user that a security warning may display but it is safe to authorize the installation.
- A problem existed when using a PIN pad reader when the PIN policy file was corrupted. This has been corrected so that now, if the PIN policy file is corrupted, the PIN pad reader uses a default PIN policy.

Supported Operating Systems and Applications

This release supports more recent versions of some applications. For information about the new versions of applications that are now officially supported by Classic Client 6.2, refer to "Supported Operating Systems and Applications" on page 2.

What's Gone?

For information about the old versions of applications that are no longer officially supported by Classic Client 6.2, refer to "Supported Operating Systems and Applications" on page 2.

What's In?

This section provides a full list of hardware, operating systems, peripherals and software that are supported by Gemalto for use with Classic Client 6.2. It also lists the minimum system requirements to run Classic Client correctly.

System Requirements

Computers on which Classic Client is to be installed must have at least:

- 1 Gigahertz (GHz) processor or faster for 32-bit or 64-bit versions of Windows
- 1 GB of RAM for 32-bit versions of Windows
- 2 GB of RAM for 64-bit versions of Windows

Pre-requisites

The computer must have the following software installed:

- .NET Framework version 2.0 or later.

Supported Operating Systems and Applications

The Administrator version is available only for 32-bit OS. However, from this, the Administrator can generate User Setups for 32-bit OS and 64-bit OS.

The following table lists the versions that are supported and indicates if a version has been added or removed. Other applications may also work successfully, but have not been validated. For information about the compatibility of Classic Client 6.2 with applications not in this list, please contact your Gemalto technical consultant.

Table 1 - Supported OS and Applications

Windows OS Version	**Supported (Added/ Removed)**
Windows XP Home (SP2 and SP3) – 32-bit only	
Windows XP Professional (SP2) – 32-bit and 64-bit	
Windows XP Professional (SP3) – 32-bit	
Windows Vista SP1 and SP2 – 32-bit and 64-bit	
Windows 7 – 32-bit and 64-bit	
Windows Server 2003 R2 SP2 – 32-bit and 64-bit	
Windows Server 2008 (up to SP2) – 32-bit and 64-bit versions	
Windows Server 2008 R2	
Browsers	
Internet Explorer 7, 8 and 9	
Mozilla Firefox 12.0	
Mozilla Firefox 13.0	Added
Google Chrome 19	
E-mail Applications	
Mozilla Thunderbird 12.0	
Mozilla Thunderbird 13.0	Added
Microsoft Outlook 2003 SP1, 2007 and 2010	
Other Applications	
Microsoft Office 2003 (up to SP1), 2007 and 2010	
Adobe Acrobat 9 – for document encryption and signature	

Table 1 - Supported OS and Applications (continued)

Windows OS Version	Supported (Added/ Removed)
Adobe Acrobat Reader 8 and 9 – for document signature	
Citrix Metaframe Presentation Server 4.5 on Microsoft Server 2003 (with Fat and Thin Clients)	
Citrix Metaframe Xenapp 5.0 on Microsoft Server 2008 (with Fat and Thin Clients)	
Citrix Metaframe Xenapp 6.0 on Microsoft Server 2008 R2 (with Fat and Thin Clients)	
Microsoft Windows 2003 CA for certificate enrollment and renewal	
Microsoft Windows 2008 CA for certificate enrollment and renewal	
Terminal Services with Windows Server 2003 R2 SP2 and Windows Server 2008 – 32-bit and 64-bit versions in both cases. Also Windows Server 2008 R2. (These are supported for Fat and Thin clients)	
Entrust Authority 7.1 for certificate enrollment and renewal (not Entrust Certified)	
Gemalto eSigner 4.2.17 (3.0.X is supported on Windows XP and Vista for customers that have these versions deployed and need to migrate to Classic Client 6.2)	
Intercede MyID v8 SP1 for certificate issuance and management (revocation, renewal etc.)	
Windows BitLocker Drive Encryption (Windows 7 only)	

Supported Readers

This section provides a list of the readers supported by Classic Client 6.2 and, for each reader, the drivers that need to be installed and the OS that are compatible.

Contact:

Reader Name	Old Name	Driver	Compatible OS
PC Card	GemPC Card for laptops	PCCard 4.0.2	32-bit & 64-bit
PC Express	GemPC Express	CCID 4.0.3	32-bit & 64-bit
USB Shell Token V2	GemPCKey	CCID 4.0.3	32-bit & 64-bit
PC Twin	GemPC Twin	CCID 4.0.3	32-bit & 64-bit
USB e-Seal Token V2	Gem e-Seal	eSealP 1.0.0	32-bit
PC USB-SL and PC USB-TR	GemPC USB	CCID 4.0.3	32-bit & 64-bit

Secure PIN Pad Readers

- PC Pinpad (driver is PinPad 4.0.7.5 - compatible with 32-bit and 64-bit OS)
- GCR 5500
- Dell keyboards - SK-3105, SK-3205 and RT7D60

Fingerprint Scanners

- DERMALOG ZF1 single finger scanner
- UPEK TouchChip TCS1
- Futronic FS80: single finger scanner
- Covadis Auriga Scanner

Supported Smart Cards

This section lists the cards supported by Classic Client 6.2 and their Answer To Resets (ATRs) and mask numbers. These values are all in hexadecimal.

- Classic TPC IXS (Classic Applet V1)
- Classic TPC IXS (Classic Applet V1) - IdenTrust version
- Classic TPC IS (Classic Applet V1)
- Classic TPC IS v2 (Classic Applet V2 default - V1 on demand)
- Classic TPC IS CC (Classic Applet V2)
- Classic TPC IM (Classic Applet V1) - IdenTrust
- Classic TPC IM (Classic Applet V2)
- Classic TPC IM CC (Classic Applet V2 default - V1 on demand)
- Classic TPC IM CC v3 (Classic Applet V3)
- TPC DM (contact and contactless) (Classic Applet V3) - same as MultiApp ID Dual Citizen EAC 80K CC
- Optelio D38-D72 R6 (Classic Applet V2)
- Optelio Contactless D72 R6 (Classic Applet V1)
- Optelio Contactless D72 R4 WR (Classic Applet V3)
- Optelio Card (Santander MPCOS) .
- MultiApp Easy 72K Type B (with IAS Classic Applet V2)
- MultiApp Combi 72K Type B (with IAS Classic Applet V2)
- MultiApp ID Combi 72K Type A (with IAS Classic Applet V2)
- MultiApp ID IAS ECC 72K CC (with IAS XL / IAS ECC Applet)
- MultiApp ID Citizen 72K CC (with IAS Classic Applet V3)
- MultiApp ID 72K (with IAS Classic Applet V2)
- MultiApp ID 144K (with IAS Classic Applet V2)
- MultiApp ID Dual Citizen EAC 80K CC (contact and contactless) (with IAS Classic Applet V3)
- MultiApp ID Dual Citizen EAC 144K CC (contact and contactless) (with IAS Classic Applet V3)
- TOP DM GX4 - MPH51 - dual (contact and contactless) card with Classic Applet V1.
- TOP DL V2 - Dual (contact and contactless) card (with Classic Applet V3).
- IAS TPC (with IAS XL / IAS ECC applet)
- MultiApp V2.1 (with IAS XL / IAS ECC applet and IAS Classic Applet V3)

ATRs

This section lists the ATRs for each card family. Those figures indicated in red and bold can differ from one card to another in the same family. All values are in hexadecimal.

Classic TPC (IXS, IS, IS V2, IS CC, IM, IM CC, IM CC V3, DM) / MultiApp ID Cards

[T=0] 3B 7D **00** 00 00 80 31 80 65 B0 **00 00 00 00** 83 **00** 90 00

[T=1] 3B FD **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 83 **00** 90 **00 00**

[T=0] Warm Reset: 3B 6D 00 00 80 31 80 65 B0 83 **00 00 00** 83 00 90 00

[T=1] Warm Reset: 3B ED 00 00 81 31 20 43 80 31 80 65 B0 83 **00 00 00** 83 00 90 **00 00**

Other TPC Cards (with MPCOS Applet)

[T=0] 3B 7A **00** 00 00 80 65 A2 **00 00 00 00** 72 D6 **00**

[T=1] 3B FA **00** 00 00 81 31 **00** 43 80 65 A2 **00 00 00 00** 72 D6 **00 00**

[T=0] Warm Reset: 3B 6A 00 00 80 65 A2 **00 00 00 00** 72 D6 **00**

[T=1] Warm Reset: 3B EA 00 00 81 31 20 43 80 65 A2 **00 00 00 00** 72 D6 **00 00**

Other TPC Cards (without MPCOS Applet - FIPS)

These cards appear as GXPPro-R3.x FIPS and GXPPro R3.x FIPS PTS

[GXPPro-R3.x FIPS] 3B 6B 00 00 80 65 B0 83 **00 00 00** 83 00 90 00

[GXPPro-R3.x FIPS PTS] 3B 7B **00** 00 00 80 65 B0 83 **00 00 00** 83 00 90 00

IAS TPC Cards

[IAS ECC Type 1] 3B **00 00 00 00** 00 31 B8 64 **00 00 00 00** 73 **00 00 00** 82 90 00

[IAS ECC Type 1, T=1]
3B **00 00 00 00** 81 31 80 43 00 31 B8 64 **00 00 00 00** 73 **00 00 00** 82 90 00

[IAS ECC Type 1 Contactless Prox-DU]
3B **00 00 00** 00 31 B8 64 **00 00 00 00** 73 **00 00 00** 82 90 00 A3

Optelio Cards (D38-D72 R6)

[T=0 Normal Speed] 3B 6D 00 00 80 31 80 65 B0 84 01 00 C8 83 00 90 00

[T=0 High Speed] 3B 7D 96 00 00 80 31 80 65 B0 84 01 00 C8 83 00 90 00

[T=1 Normal Speed] 3B ED 00 00 80 31 80 65 B0 84 01 00 C8 83 00 90 00

[T=1 High Speed] 3B FD 96 00 00 81 31 48 42 80 31 80 65 B0 84 01 00 C8 83 00 90 00

Optelio Cards (D72 R4 WR)

3B 6E 00 00 80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00

Other Optelio Card (Santander)

3B 6F 00 00 80 66 B0 07 01 01 77 **00 00 00 00 00 00** 90 00

3B 68 00 00 80 66 B0 07 01 01 77 07

Other Optelio Card (Santander MPCOS)

[Optelio Card Santander MPCOS] 3B 69 00 00 80 65 A2 **00 00 00 00** 72 D6

MultiApp Cards (Easy 72K Type B and Combi 72K Type B)

[MultiApp Easy 72K Type B] 3B 8E 80 01 80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00 1D

[MultiApp Combi 72 K Type B T=0] 3B 6E 00 00 80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00

[MultiApp Combi 72 K Type B T=1] 3B EE 00 00 81 31 80 42 80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00 8E

MultiApp ID IAS ECC 72K CC (with IAS XL / IAS ECC Applet)

[IAS ECC Type 1] 3B **00 00 00 00** 00 31 B8 64 **00 00 00 00** 73 **00 00 00** 82 90 00

[IAS ECC Type 2] 3B **00 00 00 00** 00 31 B8 64 **00 00 00 00** 73 **00 00 00** 82 90 00 **00**

[IAS ECC Type 3] 3B **00 00 00 00 00 00 00** 00 31 B8 64 00 00 00 00 73 **00 00 00** 82 90 00

[IAS ECC Type 4] 3B **00 00 00 00 00 00 00** 00 31 B8 64 00 00 00 00 73 **00 00 00** 82 90 00 **00**

MultiApp ID Dual Citizen EAC 80K CC / Classic TPC DM (with IAS Applet V3) - Contactless Mode

[MultiApp ID Dual Citizen EAC 80K CC Contactless]
3B 8F 80 01 80 91 E1 31 80 65 B0 85 02 00 CF 83 00 90 00 C1

MultiApp ID Dual Citizen EAC 144K CC (with IAS Applet V3) -Contactless Mode

[MultiApp ID Dual Citizen EAC 144K CC Contactless]
3B 8F 80 01 80 91 E1 31 80 65 B0 85 02 00 E9 83 00 90 00 E7

MultiApp ID Dual Citizen EAC 80K CC / Classic TPC DM (with MPCOS Applet installed by default) - Contactless Mode with Prox DU

[MultiApp ID Dual Citizen EAC 80K CC MPCOS Contactless Mode with Prox DU]
3B 8A 80 01 80 65 A2 01 01 01 3D 72 D6 43 97

MultiApp V2.1 (with IAS XL / IAS ECC and IAS Classic Applet V3)

[MultiApp V2.1 Type 1]
3B 7F **00** 00 00 80 31 80 65 B0 00 00 00 00 **12 0F FF** 82 90 00

[MultiApp V2.1 Type 2]
3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 00 00 00 00 **12 0F FF** 82 90 00 **00**

TOP DL V2 Cards

[TOP DL V2 on Prox DU] 3B 8F 80 01 80 91 E1 31 80 65 B0 83 11 11 E5 83 00 90 00 EF

TOP DM GX4 Cards

There is one ATR when using the contact interface. When using the contactless interface, the ATR varies according to the type of card reader used:

[TOP DM GX4 - contact interface] 3B 8F 80 01 80 91 E1 31 80 65 B0 83 11 00 AC 83 00 90 00 B7

[TOP DM GX4 on SmartLogon Pro] 3B 0F 80 91 E1 31 80 65 B0 83 11 11 AC 83 00 90 00

[TOP DM GX4 on Omnikey] 3B 8F 80 01 80 91 E1 31 80 65 B0 83 11 11 AC 83 00 90 00 A6

[TOP DM GX4 on Gemalto Prox] 3B 8D 80 01 80 91 E1 31 80 65 B0 83 11 11 AC 83 00 34

JCOP41 Cards (not supported, but recognized by Classic Client)

The ATR varies according to the type of card reader used

[T=0] 3B 6A 00 FF 4A 43 4F 50 34 31 56 32 32 31

[T=1] 3B F9 18 00 00 81 31 FE 45 4A 43 4F 50 34 31 56 32 32 AF [T=1 on OMNIKEY 1109] 3B 8A 01 43 4F 50 34 31 56 32 32 31 FF 4A

[T=0 RFID on OMNIKEY CardMan 5x21-CL] 3B 8A 80 01 4A 43 4F 50 34 31 56 32 32 31 7F

[T=1 RFID on OMNIKEY CardMan 5x21-CL] 3B 89 80 01 4A 43 4F 50 34 31 56 32 32 4D

Other Cards

The following cards are also recognized by Classic Client

[HPC card] 3B 2B 00 00 64 0E 3E 02 F0 31 80 0E 90 00

[HPC card 2] 3B 3B 94 00 00 64 0E 3E 02 F0 31 80 0E 90 00

[HIC card] 3B 3B 94 00 00 64 0E 3E 03 0F 31 80 0E 90 00

[Venez_Prox] 3B 80 80 01 01

[Venez_Omnikey] 3B 88 80 01 31 F3 5E 11 00 81 95 00 90

[GXP7 T=0] 3B 6D 00 00 80 31 80 65 B0 87 27 01 BC 83 08 90 00

[GXP7 T=1] 3B ED 00 00 81 31 80 42 80 31 80 65 B0 87 27 01 BC 83 08 90 00

What's History?

This section describes the corrected problems and enhancements in each previous version.

Improvements in Classic Client 6.2 - Patch 1 - 001 (since Classic Client 6.2 - 005)

New ATRs

The following ATRs have been added:

- Other Optelio Card (Santander MPCOS) see page 5.
- MultiApp ID Dual Citizen EAC 80K CC / Classic TPC DM (with MPCOS Applet installed by default) - Contactless Mode with Prox DU see page 6.

Corrected Problems

The following problems have been corrected in this version:

- An improvement has been made so that when Classic Client is used remotely (Terminal Services or VMWare VDI for example), services.exe no longer uses 100% of CPU (ref 141184).
- Classic Client's shared memory service has been made more robust in order to prevent it crashing when other applications using Classic Client's PKCS#11 have stopped abnormally (ref 139797).
- An enhancement has been made in order to improve the recognition of X.509 v3 root certificates (ref 141093).
- A bug has been fixed where no message was appearing after a remote unblock PIN operation (regardless of whether the operation was successful or not). The message now appears (141285).

Supported Applications

In this version, support for some old versions was removed and support for some new versions was added. The changes were as follows:

Browsers

- Mozilla Firefox - support removed for 7.0; added for 12.0.
- Google Chrome - support removed for 15; added for 19.

Mail

- Mozilla Thunderbird - support removed for 7.0; added for 12.0.

Improvements in Classic Client 6.2 - 005 (since Classic Client 6.1 Patch 4 - 001)

New Features

- Classic Client now checks IAS XL / IAS ECC cards to see if the User PIN has been changed since first use. If it has not, Classic Client forces the user to change the PIN. Note that this feature is only implemented for those IAS XL /IAS ECC cards that have a particular profile. If you require more information about this profile, please contact your Gemalto technical consultant.
- Match on Card client AID is now configurable via the registry key "HKEY_LOCAL_MACHINE\SOFTWARE\Gemplus\Cryptography\Biometry\MOCAID\Client.
- Supports virtual slots for BioPIN.
- Fixes some problems from the previous version.
- Removes legacy tokens from the User Setup plugin.
- Adds the Biometric feature option in User Setup plugin.
- Supports MultiApp v2.1 cards.

Supported Fingerprint Readers and Scanners

In this release support for the following fingerprint scanner has been added.

- Covadis Auriga scanner

Enhancements

In Classic Client 6.1 – 005 a feature was added whereby the registration tool calls the Microsoft Base CSP if Classic Client's CSP does not recognize the card. The base CSP then chooses the correct minidriver for the card according to its ATR. This feature is mandatory for people who have .Net solution for example. However if a card uses its own CSP, it will not be recognized by Classic Client's CSP and will not be recognized by Microsoft Base CSP, so the Registration Tool is calling the Microsoft Base CSP for nothing. To avoid this, an enhancement has been made whereby the registration tool only calls the base CSP if the card has an associated minidriver.

Corrected Problems

- This release corrects a problem where removing a reader was causing the Regtool to take up to 90% of CPU.
- In certain cases, Classic Client had problems detecting card events (multiple removals and insertions). This release corrects these problems.

- Under certain rare conditions, not all of the card data were read. This is corrected by improving the parsing of the PKCS#15 data structure.
- In the Toolbox splash screen, the “Show this window at startup” check box was unresponsive. This release corrects this problem.
- The reboot message at the end of the installation process in the French version of Classic Client is now displayed correctly.
- It is now possible to go into Hibernate mode in Windows when using Classic Client.
- Fast User Switching feature is now supported.
- Some localization issues are fixed.

Supported Applications

In this version, support for some old versions was removed and support for some new versions was added. The changes were as follows:

Browsers

- Mozilla Firefox - support removed for 3.5, 3.6 and 4.0; added for 7.0.
- Google Chrome - support removed for 13; added for 15.

Mail

- Mozilla Thunderbird - support removed for 2.0, 3.0 and 3.1; added for 7.0.

Other Applications

- Microsoft Identity Lifecycle Manager (ILM) 2007 - support removed

Improvements in Classic Client 6.1 Patch 4 - 001 (since Patch 3–001)

Corrected Problems

- In certain cases, Classic Client has problems detecting card events (multiple removals and insertions). This patch corrects these problems.
- Under certain rare conditions, not all of the card’s data are read. This is corrected by improving the parsing of the PKCS#15 data structure.

Improvements in Classic Client 6.1 Patch 3 – 001 (since 6.1.0 – 005)

Patch 3 corrected certain problems. There are no changes regarding the support of applications, OS, cards, and so on.

New Feature

The setup has been modified such that if you are installing Classic Client and Firefox is already installed on the computer, you are given the option of registering Classic Client as a Gemalto Cryptographic Security Module at the same time as the installation (so that it is recognized by Firefox). You must reboot the computer to perform this registration.

Corrected Problems

- Enrollment with IAS ECC card (ref #111755)

  After enrolling a certificate on an IAS ECC card, there was a problem when refreshing the toolbox: The certificate or some of its keys appeared twice.
- Internet Explorer 9 - SSL client authentication (PIN window is to the center screen) (ref #111759)

When using IE9 to perform an SSL to a web site, the PIN prompt appeared in the top left of the screen instead of in the center of the IE window.

- IE8 IE9 - SSL authentication with Protected mode on (ref #111761)

  When Protected mode was enabled for IE 8 or 9 but the web site was not added in the trusted sites list, it was impossible to connect to this site using SSL with a card.

- IAS ECC card: PIN Request on card insertion with a Pinpad reader (ref #112109)

  If the card was removed during a signature scenario, each time the card was re-inserted the PIN was requested on the Pinpad.

- Limit the number of PIN presentations required to enroll a CC key pair on a transparent reader (ref #112400)

  On Classic v2/3 cards, when enrolling a CC certificate using Internet Explorer, you were prompted to enter the PIN 4 times instead of 3 when using CertEnroll (Vista/W7). Windows XP using XEnroll was OK.

- With a Pinpad, if ppc file is not signed, PIN min size is not set to 8 for change/unblock commands. Transparent readers OK. (ref #113077)

  If you manually change a PIN policy file so that the minimum PIN length goes from 6 to 5 characters, a message appears to say that the ppc file is not signed so the most secure PIN policy will be used (minimum PIN length of 8). This is correct behavior. This minimum length applies to change and unblock PIN functions. The problem that has been fixed is that you could change the PIN to a value of length 4 characters, whereas the minimum should be 8.

- Intermittent error when trying to sign with IAS ECC cards (ref #115866)

  For IAS ECC cards, there was an intermittent error when logging in twice consecutively during a P11 session. If you do not logout between the two logins, the second login failed with an invalid PIN message.

- Key pairs duplicated on the card in certain scenarios (ref #115869)

  The following were true for all the scenarios in question:

  OS: Windows 7 ultimate 64 bits

  Card: TopDL v2 (empty card)

  Reader: PCTwin

  The problem was that when you imported a certificate, removed the card and then reinserted it, the key pair appeared twice.

- It is now possible to import a pkcs#12 in a MultiApp ID IAS ECC 72K CC Type 1 card (with IAS ECC Applet) card (IAS ECC card with IAM profile) in the Personal Data tool of the ECC Management module of the toolbox (ref #115875).

- Problem with Classic TPC MPCOS cards when running “Certutil -scinfo” under Windows 7 (ref #115965)

  The command did not end successfully

Improvements in Classic Client 6.1 – 005 (since 6.0.0 SP1 – 001)

OS supported

- Removed Windows 2000 Professional SP4 – 32-bit only

Applications Supported

- Added Google Chrome 9.0
- Added Firefox 3.6

- Removed Firefox 3.0
- Added Microsoft Outlook 2010
- Removed Microsoft Outlook Express
- Added Mozilla Thunderbird 3.0 and 3.1
- Added Microsoft Office 2010
- Added Citrix Metaframe Xenapp 6.0 on Microsoft Server 2008 R2 (with Fat and Thin Clients)
- Added the Gemalto application eSigner 4.1.9 for Windows.

Fingerprint Scanners Supported

- Added DERMALOG ZF1 single finger scanner
- Added UPEK TouchChip TCS1
- Added Futronic FS80: single finger scanner

Cards Supported

- Added MultiApp ID Dual Citizen EAC 80K CC (with IAS Classic Applet V3) / TPC DM (with Classic Applet V3)
- Added MultiApp ID Dual Citizen EAC 144K CC (with IAS Classic Applet V3)
- Added MultiApp ID Citizen BioPIN
- Added TOP DL V2 – dual (contact and contactless) card.
- Removed Classic MDE TPC IM (Classic MDE Applet)
- Removed TOP DM GX4 – MPH51 – dual (contact and contactless) card with Classic MDE Applet

New Features

- Fingerprint authentication supported. The smart card must have the MoC (Match on Card) algorithm loaded inside it.
- Global bioPIN supported (global PIN that can be PIN or fingerprints).
- Registration Tool calls Microsoft Base if Classic Client's CSP does not recognize the card.

Pre-Requisite

- .NET Framework version 2.0 or later must be installed

Corrections

- PIN Try Counter displays when entering an incorrect PIN during a Change PIN operation with the registration tool.
- When entering a PIN in the Enter PIN window, the masking characters appear correctly. This was not previously the case when the window was called from a Java applet.
- For cards that support virtual slots, it is now possible to choose a slot when enrolling a certificate (all the available slots are visible).

Improvements in Classic Client 6.0.0 SP1 – 001 (since 6.0.0 – 002)

OS supported

- Added 64-bit versions of Windows

Applications supported

- Added Firefox 3.6
- Gemalto's eSigner 4.0.7 for Windows

Enhancements

- Improvements made in session management.
- Improvements made in performance for cards with the Classic Applets V1, V2 and V3.
- The signature mechanism for the configuration file and PIN Policy file has been modified to allow Core PC deployment. Core PC deployment means that you can install Classic Client on a reference machine and take an image of the environment. You can then deploy this image to any computer with the same environment – thus avoiding the need to install Classic Client on each individual machine.
- The following modification concerns only cards containing the Classic Applet V2 or Classic Applet V3. The mechanism for asking the user to enter his or her PIN has been modified so that it seems more logical to the end user.
- Gemalto has added some registry keys to define the timeout values for PIN Pad readers.

Corrections

- A correction was made that concerns cards containing the Classic Applet V1 only. After an incorrect IdenTrust PIN entry, the number of remaining PIN tries is now returned by Classic Client.
- The following bug was corrected: It is now possible to perform smart card login and smart card unlock computer operations in Windows Vista and Windows 7 with a PIN of more than 8 characters.
- A correction was made that concerns cards containing the Classic Applet V2 or Classic Applet V3 only. If you call a PKCS#11 function when no card is inserted in the reader, Classic Client now returns the correct error code.

Improvements in Classic Client 6.0.0 – 002 (since 5.3.0)

OS supported

- Added Windows 7
- Added Windows Server 2008 R2

Applications supported

- Added Windows BitLocker Drive Encryption (Windows 7 only)

Cards supported: added the following:

- IAS TPC (with IAS ECC applet)

New Features:

- The PIN pad reader now supports the minimum PIN length as defined in the PIN management policy

Improvements in Classic Client 5.3.0 (since 5.2.0 Patch 2)

Readers Supported

- Added Gemalto's GCR 5500

Cards Supported

Support for the following cards has been added:

- MultiApp ID IAS ECC 72K CC (with IAS ECC applet)
- MultiApp ID Citizen 72K CC (with IAS Classic Applet V3)
- MultiApp ID 72K (with IAS Classic Applet V2)
- MultiApp ID 144K (with IAS Classic Applet V2)
- MultiApp ID Combi 72K Type A (with IAS Classic Applet V2)

New Features: Note that they are available only for cards that contain the IAS ECC applet.

- A PKCS#15 plug-in has been added to the toolbox. This enables you to navigate through the PKCS#15 structure of the IAS ECC applet.
- An Identity Management plug-in has been added to the toolbox. This enables you to display and modify the identity data in the IAS ECC applet.
- The User Setup plug-in has been modified so that an Administrator can include the PKCS#15 and Identity Management plug-ins and the IAS ECC token in a User Setup.
- An IAS API has been added. This provides entry points to enable you to navigate through the PKCS#15 structure of the IAS ECC applet.

Improvements in Classic Client 5.2.0–004 Patch 2 (since 5.2.0 Patch 1)

OS Supported

- Added Windows Vista SP2 (32-bit and 64-bit)
- Added Windows Server 2008 SP1 and SP2 (32-bit and 64-bit)

Applications Supported

- Added Firefox 3.5

Corrected Problems

The following issues have been resolved in this release.

- Some localization problems have been solved in the Japanese version (Ref 495)
- When selecting a PKCS#12 file in the toolbox, all the certificates in that file are automatically selected. This makes importing PKCS#12 files easier.
- The CSP is now able to sign data that has been hashed using SHA-256 (Ref 477 and 489)
- A problem with the C_Unwrap Key function has been fixed – it no longer creates an extra "ghost" key

- An object management problem has been fixed – it is no longer necessary to read the card before creating an object
- Command data objects for key set management are only updated in the card when an operation is performed on a key set (set as default; create; destroy) or by a PIN management operation (change and unblock).

Note: This is the default behavior, but it can be modified by configuring the TransientRules registry key. Please refer to the Classic Client Integration Guide for more information on how to do this.

Improvements in Classic Client 5.2.0 Patch 1 (since 5.2.0 – 004)

Readers Supported

- Driver 4.0.7.5 for Gemalto's PC Pinpad readers included.

Corrected Problems

- A problem concerning the display of the PIN prompt when using PIN Pad readers has been corrected. With certain applications (eSigner in particular), this window was hidden, but this patch ensures it is displayed in front of all other open windows.
- GPK cards under Vista can now be used with a reasonable level of performance.
- For IdenTrust cards, sometimes PIN messages would relate to the wrong PIN (IdenTrust instead of User or vice-versa). This has now been corrected.
- **PIN Pad readers only**: After changing a PIN, you need to relog on to the card with the User PIN. Previously, if the User PIN was entered incorrectly, a message displayed to say that the PIN had not been changed, when in fact it had. This message has now been changed so that it says that the PIN has been successfully changed.

Improvements in Classic Client 5.2.0 – 004 (since 5.1.8 – 001)

OS Supported

- Windows Server 2008 (32-bit and 64-bit versions) supported

Applications Supported

Support for the following applications has been added:

Browsers

- Internet Explorer 8
- Mozilla Firefox 3.0

e-Mail

- Mozilla Thunderbird 2.0
- Microsoft Outlook 2003 SP1 and 2007

Other Applications

- Office 2007
- Adobe Acrobat 9
- Adobe Acrobat Reader 8 and 9
- Citrix Metaframe Xenapp 5.0 (on Microsoft Server 2008)

Cards Supported

Support for the following cards has been added:

- Optelio D38-D72 R6 with Classic applet v2
- Optelio Contactless D72 R2 with Classic applet v1
- MultiApp Easy 72K Type B (with Classic Applet V2)
- MultiApp Combi 72K Type B (with Classic Applet V2)
- TOP DM GX4 – MPH51 – dual (contact and contactless) card with Classic Applet V1.
- TOP DM GX4 – MPH51 – dual (contact and contactless) card with Classic MDE Applet

Corrected Problems

- CSN now displays correctly when remotely unblocking user PIN (Ref 114)
- Virtual Slots 2 and 3 now correctly refreshed in the Toolbox (Ref 127)
- Certificates now correctly registered for all virtual slots by Registration Tool, even for card insertions after the first.
- SSL now works when using Firefox with a PIN Pad and CC V2 card (Ref 334)
- After resuming from standby, the padlock icon in the toolbox displays correctly (sometimes the padlock was open, when in fact the card was not logged into the toolbox (Ref 337).
- For certain cards with an IdenTrust mapping, the IdenTrust PIN prompt displays correctly (previously the PIN field contained asterisks instead of being empty (Ref 339)
- The Toolbox: Certificates Plug_In / Card Movement test / Connection fails” problem has been solved (when moving multicards with multislots from one reader to another. (Ref 340)
- Importing pkcs#12 certificates no longer freezes Classic Client (Ref 378)
- C_InitToken no longer hangs (Ref 297) – This was only a problem for customers personalizing cards themselves
- Classic Client configuration file signature is now verified (Ref 382)
- Certificates in Israeli no longer cause Classic Client to freeze (Ref 288)
- Some Localization problems resolved (Ref 231)
- Secure Pin Entry is now supported with Dell Smartcard keyboards (Ref 293)
- PIN Pad dialog box no longer displays in background, so is not longer hidden. (Ref 276)
- Toolbox: Export function now OK for multi-readers and multi-cards (Ref 342)
- With Firefox, you can now import a certificate to the second virtual slot
- Unlock now possible after a wrong card insertion (for example if when trying to unblock a User PIN, the Administrator inserts the User’s card instead of the Administrator card). (Ref 218)
- Problems with UAC under Vista fixed. (Ref 278)
- C_GetMechanismInfo(slot0, CKM_RSA_X_509) returns the correct response message (i.e. Whether or not the mechanism is supported) (SL2 ref G-7KWECE) (Ref 379)

- C_findobject() issue when trying to access the same objects twice in a row now fixed (SL2 ref : G-7KQHYQ) (Ref 381)

Improvements in Classic Client 5.1.8 – 001 (since 5.1.7 – 001)

Enhancements

- Enhancement of service management at Windows startup
- Improvement of PKCS#11 slot management

Corrected Problems

- Bug fix in First PIN Change management

Improvements in Classic Client 5.1.7 – 001 (since 5.1.6 – 001)

Enhancements

- Localization update
- Specific description for PIN policy

Improvements in Classic Client 5.1.6 – 001 (since 5.1.5 – 003)

Enhancements

- Deactivated “selective suspend” function from readers configuration
- Improvement of multi-slot management

Corrected Problems

- Bug fix in reader selection in User Setup Plugin

Improvements in Classic Client 5.1.5 – 003 (since 5.1.5 – 002)

Enhancements

- Backward compatibility with GemSafe Libraries 4.2 keyset management
- Improvement of object handle management in token v1 and GPK

Improvements in Classic Client 5.1.5 – 002 (since 5.1.4 – 002)

Enhancements

- The same certificate can be imported several times in the same card.
- The option to export private key using Microsoft certificate management environment is systematically disabled.

Improvements in Classic Client 5.1.4 – 002 (since Classic Client RC Edition 5.1.0 – 003)

Enhancements

- Support of Virtual Slot through CSP
- Support of Citrix
- Support of PKCS#11 find object with some non-standard parameters.

Corrected Problems

- Correction of C_InitToken side effects

Improvements in Classic Client RC Edition 5.1.0 – 003 (since GemSafe Standard Edition 5.1.x)

OS Supported

- Support of Windows 64-bit operating systems

Cards Supported

- GPK support available in option with User Setup

Enhancements

- New branding
- Documentation update

Improvements in GemSafe Standard Edition 5.1.x (since GemSafe Standard Edition 5.0.x)

OS Supported

- Support of Windows Vista

Cards Supported

- Support of Classic MDE applet

Enhancements

- Enhanced robustness regarding semaphore management
- Enhanced robustness regarding abnormal termination of the calling application
- Possibility to import pkcs#12 certificates not protected by password
- Changed import mechanism to be compliant with any type of string encoding in certificates.
- When the type of a certificate is unknown, it is considered to be an exchange certificate
- Stability improvement during the enrollment phase
- Full Office compatibility for multi languages in container names
- Possibility to perform common criteria signature through CSP.

Corrected Problems

- Added “critical section” of code to avoid a lock on multiple signatures in a single thread
- Correction of display error on a Chinese certificate when imported with Certificate tool or CSP
- Correction regarding import from IE store
- Corrected display of Chinese characters for certificate name in Certificate Tool, and in Registration Tool
- Corrected issue of importing certificate with Chinese name in Certificate Tool

What's Up?

The following list covers limitations and minor issues known at the time of release:

Known Issues

There are certain issues independent of Classic Client that you need to know in order to use Classic client correctly, such as Microsoft hotfixes. These are described in "Tips" on page 21.

The following Classic Client-related issues were known at the time of writing this release note.

- User setup only: In cases where a User PIN Policy and an Admin PIN policy have been defined, Classic Client checks that the new PIN obeys the rules defined in the Admin PIN policy when unblocking a PIN. It should be the User PIN policy that is used. A workaround is to make sure that the Admin PIN policy and User PIN policy are identical (Ref #4585).
- For cards with the Classic Applet V3, it is not possible to sign documents in Microsoft Word 2003 and Excel 2003 spreadsheets because the "Digital Signature" window is blank. This is not an issue for the 2007 and 2010 versions of Word and Excel. (Ref: Issue #4505)
- When locking the computer please make sure that no PIN windows are open on the desktop otherwise it may not be possible to unlock the computer using the smart card/token
- It is mandatory not to overload any Java card (such as any Classic TPC card). Use Classic Client Toolbox to check for free key containers and free memory space before adding keys and certificates on the card.
- When the Toolbox calculates the amount of free memory in the smart card, it does not take read-only certificates into account.
- The Splash Screen "display timeout" feature used in user setups is ignored. (Ref 120).
- If you remove and reinsert your card too quickly, you may find that when you attempt to unlock your system that the following message appears "Your credentials could not be verified". In this case, remove the card and allow a short pause before reinserting the card. You should then be able to unlock your system as normal.
- Unicode characters of a specific language are correctly displayed only on an OS version of the same language (for example, Simplified Chinese characters are correctly displayed only on Simplified Chinese Windows).
- For some specific card personalizations, Classic Client 6.x behaves differently than GemSafe™ Libraries 4.x.
- Firefox does not systematically refresh the certificate display when removing/inserting cards. (Ref 344)
- As Firefox uses static management of PKCS#11 slots, moving cards between readers can lead to problems. If this occurs, it is recommended to close Firefox and re-open it. (Also Ref 344)
- It is recommended not to perform a reader hot-plug on a Citrix Client.
- Normally, performing a ScardDisconnect operation should free a "Mutex" called CTXMTXSmartCard, so that it can be accessed by other programming threads. However, this does not always work.

- In a Citrix environment, it is strongly recommended not to disconnect the Citrix session. Instead you should log off. If disconnected, a Citrix session must be re-opened on the same PC to recover its specific smart card environment.
- CITRIX: 2 sessions opened from same terminal not supported - Smart Card Logon (Ref 354)
- CITRIX: 2 sessions opened from same terminal not supported - Normal Logon (Ref 355)
- If you perform a smart card logon with the Classic Applet V1, and then perform a smart card logon with the Classic Applet V2, the second log on will fail. This is also true for Classic Applet V2 followed by Classic Applet V1. (Ref 253)
- Under Vista, using the Toolbox, it is impossible to export a certificate to the IE store.
- Gemalto recommends that you close Internet Explorer after each certificate enrollment on Citrix.
- If Classic Client is used with several readers and several cards at the same time, it can become overloaded if you perform too many card movements, for example, swapping cards from one reader to another, or even withdrawing and reinserting cards in the same reader. When overloaded in this way, it is possible that Classic Client will confuse one card with another.
- Problem enrolling certificates with IE under Vista when using virtual slots (Ref 470)
- When signing a document in Adobe Acrobat Reader 9, Adobe prompts you to select SHA-256. However when using the CSP security module, the signature is performed using the SHA-1 algorithm. This means the signature cannot be successfully verified as the hash algorithm is wrong. (Ref 483)
- With IAS ECC cards only, the Card Properties plug-in does not display the amount of free memory for the private portion and public portion of the key. It also does not provide the "Advanced" view of the card. (Ref 486)
- Citrix Metaframe Xenapp 5.0 is very slow when disconnecting: (Ref 490)
  - A Winlogon temporary session appears to freeze (but in fact it just takes more than one minute to disconnect).
  - When two sessions are open simultaneously, changing from one session to the other can take over one minute.
  - When two sessions are open simultaneously, changing from one session to the other can cause a "network error" or a "Wshell error".
- When more than one session is open in Citrix Metaframe Presentation Server 4.5, the mutex of the sessions mix together. This can cause deadlock and block at least one of the sessions. (Ref 491)
- There can be installation problems when installing Classic Client on a PC that already has Classic Client installed - it depends on the version and specifics of the version that is already installed. Gemalto recommends therefore that you uninstall the old version of Classic Client before installing the new one. (Ref 492).
- If you try to update a certificate through the Personal Data plug-in, the update fails. (Ref 493).
- For the Administrator version or a user setup which includes the IAS ECC applet and an (IAS) Classic Applet (V1, V2 or V3): It is possible after opening a new session that the first SSL authentication may not work. (Ref 537)

  Solution for User Setups: Make sure that the setup includes only the tokens that are needed and in the case of IAS ECC tokens, that the setup includes the IAS ECC token only.

General Solution: After opening the session, perform another operation (such as opening the Toolbox, or signing an email) before attempting the SSL authentication.

Localization Issues

- There are still some localization issues for non-English versions of the product.
- In Windows Server 2008 64-bit version there is a sentence in the PIN administration tool that appears in English (Ref 282)
- In Windows Server 2008 64-bit version there is a sentence in the PIN dialog box that appears in English (Ref 283)

Product Limitations

- Mozilla Firefox will request a couple of times for PIN, after doing repeated entry of wrong PIN, even after the PIN has been locked. This is a limitation on the Mozilla Firefox and not of the middleware itself. (Ref #5711).
- **IMPORTANT: If a computer is using Citrix Client (ICA) or Terminal Services, Classic Client must not be installed on both the Client and the Server**.
- It is not possible to use the Covadis Auriga Reader-Scanner with the Gem PC Twin reader due to hardware limitations. Auriga uses the same PCSC channel to perform both fingerprint scanning and smartcard transactions.
- For card having two virtual slots, only the first slot will be identified and use at smartcard logon. This is because the current minidriver specification has no way to identify and select between the two virtual slots.
- It is impossible to import a "sign only" certificate through Firefox. This is a limitation of Firefox, NOT Classic Client.
- Firefox imports "sign-only" certificates into a "sign and exchange" key container. This is an issue for CC certified applications, as the certificate must be imported into a "sign-only" key pair.
- Under Vista, only the first slot can be used to perform a smart card logon.
- Impossible to import p7 and .cert certificates files in the card if the card does not contain the corresponding RSA key pair (Ref 122)
- To use EFS (encrypted file system) on Windows Vista, you must use a non self-signed certificate and perform the EFS operation with no card inserted in the reader. Wait until EFS prompts you before inserting the card.
- When you install Classic Client to the Administrator setup, the driver 4.0.7.5 for Gemalto's PC Pinpad readers is copied to the PC but it is not installed. You must install the driver manually.
- It is not possible to perform SHA-256 operations using Microsoft applications (CertEnroll, Outlook etc). This is due to the fact that Microsoft applications require the use of a KSP (key storage provider) to use certain cryptographic algorithms such as SHA-256.
- The operations Verify PIN, Change PIN and Unblock PIN cannot be performed in the secure desktop of Windows Vista and Windows 7 for cards that impose secure messaging for these operations.
- When registering Classic Client as a Cryptographic Security Module (CSM) in Firefox, it is only registered for the current user account. If another user logs on to the computer, Classic Client will need to be registered manually. This can be done either as described in the Classic Client User Guide or by using the registration

utility (Start > All programs > Gemalto > Classic Client > Cryptographic Security Module registration).

- If you uninstall Classic Client, it is not automatically unregistered as a CSM in Firefox. This is not necessarily important, but if you really want to unregister Classic Client in Firefox, do so manually before uninstalling Classic Client (Start > All programs > Gemalto > Classic Client > Cryptographic Security Module unregistration).
- With Windows 7, when using Microsoft Office 2010 with the latest update taken from Windows Update, it is not possible to sign a mail in Microsoft Outlook using a CC certificate in a card with the IAS XL / IAS ECC applet.

Tips

- It is strongly recommended to install the latest Citrix SP on the server, in order to benefit from the Citrix PC/SC enhancements.

Where's the Doc?

This section describes the documentation that is provided with Classic Client 6.2 and where to find it:

Document	Location	Description
Classic Client 6.2 Administration Guide (Windows) Document Reference: D1252185B	■ Classic Client 6.2 CD ■ Classic Client 6.2 installation folder ■ Documentation plug in the Classic Client 6.2 Toolbox GUI	Describes installation and how to create installation and user profiles for users
Classic Client 6.2 User Guide (Windows) Document Reference: D1252186B	■ Classic Client 6.2 CD ■ Classic Client 6.2 installation folder ■ Documentation plug in the Classic Client 6.2 Toolbox GUI	Describes installation and how to perform end-user tasks.
Classic Client 6.2 Release Notes (this document) Document Reference: D1265346A	■ Classic Client 6.2 CD ■ Classic Client 6.2 installation folder ■ Documentation plug in the Classic Client 6.2 Toolbox GUI	Describes the new features and cards/ readers/applications supported, added since the previous release as well as known limitations.
EULA	■ Documentation plug in the Classic Client Toolbox GUI ■ Appears during installation when asked to accept terms and conditions	Describes the End User License Agreement - the terms and condition of use for Classic Client 6.2