

Release Notes

Date: June 22, 2022

Document Reference: D1578192A

This document presents information about Classic Client 7.5 for Uruguay.

What's New?

Smart Cards Supported

- MultiApp V5.x cards.

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, 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, 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 Thales for use with Classic Client. 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

(None)

Supported Operating Systems and Applications

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 7.5 for Luxembourg with applications not in this list, contact your Thales technical consultant.

Table 1 - Supported OS and Applications

Windows OS Version	Added/ Removed
Windows 10 – 32-bit and 64-bit	
Windows 11	
Windows Server 2016	
Windows Server 2019	
Browsers	
Microsoft Edge 102.0	
Mozilla Firefox 101.0.1	
Google Chrome 102.0	
E-mail Applications	
Mozilla Thunderbird 91.0	
Microsoft Outlook 2007, 2010, 2013 and 2016	
Other Applications	
Adobe Acrobat Reader DC 2022	
Intercede MyID v8 SP1 for certificate issuance and management (revocation, renewal etc.)	
Microsoft Office 2003 (up to SP1), 2007, 2010, 2013 and 2016	
Microsoft SharePoint 2010 and 2013 web server	
Microsoft Windows 2003 CA, 2008 CA and 2012 R2 CA for certificate enrolment and renewal	

Note:

- Windows XP, Windows Vista, Windows 7 and Windows 8.1 can be used without Thales support.
- Support for older versions of applications is removed as these versions were not tested; however, they are still compatible.

Supported Readers

This section provides a list of the readers supported by Classic Client 7.5 for Uruguay, as well as the drivers needed for each reader and the operating systems that are compatible.

Table 2 - Supported Readers

Reader Name	Reader Type	Driver	OS version
ID Bridge CT30	Contact	CCID 4.1.4.0	32 & 64 bits
ID Bridge CL300	Contactless	CCID 4.1.4.0	32 & 64 bits
ID Bridge CL3000	Contactless	CCID 4.1.4.0	32 & 64 bits
ID Bridge CT 700	PIN pad	CCID 4.1.4.0	32 & 64 bits
ID Bridge CT 710	PIN pad	CCID 4.1.4.0	32 & 64 bits

Supported Smart Cards

This section lists the cards supported by Classic Client 7.5 for Uruguay and their Answer To Resets. These values are all in hexadecimal.

- MultiApp V2.1 (with 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
- MultiApp V3.x (with IAS Classic Applet V4)
 - [MultiApp V3.x Type 1]

3B 7F 00 00 00 80 31 80 65 B0 00 03 00 00 12 0F FF 82 90 00
 - [MultiApp V3.x Type 2]

3B FF 00 00 00 81 31 00 43 80 31 80 65 B0 00 03 00 00 12 0F FF 82 90 00 00
 - [MultiApp V3.x Type A]

3B 88 00 01 80 31 80 65 B0 00 03 00 00 12 0F FF 82 90 00
 - [MultiApp V3.x Type B]

3B 88 00 01 E1 F3 5E 11 00 87 95 00 00
- MultiApp V4.x (with IAS Classic Applet V4.4.x/V5.x)
 - [MultiApp V4.x Type 1]

3B 7F 00 00 00 80 31 80 65 B0 00 04 00 00 12 0F FF 82 90 00
 - [MultiApp V4.x Type 2]

3B FF 00 00 00 81 31 00 43 80 31 80 65 B0 00 04 00 00 12 0F FF 82 90 00 00
 - [MultiApp V4.x Type A]

3B 8F 80 01 80 31 80 65 B0 00 04 00 00 12 0F FF 82 90 00 00
 - [MultiApp V4.x Type B]
- MultiApp V5.x (with IAS Classic Applet V5.x)
 - [MultiApp V5.x Type 1]

3B 7F 00 00 00 80 31 80 65 B0 00 05 00 00 12 0F FF 82 90 00

- [MultiApp V5.x Type 2]
3B FF 00 00 00 81 31 00 43 80 31 80 65 B0 00 05 00 00 12 0F FF 82 90 00 00
- [MultiApp V5.x Type A]
3B 8F 80 01 80 31 80 65 B0 00 05 00 00 12 0F FF 82 90 00 00
- [MultiApp V5.x Type B]
3B 88 80 01 E1 F3 5E 11 77 A1 97 00 15

What's History?

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

Improvements in Classic Client 7.4

Smart Cards Supported

- MultiApp V4.2 cards
- IDMotion V2 cards

Enhancements

- Cogent fingerprint extractor is now statically linked to the extractor API.
- Improvements in the fingerprint extractor:
 - Added support of 82 Minutiae count.
 - Support of ANSI format template.
 - New pruning algorithm.
- Supports Green Bit DactylID20 fingerprint scanner.
- Improved logging performance by asynchronously writing to the log files.
- Includes Microsoft Visual C++ 2017 Redistributable Package (Version 14.1025017) in Classic Client User Setup installer.

Improvements in Classic Client 7.3

New Features

- Supports MultiApp V4.1 cards.
- Supports IAS transport PIN mechanism.
- Supports two different PIN usages: one for signature and one for authentication.
- Supports notification of certificate prior expiration on both RegTool and Toolbox.
- Supports latest version of PKCS#11 - Cryptographic Token Interface Standard V2.4.
- Supports latest version of ISO/IEC 7816-15 V2016 standard.
- Aligns with EU Global Data Protection Regulation (GDPR) expectations for collecting logs.

Enhancements

- Improved performance in Citrix environment by reducing the number of background calls.
- When using global PIN, PIN is entered once after successful PIN verification through PACE.
- Initial PIN label is added when PIN is uninitialized.
- Support is added for not enforcing mutual authentication on the contactless interface.
- Mutual Authentication is performed if the card profile requires it.
- Administration PIN update is not allowed.

Corrected Problems

- Fixed issue on the support of contactless profiles.
- Fixed registry entry for MultiApp V2.1 card.
- Fixed issues on CSD support for IAS V2/V3 and IAS Essential.
- Support for ISO 18013-3 standardized status word in addition to JCRE '69 99'.

Improvements in Classic Client 7.2

Enhancements

- Support for IAS Classic V3 applet based on MultiApp Essential 1.0.
- Support for IAS Classic V4.4 applet based on MultiApp 4.x:
 - PIN policy on applet.
 - Secure PIN entry using Soft PINPad on screen.
- Full support of Microsoft Edge on Windows 10 platform for SSL authentication.

What's Up?

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

Known Issues

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

- For cards with IAS Applet V3, it is not possible to do Secure Socket Layer (SSL) authentication with Google Chrome internet browser with SHA-512. This is because Chrome is using a more secure hash algorithm that is supported by IAS applet V3.
- There is an intermittent issue in Mozilla Thunderbird. In rare cases, certificates are loaded and listed on the "Others" (instead of "Your Certificates") tabbed page in the Certificate Manager. This prevents users from associating the certificate with the email address. Users are advised to remove and re-insert the card to retry.
- Firefox does not systematically refresh the certificate display when removing/inserting cards.
- 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.
- User setup only: In cases where a User PIN Policy and an Administrator PIN policy have been defined, Classic Client checks that the new PIN obeys the rules defined in the Administrator PIN policy when unblocking a PIN. It should be the User PIN policy that is used. A workaround is to make sure that the Administrator PIN policy and User PIN policy are identical.
- For cards with the IAS 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.
- When locking the computer, 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.

- When the Toolbox calculates the amount of free memory in the smart card, it does not take read-only certificates into account.
- 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.
- A specific language is correctly displayed only on an OS version of the same language (for example, Simplified Chinese characters are correctly displayed only on Simplified Chinese Windows), or on an OS with the system locale set to the same language.
- 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.

- 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.
- 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. Thales recommends therefore that you uninstall the old version of Classic Client before installing the new one.

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.
- 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.
- Impossible to import p7 and .cer certificates files in the card if the card does not contain the corresponding RSA key pair.
- When you install Classic Client to the Administrator setup, the driver 4.0.7.5 for IDBridge CT700 (formerly called PC PIN pad) readers is copied to the PC but it is not installed. You must install the driver manually.
- In TokenIASV3, it is not possible to perform SHA-256 operations using Microsoft applications (CertEnroll, Outlook, and so on). 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.
- When using Adobe Reader, users can perform login and logout in the Security Settings window. After performing a login, if users remove and re-insert the card, they can still see that the card status is "logging in". At this point, if users press the Logout button, logging out fails. This is an Adobe Reader issue due to its mechanism on getting card status. Status update of the card only occurs when the Security Settings windows is open. If the Security Settings windows is closed, Adobe Reader is unable to know the status of the card.
- Improper name of the certificate is displayed after importing the certificate using Firefox. When users import the certificate file that does not have a friendly name, Mozilla Firefox generates a new random string as the name of the certificate. As a result, a not-so-friendly certificate name is displayed in the Classic Client Toolbox.
- Google Chrome does not support Certificate Enrollment, so users are unable to perform certificate enrollment using Google Chrome.
- If TLS authentication is set to use Minidriver instead of CSP, then immediately following the enrollment, a card must be removed and re-inserted so that the change take effect correctly.
- Consecutive Signature is only supported with PKCS#11 application.
- When changing password with Cryptographic Security Module (CSM) in Mozilla Firefox, a warning is displayed after PIN change is successful regardless of the different PIN pad readers used.

Where's the Doc?

This section describes the documentation that is provided with Classic Client 7.5 for Uruguay and where to find it:

Document	Location	Description
Classic Client 7.5 User Guide (Windows)	■ Classic Client 7.5 for Uruguay installation folder . ■ Documentation plug in the Classic Client 7.5 for Uruguay Toolbox GUI .	Describes the installation and how to perform end-user tasks.
Classic Client 7.5 for Luxembourg Release Notes (this document)	■ Classic Client 7.5 for Uruguay installation folder. ■ Documentation plug in the Classic Client 7.5 for Uruguay Toolbox GUI.	Describes the new features and cards/readers/applications supported or added since the previous release, as well as the known limitations.
EULA	■ Documentation plug in the Classic Client 7.5 for Uruguay 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 7.5 for Uruguay.