

Date: April 10, 2017

Doc Ref: D1414454A

This document presents information about Classic Client 7.2 for Linux for Uruguay — b06.01.

It describes what has changed since Classic Client 7.0 for Linux.

What's New?

OS Supported

- OpenSUSE 13.2 (32-bit and 64-bit)
- OpenSUSE Leap 42.1 (64-bit)

Enhancements

- Fingerprint Authentication—New Biometric Secure Dialog box for fingerprint or User PIN authentication implemented in Classic Client. The User PIN authentication is available when all fingerprints are blocked.
- Support to not enforce mutual authentication on contactless interface. Mutual authentication is performed if the card mandates it.
- 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.
- The reader exclusion mechanism, which was implemented for the Registration Tool only, is now applicable widely in the middleware. This means that excluded smart card readers no longer appear where the Token (IAS V4 or V3) is applied to.

Corrected Problems

The following problems are corrected in this version:

- During PACE authentication, default focus is no longer on the Cancel button on the PACE password input window.
- Token now supports the removal and insertion of reader and card, without restarting of applications.

What's Gone?

For information about the old versions of applications that are no longer officially supported by Classic Client 7.2 for Linux, refer to “Supported Operating Systems, Applications and Readers” 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 7.2 for Linux. It also lists the minimum system requirements to run Classic Client correctly.

System Requirements

The workstation must have at least 25 MB of available hard disk space and meet the normal system requirements to run the version of Linux installed. 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 Linux.
- 1 GB of RAM for 32-bit versions of Linux.
- 2 GB of RAM for 64-bit versions of Linux.

Pre-requisites

For fingerprint authentication, the fingerprints must already be present in the card.

Supported Operating Systems, Applications and Readers

The following table shows which OS, applications and readers are supported for each package. The versions in brackets are those that were used in validation

Table 1 - Supported OS, Applications and Readers

Linux OS Version	V2/V3	V4
OpenSUSE Leap 42.1 – 64-bit	Yes	Yes
OpenSUSE 13.2 – 32-bit and 63-bit	Yes	Yes
Other Linux OS upon request	—	—
Browsers		
Mozilla Firefox 47.0	Yes	Yes
Google Chrome 52.0	Yes	Yes
E-Mail Applications		
Mozilla Thunderbird 45.2	Yes	Yes
Office Suites		
LibreOffice 5.2.0	Yes	Yes
OpenOffice 4.1.2	Yes	Yes
Smart Card Readers		
PC Card	Yes	Yes
ID Bridge CT510	Yes	Yes
ID Bridge K30	Yes	Yes
ID Bridge CT30	Yes	Yes
USB e-Seal Token V2	Yes	Yes
PC USB-SL and PC USB-TR	Yes	Yes
Proximity Readers		

Table 1 - Supported OS, Applications and Readers

IDBridge CL300	Yes	Yes
IDBridge CL3000	Yes	Yes
Secure PIN Pad Readers		
PC Pinpad (Gemalto)	Yes	Yes
Dell Keyboards	Yes	Yes
Fingerprint Scanners		
Futronic FS80: single finger scanner	Yes	Yes
Futronic FS80H: single finger scanner	Yes	Yes
Futronic FS82HC	Yes	Yes

Note:

- Support for older versions of applications that were removed does not mean that they do not work - just that they are no longer tested by Gemalto.
- Gemalto has tested the scanners with the Biometric Tools to ensure they work, but support for Classic Client does not normally include support for the readers themselves. It can be provided on request. Please ask your Gemalto vendor for more details.
- Biometric support requires an additional software license that is not covered by the standard Classic Client license. You can obtain this license at an extra cost from Gemalto. Please ask your Gemalto vendor for more details.

No Longer Supported

- Adobe Reader 9.x in all Linux platforms for document signature.
- Adobe Acrobat Reader with the PKCS#11 security module uses SHA256 to hash data before signing. The SHA256 signatures are not supported by the Classic Applet V1.

Supported Smart Cards

This section lists the cards supported by Classic Client 7.2 and their Answer To Resets (ATRs) and mask numbers. These values are all in hexadecimal.

- 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 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)
- MultiApp V2.1 (with IAS XL / IAS ECC applet and IAS Classic Applet V3)
- MultiApp V3.0 (with IAS Classic Applet V4)

- MultiApp V4.0 (with IAS Classic Applet V4.4)
- IDMotion V1 Type 1 (IAS Classic Applet V3)
- IDMotion V1 Type 2 (IAS Classic Applet V3)
- IDMotion V1 Type 3 (IAS Classic Applet V3 and eTravel)
- IDMotion V1 Type 4 (IAS Classic Applet V3 and eTravel)
- IDMotion V1 Type 5 (IAS Classic Applet V3 and eTravel)
- IDMotion V1 Type 6
- IDMotion V1 Type 7
- IDMotion V1 Type 8

Cards for use with Biometric Verification

The cards that support Biometric verification are MultiApp ID Citizen Bio cards. These cards support the global BioPIN feature. Their ATRs are the same as those in the first group of ATRs in the next section.

ATRs

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

IDMotion Cards (with IAS Classic Applet V3)

- [IDMotion V1 Type 1, T=0/1] 3B FF 00 00 FF C0 0A 31 FE 4D 80 31 E0 6B 00 31 05 02 00 55 55 55 55 55 00
- [IDMotion V1 Type 2, T=CL] 3B 8F 80 01 80 31 E0 6B 00 31 05 02 00 55 55 55 55 55 55 00

IDMotion Cards (with IAS Classic Applet V3 and eTravel, Default Mode)

- [IDMotion V1 Type 3, T=0/1] 3B F0 97 00 FF 81 31 FE 4D
- [IDMotion V1 Type 4, T=0/1] 3B FF 00 00 FF 00 00 31 FE 4D 80 31 80 65 00 02 30 00 00 12 0F FF 82 90 00 00
- [IDMotion V1 Type 5, T=CL] 00 00 00 00 80 91 E1 00 02 30 00 00 00 73 D4 41 40 00
- [IDMotion V1 Type 6] 3B FF 00 00 FF 91 81 31 FE 4D 80 31 E0 6B 00 31 05 02 00 55 55 55 55 55 00
- [IDMotion V1 Type 7] 3B F0 00 00 FF 91 81 31 FE 4D 0B
- [IDMotion V1 Type 8] 3B 88 80 01 00 00 00 00 77 83 95 00 00

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 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 Cards (with IAS Classic Applet V3)

- [Type 1] 3B 7F 00 00 00 80 31 80 65 B0 00 00 00 00 12 0F FF 82 90 00
- [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 V3.0 (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 8F 00 01 80 31 80 65 B0 00 03 00 00 12 0F FF 82 90 00 00
- [MultiApp V3.x Type B] 3B 88 00 01 E1 F3 5E 11 00 87 95 00

MultiApp V4.x (with IAS Classic Applet V4.4)

- [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

Supported Languages

The following languages are supported in Classic Client:

- Catalan
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Dutch
- English
- French
- German
- Greek
- Hungarian
- Italian
- Japanese
- Latvian
- Lithuanian
- Polish
- Portuguese
- Slovenian
- Spanish
- Swedish
- Turkish

- Arabic
- Russian
- Azerbaijani

What's History?

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

Improvements in Classic Client 7.0 for Linux

OS Supported

- Ubuntu 14.04
- Debian 7.6
- OpenSuse 13.1
- Fedora 20

Improvements in Classic Client 6.1 - 008 for Linux

Browsers

- Mozilla Firefox 3.5, 3.6, 7.0

E-Mail

- Mozilla Thunderbird 7.0

Other Applications

- Adobe Reader 9.5.5 (in Ubuntu 10.04 LTS 32-bit only)

New Features

- Smart cards with the Classic Applet V1 are now supported.

Corrected Problem

A problem corrected where Classic Client had a conflict if a card with Classic Applet V3 and another card with the IAS XL applet were connected at the same time.

Improvements in Classic Client 6.1- 007 for Linux

OS supported:

- Added Ubuntu 10.04 LTS – 32-bit and 64-bit
- Removed Redhat, Debian and OpenSuse

Browser applications supported

- Added Mozilla Firefox 3.5, 3.6, and 4.0
- Removed Mozilla Firefox 3.0

E-mail applications supported

- Added Mozilla Thunderbird 3.0 and 3.1

- Removed Mozilla Thunderbird 2.0

Other applications supported

- Added Adobe Reader 9.x (in Ubuntu 10.04 LTS 32-bit only)
- Removed Adobe Reader 8.1

Fingerprint scanners supported

- Added Futronic FS80: single finger scanner

Cards supported

Added the following:

- MultiApp ID IAS ECC 72K CC (with IAS XL 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)
- MultiApp ID Dual Citizen EAC 80K CC (contact and contactless) (with IAS Classic Applet V3) / TPC DM (contact and contactless) (with Classic Applet V3)
- MultiApp ID Dual Citizen EAC 144K CC (contact and contactless) (with IAS Classic Applet V3)
- MultiApp ID Citizen BioPIN
- TOP DL V2 – dual (contact and contactless) card.
- IAS TPC (with IAS XL applet)

Removed the following:

- Classic MDE TPC IM (Classic MDE Applet)
- TOP DM GX4 – MPH51 – dual (contact and contactless) card with Classic MDE Applet

New Features

- Classic Client now supports fingerprint authentication as an alternative to PIN authentication. The smart card must have the MoC (Match on Card) algorithm loaded inside it.
- Classic Client supports a global bioPIN, that is, a global PIN that can be PIN or fingerprints.

Improvements in Classic Client 5.2.0 for Linux

OS supported:

- Added Ubuntu 9.0.4

Enhancement:

- Added support of the new smart card MultiApp ID IAS ECC 72K CC (with IAS XL applet).

Improvements in Classic Client 5.1.8 - 003 for Linux

Enhancements

- Added support of Optelio card for Santander.

Improvements in Classic Client 5.1.8 - 002 for Linux

Enhancements

- Loading of PKCS#11 is enabled on Redhat rhel 5 even if SELinux is activated.
- Cards enrolled on Linux are fully usable on Windows operating systems.
- Added support of Classic Applet v1 and Optelio cards.

What's Up?

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

Known Issues

- Under some circumstances, when multiple applications are performing pulling on the PKCS#11 layer, closing one of these applications can disable the PKCS#11 access for the other applications. The user has to close the other applications, or remove and insert the card again to restore access to the PKCS#11 layer.
- Upon card insertion or removal, pcsc lite can miss the event. To go back to a normal state, insert or remove the card again.
- Using Firefox, if a user does not type the CSD when required, but clicks the "Cancel" button instead, Firefox can freeze. The user has to close Firefox and restart it to go back to a normal state.
- If a card is configured with PACE using NIST P-521 (secp521r1) ECC and with Integrated Mapping (IM), PACE authentication fails.
- Japanese characters may not display properly.
- The maximum length supported by the Pinpad reader is limited to "8" in Debian 7.x with the official release of libccid 1.4.7-1 (PC/SC driver for USB CCID smart card readers).
The same limitation is found in OpenSuse 13.x and Fedora 20 with the official release of libccid 1.4.12-2.1.1 and 1.4.13-1 respectively.
- Google Chrome browser does not support key generation on hardware. Hence, it does not support web certificate enrolment with smart card.

Where's the Doc?

This section describes the documentation that is provided with Classic Client 7.2 and where to find it:

Document	Location	Description
Classic Client 7.2 User Guide (Linux)	■ Classic Client installation folder (/usr/share/doc/libclassicclient)	Describes installation and how to perform certain tasks
Release Notes (this document)	■ Classic Client installation folder (/usr/share/doc/libclassicclient)	Describes the new features, cards, readers, and applications supported, added since the previous release as well as known limitations.
EULA	■ Classic Client installation folder (/usr/share/doc/libclassicclient)	Describes the End User License Agreement - the terms and condition of use for Classic Client 7.2 for Linux.