Middleware Universale

Per smart card Incard

Release Notes

Indice

Revisione	Autori	Note
A (18/102007)	Giuseppe Amato Vincenzo Palazzo	
B (26/10/2007)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.7.0 Aggiunte note per Mac OS X e Linux
C (29/11/2007)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.7.1
D (05/12/2007)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.8.0
E (21/01/2008)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.8.5

Revisione	Autori	Note
F (23/01/2008)	Giuseppe Amato	Aggiornate note per Mac OS X
G (04/06/2008)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.12.0
H (23/06/2008)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.14.0
I (10/07/2008)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.14.1
L (18/08/2008)	Giuseppe Amato	Version History: aggiunte note per la versione 1.1.16.0
M (15/10/2008)	Giuseppe Amato	Aggiornate note per Mac OS X
N (22/10/2008)	Giuseppe Amato	Version History: aggiunte note per la versione 1.2.0.0
O (14/04/2009)	Giuseppe Amato	Version History: aggiunte note per la versione 1.2.5.1
P (06/05/2009)	Giuseppe Amato	Version History: aggiunte note per la versione 1.2.6.0
Q (15/06/2009)	Giuseppe Amato	Version History: aggiunte note per la versione 1.2.7.1
R (11/6/2010)	Giuseppe Amato	Version History: aggiunte note per la versione 1.2.9.0

Version History

Novità della versione 1.2.9.0:

- La lunghezza del container name CSP è ora impostabile al valore massimo di 39 caratteri.
- Aggiunto sistema di licensing
- Ssupporto MacOS X 10.6 e Windows 7
- Bug Fix: il cambio del PUK DS poteva fallire

Novità della versione 1.2.7.1:

- Bug Fix: la funzione C_SignUpdate poteva essere molto lenta.

Novità della versione 1.2.6.0:

- I valori di default degli attributi PKCS#11 sono stati resti più significativi

Novità della versione 1.2.5.1:

- Implementazione delle funzioni C_SignUpdate() e C_SignFinal()

Novità della versione 1.2.0.0:

- BugFix: corretto errore nella generate key pair che si verificava nei casi in cui la carta fosse stata usata con librerie differenti dal Middleware Universale

Novità della versione 1.1.16.0:

- BugFix: risolto blocco della libreria quando usata da Internet Explorer.

Novità della versione 1.1.14.1:

- BugFix: errore “0x05” durante la lettura del modulo dalle chiavi pubbliche CNS appena generate.

Novità della versione 1.1.14.0:

- BugFix: errore “0x05” durante la lettura del modulo dalle chiavi pubbliche DS a 2048 bit appena generate.

Novità della versione 1.1.12.0:

- Aggiunto supporto per chiavi a 2048 bit nel Filesystem full P11 (carte T&S2048)
- Aggiunto supporto per chiavi a 2048 bit nel Filesystem DS-v2.0 (carte T&S2048)

Novità della versione 1.1.8.5:

- BugFix: aggiunto mechanism Generate Key Pair RSA.
- BugFix: aggiunte informazioni sulle dimensioni minime e massime delle chiavi nei mechanism RSA.
- “Modulo di gestione del PIN”: disabilitati il cambio PIN e lo sblocco PIN tramite PUK.
- Il PIN di firma forte ed il PIN CNS ora coincidono e non viene visualizzata la richiesta di PIN durante una firma forte.

Novità della versione 1.1.8.0:

- BugFix: nel caso in cui il container di default non sia stato preimpostato, viene usato il certificato che ha come CKA_ID il valore “SmartLogon”. Nel caso questo sia assente viene selezionato il primo certificato che possiede “SmartCardLogon” tra gli extended key usage.
- Il “Modulo di gestione del PIN” permette ora di impostare il certificato di default (quello usato ad esempio per le operazioni di logon).

Novità della versione 1.1.7.1:

- BugFix: lo sblocco del PIN tramite PUK non funzionava per le smart card “legacy”, gestite tramite modulo PKCS#11 esterno.

Novità della versione 1.1.7.0:

- Aggiunto supporto per le caratteristiche della carta Touch&Sign2048 nel filesystem FullP11:
  - è possibile creare/generare fino a 8 chiavi RSA 2048 bit
  - raddoppiato il numero massimo di oggetti creabili
  - raddoppiato il numero di chiavi private RSA a 1024 creabili/generabili
- Il filesystem FullP11 resta compatibile con le versioni precedenti, ad esclusione degli oggetti 2048 bit

Novità della versione 1.1.6.0:

- Aggiunte funzionalità di scrittura per i filesystem CNS, Firma Forte e FullP11.
- BugFix: non venivano letti alcuni attributi PKCS#11 degli oggetti memorizzati nel filesystem FullP11.
- BugFix: dopo la chiusura dell'ultima sessione adesso viene effettuato il logout dal token.

Novità della versione 1.1.5.0:

- Aggiunte funzionalità di scrittura per i le smartcard gestite tramite PKCS#11 esterni.
- Aggiunto supporto ai DATA OBJECT per il filesystem FullP11.
- Aggiunto supporto al DATA OBJECT dei dati personali per il filesystem CNS.

Note per versione Mac OS X

Requisiti di sistema:

- Mac OS X 10.4.x
- Mac OS X 10.5.x
- Mac OS X 10.6.x
- Un lettore di smart card supportato da **SmartCardServices di Apple**

Il Middleware Universale per Mac OS X è distribuito in due formati: **DyLib** e **BUNDLE**.
Alcuni software possono utilizzare entrambe i formati,altri software solo il formato BUNDLE, altri ancora solo il formato DyLib.
Il formato **DyLib** è costituito da 3 file:
libbit4ipki.dylib
libbit4ipki.dylib.conf
libbit4ipki.dylib_pin.py

I 3 file vanno copiati sempre insieme in una cartella di sistema, ad esempio:
/usr/local/lib
/usr/lib

Il formato **BUNDLE** è costituito da una cartella, libbit4ipki.bundle.
Il BUNDLE può essere installato copiandolo in una qualsiasi cartella accessibile da parte di tutti gli utenti.

Problemi noti:

La libreria può essere usata con Mozilla Firefox per la SSL client authentication.
Tuttavia un bug di Mozilla impedisce di specificare il percorso della libreria usando l'interfaccia grafica; infatti potrebbe capitare che dopo aver selezionato la libreria Firefox visualizzi un percorso del tipo:
AAAAAAFWAAIAAAxNYWNpbnRvc2ggSEQAAAAAAAAAAAAAAAAAAAC

Per evitare il problema è necessario inserire il percorso completo della libreria manualmente nell'apposito campo, ad esempio:
"/usr/local/lib/libbit4ipki.dylib" .

Note per versione Linux

Requisiti di sistema:

- PCSCLite 1.2.9 o successivo
- Lettore di smart card
- Una delle seguenti distribuzioni:
  - Debian 4.x o 5.0
  - Ubuntu 9.x, 10.x
  - Mepis

Il Middleware Universale per Linux è costituito da 3 file:

libbit4ipki.so
libbit4ipki.so.conf
libbit4ipki.so_pin.py

I 3 file vanno copiati sempre insieme in una cartella di sistema, ad esempio:
/usr/local/lib
/usr/lib

dopo aver copiato i file potrebbe essere necessario aggiornare la cache delle librerie col comando:
#> ldconfig