PROTECT

Gemalto Multiapp Platform V1.0

Product Description

The Gemalto Multiapp Platform V1.0 is an operating system implementing the Java Card standard (which in turn consists of several Java entities) and the GlobalPlatform Card Specification 2.2.1.

The operating system includes a cryptographic library and is contained on a separately evaluated integrated circuit embedded on a plastic card.

Users of the card can store Java applets of their own design and creation on the card; these applets interface with the Java Card standards and could conceivably implement e-identity and e-money type schemes.

The target of evaluation here is the cryptographic library which includes several DSD Approved Cryptographic Algorithms and a random number generation scheme.

Common Criteria Certification – scope

The scope of the Common Criteria (CC) certification included the following:

- Security audit
- Cryptographic support;
- User data protection;
- Security management;
- Protection of the TOE security function; and
- Trusted path/channel.

Unevaluated functionality are:

- Java card applications;
- Holograms and security printing;
- OATH which provides one time password (OTP) authentication services following the OATH standard;

- Gemsafev2 which provides electronic signature services;
- IAS Premium which provides electronic signature services;
- Cryptomanager which provides the biometric services (from Precise Biometrics);
- MPCOS, a card operating system; and
- Paypass MCHIP, a MasterCard application.

Common Criteria Certification – summary

The product was found to meet the requirements of the Common Criteria (CC) evaluation assurance level EAL2.

DSD Findings

Because the product employs cryptography, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria evaluation.

The random number generation and cryptographic primitives were found to be acceptable for use in reducing classification of data in transit from RESTRICTED to UNCLASSIFIED and HIGHLY PROTECTED to IN-CONFIDENCE/RESTRICTED.

It should be noted that the random number generation and cryptographic primitives employed by the product are NOT appropriate to protect information classified CONFIDENTIAL, SECRET or TOP SECRET.

Where possible, it is recommended that RSA (with key length greater than 1024 bits), Diffie-Hellman, and alternate Digitial Signing Algorithms be used in place of the elliptic curve based algorithms as confirmation was not able to be made that the curves used are appropriate. The reduction in performance caused by having to use these traditional algorithms with a similar bit-strength of security will generally be negligible. This recommendation is not a `MUST' compliance requirement as defined in the *Information Security Manual*.

Finally it is worth reinforcing that security will have to be considered throughout the development cycle of applets that are intended to be put on the card. Secure underlying primitives are no defense against private information being manipulated or stored poorly. Applets should take care to flush the OS wide RAM after it has finished performing calculations with secret quantities.

PROTECT

Contact

For further information regarding the certification, cryptographic evaluation or compliance with the *Information Security Manual* for Gemalto Multiapp Platform V1.0 please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

Information Security Manual 2009

The advice given in this document is in accordance with the *Information Security Manual* release date September 2009. Australian government agencies are reminded to periodically check the latest release date of the ISM at http://www.dsd.gov.au/library/infosec/ism.html.

Consumer Guide

This consumer guide was issued on 5th February 2010 by DSD.