

Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Card Management System Integration Made Easy:
Tools for Enrollment and Management of Certificates

September 2006

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.



Table of Contents

| | | |
|----------|--|-----------|
| 1 | CMS Integration Overview | 1 |
| 2 | Benefits to CMS with Entrust Integration | 2 |
| 3 | CMS Integration with Managed Solutions | 3 |
| 3.1 | CMS Integration Requirements for Managed Solutions | 3 |
| 3.2 | CMS Integration Changes for Managed Solutions | 3 |
| 3.3 | Architecture/Design | 3 |
| 4 | CMS Integration with Unmanaged Solution | 6 |
| 4.1 | CMS Integration Requirement for Unmanaged Solutions | 6 |
| 4.2 | CMS Integration Changes for Unmanaged Solutions | 6 |
| 4.3 | Architecture/Design | 7 |
| 5 | Authorizing Requests to Entrust Certification Authority | 9 |
| 6 | Planned Integration with CMS Products | 10 |
| 7 | Summary | 11 |
| 8 | About Entrust | 12 |

1 CMS Integration Overview

Many organizations are turning to **two-factor authentication** solutions to verify the identities of users on their networks. Simply put, two-factor authentication is based on something you know (for example, a PIN) and something you have (for example, a smart card). By requiring two independent elements for user authentication, this approach can help in decreasing the chances of unauthorized information access and fraud. A significant number of Entrust customers use **card management systems (CMS)** to enroll users with certificates that are stored on smart cards or tokens. (Note that throughout this document references to smart cards include both smart cards and other cryptographic tokens, such as USB tokens.)

Interest in smart card deployment has increased amongst North American organizations and their US subsidiaries around the world with the introduction of **Homeland Security Presidential Directive #12 (HSPD 12)**, which mandates the implementation of advanced identity credentials to standardize the form and level of security by which employees and contractors are identified in order to grant them access to federal facilities and information systems. In addition to assuring physical security at federally controlled facilities, the directive is aimed at securing electronic access to the federal government's information systems. It stipulates that identity must be verified by rapid, two-factor electronic authentication – specifically, the infrastructure used must support identification cards that contain both public key certificates and a PIN or password. Entrust products meet the HSPD 12 mandates and can help CMS vendors meet the process and supporting infrastructure requirements defined by the FIPS 201 Personal Identity Verification (PIV) Standard.

Using [Entrust Authority™ Toolkits](#), CMS products can enroll users for managed or unmanaged certificates thereby helping to address a broad range of government and commercial enrollment requirements. This document outlines tools developed within the Entrust Authority portfolio to facilitate easier smart card management system integration with Entrust products for both managed and unmanaged certificate solutions. To the extent that encryption key pairs are being deployed, Entrust would recommend integration using the managed identities as this approach helps to enable key recovery and prevent loss of data in the event that a key is lost or damaged. It also offers more flexibility for CMS vendors to leverage additional management features that Entrust plans to make available to CMS vendors.

2 Benefits to CMS with Entrust Integration

CMS vendors can take advantage of various benefits through integration with Entrust products. Specifically:

- Entrust has established relationships with many government departments and agencies and private sector businesses. Integration with Entrust's leading PKI product portfolio can help provide CMS vendors with opportunities for revenue growth that relate to enabling comprehensive, scalable security solutions designed to address certain needs such as compliance with corporate and government regulations for stronger authentication, encryption, and digital signatures.
- Entrust works closely with CMS vendors and customers to collect information and obtain a better understanding of the smart card requirements desired within the industry. This information is then used in selecting the features and functionality for Entrust products to enhance and complement card management solutions.
- Entrust PKI and complementary Entrust products can help in providing CMS compatibility with the Personal Identity Verification I and II (PIV I and II) system enabling the use of public key cryptography security by CMS customers for addressing HSPD-12 and Federal Information Processing Standard 201 FIPS 201 requirements.
- Integration with an Entrust PKI is designed to help provide a more cost effective option for the management of digital identity keys and certificates which is needed by many CMS customers to transparently automate security-related processes. With managed solutions, keys are automatically updated to avoid business interruption associated with expiry of keys and/or certificates. Decryption keys are backed up at the Security Manager to enable key recovery and prevent loss of data in the event that a key is lost or damaged or if an employee leaves the organization after encrypting data. Entrust also provides the flexibility to use unmanaged certificate solutions for scenarios such as when automatic key and certificate update is not required or desired.
- Entrust continues to enhance our developer tools and high-level APIs to enhance integration capabilities for both managed and unmanaged solutions.

3 CMS Integration with Managed Solutions

3.1 CMS Integration Requirements for Managed Solutions

Automated key and certificate management services are critical to many customer solutions as they enable security capabilities such as encryption and digital signature across applications in a way that is transparent and easy to use. Entrust delivers products that help CMS products to be deployed within public-key infrastructures, lower the total cost of ownership and meet organization-wide security requirements.

In general, CMS vendors and customers are looking for CMS integration APIs to achieve the following aspects of key and certificate lifecycle management:

- facilitated enrollment, key backup at the Certification Authority (CA), key recovery, automatic renewal and revocation via a card management system
- generation of keys on the CMS and transfer of keys where appropriate from software to hardware according to specific card management system standards

3.2 CMS Integration Changes for Managed Solutions

With the above goals in mind, the Security Toolkit for the Java Platform includes a card management system module designed to facilitate digital identity enrollment, key backup at the CA and associated key recovery to enable appropriate access to protected data, renewal and revocation via a CMS. Specifically, Security Toolkit for the Java Platform can:

- a) accept a decryption key generated externally via the CMS rather than requiring the key to be generated via Entrust software (All signing/verification key pairs will be generated by the CMS)
- b) provide PKCS #11 or CryptoAPI formatted information to enable the CMS to write digital identity information to the smart card, including the private keys that the CMS has created, in such a way that Entrust software can manage the keys and certificates on the smart card

3.3 Architecture/Design

The [Entrust Authority Security Toolkit for the Java Platform](#) can be used to accomplish user enrollment onto a smart card once the user has been set up and created using the Entrust Authority Security Manager software. This is done through the Security Toolkit for the Java Platform CredentialReader/CredentialWriter architecture. The Security Toolkit for the Java Platform triggers generation of the keys on the card via PKCS11 calls directly to the card, completes a Certificate Management Protocol (CMP) transaction with the Entrust Authority Security Manager software (activating the user), and writes the Entrust digital identity to the card via PKCS11 calls. The entire process is hidden from the application developer using the APIs provided in Entrust Authority Security Toolkit for the Java Platform.

In addition to these user enrollment capabilities, features have been added to the Entrust Authority Security Toolkit for the Java Platform to further facilitate CMS integration with Entrust products. With the new integration capabilities, decryption key pairs are either generated and/or backed up as necessary by the Entrust Authority Security Manager software and securely passed back to the CMS via the Security Toolkit for the Java Platform, or generated by the CMS and securely passed via the Security Toolkit for the Java Platform to the Security Manager software for backup. (The [documentation](#) for the Entrust Authority Security Toolkit for the Java Platform provides details on how to integrate a card management system with Entrust software.) The specific module that enables CMS creation of keys and certificates that can be managed via Entrust software is called **CMPForCardMS** and it can be located within the `com.entrust.toolkit.credentials` package. The main CardMS class that explains what the CardMS module is and how it is used is:

com.entrust.toolkit.credentials.CMPForCardMS

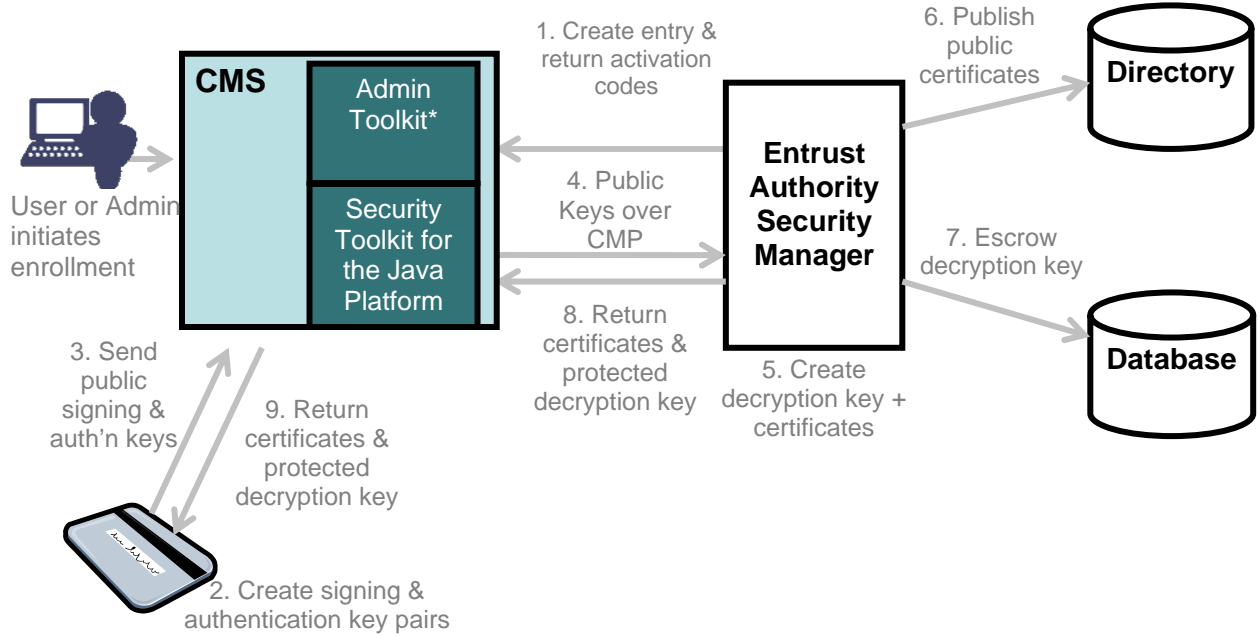
Card management system vendors may also be interested in the following classes available through the CardMS module:

com.entrust.toolkit.credentials.CardMSCertReqInfo
com.entrust.toolkit.credentials.P11StorageObject
com.entrust.toolkit.credentials.P11DataObject
com.entrust.toolkit.credentials.P11PrivateKeyObject
com.entrust.toolkit.credentials.P11X509CertificateObject

Please request a copy of the [documentation](#) for the Entrust Authority Security Toolkit for the Java Platform to learn more about the above mentioned classes and receive additional details on how to integrate a card management system with Entrust software.

Note that the diagram set out in Figure 1 below, digital identity lifecycle management is achieved using a combination of Entrust client-side software and the Certification Authority. See Section 6 titled “Planned Integration with CMS Products”, for further information regarding changes that may affect integration plans.

Figure 1: **Sample user enrollment request and response with decryption key backup**



*See Section 5 for details on administration interface options for Entrust Authority Security Manager.

4 CMS Integration with Unmanaged Solution

4.1 CMS Integration Requirements for Unmanaged Solutions

The CardMS module described above can be used to enroll users for credentials that can be managed as well as credentials that will not be managed. Entrust is seeing increased interest from customers and CMS partners in an API that addresses the following requirements for unmanaged solutions. An API that:

- enables an unmanaged certificate to be retrieved from an Entrust CA when the key is generated externally by a non-Entrust product
- supports variable per user and per card certificate extensions including biometric and subject directory attributes included as extensions to CMP requests per RFC3739 or Personal Identity Verification extensions as defined in FIPS 201
- supports flexible key pairs for users and/or devices including key pairs for authentication, non-repudiation, encryption only or encryption in combination with digital signature
- supports various types of device certificates that can be stored in hardware or software as required and used for devices, smart cards & tokens on a wide variety of platforms

Note that Unmanaged Solutions will not provide key backup and recovery or automatic renewal capabilities.

4.2 CMS Integration Changes for Unmanaged Solutions

With the above requirements in mind, the Entrust Authority Security Toolkit for the Java Platform provides a client API that accepts a request for an unmanaged user or device certificate and communicates with an Entrust CA to retrieve a certificate based on that request. The new API accepts a public key, information about the certificate policy pertaining to the request, and activation codes authorizing the request. See Entrust Authority Security Manager documentation for more information on certificate policies. Certificates may be requested for users or devices that have been setup using the Entrust CA for creation or recovery (user/device already has a reference number and authorization code). Entrust Authority Security Manager is very flexible in terms of the types of certificates that can be requested and the extensions that can be requested in the certificates and is capable of requesting critical and non-critical extensions.

An Administrator Authenticated (AA) mode has been added to the Entrust Authority Security Manager to provide additional flexibility to add certificate extensions. (This capability is only available with Security Manager 7.1 patch 96748 and later.) The Entrust Authority Security Toolkit for the Java Platform makes use of the Administrator Authenticated CMP mode to retrieve unmanaged certificates from an Entrust CA.

In addition to the Administrator Authenticated CMP mode, default certificate types and certificate definitions have been added to Security Manager Master Certificate Specification to simplify processing of unmanaged certificate requests. More specifically, an Entrust CA associates a certificate type and associated certificate definitions with each user. The definitions contain **policy** that governs the user's keys.

4.3 Architecture/Design

The Entrust Authority Security Toolkit for the Java Platform can be used to accomplish user enrollment onto a smart card once the user has been set up or created using the Entrust Authority Security Manager software. Each piece of certificate request information will contain the public key for which certification is being requested, an identifier for the certificate definition policy that the request corresponds to, and any requested X.509 certificate extensions. Every Entrust user is given a certificate type, which in turn contains a set of certificate definitions. Each certificate definition represents one of the user's key/certificate pairs, and contains the client policy settings governing this key/certificate.

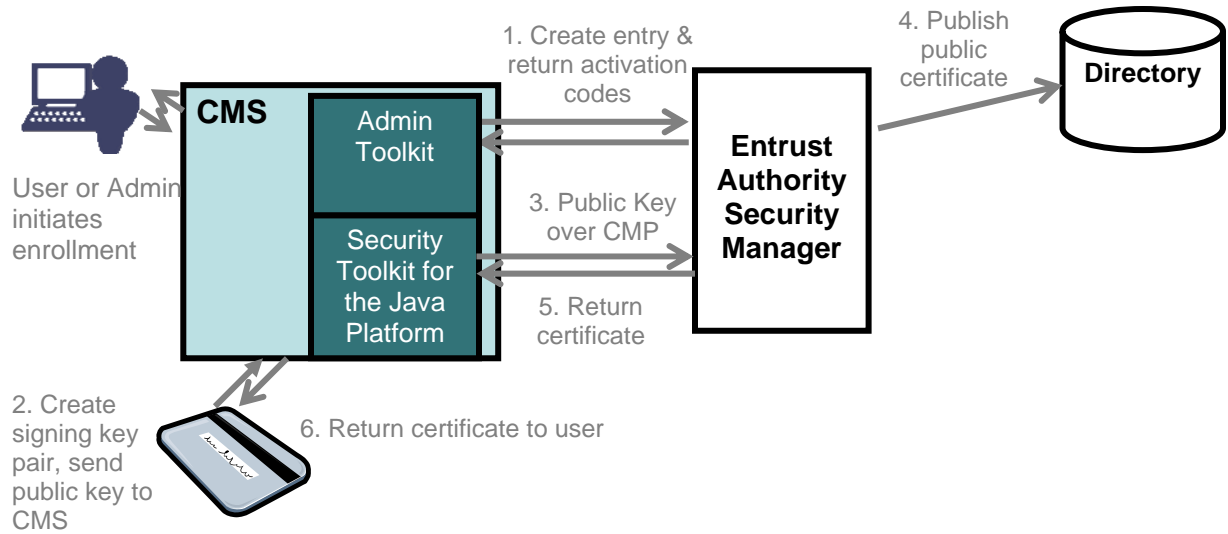
The Entrust Authority Security Toolkit for the Java Platform public class [EntrustP10CertRetriever](#) enables unmanaged end user certificates to be retrieved from the Entrust Authority Security Manager software when the key pair is generated externally. It requires the Entrust Authority Security Toolkit for the Java Platform to be set up for PKIX-CMP operation in Administrator Authenticated (AA) mode which is available with the Entrust Authority Security Manager 7.1 software, patch 96748 and later.

The Entrust Authority Security Toolkit for the Java Platform API accepts a public key, a certificate definition identifier, a reference number, and an authorization code. The request does not need to be in PKCS #10 format. The request may contain custom extension information and must contain the following:

- A public key
- Activation codes
- Information about certificate policy pertaining to the request

Further technical details are available in documentation for the Entrust Authority Security Toolkit for the Java Platform under `com.entrust.toolkit.credentials` Class *EntrustP10CertRetriever*. Request a copy of the [documentation](#) for technical integration details.

Figure 2: Sample enrollment request and response without key backup



5 Authorizing Requests to Entrust Certification Authority

Entrust Authority Security Toolkit for the Java Platform provides an API that accepts a certificate request and communicates with an Entrust CA to retrieve an end user certificate based on that request. Certificates can be retrieved for end users that exist within the Entrust Authority Security Manager in the *added* or *keyrecover* state. Requests for issuance or recovery of digital identities must contain valid activation codes authorizing fulfillment of the request by the Entrust CA.

Users may be added to the Entrust CA by an authorized Administrator, either manually via the administration GUI or programmatically via the Administration Toolkit for C.

The *createuser* sample included with the Entrust Authority Administration Toolkit for C provides the steps required to create a user and retrieve the activation codes from the Entrust CA using a programmatic approach. Request the [Entrust Authority Administration Toolkit for C Programmer's Reference Guide](#) for more details.

The required steps are:

1. Create a new directory entry
2. Create the user on the CA
3. Get the reference number and authorization codes

6 Planned Integration with CMS Products

In addition to the modifications described in the sections above, further enhancements are planned to address other integration requirements that may arise with respect to lifecycle management.

While customers generally use desktop clients to cost-effectively and transparently manage keys and certificates on smart cards or in software, some customers require all writing to a smart card be handled by a CMS via card management system standards. Entrust is currently reviewing CMS vendor requests in this area and plans to create simple high level APIs to enable CMS vendors to integrate with Entrust's lifecycle management capabilities without requiring key management expertise.

CMS vendors are encouraged to provide [feedback](#) on future integration requirements.

7 Summary

Entrust is committed to providing solutions that can help card management system vendors address customer needs in the area of smart card enrollment and management, including support for automated Digital ID management, HSPD 12 specifications and the related Personal Identity Verification I and II requirements. We are working closely with CMS vendors in an effort to proactively anticipate product features that will likely be desired by customers.

Whether CMS customers need managed or unmanaged solutions, Entrust helps provide tools for organizations to deploy credentials in a number of security applications. Entrust products provide an extensible environment that allows organizations to start with any one of Entrust's security applications and add capabilities as needed, while still leveraging their initial investment. By securing digital identities and information, Entrust solutions can help in making it possible to cost-effectively extend the enterprise to stakeholders and improve compliance with regulatory demands for stronger internal controls and information privacy.

For more information or to provide feedback on card management system needs related to integrating with Entrust products, please contact your Entrust Account Representative or one of the following:

North America Sales: 1-888-690-2424

EMEA Sales: +44 (0) 118 902 2098

Email: entrust@entrust.com

8 About Entrust

Entrust, Inc. is a world leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries use Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services can help customers in achieving regulatory and corporate compliance, while helping to turn security challenges such as identity theft and e-mail security into business opportunities. For more information on how Entrust can help secure your digital life, please visit: www.entrust.com.