Gemalto .NET 2.0 Smart Card
Certificate Enrollment using Microsoft Certificate Services
Introduction to the Gemalto .NET 2.0 Card

The purpose of this document is to provide a quick reference guide for the installation and basic configuration of Microsoft Certificate Services. This document is NOT a comprehensive guide on Microsoft Certificate Services, it just proposes a basic setup to enable enrollment of certificates on Gemalto .NET 2.0 Smart Cards. For further information on Microsoft Certificate Services, please refer to Microsoft’s documentation.

Gemalto .NET smart cards run a streamlined version of the .NET Framework in order to provide customizable two-factor authentication and full cryptographic capabilities seamlessly within the Windows® environment. Now, organizations can easily leverage Gemalto’s advanced smart card technology to secure their networks from end to end using a variety of security technologies to meet their needs while dramatically reducing implementation costs and complexity.

Gemalto .NET smart cards are natively supported in Microsoft Vista. For Windows 2000, XP and Server 2003 they are integrated with Microsoft's Base Smart Card Cryptographic Service Provider (CSP) Package, which is available for download via Windows Update. As a result, users do not need to install any proprietary middleware to use the Gemalto .NET Card.

Gemalto .NET smart cards are also compatible with Microsoft's Identity Lifecycle Manager (ILM), a policy and workflow solution for management of the lifecycle of digital certificates and smart cards.

Thanks to this high level of integration with Microsoft's Operating Systems and smart card related security solutions, Gemalto .NET smart cards offer the easiest and most cost efficient solution for implementation of a strong two-factor security infrastructure.

The Gemalto .NET 2.0 smart card architecture also provides an open platform for the development and implementation of a wide range of security solutions. It works as a seamless companion to the Microsoft .NET environment and service oriented architectures to provide support for on-card applications and services within the Windows® environment and to empower application developers through features such as advanced memory management, high security, and tight language integration.
Table of contents

CERTIFICATE ENROLLMENT USING MICROSOFT CERTIFICATE SERVICES ................................................................. 1

Introduction to the Gemalto .NET 2.0 Card ........................................................................................................... 2

Table of contents .................................................................................................................................................. 3

Introducing the Windows Smart Card Framework architecture ........................................................................ 4

Architecture Overview ......................................................................................................................................... 4

Installing Microsoft Certificate Services ........................................................................................................... 6

Prerequisites ........................................................................................................................................................ 6

Installation .......................................................................................................................................................... 6

Configuring Microsoft Certificate Authority .................................................................................................... 11

Issuance of a User Certificate on a Gemalto .NET Smart Card ........................................................................ 19

How to test and manage Gemalto .NET Test Cards ......................................................................................... 24

Glossary ........................................................................................................................................................... 25

References ......................................................................................................................................................... 25
Introducing the Windows Smart Card Framework architecture

Architecture Overview

In the past, smart card vendors made and maintained a monolithic Cryptographic Service Provider (CSP) for their own smart cards. Vendors had to write complete, custom, software CSPs to enable smart card scenarios for their cards.

The new Windows Smart Card Framework architecture is layered to separate the basic cryptography components at the top from the unique smart card hardware interfaces at the bottom; the unique hardware-specific interface for a given smart card receives the name of Minidriver (formerly called Card Module) and takes the form of a Dynamic Link Library (dll). Minidrivers leverage the common cryptographic components now included in the Windows platform.

This new architecture has been implemented in the Crypto API Next Generation (CNG) as part of the Microsoft Windows Vista™ OS, and is called the Microsoft Smart Card Key Storage Provider (KSP).

The cryptography for smart cards has also been implemented in the legacy Crypto API (CAPI) for Windows 2000 SP4, XP SP2 and Server 2003 SP1, and is known as the Microsoft Base Smart Card Cryptographic Service Provider (Base CSP). The Base CSP is not supported natively in these legacy Operating Systems, but it is available as Microsoft Windows Update # KB909520.

NOTE: The Microsoft Base Smart Card Cryptographic Service Provider should not be confused with the "Microsoft Base Cryptographic Provider v1.0", which is the default, non–smart card software CSP in Windows.

Base CSP and KSP provide the common software cryptographic portions, while the MiniDriver of a given smart card compliant with this architecture simply plugs in to provide access to the hardware and software of that particular smart card. Figure 1 illustrates the two Smart Card CSP architectures.

From an application developer perspective, the Base CSP, KSP and Minidriver interfaces provide a common way to access smart card features, regardless of the card type.

For users, the new architecture includes support for all preexistent smart card scenarios, and it also provides new tools for the management of the Personal Identification Number (PIN).
Gemalto .NET 2.0 Smart Card Certificate Enrollment using Microsoft Certificate Services

Figure 1: Microsoft Base Smart Card CSP vs. Vendor-Specific Custom Smart Card CSP
Installing Microsoft Certificate Services

Prerequisites

Prior to the installation of Microsoft Certificate Services, you shall verify your system complies with the following required components:

- Fully patched Windows 2003 Server
  - Configured as an Active Directory domain controller
  - IIS installed

- Must have administrative privileges to the server.

- Know the common name for Microsoft Certificate Authority to be defined during the CA installation.

- Microsoft Base Smart Card Crypto Service Provider (Base CSP) installed

- A PC/SC compliant Smart Card Reader (USB, Serial or PCMCIA)

Installation

1. Click Start/Control Panel
2. Select Add or Remove Programs
3. In left panel, select Add/Remove Windows Components
4. Check Certificate Services
   Click Next

5. Select Enterprise Root CA Type
   Click Next
6. Accept Warning
   - Click Yes

   ![Microsoft Certificate Services warning]

   After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?

   - Yes
   - No

7. Define Common Name for Certificate Authority (CA)
   - Click Next

   ![Windows Components Wizard]

   **CA Identifying Information**
   Enter information to identify this CA.

   - **Common name for this CA:**
   - **Distinguished name suffix:**
     DC=DemoFC, DC=com
   - Preview of distinguished name:
     CN=DC=DemoFC, DC=com
   - **Validity period:**
     - 5 Years
   - **Expiration date:**
     11/30/2010 10:33 AM
8. Select **Next** to accept Certificate Database Settings

9. Installation will Configure Components
10. Accept the prompt to temporarily stop ISS
   - Click Yes

11. Installation Complete
   - Click Finish
Configuring Microsoft Certificate Authority

The following certificate templates need to be published by the CA:

- **Enrollment Agent:** An enrollment agent certificate needs to be issued to any user who will request smart card certificate on behalf of another user during issuance
- **Smart Card User:** Any user issued a certificate based on this template may use it for Smart Card Logon, Client Authentication, secure email.
- **Smart Card Logon:** Any user issued a certificate based on this template may use it for Smart Card Logon

Follow the steps described below in order to do it:

1. Click Start/Administrative Tools/Certification Authority
2. Expand defined CA

3. Right-click **Certificate Templates** and Select **New**
   - Select **Certificate Template to Issue**
   - Select **Enrollment Agent**
   - Select **OK** to add
4. Right-click **Certificate Templates** and Select **New**
   - Select **Certificate Template to Issue**
   - Select **SmartCard Logon**
   - Select **OK** to add

5. Right-click **Certificate Templates** and Select **New**
   - Select **Certificate Template to Issue**
   - Select **SmartCard User**
   - Select **OK** to add
6. Launch IE and browse to \http://localhost/certsrv\n   Select a task: Request A Certificate

7. Select advanced certificate request
8. Select **Create & Submit Request to this CA**

   ![Image of Microsoft Certificate Services]

   **Advanced Certificate Request**

   The policy of the CA determines the types of certificates you can request. Click one of the following options to:
   - Create and submit a request to this CA
   - Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
   - Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

   Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

9. **Within Certificate Templates** drop-down box – Select **Enrollment Agent**

   ![Image of Microsoft Certificate Services]

   **Certificate Templates**

   - **Key Options**:
     - **Enrollment Agent**
   - **Key Usage**:
     - **Smartcard User**
   - **Key Store**:
     - **User specified key container name**
   - **Additional Options**:
     - **Request Format**: PKCS10
     - **Hash Algorithm**: SHA1

   ![Image of Certificate Templates selection]

   **Advanced Certificate Request**

   - **Key Options**:
     - **Enrollment Agent**
   - **Key Usage**:
     - **Smartcard User**
   - **Key Store**:
     - **User specified key container name**
   - **Additional Options**:
     - **Request Format**: PKCS10
     - **Hash Algorithm**: SHA1

   ![Image of Certificate Templates selection]
10. Within **Key Options section**
   - Create new key is selected
   - Microsoft Enhanced Cryptographic Provider v1.0
   - Click Submit

11. Within **Additional Options** section accept default settings
12. The Enrollment Certificate has been issued. Select **Install this certificate**

13. Select **Yes** to accept **Potential Scripting Violation**

   **Potential Scripting Violation**

   This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

   Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
14. Successfully generated and installed required Enrollment Certificate

The enrollment agent certificate must be issued to those users who will be requesting smart card certificates on behalf of other users, and needs to be installed in the local user store of the client computer from where the requests will be initiated. Alternatively this certificate and associated keys can reside on a smartcard.
Issuance of a User Certificate on a Gemalto .NET Smart Card

1. Ensure that the Base CSP package has been downloaded and installed on the client machine where the smart card user certificate will be issued. For the Gemalto .NET smart card there is no additional software that needs to be installed.

   Enrollment of smart card certificates via Base CSP from a CA installed on Windows Server 2003 works on Windows 2000 and Windows XP clients through a certificate enrollment component called xenroll. However on Windows Vista xenroll has been deprecated and replaced by a new component called certenroll. Unfortunately, certenroll is only compatible with Microsoft Longhorn Server, but not with Windows Server 2003.
   A workaround solution to enable enrollment of smart card certificates on a Vista client from a CA running on Windows Server 2003 is described in KB922706. Is is however not a straight forward solution.
   Microsoft is working on the issuance of an update to Windows Server 2003 SP2 and to ship the updated web enrollment pages as soon as possible. The new pages will have the logic to identify the client OS and use XEnroll or CertEnroll depending on the version making it seamless for the user or administrator.

2. Launch IE and browse to http://localhost/certsrv
   Select Request A Certificate

   ![Microsoft Certificate Services - Microsoft Internet Explorer](image)

   Welcome
   Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
   You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
   For more information about Certificate Services, see Certificate Services Documentation.

   Select a task:
   - Request a certificate
   - View the status of a pending certificate request
   - Download a CA certificate, certificate chain, or CRL

   ![Done](image)
3. Select **advanced certificate request**

4. Select **Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.**
5. Under **Enrollment Options** select **Smartcard User** as **Certificate Template**, and select **Microsoft Base Smart Card Crypto Provider** as the **Cryptographic Service Provider**.

In addition to the Microsoft Base Smart Card Crypto Provider, the drop down menu for Cryptographic Service Provider will present other options corresponding to several Monolithic CSPs. Some of them correspond to other Gemalto products, identified under the name of some of Gemalto’s former entities (Axalto CSP, Gemplus Gemsafe CSP and even Schlumberger CSP). It is important to avoid the mistake of choosing any of these monolithic CSPs for enrollment of certificates on a Gemalto .NET card. The Gemalto .NET card is compliant with the Base CSP / Minidriver architecture and accordingly relies on the Base CSP as its Crypto Service Provider.
6. Click on the **Select User** button and choose the end user for the certificate.

7. Insert a Gemalto .NET Smart Card into the Reader and click on the **Enroll** button.
8. The **Smart Card PIN** dialog box will pop up. 
   - Enter the PIN of the Smart card and select **OK**

![Smart Card PIN dialog box]

9. Upon successful verification of the PIN, the Smart Card will generate a Key Pair. The private key is securely stored in the card itself whereas the public key is returned to the Certificate Authority. The CA will then issue a certificate based on the public key received from the card, and will store it in card completing the certificate enrolment process.

   The Gemalto .NET v2 Smart Card default PIN Value is **0000**
How to test and manage Gemalto .NET Test Cards

Gemalto .NET Utilities is a Web portal offering a set of tools that enable, among others, the following operations:

**PIN Management**
- Change PIN
- Unblock PIN

**Certificate Management**
- View on-card certificates
- Delete certificate
- Delete all certificates
- Load P12 Key Pair (coming soon)

**Card Management**
- Check Card Characteristics
- Check active on-card services
- Load a .NET Assembly

All these services are freely available and fully functional on Gemalto .NET cards. The only restriction is that the card Administrative key must not have changed from its default value.

![The Gemalto .NET v2 Smart Card default administrative key value is 0000..0000 (24 bytes, 48 digits long)](image)

To use Gemalto .NET utilities visit [www.netsolutions.gemalto.com](http://www.netsolutions.gemalto.com) and select the Utilities menu.
## Glossary

<table>
<thead>
<tr>
<th><strong>Base CSP</strong></th>
<th>Microsoft Base Smart Card Crypto Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>API</strong></td>
<td>Application Protocol Interface</td>
</tr>
<tr>
<td><strong>CAPI</strong></td>
<td>Cryptography API</td>
</tr>
<tr>
<td><strong>CNG</strong></td>
<td>Crypto API Next Generation</td>
</tr>
<tr>
<td><strong>CSP</strong></td>
<td>Cryptographic Service Provider</td>
</tr>
<tr>
<td><strong>PIN</strong></td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td><strong>KSP</strong></td>
<td>Key Storage Provider</td>
</tr>
<tr>
<td><strong>CMS</strong></td>
<td>Card Management System</td>
</tr>
<tr>
<td><strong>ILM</strong></td>
<td>Microsoft Identity Lifecycle Manager</td>
</tr>
</tbody>
</table>

## References

1. Enterprise Smart Card Deployment in the Microsoft Windows Smart Card Framework  
   – Derek Adam, Microsoft, June’06