Application Note
Gemalto Smart Cards with Citrix XenApp 5.0
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms’ resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© Copyright 2009 Gemalto N.V. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.
Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

December 14, 2009
Contents

Preface........................................................................................................................................ 6
Who Should Read This Book .............................................................................................................. 6
Conventions ........................................................................................................................................ 6
Contact Our Hotline ........................................................................................................................... 6

Overview ..................................................................................................................................... 7
Citrix XenApp ........................................................................................................................................ 7
Gemalto Smart Card Products ............................................................................................................ 8
Classic TPC Applications (Java Card) ................................................................................................. 8
.NET Card........................................................................................................................................... 9
Smart Enterprise Guardian (SEG) ........................................................................................................ 9
Integration of both products .................................................................................................................. 10
Components description ....................................................................................................................... 13
Main steps of the use case ...................................................................................................................... 14

Prerequisites .................................................................................................................................. 15
On Client machine and XenApp machine: ............................................................................................. 15
  Install Base CSP to use .Net Card ...................................................................................................... 15
  SEG installation ............................................................................................................................... 16
  Install Classic Client to use Gemalto Smart Card .......................................................................... 16
On Domain controller machine: ........................................................................................................... 16
On XenApp machine: ............................................................................................................................ 16
On Web Interface machine: .................................................................................................................. 17

Installation and configuration of XenApp 5.0 ....................................................................... 27
Installation of XenApp 5.0 ...................................................................................................................... 27
Configuration of XenApp 5.0 .................................................................................................................... 36

Installation and configuration of Web Interface 5.2 ............................................................. 40
Installation of Web Interface 5.2 .............................................................................................................. 40
Configuration of Web Interface 5.2 .......................................................................................................... 43
  XenApp Services Sites: ................................................................................................................... 43
  XenApp Web Sites: ......................................................................................................................... 49

Installation of Citrix Online Plug-in ........................................................................................ 56
Pass-through with Smart card configuration ...................................................................................... 57

Access to Citrix Published Applications ......................................................................................... 62
XenApp Services Sites ......................................................................................................................... 63
XenApp Web Sites .............................................................................................................................. 65
List of Figures

Figure 1 - Global Architecture ............................................................................................................ 10
Figure 2 - Use case architecture ........................................................................................................ 11
Figure 3 - Microsoft Base CSP Installation .......................................................................................... 15
Figure 4 - Classic Client Installation .................................................................................................. 16
Figure 5 - J#Net2.0 Installation ........................................................................................................... 17
Figure 6 - IIS Setup 1/4 ....................................................................................................................... 18
Figure 7 - IIS Setup 2/4 ....................................................................................................................... 18
Figure 8 - IIS Setup 3/4 ....................................................................................................................... 19
Figure 9 - IIS Setup 4/4 ....................................................................................................................... 19
Figure 10 - IIS Configuration ................................................................................................................ 20
Figure 11 - IIS Configuration: Web Site Properties .............................................................................. 20
Figure 12 - IIS Configuration: Web Server Certificate Wizard ............................................................. 21
Figure 13 - IIS Configuration: Server Certificate ................................................................................ 21
Figure 14 - IIS Configuration: Immediate Re .................................................................................... 22
Figure 15 - IIS Configuration: Name and Security Settings ................................................................. 22
Figure 16 - IIS Configuration: Site's Common Name ........................................................................... 23
Figure 17 - IIS Configuration: Geographical Information .................................................................... 23
Figure 18 - IIS Configuration: SSL Port ................................................................................................ 24
Figure 19 - IIS Configuration: Certification Authority ........................................................................ 24
Figure 20 - IIS Configuration: Certificate Request Submission ........................................................... 25
Figure 21 - IIS Configuration: Completing Certificate Wizard ............................................................ 25
Figure 22 - Web Server Certificate ...................................................................................................... 26
Figure 23 - Secure Communications .................................................................................................... 26
Figure 24 - XenApp Setup .................................................................................................................... 27
Figure 25 - XenApp Setup: Install Server-Hosted Apps ...................................................................... 28
Figure 26 - XenApp Setup: Agreement ............................................................................................... 28
Figure 27 - XenApp Setup: Edition ...................................................................................................... 29
Figure 28 - XenApp Setup: Components ............................................................................................ 29
Figure 29 - XenApp Setup: Installation Directory ............................................................................... 30
Figure 30 - XenApp Setup: Create Farm ............................................................................................. 30
Figure 31 - XenApp Setup: Create Server Farm .................................................................................. 31
Figure 32 - XenApp Setup: Farm Credentials ...................................................................................... 31
Figure 33 - XenApp Setup: IMA Encryption ......................................................................................... 32
Figure 34 - XenApp Setup: License Server Configuration ................................................................. 32
Figure 35 - XenApp Setup: Shadowing Configuration ........................................................................ 33
Figure 36 - XenApp Setup: XML Port Configuration ......................................................................... 33
Figure 37 - XenApp Setup: RDP Configuration .................................................................................. 34
Figure 38 - XenApp Setup: Server Address ....................................................................................... 34
Figure 39 - XenApp Setup: Start Installation ...................................................................................... 35
Figure 40 - XenApp Configuration ...................................................................................................... 36
Figure 41 - XenApp Configuration: Select Products ......................................................................... 37
Figure 42 - XenApp Configuration: Select Servers ............................................................................ 37
Figure 43 - XenApp Configuration: Preview Discovery ...................................................................... 38
Figure 44 - Delivery Services Console ............................................................................................... 38
Figure 45 - Web Interface Setup ......................................................................................................... 40
Figure 46 - Web Interface Setup: License Agreement ......................................................................... 41
Figure 47 - Web Interface Setup: Installation Location ....................................................................... 41
Figure 48 - Web Interface Setup: Location of Clients ......................................................................... 42
Figure 49 - Web Interface Setup: Ready to Install ............................................................................. 42
Figure 50 - Web Interface Setup: Create Sites .................................................................................... 43
Figure 51 - WI Configuration: XenApp Services Sites ...................................................................... 44
Figure 52 - WI Configuration: Summary Configuration ..................................................................... 45
Figure 53 - WI Configuration: XenApp Service Site Created ............................................................... 45
Figure 54 - WI Configuration: Server Farm ....................................................................................... 46
Preface

The Gemalto two-factor authentication solution provides strong authentication based on smart cards for the enterprise, banking, and internet service provider (ISP) markets.

This solution enables organizations to deploy a strong authentication solution for their end-users, whether local or remote. The system can service a broad range of deployments, from small corporations with less than 100 users to ISPs with potentially millions of users.

Who Should Read This Book

This guide is intended for system administrators responsible for configuring the Microsoft Active Directory in order to use Gemalto Smart Cards to authenticate mobile users with Citrix XenApp.

Administrators should be familiar with:

- Certification Authority and PKI Concept
- Citrix XenApp

Conventions

The following conventions are used in this document:

In this manual, the following highlighting styles are used:

- **Bold** – Instructions, commands, file names, folder names, key names, icons, menus, menu items, field names, buttons, check boxes, tabs, registry keys and values.
- *Italic* – Variables that you must replace with a value, book titles, news or emphasized terms.

In this manual, hyperlinks are marked as described below

- **Internal Links** – Displayed in quotation marks. When viewing this book online, click an internal link to jump to a different section of the book.
- **External Links** – Displayed in blue, underlined text. When viewing this book online, click an external link to launch your default browser (or email program) to navigate to that Web address or compose an email.

In this manual, *notes* and *cautions* are marked like this:

**Note:** Information that further explains a concept or instruction, tips, and tricks.

**Caution:** Information that alerts you to potentially severe problems that might result in loss of data or system failure.

Contact Our Hotline

If you do not find the information you need in this manual, or if you have any questions, contact our hotline commissioning.support@gemalto.com
Overview

This document provides a deployment scenario in order to configure the XenApp from Citrix to use Gemalto Smart Card to authenticate Mobiles Users through a Microsoft Active Directory to access their streamed applications.

Caution: Consequently, this document should not be considered as an instruction manual on how to configure your system.

Citrix XenApp

Citrix XenApp is an application virtualization/application delivery product that allows users to connect to their corporate applications. XenApp can either host applications on central servers or allow users to interact with them remotely or stream and deliver them to user devices for local execution.
Gemalto offers a complete family of compatible smart cards, smart card readers, authentication and secure memory tokens, software, and more. These products are based on our proven smart card expertise and enable component optimization and integration with existing hardware infrastructures.

The Gemalto strong authentication portfolio supports current industry standards and provides solutions that operate in both Java and .NET environments.

**List of smart card product:**

**TOP Java Card**  
Trusted Open Platform Java Card

**Classic TPC**  
For PKI applications

**Classic TPC MDE**  
Microsoft mini-driver and PKCS#11 support

**IAS TPC**  
Java Card fully compliant with IAS specifications

**.NET Smart Card**  
Fully integrated with Microsoft platform

**.NET Bio smart card**  
Biometric Authentication solution for Microsoft Windows

**Hybrid Card Body**  
Hybrid card body for converged physical and logical access systems

**Instant Badge Issuance**  
Smart card badge issuance system compatible with Microsoft ILM & CLM

**Classic TPC Applications (Java Card)**

Classic TPC is a smartcard designed for Public-key based applications. Classic TPC is immediately compatible with the Classic Client software, which is offering both CSP API and PKCS#11 API allowing Classic TPC integration with any type of PKI application.

The Classic TPC product range is the following:
- Classic TPC IS V2
- Classic TPC IM
- Classic TPC IM CC

Detailed information about Classic TPC is available in the [Product Information Sheet](#).
.NET Card

Gemalto .NET is an implementation of a .NET Framework for Smart Cards, empowering developers to build services that take advantage of the enhanced programming and communication capabilities of the .NET Framework and the advanced security and cryptographic services that are the foundation of Gemalto Smart Cards. Combined with the award winning SConnect technology, Smart Cards and Tokens can now communicate with all kind of Web Services, and hefty client based solutions can be replaced with zero footprint web based solutions.

More information can be retrieve at this URL: [http://www.gemalto.com/products/dotnet_card/](http://www.gemalto.com/products/dotnet_card/)

Smart Enterprise Guardian (SEG)

Strong Authentication and Secure Data Storage Solution

Smart Enterprise Guardian (SEG) is a unique USB device based on industry standards that secures identity credentials and sensitive files with proven smart card technology. Jointly developed by Gemalto and Lexar, it protects up to 2 GB of data on a USB drive and supports strong authentication, digital signature and file encryption.

The SEG combines Gemalto .NET technology and Lexar hardware-based memory encryption technology to provide unrivaled secure mobility

This device is one of the first personal portable security device (PPSD) that offers secure portable memory with AES 256-bit hardware-based encryption and strong authentication using Gemalto One-Time-Password or PKI (Public Key Infrastructure) services. Native support for the device is built into Windows Vista™ and also is available as a Microsoft update for Windows® XP and 2000 systems.

Integration of both products

By delivering certificates into the **Gemalto Classic TPC or .Net Smart Card** users will be able to establish a connection to enjoy safely their session from their computer.

User’s certificates are generated using the certificate authority and stored on users smart cards. The smart-card contains the certificate then the smart-cards are associated to users.

![Figure 1 - Global Architecture](image)

**Description**

When a user wants to log on, he would be prompted to insert his smart-card and enter his PIN Code. Then the authentication using the certificate will occur. The **Domain Controller** will check the validity of the certificate and the existence of the user.

Once the authentication is successful the user will access to his desktop.

The Citrix XenApp Plug-in will authenticate to the XenApp Services Site using Integrated Windows Authentication and to the server Farm using Smart card authentication.

With pass-through authentication, the user doesn’t have to present his credentials again to access his applications.
Use Case

The Use Case shows a basic configuration of Citrix XenApp. The end user has a smart car and wants to access his applications with Citrix. The main interest of this use case is to see how the end-user can use his smart card for his Windows session and access to his Citrix published applications.

![Use Case Architecture](image)

**Requirement**

In order to setup such architecture, we need:

- On the domain controller machine
  - A directory to manage users: in our case it is Active Directory
  - A Certificate Authority to deliver certificate to users

- On the XenApp machine
  - A installation of Citrix XenApp 5.0 (Enterprise Mode)
  - All packages installed for smart card (middleware)

- On the Web Interface Machine
  - A standard installation of Web Interface 5.2

- One the client machine
  - A client machine installed with Windows XP SP3, with all packages for smart card (readers and middleware)
  - A Classic TPC, SEG or .NET smart card with a smart card logon certificate for the company domain
- An installation of Citrix Online Plug-In with a configuration for Pass-through with Smart card
Components description

**Domain Controller:**
This is the domain controller hosting the Active Directory. The Certificates Authority is installed on this machine for convenience.

<table>
<thead>
<tr>
<th>Name</th>
<th>Dctest</th>
</tr>
</thead>
<tbody>
<tr>
<td>O.S</td>
<td>Microsoft Windows 2003 Server Enterprise</td>
</tr>
<tr>
<td>IP</td>
<td>10.10.237.130</td>
</tr>
<tr>
<td>AD Domain</td>
<td>testing.solutions.gem</td>
</tr>
<tr>
<td>DNS Client</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>Services</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td></td>
<td>Microsoft Certificates Authority</td>
</tr>
</tbody>
</table>

**Citrix XenApp:**
This is the machine hosting Citrix XenApp, with Citrix Delivery Services Console to manage the publish the applications you want to.

<table>
<thead>
<tr>
<th>Name</th>
<th>Citrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>O.S</td>
<td>Microsoft Windows 2003 Server Enterprise</td>
</tr>
<tr>
<td>IP</td>
<td>10.10.236.130</td>
</tr>
<tr>
<td>AD Domain</td>
<td>testing.solutions.gem</td>
</tr>
</tbody>
</table>

**Web Interface:**
This is the machine hosting the Web Interface. The Web Interface provides secure access to XenApp resources from anywhere through any device with a Web browser.

<table>
<thead>
<tr>
<th>Name</th>
<th>Xenapp</th>
</tr>
</thead>
<tbody>
<tr>
<td>O.S</td>
<td>Microsoft Windows 2003 Server Enterprise</td>
</tr>
<tr>
<td>IP</td>
<td>10.10.198.132</td>
</tr>
<tr>
<td>AD Domain</td>
<td>testing.solutions.gem</td>
</tr>
</tbody>
</table>

**Client Machine:**
The user will use this machine to reach the Domain.

<table>
<thead>
<tr>
<th>Name</th>
<th>Citrixtest</th>
</tr>
</thead>
<tbody>
<tr>
<td>O.S</td>
<td>Windows XP SP3</td>
</tr>
<tr>
<td>IP</td>
<td>39.0.0.1</td>
</tr>
</tbody>
</table>
Main steps of the use case

The main steps are:

Administrator tasks:
1. Prerequisites
2. Installation and configuration of XenApp 5.0
3. Installation and configuration of Web Interface 5.2
4. Installation of Citrix Online Plug-in
5. Pass-through’s configuration for end-users

End-users tasks:
6. Access to Citrix published applications
Prerequisites

Note: Some packages you need are on the Citrix XenApp CD in /Support/

On Client machine and XenApp machine:

Install Base CSP to use .Net Card

Not needed for VISTA machine

1. Download from Microsoft site, the Microsoft Base Smart Card Cryptographic Service Provider Package (KB909520)

2. Execute this package and follow the setup instructions

Figure 3 - Microsoft Base CSP Installation
SEG installation

The first time you insert the SEG you have to install the drivers. Read the SEG_Documentation.pdf in the public storage of the SEG.

Note: On VISTA, the SEG is automatically recognized

Install Classic Client to use Gemalto Smart Card

1. Execute the package Classic Client and follow the setup instructions

![Figure 4 - Classic Client Installation](image)

On Domain controller machine:

In our use case we used a user named “jdoe”.

This user has a smart card with a certificate issued from a CA named GemaltoCA. It is a certificate from the template Smart User.

On XenApp machine:

1. Install Dot Net Framework 3.5 SP1
2. Install Windows Server 2003 KB961118
On Web Interface machine:

1. Install Dot Net Framework 3.5 SP1

2. Install J#Net 2.0

![J#Net 2.0 Installation](image)

Microsoft Visual J# is a tool that developers, particularly those familiar with the Java language syntax, can use to build applications and services on the JET Framework. Visual J# allows you to develop applications that run on a Java Virtual Machine and access .NET applications and services built using Visual .NET, if not only on the JET Framework.

Figure 5 - J#Net 2.0 Installation
3. **Install Internet Information Services**
   - Go to Control Panel -> Add or Remove Programs -> Add/Remove Windows Components

   ![Image of Windows Components](image1.png)

   **Figure 6 - IIS Setup 1/4**

   - Check **Application Server** and click on **Details**

   ![Image of Application Server](image2.png)

   **Figure 7 - IIS Setup 2/4**

   - Check **ASP.NET** and **Internet Information Services** and click on **Details**
- Click on **World Wide Web Service** and then click on **Details**

- Check **Active Server Pages** and click **OK** until you have the Windows Components Wizard

- Finally click on **Next** and follow the setup instructions
Now we need to create our Web Site SSL for the future Web Interface Site.

- Go to Administrative Tools -> IIS

- Right click on Default Web Site -> Properties

- In Secure Communications click on Server Certificate to create a Web server certificate
We will now request a certificate for our website.

Choose Create a new certificate.
- We need to request immediately a certificate from the CA

- Name your new certificate. In our use case it is *Web Interface*
Figure 16 - IIS Configuration: Site’s Common Name

- Enter your site’s common name. In our use case it is xenapp.testing.solutions.gem

Figure 17 - IIS Configuration: Geographical Information
• Choose your **SSL port**. In our case we let the port by default: 443

• Choose your **Certification Authorities**. In our use case it is our CA from Domain controller *dctest*
• Click on Finish to request your Web Server certificate
In Secure Communication, by clicking View Certificate, you'll see information about your Web Server Certificate.

Figure 22 - Web Server Certificate

Also in the Secure Communications we need to configure the SSL communication.

Figure 23 - Secure Communications

- Check **Require secure Channel (SSL)** and **Require 128-bit Encryption**
- Choose **Ignore Client Certificates**
Installation and configuration of XenApp 5.0

On Citrix machine…

Installation of XenApp 5.0

Launch the installation of XenApp 5.0 FP2 for Windows Server 2003 and follow the setup instructions:

- Click on Install XenApp

![Figure 24 - XenApp Setup](image)
Figure 25 - XenApp Setup: Install Server-Hosted Apps

- Choose **Install Server Hosted Apps**

Figure 26 - XenApp Setup: Agreement

- Check the license agreement and click on **Next**
• Choose XenApp Enterprise Edition

• Check XenApp / Management Console / Citrix Plugin-in
Figure 29 - XenApp Setup: Installation Directory

Choose the installation folder

Figure 30 - XenApp Setup: Create Farm

Choose a name for your farm. In our case it is *CitrixGem*
• Create a local database server

• Enter the administrator credentials for your domain. In our case it is TESTING\Administrator
Let's **IMA Encryption** unchecked

Choose **Configure license server at a later time**

**Note:** You will have a warning message each time you will open your application until license server is not configured
Let's the option by default

Use a separate port for the Citrix XML service. In our case it is 8888
Let's the option by default

Enter the URL of your Citrix Web Interface. In our use case it is:
- https://xenapp.testing.solutions.com
Figure 39 - XenApp Setup: Start Installation

- Click **Next** to finalize the installation of **Citrix XenApp 5.0**
Configuration of XenApp 5.0

Now we need to configure for the first time our XenApp 5.0 and run the discovery.

- Click on **Next**
• Choose the products you want to use and click on Next

• Click on Add Local Computer and click on Next
You have now configured your XenApp Server. Click on **Next** to discover it.

We need now to publish an application from our server **XenApp**.

1. Open **Delivery Services Console** in **Start->All Programs->Citrix->Management Consoles**
2. Follow the publishing applications wizard for XenApp to publish a new application from your farm Citrix. In our use case we decided to publish *Notepad*
Installation and configuration of Web Interface 5.2

On XenApp machine...

Installation of Web Interface 5.2

Figure 45 - Web Interface Setup
Figure 46 - Web Interface Setup: License Agreement

- Accept the license agreement and click **Next**

Figure 47 - Web Interface Setup: Installation Location

- Choose your installation location
Figure 48 - Web Interface Setup: Location of Clients

- Choose **Skip this step** and click **Next**

Figure 49 - Web Interface Setup: Ready to Install

- Click **Next** to finalize the installation
Figure 50 - Web Interface Setup: Create Sites

Configuration of Web Interface 5.2

We need now to create Sites from **Citrix Web Interface** for end-users.

- Open **Citrix Web Interface Management**
End-users can access their Citrix applications in two ways, either through the Web Interface or by PNAgent. For this, we must configure two separate sites for each way to authenticate.

**XenApp Services Sites:**

- Click on **Create Sites**

![Create Site](image)

**Figure 51 - WI Configuration: XenApp Services Sites**

- Specify the IIS location and click **Next**
Figure 52 - WI Configuration: Summary Configuration

Figure 53 - WI Configuration: XenApp Service Site Created
Once the site set up, configure it.

- Specify the farm name, the IP address of the Citrix server and the XML Service port.

- Select the resource type. In our use case we used Online resource.
Figure 56 - WI Configuration: Confirm Settings

- Click Finish to finalize the site’s configuration

Figure 57 - Web Interface Management
We now need to configure how users will connect to the Web Interface. In our case we use Pass-through with Smart Card.

- Select your XenApp Services Sites and click on Authentication Methods

  ![Figure 58 - PNAgent Authentication Methods](image)

  - Check Pass-through with smart card and click on Properties

  ![Figure 59 - PNAgent Properties](image)

- In General->Kerberos Authentication check the option about the Kerberos

The XenApp Services Sites is now configured to use Pass-through with smart card.
XenApp Web Sites:

In XenApp Web Sites:

- Click on Create Sites

Specify the IIS location and click Next

Figure 60 - WI Configuration: XenApp Web Sites
Figure 61 - WI Configuration: Point of Authentication

- Specify where user authentication takes place. In our use case we use *At Web Interface*.

Figure 62 - WI Configuration: Summary Configuration
Figure 63 - WI Configuration: Web Site Created
Once the site set up, configure it.

Figure 64 - WI Configuration: Server Farm

- Specify the **Farm name**, the **IP address** of the Citrix server and the **XML Service port**

Figure 65 - WI Configuration: Authentication Methods

- Check **Pass-through with smart card** and click **Next**
Choose **Allow any domains**

Choose the logon screen as your convenience
Verify settings and click Finish to finalize the configuration.
Figure 70 - Web Interface Management

The XenApp Web Sites is now configured to use Pass-through with smart card.
Installation of Citrix Online Plug-in

On Client machine…

Open a session with **Administrator rights**.

- Launch the **Citrix Full plug-in** installation

- Once installation is completed, close the **Citrix Change Server** window
Pass-through with Smart card configuration

- Open the registry and navigate to:
  - HKLM\System\CurrentControlSet\Control\NetworkProvider\HwOrder
  - Double-click on ProviderOrder string and place PnSson at the beginning of the string
  - Do the same for:
    - HKLM\System\CurrentControlSet\Control\NetworkProvider\Order

- Reboot the PC

At this point, if you look at the services that are running on your machine, you can see SSONSVR.EXE service as running.

Now we need to configure the Group Policy about Citrix.

- Run `gpedit.msc`
Choose `icaclient.adm` in `C:\Program Files\Citrix\ICA Client\Configuration\` and click **Open**

Once the template is added, go to the new components Citrix.
Figure 74 - Group Policy Configuration: User Authentication

- Open **Citrix Components->Citrix Online Plug-in->User authentication** and open **Local user name and password**

Figure 75 - Group Policy Configuration: Pass-through Authentication

- Choose **Enabled** and check **Enable pass-through authentication**, click **OK**
Now we must configure Internet Explorer settings for our future end-users.

- Open Internet Explorer and add your XenApp Web Sites to your **Trusted Sites**
  - Tools->Internet Options->Security->Trusted Sites

- In Group Policy go to User Configuration
  - Go to Windows Settings->Internet Explorer Maintenance->Security and open Security Zones and Content Ratings
Choose **Import the current security zones and privacy settings** and click **Apply**

The **XenApp Web Site** is now trusted by the computer.
Access to Citrix Published Applications

Our infrastructure is made up of two sites deployed. We can access to our published applications by web browser through Web Interface and by the Citrix Agent (PNAgent).

The client is part of the domain TESTING. We use Smart card for the authentication.

You need to log on your session with your Smart card:

- Insert your Smart card and enter your PIN to log you on your session safely
Once connected to your session, **Citrix** asks you to enter the address of **XenApp Services sites**

**Figure 77 - Citrix Online Plug-in**

- Enter the server address where your XenApp Services Sites is created

**Note:** It is possible that you have a warning message about the authentication method. Log out your Windows session and log in again with your Smart card.

**Figure 78 - Authentication Method Warning Message**

- You are not logged on XenApp Services Sites:

- You are logged on XenApp Services Sites:
Once connected with the PNAgent, go to **Options -> Display Applications**:

- In **Desktop Options**, check **Show Applications on desktop**, and name the folder.

If everything is fine you should have a Citrix icon on your desktop with all your applications published.
XenApp Web Sites

After your smart card log on your session open your web browser and go to your XenApp Web Sites:

- In our use case it is:
  - [https://xenapp.testing.solutions.gem/Citrix/Xenapp/](https://xenapp.testing.solutions.gem/Citrix/Xenapp/)

- Click on your application to access it