

Guide To Establishing A Global Trusted PKI

Establishing a Global trusted PKI using Microsoft Windows Certificate Services & WIS@Key CertifyID TrustCentre™ (CertifyID BlackBox™)

Date: September 2007

Version: 1.3

Authors: WIS@Key SA

Table of content

INTRODUCTION.....	3
ABOUT MICROSOFT WINDOWS CERTIFICATE SERVICES (CA) PKI	3
ABOUT CERTIFYID TRUSTCENTRE™ (CERTIFYID BLACKBOX™).....	3
ABOUT OISTE WISEKEY GLOBAL ROOT CA	4
CERTIFICATION AUTHORITIES	4
CERTIFYID BLACKBOX™ COMPONENTS	5
INSTALLATION OF CERTIFYID BLACKBOX™	6
CERTIFYID BLACKBOX™ PHASE 1.....	6
REGISTRATION	6
ADMINISTRATOR'S CREDENTIALS	7
CERTIFICATION AUTHORITY DATA	7
SUBSCRIBER AGREEMENT.....	10
CONFIRMATION	11
PREPARATION OF THE CA SERVER.....	11
CERTIFYID BLACKBOX™ PHASE 2.....	12
ADMINISTRATOR CERTIFICATE DOWNLOAD	12
SECURITY AND AUDIT REQUIREMENTS	14
DOWNLOAD CA INSTALLATION DATA	14
CERTIFYID BLACKBOX™ CA INSTALLATION	15
UPLOAD CA_AUDIT FILE	19
UPLOAD CA CERTIFICATE REQUEST FILE	19
DOWNLOAD CA CERTIFICATE	19
CDP AND AIA LOCATIONS CONFIGURATION	19
DEFINING YOUR CDP LOCATIONS	20
DEFINING YOUR AIA LOCATIONS	21
INSTALL YOUR CA CERTIFICATE.....	22
TEST ACCESS TO WISEKEY CRL AND AIA LOCATIONS	22
START THE CA SERVICE.....	22
INSTALL THE CA CERTIFICATE	22
START THE CA SERVICE.....	23
PUBLISH YOUR CA CERTIFICATE TO THE AIA LOCATION.....	23
SETUP CRL PUBLISHING	23
TEST THE CDP LOCATIONS	23
TEST THE AIA LOCATIONS.....	23
PROXY SETTINGS.....	23
PROVISION USER CERTIFICATES.....	23
CONCLUSION	24

Introduction

About Microsoft Windows Certificate Services (CA) PKI

The Microsoft Windows CA, or Windows Certificate Services, or Active Directory Certificate Services, enables the deployment of a cost-effective, robust, flexible and scalable enterprise PKI provisioning system.

Across many sectors and countries, an increasing amount of organisations are installing their own Certification Authorities (CA) or Certificate Service Providers (CSP). The majority of such CAs are NOT trusted (or recognised) by the most popular Internet browsers such as Mozilla Firefox, Internet Explorer or email clients such as Thunderbird, or Microsoft Outlook.

Users thus receive warnings that the organisation's signed email, and websites are not trusted. This creates a huge problem for the organisation, as it results in damage to their reputation, loss of confidence and trust in that organisation by the user. It would be practically impossible for each such organisation to meet the needs and requirements that are necessary to embed their Roots in those applications. However there is no need for organisations to undertake this expensive exercise and burden, WISEKey developed the CertifyID Trust Service, delivered in the cost-effective CertifyID TrustCenter to address the need of such organisations.

About CertifyID TrustCentre™ (CertifyID BlackBox™)

The WISEKey CertifyID TrustCentre™ (CertifyID Blackbox™) is a unique product offering a complete and affordable out-of-the box solution for establishing a Trusted Identity Infrastructure dedicated to your organisation. WISEKey CertifyID BlackBox facilitates the installation of the Windows CA subsystem and most importantly enables the provisioning of internationally trusted certificates from the using the OISTE foundation's Global Trust Network signing service.

OISTE (l'Organisation Internationale pour la Sécurité des Transactions Électroniques) is Swiss-based, independent, not-for-profit foundation created in 1998 with the aim of expanding the use of digital certification and to ensure the interoperability of certification authorities and e-transaction systems.

The CertifyID TrustCentre™ enables easy and effective digital certificate and identity management within your organisation by extending the organisation's PKI and enabling the issuance of S/MIME and SSL certificates chained to WISEKey's pre-distributed root certificate. WISEKey's certificate is present in the majority of web browsers worldwide, and is available in most popular operating systems, servers, and email clients.

Using the CertifyID Trust Service, the Root or Issuing CA of an organisation is chained under the OISTE WISEKey embedded Root Certificate. Organisations to benefit from:

Global Trust Recognition & Acceptance

The OISTE WISEKey Root is a globally accepted Root Certification Authority, and thus permits all other Certification Authorities that subscribe to the CertifyID Trust Service, and are chained under it, to benefit from its presence and acceptance in the majority of Internet browsers and operating systems. Thus all the certificates of the organisation's certification authority become recognised and trusted internationally, ensuring the global use and acceptance of their certificates across business sectors, and geographies.

Global Interoperability and Neutrality

The International Organisation for Secure Electronic Transactions (ISETO/OISTE) is a Swiss based not-for-profit organisation that owns the OISTE WISEKey Global Root certification authority.

OISTE appoints WISEKey as the private operator responsible for managing this Root Certification Authority on behalf of the OISTE organisation. WISEKey created the CertifyID Trust Service as a commercial offering linking organisations to the OISTE Root through a certificate signing service.

Customers of the CertifyID Trust Service can request representation at the OISTE organisation to have complete oversight of the Root certification practices and operations, and participate in the OISTE Geneva Security Forum and other events.

OISTE ensures Swiss neutrality, and multipartite responsibility – CertifyID TrustCentre customers can thus have transparency and participate in the Root process.

Privacy and Independence

The Organisation remains in complete sovereign control of their certification authority.

Independent Management

Management of the certificate lifecycle, such as issuance, revocation, and suspension of certificates, is done by the enterprise, and does not involve WISEKey or OISTE.

CP/CPS Template / Customisable Policies

The organisation has the advantage of a template set of policies and practices that he is free to customise to produce his own policies. Guidelines are provided for key management, Security policies, personnel policies, and other organisation policies. The organisation can use these documents as is, with little or no modification, or can customise it to their needs and submit it for approval.

Brand Name

The organisation chooses its own brand name that can be completely independent of WISEKey. This brand name is used in the customer's certification authority, and all of the certificates that it issues.

Effective Integration

The CertifyID Trust Service has been specifically designed to interoperate with the most popular commercial operating systems, notably Microsoft Windows Server, and it takes advantage of Windows Certificate Services to provide an effective solution for global trust assurance. Organisations can integrate closely with Active Directory and their Identity and Access Management solutions thus significantly reducing the typical cost of ownership of a PKI.

About OISTE WISEKey Global Root CA



The OISTE WISEKey Global Root CA is in conformity with the Trust Services Principle(s) and Criteria established by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants for Certification Authorities, and has obtained the AICPA/CICA WebTrust Seal of Assurance.

The Trust Services Principles and Criteria is an international set of principles and criteria for systems and electronic commerce developed and managed jointly by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants. By demonstrating compliance with Trust Services criteria through an examination by an independent practitioner, entities earn the right to display the seal of assurance.

The Seal of assurance combines high standards for identified activities with the requirement for an independent verification/audit. Together they build trust and confidence among consumers and businesses conducting business over the Internet.

The **OISTE WISEKey Global Root CA** has earned the right to display the Seal of assurance with respect to the Trust Service Principle(s) of:

CERTIFICATION AUTHORITIES

The WebTrust Seal of assurance for Certification Authorities (CA) symbolizes to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria. An unqualified opinion from the practitioner indicates that such principles are being followed in conformity with the WebTrust for Certification Authorities Criteria. These principles and criteria reflect fundamental standards for the establishment and on-going operation of a Certification Authority organization or function.

CertifyID BlackBox™ components

CertifyID BlackBox is composed of a set of applications that allow the installation of an Enterprise Subordinate Certification Authority (CA) on the customer's premises.

The WISEKey CertifyID service enables customers to incorporate their certification authority (CA) into the CertifyID Trust Network. Their CA thus becomes part of the CertifyID trust community, and the end-entity digital certificates can be used within applications that trust the OISTE WISEKey Root CAs, such as Microsoft Internet Explorer 7, Microsoft Outlook 2007, Windows Vista, Windows XP, Windows Server 2000, Windows Server 2003, Macintosh OS/X and other browsers and operating systems. Using this service, organizations can federate trust between suppliers, partners and other members, by issuing interoperable CertifyID trusted certificates and thus create and extend secure relationships beyond the enterprise perimeter and enable secure communication, document signing, email and other services between enterprises.

The CA certificate is issued by Standard or Advanced WISEKey CertifyID BlackBox Policy CA, according to the CA's service class.

The CertifyID BlackBox™ contains the following material:

- CertifyID BlackBox Installer and related documents;
- CertifyID Guardian – A Windows Certificate Services exit module that enables data persistency and CA recoverability for business continuity;
- CertifyID MS CA Web Services – a Web Service API using SOAP (the Simple Object Access Protocol, that allows CertifyID BlackBox users to easily interface their CertifyID CA into their enterprise applications through a simple XML message exchange);
- CertifyID CRL Manager – designed to facilitate the publishing of Certificate Revocation Lists to publicly available web sites, which is a requirement for CertifyID CAs.
- Smart card driver software and utilities – Smartcard driver software and utilities for your bundled smartcard or secure USB token device.
- Smartcard USB Token (for the administrator's certificate)

Installation of CertifyID BlackBox™

CertifyID BlackBox™ Phase 1

The first phase of the CertifyID BlackBox™ consists of gathering information about:

- The administrator in charge for the configuration and installation of the enterprise CA
- The customer i.e. organisation that will own and manage the CA
- The type of CA that is requested:
 - Standard
 - Advanced
 - Qualified

At the end of this process, WISEKey SA staff will validate the information in order to proceed with the 2nd phase described in next section of this document.

REGISTRATION

The Registration process is needed in order to obtain a login and password for the CertifyID BlackBox™ Subscription web portal.

Launch the CertifyID Blackbox Installer and you will be taken to the Subscription Web Portal.

- Enter your email address and click 'Register'

WIS@key CertifyID

WELCOME TO THE CERTIFYID BLACK BOX SUBSCRIPTION SITE

CertifyID Subscription Logon

The WISEKey CertifyID Black Box is an Install Kit designed to simplify enterprise enrollment of the WISEKey CertifyID trust network. The software and hardware delivered with the black box will assist you to install the necessary CertifyID software components, obtain your administrator certificate, and complete the request and retrieval of the Enterprise's Certificate Authority certificate.

Phase I

Step 1. Basic Info At the end of the process the enterprise is part of the [WISEKey CertifyID Trust Network](#).

Step 2. CA Data We will now collect some basic information about you, and your enterprise, in order to validate your identity. Once this step has been completed you will be sent payment instructions and after payment we will ship your personalised CertifyID black box to you.

Step 3. Agreement

Step 4. Confirm In order to sign up for your CertifyID Black Box you need to register by providing your contact email address in the logon section below.

Phase II

Step 5. Admin certificate

Step 6. CA Audit

Step 7. CA Installation

Step 8. CA cert request

Step 9. CA activation and verification

Step 10. Success

LOGON TO THE CERTIFYID BLACK BOX SUBSCRIPTION SITE

Logon ID (Email)

Have you already registered and got your password?

Your password:

New Subscriber:

This message will appear on the screen:

Your profile is generated. Your password is sent to you by email

An email will be sent containing the logon password to the email address used above. Be sure to keep this generated password as it will be required for each logon to the Subscriber Web portal.

- Logon to the Subscriber Web portal by entering the same email address and password and click 'Logon'

ADMINISTRATOR'S CREDENTIALS

Validation of the administrator's credentials and company information is mandatory. This process is important for compliance with the CertifyID Trust Model.

The additional information section is to be used as a reminder and check list for you to acknowledge that the required documents have been prepared and are ready to be sent to WISeKey SA.

CERTIFICATION AUTHORITY DATA

Several elements are necessary to prepare the CA installation data that will be sent to WISeKey SA for verification and validation. The information entered on this page will reflect the type of CA requested and it should correspond with the name of the organisation, the internal domain and Internet domains that are used and owned by the organisation.

CERTIFYID INSTALL KIT - CA DATA

Phase I
In order to sign up for the CertifyID service, your enterprise's CertifyID Administrator must complete this form, accept the terms and conditions, and submit it to WISEkey SA.

Step 1. Basic Info
* - required field
? - recommended field

Step 2. CA Data

Step 3. Agreement

Step 4. Confirm
SERVICE CLASS [2]

Phase II
CA Service Class *

Step 5. Admin certificate
CA CERTIFICATE [2] DATA

Step 6. CA Audit
Common Name *

Step 7. CA Installation
Organisation *

Step 8. CA cert request
Dept / OU

Step 9. CA activation and verification
Locality

Step 10. Success
State

Country

OTHER REQUEST [2] DATA

CA Type *

CSP *

Hash Algorithm *

Key Length *

If you have a HSM CSP installed but not listed above please choose "Select from the installed CSPs list" option and pick up your CSP

Installed CSPs

Key Length

ORGANISATION DOMAIN [2] DATA

Domain name (internal)*

Domain name (external)

You submission status is [Basic data prepared](#)

[NEXT SCREEN](#)

Copyrights WISEkey SA, info@wisekey.ch, 2005

CA Service Class

CA Service Classes are available as follow:

- **Standard (default):** This class level enables the organisation to issue and use CertifyID chained certificates for Client Authentication to Web Sites, Digital Signature of documents and email, and encryption of email, documents and files.
- **Advanced:** This class level enables the organisation to issue and use CertifyID chained certificates for all the purposes described for Standard, plus the ability to issue SSL Server certificates for authentication of web sites, Windows SmartCard Logon Certificates. The Advanced class level also enables automatic update of certificates in the MicroSoft Exchange Address Book for easy lookup across the organisation.
- **Qualified:** Only choose this option if you're advised to do so by WISEkey or a WISEkey partner.

CA Type

Only one CA type is available:

- Enterprise Subordinate

Cryptographic Service Provider (CSP)

A variety of CSPs are available. Please choose the CSP that corresponds to your chosen Hardware Security Module (HSM).

Please note that if you are using the SPYRUS Links II USB CSP, the correct CSP to choose is "SPYRUS Hardware RSA CSP".

Hash Algorithm

Available hash algorithms are as follows:

- MD5
- SHA-1 (default and recommended)

Key Length

Two key lengths are available as follows:

- 1024 (default)
- 2048

Installed CSPs

If your CSP does not feature in the CSP drop down box, select '...' in the list and then select the correct HSM CSP in the "Installed CSP" drop down box.

Organisation Domain Data

This part has the following 2 fields:

- Domain Name Internal (Internal Namespace): The information required in this field is the Domain Name that is in use in your enterprise context i.e. by your internal enterprise domain controller.
- Domain Name External (Internet Namespace): These are the Internet Domains in use by the organisation. They should be owned by the organisation, or a letter authorising their use by the organisation should be obtained from the domain name owner.

These domain names should be entered in Internet DNS format, and if more than one is needed they should be separated by commas.

E.g. for your internal domain namespace your Root Contexts might be:-

DC=MYCOMPANY, DC=LOCAL

DC=MYCOMPANY, DC=EXTERNAL

You would then enter them as: **mycompany.local, mycompany.external**

You might own the following internet domain names: mycompany.net, and mycompany.com. You would enter these domain names in the field as: **mycompany.net, mycompany.com**


As a general rule, Microsoft recommends that you register DNS domain names for internal and external namespaces with Internet authorities. This includes the DNS names of Active Directory domains, unless such names are sub-domains of names that are registered by your organisation name, for example, "corp.example.com" is a sub-domain of "example.com". When you register DNS names with Internet authorities, it prevents possible name collisions should registration of the same DNS domain be requested by another organisation, or if your organisation merges, acquires or is acquired by another organisation that uses the same DNS names.

Important:

WiseKey SA will NOT be able to issue a CertifyID CA to an organisation that is using a DNS domain name that they do not own, regardless of whether it is for an internal or an external domain namespace.

SUBSCRIBER AGREEMENT

This Subscriber Agreement binds you to the Terms and Conditions that are in force.



CERTIFYID INSTALL KIT - SUBSCRIBER AGREEMENT

In order to sign up for the CertifyID service, you must agree to the Terms and Conditions of the CertifyID Agreement. You must complete this form, accept the terms and conditions, and submit it to WIS@key SA.

Phase I	In order to sign up for the CertifyID service, you must agree to the Terms and Conditions of the CertifyID Agreement. You must complete this form, accept the terms and conditions, and submit it to WIS@key SA.			
Step 1. Basic Info	Administrator Details			
Step 2. CA Data	First Name	John	Last Name	Doe
Step 3. Agreement	Title	Administrator	Dept	Technical
Step 4. Confirm	Email	John.Doe@mycompany.com		
Phase II	Organisation Details			
Step 5. Admin certificate	Organisation Name	MyCompany		
Step 6. CA Audit	Address	123, Street		
Step 7. CA Installation	City	Geneva	Locality	Geneva
Step 8. CA cert request	Zip	1200	Country	CH
Step 9. CA activation and verification	Phone No.	+41229295757	Fax No.	
Step 10. Success	DUNS no.			
	CA Certificate Data			
	Common Name	MyCompany CA		
	Organisation	MyCompany		
	Dept/OU	Technical		
	Dept/OU			
	Locality	Geneva	State	Geneva
	Country	CH		
	CA Service Class	Standard		
	CA Type	Enterprise subordinate CA		
	CSP	Microsoft EnhancedCryptographic Provider v1.0		
	Cert Lifetime	5	Key Length	1024
	Hash Algorithm	SHA-1 Algorithm		
	Domain name (internal)			
	Domain name (external)	mycompany.com		

After submission of your subscription request we will validate your request and identity and you will receive payment instructions.

SUBSCRIBER AGREEMENT

WISEKEY CertifyID Application Statement

Terms and Conditions
 TO REGISTER FOR THE CERTIFYID BLACKBOX PROGRAM OF WISEKEY SA, YOUR COMPANY MUST ACCEPT THE TERMS AND CONDITIONS OF THIS CERTIFYID AGREEMENT. PLEASE READ CAREFULLY. AT THE END OF THE CERTIFYID AGREEMENT SET FORTH BELOW, YOU WILL BE ASKED TO ACCEPT OR REJECT SUCH TERMS ON BEHALF OF YOUR COMPANY. BY INDICATING YOUR ACCEPTANCE, YOU SHALL REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO BIND YOUR

I agree with the subscriber agreement.

Agree and Submit

CONFIRMATION

The Confirmation page is displayed when the first phase has been completed successfully.

WIS@key
CertifyID

CERTIFYID INSTALL KIT - INITIAL SIGN UP COMPLETED

Phase I
SIGN UP COMPLETED

Step 1. Basic Info Thank you for signing up to the CertifyID service. You should receive an email message indicating that your application has been received with a summary of the information that you have presented.

Step 2. CA Data

Step 3. Agreement Please don't forget to post the photocopies of the support documents required to verify and approve your application to join the CertifyID Community. The documents that you are required to submit to us are the following:-

Step 4. Confirm

- A copy of your National ID Card, Passport, Driver's License or equivalent identification document.
- A copy of your Organisation's Certificate of Incorporation, Trade Registry Certificate, or other equivalent identification document.
- A signed and company stamped CertifyID Administrator eID End User Agreement
- A signed and company stamped letter confirming your authority to engage your organisation in the CertifyID agreement.

Please download pro-forma documents here: ProForma Documents [WORD] [PDF]

Phase II

Step 5. Admin certificate

Step 6. CA Audit

Step 7. CA Installation

Step 8. CA cert request Upon approval of your application, you will receive email notification that contains instructions on payment and invoicing. After payment you will receive your CertifyID BlackBox.

Step 9. CA activation and verification For more information and support with this process please contact:-

Step 10. Success

Validation Office
WIS@key SA
Case Postale 885
29 Rte de Pre Bois
Geneva CH-1215
Switzerland
Ph +41 22 929 5757
Fx +41 22 929 5702
deployment@wisekey.ch

Copyrights WIS@key SA, info@wisekey.ch, 2005

WIS@key will then begin the validation and verification process to confirm all of the details that you have submitted. At the end of this process you will be notified by email that you should continue with the installation process.

PREPARATION OF THE CA SERVER

You should prepare your CA server while awaiting the response from WIS@key's validation and verification department.

Core installation requirements:

- Microsoft Windows Server 2003 SP1 should be installed on hardware that meets the requirements of your Hardware Security Module.
- The server must be a member of the enterprise domain for which you will be issuing certificates.
- This server should be updated with all security patches available from Microsoft.
- Microsoft Internet Information Server must be installed along with:

- ASP.NET
- Network COM+ access
- WWW
- Active Server Pages

Other components:

- An AntiVirus software package should be installed on the server.
- An AntiSpyware package should be installed on the server.
- Optionally, an antikeylogging package can be installed on the server. (Note that certain software components such as the Smartcard drivers, and HSM drivers must be given access to intercept keyboard events).
- The Windows Firewall should be turned on and only port 80 and 443 access allowed. Remote desktop connections from the internal IT environment can also be allowed for server management.
- The Server should be configured to meet the requirements of the Security and Audit Guidelines for CertifyID Certification Authorities.

Other requirements:

The CA Server must be able to access certain web sites over the public internet for proper functioning. Please review the Appendix on Operating Requirements for more information.

CertifyID BlackBox™ Phase 2

Once your identity, and that of your organisation has been verified and validated, you will receive notification and should proceed to the CertifyID BlackBox portal from your administrator workstation (this should NOT be the CA Server) to create your administrator key pairs and obtain your administrator certificate.

ADMINISTRATOR CERTIFICATE DOWNLOAD

The administrator's certificate is available for download and installation on the hardware device (smartcard or eToken).

WIS@key
CertifyID

CERTIFYID INSTALL KIT - ADMINISTRATOR CERTIFICATE

Welcome to Phase 2 of the installation process.

Please make sure that your smartcard is inserted and is detected, that you are connected to the internet and that the SSL port 443 is open, and then click on generate to obtain your CertifyID Administrator certificate.

You need to install [CertifyID Root Certificate](#) to make CertifyID certificates chain trusted by your computer.

ADMINISTRATOR CERTIFICATE SUBSCRIBER AGREEMENT

WISEKEY CertifyID Application Statement

Terms and Conditions
TO REGISTER FOR THE CERTIFYID EID PROGRAM OF WISEKEY SA, YOUR COMPANY MUST ACCEPT THE TERMS AND CONDITIONS OF THIS CERTIFYID AGREEMENT. PLEASE READ CAREFULLY. AT THE END OF THE CERTIFYID AGREEMENT SET FORTH BELOW, YOU WILL BE ASKED TO ACCEPT OR REJECT SUCH TERMS ON BEHALF OF YOUR COMPANY. BY INDICATING YOUR ACCEPTANCE, YOU SHALL REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO BIND YOUR COMPANY AND THAT YOU, ON BEHALF OF YOUR COMPANY, HAVE READ ALL OF THE TERMS AND CONDITIONS IN THIS WISEKEY CERTIFYID AGREEMENT, UNDERSTAND THEM AND AGREE TO BE BOUND BY THEM.

I agree

You status **CA data approved**

Cryptographic Service Provider (CSP) eToken Base Cryptographic Provider

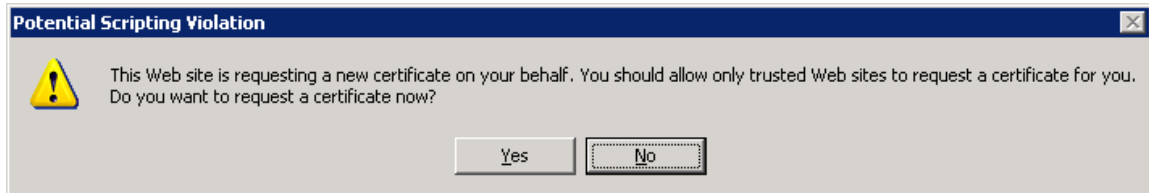
Key usage Signature and Exchange

Key Size 1024

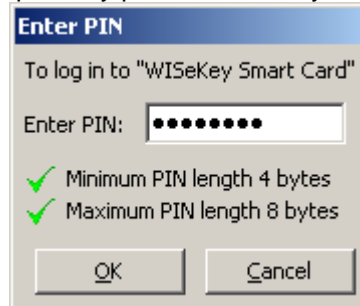
Agree and Submit

Copyrights WISEkey SA, info@wisekey.ch, 2005

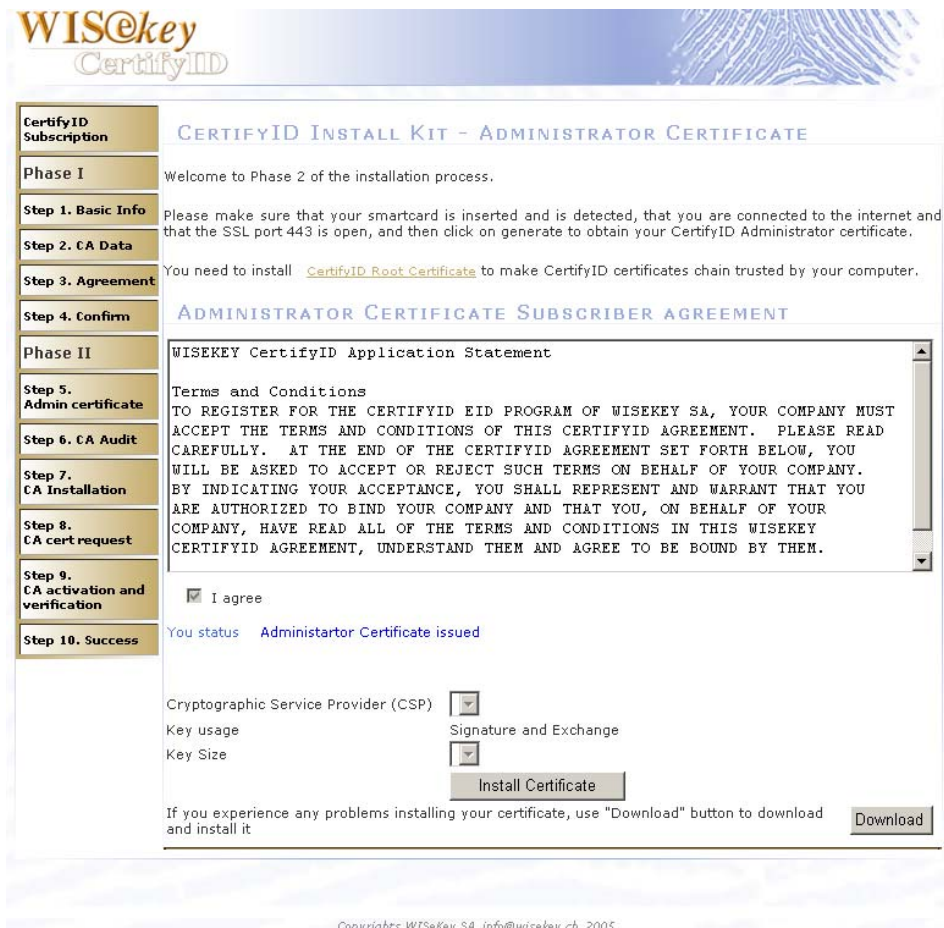
Click on "Agree and Submit" to begin the process.



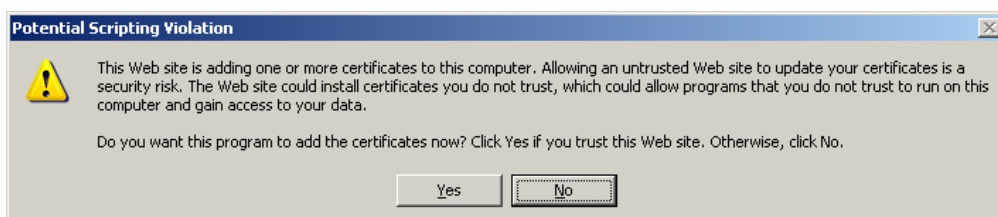
Click on yes to generate your cryptographic key pair and submit your certificate signing request.



Enter your token or smartcard PIN in order to generate the key pair.



Click on the "Install Certificate" button to install your administrator certificate.



Click “Yes” in order to add these certificates to your certificate store.

SECURITY AND AUDIT REQUIREMENTS

Please ensure that you have prepared your Certification Authority server according to the Security and Audit Guidelines before completing this step.

Complying with the security and audit requirements is mandatory. If you are a Standard customer you may receive a visit from WISEKey SA and OISTE appointed auditors. If you are an Advanced or Qualified customer then you will definitely be reviewed by WISEKey SA and OISTE auditors.

Please ensure that you follow these requirements, and have internally audited or checked their successful implementation. Please be aware that you are liable for any abuse or misuse of your CA if you do not meet these requirements.

The screenshot shows a web browser window with the following content:

- Browser Title:** CertifyID BlackBox Subscription Phase II - CA installation - Microsoft Internet Explorer
- Address Bar:** http://10.10.10.188/projects/cid/blackbox/subscribe/CAAudit.aspx?p=qpv9Yrfg8DkglWamhOp
- Page Header:** WISEKey CertifyID
- Section Title:** CERTIFYID INSTALL KIT - CA SECURITY AND AUDIT REQUIREMENTS
- Navigation Menu (Left):**
 - CertifyID Subscription
 - Phase I
 - Step 1. Basic Info
 - Step 2. CA Data
 - Step 3. Agreement
 - Step 4. Confirm
 - Phase II
 - Step 5. Admin certificate
 - Step 6. CA Audit
 - Step 7. CA Installation
 - Step 8. CA cert request
 - Step 9. CA activation and verification
 - Step 10. Success
- Main Content:**

Phase I
Integration of a Certification Authority into the MS-WISEKey Trust Infrastructure Security Requirements and Audit Guidelines
Procedure Release No. version 1.1

Information in this document is subject to change without notice and does not represent a commitment on the part of WISEKey SA (World Internet Security). WISEKey SA does not accept any responsibility for any errors that may appear in this document. No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from WISEKey SA. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of WISEKey SA. All URLs contained in this document were active at the time of product release. WISEKey SA makes no guarantee of their continued validity and takes no responsibility for their content. This document has been written and published by WISEKey SA. Copyright 2005 WISEKey SA. All Rights Reserved.

Security Requirements for Subsidiary Certification Authorities

This appendix lays out the security requirements for issuing certificates under the MS-WISEKey PKI Trust Infrastructure.

The certificates that you will issue as a MS-WISEKey Certification Authority support the authentication, privacy, data integrity, and access control functions that are critical features of your end-system application. For the certificates to serve their intended security functions within those applications, it is essential that they be issued and managed in a trustworthy fashion.

WISEKey SA has made substantial investments in the security robustness of the technology, infrastructure, facilities, personnel, and practices upon which the WISEKey PKI Hierarchy is based. Indeed, the strong inherent security of the WISEKey PKI was likely an important factor that contributed to your decision to become a sub-ordinate PKI entity of the MS-WISEKey Certification Authority as your certificate solution.

DOWNLOAD CA INSTALLATION DATA

WIS@key CertifyID

CERTIFYID INSTALL KIT - CA INSTALLATION

Phase I
Your Administrator Certificate has been downloaded and installed on the smartcard.

Step 1. Basic Info
[DOWNLOAD YOUR CUSTOMIZED INSTALLATION DATA \[?\]](#)

Step 2. CA Data

Step 3. Agreement
The CA Installer setup files have been created and should now be copied to a floppy or USB key and transferred to the CA.

Step 4. Confirm

Phase II

Step 5. Admin certificate

Step 6. CA Audit
[LAUNCH CA INSTALLER \[?\]](#)

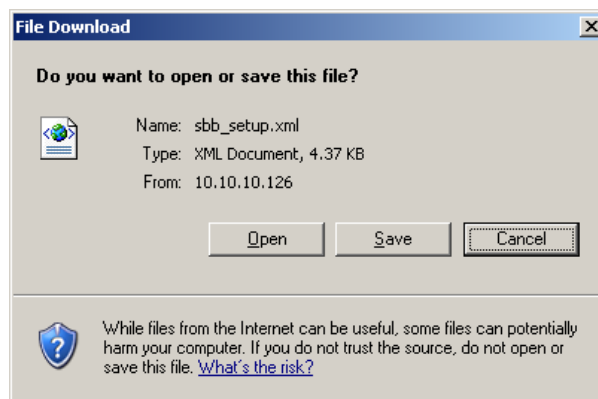
Step 7. CA Installation
Run the CertifyID installer on your Windows Certification Server computer to install your Certification Authority and generate a CA certificate request. You will need to upload generated request file to obtain your Certification Authority certificate, issued by the WISEKey CertifyID CA.

Step 8. CA cert request
[NEXT SCREEN](#)

Step 9. CA activation and verification

Step 10. Success

After completing the Audit Requirements check list you will be presented with the CA Installation Data page.

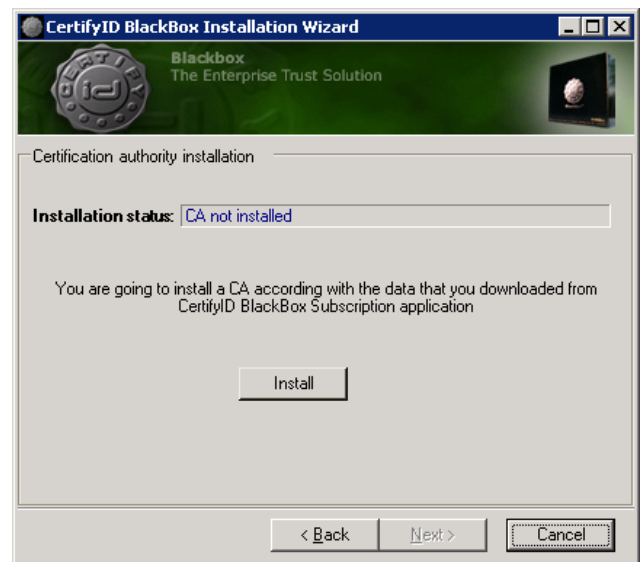
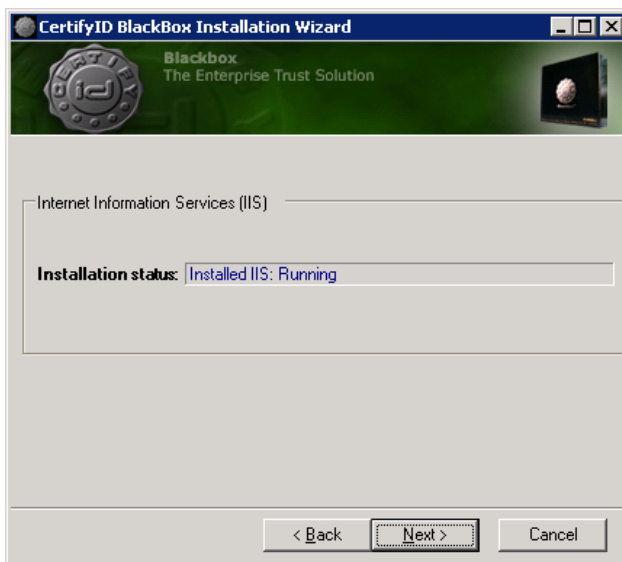
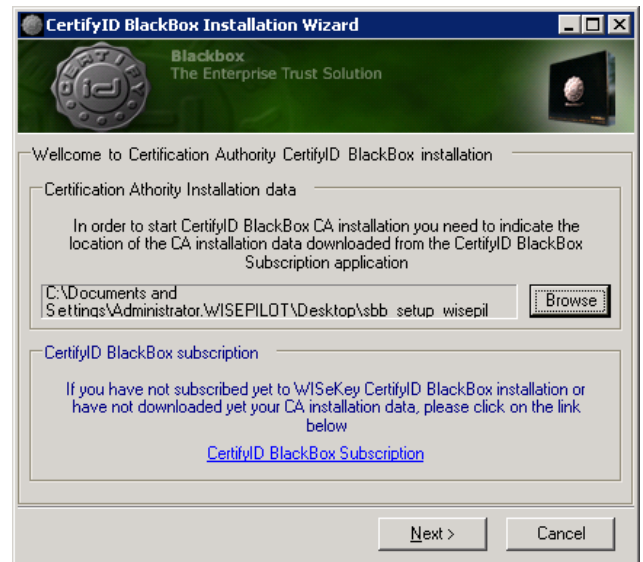
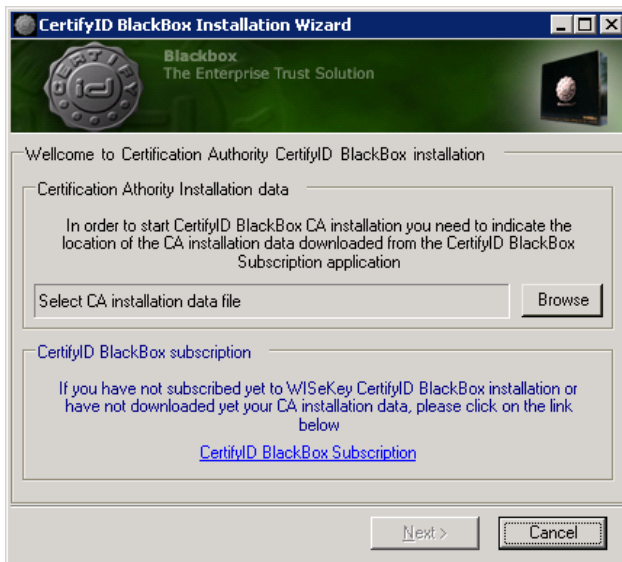


Please click on “Download CA Installation Data” and save the resulting file to a portable media for transfer to the CertifyID CA Server that you have prepared.

CERTIFYID BLACKBOX™ CA INSTALLATION

The CertifyID BlackBox CA Installer should now be installed on the CA server. Please ensure that you have set the correct time on your CA Server (GMT), and that you have a network time synchronisation to a trusted time source before conducting the CA Installation.

The CA Server should be a member of the Enterprise Domain, and it should have been named appropriately. Internet Information Services (IIS) should have been installed.

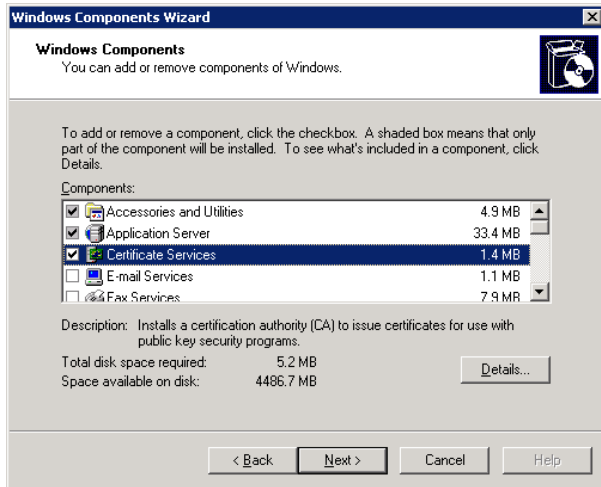


You will now receive a message from the CertifyID BlackBox Installer with detailed instructions on:

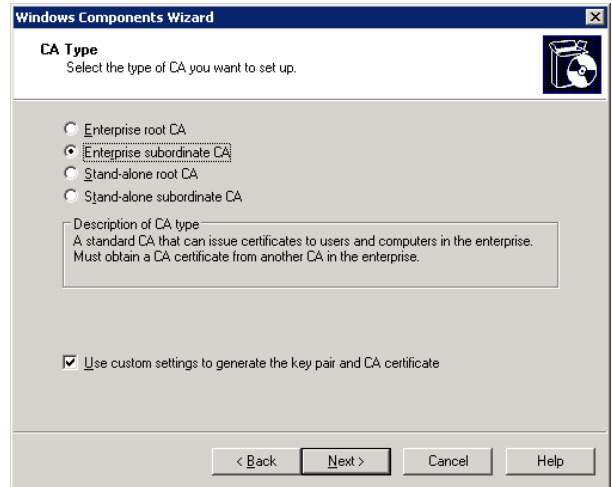
- Installing Windows Certificate Services
- Selecting your Hardware Security Module CSP, key size, and hash algorithm
- Entering your Certification Authority Naming parameters

Note: The screen shots below are examples only. Do not use the details and information they contain.

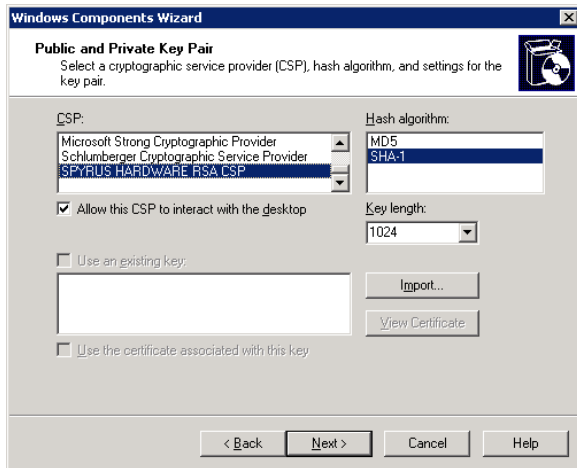
Screen 1.



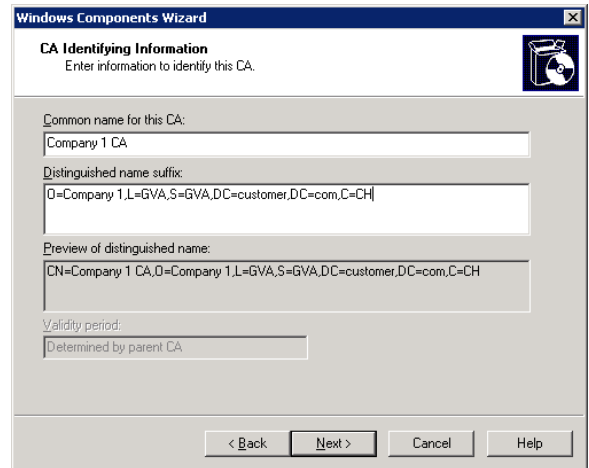
Screen 2.



Screen 3.



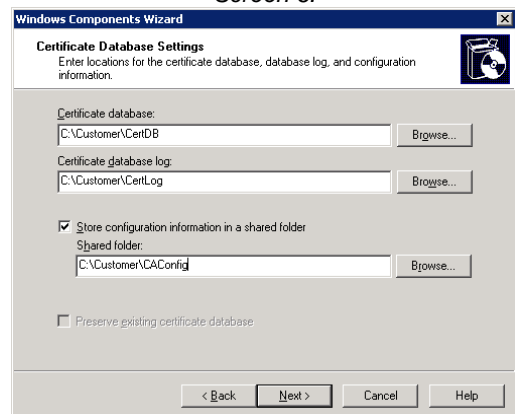
Screen 4.



Screen 5.



Screen 6.

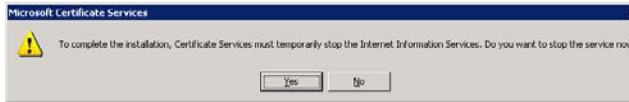


Screen 7.

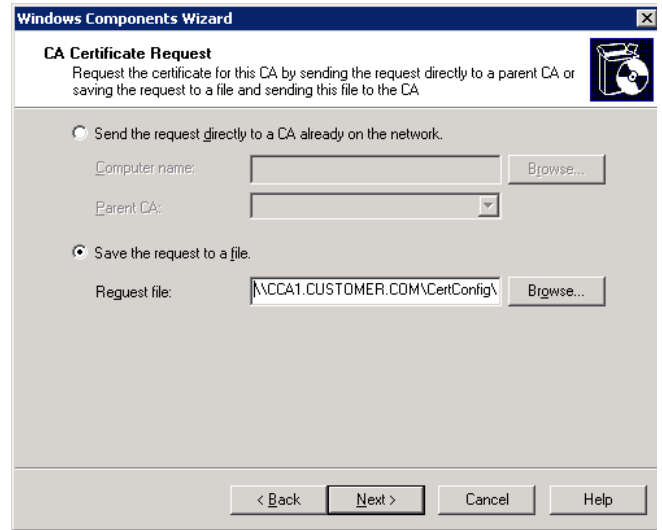
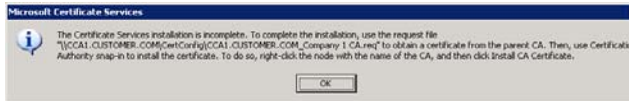
Screen 8.



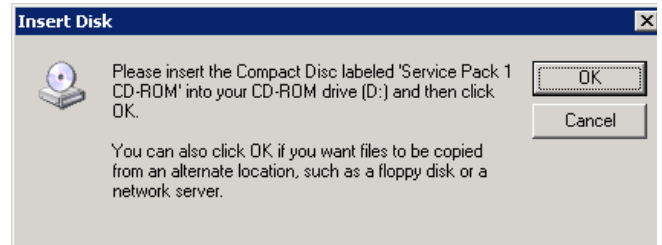
Screen 9.



Screen 11.

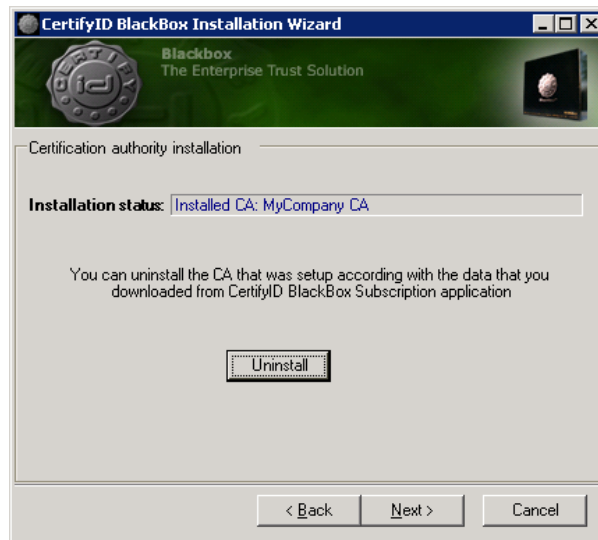


Screen 10.



Screen 12.





The above message will appear after you have completed the Certification Services installation.

Click on the “Next” button.

UPLOAD CA_AUDIT FILE

A CA_audit file has been automatically generated by the application and is stored in the same folder where you saved the CA_data XML file. Browse and upload the file in the corresponding field of the Subscriber portal.

UPLOAD CA CERTIFICATE REQUEST FILE

You should now upload your Certification Authority's Certificate request file to the subscription portal. This file with the extension “.req” is located in the CA Config subfolder that you created earlier during the CA installation process.

Your request file will be checked and if all attributes are verified correctly, your CA certificate will be issued by WISEkey, and you will receive confirmation via email.

DOWNLOAD CA CERTIFICATE

After receiving the email confirmation that your CA certificate has been issued, please proceed to WISEKey's CertifyID BlackBox subscription portal to download your CA certificate.

Note: Please define your CRL and AIA Locations before installing your CA Certificate.

CDP and AIA Locations Configuration

The CRL Distribution Points (CDP) and Authority Information Access (AIA) are vital for the usage of certificates. These access points must be available internally and externally for verification of Parent CA Certificates and Certificate Revocation List.

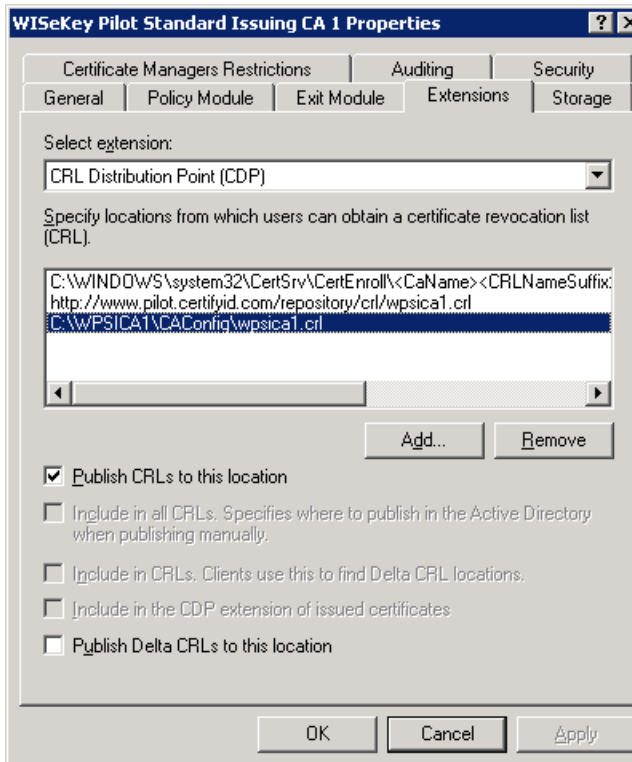
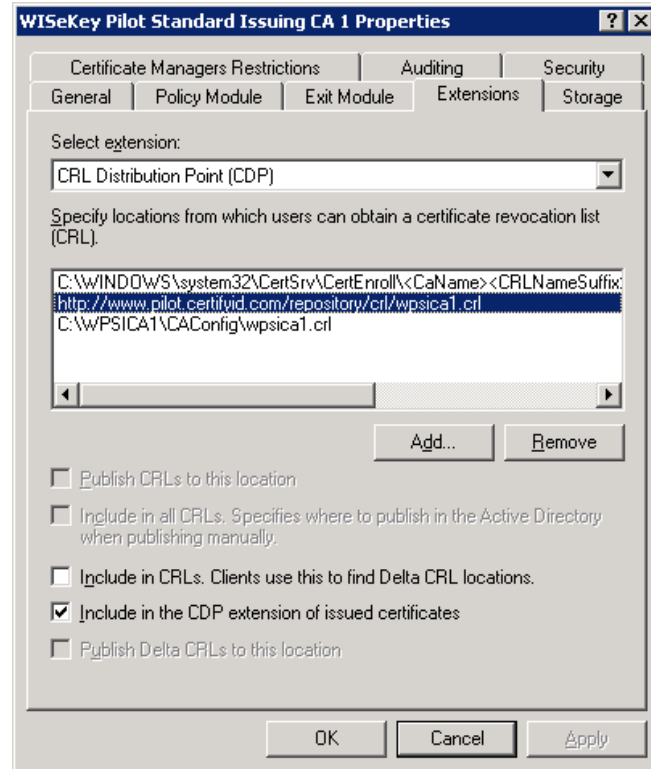
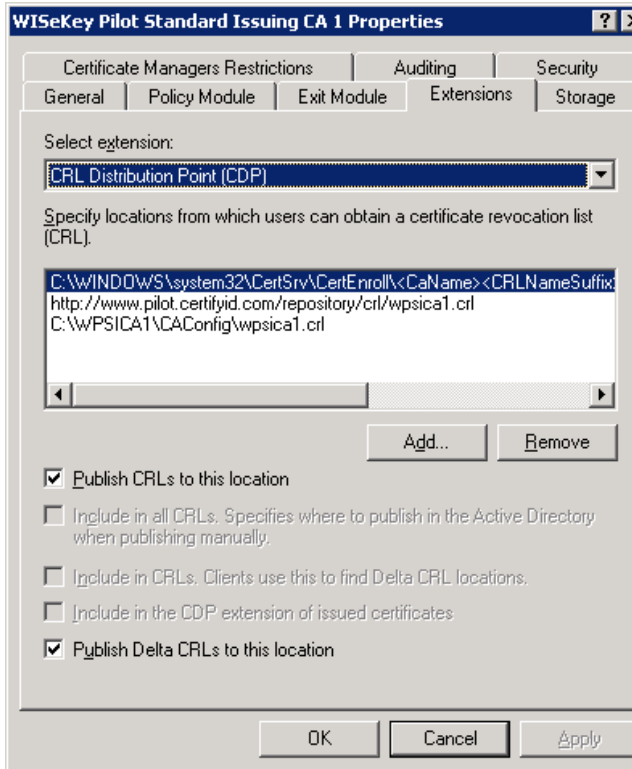
CRL files are the most critical as if they are not available the certificates will not be able to be used. All revoked certificates are listed in these files and they are checked each time a certificate is used.

Before installing your CA certificate, you should define your CDP locations and AIA locations in the Certification Services Management Console.

DEFINING YOUR CDP LOCATIONS

You must choose a publicly available internet URL for your CRL locations. We recommend that you create an HTTP location. It must NOT be an HTTPS or LDAPS location.

The first line containing the C:\Windows\system32\... path must be kept as it is and the other lines need to be deleted by clicking on the “Remove” button. To add entries, click on the “Add” button and enter the corresponding information related to your configuration.



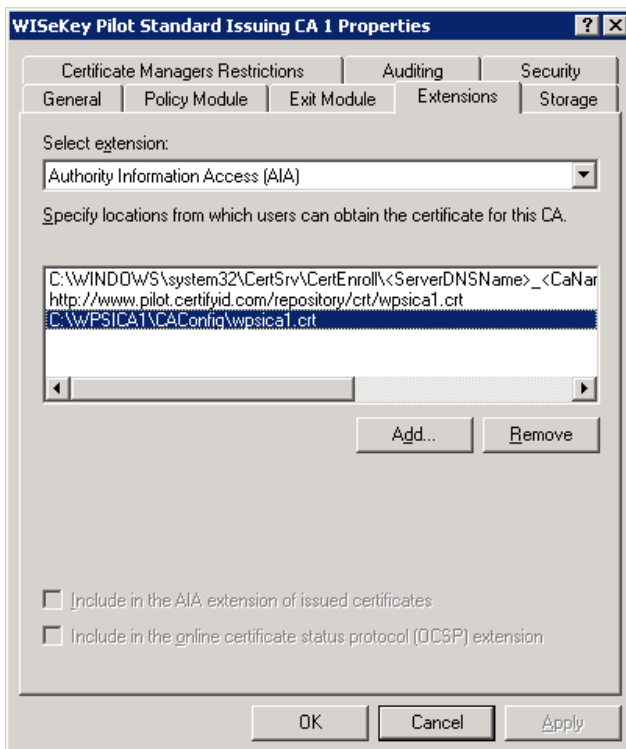
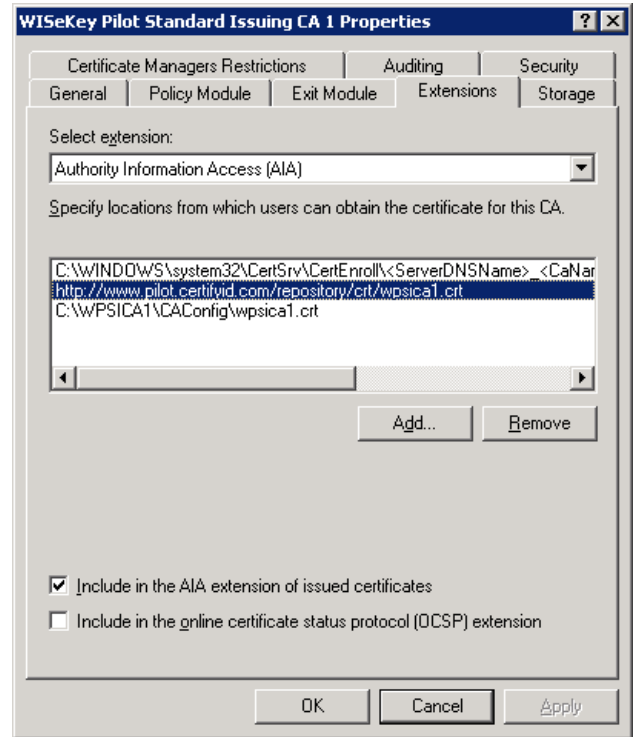
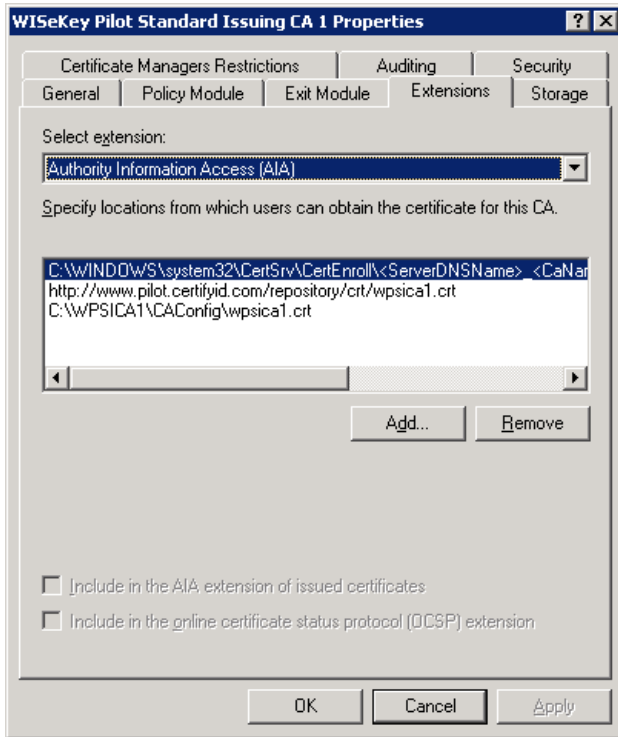
The local storage of the CA CRL is optional

Note: These screen shots are examples only. Do not use the details and information they contain. Only configure the check boxes as shown.

DEFINING YOUR AIA LOCATIONS

You must choose a publicly available internet URL for your AIA locations. We recommend that you create an HTTP location.

The first line containing the C:\Windows\system32\... path must be kept as it is and the other lines need to be deleted by clicking on the “Remove” button. To add entries, click on the “Add” button and enter the corresponding information related to your configuration.



The local storage of the CA certificate is optional

Note: These screen shots are examples only. Do not use the details and information they contain. Only configure the check boxes as shown.

Install your CA Certificate

The following steps should be done on the CA Server as a user logged on with administrative rights.

TEST ACCESS TO WISEKEY CRL AND AIA LOCATIONS

Ensure that you can browse the following web sites from internet explorer on the CA Server:-

<http://public.wisekey.com/crl>
<http://public.wisekey.com/crt>

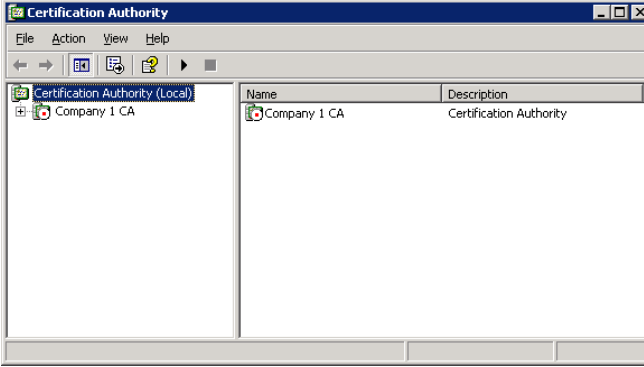
Also ensure that this site: <http://public.wisekey.com> is in Internet Explorer's Trusted Sites list. This is required to allow your CA server to download the CRL and CRT files of the Root and Policy CA to the CA Server, which is required for the operation of your Certification Authority.

START THE CA SERVICE

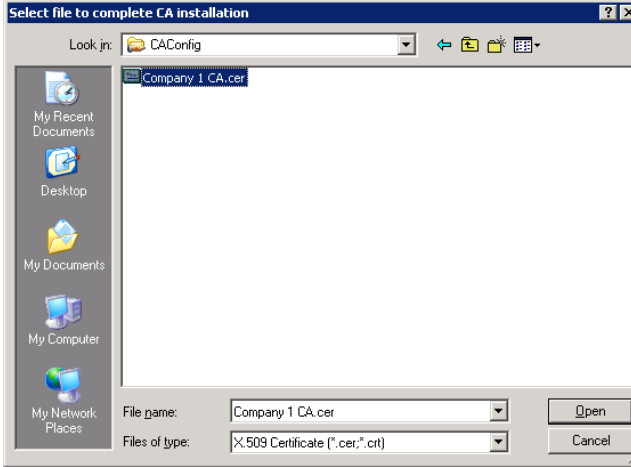
In order to start the CA service, you need to first install the CA Certificate.

INSTALL THE CA CERTIFICATE

Screen 1.



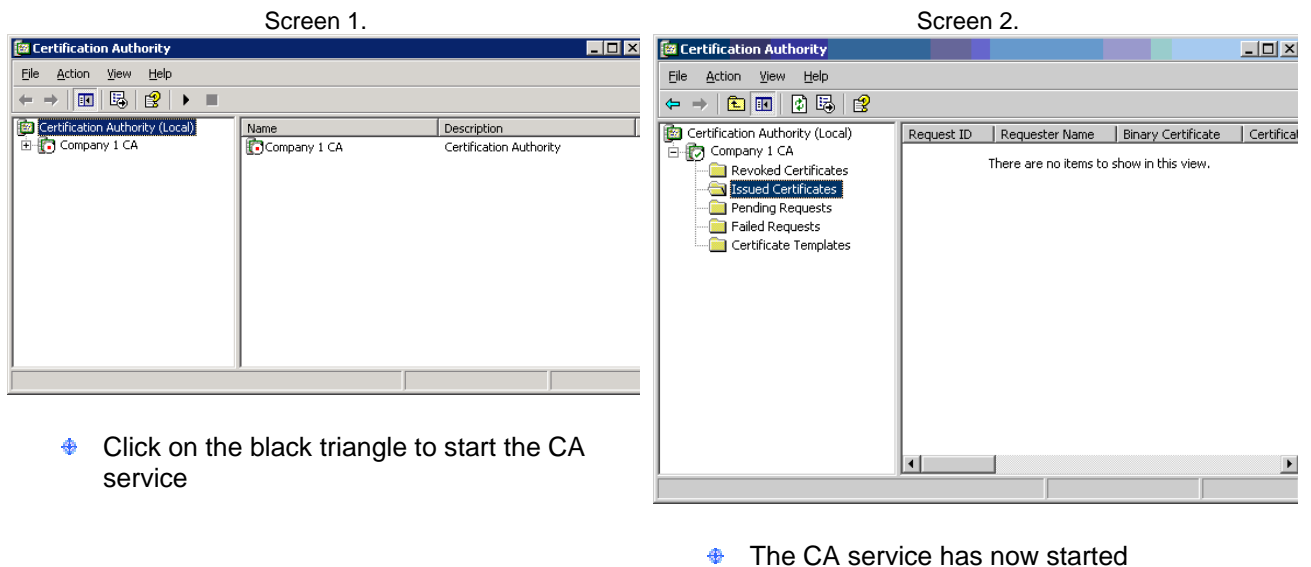
Screen 2.



- ✦ Right click on the CA name
- ✦ Select "All tasks"
- ✦ Select "Install Certificate"

- ✦ Chose the CA certificate
- ✦ Click on "Open"

START THE CA SERVICE



PUBLISH YOUR CA CERTIFICATE TO THE AIA LOCATION

Please copy your CA certificate to the external AIA URL location.

SETUP CRL PUBLISHING

Create a batch job to copy the CRL to appropriate directory on the external web server. WISEKey CRL Manager may also be used to do automated CRL fetching, and checking. The setup of WISEKey CRL Manager is described in its accompanying documentation.

TEST THE CDP LOCATIONS

Please test the HTTP CDP location after installing your Certification Authority by using an Internet browser.

TEST THE AIA LOCATIONS

Please test the HTTP AIA location after installing your Certification Authority by using an Internet browser.

Proxy settings

In some cases, a proxy server is configured within the network environment. All proxy settings must be configured in the Internet Explorer of the Certification authority and imported to the WinHTTP settings by using the following command:

```
C:\proxycfg -u
```

Provision user certificates

Your Microsoft CA Server is now set up and ready for use within the WISEKey OISTE Global Trust Network, although you may continue to modify your certificate profile configuration according to local business or legislative requirements. The Microsoft publication Microsoft Windows Server(TM) 2003 PKI and Certificate Security is a good reference.

Conclusion

This solution has demonstrated how to install Microsoft Windows CA Server with WISEKey CertifyID BlackBox. This combination provides:

- Extensible robust enterprise-integrable PKI infrastructure
- Externally-trusted individual email (client) and SSL server digital certificates
- Plug and play with existing Microsoft infrastructure and applications
- Integration with identity management platforms and other third-party software
- World class support from Microsoft and WISEKey

For more information on how to cost effectively implement your globally trusted and interoperable public key infrastructure and certificate authority please contact:-

WISEKey SA
29 Rte de Pré Bois
Geneva 1215
Switzerland
e-mail : info@wisekey.com
Tel: +41 22 594 3000
Fax: +41 22 594 3001
<http://www.wisekey.com>