



**European Commission – DG Enterprise**

**IDA PKI**

**European IDA Bridge and Gateway CA  
Pilot**

**WP 1.2 - doc5 - Test Programme**

***Certipost n.v./s.a.***

***Muntcentrum 1***

***B-1000 Brussels***

***Belgium***



*Disclaimer*

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission. The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof. Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission. All care has been taken by the author to ensure that he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from his or their legal representative.

## 1. Executive Summary.

This document is part of Work Package 1.2 of the Bridge and Gateway CA Pilot project of the IDA PKI.

This document explains the test program to be executed within the framework of the European IDA Bridge and Gateway CA Pilot.

The first section is an introduction explaining the background and requirements for the test programme.

The second section details the technical infrastructure that will be used for executing the test programme.

The third section describes the complete test programme.

In annex, detailed test scripts and a reporting template is available.

## 2. Table of Contents

1.	Executive Summary.....	3
2.	Table of Contents.....	4
3.	Introduction .....	5
3.1.	Test programme.....	5
3.2.	How to join the interoperability test programme .....	6
4.	Test Bed.....	7
4.1.	Requirements.....	7
4.2.	Test Bed Architecture.....	7
4.2.1.	Overview.....	7
4.3.	Access to the EBGCA Pilot Test Bed.....	8
5.	Test Programme.....	9
5.1.	Overview.....	9
5.1.1.	Functionality Test.....	9
5.1.2.	Interoperability Test.....	9
5.1.3.	Excluded from testing.....	9
5.1.4.	Validation.....	10
5.2.	Functionality Test Programme.....	10
5.3.	Interoperability Test Programme.....	11
5.4.	Member State Test Programme.....	12
	ANNEX I - Test Scripts.....	13
	ANNEX II - Reporting Template.....	28
	ANNEX III – Sample Completed Report .....	29

## 3. Introduction

### 3.1. Test programme

The main objective of the EBGCA pilot is to be able to perform a technical test of the Bridge and Gateway CA concept. This technical test will be executed in the form of an elaborate test programme.

The EBGCA Test programme constitutes of three test plans.

#### 1. Functionality Test.

The purpose of the first test plan is to assure that “the mechanics work”, in particular the technical steps around the “Trust List” issuance process (issue Trust List, import Trust List in applications, etc...)

The Bridge and Gateway CA Service Provider will perform this first test plan in order to validate the required functionality by the EBGCA Pilot infrastructure.

These tests will be executed on the EBGCA Pilot Platform. The architecture of the EBGCA Pilot Platform is described in detail in WP1.2 document #4 – Technical Architecture.

#### 2. Interoperability Test.

The purpose of the second test plan is to validate the use of Trust Lists in the real life. The member states as Bridge and Gateway CA participants will use the Trust List in communications secured by Certificates, via the test bed. Here the test bed plays the role that the IDA network would fulfil in reality.

The EBGCA Pilot Participants will perform this second test plan. The Service Provider will provide the required infrastructure, and assist the participants to actually perform these tests.

These tests will be executed on the Bridge and Gateway CA Test Platform. This is a dedicated Test platform that will be set up for the Bridge and Gateway CA Pilot. This test bed is described in detail in the next chapter.

#### 3. Member Test.

In a third test plan, the member states can execute tests amongst each other.

This test plan will not be guided by the EBGCA, but the participants are free to organise these tests amongst themselves.

These tests will be executed on the EBGCA Test Platform.

### **3.2. How to join the interoperability test programme**

#### **Applying for the interoperability test**

Before starting the interoperability test, the participant should have signed up for participation in the European IDA Bridge and Gateway CA Pilot by signing off the **participation form** where conditions and basic information is provided.

The European Commission will send this participation form towards all Member States during the fourth quarter of 2004 in order to obtain the official subscription for participating in the EBGCA Pilot.

In order to start with the test programme, the Bridge and Gateway CA service provider should be contacted.

European IDA Bridge and Gateway CA Pilot  
Certipost E-Trust  
Muntcentrum 1  
B-1000 Brussel  
[ebgca@e-trust.be](mailto:ebgca@e-trust.be)

Please be ready to provide following details

- Name of Technical Contact Person (for test phase) + Contact details
- Technical information, IP addresses, DNS Names, ...

When contacting the Bridge and Gateway CA Service Provider, you will make an appointment of when you will perform the interoperability tests, i.e. start of the testing process, and scheduled duration.

#### **Performing the test steps**

The participant is at liberty to proceed with the test steps at his convenience.

For those parts of the tests that are performed together with the Bridge and Gateway CA Service provider, make sure that test are performed in sync (via email for example).

#### **Reporting Guidelines**

When performing the Interoperability test, the standard "Test Report Template" should be completed detailing the results of the tests.

The completed "Test Report" should be submitted to the IDA Project Management and forms an integral part of the Bridge and Gateway CA pilot project.

## 4. Test Bed

This section contains a high level description of what constitutes the test bed and how to interoperate with it.

A detailed technical description of the test bed is provided in the document “**Technical Architecture**”.

### 4.1. Requirements

The Test Bed should provide following functionality.

- **Test Environment**  
 Provide realistic testing environment for participants in the Pilot.
- **Reference implementation**  
 Provide reference implementation of a “Virtual DG”, i.e. a set up giving an example of how to interface with the Bridge and Gateway CA Pilot, and how to set up secure communications making use of certificates issued by CA’s participating in the pilot.
- **Allow to execute the test plan**  
 The test platform should enable all participants to execute every test mentioned in the test plan.

### 4.2. Test Bed Architecture

#### 4.2.1. Overview

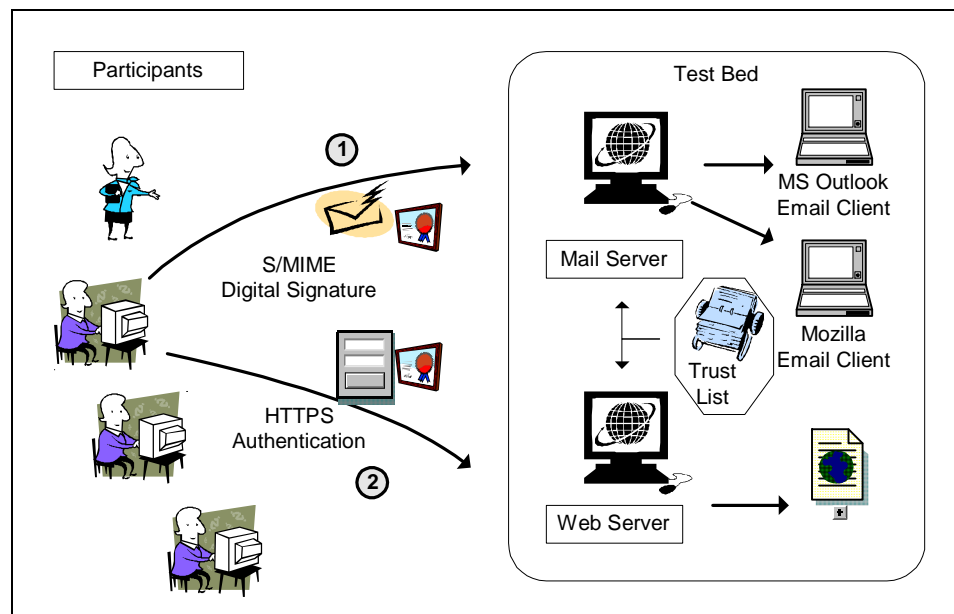


Figure 1 - Test Bed Conceptual Overview

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

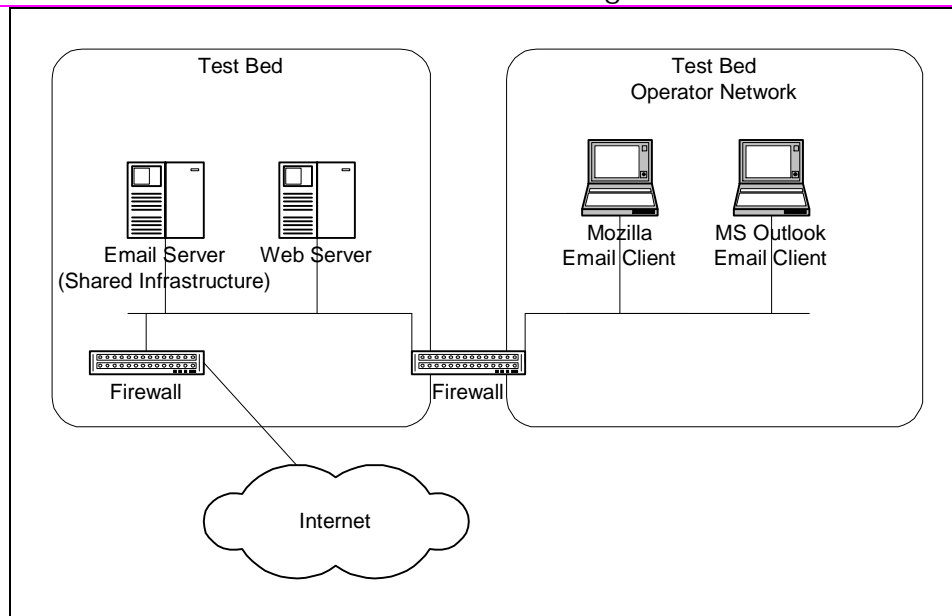


Figure 2 - Test Bed Technical Overview

### 4.3. Access to the EBGCA Pilot Test Bed

On the Bridge and Gateway CA Pilot test bed, following addresses are known.

#### Email Addresses

Email address	purpose
<a href="mailto:ebgca@e-trust.be">ebgca@e-trust.be</a>	General contact address for EBGCA Pilot
<a href="mailto:ebgca-enroll@e-trust.be">ebgca-enroll@e-trust.be</a>	in order to enrol on the EBGCA Pilot
<a href="mailto:ebgca-subscribe@e-trust.be">ebgca-subscribe@e-trust.be</a>	in order to subscribe to the mailing list
<a href="mailto:ebgca-list@e-trust.be">ebgca-list@e-trust.be</a>	the mailing list itself
<a href="mailto:ebgca-test1@e-trust.be">ebgca-test1@e-trust.be</a> <a href="mailto:ebgca-test2@e-trust.be">ebgca-test2@e-trust.be</a>	email test clients (MS Outlook, Mozilla)

#### Web Pages

URL	purpose
<a href="http://ebgca.e-trust.be/">http://ebgca.e-trust.be/</a>	European IDA Bridge and Gateway CA Pilot - main page
<a href="http://ebgca.e-trust.be/trustlist">http://ebgca.e-trust.be/trustlist</a>	Trust List Files
<a href="http://ebgca.e-trust.be/participants">http://ebgca.e-trust.be/participants</a>	List of participants
<a href="http://ebgca.e-trust.be/testplan">http://ebgca.e-trust.be/testplan</a>	Test Plan

## 5. Test Programme

### 5.1. Overview

#### 5.1.1. Functionality Test

The functionality Test will test following basic Trust List Functionality, and actions of the Bridge and Gateway CA

- Issue a Trust List
- List the contents of a Trust List
- Add a CA Certificate to the Trust List
- Remove a CA Certificate from the Trust List
- Validate the signature of the Trust List

#### 5.1.2. Interoperability Test

The functionality Test will test following actions of the Participant CA

- Join the Bridge and Gateway CA Pilot
- Import the "Trust List" into an application (Outlook, Mozilla)
- Communicate via S/MIME message to the test bed
- Log on to Test Bed web site using certificate
- Re-Sign and publish the Trust List

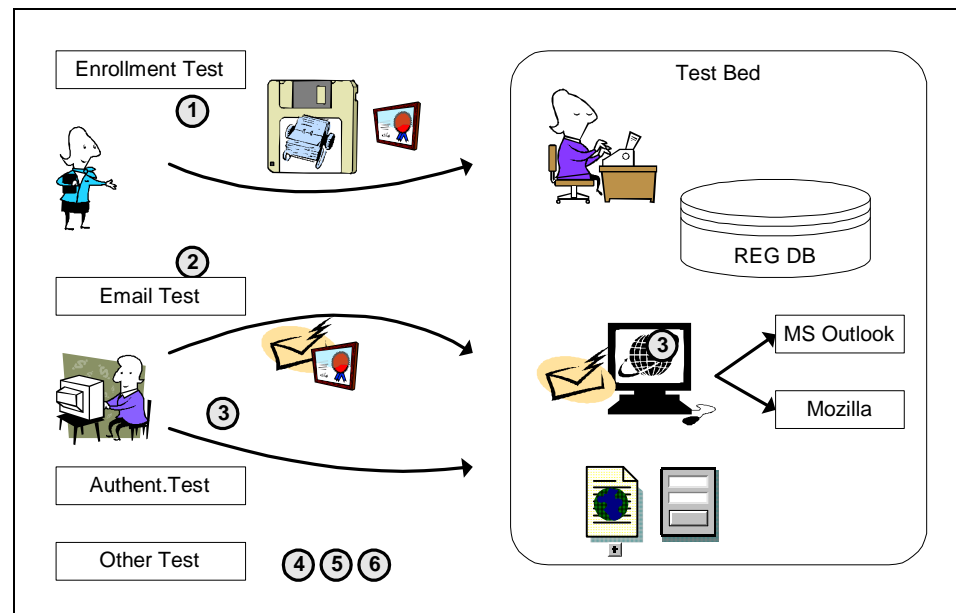


Figure 3 – Interoperability Test

#### 5.1.3. Excluded from testing.

The Bridge and Gateway CA Pilot is a first pilot for experimenting with Bridge CA / Gateway CA functionality across public administration within the European Community. As such only the basic functionality will be tested in a first stage. Advanced functionality may be tested in a later stage in a late phase of the project.

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

Following functionality is not within the scope of the Bridge and Gateway CA pilot, and will not be tested.

- Retrieval of certificates from Directory, retrieval of CRL's from directory
- Common gateway for online certificate status checking
- Directory services
- Etc...

#### 5.1.4. Validation

In General, the validation of a certificate requires checking the status of the certificate. Usually this is performed via a downloaded file, a CRL (Certificate Revocation List) or an on-line service (OCSP – Online Certificate Status Protocol).

The exact procedure to verify a certificate status however depends on the certification authority that issued the certificate, and the corresponding certificates provided. In addition the configuration of such a status check depends on the application used. As such, no general description can be provided, but one has to rely on documentation provided by the Certification Authority that issued the certificate.

As the validation of a certificate is actually an important step, it is also included in the test scripts. However, a generic description is provided for the “validation” step. The user should in every case verify the recommended procedure for certificate status validation.

In the case of the certificates issued by the Bridge CA Root CA (used for example to issue the certificate signing the Bridge CA “Trust List”), the validation will require checking a CRL, that can be downloaded from the Bridge and Gateway CA Pilot Web Site.

### 5.2. Functionality Test Programme

Test Nr.	Description	Goal
1.1	Issue Trust List	Validate that it is possible to create / publish a Trust List. <ul style="list-style-type: none"> <li>• Issue “Trust List” File</li> <li>• Publish “Trust List” File</li> </ul>
1.2	Validate “Trust List” correctness	Check whether it is possible to manually check the trust list file, check the content as well as the validity. <ul style="list-style-type: none"> <li>• List “Trust List” File contents</li> <li>• Validate Signature on “Trust List” File</li> <li>• Validate the Certificate status of the Certificate used to sign the “Trust List” File</li> </ul>
1.3	Add new CA to the “Trust List”	Validate the functionality when a Certification Authority joins the Bridge and Gateway CA Pilot. <ul style="list-style-type: none"> <li>• Add CA Certificate to the “Trust List” file.</li> <li>• Sign “Trust List” file again.</li> </ul>
1.4	Remove CA from the “Trust List”	Validate the functionality when a Certification Authority leaves the Bridge and Gateway CA Pilot. <ul style="list-style-type: none"> <li>• Remove CA Certificate to the “Trust List” file.</li> <li>• Sign “Trust List” file again.</li> </ul>

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

1.5	Import in Internet Explorer	<p>Validate the compatibility of the "Trust List" with internet explorer.</p> <ul style="list-style-type: none"> <li>• Import all the certificates from the "Trust List" file into Internet Explorer.</li> </ul>
1.6	Import in MS Outlook	<p>Validate the compatibility of the "Trust List" with MS Outlook.</p> <ul style="list-style-type: none"> <li>• Import all the certificates from the "Trust List" file into MS Outlook.</li> </ul>
1.7	Import in Mozilla	<p>Validate the compatibility of the "Trust List" with Mozilla.</p> <ul style="list-style-type: none"> <li>• Import all the certificates from the "Trust List" file into Mozilla.</li> </ul>

### 5.3. Interoperability Test Programme

Test Nr.	Description	Goal
2.1	Enrollment Test	Test technical infrastructure of participating CA for compliance with Bridge and Gateway CA
2.2	Import in Internet Explorer	<p>Validate the compatibility of the "Trust List" with internet explorer.</p> <ul style="list-style-type: none"> <li>• Import all the certificates from the "Trust List" file into Internet Explorer.</li> </ul>
2.3	Import in MS Outlook	<p>Validate the compatibility of the "Trust List" with MS Outlook.</p> <ul style="list-style-type: none"> <li>• Import all the certificates from the "Trust List" file into MS Outlook.</li> </ul>
2.4	Import in Mozilla	<p>Validate the compatibility of the "Trust List" with Mozilla.</p> <ul style="list-style-type: none"> <li>• Import all the certificates from the "Trust List" file into Mozilla.</li> </ul>
2.5	Email Test	Test for recognising certificates by participants of the Bridge and Gateway CA Pilot in email communication.
2.6	Authentication Test	Test for recognition of certificates by participants of the Bridge and Gateway CA Pilot in SSL Client Authentication.
2.7	Trust List Sign Test	Test for re-signing of the "Trust List" by a participant, and publishing of this re-signed trust list.

#### **5.4. Member State Test Programme**

In the "Member State" test programme, any participant can perform interoperability tests with other participants. These tests will not be guided and managed by the Bridge and Gateway CA service provider, but are optional for all participants.

The test scripts form the "Interoperability Test Programme" can be taken as a guideline for planning the test that the member states wish to plan amongst themselves.

##### Possible Basic Test Program between participants:

A suggestion for tests that can be performed at least between the member states:

Email Test	Test for recognising certificates by participants of the Bridge and Gateway CA Pilot in e-mail communication.
Authentication Test	Test for recognition of certificates by participants of the Bridge and Gateway CA Pilot in SSL Client Authentication.

Indicative scripts can be found in below Annex I (where it is clear that these tests will not be guided and managed by the Bridge and Gateway CA service provider).

## ANNEX I - Test Scripts

### 1.1 Issue Trust List

**GOAL:** Validate that it is possible to create and publish "Trust list" files.

The first test constitutes of a series of tests to verify whether the Bridge and Gateway CA to correctly product a "Trust List" (TSL File, "Trust Status Provider Status List" – ETSI standardised file format).

#### Test Prerequisites

Bridge and Gateway CA Pilot Infrastructure should be operational.

- Public Web Site
- Repository for "Trust List" files

Test Step Nr	Test Step	Actions
1	Create "Trust List"	Create the "Trust List" file that will be distributed, using the provided tool (see EBGCA Technical Architecture).
2	Publish "Trust List"	Publish the "Trust List" file on the Bridge and Gateway CA Pilot Web Site. <a href="http://ebgca.e-trust.be/trustlist">http://ebgca.e-trust.be/trustlist</a>  Update the list of participants on the Bridge and Gateway CA Pilot Web Site. <a href="http://ebgca.e-trust.be/participants">http://ebgca.e-trust.be/participants</a>
3	Validate "Trust List" is published	Download the "Trust List" file from the web site <a href="http://ebgca.e-trust.be/trustlist">http://ebgca.e-trust.be/trustlist</a>  Check this file: <ul style="list-style-type: none"> <li>• Check that the file can be downloaded from the Trust List Web Site.</li> <li>• Check the date.</li> <li>• Check whether the file is the correct one.</li> <li>• Check the file with the tool in order to check the contents of the file</li> <li>• Check the contents <ul style="list-style-type: none"> <li>○ Certificates</li> </ul> </li> <li>•</li> </ul>

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

**1.2 Validate Trust List**

**GOAL:** Check whether it is possible to manually check the trust list file, check the content as well as the validity.

**Test Prerequisites**

- Bridge and Gateway CA Pilot Infrastructure should be operational.
- Test 1.1 should be done successfully : A First "Trust List" File should have been generated

Test Step Nr	Test Step	Actions
1	Check Trust List Contents	<p>Goal: Validate that the Trust list can be read</p> <p>Actions:</p> <ul style="list-style-type: none"> <li>• Extract list of certificates from Trust List</li> <li>• Extract every certificate on the Trust List individually</li> </ul>
2	Check Trust List Signature	<p>Goal: Check that the signature can be properly validated</p> <p>Actions:</p> <ul style="list-style-type: none"> <li>• Validate Signature is correct</li> <li>• Validate Signature is made by "Trust List Signing Certificate"</li> </ul>
3	Validate Trust List Signing Certificate Status	<p>Goal: Check that the certificate used to generate the signature can be properly validated</p> <p>Actions:</p> <ul style="list-style-type: none"> <li>• Download the CRL from the Bridge and Gateway CA Pilot Web Site. <a href="http://ebgca.e-trust.be/trustlist">http://ebgca.e-trust.be/trustlist</a></li> <li>• Validate the Certificate status of the "Trust List Signing Certificate" by verifying the CRL manually.</li> </ul>
4	Validate Trust List Content.	<p>Goal: Validate that the Trust list is complete</p> <p>Actions:</p> <ul style="list-style-type: none"> <li>• Compare Trust List Content with list of participants on the web site.</li> </ul>

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

**1.3 Add new CA to the “Trust List”**

**GOAL:** Validate the functionality when a Certification Authority joins the Bridge and Gateway CA Pilot.

**Test Prerequisites**

- Bridge and Gateway CA Pilot Infrastructure should be operational.
- Test 1.1 and 1.2 should be done successfully: A First “Trust List” File should have been generated, and validated.

Test Step Nr	Test Step	Actions
1	Upload new CA Certificate	Send a new CA Certificate to the Bridge and Gateway CA  Send the certificate via email to ebgca-enroll@e-trust.be
2	Validate new CA Certificate in Trust List	Check Certificate Fingerprint  Fingerprint of the received certificate should match the fingerprint published by the CA.
3	Add new CA Certificate to Trust List	Include new CA Name in list of CA's (database) <ul style="list-style-type: none"> <li>• Participant</li> <li>• CA Name</li> <li>• Certificate Fingerprint</li> <li>• Certificate</li> </ul>
4	Include new CA Certificate in Trust List	Create New “Trust List” File (see EBGCA Architecture)
5	Publish new Trust List	Publish “Trust List” File (see EBGCA Architecture)
6	Validate Trust List	Validate Published “Trust List” File <ul style="list-style-type: none"> <li>• List of CA's should be updated and contain new CA Certificate.</li> <li>• New Certificate should have been included.</li> </ul> Validate published list of participants

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

**1.4 Remove CA from the "Trust List"**

**GOAL:** Validate the functionality when a Certification Authority leaves the Bridge and Gateway CA Pilot.

**Test Prerequisites**

- Bridge and Gateway CA Pilot Infrastructure should be operational.
- Test 1.1 and 1.2 should be done successfully: A First "Trust List" File should have been generated, and validated.

Test Step Nr	Test Step	Actions
1	Remove CA Certificate	Remove a certain CA certificate from the list of list of CA's (database) <ul style="list-style-type: none"> <li>• Participant</li> <li>• CA Name</li> <li>• Certificate Fingerprint</li> <li>• Certificate</li> </ul>
2	Update Trust List	Create New "Trust List" File (see EBGCA Architecture)
3	Publish Trust List	Publish "Trust List" File (see EBGCA Architecture)
4	Validate Trust List	Validate Published "Trust List" File <ul style="list-style-type: none"> <li>• List of CA's should be updated and contain new CA Certificate.</li> <li>• New Certificate should have been included.</li> </ul> Validate published list of participants

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

**1.5 Import in Internet Explorer**

**GOAL:** Validate the compatibility of the "Trust List" with Internet explorer.

**Test Prerequisites**

- Bridge and Gateway CA Pilot Infrastructure should be operational.
- Test 1.1 and 1.2 should be done successfully: A First "Trust List" File should have been generated, and validated.

<b>Test Step Nr</b>	<b>Test Step</b>	<b>Actions</b>
1	Preparations	Clean Internet Explorer Certificate Store
2	Get new trust list	Download "Trust List" file From Web Site
3	Import Into Internet Explorer	Extract all certificates into folder Import manually every certificate into Internet Explorer
4	Validate Certificate Store	Check list of Root Certificate in Internet Explorer. Check certificate Fingerprints

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

**1.6 Import in MS Outlook**

**GOAL:** Validate the compatibility of the "Trust List" with MS Outlook.

**Test Prerequisites**

- Bridge and Gateway CA Pilot Infrastructure should be operational.
- Test 1.1 and 1.2 should be done successfully: A First "Trust List" File should have been generated, and validated.

<b>Test Step Nr</b>	<b>Test Step</b>	<b>Actions</b>
1	Preparations	Clean MS Outlook Certificate Store
2	Get new trust list	Download "Trust List" file From Web Site
3	Import Into Internet Explorer	Extract all certificates into folder Import manually every certificate into MS Outlook
4	Validate Certificate Store	Check list of Root Certificate in MS Outlook. Check certificate Fingerprints

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

---

**1.7 Import in Mozilla**

**GOAL:** Validate the compatibility of the "Trust List" with Mozilla.

**Test Prerequisites**

- Bridge and Gateway CA Pilot Infrastructure should be operational.
- Test 1.1 and 1.2 should be done successfully: A First "Trust List" File should have been generated, and validated.

<b>Test Step Nr</b>	<b>Test Step</b>	<b>Actions</b>
1	Preparations	Clean Mozilla Certificate Store
2	Get new trust list	Download "Trust List" file From Web Site
3	Import Into Internet Explorer	Extract all certificates into folder Import manually every certificate into Mozilla
4	Validate Certificate Store	Check list of Root Certificate in Mozilla. Check certificate Fingerprints

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

**2.1 - Enrollment Test**

**GOAL:** Test technical infrastructure of participating CA for compliance with European IDA Bridge and Gateway CA

This test will validate that the Participant CA is able on technical level to recognize the EBGCA as a Certification Authority, and the certificate trust list published by it.

The first test constitutes of a series of tests to verify whether the participant is able to enrol to the Bridge and Gateway CA and accept "Trust Lists" files. This test plan involves 4 distinguished phases.

**Enrollment Test Prerequisites**

The Candidate Participant should have signed up for participation in the Bridge and Gateway CA Pilot before enrolling into this test phase. Formal requirements are specified in the MOU and in the "Recommendation for an operational Bridge and Gateway CA".

Test Step Nr	Test Step	Actions
1	Install Bridge and Gateway CA Root Certificate	<p>This test will validate that the Participant CA is able on technical level to recognize the Bridge and Gateway CA as a Certification Authority, and the certificate trust list published by it.</p> <p><b>Steps:</b></p> <ul style="list-style-type: none"> <li>Download the Bridge and Gateway CA Root Certificate from <a href="http://ebgca.e-trust.be/trustlist">http://ebgca.e-trust.be/trustlist</a></li> <li>Check the certificate Fingerprint</li> <li>Import the root certificate into your windows platform (double click on .crt file)</li> <li>You can check the certificate in internet explorer by choosing Tools-&gt; Internet Options, tab "Content", click button "Certificates", select tab "Trust Root Certification Authorities". Now check that the Bridge and Gateway CA Root Certificate appears in the list:               <ul style="list-style-type: none"> <li>European IDA Bridge and Gateway CA</li> </ul> </li> </ul>
2	Enroll in Bridge and Gateway CA	<ul style="list-style-type: none"> <li>Make sure MOU is prepared</li> </ul> <p>Optional (If you want a dedicated section on the Bridge and Gateway CA Web Site)</p> <ul style="list-style-type: none"> <li>Supply SSL Server Certificates</li> </ul> <p>Send an email with</p> <ul style="list-style-type: none"> <li>The CA ROOT certificate;</li> <li>All CA Primary, Operational, or other Sub-CA Certificates;</li> </ul> <p>to</p>

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

		ebgca-enroll@ e-trust.be
3	Participant subscribes to mailing list.	<p>Send an email with</p> <ul style="list-style-type: none"> <li>• E-Mail Address;</li> <li>• Organisation Name;</li> <li>• Contact details (Name, Address, Phone, Fax);</li> </ul> <p>to</p> <p>ebgca-subscribe@e-trust.be</p>
4	CA Issues Updated "Trust List"	<p>Trust List is published here <a href="http://ebgca.e-trust.be/trustlist">http://ebgca.e-trust.be/trustlist</a></p> <p>Bridge and Gateway CA sends an announcement that a new participant has joined.</p>
5	Check email announcement	<p>Participant checks that an email announcement is received on the Bridge and Gateway CA mailing list.</p> <p>Participant should receive a message in his mailbox with notification to all Bridge and Gateway CA mail list members announcing that a new CA has joined the Bridge and Gateway CA.</p>
6	Check CA appears on list of trusted CAs	<p>Participant checks its own CA appears on the Web Site Trust List</p> <p>URL: <a href="http://ebgca.e-trust.be/participants">http://ebgca.e-trust.be/participants</a></p> <p>Check that CA is mentioned on trusted list</p>
7	Participant Downloads updated Bridge and Gateway CA Certificate Trust List	<p>Validate the communication and the procedures established between the Bridge and Gateway CA and the participant CA.</p>
8	Participant installs updated Bridge and Gateway CA Certificate Trust List	<p>Second Validation of the compliance of the technical infrastructure of the participant CA, proving the ability to continuously download and update the Certificate Trust Lists during the operational phase of the Bridge and Gateway CA.</p>

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

**2.2 - Email Test**

**GOAL:** Test for recognising certificates by participants of the Bridge and Gateway CA Pilot in email communication.

The second test plan constitutes of a test for evaluating secured email communications under the Bridge and Gateway CA participating CA's. This test plan contains a series of tests that will validate step by step the ability for S/MIME secured Email communications.

**Email Test Prerequisites**

The Participant should successfully completed the "Enrollment Test".

The Participant should have successfully completed the "MS Outlook" / "Mozilla" import test.

The Participant should have installed the Bridge and Gateway CA Root Certificate

Test Step Nr	Test Step	Actions
0	Verify	Verify that the Certificates from the Trust List are still available in the Certificate Store from previous test (X.X Import in MS Outlook). If this is not the case, re-install these certificates in MS Outlook.
1	Issue <b>Email</b> Certificate	Participant issues a new certificate to be used for <b>S/MIME</b> , under it's own CA, which is recognised under the Bridge and Gateway CA.  Note1: Alternately, an existing certificate may be used. Note2: The mail address in the certificate should match the e-mail address the tests are performed on.
2	Install Certificate	Participant installs the new certificate into his MS Outlook email client.
3	Send Signed Email	Participant sends a signed (S/MIME) email message to the Bridge and Gateway CA Test Email Address. Test1@ebgca.e-trust.be To sign the email, he uses the certificate issued and installed in step 1 and 2.
4	Check	Bridge and Gateway CA checks the receipt of the email, and checks whether the signature is validated correctly. i.e. <ul style="list-style-type: none"> <li>• The signature should be valid.</li> <li>• As all CA's on Bridge and Gateway CA trust list should be imported in MS Outlook, the certificate should be reported as being valid (Signed by participant CA).</li> <li>• The Certificate should be valid (i.e. not suspended or revoked). This requires a certificate &amp; CA dependent validation: <ul style="list-style-type: none"> <li>○ The Certificate is checked for validation information (CRL, OCSP)</li> <li>○ The Certificate Policy is checked for</li> </ul> </li> </ul>

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

		<p>validation information</p> <ul style="list-style-type: none"> <li>○ The CRL is downloaded, or an on-line evaluation is requested of the certificate.</li> </ul>
5	Reply with correctly signed email	<p>Bridge and Gateway CA sends a reply email to the participant (originating Email Address).</p> <p>This mail is signed with an Email Certificate issued by the Bridge and Gateway CA.</p> <p>This email is signed with an Email Certificate issued by the "Virtual DG" (IDA PKI CA).</p>
6	Check	<p>Participant checks the receipt of the email, and checks whether the signature is validated correctly.</p> <p>i.e.</p> <ul style="list-style-type: none"> <li>• The signature should be valid.</li> <li>• As all CA's on Bridge and Gateway CA trust list should be imported in MS Outlook, the certificate should be reported as being valid (Signed by IDA PKI).</li> <li>• The Certificate should be valid (i.e. not suspended or revoked). This requires a certificate &amp; CA dependent validation: <ul style="list-style-type: none"> <li>○ The Certificate is checked for validation information (CRL, OCSP)</li> <li>○ The Certificate Policy is checked for validation information</li> <li>○ The CRL is downloaded, or an on-line evaluation is requested of the certificate.</li> </ul> </li> </ul>
7	Reply signed email with unknown CA certificate	<p>Bridge and Gateway CA sends a reply email to the participant (originating Email Address from step 5).</p> <p>This email is signed with an Email Certificate issued by an unknown (fictitious) CA.</p>
8	Check	<p>Participant checks the receipt of the email, and checks whether the signature is invalid because a CA that is not trusted issued the certificate.</p> <p>i.e.</p> <ul style="list-style-type: none"> <li>• The signature should be valid.</li> <li>• As only CAs on Bridge and Gateway CA trust list should be imported in MS Outlook, the certificate should be reported as being invalid (Signed by a CA that is not trusted).</li> <li>• A Certificate Status check should not be performed in this case.</li> </ul>
<b>Optional Steps</b>		
9	Issue Certificate	Participant issues a new certificate to be used for S/MIME,

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

	Under unknown CA	under it's a CA not recognised as under the Bridge and Gateway CA (this may be a fictitious CA).
10	Install Certificate	Participant installs the new certificate into his MS Outlook email client.
11	Send Signed Email	Participant sends a signed (S/MIME) email message to the Bridge and Gateway CA Test Email Address. Test1@ebgca.e-trust.be
12	Check	Bridge and Gateway CA checks the receipt of the email, and checks whether the signature is invalid because a CA that is not trusted issued the certificate.  i.e. <ul style="list-style-type: none"> <li>• The signature should be valid.</li> <li>• As only CAs on Bridge and Gateway CA trust list should be imported in MS Outlook, the certificate should be reported as being invalid (Signed by a CA that is not trusted).</li> <li>• A Certificate Status check should not be performed in this case.</li> </ul>
<b>Further Optional Steps</b>		

European IDA Bridge and Gateway CA Pilot  
WP 1.2 - doc5 - Test Programme

**2.3 - Authentication Test**

**GOAL:** Test for recognition of certificates by participants of the Bridge and Gateway CA Pilot in SSL Client Authentication.

The third test validates the use of Bridge and Gateway CA issued certificates for authentication purposes, more specific a user authenticating him self to a web server application (also known as SSL Client Authentication).

**Note:** During the pilot it may also be considered to test “SSL Server Authentication” as this is always used in combination with “SSL Client Authentication”.

**Authentication Test Prerequisites**

The Candidate Participant should have successfully completed the “**Enrollment Test**”.  
The Participant should have installed the Bridge and Gateway CA Root Certificate

Test Step Nr	Test Step	Actions
1	Check CA appears on list of trusted CA's	Participant checks its own CA appears on the Web Site Trust List  URL: <a href="http://ebgca.e-trust.be/participants">http://ebgca.e-trust.be/participants</a>  Check that CA is mentioned on trusted list
2	Issue <b>Web Certificate</b>	Participant issues a new certificate to be used for <b>SSL Client Authentication</b> ; under it's own CA, which is recognised under the Bridge and Gateway CA.  Note1: Alternately, an existing certificate may be used. Note2: The certificate from test 2.2 may be used provided that it can be used both for SSL Client Authentication as for S/MIME communication.
3	Log in on web site	Participant logs in on SSL Protected Web Site using this certificate.  URL: <a href="http://ebgca.e-trust.be/testplan/authentication/">http://ebgca.e-trust.be/testplan/authentication/</a>
4	Server validation of certificate	SSL Web Server validates “client certificate” upon log in of the client.  Bridge and Gateway CA operator should check web server log files to validate success.  A Certificate Status check is not foreseen for the authentication test, as this would lead to an overly complex set up and configuration of the applications. It could be foreseen to include a manual validation of the CRL or the OCSP.
5	Validate log on	Participant Checks whether he is allowed to access the protected web page  URL: <a href="http://ebgca.e-trust.be/testplan/authentication/logon">http://ebgca.e-trust.be/testplan/authentication/logon</a>

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

		<p>after logon, user should see :</p> <p>Welcome &lt;user-name&gt; to the European IDA Bridge and Gateway CA,          You appear to have a certificate issued by participant CA &lt;ca-name&gt;,          You successfully logged on to this web page.</p> <p>Where</p> <ul style="list-style-type: none"> <li>• <b>user-name:</b> Common Name of the subject as it appears in the Certificate</li> <li>• <b>ca-name:</b> Common name of the Certification Authority as it appears in the Certificate.</li> </ul>
<b>Optional Steps</b>		

European IDA Bridge and Gateway CA Pilot  
 WP 1.2 - doc5 - Test Programme

**2.4 – Trust List Sign Test**

**GOAL:** Test for re-signing of the Trust List by a participant, and publishing of this re-signed trust list.

The third test validates the use of Bridge and Gateway CA issued certificates for authentication purposes, more specific a user authenticating him self to a web server application (also known as SSL Client Authentication).

**Trust List Sign Test Prerequisites**

The Candidate Participant should have successfully completed the “**Enrollment Test**”.  
 The Participant should have installed the Bridge and Gateway CA Root Certificate

<b>Test Step Nr</b>	<b>Test Step</b>	<b>Actions</b>
1	Preparation	Participant indicates to Bridge and Gateway CA which Certificates are to appear in re-signed trust list.
2	Re-Sign Trust List	Bridge and Gateway CA will publish an updated re-signed trust list (signed on behalf of the participant)
3	Validate Trust List	Participant downloads and validates the new Trust List  URL: <a href="http://ebgca.e-trust.be/&lt;participant&gt;/trustlist">http://ebgca.e-trust.be/&lt;participant&gt;/trustlist</a>  Check that the new trust list contains all requested certificates. Check that the list of participants is corresponding  URL: <a href="http://ebgca.e-trust.be/&lt;participant&gt;/participants">http://ebgca.e-trust.be/&lt;participant&gt;/participants</a>
4		
<b>Optional Steps</b>		

## ANNEX II - Reporting Template

### *Administrative Information*

<b>Participant</b>	
<b>Test Plan Reference</b>	
<b>Date of performing tests</b>	
<b>Name of person performing the tests</b>	
<b>Overall Test Result</b>	OK / NOT OK

<b>Test Step Nr</b>	<b>Test Step Description</b>	<b>Test Result (OK / NOK)</b>	<b>Comments</b>
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

## ANNEX III – Sample Completed Report

### Administrative Information

<b>Participant</b>	<i>IDA PKI</i>
<b>Test Plan Reference</b>	<i>Authentication Test – 2.3</i>
<b>Date of performing tests</b>	<i>12/03/2004</i>
<b>Name of person performing the tests</b>	<i>Mr. Janssen</i>
<b>Overall Test Result</b>	<b>OK</b>

### Test Results

<b>Test Step Nr</b>	<b>Test Step Description</b>	<b>Test Result (OK / NOK)</b>	<b>Comments</b>
1	Check CA is trusted	OK	
2	Issue Certificate	OK	<i>Re-used existing certificate CN=Jan Janssen, S/N=01002423</i>
3	Log in on web site	OK	<i>Received pop-up about trusting the server certificate. This is ok as the trust list was not installed in the internet explorer yet.</i>
4	Server validates certificate	OK	<i>Confirmation from mr. Piet Pieters.</i>
5	Client validates log on	OK	<i>Client certificate is recognised correctly</i>