



EBGCA Pilot WP1 - Technical Description Pilot platform setup

European IDA Bridge/Gateway CA Pilot for Public Administrations



Document control

1. Document Information

Document title:	EBGCA Pilot WP1 - Technical Description Pilot platform setup
Project Reference:	IDA PKI II Specific Contract#4/ EBGCA WP1
Document Archival Code:	EBGCA-DEL-024 - EBGCA Pilot WP1 Technical Description platform

2. Related documents / References

Reference	Document filing code
[1]	A bridge CA for European public administrations Feasibility study.
[2]	ETSI TR 102 030 V1.1.1 (2002-03) Provision of harmonized Trust Service Provider status information
[3]	IDA-BridgeCA-WP1-Annex-6.doc
[4]	ETSI TS STF 102 231 V1.1.1 (2003-10) Requirements for Trust Service Provider status information
[5]	European Bridge and Gateway CA Pilot WP 1.2 - Doc 1 - MEMORANDUM OF UNDERSTANDING
[6]	European Bridge and Gateway CA Pilot WP 1.2 - Doc 4 - Technical Architecture
[7]	European Bridge and Gateway CA Pilot WP 1.2 - Doc 5 - Test Programme
[8]	CWA 14167-2 : CEN Workshop Agreement – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signature – Part 2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)
[9]	EBGCA-DEL-004 - WP2 ParticipationForm Member State
[10]	EBGCA-DEL-024 mini-CPS for the EBGCA Pilot
[11]	EBGCA-DEL-009 - EBGCA Pilot WP1- Use Cases

3. Version control

Version	Date	Description / Status	Responsible
V0.1	20/12/2004	TOC	KVA
V0.2	10/01/2005	First Draft	JBL
V1.0	25/01/2005	Final version	WCL

4. Distribution

Version	Company	Name	Action required
V1.0	European Commisison - IDA	Gzim Ocakoglu	Deliverable of WP1 Task 1.1
	Certipost	EBGCA projectcteam	Project repository

Table of content

DOCUMENT CONTROL	2
1. DOCUMENT INFORMATION.....	2
2. RELATED DOCUMENTS / REFERENCES	2
3. VERSION CONTROL.....	2
4. DISTRIBUTION.....	3
TABLE OF CONTENT	4
ABBREVIATIONS	5
1. INTRODUCTION	6
1.1. DOCUMENT SCOPE	6
1.2. HOW IS THIS DOCUMENT ORGANIZED.....	6
2. TEST BED	7
2.1. MEMBER STATES	7
2.2. EBGCA PLATFORM: COMPONENT OVERVIEW	8
2.2.1. <i>EBGCA Test system</i>	8
2.2.1.4. <i>EBGCA Platform Functionality</i>	8
2.2.1.5. <i>Update Mailing list</i>	8
2.2.2. <i>Architecture details</i>	8
2.2.2.4. <i>Architectural overview</i>	8
2.2.2.5. <i>Mail server</i>	9
2.2.2.6. <i>Three tier application architecture</i>	9
2.2.3. <i>Hardware</i>	9
2.3. SW DEVELOPMENT.....	9
2.4. PRACTICAL	10
2.4.1. <i>DNS</i>	10
2.4.2. <i>Main WebPage</i>	10
2.4.3. <i>TSL update Mailing List : e-mail addresses</i>	10
3. PKI INFRASTRUCTURE	10
3.1. FUNCTIONALITY	10
3.2. PKI ARCHITECTURE.....	10
3.3. HARDWARE.....	11
3.4. CERTIFICATES	12

Abbreviations

EBGCA:	European Bridge Gateway CA
BCA :	Bridge Certification Authority
CA :	Certification Authority
MS:	Member State
PKI :	Public Key Infrastructure
TSL :	Trust Service Provider List (as defined by [2], ETSI TR 102 030 V1.1.1 (2002-03))
TSP :	Trust Service Provider

1. Introduction

1.1. *Document scope*

This document has as purpose to describe the technical setup of the European IDA Bridge/Gateway CA Pilot.

1.2. *How is this document organized*

First of all this technical description of the platform, describes the Test bed setup, that consists physically of a platform at the EBGCA administrator side and on the other side the participating Member states test PC.

Further, a Component overview is given, describing the test system, update mailing list, PKI system and a schema giving the architectural overview of the EBGCA proof of concept - platform.

Hereafter, a more detailed architecture on is given.

The software development has been an iterative process that has been guided and has been described with a number of Use Cases (see [11]).

A final chapter resumes practical aspects such as the DNS, main webpage, TSL update Mailing list email address etc.

2. Test bed

2.1. *Member states*

The setup at the side of participating member states consists mainly of a test PC with JAVA installed, and an e-mail address to communicate with the Bridge administrator. This platform has been described in [9] the Participation Form¹ for Member States.

Recapitulation:

Pre-requisites for the applications, used by the member state administrations:

It is required that the administrations are using actively at least one of the applications that are included in the EBGCA Pilot Program. The applications that are included in the EBGCA Pilot Program are the following:

<u>Application type</u>	<u>Application</u>	<u>Version</u>
Web browser	MS Internet Explorer	6.0
	Mozilla	1.6
E-mail clients	MS Outlook	2000, 2002, XP
	Mozilla	1.7
	Lotus Notes	6.5

Prior to participation to the EBGCA Pilot, these applications have been tested successfully with the operational PKI already in place within the administration of the member state. The functionalities that need to be tested, include at least:

<u>Application Type</u>	<u>Functionality</u>
Web-browsers	SSL mutual authentication
E-mail clients	Digitally sign and verify an e-mail
	Digitally Encrypt and decrypt an e-mail

In order to be able to use the software that will be provided by the contractor to facilitate the integration, on all systems which will participate in the test, Java 2 Platform, Standard Edition, v1.4.2 (JRE is sufficient) needs to be installed. This software is downloadable from <http://java.sun.com/j2se/1.4.2/download.html> .

¹ EBGCA-DEL-004 - WP2 ParticipationForm Member State

2.2. **EBGCA platform: component overview**

2.2.1. **EBGCA Test system**

2.2.1.4. **EBGCA Platform Functionality**

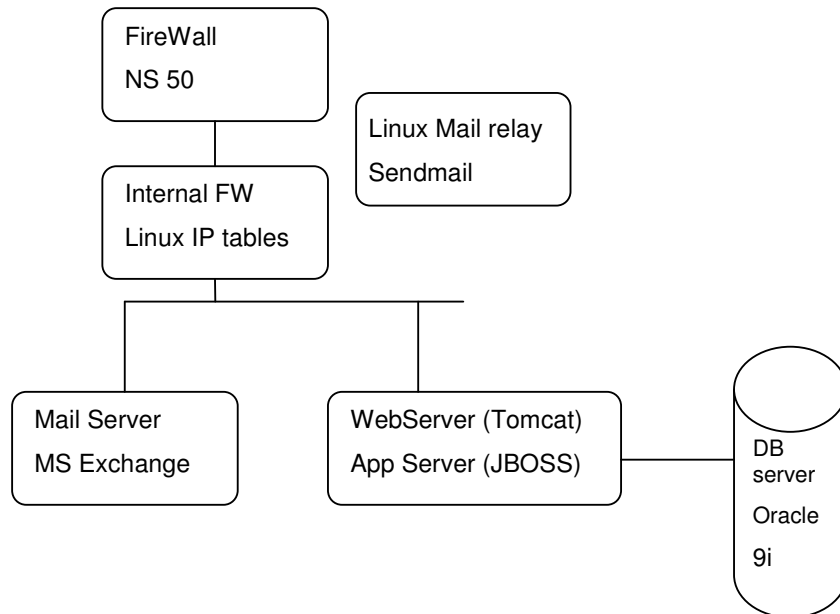
The EBGCA system has the goal to offer the required functionality to IDA and possibly the Member States to be able to manage a Scheme and issue TSL's. This functionality requires much more than it would seem at first sight. Not only do we have to provide the functionality to manage Schemes and TSL's, we also have to manage the whole Identity and User Management of the different actors of the different organisations in different roles. More explanation on this functionality has been described in the Uses Cases that are provided [11].

2.2.1.5. **Update Mailing list**

The update mailing has the purpose to make sure that all users of the system can be updated on events that occur during the testing period. Although the EBGCA system might send some automatic mails, the Update Mailing list is mainly to be used in a manual fashion. Any person that is involved in the pilot can, when there is a need to inform the others involved, send a mail to this mailing list. The Mailing list system will then automatically forward this mail to all users involved.

2.2.2. **Architecture details**

2.2.2.4. **Architectural overview**



Point of view network security, the architecture foresees two FireWalls (FW): one HW FW NS50 that is open to the external network, and one Linux IP tables FW that protects the internal network. Between them we find the DMZ (Demilitarized Zone) where the external mail is relayed by the Linux Mail Relay to the MS Exchange server after virus verification and spam filtering. Logically the webserver would as well be placed in the DMZ, but since this is only serving for a short term span pilot, no extra machine has been set-up.

From application architecture – point of view, a three tier architecture has been set up. See details below.

2.2.2.5. **Mail server**

The Update Mailing list is created on an MS Exchange Server managed by Certipost.

2.2.2.6. **Three tier application architecture**

The application that provides this functionality exists of three tiers:

- A web layer provided by a Tomcat webserver. This webserver delivers the presentation layer in the form of a web GUI that allows to handle the business logic in a user convenient way.
- An application server provided by JBOSS. This application server runs all the business logic that has been especially developed for this pilot, as identified by the Use Cases (see [11]).
- A storage layer provided by an Oracle 9i Database server. This storage component serves to store persistently all data concerning the Scheme(s) and user management.

2.2.3. **Hardware**

Since this is a Pilot used for testing purposes, there were no sizing requirements. As such HW requirements were not high.

1. External FW: dedicated Netscreen HW (NS50)
2. Internal FW: Compaq Proliant 1U (Red Hat Linux with IP Tables)
3. Mail Relay: Compaq Proliant DL360 (Red Hat Linux with Sendmail and bitdefender)
4. Mail Server: Unipress (Windows 2003 server with MS Exchange Server)
5. Webserver & Application server: Compaq (Windows 2000 server with Tomcat and JBOSS 3.2.6)
6. DB server: SUN (Solaris with Oracle 9i)

2.3. **SW development**

The software was developed based on the Use Cases (see [11]).

2.4. Practical

2.4.1. DNS

The DNS is defined as the external subdomain (ebgca.certipost.be) of the certipost.be domain.

2.4.2. Main WebPage

The EBGCA system is accessible by all EBGCA pilot users on the following URL:
<http://www.ebgca.certipost.be/>.

2.4.3. TSL update Mailing List : e-mail addresses

Mails to be distributed are to be sent to ebgca@staff.certipost.be.

3. PKI Infrastructure

3.1. Functionality

In order to be able to perform the testing, different types of certificates are required and will be delivered by Certipost. See [6] chapter 3.1 for more details on these different types of certificates and the reasons why they are required.

3.2. PKI architecture

The same architecture as for the standard Certipost PKI infrastructure is used for the provisioning of the certificates for the pilot.

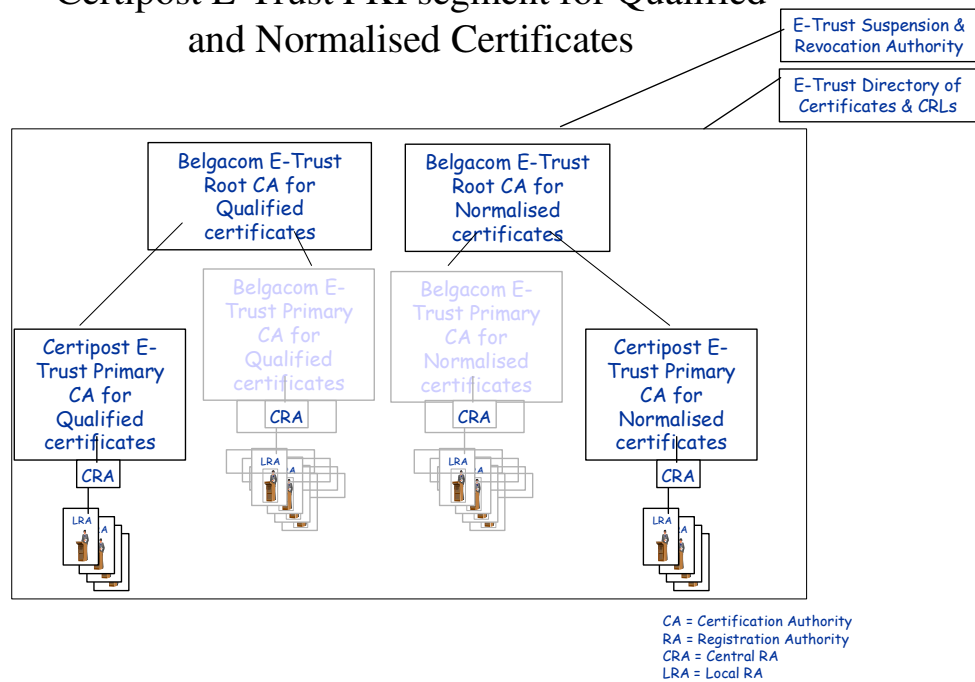
Certificate Authorities (CA's)

The certificates that will be used in this pilot will be delivered from the Certipost Normalised Test CA, which is part of the total Certipost E-Trust Qualified & Normalised CA hierarchy.

Certipost E-Trust has a Qualified & Normalised CA hierarchy beginning at the top level with two Root CAs, one for Qualified Certificates and the second for the Normalised Certificates, issuing only Sub-CAs' Certificates, respectively for Qualified Certificates and for Normalised Certificates. This infrastructure is consistent with the PKIX / X.509 standard.

The following figure depicts the current Certipost E-Trust Qualified & Normalised PKI segment:

Certipost E-Trust PKI segment for Qualified and Normalised Certificates



Registration Authority

For the communication with the CA's the Registration Authority Officers will use the standard RA platform that is available for Certipost RA Officers.

3.3. Hardware

1. CA's: Compaq (Windows 2000 Server with Unicert 3.5.3 p5, Oracle 8i)
2. RA: Compaq (Windows 2000 Server with Unicert WebRAO)
3. LDAP (CRL distribution): none

3.4. Certificates

The issuance of certificates is governed by a mini-CPS that has been created specifically for this pilot (see [10]).

Annexes :

Annex 1: EBGCA-DEL-009 - EBGCA Pilot WP1- Use Cases v1 0