NTNU

Norwegian University of
Science and Technology

Interoperability for electronic ID

Zuzanna Zygadlo

Master of Science in Computer Science
Submission date: October 2009
Supervisor: Torbjørn Skramstad, IDI
Co-supervisor: Ole Kristian Svendsen, BBS

Norwegian University of Science and Technology
Department of Computer and Information Science

Problem Description

Proposal of a PKI trust model based on the Validation Authority concept for global interoperability for electronic IDs.

Assignment given: 15. June 2009
Supervisor: Torbjørn Skramstad, IDI

Abstract

Electronic Business, including eBanking, eCommerce and eGovernmental services, is today based on a large variety of security solutions, comprising electronic IDs provided by a broad community of Public Key Infrastructure (PKI) vendors. Significant differences in implementations of those solutions introduce a problem of lack of interoperability in electronic business, which have not yet been resolved by standardization and interoperability initiatives based on existing PKI trust models.

It is not only the technical interoperability of electronic IDs which today makes many electronic transactions impossible. The main obstacle to global interoperability of electronic IDs is the lack of trust in digital certificates issued by various Certification Authorities (CAs). Relying Parties (RPs) need to trust digital certificates in order to be able to validate them. We observe that the multi-vendor PKI community lacks an independent source of electronic IDs quality information, which could make digital certificate validation possible on a global scale.

Therefore, this thesis presents the concept of a new PKI trust model which introduces a Validation Authority (VA) as a single trust point in the global PKI trust network. The main goal of this thesis is to develop a model of Global Validation Service (GVS), which uses Global Validation Authority (GVA), based on the VA concept, to provide digital certicate validation and signature verication to Relying Parties. The presented research focuses on investigating technical, legal and business issues which would enable RPs to delegate the certificate validation to an independent Validation Authority.

Preface

This thesis is the result of the research which was conducted with a significant contribution of many people. For this reason, I would like to thank all those, who shared their valuable experience with me, in order to make this thesis a complete study of the PKI and the Validation Authority concept.

Acknowledgements

I would like to express my particular gratitude to my supervisors: Ole Svendsen and Torbjørn Skramstad for their extended guidance throughout the entire process of my research. Their valuable comments and advises reflect in the structure and the content of my thesis, and their indescribable support made my research an exciting experience.

Besides, I would like to thank all those who agreed to contribute to this thesis by participating in the interviews. I am specially grateful to Leif Buene for his unspeakable contribution when introducing me to the VA concept and commenting on this thesis. I am also thankful to Jon Ølnes and Anette Andresen, for sharing their unique knowledge and experience on the VA subject with me.

Finally, I would like to thank Bishwajit Choudhary, Wenke Skjærve, Ketil Kintel and Halvor Sakshaug for their precious expertise. Their comments became an important input to my research and their advises helped me answer many of my research questions. I would also like to thank all persons working in Tillitstjenester i BBS, especially the eSecurity Team, for their everyday kindness that helped me to feel welcomed at BBS. Thank you all!

Acronyms

AC - Attribute Certificate
ADSS - Advanced Digital Signature Services

C4 - Citizens and Commerce Class Common
CA - Certification Authority
CARL - Certification Authority Revocation Lists
CDP - CRL Distribution Points
CMP - Certificate Management Protocol
CP - Certificate Policy
CPS - Certification Practice Statement
CRL - Certificate Revocation List
CRT - Certificate Revocation Trees
CSP - Certification Service Provider or Cryptographic Service Provider or Certificate Service Provider

DBMS - Database Management System
DES - Data Encryption Standard
Difi - Direktoratet for forvaltning og IKT (The Agency for Public Management and eGovernment)
DN - Distinguish Name
DNV - Det Norske Veritas

ECAF - The European Certification and Authority Forum
EE - End entity
EEA - European Economic Area
EFVS - European Federated Validation Service
EEMA - European Forum for Electronic Business
EGCA - E-Governance Certification Authority
eID - electronic identification
EPRL - End-entity Public-key Certificate Revocation List

FBCA - Federal Bridge Certification Authority
FCPF - Federal Common Policy Framework
FFC - Finite Field Cryptography
FPKI - Federal Public-Key Infrastructure
FTP - File Transfer Protocol

GPKI - Governmental Public-Key Infrastructure
GR - General Requirement
GVA - Global Validation Authority
GVS - Global Validation System

HTTP - Hypertext Transfer Protocol

IDABC - Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens
IPsec - Internet Protocol Security
ISIS-MTT - Industrial Signature Interoperability Standard and MailTrusT

JCA - Java Cryptography Architecture
JPKI - Jumin Public-Key Infrastructure

LDAP - Lightweight Directory Access Protocol
LDAPext - Lightweight Directory Access Protocol Extension
LGPKI - Local Governmental Public-Key Infrastructure

MAC - Message Authentication Code
MISPC - Minimum Interoperability Specification for PKI Components

NIST - National Institute of Standards and Technology
NSA - National Security Agency

OASIS DSS - OASIS Digital Signature Service
OCSP - Online Certificate Status Protocol

PEPPOL - Pan-European Public Procurement Online
PGP - Pretty Good Privacy
PKCS - Public-Key Cryptographic Standards
PKI - Public Key Infrastructure
PKIX - Public-Key Infrastructure X.509

RA - Registration Authority
RCA - Root Certification Authority
RFC - Request For Comments
RP - Relying Party

SCVP - Simple Certificate Validation Protocol
SET - Secure Electronic Transaction
S/MIME - Secure / Multipurpose Internet Mail Extensions
SPKI - Simple Public Key Infrastructure
SR - Specific Requirement
STORK - Secure idenTity acrOss boRders linKed

TDEA - Triple Data Encryption Algorithm

VA - Validation Authority

XKMS - XML Key Management Specification

Contents

Chapter 1

Introduction

This chapter introduces the research problem of the thesis. It presents my motivation and the methodology used in the research. Besides, this chapter also contains an outline of the entire thesis.

1.1 Motivation

All participants of the electronic business, that is also referred to as *eBusiness*, agree, that one of the most important issues concerning modern *eCommerce*, *eGovernment* and *eBanking* is *security*. On one hand electronic commerce constantly changes from a structure based on bilateral agreements towards a complex network were many actors interacts with many other. On the other hand, more and more government services and banking services use information and communication technology (ICT) in order to become more available to their users.

Nowadays, numerous transactions using ICT must be done between entities which are unknown to each other and which interact only one time with each other. Besides, this interactions often occur over untrustworthy communication networks, such as the Internet. For those reasons, the problem of authentication of electronically communicating entities and the problem of non-repudation of performed transactions becomes so important in the eBusiness.

It is, however, also important to point out that the term security, as it is an abstract concept, doesn't mean exactly the same thing to all of the electronic business participants. Therefore, by independently realizing one's own concept of security and trust, electronic commerce participants lead the security solutions, used by the entire eBusiness community, to become highly diversified, because of its large scale of use.

This large variety of security solutions consequently leads to an important incompatibility among them. Some existing solutions simply cannot work together, because of the significant differences between them. This situation introduces a problem of lack of *interoperability* in electronic business, which without strong efforts from standardization organizations cannot be resolved.

In the current situation, when no unified international classification of available security solutions exists [1], electronic business requires new interoperability solutions to be introduced. New interoperability models can help different actors of eCommerce, eGovernment and eBanking to develop their networks of trust, and therefore expand their services and activities.

1.1.1 Electronic ID as a public-key certificate

Digital signatures, which according to many legislations are interchangeable with handwritten signatures, play an important role in electronic business. They have an important legal and business value, as they certify one's agreement to certain legal documents, i.e. transactions or statements. Therefore, electronic IDs, which are digital certificates used to produce digital signatures, must be trustworthy and secure in their use, in the same way as handwritten signatures have been for hundreds of years.

For this reasons, electronic IDs use one of the best of todays known cryptographic techniques, which is *public-key cryptography*. What is more, because of their high value, thus complexity, electronic IDs require to be supported by a broad security infrastructure called *Public Key Infrastructure (PKI)*. PKI includes many elements and concepts that enables a variety of entities to obtain their electronic IDs in a form of digital certificates, called *public-key certificates*.

PKI allows electronic IDs to function correctly and securely over a certain period of time. Because of the fact that the world of electronic commerce expands continuously, electronic IDs issuers must make sure that certificates they produce will withstand the constant changes of the environment in which they have to work.

1.1.2 Interoperability issue in PKI

Nowadays, there exists many very different PKIs in the world. Many companies from all over the globe try to act as certification providers, in some publications referred to as *Certification Service Providers (CSPs)* [1]. Those companies sell different types of certifications, varying in their purposes, forms, complexities and qualities. *Certification*

Authorities (CA) are special certification service providers issuing public-key certificates, that may be used as electronic IDs. Therefore, further in this thesis we will use the term CAs to refer to certification services providers.

Since most of CAs are private companies, they all use their own policies and terminology. That is why, it becomes more and more difficult to classify all existing CAs in an unified way [1], and thus to know which of them the *Relaying Parties (RPs)* can trust (see section 2.2.4). In order to make electronic IDs interoperable in the electronic commerce, RPs must be able to validate many types of existing certificates.

This problem of certificate validation obliges RPs to build their own trust networks. Each node of those networks is achieved through agreements, which are resource and time consuming for the RPs. Besides, the number of CAs grows continuously, making it nearly impossible for any RP to achieve an agreement with every single CAs. Therefore, electronic commerce requires a new interoperability solution for the electronic ID.

1.2 Problem definition

This thesis presents the concept of a new PKI trust model which introduces a *Validation Authority (VA)* as a single trust point in the global PKI trust network. This solution was born in the late '90, and it was published in 2006 in two papers titled : *"PKI Interoperability by an Independent, Trusted Validation Authority"*[2] by Jon Ølnes, and *"Use of Validation Authority to Provide Risk Management for the PKI Relying Party"*[3] by Jon Ølnes and Leif Buene form DNV AS.

Those papers introduced a new PKI concept, the Global Validation Authority, which can act as a global *trust anchor* . This means that the Global VA is to be seen by all RPs as the most trustworthy entity in all existing PKIs. With the use of the global VA, as an independent external validation entity, RPs will no longer need to sign multiple agreements with various CAs. They will be able to rely only on one agreement with the Global Validation Authority, delegating the entire certificate validation procedure to the external entity.

The main goal of this thesis is to develop a model of Global Validation Service (GVS), which uses Global Validation Authority (GVA) to provide digital certificate validation and signature verification to the Relying Parties. The research focuses on investigating technical, legal and business issues related to the Global Validation Service. Besides, in this thesis we study advantages and drawbacks of introducing the Global Validation Service for all entities involved in this new PKI trust model.

1.3 Research methodology and work process

The research presented in this thesis results from the combination of the following methods :

- literature study of the public-key cryptography and Public-Key Infrastructure, as well as a study of existing interoperability initiatives, both practical steps being taken by legislative authorities in different countries, and more theoretical outcomes of current research on eID interoperability
- face-to-face interviews and consultations with experienced PKI business, legal and technical specialists, who have been working with the concept of Validation Authority, in function of Senior Vice President eSecurity at BBS, Senior Principal Engineer at DNV, BBS Identity Manager, eSecurity Team Manager and System Developer at BBS (see Appendix .1).
- analysis of gathered papers, specification documents, CPs, CPSs, agreements with CAs and RPs, and other PKI related information,
- a laboratory exercise, using a GVS test application provided by BBS
- validation of the conclusions drawn from the presented research

In order to understand basic principles of PKI and of the problem of public-key certificate validation, we first searched through a literature in order to study the underlying theory. Once basic concepts were acquired, we needed to read PKI technical reports and standardization proposals, in order to understand the problem of interoperability of electronic IDs and current solutions to this problem.

Then, we got access to expertise from PKI technical, business and legal specialists, who had a deep knowledge of the functioning of electronic IDs in the electronic commerce. We interviewed them in person and we discussed their experience with PKI and the Validation Authority concept. We tried to understand the motivation for VA creators, the evolution of the concept, its current state, and its possible future development. We were interested in documented statements, as well as interviewed persons' private opinions on the Global Validation Authority subject.

After gathering and analyzing all the collected information, as well as having our "hands-on" exercise with the current Global VA implementation, we proposed the theoretical solution to the research problem. Then, we compared the outcome of our analysis with the current state of the VA concept, and we evaluated and discussed its different characteristics. Finally, we drew conclusions from our evaluation, we validated them and we present them together with suggested further continuation of the research.

1.4 Thesis outline

This thesis consists of eight chapters and it is organized as follows :

Chapter 1 Introduction to the research problem of electronic ID Interoperability. Description of the motivation and the research methodology of the thesis.

Chapter 2 Literature study of Public Key Infrastructure. Definitions and description of PKI concepts and services. Insight into public-key certificates and PKI protocols.

Chapter 3 Study of different PKI trust models and existing interoperability solutions for digital certificates usage.

Chapter 4 Analysis of PKI use cases and presentation of interoperability initiatives in the world. Focus on advantages and weaknesses of different approaches, as well as analysis of some barriers of deployment and related legal issues.

Chapter 5 Requirements specification for the Global Validation System, and proposal of a PKI trust model using Global Validation Authority, satisfying those requirements.

Chapter 6 Description of the evolution of the Validation Authority concept. Overview of the current state of the concept and its actual technical implementation.

Chapter 7 Evaluation and validation of the entire research. Focus on strong and weak points of all steps taken in the research.

Chapter 8 Summary of the entire work. Proposal of the further continuation of the research.

This thesis also contains a literature reference list included in the Bibliography at the end of the document, an Index listing all important concepts discussed in the research, and a vocabulary reference with the list of Acronyms used in this thesis. The Appendix also contains a detailed list of all interviews which contributed to the research.

Chapter 2

Public Key Infrastructure

This chapter describes the principles of public-key cryptography. It explains the essential definitions and concepts of Public Key Infrastructure. Finally, it presents PKI services, certificates and protocols.

2.1 Introduction to public-key cryptography

The concept of cryptography exists for as long as humans have been communicating with each other. People over thousands of years have developed many techniques for encrypting their communication and keeping it confidential from unwanted potential eavesdroppers [4].

Each of these old encryption techniques used a *secret key* which enabled to transform a meaningful message, known in the modern cryptography as *plaintext* into a very difficult to decrypt collection of words, letters or signs, called *cyphertext*. The same symmetric secret keys where used for both encryption and decryption of messages, and therefore those techniques were called *symmetric cyphers*.

It was relatively recently, in the mid-1970, when Whitfield Diffie and Martin Hellman introduced a new concept of *asymmetric cyphers*. They proposed a model where the key used for encryption and the key used for decryption would be different, but related to each other. Although their article "New Directions in Cryptography" [5] didn't give any precise example of such a cypher, their work was a revolutionary invention in the domain of cryptography.

2.1.1 Symmetric versus asymmetric cryptography

There exists many different symmetric cyphers and still many new ones continue to be invented. They vary from simple substitution cyphers to very sophisticated transformations, that allow to transform confidential data into cyphertext. Although those cyphers have many advantages such as small implementation size, and fast encryption and decryption [4], they have some inconveniences that are very difficult to overcome, especially in electronically based communication.

The main drawback of symmetric cryptography is the problem of exchange of a secret key which is used for both encryption and decryption (see figure 2.1). In order to keep a communication confidential, but understandable for its participants, it is very important to ensure that the secret key is not revealed to any third parties. Therefore, participants of a confidential conversation must first exchange the secret key in a secure way between each other, before they begin to exchange any encrypted messages.

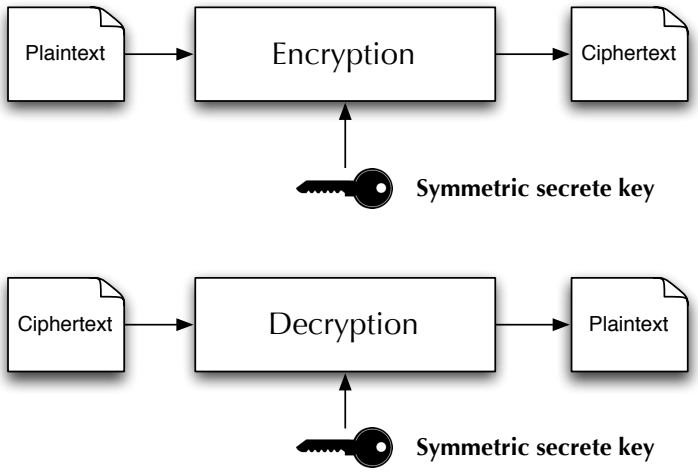

Figure 2.1: The principle of symmetric cyphers.

The problem of the secret key exchange highlights two main inconveniences of the use of symmetric cyphers :

- It is very difficult to ensure that a secret key exchange is secure, especially if there exist no secure channel of communication between the communicating parties.
- It is impossible to ensure a secure communication between unknown entities, because they need to exchange a secret key before they begin to communicate. The key exchange requires entities to trust each other. However, it is difficult to ensure

the identity of an unknown entity if one did not have any previous conversation with it.

Those two problems can be resolved when using asymmetric cyphers. Asymmetric cyphers consist of pairs of keys, where the recipient's *public key* is used for encryption and the recipient's *private key* is used for decryption (see figure 2.2). In this type of cyphers only the private keys must be kept secret to the recipients, whereas the public keys can be revealed to anyone who wish to send a confidential message to the recipients.

This is how in asymmetric cryptography communicating entities doesn't have to exchange confidential keys. The only confidential key is the recipient's private key, which is always kept private. On the other hand, in asymmetric cryptography a secure communication between unknown entities is possible, as any unknown entity to the recipient can send it a message using an available recipient's public key.

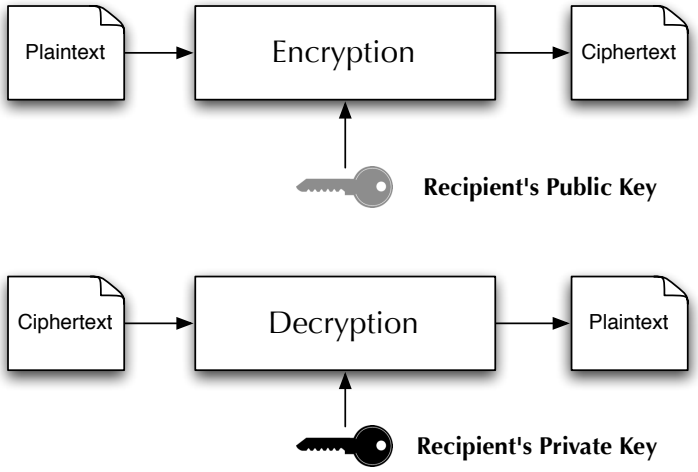

Figure 2.2: The principle of asymmetric cyphers.

The security of the asymmetric cryptography is based on the fact that it is computationally infeasible, for anyone except the creator of the key pair, to derive the private key by knowing only the public key [4]. Diffie's and Hellman's idea of making the encryption key public was so revolutionary that this asymmetric method of protecting confidential communication became known as *public-key cryptography*.

Finally, asymmetric cyphers have also solved the scalability problem of symmetric cyphers. In symmetric cryptography any secret key can be used only by one couple/group of confidentially related communicating entities. Therefore, in a community of n users up to $n^2/2$ secret keys can be required to use if every user wants to communicate confidentially with all the other users.

However, when using asymmetric cyphers the number of required key pairs does not exceed the number of recipients. Therefore the maximum number of key pairs in a community of n users, where every entity wishes to communicate with every other entity is n. That is how, when using public-key cryptography the number of key pairs required to ensure secure message exchange among communicating entities grows linearly to the number of those entities, instead of the exponential growth observed when using symmetric cyphers.

2.1.2 Public-key cryptography services

Public-key cryptography has enabled many new services which were not possible to achieve with symmetric cyphers. This section presents some of the most important services that have been developed with the use of asymmetric cyphers.

Security between unknown entities

Public-key cryptography allows unknown parties to communicate securely, if only the recipient's public key is known to the message sender and the understanding of underlying algorithms is achieved between communicating entities. Theoretically, the sender entity could look up the recipient's public key in a public repository and use it to encrypt the message it desires to send confidentially to the recipient.

It is however important for the sender entity to be sure that it uses the correct public key. Therefore, to find the correct public key the sender entity is required to use a trusted repository, or it must find a way to trust the information it has found in a public repository. The sender can often be obliged to perform an independent verification of a public key returned by the public repository.

In general, in the electronic world public repositories can not be trusted for the reason of unlimited possible network-based attacks that can result in data tempering. Therefore, all data contained in public repositories must be independently verifiable by their users, what is usually done with a use of a common mechanism known as public-key *certificate validation* [4].

Encryption

In public-key technology it is possible to encrypt data directly with a recipient's public key. However, this method is not often used in practice, because of its long time demanding computations, which are impractical in many environments [4]. Therefore, it is much more common to use a *two-step encryption* method.

In the first step of this method, the sender entity randomly generates a symmetric key with which it encrypts the message to be sent. Then, the sender uses recipient's public key to encrypt the symmetric key and to send it together with the encrypted message (see figure 2.3).

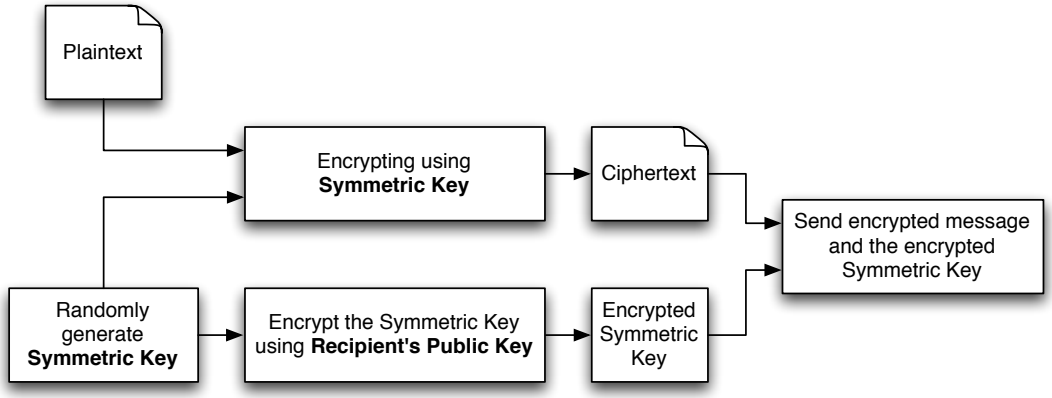

Figure 2.3: The principle of encryption using public-key algorithms.

At the reception, the recipient entity first decrypts the symmetric key by using its private key. Then it uses the decrypted symmetric key to finally decrypt the received message (see figure 2.4).

In order to keep the encryption coherent, this two-step encryption method is most often used even when the amount of data to be sent is small. That is how the recipient entity always knows, that the data it has decrypted with its private key is the symmetric key used to encrypt the confidential message, and not the confidential message itself.

As an example of two-step encryption, we can present a commonly used standard *Secure / Multipurpose Internet Mail Extensions (S/MIME)*. S/MIME provides cryptographic security services for electronic messaging applications, among others e-mail encryption. A user who wishes to send a confidential e-mail to many recipients, using

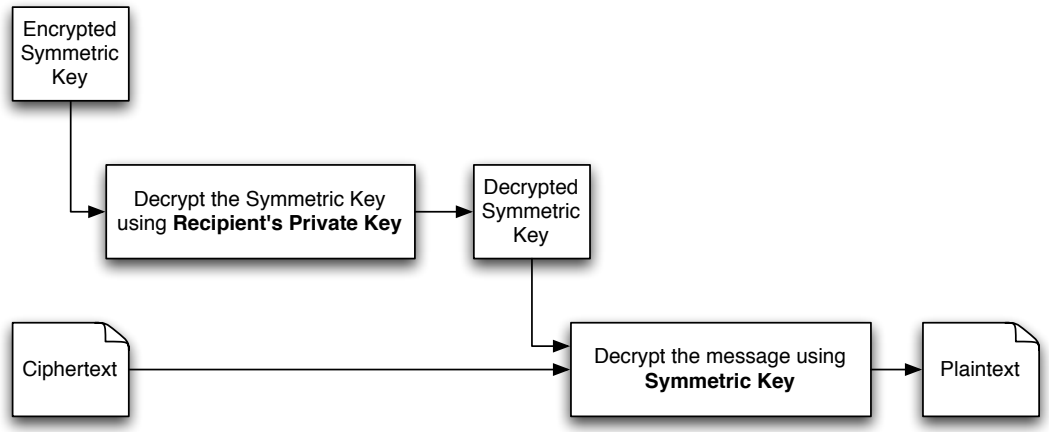

Figure 2.4: The principle of decryption using public-key algorithms.

the two-step S/MIME encryption, does not have to encrypt the entire message separately for every recipient with the recipient's public key. Instead, the sender encrypts the confidential message with a randomly generated symmetric key and then encrypts only the secret key for every recipient separately.

This solution simplifies the entire process of encryption by avoiding complicated multiple public-key operations on a plaintext. Besides, it ensures secure communication between message senders and recipients by using the combination of symmetric and asymmetric cyphers.

Digital signature

Public-key cryptography also allows different entities to sign certain data with a *digital signature*, which is equivalent to a handwritten signature. In this process, the signer entity uses its private key to encrypt some part of data, which can be then decrypted by anyone who knows the signer's public key. Since the signer entity is the only one that knows its private key, by performing a private-key transformation on a piece of data, it confirms that the data has been issued by this entity, and nobody else.

It is however important to point out that the private-key encryption takes a fixed amount of data as the input and it produces an output of precise size. Therefore, as the size of message to be signed varies, the sender must use a *cryptographic hash function* that transforms the message content into a fixed-size value [4].

Cryptographic hash functions play an extremely important role in PKI and therefore must be appropriately chosen and used. Hash functions, by principle, should transform two different inputs into two different outputs, in order to ensure that all messages encrypted with the same private key will have different forms (see figure 2.5). However, it happens that two distinct piece of data have the same hash value, what is known in PKI as a *collision*, because collisions are impossible to avoid when a large piece of data is being mapped to a short string, which is the hash value. Therefore, cryptographic hash functions should be chosen in a way that the probability of collisions occurrence is reduced to minimum.

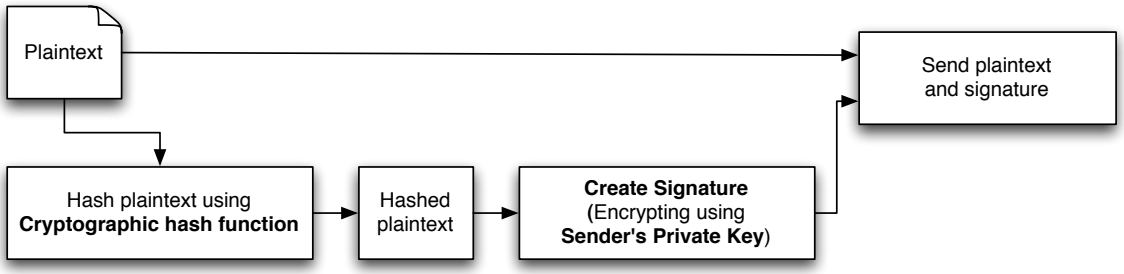

Figure 2.5: The principle of digital signature generation.

In order to verify a digital signature, the receiver must first hash the received message to a fixed value, by using the same cryptographic hash function as the receiver. Then, the receiver can decrypt the received signature, using the sender's public key, and compare the output of the decryption with the calculated hash value. The sender's signature is verified if those two values match.

XML syntax is often used to represent digital signature over any piece of data. There exists three types of digital signatures expressed in the XML format [6], which have different structures and which are the following (see figure 2.6) :

- *Enveloped signature*, which is embedded within the signed data.
- *Enveloping signature*, in which is embedded the signed data.
- *Detached signature or independent signature*, which is completely separated from the signed data.

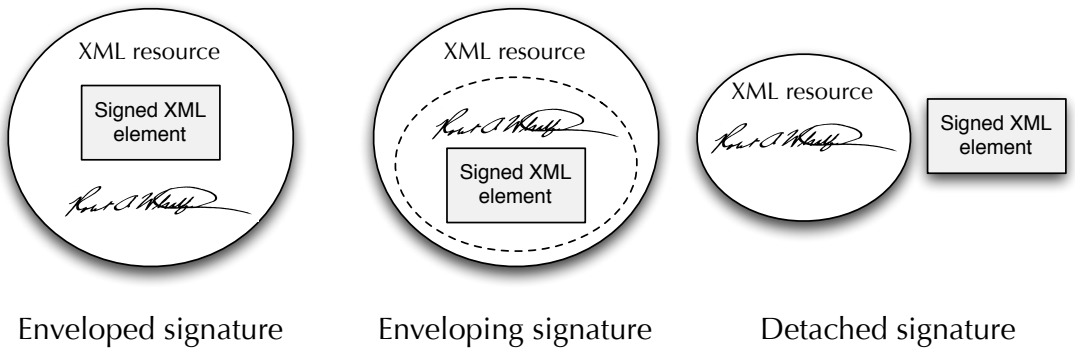

Figure 2.6: The three types of XML digital signatures.

Key establishment

Public-key cryptography also allows exchanging secret keys securely between two or more communicating entities. This exchange, called key establishment, can be done in two different ways :

1. *key exchange*
2. *key agreement*

Key exchange simply allows one entity to generate a secret key, encrypt it using the recipient's public key and send it securely over a communication channel. Key agreement, on the other hand, makes two or more entities participate in the creation of a secret key. One of the first public-key agreement protocol was Diffie-Hellman key exchange, where one of the two communicating entities uses its own private key and the public key of the other entity to create a symmetric key, impossible to compute by any third party entity.

Authentication

Authentication is a particular case of providing a security between unknown entities, where one entity needs to be identified by another. Public-key cryptography is extremely useful in remote authentication, when some authentication proofs must be sent over an insecure communication channel. By using a pair of asymmetric keys one entity doesn't need to send any sensitive authentication information exposing it to the risk of being eavesdropped.

An entity who wishes to get authenticated by a remote entity can encrypt with use of its private key a piece of data sent to it by the remote entity (see figure 2.7). This piece of data, often referred to as a *challenge* can be, after the encryption, sent to the remote

entity which will decrypt it using the sender's public key. If the decrypted message matches the original data sent by the remote entity, the sender gets authenticated, which means that its identity gets confirmed.

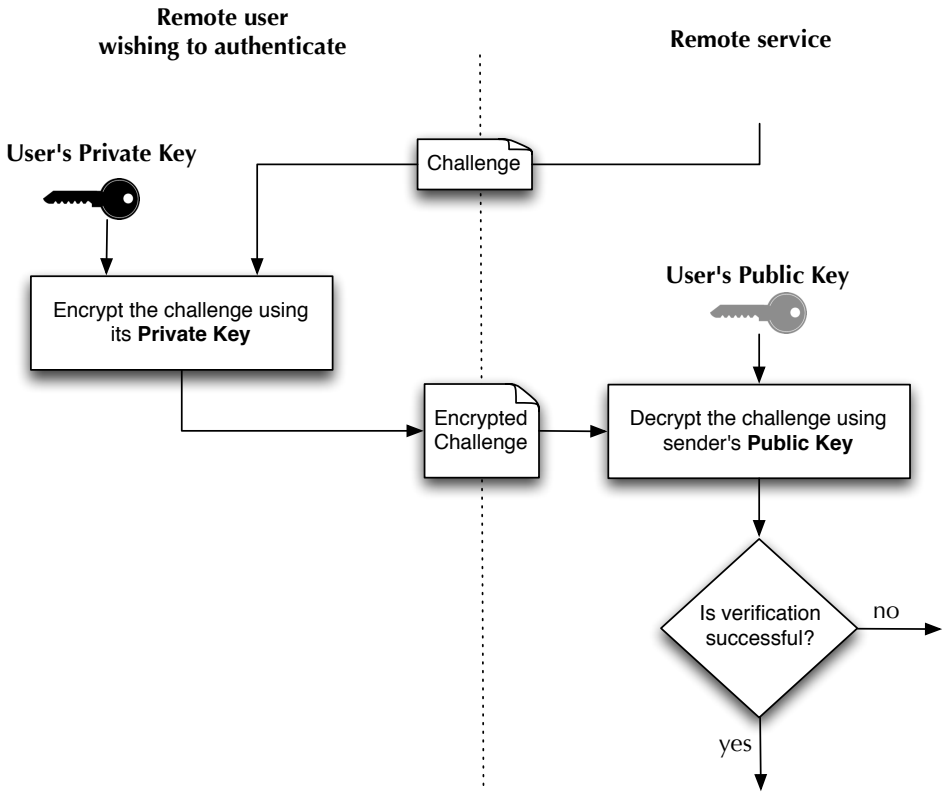

Figure 2.7: The principle of authentication using public-key algorithms (an example of a remote user authenticating to a remote service).

Data integrity

In general, PKI may provide data integrity in two ways :

1. By mean of a cryptographic hash function used with a digital signature, or
2. Using *Message Authentication Code (MAC)*.

Cryptographic hash algorithms, although essential for creating digital signatures, are also an extra integrity check on data which is sent from the signer to the receiver. The receiver can always be sure that if received digital signature is successfully verified, then the received data is also identical with the original one.

The second method of providing data integrity, called Message Authentication Code (MAC) algorithm, or keyed cryptographic hash function, typically uses a symmetric cypher. MAC algorithm takes as an input a fixed-length message and a secret key, generated by one of the communicating entities, and it produces a MAC that can be verified by the receiver.

There exists two alternative variations of MAC algorithms [4]. The first procedure consists of using a freshly generated symmetric key to compute a MAC for the data to be transmitted. Once MAC is computed, the sender can transmit to the receiver the desired data with MAC, and the secret key encrypted with the receiver's public key.

The other method uses the key agreement method to establish a symmetric key, by using the receiver's agreement public key and the sender's agreement private key. The data to be transmitted is consequently computed with the generated symmetric key creating a MAC. Finally, the data together with MAC and sender's public key is transmitted to the receiver.

Non-repudation

Non-repudation is a concept of making an action impossible to deny by any entity which was involved in performing it. This concept applies to electronic transactions that could possibly be denied by signing entities. Public-key cryptography makes non-repudation of digital signatures possible by providing unique private keys to the signing entities which strongly bind their identity to a particular key. However, to provide a complete service of non-repudation some specific infrastructure is required. For this reason, non-repudation is discussed more in details in section 2.2.9.

2.1.3 Public-key cryptographic algorithms

There exists many different cryptographic algorithms which are all used to implement different public-key cryptography services. They can be classified into three main categories :

1. asymmetric-key algorithms (public-key algorithms),
2. symmetric-key algorithms,
3. hash algorithms.

This section will briefly describe only some of the most important algorithms in the public-key cryptography. The presented algorithms are the most commonly used algorithms, usually together with other associated algorithms in order to provide complete

public-key cryptography services, or they are known for other important reasons. The following list is not exhaustive.

RSA

RSA is one of the earliest public-key algorithms. It was invented in 1977 by Ron Rivest, Adi Shamir and Len Adleman [7]. The security of this algorithm is based on the fact that it is computationally infeasible to factorize very large integers, but on the other hand it is easy to calculate a multiple of two large prime numbers. To make RSA algorithm secure according to the current research, RSA keys should be at least 1024 bits long.

RSA algorithm is suitable for encryption/decryption, for digital signing/signature verification, and for key establishment. Because of the fact that the key generation of RSA keys is carried out only occasionally, the computational efficiency of the algorithm is less of an issue [7].

RSA algorithm may show some weaknesses, if it is not properly used. According to [7], it should be avoided to use small encryption exponents, especially when sending an encrypted message to many recipients. This is because an eavesdropper of such encrypted messages can computationally manage to decrypt the plaintext. Besides, the same key pair should not be used for both encryption and signing. This is because signing a piece of data means revealing one's private key, that can be afterwards used by an unwanted entity do decrypt confidential messages, if they were encrypted using the corresponding public key.

DSA

Digital Signature Algorithm (DSA) , proposed by National Institute of Standards and Technology (NIST) in 1991, is a United States Federal Government standard for digital signatures [4]. DSA algorithm was invented specially for signing and verification, and is, therefore, also suitable for providing data integrity.

The security of DSA algorithm is based on the fact that it is difficult to compute logarithms in finite fields [4]. Therefore, DSA algorithm belongs to the domain of *finite field cryptography (FFC)*. NIST recommendations provides guidance and best practice for the use of cryptographic keys, e.g. they approve specific cryptographic hash algorithms. According to NIST recommendation [8], DSA keys should be 2048-bites long in order to extend their lifetimes beyond 2010, or 3072-bites long to extend keys' lifetimes beyond 2030.

DH

Diffie and Hellman (DH) algorithm, proposed in 1976 is the oldest public-key algorithm which still plays an important role in many Internet protocols, such as Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPsec) [9]. DH is a key agreement algorithm that is used to exchange shared secret key between two communicating entities.

DH algorithm belongs also to FFC algorithms, and it is based on relatively simple mathematical operations. Therefore, according to NIST standards [8] its length should be at least 1024 bits (preferably 2048 bits) in order to provide adequate security over some years.

DES

Data Encryption Standard (DES) was selected in 1976 as symmetric encryption standard in U.S. It is a is a *block cypher* with a 56-blit long key [10]. Block cyphers operates on a fixed-seize blocks and transform them into blocks of the same size. They can be contrasted with the second group of symmetric keys, called *stream cyphers*, which take only one bit of plaintext at a time, and where the transformation varies along the encryption process.

There exists a special form of DES called *Triple DES* or *Triple Data Encryption Algorithm (TDEA)* which applies DES cypher algorithm three times to each data block. This algorithms increases DES resistance to attacks by increasing the key length to 168 bits and they are mainly used in electronic payment systems.

AES

Advanced Encryption Standard (AES) announced by NIST in 2001 is a symmetric key encryption standard adopted by U.S. government [11], which replaced the previous U.S. standard : DES. This standard accepts three block cyphers : AES-128, AES-192 and AES-256.

SHA

Secure Hash Algorithms is a set of cryptographic hash functions published by NIST as a U.S. Federal Information Processing Standard [12]. SHA-0 and SHA-1 are the two earliest SHA algorithms and some important weaknesses and flaws have already been reported in them [13]. SHA-2 is a family of hash functions that composes of SHA-224, SHA-256, SHA-384 and SHA-512, where numbers symbolize the length of the hash algorithm output, also called *message digest*.

In 2007 begun the development of a new secure hash algorithm which is called SHA-3 [12]. SHA-3 algorithm is supposed to improve the properties of SHA-2 and be able to withstand successful attacks on SHA-2. However, the final selection of the SHA-3 algorithms was not yet done by NIST.

MD5

Message-Diges algorithms is a series of cryptographic hash functions, among which the MD5 algorithms is one of the most known functions, mainly because of its flaws. MD5 was designed in 1992 by Ron Rivest and it became a widely used cryptographic hush function. However, very soon first flaws in the algorithm were discovered, and further successful attacks on it made the further use of the algorithm questionable [14].

For this reason, it is important to underline that the MD5 cryptographic hash algorithm should no longer be used in public-key cryptography, as it is no longer secure.

2.2 The concept of infrastructure applied to public-key cryptography

Infrastructure can be defined as a structured support providing fundamental benefits on which associated services can be built. In the domain of security, a security infrastructure must provide a structured environment compatible with all applications and objects of an organization that requires the security.

Therefore, the main goal of the security infrastructure, as of any other type of infrastructure, is to act as an *application enabler* [4]. It means that the security infrastructure must have clearly defined entry points, through which it can provide security service to many applications/devices.

Public-Key Infrastructure (PKI) is a security infrastructure that implements and provides services using public-key cryptography techniques. Its structure contains many elements and concepts that need to be defined, in order to ensure the compatibility of the applications enabled by the infrastructure. This section defines important elements and concepts of the PKI, which will be constantly used in the following chapters of the thesis.

2.2.1 Certification Authorities (CA)

In order to ensure a secure communication, encrypted with a use of pubic-key algorithms, two communicating entities require a pair of asymmetric keys. This pair of keys must be issued by a trusted authority which can certify that the keys conform to some predefined security standards.

Institutions which can produce such asymmetric keys, and which can certify the keys owners' identities, in PKI are called *Certification Authorities (CAs)*. CAs certify that a particular public key belongs to a particular entity, by what is called *identity binding*. This identity binding is in fact the *public-key certificate*. CAs actually sign a certain data structure which contains some representation of the keys owner's identity and a corresponding public key [4] to provide public-key certificates.

2.2.2 Registration Authorities (RAs)

Registration Authorities (RAs), are optional systems or organizations to which CAs delegate certain certificate management functions. CAs can register new PKI end entities by itself, or they can delegate this task to independent RAs. RAs should be authorized by CAs to perform the assigned tasks concerning the life-cycle management of certificates issued by the CAs.

2.2.3 Certificate owner

The entity which purchases (or receives) a certain public-key certificate from a CA becomes a *certificate owner*. This entity can then use its certificate e.g. to produce digital signatures, to decrypt a confidential communication received from another entity, or to ensure data integrity of a received data (as described in the section 2.2.1).

For the purpose of this thesis, which focuses only on the digital certificate service of PKI, we will use the term *electronic ID owner (eID owner)* to refer to an entity, that needs to confirm its identity to another entity by providing its certified digital signature, which is an electronic ID.

2.2.4 Relying Party (RP)

Relying Party (RP) is the entity that wants to identify another entity, which uses its digital signature. An RP is often a service provider who needs to verify an end user's identifier, which in the case of this thesis, is an electronic ID. An RP, when it receives an electronic ID included in a digital certificate of an end user, it must make the decision

either to trust or not the certificate. For this reason, RPs directly rely on trust relationships they have with certain CAs, which issue certificates to end users that RPs need to identify.

It is, though, common that RPs receive certificates issued by a CA, which the RPs has no previously established trust relationship with. In this case, an RP can not rely on any direct agreement with a particular CA. It must instead perform a thorough verification of the received certificate according to the RP's own trust policy.

2.2.5 Certificate repository

Particular entities in order to communicate securely with each other, or to sign and verify their signatures, must be able to know each other's public keys. Those public keys, which are included in digital certificates should be available on-line to those who wish to communicate with the certificate owners. Therefore, *certificate repositories* are trustworthy, scalable and robust collections of those public keys.

2.2.6 Certificate revocation

Certificate revocation is a process of changing certificate status under particular circumstances. A trusted Certification Authority, which issued a valid certificate, may be obliged to revoke it, if for some reasons the certificate can not be trusted any more. It is important for Relying Parties to make sure that certificates they receive, even if they are still valid, can be used as secure identity bindings.

There are many reasons for which a certificate should be revoked. One example of such a situation can be that the certificate owner changed his/her name, or position in his/her organization, so his/her certificate no longer certifies his/her true identity. Another common example can be the private key getting lost, stolen or revealed to any third parties, so it is no longer secure to use.

In order to enable RPs perform correct certificate revocation, Certification Authorities should use an alerting mechanism, which updates certificate repositories used by Relying Parties, and guaranties a complete verification of any certificate issued by a trustworthy CA. Those repositories usually take the form of special lists called *Certificate Revocation Lists (CRLs)*.

2.2.7 Key backup and recovery

In order to protect any operational PKI environment against the problem of data inaccessibility, due to the loss of a private key, with should be used to decrypt data encrypted with a corresponding public key, PKI may provide a system of *key backup and recovery*. There exists multiple reasons for which a certificate owner can loose the access to the data protected by his/her private key. This may include e.g. forgotten passwords, destruction of a storage medium or a replacement of medium [4].

Because of those possible scenarios PKI should provide a service of private decryption keys backup, which would enable a decryption of data encrypted with a public key corresponding to the lost private key. On the contrary, a backup system for signing private keys is not necessary, as the certificate owner shall never use the signing private key to encrypt any data (see RSA in section 2.1.3).

2.2.8 Key updates and key history

Every public-key certificate has a finite lifetime [4]. Therefore, PKI should provide a system of continuos updates, in the best practice an automatic one, which would provide certificate owners with an easy way of always having one valid certificate.

Besides, PKI users must store their expired certificates, because they are often still needed to decrypt data that was encrypted in the past with a use of corresponding public keys. For this reason, PKI must provide to certificate owners a solution for *key and certificate history*, where users can find all their old private keys.

2.2.9 Support for non-repudation and time stamping

Public-key digital signatures are used to confirm one's identity while performing an action, that by principle should not be denied by the signing entity in the future. Therefore, PKI must provide a *non-repudation support* which can provide some technical evidence, that certain piece of data was signed by a particular entity at a particular time in the past.

The non-repudation support is crucial to business related operations, as it prevents different entities from breaking signed agreements by denying their signatures. Therefore, it is an important concept of the PKI, especially for the electronic ID.

One of the methods to provide a non-repudation support is *time stamping*. The concept of time stamping provides a trustworthy source of time for an entire PKI. Every data signed or encrypted by any of PKI users should contain an evidence of the time at which it was signed or encrypted. Although time stamping is the most important concept related to the non-repudation of a PKI, the trustworthy time source is also used in many other services enabled by a PKI.

2.2.10 Client software

PKI can often be seen as a structure with client-server architecture, where the server provides all services, such as certification services, revocation procedures, key updates and time stamping, and where clients request those services directly from the server. In PKI, all applications responsible for e.g. updating or revoking certificates, or stamping document, are connected to the client software and they use the infrastructure [4] to provide required services in cooperation with the server.

2.3 Public-key certificates

Public-key certificates issued by Certification Authorities are documents which uses digital signatures. Their two main purposes are :

1. identity binding, and
2. ensuring public-key integrity, when keys are distributed to many certificate repositories or different PKI users.

There exist many different types of certificates which all have different formats. In 1988 the Internet Engineering Task Force (IEFT) proposed first version of X.509 public-key certificate recommendations intended for the Internet community. The newest version of X.509 is called v3 and the last update of X.509 recommendations was done in 2002 [15], and it is the most common type of currently used public-key certificates. For this reason, we will discuss the pubic-key certificate structure, life-cycle and revocation procedures, basing on X.509 recommendations.

We should, however, underline that there exists also other types of public-key certificates, which are the following :

- *Attribute certificates (AC)*, also called *authentication certificates*
- *Simple Public Key Infrastructure (SPKI)* certificates

- *Pretty Good Privacy (PGP)* certificates
- *Secure Electronic Transaction (SET)* certificates

X.509 Attribute certificate [16] is a recommendation for use of attribute certificates (AC). This type of certificates is used for authorization purposes. ACs don't last for as long as traditional public-key certificates do. In the everyday life we can compare ACs to visas, whereas traditional pubic-key certificate to passports [16]. Those certificates are typically issued by different authorities and they are not similarly difficult to obtain. Besides, ACs cannot be issued to an entity who doesn't have a proper identification proof, therefore they are typically being attributed to entities that have a public-key certificate.

Although attribute certificates can be issued together with traditional public-key certificates, it is a common practice to make them separate from each other. The reason for this is, that AC coupled with public-key certificates, as a public-key certificate extensions, can shorten public-key certificates lifetime. Besides, public-key certificates issuers are generally not authorized to issue authentication certificates. Therefore, there is a need for separate authorization and authentication certificates.

Simple Public Key Infrastructure certificates were also developed to serve the purpose of authorization rather than authentication [17]. They were proposed to overcome traditional X.509 scalability problems and the high level of complication of separate authorization and authentication certificates. SPKI structure can be used to bind either names or explicit authorizations directly to keys, or indirectly through keys' corresponding hash algorithms or keys names.

Pretty Good Privacy (PGP) was first introduced by Phil Zimmermann in 1999. It is mainly used for protecting e-mails and stored files. Modern PGP, also referred to as OpenPGP relies on a trust model entirely deferent from X.509-based PKIs. Therefore, PGP certificates are completely incompatible with X.509 certificates. In PGP environment any user can create its own OGO certificate [18], and any user can act as a Certification Authority and validate another user's PGP certificate. Because of those major differences between PGP and X.509 environments, we will not focus on PGP certificates in this thesis. In practice, PGP certificates have different use than X.509 certificates, and therefore they don't apply to our scope of electronic IDs interoperability. For more details on PGP see [18].

The Secure Electronic Transaction (SET) is a defined standard to support credit card payment transactions over distributed networks, i.e. mainly the Internet [19]. SET is

based on the X.509 v3 format, but it includes its own private extensions that are not understandable for non-SET applications. Therefore, although SET defines payment standards protocol it can still introduce some interoperability problems in PKIs where SET and non-SET applications are supposed to work together.

2.3.1 Certificate structure

Disregarding the particular form of a public-key certificate, a public-key certificate must contain some essential information that can be used by its owner. The version 3 of X.509 contains the following elements (which are in principle common to all public-key certificates) :

- **Version** indicates the version of the certificate, in the case of X.509 it could be v1, v2 or v3, although version v2 is not commonly used.
- **Serial number** is a unique number within the issuer CA and it allows the certificate issuer to identify the certificate in a unique way.
- **Signature algorithm** specifies the algorithm that is being used to create the digital signature (e.g. SHA-1 with RSA).
- **Issuer** is an identification of the Certification Authority who issued the certificate. According to X.500 standards all PKI entities have their own *Distinguished Names (DN)* that are unique and therefore can be used as issuer and subject identifiers.
- **Validity** specifies from which date to when is the certificate valid.
- **Subject** is a DN of the certificate owner.
- **Subject Public Key** is the public key associated with the owner of the certificate.
- **Thumbprint algorithm** is the algorithm that is used to hash the certificate. It is used as an extra protection of the certificate and it is used together with the *thumbprint*.
- **Thumbprint** is the value of the hashed certificate. Any entity that is going to use the certificate can first verify it by hashing it with the included *thumbprint algorithm* and then compare the obtained value with the certificate thumbprint.
- **Extentions** were defined only for X.509 version 3 and they determine some additional associations of attributes with public keys, or users, and they provide methods for managing the certification hierarchy [15]. There exist two types of extensions : *standard extensions* for inter-domain use, and *private extensions* which are

defined for domain-specific use [4]. Extensions can also be divided into *critical* and *non-critical* extensions. Critical extensions have to be processed and understood by the RPs in order to use and validate certificates, whereas non-critical extensions may be ignored by RPs, if they can not be recognized [4].

2.3.2 Certificate life-cycle

Because of the limited lifetime of public-key certificates, their entire life-cycle must be managed by their PKIs. The related PKI should provide as much automated management as possible to make the certificate as much easy as possible in use and operate for the certificate owner, issuer CAs and RPs.

PKI shall support three stages of the public-key certificates' life-cycle : *initialization*, *issuance* and *cancellation* (see figure 2.8). In the *initialization phase*, an end entity must first register itself by establishing and verifying its identity with the CA or the RA. Then a key pair must be generated for the entity, including an important aspect of the future key pair location, as it has an important influence on the performance, assurance and usage of the keys [4].

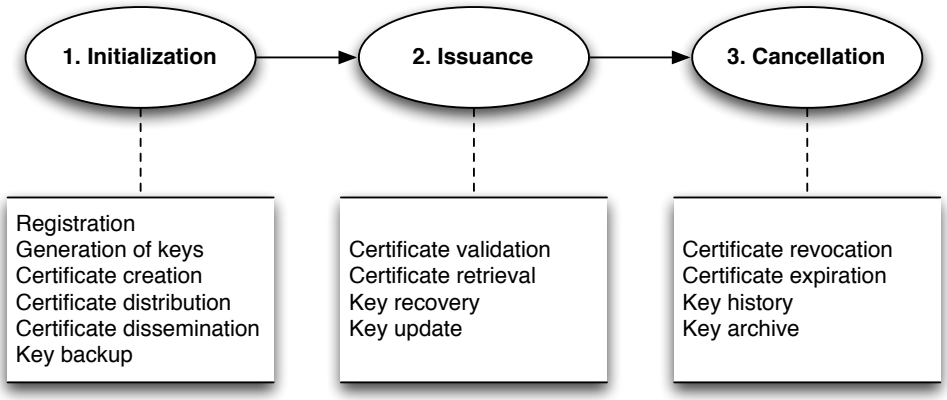

Figure 2.8: The life-cycle of public-key certificate and related certificate management.

After the pair of keys was created CAs shall bind them to the end entity identity by creating and distributing the public-key certificate. Then the certificate shall become readily available for intended recipients, which in the future will use it in the communication with the certificate owner. Finally, a private key backup may be created to be kept by a trusted third party (see section 2.2.8).

When the certificate enters into the *issuance phase*, PKI shall support its correct functioning with certificate retrieval and validation procedures. Besides, the key recovery shall be ensured by the PKI, as well as regular automated updates.

Finally, the certificate entering into the *cancelation phase* shall naturally expired. PKI shall provide a system of certificate revocation, i.e. an update of corresponding CRLs. All information concerning the expired key shall be included into the key history, which shall be stored in a corresponding key archive.

2.3.3 Certificate revocation methods

As described in the section 2.2.4, Relying Parties, before accepting any public-key certificate, are obliged to verify the certificate validity. For those reasons, RPs shall consult Certificate Revocation Lists (CRLs) created by particular CAs to verify the validity of certificates which are not expired. CAs complete those lists with information concerning all issued certificates, which for various reasons were revoked.

There exists several types of CRLs. According to [4], we distinguish two main types of CRLs :

1. *Certification Authority Revocation Lists (CARLs)* are used to store information about the Certification Authority certificates, which were revoked. Those lists do not contain information about end user certificates, and they shall be available for all entities involved in the PKI containing the CA.

2. *End entity Public-key Certificate Revocation Lists (EPRLs)* contain information about end entity certificates issued by one CA, which have been revoked.

However, all types of CRL can also be classified into two groups, according to their coverage of the PKI domain (see figure 2.9) :

1. *Complete CRLs* contain all revocation information concerning one CA domain. They are often used when the number of subordinate CAs in the trust structure is not too high, because in large domains those lists may become voluminous, thus difficult to use for RPs.

2. *Partitioned CRLs* are easier to manage, as they contain revocation data concerning only a part of the PKI domain. If they are used with good location indications they can help RPs easily find information concerning particular certificate without having any previous knowledge about the list.

In general, any RP, in order to find revocation information about a particular certificate, shall be able to localize the corresponding CRL. This is done by a use of *CRL Distribution Points (CDP)*. Distribution Points are special extensions in digital certificates which point out the location of the corresponding CRL.

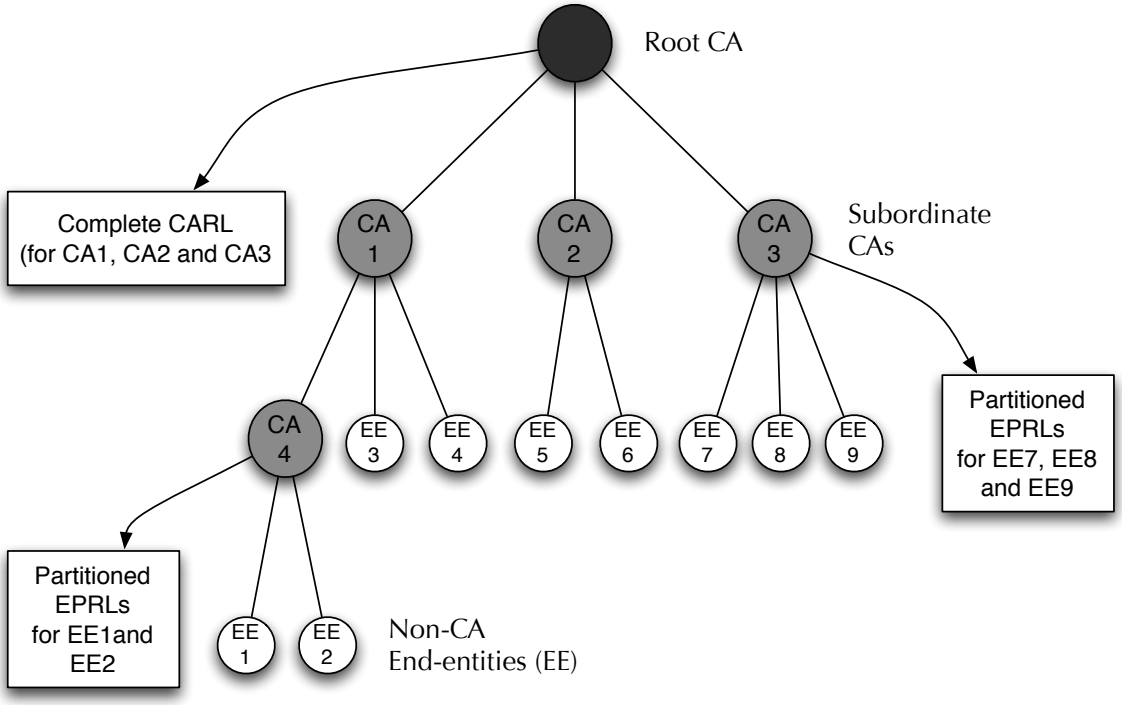

Figure 2.9: An example of different types of CRLs, in a hierarchy of CAs trust model (sees section 3.2).

There exist, however, different ways to organize and localize CRLs, depending on particular characteristics of a certain PKI domain. Regular Distribution Points associate statically partitioned CRLs to digital certificates, for their entire life-cycles, which in some cases can be undesirable. This is because a large distribution of partitioned CRLs makes certificate path validation difficult for RPs. Therefore, we distinguish some other types of CRL Distribution Points and organization of Certificate Revocation Lists, such as :

- *Redirect CRL* are *dynamic CRL Distribution Points*, which make the location indication of certificate revocation information change throughout the certificate lifetime.

- *Delta and Indirect Delta CRLs* are based on the increments and time reference of CRLs. Certificate revocation information may be found in such lists by referencing the base of the CRL or by referencing a particular point in time, and thus finding recent updates of the revocation information.
- *Indirect CRLs* allow to combine into one list CRLs issued by separate CAs within one PKI. Those lists are most often used to make for RPs finding revocation information easier within one PKI.
- *Certificate Revocation Trees (CRTs)* use hash trees to represent revocation information concerning a group of PKIs. Hash trees contain separate sequences of expresions generated for each issuer CA included in the PKIs, making it easier to find revocation information concerning end user certificates issued by the CA in the entire PKI.

2.3.4 Certificate Policy and Certification Practice Statement

Certificate Policy (CP) and *Certification Practice Statement (CPS)* are important documents in PKIs. They describe requirements and corresponding procedures regarding the issuance, management, usage, revocation and renewing of digital certificates. A CP specify requirements for the applicability of a certificate for a particular purpose i.e. a particular community or a class of applications with common requirements, which can e.g. correspond to different levels of assurance.

Internet X.509 Public-Key Infrastructure Certificate Policy and Certification Practices Framework [20] provides the list of topics that should be included in a CP. This guidelines contain requirements concerning all : the technical, business and legal issues regarding the certificates' life-cycle operation that should be included in both CPs and CPSs.

A CPS is a statement describing how the requirements specified in the corresponding CP are being met by the issuer CAs. A CPS explains practices regarding certificates' life-cycles services and management. Usually one CP and one CSP is written for each issuer CA. Those documents can be used by any third party to assess the quality of a certificate issued by the corresponding CA, therefore they can be used in the certificate validation process. CPSs may, however, contain sensitive information concerning detailed issuer CA security practices. Therefore, CAs may sometimes decide not to reveal publicly their entire CPS, in order to avoid exposing themselves to potential attacks.

2.4 PKI protocols

In this section we will briefly describe different groups of PKI protocols, basing on X.509 Recommendations issued by IETF [21]. There exists, according to [21], three groups of PKI protocols :

1. **Operational protocols** which are responsible for certificate and CRL distribution in the PKI [22]. They include e.g. *HTTP*, *FTP*, *S/MIME*, *Lightweight Directory Access Protocol (LDAP)* and many other protocols.

2. **Management protocols** which are responsible for service messages exchange used in certificate life-cycle management [23]. Those protocols include e.g. *Public-Key Cryptography Standards (PKCS)*, *Certificate Management Protocol (CMP)* [24] and other protocols.

3. **Validation protocols** which are responsible for validation of different PKI objects. *Online Certificate Status Protocol (OCSP)* is a simple request-response protocol than enables revocation of a certificate by consulting a trusted CRL. There is being also developed *Simple Certificate Validation Protocol (SCVP)* which is supposed to significantly simplify the RPs obligation when validating a certificate, and *Data Validation and Certification Server (DVCS) Protocols*.

2.5 Summary

Public-key cryptography is an asymmetric cryptographic technique which was invented in mid-1970, and which revolutionized the domain of cryptography. It offers many services, such as : security between unknown entities, encryption, digital signatures, authentication, data integrity and non-repudation, some of which were not available with the old symmetric cryptography techniques. Although public-key cryptography was an innovative concept, that set a new direction in cryptography, it actually combines many types of cryptographic techniques and algorithms i.e. asymmetric-key algorithms, symmetric-key algorithms and hash algorithms.

This chapter introduced the concept of Public-Key Infrastructure (PKI), which acts as an application enabler providing different public-key cryptography services. PKI contains many elements which are involved in the management of digital certificates during their entire life-cycles. This chapter described different types and purposes of digital certificates. It also explained important concepts related to certificate management, such as certificate revocation, Certificate Policy and Certification Practice Statement. Finally, this chapter described different PKI protocols used to support operation, management and validation of digital certificates.

Chapter 3

PKI Trust Models

This chapter presents different PKI trust models and related public-key certificate management. It discuss advantages and drawbacks of different approaches and shows why currently available PKI trust models are not suitable for large scale eID interoperability.

3.1 Introduction

One of the most important functions of Public Key Infrastructure is to provide and manage trust relationship between different PKI entities. Relying Parties, in order to be able to validate end user digital certificates, follow their own trust policies, which are all based on different *trust models*.

Because the number of public-key certificate providers continuously grows in size, many RPs become more and more troubled with deciding which Certification Authorities to trust, especially if they have no direct agreement or any previous communication with some CAs. Besides, more and more CAs begin to issue certificates on large scales, exceeding their local domains. Therefore, more and more RPs are obliged to build up broad trust networks in order to validate various *certification paths*.

A certification path is a chain of certificates, established from a trust anchor to the certificate owner over a particular trust model. Every certificate included in a particular certification path should get validated by an RP, in order to accept the public-key certificate of an end entity. That is how RPs depend on chains of CAs. Those chains begin with reliable trust anchors, that is an established point of trust, and continue through intermediary CAs till end entities owning particular certificates [25].

Over recent years, we observed several types of those PKI trust networks being developed on large and small scales which can be described as *PKI trust models* [26]. According to the paper titled : *"Trust Models and Management in Public-Key Infrastructure"* [26] we can classify existing PKI trust models into five following types :

1. *Subordinate hierarchy of Certification Authorities*
2. *Cross-certified mesh* of CAs
3. *Hybrid model*
4. *Bridge CAs*
5. *Trust lists*

The following sections of this chapter will describe and discuss each of these trust models separately.

3.2 Subordinate hierarchy of Certification Authorities

One of the oldest PKI models of trust, that was developed with early X.509 recommendations, is a subordinate hierarchy, also referred to as *strict hierarchy of Certification Authorities*. This structure consists of one well-known and trusted root CA, from which its subordinate CAs descend (see figure 3.1). Those intermediate CAs must know the root CA's public key which is included into end entities' certification paths and acts as a trust anchor for all subordinate CAs end entities' certificates.

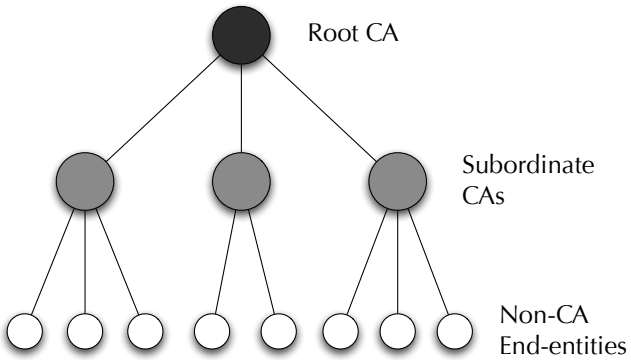

Figure 3.1: Strict subordinate hierarchy trust model.

Because of the root CA's public key role in building certification paths of all hierarchy participants, the corresponding private key should be carefully protected. For this reason, in the best practice, the root CAs may often stay off-line, in order to limit the possibility of compromising their private keys [26].

However, root CAs still participate in the certificate revocation of their subordinate CAs. CRLs containing the revocation status of subordinate CAs are stored off-line in safes, and they are being modified manually approximately every 6-12 months. Those CRLs are usually not long, comparing with CRLs of every single subordinate CA. Therefore, relatively rare manual updates of root CAs' CRLs does not pose problems for the correct functioning of the certificate revocation in the whole hierarchy.

Among the most important advantages of the subordinate hierarchy trust model we shall mention the following :

- **applicability to isolated, hierarchical enterprises** because of its hierarchical structure
- **simple certification path construction**, as the traversal of the hierarchy trees is very simple, from the root to any leaf
- **tight control** over certification paths, as all CAs that certify a particular certificate are in a strict relationship with each other (each subordinate CAs has only one superior)
- **unique certification paths**, as there is only one valid path to any leaf in a hierarchy structure
- **easy certification path acceptance within the structure**, as any entity within the structure accepts a certificate issued by any other CA within the same structure, because all CAs are approved by the root CA

However, the subordinate hierarchy trust model has also many disadvantages. The most important drawback of subordinate hierarchies is the fact, that it is often difficult to apply this model to a structure composed of many equal CAs. This is mainly because it is difficult to find one entity which all communicating entities would trust, and it is also difficult to compromise similar trust policies among all those entities [26]. To overcome these problems, two main variations of strict hierarchy trust model were introduced, and these are : *loose hierarchy of CAs* and *policy-based hierarchy of CAs*.

3.2.1 Loose hierarchy of CAs

The concept of loose hierarchy allows any pair of entities, within one hierarchy model, to build a trust relationship between them without being obliged to construct a full certification path beginning at the root CA [4]. For example, two entities owning two certificates issued by two CAs which have the same superior root CA, shall mutually trust each other without having to check their entire certification paths, as the two CAs mutually trust each other (see figure 3.2).

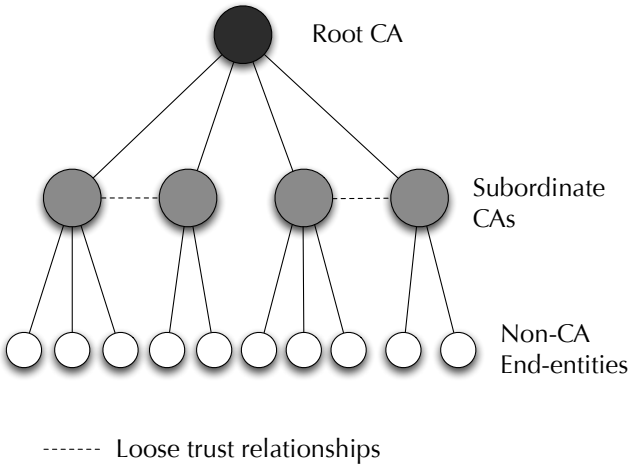

Figure 3.2: Loose hierarchy trust model.

This solution, in some cases, could simplify the certificate validation process for the RPs, and would make the hierarchy trust model more applicable to many PKI environments, which are not structured in a purely hierarchical manner.

3.2.2 Policy-based hierarchy of CAs

Another variation of the subordinate hierarchy model is a policy-based hierarchy where any subordinate CA can have more than one superior [4]. It means that any CA could belong to many different trust policies, as it could be part of more than one hierarchy. This solution makes many certification paths, thus certification path verifications, possible for one certificate.

The policy-based hierarchy, in general, reduces the negative impact that a compromised root CA's private key could have on the entire structure. Some certificates, which have a multiple certification path, could still, in this case, be validated by using another

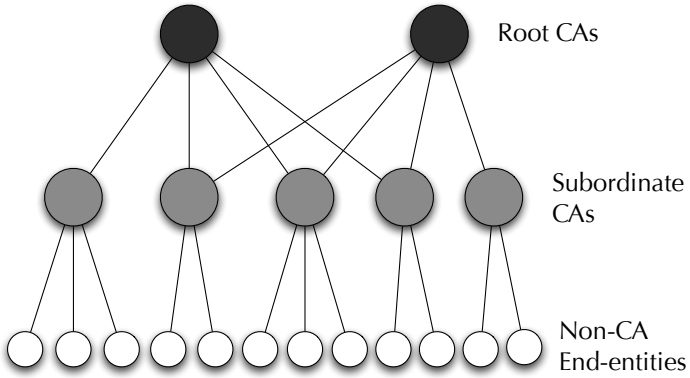

Figure 3.3: Policy hierarchy trust model.

root CA certificate. Besides, this model encourages the diversity of employed trust policies within one PKI, including e.g. possible variety of used public-key lengths, and PKI algorithms.

3.3 Cross-certified mesh

Cross-certification is a binding between two CAs which certify one another mutually. Depending on wether the two CAs belong to one or two different domains, we can distinguish between two types of cross-certification : *intra-* and *interdomain cross-certification* [4]. Cross-certified mesh are any trust networks where such relationships exist, and therefore the concept of cross-certified mesh trust model is wide.

According to [27], we can also distinguish between two main cross-certification methods : *peer-to-peer cross-certification* and *hierarchical cross-certification*. The distinction can be done by looking at where the client application places its trust anchor. On one hand, if a user considers its local CA to be its trust anchor, then any cross-certification of this CA with another one will be considered as a peer-to-peer cross-certification. On the other hand, if the user considers a superior CA to its local CA a trust anchor, then the local CA can only add subordinate CAs to the structure by hierarchical cross-certification.

The cross-certified mesh model has many advantages, the main are :

- **adaptability to dynamically changing organizational structures**, as it is relatively easy to add or remove a CA from the trust network. It is also easy to modify the trust network if any CAs establish a new cross-certification, or any CAs break their mutual cross-certifications

- **ability to extend trust among many distinct PKIs**, as it is easy to use transitive trust relationships over a pair of iterdomain cross-certified CAs
- **possible control of cross-certifications** with use of specific cross-certification policies (see section 3.3.1)

However, mainly because of the scale to which a cross-certified mesh may grow, this trust model presents some major disadvantages. The most important drawbacks of cross-certified mesh are the following :

- **inappropriate cross-certifications** may happen as any CA is allowed to certify any other CA, and it may happen that CAs which doesn't have the same certificate policies cross-certify without verifying their mutual policies
- **not uniformly trustworthy certification paths**, as it is often impossible to identify CA's policy only by looking at CA's name included in the certification path [26]
- **no acceptance of valid certification path** can happen, when certain verifiers don't accept one of multiple certification paths possible for one certificate, because e.g. of a lack of information about all CAs involved in construction of one of possible certification paths for the certificate
- **difficult certificate processing**, which, depending on the length of the certification path, can become time and resource consuming

3.3.1 Cross-certification policies

Because cross-certificaton is mainly used to extend trust to another CA, it is important to make sure that both CAs involved in the cross-certification share the same definition of trust. Therefore, it is often convenient to define the level of trust of a cross-certification depending on specific business situation of two involved PKI entities. This mainly apply to disparate organizations, which have specific and limited business relationships, and which must take precautions before trusting any other CA [27].

Therefore, CAs wishing to cross-certify have the possibility to control to which extent they will trust themselves. The level of control can be suitably chosen based on each CA's private business relationships, and can take one of the following forms : *path-length constraints*, *name constraints* or *policy constraints*.

Path-length constraints

Path-length constraints are generally used to limit the transition of trust over consequent CAs cross-certifications. In the case of peer-to-peer cross-certifications, this constraint can be used e.g. to limit the trust only to the closest cross-certified CAs. In the case of hierarchical structure, path-length constraints may be used to limit the possibility of adding new subordinate CAs by any other intermediate CAs. This constraint is particularly important for hierarchical structures, as all entities belonging to one hierarchical trust model trust each-other [27], so it is important to define which intermediate CAs can add new subordinate CAs.

Name constraints

Name constraints can be used to delimit the trusted CAs to a particular sub-group of an organization by specifying a DN, or a part of it, which should be trusted. This situation can apply, e.g. to large organizations, where only some organizational units should be included in a cross-certification agreement. This constraint has approximately the same importance and use in both peer-to-peer and hierarchical cross-certification methods.

Policy constraints

Finally, the policy constraints may be used to limit the way and the purposes for which cross-certified certificates may be used by cross-certified CAs. Policy constraints allow CAs, which e.g. deserve differentiated groups, to cross-certify according to their different levels of assurance. For example, if one organization, because of its business relationships, wishes to cross-certify with only the high assurance group of users of another organization, then this can be done with the use of a particular policy constraint [27].

3.4 Hybrid model

Hybrid model is another PKI trust model, which is based on the combination of hierarchies of CAs and a cross-certified mesh. This model consists of separate, subordinate hierarchies of CAs, where the root CAs are cross-certified with each other, creating a cross-certified mesh (see figure 3.4). In some publications, hybrid model is also referred to as *distributed trust architecture* [4].

The main advantage of this trust model is that, on one hand, separate PKIs can preserve their hierarchies, and thus strictly control the certification paths of all their end entity certificates (see section 3.2). On the other hand, each separate hierarchy can

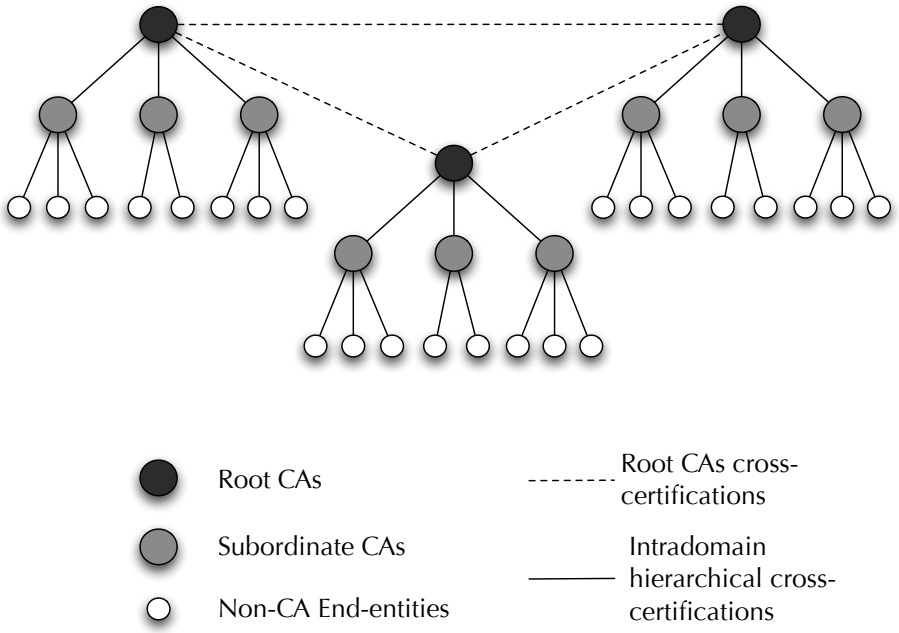

Figure 3.4: Hybrid trust model.

reach any other hierarchy by a simple peer-to-peer cross-certification of the root CAs [26].

It is also important to underline that, in hybrid model cross-certification of subordinate CAs is also allowed, like in a loose hierarchy model [26]. Therefore, the hybrid trust model is very flexible, and, that is why, it can be applied to many PKIs. However, on a large scale it does not solve problems of large cross-certified mesh.

In order to achieve a global interoperability with a use of a universal hybrid model, all separate root CAs should cross-certify with each other. This demands an enormous amount of agreements to be achieved among root CAs. Achieving those agreements, in some cases, may be very difficult and time consuming, however, long certification paths, required when not all root CAs are interconnected with cross-certification agreements lead to long and resource consuming certification path processing by RPs. Therefore, the hybrid trust model, although advantageous on a limited scale, can not be considered as a solution for global PKI interoperability.

3.5 Bridge CAs

The bridge CA trust model improves the hybrid trust model applied on a large scale. In the case where many separate hierarchies of CAs exist, it is convenable to implement one central entity, called a *bridge CA*, which could cross-certify with all root CAs, reducing the number of cross-certifications in the entire trust model (see figure 3.5). The maximum possible number of cross-certifications in a bridge CA model with n root CAs is n, whereas in the hybrid model it can rise up to $n^2/2$, if all n root CAs wish to cross-certify with each other.

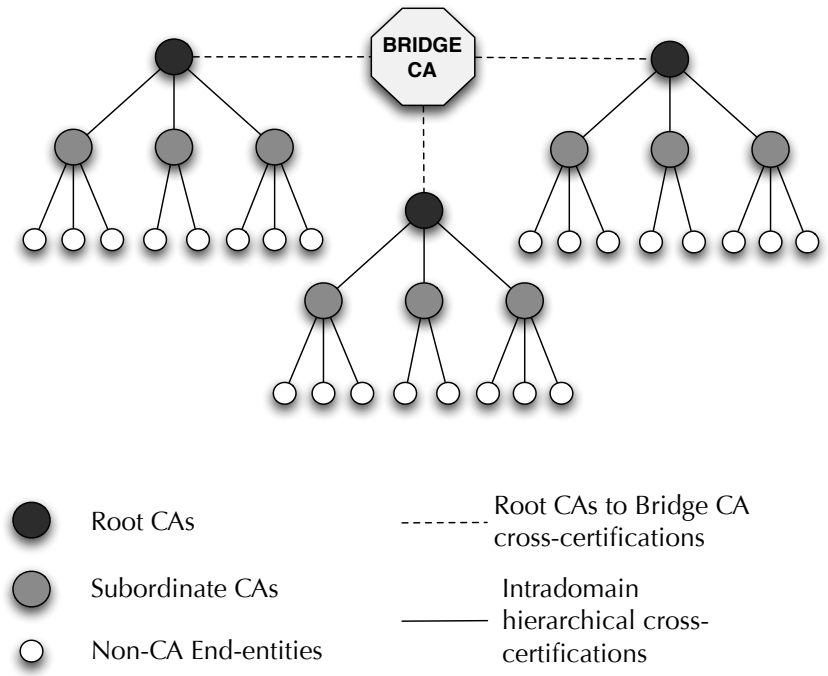

Figure 3.5: Bridge CA trust model.

The bridge CA is a central cross-certification authority connecting the root CAs via peer-to-peer cross-certifications [26]. Any organization or company, which cross-certifies with a use of a bridge CA can easily construct certification paths, and validate any paths certified by other root CAs, which also cross-certified with the same bridge CA.

In order to preserve the quality of cross-certifications, the bridge CA may define its own trust policies, and e.g. classify different cross-certified CAs, by matching the corresponding cross-certification agreements to different levels of assurance. US Federal

Bridge CA (FBCA), for example, has defined its own five-level trust policy [28] (see section 4.3.1). Other existing implementations of bridge CAs in the world also have their own trust policies. In the chapter 4 we present more examples of bridge CAs implemented in Japan and Germany.

The bridge CA trust model first appeared to be the best interoperability solution for large networks of PKIs [26]. However, while numerous bridge CAs were being simultaneously implemented, it turned out that the global interoperability is nearly impossible to achieve, as many bridge CAs' trust policy frameworks are too different from each other [3]. Therefore, this trust model could in theory be regarded as a possible solution to achieve global interoperability, however when put into practice it proves the opposite.

3.6 Trust lists

Trust lists are one of the most commonly used trust architectures today [29]. They can take various forms and, therefore, they are difficult to define. However, in most cases trust lists consist of named CAs and their public keys [3]. According to [29], they can be divided into two groups :

1. *user trust lists*, that are being managed by single users
2. *provider trust lists*, that are being managed by an external trust provider

An example of a user trust list is the hundred CAs list included in distributions of Microsoft OSs [29]. Because most of the users do not have necessary means or abilities to construct their own trust lists on their own, they are often being provided with applications, like e.g. web browsers, which already contain some trust lists. End users may however modify those lists according to their private trust policies, by adding or removing certified CAs from those lists.

In general, the main difference between trust lists and any other PKI trust model is that trust lists move the trust management from intermediary CAs directly towards the end entities [26]. Therefore, according to [26], those lists are very useful among small number of universally known and trusted CAs, e.g. for the signers of SSL server certificates, or in small domains, such as e.g. within one organization or a predetermined group of enterprises.

Preparing and managing trust lists demands, however, some PKI knowledge, but, in the real life, most of the end entities who uses trust lists have not enough competences to take trust decisions on their own. Therefore, they rely on software providers, who

often incorporate trust lists into their applications. In general, those software providers, however, do not specialize in PKI ether, and therefore, they shall not be considered as reliable impartial third party trust anchors. Besides, they most often do not take on any liabilities for certificates issued by CAs included in their trust lists.

For those and other reasons, trust lists, can not be considered as a solution to global PKI interoperability. There exists some trust lists, such as the european IDABC Bridge/ Gataway CA (EBGCA) that contains nationally approved certificate issuers, and which takes on some liability regarding the RP [3]. However, on a large scale trust lists require extensive management [26], without necessarily taking on the liability [3], and therefore are not a suitable solution for global PKI interoperability.

3.7 Gateway CAs

A new PKI trust model based on gateway CAs (GWSA) was proposed in the paper titled : *A New Trust Model for PKI Interoperability*, at the Joint International Conference on Autonomic and Autonomous Systems in 2005 [30]. The goal of this model was to solve the problem of the global PKI interoperability.

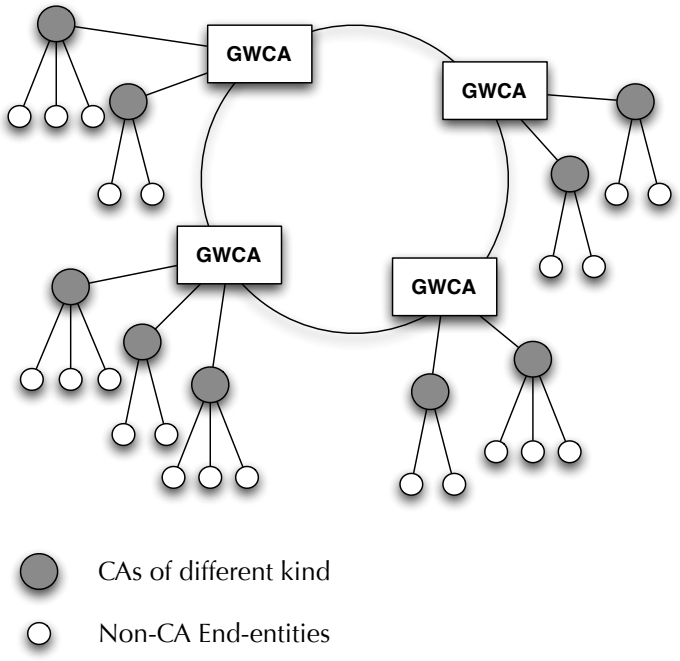

Figure 3.6: PKI trust model using gateway CAs.

Gateway CAs are trust anchors that are connected in a ring in a global trust network [30]. Those gateways allow CAs to certify to other CAs which are placed anywhere in different trust sub-networks within one network (see figure 3.6). According to [30], this trust model is based on the following principles :

- If an end entity trusts one GWCA, it can trust all others GWCAs connected on the same ring.
- GWCAs on one ring behave like one single root CA divided into several parts. Those parts, which are separate GWCAs, can trust each other without needing to cross-certify. For this reason all GWCAs are supposed to have the same public key to be able to verify their signatures mutually.
- GWCAs can provide certification services according to their intermediate CAs.

This model is currently, however, purely theoretical. According to the authors of this proposal [30], there exists no public-key generating algorithm today which could create a set of key-pairs, that could be used by GWCAs in a secure way. The Gateway CAs trust model requires that all GWCAs on the same ring share one public key, whereas each of them keep its own private key, which should not be compromised.

For this reason, this solution must wait until new key pair generation algorithms become invented and implemented first. Therefore, we can not consider GWCAs to be a potential solution to global PKI interoperability today, because we cannot estimate the amount of time that is needed to put GWCAs into practice.

3.8 Summary

This chapter presents six different PKI trust models, both those that are commonly used nowadays e.g. trust lists or hierarchies of CAs, as well as e.g. Gateway CAs which remains a theoretical model. We tried to present advantages as well as disadvantages of all those solutions trying to explain why none of them could satisfy the current need of eCommerce and eGovernment for global PKI interoperability. The table 3.1 summarizes the most important characteristics of PKI trust models presented in this chapter.

All presented PKI models were described based on a literature study of available standards and publications. More practical approach to many PKI trust models and different interoperability initiatives is presented in the next chapter 4.

Table 3.1: Comparison among different PKI trust models.

PKI Trust Model	**Trust anchor**	**Interoperability support**	**Strong points**	**Weak points**
Subordinate hierarchy	Hierarchy root CA	Good interoperability within the hierarchy; weak beyond the root CA	applicability to hierarchical enterprises; tight control; simple path construction and acceptance	difficult to adapt to non-hierarchical structures; difficult to compromise trust policies among many CAs
Cross-certified mesh	Local CA	Good interoperability through moderate number of CAs; high complexity on large scale	dynamical adaptation to changing structures; possible control of cross-certification by choosing different constraints	risk of inappropriate cross-certifictions; difficult certification path processing
Hybrid model	Hierarchy root CA or local CA	Good interoperability through moderate number of root CAs; high complexity on large scale	combination of strong points from both : subordinate hierarchy model and cross-certified mesh	complexity on large scale related to high number of needed cross-certifications
Bridge CAs	Local CAs	Good interoperability on large scale if CAs' policies are not different from each other	reduces the number of cross-certifications; preservation of cross-certification quality by defining bridge CA trust policies	difficulty of compromising CAs policy frameworks on large scale
Trust lists	CAs listed as acceptable signers	Good interoperability for well known and trusted CAs	large spectrum of possible implementations; useful among groups of universally trusted CAs	require extensive management, if applied on large scale; can't be trusted if managed by poorly qualified entities

PKI Trust Model	**Trust anchor**	**Interoperability support**	**Strong points**	**Weak points**
Gateway CAs	Gateway CAs	Good interoperability for a moderate number of GWCAs	easy certificate path construction and acceptance	lack of possible implementation solutions according to the current research

Chapter 4

PKI Interoperability in Practice

This chapter presents different aspects of the PKI interoperability in practice. It discusses standardization efforts and interoperability initiatives in various countries. Finally, it describes weaknesses and vulnerabilities related to those interoperability practices, and existing deployment obstacles.

4.1 Introduction

Ensuring PKI interoperability is a complex process which involves agreements among many PKI entities. It demands close cooperation among both private and public institutions. Those organizations shall work together in order to develop interoperability initiatives and to elaborate various *standards*. These standards and interoperability initiatives, which are a result of long negotiations and compromises, are often difficult to achieve, and sometimes they even more difficult to put into practice.

In the multivendor domain of PKI, achieving interoperability is closely related to standardization activities. Standards are necessary but not sufficient in guaranteeing multivendor PKI interoperability [4]. Their purpose is to provide common basis for various implementations, such as establishing common PKI definitions and specifying PKI syntax to be used in precise contexts.

Standards, however, are simultaneously elaborated by many different organizations, committees and working groups, which are often voluntary in nature. Therefore, some standards happen to be of different qualities and they also can take various forms. Some standards may appear to be too specific, whereas others may be too vast, leading to many possible interpretations. In order to avoid important misinterpretations, all standards which focus on PKI interoperability, shall satisfy three groups of PKI requirements for interoperability.

The larger the variety of available PKI standards, the more difficult it is to guarantee the PKI interoperability. In order to avoid issuing PKI standards which lead to interoperability problems, standardization organizations should consider satisfying different requirements for interoperability, which, according to [31], can be classified into the three following groups :

1. **technical requirements** specify PKI technology that shall be used, such as e.g. PKI algorithms and PKI protocols,
2. **operational requirements** specify operational procedures for CAs, e.g. certificate validation or cross-certification methods,
3. **legal requirements** specify signature laws, which should be investigated, and which should be specified in CPs and CPSs according to legislations in different countries.

Only by satisfying requirements from the three groups, a realization of interoperability among PKIs is achievable. We also consider this requirements classification, when specifying requirements for our solution for PKI interoperability, in the section 5.2.

In the following sections we discuss different PKI standards activities and existing interoperability initiatives. We also present different implementations of those initiatives in national PKIs around the world. Finally, we analyze to what extent those existing interoperability solutions satisfy the requirements for interoperability, specified in the introduction.

4.2 PKI standards activities

There exist many independent organizations and working groups all around the world which are simultaneously working on developing PKI interoperability standards. In this section we present only the most important standards, which have been implemented in different PKIs (implementations of those standards are discussed in the section 4.3).

4.2.1 X.509

X.509 standard [32] was one of the first and the most important international PKI standards. It specifies a general, flexible format for digital certificates, which made public-key technology available to environments of unknown multiple users [4].

The most important aspect of X.509 are extensions, that became available in its version v3. Those extensions give the possibility of specifying digital certificates according to special demands of various PKI environments. Over the last 10 years, this standard evolved, being developed by the special working group of the Internet Engineering Task Force (IETF) (for more details see the last version [15]).

4.2.2 PKIX

Public-Key Infrastructure X.509 (PKIX) is a working group formed in 1995 by IETF. Its main goal was to develop Internet standards to support X.509-based Public-Key Infrastructures [33]. However, over time PKIX focused also on other initiatives that were supposed to satisfy the needs of X.509-based PKI in the Internet. The main areas of the PKIX activity, which all became subjects of different *Request For Comments (RFC)* documents, were :

1. Digital certificate and CRL profile [15]
2. Certificate management protocols [24]
3. Operational protocols [22]
4. Certificate Policy (CP) and Certification Practice Statement (CSP) framework [20] and [34]

PKIX's work was essential in order to bring the PKI concept to the Internet [4]. However, PKIX still continues to work on new standards needed for developing the domain of X.509-based PKI. The standards which PKIX has defined are flexible and general, and therefore they can be applied to different Internet-based environments.

4.2.3 LDAPext

LDAPext is a IETF Working Group, that was formed to define *Lightweight Directory Access Protocol (LDAP)* version 3 [35]. LDAP is an application protocol which is used for querying and modifying directory services, and which runs over TCP/IP protocol. In the context of PKI LDAP is used to localize and modify public-key certificates and CRLs [4]. Therefore, it works as a useful access protocol for certificate repositories and CRLs.

Version 3 of the LDAP, specified in a series of RFCs : from RFC4511 to RFC4519 and RFC4510 [36], defines particularly important extensions, that are helpful in adding new capabilities over time in a standardized way. Therefore, LDAPv3 can easily evolve,

allowing greater deployment [4]. Finally, LDAPv3 also enables the interoperability among different PKI vendors in an LDAP environment.

4.2.4 S/MIME

As mentioned in the section 2.1.2, Secure / Multipurpose Internet Mail Extensions is a standard for public-key encryption used for signing MIME-encapsulated e-mails. IETF S/MIME group was created to define specifications that will maintain the compatibility of previously implemented MIME products with new security solutions [4]. S/MIME specification also describes different PKI concepts, according to X.509 standard, which are relevant to handling of S/MIME messages (for more details see [37] and [38]).

4.2.5 ISIS-MTT

ISIS-MTT standards were established by industrial companies and research institutes in Germany. According to [39], IETF standards have been designed for a large variety of computer and communication applications, and therefore they are in some cases too general and too flexible. This flexibility allows many different interpretations which can lead to various implementations of the standards. As a result, this variety creates a lack of interoperability among different implementations.

Therefore, the goal of ISIS-MTT has been to promote interoperability by defining a more specific standard, which is based on IETF standards, but which restricts the possible implementation alternatives. This standard specifies the data format, communication protocols and interfaces, but it avoids specifying any particular certificate policy.

ISIS-MTT specifications consist of core parts and optional profiles. Core parts describe certificates and CRLs, PKI management, message formats, operational protocols, certificate path validation, cryptographic algorithms, cryptographic token interface and XML signature and encryption [39]. Requirements presented in those parts are to be met in order to conform to the ISIS-MTT standard.

On the other hand, the optional profiles concern special application areas or user groups, and do not need to be fulfilled in order to satisfy the ISIS-MTT standard. However, any components confirming to the optional profiles are automatically conforming to the ISIS-MTT standard [39].

4.2.6 Other activities

There exist many other standards that are being elaborated within various communities. According to [4] we should briefly mention the following four ones :

- **SPKI** IEFT Working Group created in 1996 as an alternative to the PKIX group. It was supposed to propose a simplified certificate format, SPKI. SPKI standards, however, were not implemented widely contrary to the X.509 standard [17].
- **IPsec** is a secure Internet Protocol (IP) providing cryptographic security services, which flexibly support a combination of authentication, integrity, access control and confidentiality [40]. IPsec was officially specified by IETF by a series of RFCs.
- **TLS** is an IETF standard cryptographic protocol that provides security and data integrity for communications over the Internet. The last update of the protocol specification is described in RFC5246 [41].
- **ANSI X9F** is the American National Standards Institute (ANSI) committee X9, which specializes in Financial Services. The subcommittee of this organization, ANSI X9F, is responsible for standardization of data and information security related subjects [4].

4.3 Interoperability initiatives

The need of PKI interoperability raised simultaneously with the widely developing and spreading PKI technology all around the world. Different PKI environments began to feel the need to interoperate with each other in different contexts. As a result, many parallel interoperability initiatives developed, being carried out by various independent organizations.

Because of the large variety of contexts in which those interoperability initiatives developed, their forms and purposes are very different. Some initiatives have a national scope, specifying PKI policy and practice framework for the purpose of only one country, i.e. the *German Root Certification Authority (German CRA)* or U.S. Federal PKI. Other initiatives are designed to suit a wider community, such as the European Digital Signature Directive or AsiaPKI Forum.

This section presents different interoperability initiatives that have been sponsored by governments or private companies in various parts of the world. It is important to underline that all presented initiatives may be regarded as solutions for PKI interoperability

only on limited scales. None of the following initiatives is meant to solve the problem of global PKI interoperability.

4.3.1 U.S. Federal Public-Key Infrastructure

The U.S. *Federal Public-Key Infrastructure (FPKI)* is an initiative of the U.S. government which defines the Public-Key Infrastructure for use of the United States federal agencies. FPKI was developed under the lead of the General Services Administration (GSA), and it conforms to NIST and *National Security Agency (NSA)* standards [20].

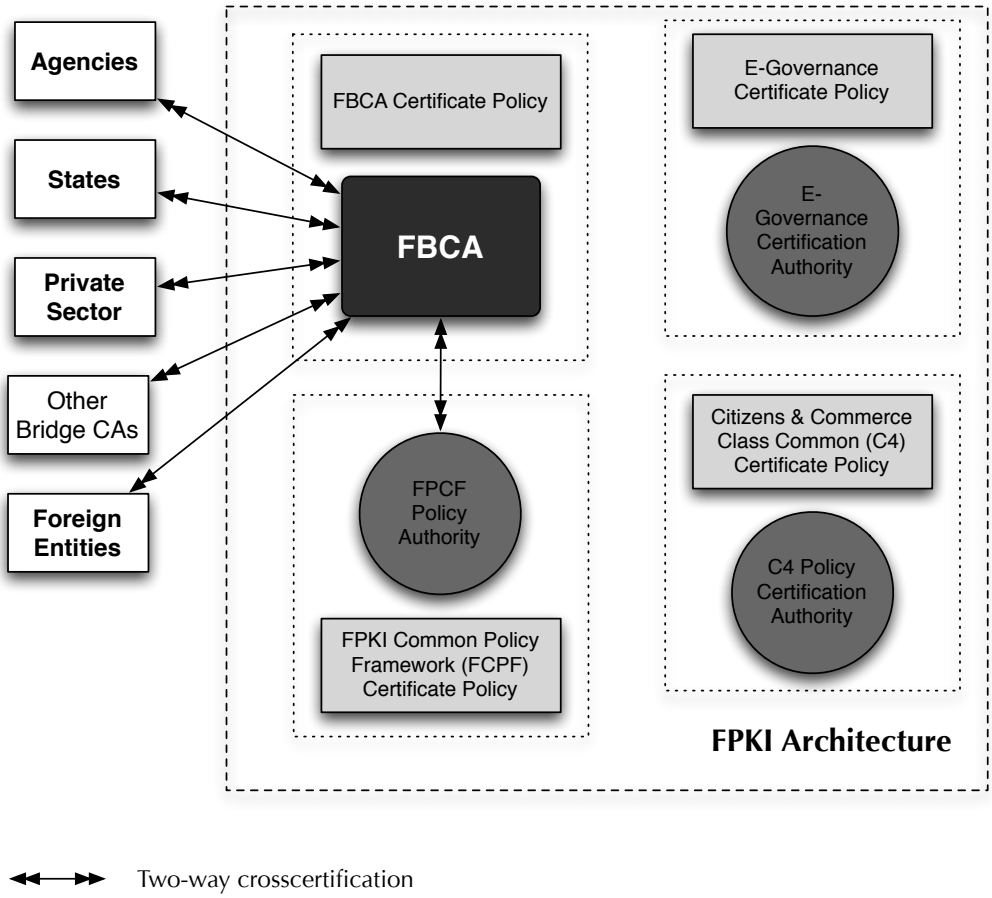

Figure 4.1: FBCA interoperability model.

The main goal of FPKI is to ensure a cross-governmental, interoperable Public-Key Infrastructure which supports Agency business processes, by using special PKI appli-

cations. According to the technical overview of the FPKI [42] the FPKI architecture consists of the four following main parts (see figure 4.1) :

- *Federal Bridge Certification Authority (FBCA)*, which is the central part of the FPKI architecture,
- *E-Governance Certification Authority (EGCA)*, which supports the identity assurance services for Federal electronic business, and which is not cross-certified with the FBCA,
- *Federal Common Policy Framework Certification Authority (FCPF CA)*, which is a trust anchor for Common FPKI Policy hierarchical PKI subscribers,
- *Citizens and Commerce Class Common (C4) Certification Authority*, which supports certificates accepted by U.S. Federal Government, used for authentication of citizens and commercial enterprises in many electronic services.

The FPKI model supporting technical interoperability among various PKIs involves the use of a central *Federal Bridge Certification Authority (FBCA)*. FBCA is an information system, which merges individual entities using commercial PKI products into the Federal PKI, which guarantees the assurance of digital certificates [42].

FBCA is a non-hierarchical hub that enables transitive trust by cross-certifying with principal certification authorities in various trust domains. The initial concept of FBCA consisted of implementing the FBCA as a root CA with which were cross-certifying multiple CAs, creating a hierarchical structure. Today FBCA is incorporated into the complex FPKI divided into four separate CAs which all support different FPKI Certificate Policies.

4.3.2 European interoperability initiatives

In Europe, contrary to the U.S., the European Union has not yet implemented a unified Public-Key Infrastructure. There exists European Directives and Acts, issued by the European Union Parliament concerning digital signatures, which are supposed to promote interoperability of PKIs within the EU. However, each Member State of the EU may have its own Public-Key Infrastructures, and its own rules and legislations.

In this section we present European Union interoperability initiatives, such as the European Digital Signature Directive [43], as well as independent initiatives, such as European Association for e-Identity and Security (EEMA, see 4.3.2). We also present an example of German RCA as a national interoperability initiative that was taken in one of the EU countries.

European Digital Signature Directive

European Digital Signature Directive [43] focuses on certification services and defines criteria on which is based the legal recognition of electronic signatures. It specifies the common obligations for Certification Authorities to secure recognition of signatures and certificates within the European Union. It defines common rules on liability to build users' confidence in digital certificates, and it specifies mechanisms to enable certificate and signature recognition within all Member States of EU.

The Directive differentiates between the *electronic signature* and the *advanced electronic signature*, and it provides corresponding definitions. According to [43], an electronic signature is any electronic data which is logically associated with other electronic data, and which serves as a method of authentication. The advanced electronic signature, on the other hand, is an electronic signature which meets the following requirements :

- it is uniquely linked to the signing entity (it provides strong identity binding),
- it is capable of identifying the signing entity (it provides authentication service),
- it is created using means that the signing entity can maintain under its sole control, and
- it is linked to the signed data in such a manner that any subsequent change in data is detectable (it provides data integrity service).

The Directive also specifies requirements for *qualified certificates* which may be issued by CAs which meet specific requirements laid down in the Directive. The required content of the qualified certificate conforms to the certificate structure described in section 2.3.1, however the requirements for issuers of qualified certificates are higher that those imposed on CAs issuing advanced certificates.

Besides, the Directive specifies the rules for Member States to promote the development of certification services on the market, as well as principles for internal markets of all Member States. It obliges Member States to ensure that certification authorities, which issue certificates on a national scale, are liable for damage that may be caused to any entity which relies on those certificates.

Finally, the Directive settles requirement for certificate and signature recognition in the international aspect. It obliges all Member States to ensure that any certificate which is issued in a third country fulfills special requirements, in order to get recognized as a qualified certificate.

All requirements specified in the European Digital Signature Directive have an important legal value in all EU Member States. It is important that any global interoperability solution, which by principle would be proposed also to EU countries, conforms to this Directive. Therefore, satisfying requirements enclosed in this Directive shall be taken into account when elaborating our global interoperability solution in chapter 5.

European Association for e-Identity and Security (EEMA)

European Association for e-Identity and Security (EEMA) was established in 1987 as an independent trade association for e-Business [44]. Its goal is to promote e-Business initiatives within Europe and to work on technology and legislations with governmental bodies, standards organizations, private companies and academic institutions, as well as some other European organizations.

The European Certification and Authority Forum (ECAF) is one of the EEMA working groups that was designed to focus on promoting PKI technologies. EEMA has issued Security Best Practice Papers specifying e.g. requirements for registration and revocation of digital certificates, PKI costs evaluation and PKI interoperability guidelines.

Between January 2001 and April 2003, EEMA carried out a project called *PKI Challenge*, which was one of the largest European interoperability initiatives [45]. The project was sponsored by the Swiss Government and the European Commission. The outcome of the project was the identification of interoperability problems and other issues, which could cause problems in security environments. In order to see detailed results of the project see to [46].

German RCA and FlexiPKI

The new German root certification authority is based on the concept of FlexiTrust. The central part of the national RCA is the FlexiTrust software which conforms to both ISIS-MTT and the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (RegTP) requirements. The national German RCA is fully controlled by the RegTP. All subordinate CAs are consequently cross-certified with the RCA in a strict subordinate hierarchy of Certification Authorities (see figure 4.2).

FlexiPKI [47] is a concept of a flexible and interoperable PKI, developed by researchers from Darmstadt University of Technology and T-Systems, which is a provider of information and communications technology services.

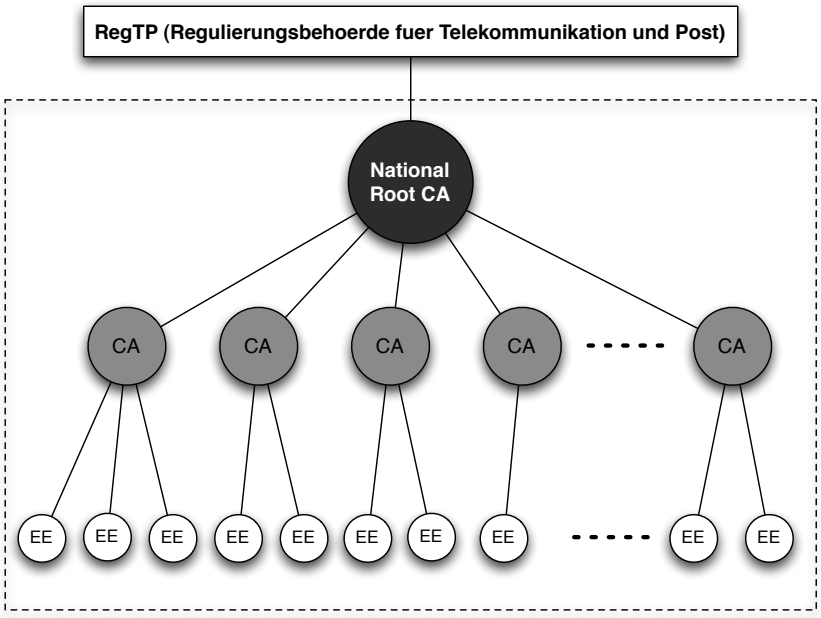

Figure 4.2: Illustrative PKI in Germany.

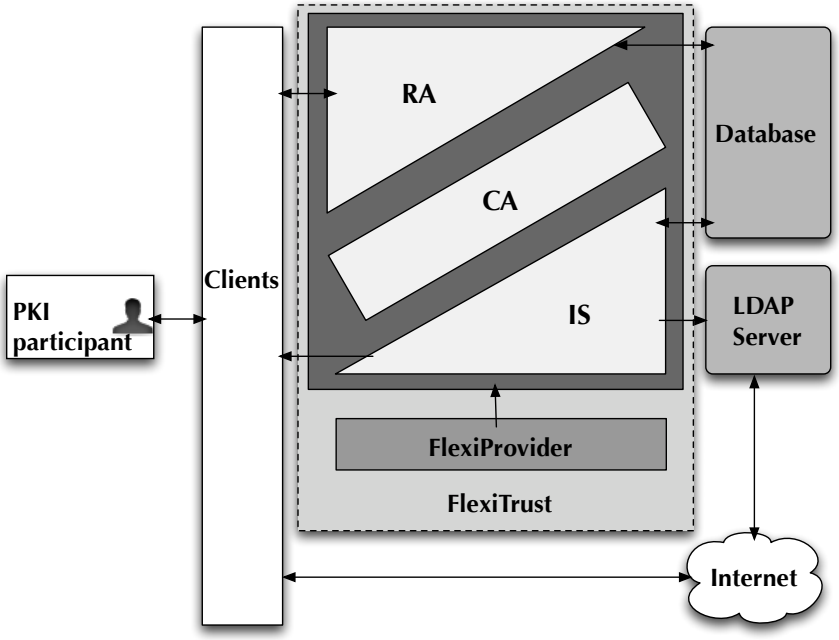

Figure 4.3: FlexiTrust core design.

FlexiPKI has a very specific structure, which is based on *Java Cryptographic Architecture (JCA)*. FlexiPKI also makes use of FlexiPrivider, which is a *cryptographic service provider (CSP)* for JCA. The two main parts of the FlexiPKI are the FlexiProvider and FlexiTrust [47]. FlexiProvider implements various cryptographic algorithms, whereas FlexiTrust is a trust-center software which consists of three parts : RA, CA and *Infrastructure Services (IS)* (see figure 4.3). IS provides support for handling the entire certificate life-cycle after its generation and registration performed by the CA and RA modules.

FlexiPKI could be successfully implemented in Germany, because it achieves requirement specified in the German Signature Law. This law was established in 2001 basing on the European Digital Signature Directive [48], in order to establish general security requirements for digital signatures in Germany. This act specifies, for example, that digital certificates for e-Government use should be verifiable for over 30 years. The ability of the FlexiPKI solution to use different cryptographic algorithms, which should be secure for a long time, satisfies, for example, this 30 year-long validity requirement for digital certificates [47].

4.3.3 Asia PKI Forum

Asia PKI Forum is a non-profit organization that has for a goal promoting PKI interoperability among countries in Asia and in the Oceanian Region [31]. The organization, was created in 2001, and its two working groups : Technical and Business Working Groups, focus on realization of a cross-border Asian eCommerce.

Asia PKI Forum gathers eight participating members : Australia, China, Hong Kong, Japan, Republic of Korea, Malaysia, Singapore and Chinese Taipei. Interoperability Guidelines of Asia PKI Forum conform with IETF standards, by establishing a PKI profile which can be regarded as a subset of the IETF PKI profile [49]. However, those guidelines remain general, allowing potential PKI designers to adapt those specifications for particular needs of various PKI environments (for more details see [49]).

The following subsection presents the national interoperability initiative in Japan, one of the countries participating in the Asia PKI Forum.

Asia PKI experimental project

In June 2001, three Asian countries : Japan, Korea and Singapore, agreed to participate in a proof experiment for PKI interoperability. The main goal of this experiment

was to explore possible interoperability of nationally certified CAs and to build an integrated heterogeneous PKI framework to facilitate future deployment of Asian PKI interoperability [31].

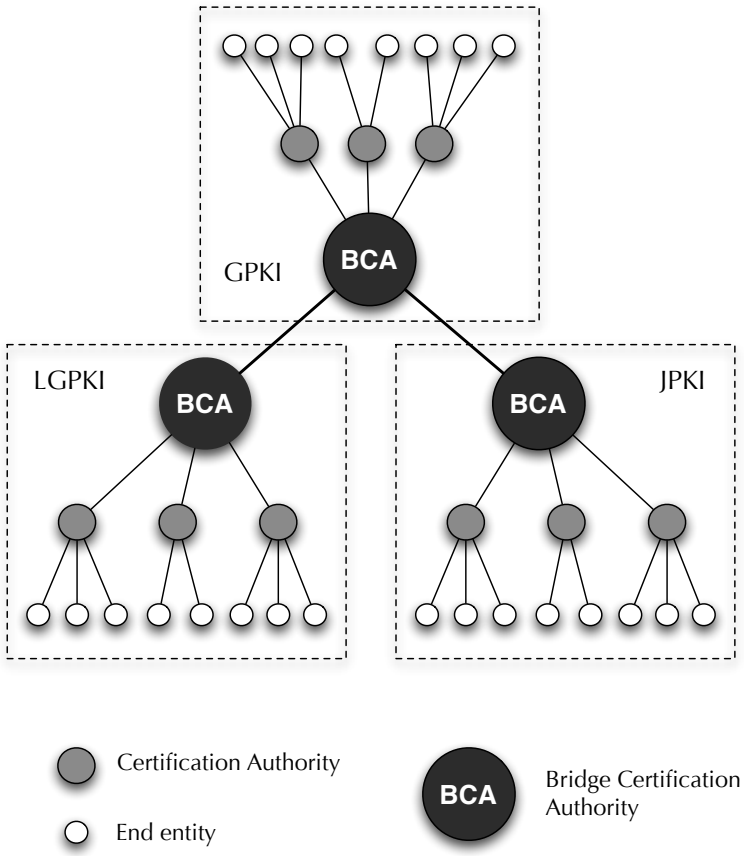

Figure 4.4: Illustrative PKI in Japan.

Japanese Government PKI System

The government PKI system in Japan is composed of three separate PKIs [50] :

1. *Government Public-Key Infrastructure (GPKI)*, which is used to certify documents being exchanged between the government and citizens via the Internet,
2. *Local Governmental Public-Key Infrastructure (LGPKI)*, which is the PKI constructed for the use of local authorities,
3. *Jumin Public-Key Infrastructure (JPKI)*, which is used to provide public service for Japanese citizens.

All of the three PKIs adopt a bridge CA trust model, so that all separate PKIs follow the vertical structure of the governmental administration where each ministry has its own CA [50], as shown on the figure 4.4. Besides LGPKI bridge CA and JPKI bridge CA are cross certified with the GPKI bridge CA, creating the multi-domain PKI of the Japanese Government.

4.3.4 Norway

Norway is a relatively small country in the world, with the population of nearly 4,800,000 citizens [51]. Although, the PKI technology is very well developed in Norway, there does not exist many vendors selling PKI solutions. This is mainly because, even though the general demand for PKI technologies in Norway is high, the number of potential certificate holders is limited due to the small Norwegian population.

Nowadays, there exist only two Norwegian PKI technology vendors, that are the following :

- **BBS AS** is the biggest Norwegian provider of electronic IDs, and payment and information solutions [52]. It provides both : digital certificates, which operate within the BBS Public-Key Infrastructure, as well as independent managed PKIs, which are being run in client companies. In 2005 BBS bought **ZebSign**, which between 2001 and 2004 was also an electronic ID service provider for the corporate market [53].

- **Buypass AS** is the second biggest vendor of electronic IDs in Norway, with more than 2 millions Norwegian clients having Buypass Smartkort with an electronic ID. Buypass specializes, however, in a very precise domain of Norwegian gambling, called *Norsk Tipping*. Certificates issued by Buypass operates in Buypass PKI, which is used mainly for gambling. However, Buypass IDs can also be used for other purposes (for more details see [54]).

Because of the limited number of independent PKIs in Norway, the problem of national interoperability of PKIs has not yet become as important as in some other countries. The two Norwegian electronic ID services vendors focus on separate domains. BBS mainly provides BankID PKIs to banks, and corporate PKIs to big Norwegian companies, whereas Buypass sells Buypass Smartkorts to individuals interested in gambling.

There exist, however, an important problem of PKI interoperability in Norway on the international scale. Norway, because of its relations with the European Union, has to conform to EU regulations concerning the *European Economic Area (EEA)* [55].

Norway should conform to European Digital Signature Directive, which means that the Norwegian RPs should accept digital certificates issued by CAs in different European Union Member States.

To overcome this problem of interoperability in Norwegian public sector, the Norwegian government established in January 2008 *The Agency for Public Management and eGovernment (Difi)* [56]. The Agency focuses on improving many aspects of the organization and efficiency of government administration, also of the PKI interoperability in the public sector. One of its role regarding electronic IDs is to promote interoperability of PKI solutions applied to the Norwegian public sector.

In Norway also exists a world's leading certification organization : *DNV*, offering many services such as assessment, classification, consulting and verification. *Det Norske Veritas (DNV)* has a world recognition and its goal is to promote safety and security in many areas e.g. biorisk, climate change, hospital accreditation, quality management, risk management and IT, software and systems. DNV is an impartial organization, which has the capacity to asses the quality of digital certificates, and therefore, it can provide signature verification and certificate validation services which are important for spreading PKI interoperability.

4.3.5 Other interoperability initiatives

There exist many other governmental, industrial, or combined interoperability initiatives in the world. On one hand, many countries have already developed their national PKI policies, such as e.g. Government of Canada PKI. On the other hand, many organizations tries to carry out specifications for international PKI interoperability in specific domains, e.g. Automotive Network eXchange (ANX) [4].

However, there also exist other important cross-border interoperability initiatives, which do not apply to any specific geographic area, neither to any specific industrial domain. Among the most important of those initiatives we should mention the following ones :

- **Minimum Interoperability Specification for PKI Components (MISPC)**, which was an initiative taken by NIST in cooperation with ten industry partners [57]. The purpose of this specification was to provide basis for companies interested in providing interoperable PKI components. This specification also became a basis reference for the first implementation of the Federal Bridge Certification Authority.

- **Secure Electronic Transactions (SET)**, which was a set of protocols and formats for securing credit card transactions over insecure networks, specially the Internet (see section 2.3). This initiatives didn't manage, however to win the market share, mainly because of its complexity and high implementation costs comparing to existing SSL based alternatives.

4.4 Weaknesses and vulnerabilities of existing interoperability initiatives

The domain of PKI interoperability initiatives has existed for approximately 20 years, as it was in the late 90' when the first PKI standards were elaborated. Therefore, it can be considered as relatively young, and it keeps on evolving continuously. Some interoperability standards have not begun to be implemented yet, and many others are being worked on as new vulnerabilities and weaknesses are being discovered when those solutions are being tested and implemented.

Because achieving PKI interoperability requires satisfying technical, as well as operational and legal requirements, it is a complex process which can not be performed without a proof experiment [31]. Therefore, any attempt of implementing interoperability initiatives should take two steps. First, specifications for interoperability should be defined for a precise PKI domain. Second, the specified interoperability behavior should be confirmed (tested) by using a real system in a specific PKI domain.

In this section, we present the outcome of analysis which were performed on one of the presented examples of implemented interoperability initiative in Japan. It is important to mention, that many of the implemented initiatives, especially those using a bridge CA PKI trust model, showed weaknesses which are comparable to the ones described in the following example.

4.4.1 Weaknesses of Japan Government PKI

During the deployment of the bridge model in the Japanese PKI, many difficulties were encountered. It turned out that the management of X.509 certificate extensions used to support certificate policies is complicated [50]. According to the X.509 specification [34], those extensions are the following :

- **Certificate Policies extension**, which indicates how the certificate should be used,

- **Policy Mappings extension**, which indicates if the certificate policies in the CA's domain are equivalent to any certificate policies in the subject's CA domain,
- **Policy Constraints extension**, which indicates if certificate policies should be explicit in all subsequent certificates in the certification path, and which also indicates if the policy mapping shouldn't be disabled by subsequent CAs in the certification path.

The Japanese Government PKI example showed, that building and validating certification paths in case of cross-certified bridge CAs, demands additional processing to conform all cross-certificates to its specific certificate policies. It also turned out that only compatible CPs of cross-certified bridge CAs allow building and verification of certification paths in such a structure.

Although much effort was put to develop complicated client applications that implement the certificate path building and validation, the government PKI systems did not became widely used [50]. The only common uses of those systems are the electronic bidding and procurement systems. Among the main causes for the limited use of government PKI systems, the document [50] mentions the following :

- insufficient enforcement measure of the government PKI systems,
- limited number of potential users,
- low activity of CA business concerning certificates under the Japanese Law Concerning Electronic Signatures and Certification Services.

Currently the Japanese government works on optimizing the GPKI to make it simpler to use. There is also work being done to put in practice issuing certificates for authentication, which were never issued before [50]. Only non-repudation certificates were mainly used until 2008, as the main focus of GPKI was to replace traditional paper documents by signed digital documents. With the planned improvement the Japanese government count on making the use of GPKI significantly broader in the future.

4.5 Summary

Since around 20 years many various standardization organizations have been working on elaborating standards related to PKI technologies. In may different communities the need for interoperability appeared nearly simultaneously. Therefore, we observed many independent organizations, both public and those founded by private companies, working simultaneously and developing a large variety of often incompatible PKI standards.

Some of those standards seem to be too vast, allowing too many incompatible implementations, whereas some others have, for various reasons, never even got implemented. In this chapter we presented the most commonly used PKI standards all around the world, such as X.509, PKIX, LDAPext, S/MIME and ISIS-MTT. Besides, we described interoperability initiatives that were being taken in various geographic locations, and their current situation in countries like : U.S., Germany, Japan and Norway. We also mentioned some cross-border interoperability initiatives, such as MISPC and SET.

Although, there exist many practical implementations of interoperability solutions in the world e.g. FPKI, German RCA or Asia PKI, we clearly observe that non of those solutions is ready to expand across its geographical borders or domain limitations. Therefore, in the section 4.4 we clearly underline the need for the solution to the global PKI interoperability problem.

Chapter 5

Solution Proposal for Global PKI Interoperability

This chapter presents the concept of the Global Validation Authority (GVA) and the Global Validation Service (GVS) which form a new PKI trust model, and which are our solution for global PKI interoperability. In this chapter we explain the concept of the GVA, we describe requirements specification for the GVS, we discuss the advantages and disadvantages of the proposed solution, and we suggest some business scenarios for the GVS.

5.1 Introduction

The main challenge of PKI interoperability is to provide a PKI trust model which makes it possible for all Relying Parties to validate digital certificates issued by any CA, without having any previous knowledge about the CA. All of the trust models presented in the chapter 3 oblige RPs to have relationships, or some previous knowledge about CAs, in order to be able to trust certificates issued by those CAs.

As we showed in the chapters 3 and 4, strict hierarchies of CAs, cross-certified mesh, hybrid and bridge CA models have their limitations and weaknesses. This is mainly because the complexity of those models grows exponentially when those models are being applied on large scales (see section 3.5). Therefore, none of these models is suitable to become the solution to the global PKI interoperability.

For this reason, Jon Ølnes and Leif Buene ([2], [3]) together with other researchers working for DNV AS, developed the concept of a new PKI trust model, in which an independent Validation Authority (VA) provides risk management for the Relying Parties.

Validation Authority is not only a provider of validation services for the RPs on behalf of CAs, but it also supplies RPs with independent quality assessment of the digital certificates and related signatures.

This model assumes, that the VA is theoretically able to enter into relationships with all existing CAs and RPs, regardless which PKI they belong to. That is how, the VA could provide validation services for all existing RPs, and therefore it could become the Global VA.

5.1.1 Scope and vocabulary of this chapter

The concept of the Validation Authority was continuously evolving for the last 10 years. We present a short history of VA and its current implementation in the chapter 6, together with the outcome of the exercise we performed with a test application of this system. In this thesis, however, we do not only focus on the existing Global Validation Service. We explore the concept of the *Global Validation Authority (GVA)*, which is our theoretical solution for global interoperability for electronic IDs. We use the term GVA in order to refer to the PKI interoperability model, which includes the Global VA.

In this chapter, we also use the term *Global Validation Service (GVS)* in order to refer to a theoretical implementation of the Global VA concept, which does not correspond to the actual version of the VA implementation owned by BBS. Besides, we use the term *GVS provider* to refer to any potential organization, which could run an implemented Global VA services, i.e. the GVS.

This chapter first presents the requirement specification for the Global Validation Service, then it presents the theoretical GVS solution for global PKI interoperability. We describe the GVS technical, business and legal issues, which should all together satisfy the requirements, specified in section 5.2. Finally, we discuss the main advantages and disadvantages of the GVS for all PKI entities involved in the service : RPs, CAs and certificate holders, also referred to as end entities.

5.2 Requirements specification for GVS

We decided to specify the requirements for GVS, in order to better understand what conditions should the GVS satisfy in order to fulfill its role as the solution for global PKI interoperability. The requirements were derived from the literature study of the following papers : [3], [2], and [58], as well as from the interviews with professionals, who worked on developing the VA concept in DNV and BBS, and from my personal analysis of all data collected during the research.

As mentioned in section 4.1, the requirements for interoperability can be divided into three groups : technical, operational and legal requirements. Bearing in mind this classification, we present in this section both functional and non-functional requirements for the GVS, which cover all three groups of interoperability requirements.

5.2.1 Functional requirements for GVS

In general, functional requirements define functions of a system, and they specify the inputs, outputs and behavior of the system. They can be divided into general and specific requirements, depending on how detailed they are. This section specifies both general functional requirements for the GVS, and its main component GVA, as well as the specific functional requirements, which precisely describe the desired behavior of all GVS components.

General requirements

The general functional requirements for GVS mainly concern the operational and legal interoperability requirements, and they are the following :

GR1 The GVS should allow all certificate holders to use their digital certificates towards all relevant RPs, regardless the PKI used by the RPs, and regardless the length of their certification paths.

GR2 The GVS should allow all RPs to use and validate digital certificates from all relevant certificate holders, regardless the PKI used by the certificate holders.

GR3 The GVS provider, as well as the GVS itself, should be neutral regarding all CAs it answers for. GVS's services shall be independent from all CAs, guaranteeing the reliability and trustworthiness of the GVA.

GR4 The GVS should provide RPs with the support for risk management. Therefore, in order to provide trustworthy quality information, it should base its quality assessment on a trusted third party auditor's results. In any other case it should provide information specifying how the quality evaluation was performed, providing an objective evaluation of the assurance level.

GR5 The GVS should provide services for certificate validation, the quality assessment of the digital certificates, and the issuer CAs, as well as information on particular certificate policies and liabilities of issuer CAs.

GR6 The GVS should provide validation services for digital certificates and verification services for digital signatures.

GR7 The GVA should provide both general ("one-fits-all"), as well as customizable services, which are based on specific criteria, or requests of each client RP.

GR8 The GVS provider should take the liability for its own actions, which should correspond to the liabilities of the CAs the GVS answers for. Therefore, the GVS should conform to national laws which govern liabilities of different CAs it answers for. The GVS provider should specify all liability issues in its agreements with particular CAs and with the client RPs.

GR9 The GVS should provide a flexible classification system of qualities of CAs and digital certificates. In order to provide international interoperability the GVS should provide classification that is compatible with different local (national) classifications, e.g. EU or FBCA classifications.

Specific requirements

The specific functional requirements for GVS concern mainly the operational and technical interoperability requirements, and they are the following :

SR1 The GVS shall be an on-line service, which shall answer in real time to RPs' requests. By real time we mean time which is nearly unremarkable for humans, it means around 1 second.

SR2 The GVS shall take RPs' requests as its inputs. Each request shall contain :

- some information allowing to identify the RP
- request for general certificate/signature information
- the digital certificate/digital signature, which should be assessed and/or validated by the GVA
- an information on how the certificate/signature is being used
- eventual information about the validation policy of the RP
- an eventual request for auxiliary information the RP wants to obtain about the certificate/signature, or the certificate owner in question.

SR3 The GVA shall support a variety of certificate profiles (enveloped, enveloping and detached certificates), cryptographic algorithms and protocols, in order to provide the support for global PKI interoperability.

SR4 The GVA shall perform parsing and syntax checking on digital certificates. It shall check if the the certificate in question contains all mandatory fields and critical extentions.

SR5 The GVA shall perform the semantic processing of the certificate content. It shall be able to recognize and extract certificate's mandatory fields and critical extensions. It should also be able to recognize and extract all extensions of the digital certificate in question.

SR6 The GVA shall check if the purpose, for which the certificate is used, corresponds to the allowed uses specified in the certificate.

SR7 The GVA shall perform the assessment of risk related to acceptance of the digital certificate. This should include the assessment of the following : CA's trustworthiness, the quality of the digital certificate, and the liability situation.

SR8 The GVA shall perform the validation of the digital certificate on behalf of the RP. This requires that the GVA processor is able to obtain through certification path processing a trusted copy of the issuer CA public key.

SR9 The GVA shall perform the check on revocation status of all digital certificates it answers for. The GVA shall be able to verify revocation status using OCSP and CRLs, depending on the certificates' extensions. Besides, the GVA shall be able to check the revocation status of currently signed documents, as well as old documents, by verifying the revocation status of the certificate at the time when the document was signed. Therefore, GVS shall store the full history of all CRLs.

SR10 In case of certificate paths, the GVA shall perform the processing of all certificates in the path.

SR11 The response to the RP's request, which is the output of the GVS, shall contain the following information :

- the certificate validation status, containing all general certificate information presented in the user interface (i.e. the corresponding public key, hash and encryption algorithms, validity period, certificate serial number, issuer name). In case when certificate is not validated a clear reason should be provided to the RP.
- information about allowed normal and extended usage of the certificate
- information about the quality of the certificate and/or the digital signature
- information about risks related to the use of the certificate, and liabilities of the issuer CA
- eventual auxiliary information requested by the RP

SR12 The GVS should provide GVA API which could support communication of GVA with many different client softwares.

SR13 The GVS should be possible to implement into many standard applications on the client side, e.g. Microsoft Outlook or Adobe, in order to be more widely used, and also to accelerate the global usage of GVS.

5.2.2 Non-functional requirements for GVS

Non-functional requirements specifies overall characteristics of a system, focusing on the qualities which the system should have. They impose constraints on the design or/and implementation of a system in order to preserve its qualities. The main non-functional requirements for the GVS are the following :

NR1 Response time

The GVS shall be an on-line system responding in real time to requests sent by client RPs. Therefore, it should ensure good communication between the client RP and the GVS servers. In order to make the GVS attractive to potential clients, its response time to RPs' requests should be comparable, or better, than the time RPs usually need to communicate with an issuer CA, in order to validate a certain certificate. For human users, the response time shall be around 1 second. However, if the GVS is supposed to be used also by client machines, then the response time of the services shall be reduced.

NR2 Availability

The GVS should be available 24/7. The GVS provider should take on liability for any consequences of the system being out of order for a certain period of time.

NR3 Robustness

The GVS should be secured, preventing it from potential attacks. Although, most of the information it provides about the CAs and issued certificates is public, the GVS should be protected against any data tempering attacks or denial of service attacks (DoS), for example by using a good firewall policy.

NR4 Security

Besides, the communication between the client RP and the GVS servers should be secured, limiting the possibility of a "man-in-the-middle" attack, which could manipulate the RPs' requests and/or GVS's responses. For this purpose a *cryptographic nonce* or SSL communication protocol could be used. On one hand, nonce stands for "number used once", and it is a random number issued in authentication protocol, which helps to protect against replay attacks or dictionary attacks. On the other hand SSL uses digital certificates, which beside providing authentication, can also provide other services.

NR5 Modifiability

The GVS needs to evolve continuously. It is important that adding and removing CAs, as well as modifying all details concerning them is easy for system administrators. GVS should also easily enable new services, according to particular needs of client RPs. Finally, as GVS is continuously growing in size, because of the need of storing the full history of CRLs, its storage databases should be easily extensible and their management should be easily adaptable to the amount of data they contain.

NR6 Efficiency

It is important, that besides all technical requirements the GVS also satisfies business requirement, being a profitable service for the GVS provider. For this reason, the GVS should be efficient by minimizing the costs of the GVS implementation, while maximizing the benefits from provided services.

NR7 Efficacy

Finally, in order to ensure global interoperability, the GVS should be able to handle multiple requests form a large number of client RPs. The GVS server should have a good on-line performances, limiting the possibility of saturation or dead-lock provoked by too large number of concurrent RPs' requests.

5.3 Global Validation Service (GVS)

The Global Validation Service (GVS) is a new PKI trust model, which is based on the concept of introducing a Global Validation Authority (GVA) as a new actor to the Public-Key Infrastructure. In the current situation, every RP, which desires to perform a validation of a particular certificate, has to communicate directly with the corresponding issuer CA, being entirely dependent on the information provided by the CA.

Today's situation imposes on RPs to have relationships with all issuer CAs in order to achieve global PKI interoperability. Those multiple agreements, with a huge number of existing CAs, are leading to a complex communication scheme between RPs and CAs, as presented in figure 5.1. Today, imaging that there exist n RPs and m CAs, in order to achieve the global PKI interoperability the number of agreements between RPs and CAs can rise up to $(n * m)$ agreements.

Therefore, not only, do we currently observe, that the current certificate validation process demands RPs to have multiple agreements with many CAs, but it also makes

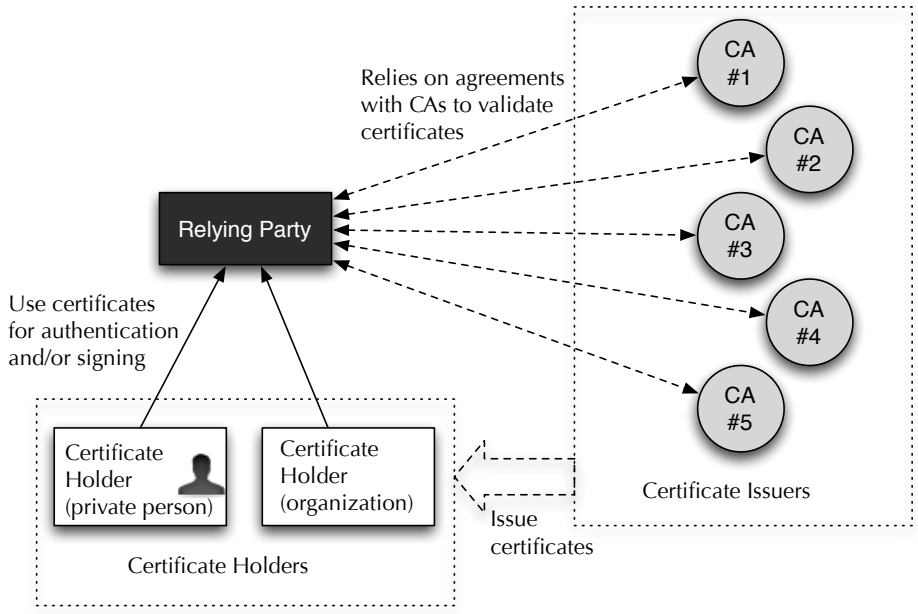

Figure 5.1: PKI trust model without the GVS.

issuer CAs, the only trusted entities in PKIs, the trust anchors. In order to provide an independent and neutral trustworthy validation service, we introduce a new validation entity, which detaches RPs from CAs, leading to significant increase of PKI interoperability, and in a decrease of the number of necessary agreements which could enable global PKI interoperability.

5.3.1 Global Validation Authority (GVA)

Global Validation Authority (GVA) is the core of the Global Validation Service. GVA is an independent and neutral third party, which provides risk management support for Relying Parties. GVA allows RPs to take trust decisions independently from any CA, and it simplifies the process of certificate validation for RPs, by providing one point of trust, one agreement, one point of billing and one liable actor [2].

In the Global VA PKI trust model, the GVA becomes the trust anchor, which takes over the certificate validation process from both RPs and issuer CAs. In this model, RPs need only to communicate with the Global VA, in order to validate certificates, or signatures, or to obtain some precise information on the quality of the certificates or the issuer CAs. The GVA acts like an independent provider of trustworthy information to the RPs. Therefore, it allows RPs to be independent from CAs, and, as a result, to accept

any certificate issued by any CA, that the GVA has an agreement with (see figure 5.2).

That is also how the total number of necessary agreements to ensure global PKI interoperability decreases when introducing the GVA from $(n * m)$ to $(n + m)$, in the case where there exist n RPs and m CAs. This is because the Global VA needs to make n agreements with all existing RPs and m agreements with all existing CAs, in order to ensure the global PKI interoperability.

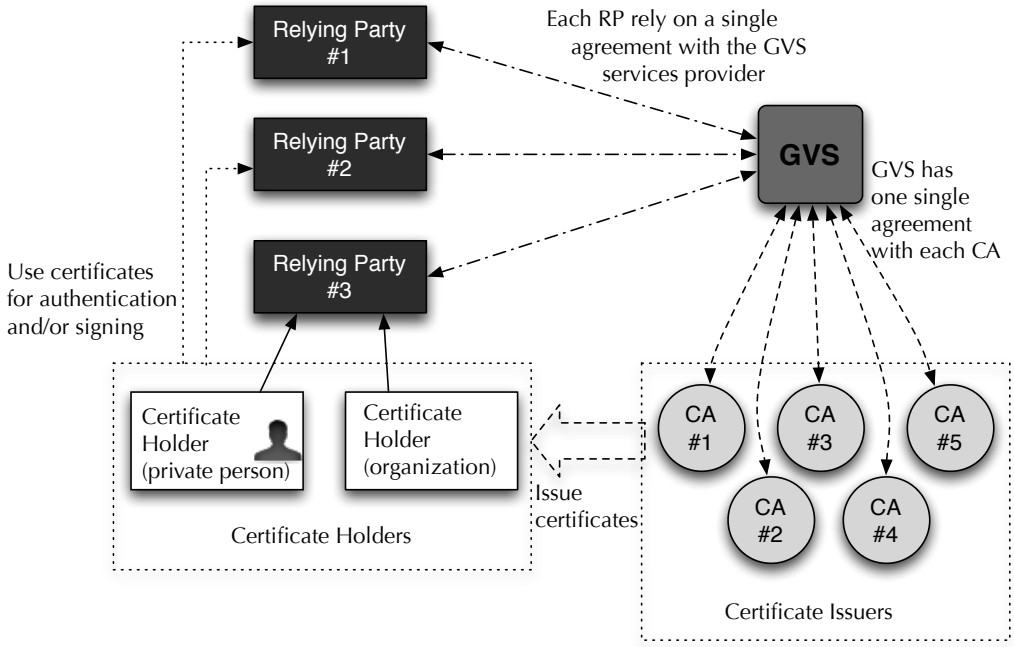

Figure 5.2: PKI trust model with the use of the Global VA.

The most important characteristics of the Global VA are :

- **GVA doesn't issue certificates** in order to keep GVA independent from any issuer CA. This means that, although in many existing trust models GVA could be compared to a bridge CA [2], it does not function in the same way, as it doesn't provide CA services.
- **GVA handles all CAs individually** regardless of the trust structures they are in [2]. GVA simplifies the certification path processing, because after a particular CA is objectively assessed and the agreement between the CA and the GVA is signed, there is no need to provide a path to any "trusted CA", because the GVA becomes the trust anchor.

- **GVA provides validation, time-stamping and quality assessment services** providing RPs with main and auxiliary information regarding the signatures/certificates or the issuer CAs.
- **GVS provides support for global PKI interoperability**, as the GVA can have as many agreements with CAs and RPs, as possible, and it supports various certificate profiles, cryptographic algorithms and protocols.

Global VA, in order to be a trusted third party, should perform its processes locally, so it can provide its auditors with complete records regarding its operations. It means, that GVA should store a trusted local copy of all information coming from CAs, and make regular updates. The GVA should also follow any changes concerning CAs, so it can perform a reverse validation of old signatures and certificates. This operation can be done, only if the GVA has a full history of all trusted CAs and corresponding CRLs.

Besides, the Global VA shall store traces of all its actions, so it can provide proofs in case of any disputes [2]. The main condition for the Global VA to be considered as a trust anchor by RPs, is to be able to supply a trustworthy documentation of its own actions. Becoming a trust anchor for a large spectrum of PKIs demands taking significant responsibilities by the GVS provider.

5.3.2 GVS relationships

The GVS is a complex system, which works in close relationship with other PKI entities. The GVS, in order to become a trusted system, should work together with a trustworthy third party auditor, which could provide the Global VA with a reliable assessment of CAs' qualities and the qualities of particular digital certificates. Det Norske Veritas (DNV) (see section 4.3.4) with its long history and worldwide recognition could play the role of this third party in the global context.

DNV could assess the qualities of any CA which desires to join the GVS structure (see figure 5.3). DNV could perform an auditing of the CA and attribute the certificates issued by the CA a certain quality level which could be used afterwards by the Global VA to provide the quality assessment service to the RPs. It is important to point out, that the quality classification system used by DNV should be flexible, allowing possible adaptation to other existing assessment scales, used in other countries (see GR9 in section 5.2.1). However, DNV (presented in the figure 5.3) can be replaced by any other trusted third party auditor, which could provide quality assessment services to the GVS.

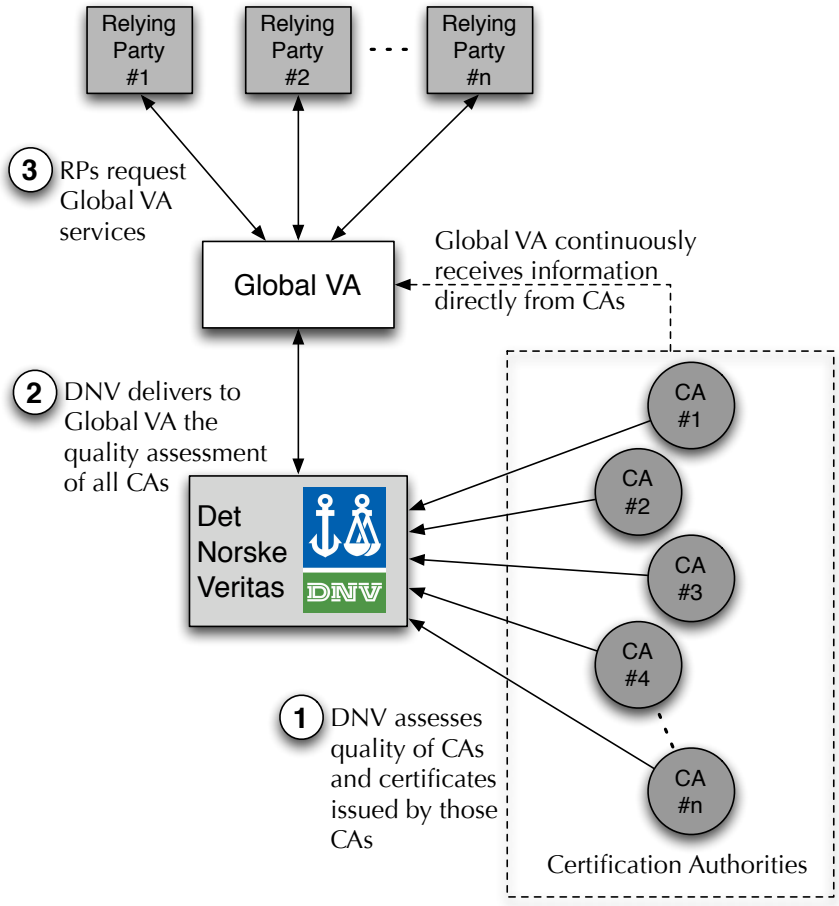

Figure 5.3: The communication between GVS, RPs, CAs and the quality assessment authority : DNV.

For this reason, the GVS provider should have a special cooperation agreement with the trusted third party auditor, who will outsource the quality assessment according to special needs of the Global VA. The GVS also needs to have agreements with all CAs it answers for. CAs need to deliver to the Global VA all information necessary for the validation of certificates requested by RPs, as well as some auxiliary information which could be provided to RPs in its secondary services.

Although, DNV is a perfect candidate for the third party auditor for GVS, the GVS provider could theoretically use more than one auditor for the quality assessment of issuer CAs. It is, however, important to underline, that all of those auditors should conform to the same requirements of the Global VA, and they should deliver the assessment

services of the same quality.

5.3.3 GVS legal issues

In order to complete its role of impartial and neutral third party, the GVS should be run by a trustworthy organization. This condition imposes an important business constraint on the GVS provider, which should have appropriate background and resources, to be able to provide validation services on a global scale. For those reasons, there exist two categories of possible GVS providers :

1. Public authorities
2. Large, independent companies, with appropriate recognition as a security solution providers, which also have an important experience in PKI technology

Some public authorities, such as governmental agencies, or cross-border organizations, e.g. EU could have necessary recognition and means to provide validation services. However, there exist an important legislative barrier, which make it nearly impossible for them to run such a service. This is because public authorities usually conforms to the local legislations, which could be difficult to impose on all entities which want to participate in the global, cross-border GVS structure.

Therefore, independent private companies with appropriate background, resources and recognition have an important advantage over public authorities in providing validation services. For all of its agreements, the GVS provider can define the *contractual laws*, which doesn't have to conform to the *national laws* of the countries, in which the GVS provider, client RPs or issuer CAs reside. The GVS provider can specify in each of its agreements separately which legislation apply to the particular agreement. That is how the company providing validation services can be independent from local legislations, and therefore can reach the goal of the global PKI interoperability.

5.3.4 GVS business model

Since the Global Validation Service is provided by a private company, as a commercial service, it has to bring profits to its owner and operator. In order to generate profit, the GVS provider should charge its client RPs, for the validation services it provides to them. The prices and payment terms should be specified according to the GVS provider business plan, and they should cover all the expenses of the development, operation and maintenance of the GVS.

In the first phase of GVS development we can assume that the GVS provider shall encourage the issuer CAs to join its structure. That is why GVS could provide CAs with a free of charge quality assessment, and it shall pay them a percentage of the total amount of transactions the GVS had with its client RPs concerning the certificates issued by those CAs (see figure 5.4). That is why the GVS provider shall also cover the expenses of the third party audit, and pay the auditor for the quality assessment of the certificates issued by agreed CAs.

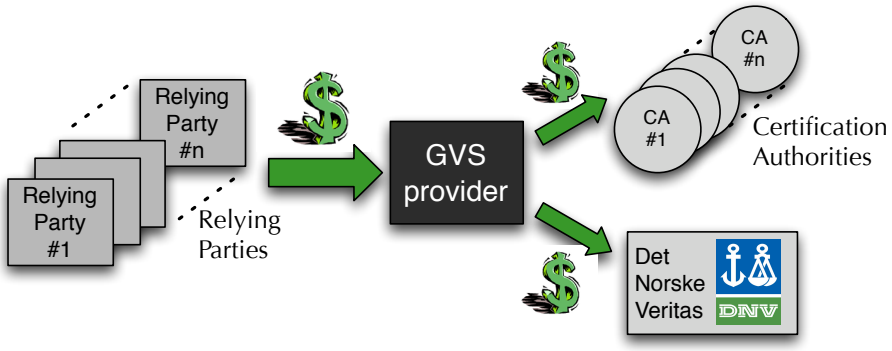

Figure 5.4: The business relationship of the GVS provider.

A similar business plan was developed by DNV when implementing the VA service (see chapter 6 for VA concept presentation). It could, however, be assumed, that once the concept of independent validation authority as a solution for global PKI interoperability spreads on a large scale, issuer CAs would no longer receive any financial benefit from the GVS provider. In this scenario, most of the CAs as well as RPs would look forward to join the GVS structure in order to increase their interoperability and grow on the market, and would not need an extra financial encouragement.

5.3.5 GVS agreements

The Global VA, which acts as an intermediary in certificate validation between the RPs an CAs should have two types of agreements, which are strongly related with each other : Relying Party Agreements and Certification Authority Agreements. On one hand, the GVS provider, in order to be considered as a trusted third party providing validation services, should define its own limitations of use, and limitations of liabilities for its client RPs. On the other hand, the GVS provider is obliged to transfer some of its liabilities to the related CAs, which should be specified in its agreements with issuer CAs.

Besides, because of the fact that the GVS provider outsources the quality assessment of certificates, it should also have a specific agreement with its *third party auditors*. Therefore, GVS provider should have three types of agreements, Relying Party Agreement (RPA), Certification Authority Agreement and third party authority agreement are described in details in this section.

Relying Party Agreement (RPA)

Today, *Relying Party Agreements (RPAs)* are documents prepared by CAs, which specify the terms of use of the CAs' repositories by RPs wishing to validate digital certificates issued by those CAs. Any RP, that uses issuer CA's certificate repositories, CRLs, OCSP services or any other certificate-related information in order to validate a particular certificate, have to sign a corresponding CA's RPA. Only when agreeing to terms of RPA, RPs can submit the certificate-related query to the CAs and rely on information provided by the CAs.

Current RPAs usually contain some definitions of important PKI concepts, they specify the obligations and responsibilities of RPs regarding the certificate validation, and they define the limitations of use, in order to make the RPs aware of risks related to the possibility of private keys getting compromised. Finally, RPAs describe the liabilities and the limitations of the liabilities, that the CAs take on in case of misuse of any particular certificate. CAs define the exact financial liability caps, that can be claimed by an RP, that experienced a damage while using, and/or validating, a particular certificate. For more details on existing RPA, see the example of RPA [59].

However, in the PKI model with Global VA, which provides the risk management for certificate validation for RPs, the Relying Party Agreement takes a completely new dimension. The RPA becomes an agreement between the GVS provider, and an RP. According to the general functional requirement GR8 (see section 5.2.1), the GVS provider should take on liabilities for the validation services it provides, what should be specified in an RPA.

Therefore, from the legal and operational point of view, a Relying Party Agreement between a GVS provider and the client RP should contain the following :

1. **definitions** of important terms used in the agreement, both legal and PKI oriented terms
2. specification of the **scope and execution of services** furnished by the GVS provider
3. specification of the **terms of payment** for the validation services

4. conditions of possible **variation and termination** of the agreement
5. **confidentiality closure** specifying what information obtained from the other party can and what can not be disclosed
6. specification of the **liability cap** for losses or damages caused by validation of any certificate issued by an agreed CA. An RPA should specify the limited amounts per year per CA, and a total cumulative amount per year.
7. specification of **governing law** according to which disputes, which cannot be solved through negotiations, should be resolved. An RPA can also specify the **legal venue** where those disputes should be resolved.
8. closure about **liability insurance of the GVS provider**, which can be compulsory according to the chosen legislation for the agreement, or can be decided independently of the legislation
9. closure about **force majeure**, which specifies conditions which don't give rights to any claim
10. closure about **intellectual property rights**
11. specification of any **special conditions**

Certification Authority Agreement

Global Validation Authority does not issue certificates it answers for. Therefore, it can not take on full responsibility of possible misuses of those certificates, on behalf of the issuer CAs. For those reasons, the liabilities of GVS provider should correspond to the liabilities of the relevant issuer CAs, and they should be specified in the agreement between the GVS provider and the CA.

The Certification Authority Agreement, should contain the following :

1. **definitions** of important terms used in the agreement, both legal and PKI oriented terms
2. specification of the **scope and execution of quality assessment services** furnished by the GVS provider to the CA, and the specification of the **scope and execution of certificate-related information service** by the CA to the GVA
3. specification of the **terms of payment** of the GVS provider to the CA
4. conditions of possible **variation and termination** of the agreement

5. **confidentiality closure** specifying what information obtained from the other party can and what can not be disclosed

6. specification of the **liability cap for the GVS provider** cumulative for the total amount of agreed CAs, and the **liability cap for the CA** cumulative for all certificates issued by the CA. The agreement should also specify how the parties are going to indemnify each other if claims resulting in errors made by one party are directed against the other party.

7. specification of **governing law** according to which disputes, which cannot be solved through negotiations, should be resolved. A Certification Authority Agreement can also specify the **legal venue** where those disputes should be resolved.

8. closure about **liability insurance of both parties**, which can be compulsory according to the chosen legislation for the agreement, or can be decided independently of the legislation

9. closure about **force majeure**, which specifies conditions which don't give rights to any claim

10. closure about **intellectual property rights**

11. specification of any **special conditions**

Third party auditor agreement

Finally, in order to provide an independent quality assessment of certificates and signatures the Global VA needs to sign an agreement with the third party auditor, who will provide compensated quality assessment services to the Global VA. For this reason, the agreement with the third party auditor should, in general, contain the same type of closures as the Relying Party Agreement, with some exceptions.

The agreement should specify the scope and execution of the quality assessment services, and the terms of payment. It should also contain definitions, a closure of variation and termination of the agreement, a confidentiality closure, a force majeure and intellectual property rights closure. However, this agreement does not need to contain any liability closure regarding the certificate validation as the third party auditor does not take on any liability for certificates and signature it assesses.

Nevertheless, it should be specified in the agreement, to which extend is the third party auditor liable for any possible mistakes done in the certifiacte/signature quality

assessment process. This is because the Global VA should not be responsible for providing RPs and CAs with wrong quality information, if this information is delivered to the GVA directly by the third party auditor.

5.3.6 GVS quality assessment scheme

The GVS should provide trustworthy and complete information on the quality of digital certificates and corresponding digital signatures, through its multilevel quality assessment framework. It is important, that the quality levels, defined by the GVS, or the third party auditor, are flexible enough to be easily interpretable in different PKIs, so the GVS can ensure a high interoperability of its validation and quality information services.

In order to be flexible, the multilevel framework not only should be finely grained, but it also should comply with the national and international legislations. It should be based on some international standards, so it can ensure that digital certificates and corresponding signatures meet legislative requirements, e.g. those of qualified certificates in the EU.

Besides, in order to provide a complete information on the certificate quality, the quality assessment of the certificates should be done in the two following steps :

1. **assessment of the certificate policy** used by the issuer CA, and the actor running the CA, i.e. by analyzing its market share and reputation. The third party auditor can also take into account other documentation, i.e. CA's certification practice statement, its agreements with the certificate holders and other actors, the CA's position in any PKI structures, and its compliance with national and international legislations.

2. **assessment of the trustworthiness claimed by the CA**, which basically indicates the RPs to what extend they can trust the CA's documentation, mainly the CP and CSP. It is important to provide this information by the third party auditor, as all documentation taken into account in the first step of the quality assessment is delivered by the CA itself, so it doesn't come from an independent source.

Finally, the GVS should provide RPs with information on the quality of digital signatures used by certificate holders. The quality of a digital signature should be assessed taking into account : the hash algorithm, the public-key algorithm and the key size used in the digital signature. This parameters, together with the quality of corresponding digital certificate, give RPs a complete indication of the quality of a signature used with the digital certificate, issued by evaluated CAs.

5.4 GVS technical specification

The Global Validation Service is an on-line service, which responds to RPs' requests in real time (see SR1 in setion 5.2.1), providing them with validity, quality and eventually auxiliary information demanded by the RPs. GVS accepts queries for both :

- *digital certificate validation*, which among others consists on checking the validity of a particular certificate, its revocation status, and its limitations of use. GVS also provide the requesting RPs with quality information concerning the requested certificate,
- *digital signature verification*, which consist of verifying if the signature is valid (by checking the hash value of the signed document), and the validation of the certificate corresponding to the requested signature.

In order to provide those two services, the GVS should be able to access all information necessary to answer the RPs requests in real time. For this reason, the GVS have to store locally downloadable CRLs, and quality information in its internal database. It should be in regular communication with issuer CAs, making it possible to regularly update manually, or automatically, all relevant information. It should also be able to access revocation status information via OCSP protocol.

In order to become the solution for global PKI interoperability the Global Validation Service should support all public-key certificate standards, and it should handle all types of signatures format, for both single and multiple signatures. This means that the GVS should also support all types of hash and cryptographic algorithms used in those signature formats.

5.4.1 GVS communication protocols

The GVS should also ensure easy, fast and reliable communication with its client RPs. It is not necessary to build any special communication network to provide validation services to RPs, which can be provided over the Internet using protocols ensuring secure communication.

This can be done with *Simple Object Access Protocol (SOAP)* which uses Internet application layer protocols, such as transport protocols, i.e. SMTP, HTTP or HTTPS. SOAP is a platform and language independent protocol which relies on XML message format, and therefore its very easy to implement in the GVS. Besides, when using HTTPS protocol, which simply is the HTTP protocol applied over an encrypted SLL

or TLS connection, the communication between the Global VA and the RPs is secured with a use of encryption and two-side authentication.

SCVP

However, the communication protocol used by GVS should be based on an existing standard protocol used for certificate validation, in order to make the system follow international standards. Therefore, one of the possibilities is to use *Server-based Certificate Validation Protocol (SCVP)*. SCVP is a simple request-response protocol that is used over HTTP, however, it can be used over e-mail or other protocols, which can transport digitally signed objects [60]. It simply delegates the certificate validation to a server according to a previously agreed validation policy, that parameters are validation algorithms represented as an OID.

SCVP doesn't use any confidentiality mechanism, but it can be added if SVCP is used over a lower-layer security protocol, e.g. SSL or TLS. Instead SCVP uses cryptographic nonce (see section 5.2.2) in order to protect the message exchange between the client and the SCVP server against man-in-the-middle attacks. Besides, the integrity of SVCP requests and responses can be ensured by using MACs or by digitally signing all exchanged messages. For detailed specification of SCVP protocol see [60].

DVCS

There exists also another standard protocol, which can be used for ensuring communication between RPs and the Global VA. *Data Validation and Certification Server (DVCS) Protocols* [61] provide support for four types of validation services, which are : certification of possession, claim of possession of data, validation of digitally signed documents, and public-key certificates validation. DVCS services should rely on CRLs and OCSP to provide complete validation of digital certificates.

An important feature of DVCS protocol is that DVCS validation services can be used after expiration of a digital certificate. Besides, the DVCS responses, also called Data Validation Certificate (DVC), can be validated with the use of the same protocol. Besides, there exists no mandatory transport mechanism for DVCS protocol. It is, however, highly recommended to provide server authentication, which could be done using HTTPS protocol, and it is mandatory that all DVCS responses are signed. For the complete specification of the DVCS protocol see [61].

XKMS

Finally, another protocol, which could be used to implement GVS communication with the RPs is XKMS [62], which was used in PEPPOL project (see 5.5.1). XKMS uses XML message syntax and it allows use of the Simple Object Access Protocol (SOAP). The main advantage of XKMS is its flexibility, which e.g. comprises message extensions. Those extensions can be used, to define auxiliary information that shall be provide in some types of validation requests and/or responses. Those message extensions allow high customization of GVS validation services, and therefore improve its interoperability. For more examples, see section 5.5.1.

5.4.2 GVS front-end and back-end implementation

Similarly to the communication protocols, there also exist a few possibilities for front-end implementation of the GVS, as well as the back-end implementation, which are of course dependent on each other. After analyzing some existing solutions, e.g. the current implementation of Global VA, and its concurrent solutions evaluated by the EFVS Study (see section 6.4), we propose three independent, but not exclusive, solutions for the front-end implementation of the GVS. These are the following :

1. Creating a GVS client software
2. Creating a GVS Gateway
3. Implementing the validation service into existing applications.

GVS client software

It is possible to imagine creating an independent client software, which could handle clients' validation requests and display easily readable responses to the users from the Global VA. Such client software shall be possible to install on every RP's personal machine (see figure 5.5). In this case any person who needs to validate a digital certificate and/or to verify a digital signature could import the signed document directly into the GVS client software and send it from his/her computer to the Global VA.

In order to ensure wide interoperability, the client software should accept many file formats containing digital signatures. Those signatures shall be consequently extracted from the documents imported to the client software and adapted to fit the validation request format. Besides, the software shall locally hash the imported file, and send in the validation request only the hash value of the file. This should be done not only to avoid sending the entire files in order to reduce the traffic between RPs, but also, because those files could often contain sensitive information.

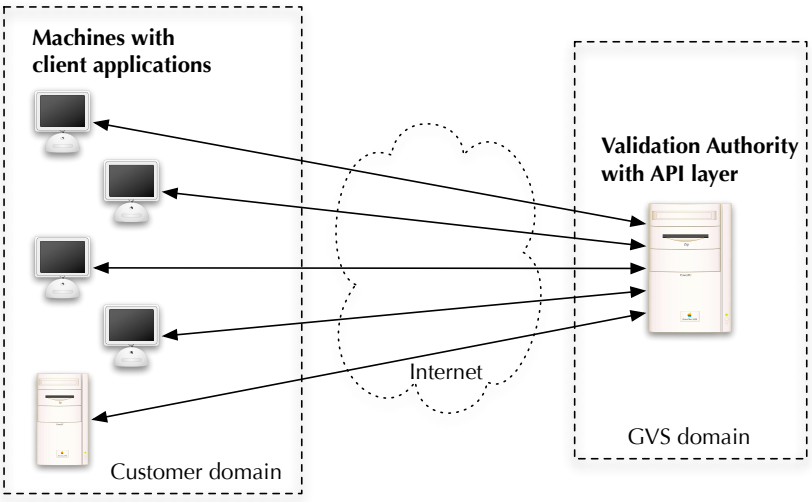

Figure 5.5: The GVS implementation scheme with many GVS client softwares.

GVS Gateway

It is, however, also possible to create a GVS Gateway, which could replace locally installed GVS client software inside an internal network of an organization comprising many members, who could act as RPs (see figure 5.6). Particular users who wish to validate digital certificates, could in this case send validation requests from their PCs to the GVS Gateway over their organizational network, e.g. in an e-mail, or by uploading a file into a internal validation portal.

GVS Gateway software, similarly to the GVS client software, could consequently extract signatures and hash the received files, and then send them to the GVS. This solution would simplify the communication scheme between the RPs and Global VA comparing to the GVS client software solution. This is because the GVS gateway reduces the traffic from n RPs within one organization sending validation requests simultaneously, to only 1 GVS Gateway communicating with the GVA (see figure 5.6).

The main advantage of the GVS Gateway solution is that it provides a single point for authentication of all RPs within one organization towards the Global VA. It also can be seen as an enforcement of customer specific policies, as specific policies would be applied by the GVS Gateway for all validation requests sent from one organization. Particular users of the GVS services, would consequently have less control over the validation process, which will be decided by the GVS Gateway for the entire organization.

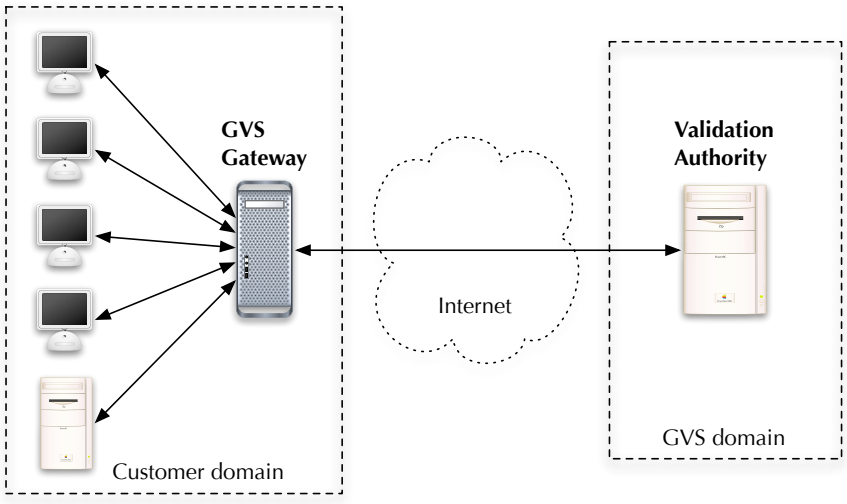

Figure 5.6: The GVS implementation scheme with the GVS Gateway.

Implementing the validation service into existing applications

Finally, it is also possible to implement a GVS validation module into some broadly used applications which handle documents signed digitally. Those applications include e-mail handling software (e.g. Microsoft Outlook), and text documents handling software (e.g. Adobe, Microsoft Word). In this solution, when opening a document signed electronically an application with integrated GVS validation module could ask the user automatically, if he/she wishes to verify the digital signature.

The main inconvenience of this solution, is that in this case the Global VA could not provide its services independently from important software vendors. This front-end implementation is, however, an interesting solution for supplementary implementation of GVS services. Implementing a validation service into existing applications would make GVS services easily available to users all around the world.

GVS back-end implementation

When it comes to the back-end of the GVS, it should consist of a GVS server, which could handle the communication of the Global VA with the RPs, and an extensible database which would contain all information necessary for certificate validation.The GVS back-end could also include a Global VA API, which would define the structure of RPs' request messages and GVA's response messages, and which would enable the Global VA to receive validation requests sent by different types of client software.

It is also important to ensure the security of the GVS back-end for two reasons. First, the GVS repositories may contain sensitive information, such as end user data included in their digital certificates. Second, the answers of GVS to validation requests should not be tempered with, in order to ensure GVS trustworthiness.

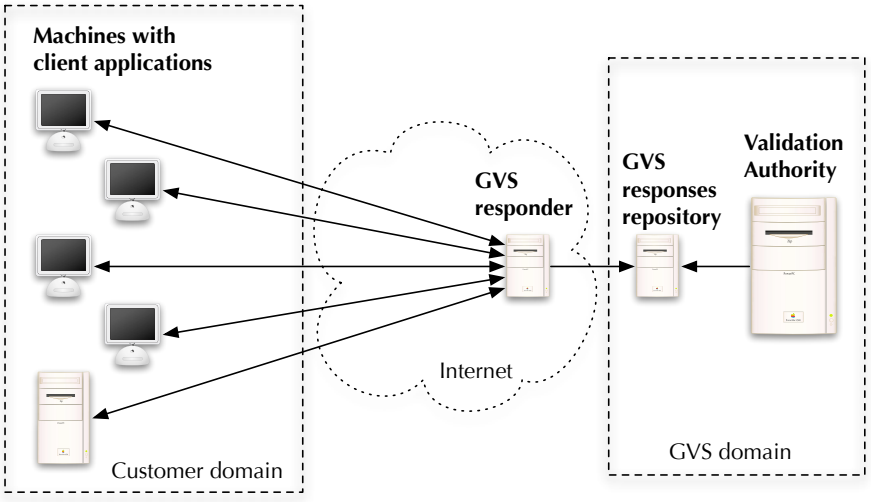

Figure 5.7: The GVS back-end implementation scheme with the GVS responder and GVS responses repository.

For these reasons it may be worth to consider implementing a GVS responder and a GVS responses repository which would be installed on two separate machine from the main GVS server (see figure 5.7). The GVS responder could only access information copied from the GVS server to the GVS responses repository, separating the protected back-end zone of the GVS from the request-response module commonly accessible over the Internet.

Implementing multiple GVS responders seems also to be a reasonable solution when thinking about providing a global service. GVS responders, shall in this case be located at different places in the world, enabling simple and fast communication of the RPs with the GVS, depending on their geographical location. Multiplying the GVS responders would also improve the availability of GVS, allowing some responders take over the communication of another responded which went down, as a result of a technical failure, or an attack.

5.5 Business scenarios for GVS

Many PKI interoperability initiatives are currently being taken in Europe. Some of these project can become a good business scenarios for the GVS, as they require a solution providing cross-border interoperability for electronic signatures across Europe. Therefore, GVS could successfully integrate with those projects and that is how it could launched on a European scale.

Among the most important EU projects which could perfectly suit as a starting point for developing a Global Validation Service, are PEPPOL and STORK, which are presented in details further in the following section.

5.5.1 PEPPOL

Pan European Public Procurement Online is a 3 year lasting EU project, which has as its goal to set up a pilot solution to European public eProcurement. PEPPOL shall enable all private companies across EU to communicate electronically with European governmental institutions. The project started in May 2008, and it will last till April 2011. Apart from countries which are partners of the project i.e. Germany, France, Italy and Norway, PEPPOL shall also involve other Member States of EU [63].

PEPPOL is structured in four independent projects, which are: Virtual Company Dossier, eCatalogues, eOrdering, and eInvoicing, and they are supposed to support all three phases of procurement process, which includes pre-award tendering, post-award procurement and payment [63]. Besides, all those projects are based on using electronic signatures to provide necessary security to public European eProcurement.

One of the main goals of PEOPPOL is to promote the use of electronic signatures across Europe, that is why it recommends imposing flexible requirements on signature formats, making the participation in eProcurement relatively easy and accessible for potential participants [64]. This in why, eProcurement will require an effective validation mechanism in order to make it possible for European governmental institutions to validate such a variety of electronic signatures. This situation seems suitable for GVS, which shall provide verification services for all possible formats of electronic signatures.

Besides, the number of economic operators, which are companies that could participate in the eProcurement is high on the European scale. That is why, one of the main obstacles for PEPPOL is to provide solutions for signing and verification on a large

scale. GVS has all necessary characteristics to operate and provide validation and verification services for a large number of users, and that is why it seems to be a good solution to the scalability problem of PEPPOL.

Finally, PEPPOL is also aware of existing conflicting legislations regarding electronic signatures in all Member States of EU. This situation definitely becomes another major obstacle to legal interoperability for European eProcurement. Therefore, introducing a Global Validation Service, which provides an agreement-based structure, can overcome many legislation problems. GVS introduces contractual laws, and that is why it does not have to conform only to local legislations, so it can provide a cross-border legal interoperability for PEPPOL (see section 5.3.3).

For those three main reasons the PEPPOL project seems to be an important opportunity for GVS's development in Europe. That is why, all effort shall be taken by the GVS provider to integrate the GVS into the PEPPOL project.

5.5.2 STORK

Secure idenTity acrOss boRders linKed (STORK) is another important European project promoting cross-border interoperability for electronic IDs [65]. The aim of STORK is to provide European citizens with a solution which would enable cross-border authentication using eIDs. STORK aims to replace all services which now require physical presence of European citizens, such as delivering tax papers, university papers etc., by Internet-based services, where citizens could easily authenticate themselves using their eIDs.

The main problem in achieving European cross-border interoperability for eIDs issued locally in different Members States, is that all European countries have their local solutions for identification and authentication of citizens. Besides, many Member States recognize various levels of authentication, which does not provide the same level of assurance. Therefore, EU needs to find a solution to qualify the authentication assurance levels in a common way in all European countries. That is also why, the proposal of IDABC *Proposal for a multi-level authentication mechanism and mapping of existing authentication mechanisms* [66] became the starting point for the STORK project.

The quality information provided by the Global Validation Service seems to be a valuable solution proposal to qualifying the authentication assurance levels of eIDs across Europe. One of GVS main advantages beyond all other validation systems is that it provides independent quality assessment information on certificates and signatures which

are to be validated and/or verified (see section 5.3.6). Therefore, the GVS could successfully resolve one of the main obstacles in providing European cross-border interoperability for eIDs.

Besides, GVS could also resolve the STORK problem of scalability, which is very important when providing solutions to European Union population, which is estimated to be around 500,000,000 citizens. Finally, the contractual legal framework provided by the GVS could also resolve the problem of local legislations regarding issuance and usage of eIDs in all Member States of EU. That is why, similarly to PEPPOL project, the GVS provider shall take all efforts to integrate the GVS to STORK project and in this way promote this PKI interoperability solution in Europe.

5.6 Pros and cons of GVS

In this section we present the most important advantages and disadvantages of the GVS. This evaluation is a result of the our solution analysis through Global VA literature gathered in the study, interviews, and some personal reflections. Both pros and cons of the Global VA are divided regarding the entities that the GVS is supposed to serve, which are : RPs, CAs and certificate holders.

5.6.1 Advantages of GVS

This are the main advantages of the GVS :

Advantages for Relying Parties

1. Possible validation of certificates issued by, in principle, any CA all around the world.
2. Possible validation of multiple signatures.
3. Reverse verification and validation of old documents.
4. RPs don't need to possess necessary resources to perform the certificate processing, which can become in some cases very resource consuming, as it is being performed by the GVS.
5. RPs don't need to sign multiple agreements with many CAs. They rely on one agreement with the GVS provider, that is written and applied according to only one legislation.
6. RPs can take trust decisions independently form all CAs.

7. RPs can easily receive information about any CA (e.g. audit trails, quality information, liability information) from a trusted source.

Advantages for Certification Authorities

1. Possible financial benefits for CAs in the initial phase of GVS development, which is a percentage of the GVS provider income proportional to the number of requests concerning certificates, issued by the CAs, the Global VA has answered for.
2. CAs receive a free of charge assessment of quality of the certificates they provide, which is recognized all around the world.
3. GVS gives CAs possibility to grow on the market, by increasing the interoperability of certificates, issued by those CAs.
4. GVS provides possible hosting of CRLs and their history, so CAs don't have to store them locally, on their own.
5. Cross-border openness.
6. CAs doesn't have to adapt their PKIs, or change their position in existing trust structures, in order to be able to join the GVS structure, because the GVS is a "build-on" type interoperability solution.
7. CAs gain a more predictable risk situation, basing on their agreements with the Global VA, and the RPAs.
8. CAs have a choice of legislation which apply to the agreement they have with the GVS provider, and they no longer have to conform to local legislations.

Advantages for certificate holders

1. Possibility of using one digital certificate world-widely.
2. Complete freedom of choice of the issuer CA, as in principle, all CAs should be integrated into the GVS structure.
3. Independent assessment from the trusted third party auditor of the holder's certificate quality.

5.6.2 Disadvantages of GVS

This are the main disadvantages, we can identify, of the GVS :

Disadvantages for Relying Parties

1. Costs, which can be higher that in current certificate validation. RPs should cover the expenses of CAs' audits, and the costs related to implementation, maintenance and operation of the GVS.
2. RPs will have no choice of GVS provider, as the concept of Global VA assumes that only one GVS would be available on the market.
3. RPs may need to adapt to new GVS client softwares and change their internal procedures regarding the certificate validation.

Disadvantages for Certification Authorities

1. CAs need to make effort of preparing new agreements with the Global VA.
2. Going through an audit can require additional resources, and in some cases can be difficult for the CAs.

Disadvantages for certificate holders

Introducing the GVS will not affect directly the certificate holders, as they don't directly participate in the functioning of the GVS. It is only the issuer CAs audits that can directly affect certificate holders, who can discover the low quality of their certificate and corresponding issuer CAs. However, we don't believe that introducing GVS would result in any major obstacles or disadvantages for the certificate holders.

5.7 Summary

Global Validation Service (GVS) is a solution proposal to the global interoperability for electronic IDs. In this chapter we present both functional and non-functional requirements for the solution for global validation of digital certificates. Then, we answer the question: how the GVS, and its main component the Global Validation Authority (GVS) is supposed to satisfy those requirements. Tables 5.1, 5.2 and 5.3 show how all requirements from section 5.2 are satisfied by our solution proposal.

GVS is based on the contractual relationships with many PKI entities : Relying Parties, Certification Authorities and a trusted third party auditor, which provides independent quality evaluation of digital certificates and digital signatures. In section 5.3 we describe the GVS relationships and all necessary agreements from both legal and business perspective. We also propose different technical implementations for the GVS in section 5.4.

Finally, in the section 5.5 we present some business perspectives for use of the Global Validation System, and we clearly indicate the need for such a system in Europe. We also present the main advantages and disadvantages of the GVS in the section 5.6. We focus on particular PKI entities, involved in the Global VA trust model, and we point out the main pros and cons of the GVS for those entities.

Table 5.1: GVS features meeting the functional general requirements

GVS features	**GR1**	**GR2**	**GR3**	**GR4**	**GR5**	**GR6**	**GR7**	**GR8**	**GR9**
GVA	X	X			X	X			
GVS agreements	X	X					X	X	
Contractual laws	X	X					X	X	
Third party auditor			X	X					X
Quality assessment scheme			X	X	X				X
Certificate validation service					X	X			
Signature verification service						X			

Table 5.2: GVS features meeting the functional specific requirements

GVS features	**SR 1**	**SR 2**	**SR 3**	**SR 4**	**SR 5**	**SR 6**	**SR 7**	**SR 8**	**SR 9**	**SR 10**	**SR 11**	**SR 12**	**SR 13**
GVS web server	X												
GVS front-end implementation		X											X
GVA API layer		X										X	X
GVA			X	X	X	X	X	X	X	X	X		
Third party auditor							X						
Quality assessment scheme							X						
GVS contractual framework								X	X				
OCSP support									X				
CRL support									X				
GVA database									X				
GVS responders	X										X		

Table 5.3: GVS features meeting the non-functional requirements

GVS features	**NR1**	**NR2**	**NR3**	**NR4**	**NR5**	**NR6**	**NR7**
GVS web server	X	X	X				X
GVS responders	X	X					X
GVA			X	X	X		X
GVS front- and back-end implementation			X	X			X
Quality assessment scheme					X		
GVS contractual framework					X		
GVS business model						X	

Chapter 6

Validation Authority in Practice

This chapter presents the evolution of the concept of the Validation Authority as a solution for the global PKI interoperability. It contains a description of the current state of the Global Validation Service, and its actual implementation. Finally, it shows the outcome of our manipulations with a test application of the GVS.

6.1 Introduction

The concept of Validation Authority as an independent third party trust anchor was born around the year 2000. For the last 10 years it was mainly being carried out by Jon Ølnes through many Norwegian companies, from PKI Consulting Services AS to DNV.

In this chapter we present the short history of the VA concept, and we try to explain were the Global Validation Service is today. We also describe the current implementation of the GVS, owned and run by BBS. Finally, we present the outcome of our manipulations with a test application for the GVS for both certificate validation and signature verification.

6.1.1 Short history of VA concept

This section presents the chronology explaining the evolution of the VA concept in Norway.

end of '90 The concept of VA is born inside the company PKI Consulting Services AS, in Norway.

2000 PKI Consulting Services AS evolves into a startup company called Validsign, where the work on the VA concept is continued.

2001	Validsign presents for the first time to DNV the concept of the VA. DNV finds the concept interesting, but it refuses, however, to invest into the project.
2001 - 2003	Validsign is bought by IBM Norge, further discussions over the VA concept are being carried out between IBM Norge and DNV.
December 2003	Agreement is signed between IBM Norge and DNV to make DNV participate in the development of the VA concept.
2004 - 2005	Marketing analysis and promotion/advertisement of the VA concept is being done by DNV on international scale.
November 2005	DNV decides to implement the VA service.
2006	DNV chooses Ascertia to develop software for the VA service.
Summer 2006	The first version of Ascertia implementation of VA service is ready.
2007	VA service is being improved and presented to potential clients.
March 2008	DNV signs the agreement with the first client of the VA service.
February 2009	BBS takes over the VA service from DNV together with the agreements with the subscribed RPs and CAs.

6.1.2 Current situation of the VA concept

Today, the VA concept is being developed and operated by BBS, under the name of BBS Validation Authority Service. Although, the BBS VA platform is fully operational, and BBS took over all DNV's agreements with the client RP and assessed CAs, no transactions using BBS VA Service are yet made. BBS is, however, developing and promoting its validation services, trying to get more interest from private companies and public institutions all across Europe.

Recently, the BBS VA Service was proposed to the *Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC)*,

as one of the solutions for European Federal Validation Services. The outcome of the EFVS Study is presented in this chapter, in the section 6.4.

Finally, BBS is also currently working on the agreement with DNV concerning the outsourcing of quality assessment of digital certificates and corresponding signatures. That is how, DNV is still planning to participate in the development of the VA concept as the independent third party auditor. The role of DNV is described in section 6.3. BBS is also currently preparing its standard agreements with RPs and CAs, which could soon be signed by entities joining the BBS VA trust network.

6.2 BBS VA Service implementation

After BBS took over the VA Service from DNV, not much has changed in its implementation. The number of CAs that BBS has agreements with is very limited (around 15 CAs), and there is only one client RP at the moment. BBS VA Service is still based on the software developed by Ascertia, an international company managed from UK [67]. Ascertia provides PKI solutions, which integrate with existing products around the world, making use of digital signatures and encryption.

During the laboratory exercise we could exercise a test application of the BBS VA Service, which sent requests to the ADSS server for both certificate validation and signature verification. We analyzed the structure of XML requests and responses, and observed the communication between ADSS server and the client test application.

We saw that not all services are yet implemented in the BBS VA, i.e. TSA and OCSP services. We could, however observe, how the certificate validation and the signature verification work, and how the certificate revocation status check is done based on consulting previously downloaded and updated CRLs. We also analyzed the DNV XML Schema Description [68] on which the XML structure of the BBS VA requests and responses is based. In the following sections we present the main aspects of the current BBS VA Service implementation : the ADSS, XML request/response format and the ADSS-client communication scheme.

6.2.1 Advanced Digital Signature Services (ADSS)

Advanced Digital Signature Services (ADSS) is one of the Ascertia products, and it is the core of current VA Service. ADSS provides a flexible framework for signature verification and certificate validation, as well as time-stamping, signing and certificate generation.

ADSS makes the validation services being implemented as Web Services, where the following services are enabled in version 3 of the ADSS : Signing service, Certification service, Verification Service, CRL Management Service, OCSP Service, TSA Service (time-stamping service). Not all of these services are yet used in the BBS VA Service implementation.

The ADSS system consists of three core parts : ADSS server, Database Management System (DBMS) and operator browser. Besides, the ADSS enables many possible external services (see figure 6.1). All external applications communicate with the ADSS server through requests conducted over HTTP/S transport protocol, and they can access ADSS services using either Web Services (XML/SOAP request) or Java API [69].

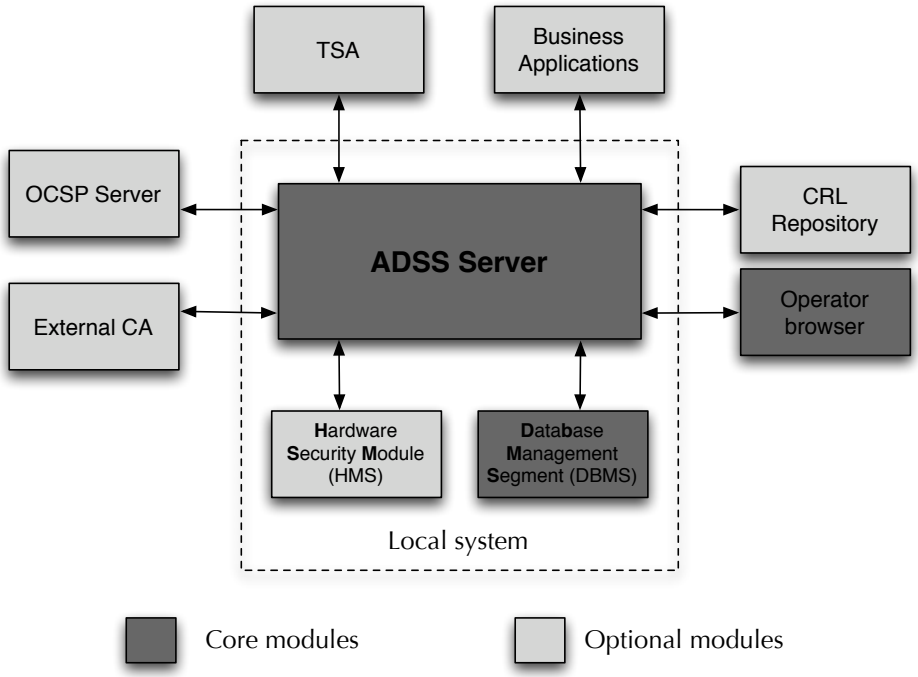

Figure 6.1: The model of ADSS external interfaces.

6.2.2 Request/response format

Requests and responses are currently defined as XML structures which are based on XKMS 2.0 specifications [62]. Figure 6.2 shows an example of the structure of one of the analyzed XML request, which is a certificate validation request. Its root element is

`Verify Request`, which contains the mandatory attribute `TransactionID`, and many mandatory and optional elements.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--    Document Type: ex PDF [5 lines]
<VerifyRequest xmlns="http://www.dnv.com/ict/va/xdsss/" TransactionID="VAS-test-02_CV003">
    <TimeInstant>0012-12-03T02:02:02.002+00:02</TimeInstant>
    <OriginatorInfo>
        <OriginatorID>VAS-test-02</OriginatorID>
        <!-- RespondAddress>info-va@dnv.com</RespondAddress -->
    </OriginatorInfo>
    <QualityLevelRequest>
        <CertificateQualityLevel>3</CertificateQualityLevel>
        <SignatureQualityLevel>3</SignatureQualityLevel>
    </QualityLevelRequest>
    <Version>2.0</Version>
    <RespondWith>KeyValue</RespondWith>
    <RespondWith>HashAlgorithm</RespondWith>
    <RespondWith>X509CertificateChain</RespondWith>
    <!-- RespondWith>X509CRL</RespondWith -->
    <RespondWith>SKI</RespondWith>
    <RespondWith>OCSP</RespondWith>
    <RespondWith>Timestamp</RespondWith>
    <RespondWith>SignHash</RespondWith>
    <RespondWith>ContentHash</RespondWith>
    <!-- RespondWith>Content</RespondWith -->
    <RespondWith>SignatureQualityLevel</RespondWith>
    <RespondWith>CertificateQualityLevel</RespondWith>
    <RespondWith>KeyUsage</RespondWith>
    <RespondWith>ExtendedKeyUsage</RespondWith>
    <RespondWith>BasicConstraints</RespondWith>
    <RespondWith>ValidFrom</RespondWith>
    <RespondWith>ValidTo</RespondWith>
    <RespondWith>CertificateSerialNumber</RespondWith>
    <RespondWith>IssuerName</RespondWith>
    <Request> [43 lines]
</VerifyRequest>
```

Figure 6.2: The XML request for certificate validation.

The `OriginatorInfo` consists of the required element `OriginatorID`, which is a unique identifier for client RPs inside the VA Service. The `QualityLevelRequest`, which is at level 3 by default, indicates the minimum required certificate and signature quality level. The `RespondWith` optional element specifies the parameters that should be included in the ADSS server response.

Finally, the XML request scheme contains the `Request`, which can be of two types: `SV` for signature verification, or `CV` for certificate validation. The presented example is of CV type, and it contains the certificate to be validated by the VA. For more details, on the XML request format see [68].

Figure 6.3 shows the structure of the ADSS response to the request. The `VeryfyResponse` element, which is the root element contains two mandatory attributes, `ResponseID` and `ResponseType` which can take two values : `SV` or `CV`.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP:Header/>
    <SOAP:Body>
        <VerifyResponse xmlns="http://www.dnv.com/ict/va/xdsss/" ResponseID="VAS-test-02_CV003"
            ResponseType="CV">
            <VASID>EMAIL=info-va@dnv.com,CN=SSL Server Authentication,OU=Validation Authority
                Services,O=Det Norske Veritas AS - NO 945748931,C=NO</VASID>
            <QualityLevelResponse>
                <CertificateQualityLevel>3</CertificateQualityLevel>
                <SignatureQualityLevel>3</SignatureQualityLevel>
            </QualityLevelResponse>
            <TimeInstant>2009-07-22T09:42:12.530+02:00</TimeInstant>
            <Version>2.0</Version>
            <OriginatorInfo>
                <OriginatorID>VAS-test-02</OriginatorID>
            </OriginatorInfo>
            <ResultMajor>Success</ResultMajor>
            <ContentsVerifyResult>
                <ContentVerifyInfo OverallAssertionStatus="Trusted">
                    <VerifyInfo AssertionStatus="Valid" Id="Cert.id.01_1">
                        <SignatureAuxInfo> [58 lines]
                        <CertificateValidityInfo>
                            <ValidityInfo>
                                <ThisUpdate>2009-05-15 13:11:45.0</ThisUpdate>
                                <NextUpdate>2009-11-16 00:31:45.0</NextUpdate>
                            </ValidityInfo>
                            <Certificate>MIIGGDCCBACgAwIBAgIKYTGSXgAAAAAAEzANBgkqhkiG9w0BAQUFADCBgzELMAkG&#xD; [32 lines]
                        </CertificateValidityInfo>
                        <Name>EMAIL=dolly.duck@dnv.com,CN=Dolly Duck,OU=Validation Authority
                            Services,O=Det Norske Veritas AS - NO 945748931,C=NO</Name>
                    </VerifyInfo>
                </ContentVerifyInfo>
            </ContentsVerifyResult>
            <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"> [20 lines]
        </VerifyResponse>
    </SOAP:Body>
</SOAP:Envelope>
```

Figure 6.3: The XML response from the ADSS Server to the XML request.

Other main mandatory elements of the response are : The Validation Authority Service Identification `VASID`, `OriginatorInfo`, `QualityLevelResponse`, the overall result of the certificate validation `<ResultMajor>Success</ResultMajor>`, and `ContentsVerifyResult`, which contains a detailed outcome of the certificate validation. The element `SignatureAuxInfo` can also contain some auxiliary information requested by the client.

Finally, all ADSS responses are signed by the VA Service, and the signature in included in the `Signature` element of the `VeryfyResponse`. For more details on the XML scheme see [68].

6.2.3 ADSS - client communication

During our laboratory exercise we observed the communication between the test client RP and the ADSS Server. This communication is protected by HTTPS, using SSL protocol. The client authenticate itself with SSL client certificate issued by the BBS VA Service.

Therefore, the ADSS - client communication begins with an SSL client-authenticating handshaking procedure, see figure 6.4. During this procedure the client sends the `client_hello` message specifying the highest TLS protocol version it supports, which is `3.1`. ADSS server receives the message and it accepts the specified version.

```
***                                                                    ***

Sending request to ADSS using SSL client authentication
ssl_debug(1): Starting handshake (iSaSiLk 3.06)...
ssl_debug(1): Sending v3 client_hello message, requesting version 3.1...
ssl_debug(1): Received v3 server_hello handshake message.
ssl_debug(1): Server selected SSL version 3.1.
ssl_debug(1): Server created new session 54:3B:00:00:AF:DB:E8:A0...
ssl_debug(1): CipherSuite selected by server: SSL_RSA_WITH_3DES_EDE_CBC_SHA
ssl_debug(1): CompressionMethod selected by server: NULL
ssl_debug(1): Received certificate handshake message with server certificate.
ssl_debug(1): Server sent a 2048 bit RSA certificate, chain has 2 elements.
ssl_debug(1): ChainVerifier: No trusted certificate found, OK anyway.
ssl_debug(1): Received certificate_request handshake message.
ssl_debug(1): Accepted certificate types: RSA
ssl_debug(1): Accepted certificate authorities:
ssl_debug(1):    CN=DNV VA Services CA 1,OU=Validation Authority Services,O=Det N
orske Veritas AS - NO 945748931,C=NO
ssl_debug(1):    CN=va-services.dnv.com,OU=Validation Authority Services,O=Det No
rske Veritas AS - NO945748931,C=NO
ssl_debug(1): Received server_hello_done handshake message.
ssl_debug(1): Sending certificate handshake message with RSA client certificate.
..
ssl_debug(1): Sending client_key_exchange handshake message (2048 bit)...
ssl_debug(1): Sending certificate_verify handshake message...
ssl_debug(1): Sending change_cipher_spec message...
ssl_debug(1): Sending finished message...
ssl_debug(1): Received change_cipher_spec message.
ssl_debug(1): Received finished message.
ssl_debug(1): Session added to session cache.
ssl_debug(1): Handshake completed, statistics:
ssl_debug(1): Read 3446 bytes in 3 records, wrote 2144 bytes in 5 records.
ssl_debug(1): Exception reading SSL message: java.io.EOFException: Connection cl
osed by remote host.
ssl_debug(1): Shutting down SSL layer...
ssl_debug(1): Read 25387 bytes in 7 records, 25178 bytes net, 3596 average.
ssl_debug(1): Wrote 64782 bytes in 118 records, 61476 bytes net, 520 average.
ssl_debug(1): Closing transport...
ssl_debug(1): Closing transport...
ssl_debug(1): Closing transport...
ssl_debug(1): Closing transport...
Time taken to process the request : 5.619 second(s)
```

Figure 6.4: The message exchange between the ADSS Server and the client sending the XML test request.

Next, the server chooses a random number, the cypher suite and the compression method, and it sends it together with the server certificate to the client. The client analyzes the received certificate, it verifies the chain, `ChainVerifier`, and it decides

to trust the root CA. The server also asks the client to send its certificate in exchange, in the `certificate_requets` message, so the communicating entities can mutually authenticate each other.

Once the public keys are exchanged between the ADSS server and the client, the verification of the certificates occurs. The client sends `client_key_exchange` message which contains randomly generated number, called *PreMasterSecret (PMS)*. Then, the both sides calculate the *Master Key (MK)* which will be now on used for the encryption of any further messages.

From now on the client and the server change to the encrypted connection and the client finally sends the certificate to be verified by the Global VA, which is included in the message `certificate_verify`.

6.3 The role of DNV in the BBS VA Service

DNV agreed on providing BBS with the quality assessment of digital certificates and corresponding signatures. The certificates' quality assessment is done today mainly by evaluating the CAs' certificate policies, whereas signatures' evaluation is based on assessing the cryptographic algorithms used to generate those signatures and the Certificate Policies for the corresponding digital certificates. No assurance level is yet provided by DNV, but DNV is currently working on implementing its third version of quality parameters, which will include the second quality parameter indicating the level of independent assurance which can be associated with the quality claimed by the CAs in their CPs.

The DNV classification scheme for digital certificates is nowadays composed of 7 quality levels, from 0 to 6, where 0 corresponds to an inadequate or non-determined level, and 6 corresponds to a qualified signature level (for complete list of all six DNV quality levels for certificates see [70]). Including in the classification scheme the qualified approved level number 5 and qualified signature level number 6 makes the GNV scheme conform to the EU legislations concerning qualified certificates.

DNV determines the digital signature quality, using the following formula :

$$Signature\ quality = certificate\ quality + hash\ algorithm\ quality + public\ key\ algorithms\ and\ key\ size\ quality$$

However, it is the certificate quality level that determines the most the final quality of the assessed signature. If the certificate quality is 0, then automatically the signature quality

obtains the 0 quality level. However, if the certificate quality level is 6, and all other parameters have at least the value 1, then the assessed signature is directly classified as a qualified signature. The detailed specification of DNV version 2.0 quality parameters is described in [70].

6.4 BBS VA Service and the European Union

European Union has recently taken interest into ensuring electronic signature verification at European level. *Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC)* [71] develops solutions and prepares recommendations to enable electronic communication among administrative bodies inside EU. IDABC provides services to both business and citizens of EU.

Among its other activities, in 2009 IDABC conducted an *European Federated Validation Service (EFVS)* Study [72], which aimed to asses the availability of a solution for digital signature validation on the European scale. Many companies from all over the world submitted their solutions, which were then independently assessed.

One of the submitted solutions was the BBS Validation Authority, which was chosen as one of the three most complete solutions currently available. In the next section we will present the evaluation of the BBS VA Service by EFVS and we will specify how, according to the results of this study, the VA Service should be improved to become the most suitable validation authority service for European Union.

6.4.1 EFVS Study

EFVS Study aimed to asses the feasibility of electronic signature verification service, which should provide the three most demanded functionalities : validation of certificates, verification of signatures, and liability towards the end users [72]. Three out of twenty proposed solutions possessed those three characteristics and they were the following : *@firma* platform form Spain, *e-Notarius* solution form Poland and BBS Validation Authority from Norway.

On one hand, both @firma and e-Notarius created their solutions built on existing trust model based on the concept of qualified certificates supervised nationally by every EU Member State. On the other hand, BBS proposed a solution that introduced a complete new trust model, which is based on a large cross-border contractual framework.

First we will present the evaluation of the BBS VA Service by the EFVS Study. Then we will compare the BBS VA Service together with @firma and e-Notarius solutions, in order to point out the weak and strong points of the BBS VA Service based on the EFVS Study. Finally, we will conclude how BBS VA Service should be improved to stand up to the expectations of the IDABC.

6.4.2 Evaluation of BBS VA Service by EFVS Study

The EFVS Study assessed the signature verification service proposals in three main steps [72] :

- **functional and organizational characteristics**, focussing on geographical and sector scope of the solution, as well as the business model of proposed solutions and its actual uses.
- **technical characteristics**, assessing the technical operation of the solutions, their certificate validation and signature verification approaches and their logging, or auditing systems. The key factors of the assessment were the flexibility and scalability of the solutions, as in European context the number of users and transactions will probably increase over time, so will the number of existing standards. Therefore, it is important for technical interoperability, that the proposed solutions respect existing most broadly used standards, and that they can easily adapt to potential new standards.
- **legal characteristics**, focussing on their relationships with the CAs and RPs, used criteria for assessment of certificate quality and for determining legal signature value, as well as assessing their liability/responsibility model and international legal model.

We will present the assessment of the BBS VA Service solution, contrasting it with the closest concurring solutions, which was also assessed in the EFVS Study [72].

Functional and organizational characteristics

EFVS Study showed that BBS VA Service Validation Authority solution, unlike the other proposed solutions, has nearly no geographical restriction, because it provides an independent assessment of CAs to ensure that they meet required standards. Besides, it also confirmed that BBS solution, together with e-Notarius solution, is generic in scope, and therefore can be applied to any sector.

The business model of the BBS for-profit solution also confirmed that BBS can provide its services internationally, as BBS uses its own multi-level policies, which result in particular agreements with CAs issuing both qualified and non-qualified certificates. The other for-profit solution, e-Notarius, focuses only on CAs issuing qualified certificates. Those CAs are supervised on national scales, and thus e-Notarius doesn't provide any independent assessment of those CAs.

The main weak point of the BBS solution is that its actual use is very limited, comparing with the e-Notarius and @firma solutions. According to the EFVS Study, @firma solution seems to be the leader in use, being active in use since March 2006, and having a throughput of 900.000 transactions per month. BBS solution, on the other hand, is fully operational, but it hasn't yet been used in any transactions.

Technical characteristics

The EFVS Study pointed out many technical drawbacks in the BBS solution. First, the BBS VA Service does not support all signature standards, i.e. XKMS [62] or OASIS DSS [73]. Second, it doesn't provide certificate content mapping to normalized XML scheme. Third, contrary to e-Notarius and @firma, BBS doesn't provide time stamping services [72].

Those drawbacks show that the BBS solution is technically weak comparing with other assessed proposals. However, BBS VA Service has also some technical advantages. According to the EFVS Study, BBS is the only solution which foresees to build on XKMS for certificate verification, to meet PEPPOL requirements. Other proposals, on the contrary, only operates basing on the OCSP and CRLs.

When it comes to the certificate verification, BBS VA Service doesn't support many signature formats, i.e. PDF, ODF or XMLDsig. Therefore, the BBS solution is not as complete as e.g. the @firma proposal, although it supports the main standard signature formats. Implementing those signature formats into the BBS VA Service would improve its interoperability and would help it extend its use globally.

Finally, the EFVS Study assessed the logging and auditing systems of proposed solutions. The Study showed that, comparing to the @firma solution, the BBS proposal has a less complete logging system. It could be improved if e.g. logs were signed every day to guarantee its integrity and authenticity, as it is done in @firma. Besides, it could be useful to implement the possibility of filtering logs by transactions, and aggregate them into easy-to-read formated file.

Legal characteristics

The EFVS Study underlined that the BBS solution is based on double agreements, with RPs and CAs, which define services and liabilities of each party. Those agreements also specify the compensations to be paid by RPs to BBS, and by BBS to CAs. The BBS solution, was the only one, among the 20 assessed proposals, which precisely regulated its relationships with both RPs and CAs.

Besides, BBS provided the most detailed criteria for the certificates' quality assessment among all submitted solutions. The study pointed out the independent multilevel framework of certificate assessment created by BBS, which takes into account the European concept of qualified certificates, thus it meets EU requirements. BBS VA Service, however, also potentially allows to integrate non-European CAs into the European model, which can can extend the international perspective of the European signature validation service.

The EFVS Study underlined, however, that qualified certificates are not really broadly used in practice across EU. Therefore, according to the study, it seems currently that the BBS solution, which allows its users to make the distinction between qualified and non-qualified certificates, is too complicated for now. This point, however, seems to us as a very short-time vision, since qualified certificates are supposed to become more and more used in practice in the future. We also believe that, in this context, the BBS VA Service proves its long time usability.

At the same time, the BBS VA Service is the only solution which does not provide an autonomous assessment of certificates quality, but also of the digital signature value. BBS provides a fine-grainded scale of both certificate and signatures assessment, allowing the client RPs to specify what type of signatures and certificates they consider acceptable for their use.

According to the EFVS Study, BBS was also the only company, which is willing to take on liability, becoming the sole point of responsibility as the Validation Authority. All other assessed companies position themselves as intermediary services providers. Finally, BBS VA Service, as the only one from all proposed solution, has an international model in place.

6.4.3 Summary of the EFVS Study

In this section we present a summary of the BBS VA Service evaluation by the EFVS Study in comparison with the two main competing solutions investigated in details in

the Study [72]. For the short summary, see the table 6.1, or consult [72] for more detailed evaluation of all solutions submitted to the EFVS Study.

Table 6.1: Comparison of three main solutions evaluated by the EFVS Study.

Assessed feature	**@firma**	**e-Notarius**	**BBS**
Sector scope	Primarily designed to public administration, but no restrictions in principle	No restrictions	No restrictions
Geographical scope	By principle restricted to Spain	By principle restricted to Poland	No geographical restrictions
Business model	Non-profit	For-profit with free service for non-commercial use	For-profit
Actual use	900.000 transactions per month	250.000 proofs of transactions delivered for the Study	Fully operational, but not yet in use
Important standards	Validation service based on OASIS WS-I Basic Profile v1.1	Validation services based on DVCS protocol	Usage of XKMS is foreseen
Supported signature formats	PKCS#7, CMS, CADES-BES, -T, -C, -X, -XL, -A, XMLDsig, XADES-BES, -T, -EPES, -C, -X, -XL, -A, PDF and ODF	PCKS#7, CMS, XML, PDF, XML, PDF, XAdES, CAsES, SDOC, SignPro and ZEP	PKCS#7, CMS, XML, PDF, XAdES, CAdES
Logging/ auditing	Particularly complete	Complete	Complete (in theory could be improved)
Agreements with CAs	Yes	No	Yes, with precisely regulated compensation
Agreements with RPs	Yes	Yes	Yes, with precisely regulated compensation

Assessed feature	**@firma**	**e-Notarius**	**BBS**
Certificate validation approach	Supports only qualified certificate	Supports only qualified certificate	Multilevel assessment of quality
Signature verification approach	Provides information on SSCDs	Distinguish between qualified/non-qualified signatures	Multilevel assessment of quality
Liability	Intermediary service, not taking any liability	Relies on general liability provisions of the eSignatures Act in Poland	Is willing to take on liability for its transactions
International model	Not supported	Not supported	Yes

6.5 Summary

In this chapter, we presented the complete evolution of the Validation Authority concept over the past 10 years to its current implementation at BBS. We underlined, that, although the certificate validation and signature verification services are tested and operational, the BBS VA Service still doesn't provide time-stamping services, nor is the certificate validation using the OCSP implemented yet in the ADSS Server.

BBS VA Service is currently a Web Service, which uses HTTPS, over a SSL channel, to protect its communication with client RPs. The client requests and ADSS responses are defined using XML structures, which are described in details in [68], and which are based on XKMS 2.0.

Finally, we presented the BBS VA Service evaluation by an independent EFVS Study, and we compared it to other concurrent solution proposals for European Federal Validation Service. We pointed out its weak points, which are mainly on the technical side. We also described its strong points, which is a high interoperability potential on international scale, and its solid contractual framework.

Chapter 7

Validation of the Research

This chapter contains the validation of the research presented in the thesis. We evaluate how the goals of particular steps of the research were realized. We focus on strong and weak points of our research, and we present some suggestions for improvements that could have been made. Finally, we briefly discuss some confidentiality issues concerning our research.

7.1 Realization of goals

This section evaluates all steps of the research, in order to be able to validate our conclusions. For each step of the research we focus on answering the following questions:

1. why was this step taken?
2. what was the goal of the research step?
3. how well was the research data gathered?
4. how relevant was the gathered data?
5. how exhaustive was the data analysis?
6. how did the the research step contribute to solving the research problem?
7. was the goal of the step attained?

This chapter also analyses what were the strongest and the weakest points of every research step. Those are described as Pros and Cons.

7.1.1 PKI study

The research began with the literature study of the cryptographic theory and the most important PKI concepts, which were then described in chapter 2. The goal of this research step was to understand the underlying theory of electronic IDs, and become aware of important PKI issues related to the entire life-cycle of digital certificates.

For the PKI study, we selected a large variety of PKI literature, which comprised books, PKI-related research papers, technical reports, PKI standards and PKI conference proceedings. All gathered documents were coming from different and independent sources, and were written by European, American or Asian authors. We believe that the large variety of selected literature (see Bibliography, at the end of the document) shows that all important PKI issues were broadly covered in our research.

Besides, we believe that the volume of chapter 2, and all included definitions and explanations demonstrate the deep PKI understanding, that we gained during the first phase of the research. That is how, we attained the goal of this step, and everything we learned about PKI became essential for all following steps of the research.

Pros

The strongest point of the PKI study presented in this thesis, is its scope and broad coverage of all important PKI issues. In chapter 2 we presented an exhaustive list of public-key cryptography services, public-key algorithms and PKI concepts.

Cons

Some of presented concepts lack, however, in detail and technical descriptions. In order to limit the volume of the thesis, we couldn't provide all relevant information about all existing public-key algorithms, services and PKI concepts. That is why, we tried to provide the readers with indications on possible further reading on those subjects (see Bibliography).

7.1.2 PKI trust models study

In the second step of the research we had to analyze existing PKI trust models in order to understand why they are not sufficient in providing the solution to global interoperability for electronic IDs. The goal of the study, was to demonstrate why those models can not become the solution to our research problem, and why there is a need for a new PKI trust model.

In this step we also studied PKI literature, which included mainly research papers on PKI, some of which were proceedings from PKI conferences. This study gave us a good understanding of existing PKI models, e.g. subordinate hierarchies, cross-certified mesh, bridge CAs and trust lists, as well as some theoretical models, i.e. gateway CAs. We evaluated their possibilities of becoming solutions to global PKI interoperability, and we compared them.

Chapter 3 presents an exhaustive list of existing PKI trust models, and it highlights their strong and weak points. This chapter clearly demonstrate that, in order to achieve a global PKI interoperability a new implementable PKI trust model is required. That is how we achieved the goal of this research step.

Pros

The chapter 3 clearly shows weak and strong points of presented PKI trust models, based on documented literature study and on my own assessment. Besides, we believe that the presented list of existing models is exhaustive, and it includes all currently available solutions to PKI interoperability. Finally, our research covered an interesting solution, called gateway CAs. This demonstrates that in our research we went outside well-known and available solutions, and we presented an outcome of the most recent research being done in the domain of PKI trust models.

Cons

In chapter 3 we present only one proposition of a a new theoretical PKI trust model. During our research, we did not come across other interesting research which would describe new propositions for PKI trust models. This is why, in our research we did not cover exhaustively all newest research in the domain of PKI trust models.

7.1.3 Interoperability initiatives study

The goal of the third step of our research was to provide us with understanding of PKI standardization efforts, as well as existing interoperability initiatives that have been existing all around the world in the past 20 years. To achieve this, we gathered many various PKI standards, description of interoperability projects and technical specifications of existing interoperable PKIs in some countries, i.e. U.S., Germany, Japan and Canada (see Bibliography).

When analyzing those interoperability initiatives we tried to understand and describe what were their strong and weak points, and why those solutions were unsuccessful in

becoming globally interoperable PKIs. We analyzed documents which were not interpretations or descriptions of existing standardization initiatives, but the standards itself. That is why, we believe that our analysis was based on highly relevant documentation.

We believe, that we clearly presented all positive and negative points of interoperability solutions taken in various countries all around the world, and this is how we achieved the goal of this research step. Finally, this step helped us to understand how to specify our solution to PKI interoperability, in order to avoid repeating weaknesses of already existing interoperability initiatives.

Pros

The outcome of our research, presented in chapter 4 contains a long list of PKI standards activities and PKI interoperability initiatives, which are all relevant to answer our research problem. In this step we gave readers an overview of many interesting PKI interoperability initiatives, that were taken simultaneously in many different places in the world, including North America, Europe and Asia. We believe that the spectrum of presented solutions is large, and that it gives an interesting insight to global activity in PKI interoperability.

Cons

Chapter 4, however, does not contain an exhaustive list of PKI interoperability practices in all countries in the world. We selected only those countries, where PKI interoperability initiatives were well documented, and were the most relevant for our research. Therefore, the readers shall be aware of that many other countries, although they were not presented in chapter 4, may have some PKI interoperability activity.

7.1.4 VA concept study

In the next research step, which was done in parallel with the solution proposal study and which is described in chapter 6, we studied the VA concept by reading relevant literature. We also interviewed many persons who have been developing this concept over the last 10 years. We needed to well understand the concept, in order to be able to write an exhaustive requirement specification for our solution, and to be able to critically analyze and asses the BBS VA service.

All interviewed persons were highly qualified experts with important PKI experience. Besides, some of them were among the main creators of the VA concept. All of them have to some extent contributed in the implementation of the VA service, which is today

the BBS VA service. All information gathered during the interviews, was valuable and relevant for our research.

We analyzed the gathered data to provide a complete overview of the BBS VA service in chapter 6. Finally, we presented an independent evaluation of the BBS VA service done by the IDABC, which compared the BBS VA service with other validation services available in different countries around the world. All information learned during the VA concept study gave us an important input to the solution proposal presented in chapter 5.

Pros

The presentation of the VA concept in chapter 6 is a result of a unique experience, which included interviews with the most important persons, who have been developing the VA service, as it is today. During our research we gained a broad knowledge of the VA concept, from many various perspectives. Finally, we analyzed and presented the outcome of the IDABC study, which highlighted all weak and strong points of the BBS VA service.

Cons

Although, we present the detailed structure of requests/and responses of the BBS VA service, as well as we briefly introduce its technical implementation, our description lacks in an overall architectural design of the BBS VA service. This architectural description could be added in a continuation of the research on VA service.

7.1.5 Solution proposal validation

The goal of the solution proposal described in chapter 5 was to present in details all aspects of the Global Validation Service, including its technical, business, and legal issues. We used all information gathered throughout all preceding steps as input to this research step. We also received some advices from different experts, such as e.g. a security officer, during consequent interviews.

Chapter 5 includes a long list of requirements specification for the GVS. This proves our deep understanding of the PKI interoperability problem, and the need for a new service, which could become the solution to global PKI interoperability. Besides, the solution proposal includes a detailed description of the Global VA, GVS relationships, legal issues, GVS business model, GVS agreements and the quality assessment scheme. Chapter 6 also includes different propositions for technical front-end and back-end implementation of GVS.

We believe, that the solution proposal to global PKI interoperability presented in the thesis is exhaustive, and that it provides solid basis for future development of the BBS VA service. That is how, we believe that the goal of the entire research was achieved.

Pros

Chapter 5 covers all important issues concerning the implementation and management of the Global Validation Service. It provides solutions to many technical, legal and business issues, and it describes different technical and business possibilities for the GVS. That is why, the solution proposal is detailed and complete, and it provides clear description of advantages of the GVS, as well as it introduces some disadvantages and/or obstacles, which could be encountered when developing the service.

Cons

Although the solution proposal is complete, it presents only European business scenarios for GVS, which are only one of the steps in achieving global PKI interoperability. More business scenarios for GVS shall be presented in a future research on the GVS subject.

7.2 Confidentiality issues

For some business and security reasons, not all information gathered during the research was directly reflected in the thesis. This is perfectly understandable, as the current implementation of the validation service is one of BBS products, and it also involves other companies, such as DNV, contracted RPs and CAs. We believe, however, that this thesis, which is an open document, presents a complete overview of the VA concept and that our solution proposal to the global PKI interoperability covers all important aspects of a validation service, without disclosing any confidential information related to BBS and other involved companies' business.

Chapter 8

Conclusion

This chapter presents the conclusions drawn from the entire research. It also describes our suggestions for future research in the domain of interoperability for electronic IDs, especially on the subject of the Global Validation Service.

8.1 Conclusion

Interoperability is a critically important issue for multi-vendor community of Public Key Infrastructure providers. Interoperability, which covers many issues, such as technology, business and legal aspects, ensures flexibility and freedom of choice among vendors. That is how the global interoperability for eIDs would allow a wide-scale deployment of PKIs.

In our research we presented PKI concepts, explaining why electronic IDs are an important solution to ensure security in remote communication. We demonstrated that a PKI, which acts as an application enabler, is a vast framework providing support to many security services. In our thesis we explained why PKI-based solutions are valuable, and why they are broadly used all around the world.

Our research also demonstrates, that although the PKI technology has been used in the world for around 20 years, no successful solution to provide global PKI interoperability has yet been introduced. In the thesis we presented all existing PKI interoperability models, and clearly indicated their weak points, which provoked that none of these models was applied on the global scale.

We also described the most important standardization efforts and interoperability initiatives that have been taken all around the world in the past 20 years. Thus, we showed

that although many of the efforts contributed to providing PKI interoperability to limited environments, the global PKI interoperability have not yet been achieved. In our research we tried to focus on positive benefits from existing standards and interoperability solutions when proposing our solution to global PKI interoperability.

In the thesis we introduced the concept of Global Validation Service (GVS). Our solution is based on the VA concept, which in the last 10 years was mainly carried out by researchers working at DNV, and which recently became a BBS product, called BBS VA. The GVS is a "build-on" type solution which does not require modifying already existing interoperable PKI trust networks. On the contrary, it introduces a new PKI entity, called Validation Authority (VA), which could provide validation services for RPs independently from CAs, disregarding any trust networks that the RPs and CAs are involved in.

In our research we studied all aspects of the GVS and presented a complete overview of technical, business and legal issues related to developing and managing of the GVS. We clearly underlined, that among the most important advantages of the GVS service were the following GVS properties:

1. GVS provides independent and trustworthy quality information on digital certificates, and related signatures, allowing qualifying of certificates' assurance levels on the international scale.

2. GVS provides a contractual legal framework, which guarantees all entities joining the GVS structure the flexibility of choices of legislations which will govern the entities' agreements with the GVS provider. That is how GVS contractual laws may in many cases be advantageous over local legislations.

3. GVS solves the problem of global/international scalability, because it provides a single trust point for all RPs, and it reduces the total number of agreements required to provide PKI interoperability framework in an environment with numerous CAs and RPs.

4. GVS allows mapping of local certificates' assurance levels on an international scale, by providing an independent and trustworthy quality assessment framework.

We also focused on some existing competing propositions to provide cross-border validation services in Europe which were submitted to EFVS study by IDABC. We presented important results of this study, and demonstrated what are the weak and strong

points of the BBS VA service, compared with two other solutions to global interoperability. We clearly suggested how the BBS VA service should be improved to become considered as the solution to European PKI interoperability for eIDs.

Finally, we demonstrated two of the currently most important opportunities for development and promotion of GVS service internationally. Two business scenarios PEPPOL and STORK can contribute to make the VA concept emerge in Europe. The VA concept, which according to many PKI experts was born too early for its time, could finally come out and become integrated in large-scale European projects aiming to ensure interoperability for eIDs and electronic signatures .

8.2 Future work

Our research provided an exhaustive list of propositions to the development and implementation of Global Validation Service, as well as an objective evaluation of the BBS VA service. In the continuation of the research on providing validation services globally and making eID interoperable internationally, we suggest that improvements should be made to the current implementation of the BBS VA service.

On the technical side, one of the proposed communication protocols should be chosen and implemented in the service. This protocol should, however, conform to the business scenarios that are going to be chosen for the service. It means that if the BBS VA service is to be integrated with the PEPPOL project the technical specification of the service should conform to the requirements specified in the PEPPOL deliverable [63]. Besides, the future research should investigate the possibility of implementing validation services in standard applications handling digitally signed documents, such as Adobe or Microsoft Outlook. The implementability of such a solution should be assessed, and a technical specification for such implementation should be performed in future research.

On the legal and business side, the future research should focus on implementing GVS agreements and on investigating local legislations which could govern those agreements, depending on the geographical focus for the validation service development. Besides, a clear quality assessment scheme for digital certificates and related signatures should be prepared in order to provide a solid framework for qualifying certificates' assurance levels on an international scale.

Index

Bibliography

[1] Javier Lopez, Rolf Oppliger, and Günther Pernul. *Classifying Public Key Certificates*. In David W. Chadwick and G. Zhao, editors, *EuroPKI 2005*, pages 135–143. Springer-Verlag Berlin Heidelberg, 2005.

[2] Jon Ølnes. *PKI Interoperability by an Independent, Trusted Validation Authority*. *DNV Research*, February 2006.

[3] Jon Ølnes and Leif Buene. *Use of a Validation Authority to Provide Risk Management for the PKI Relying Party*. In A.S. Atzeni and A. Lioy, editors, *EuroPKI*, June 2006.

[4] Carlisle Adams and Steve Lloyd. *Understanding PKI, Concepts, Standards, and Deployment Considerations*. Number ISBN 0-672-32391-5. Addison-Wesley, second edition, 2003.

[5] *New Directions in Cryptography*, number 22(6):644-654. IEEE Transactions on Information Theory, November 1976. `http://www.cs.purdue.edu/homes/ninghui/courses/Fall04/lectures/diffie-hellman.pdf`.

[6] XML Signature Syntax and Processing (Second Edition), June 2008. `http://www.w3.org/TR/xmldsig-core/#def-SignatureEnveloped`.

[7] DI Management Services. RSA Algorithm. Webpage, January 2008. `http://www.di-mgt.com.au/rsa_alg.html`.

[8] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. *Recommendation for Key Management - Part 1: General (Revised)*. National Institute of Standards and Technology, May 2006.

[9] David A. Carts. *A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols*. SANS Institute, November 2001.

[10] U.S. Department of Commerce/National Institute of Standards and Technology. *Data Encryption Standard (DES)*, number FIPS PUB 46-3. Federal Information Processing Standards Publication, October 1999.

[11] *Announcing the Advanced Encryption Standard (AES)*, number 197. Federal Information Processing Standards Publication, November 2001.

[12] Shirley Radack, editor. *The cryptographic hash algorithm family : revision of the secure hash standard and ongoing completition for new hash algorithms*. National Institute of Standards and Technology, March 2009.

[13] Reinhard Wobst and Jürgen Schmidt. Hash cracked. The consequences of the successful attacks on SHA-1. *The H Security*, August 2006. `http://www.h-online.com/security/Hash-cracked--/features/75686`.

[14] Xiaoyun Wang and Hangbo Yu. How to break MD5 and other hash functions. In *In EUROCRYPT*. Springer-Verlag, 2005.

[15] Russell Housley, Warwick Ford, William Polk, and David Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Technical Report RFC 3280, Internet Engineering Task Force, April 2002. `http://www.ietf.org/rfc/rfc3280.txt`.

[16] Stephen Farrell and Russell Housley. An Internet Attribute Certificate Profile for Authorization. Technical Report RFC 3281, Internet Engineering Task Force, April 2002. `http://www.ietf.org./rfc/rfc3281.txt`.

[17] Carl M. Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian M. Thomas, and Tatu Ylonen. SPKI Certificate Theory. Technical Report RFC 2693, Internet Engineering Task Force, September 1999. `http://tools.ietf.org/html/rfc2693`.

[18] *An Introduction to Cryptography*. Network Associates, Inc, 2000. `ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf`.

[19] Yoshiaki Kawatsura. Secure Electronic Transaction (SET) Supplement for the v1.0 Internet Open Trading Protocol (IOTP). Technical Report RFC 3538, Internet Engineering Task Force, June 2003. `http://www.faqs.org/ftp/rfc/pdf/rfc3538.txt.pdf`.

[20] Santosh Chokhani, Warwick Ford, Randy Sabett, Charles Merrill, and Stephen Wu. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Technical report, Internet Engineering Task Force, November 2003.

[21] Microsoft Information Security and Technology Training Center Moscow Engineering Physics Institute. Pki Protocols, 2004. http://maic.ru/PKI/eng/ppt/05.%20pki%20protocols.ppt.

[22] Russell Housley and Paul Hoffman. Internet X.509 Public Key Infrastructure Operational Protocols : FTP and HTTP. Technical Report RFC 2585, Internet Engineering Task Force, May 1999. http://www.ietf.org./rfc/rfc2585.txt.

[23] Carlisle Adams and Stephen Farrell. Internet X.509 Public Key Infrastructure Management Protocols. Technical Report RFC 2510, Internet Engineering Task Force, March 1999. http://www.ietf.org./rfc/rfc2510.txt.

[24] Carlisle Adams, Stephen Farrell, Tomi Kause, and Tero Mononen. Internet X.509 Public Key Certificate Management Protocol (CMP). Technical Report RFC 4210, Internet Engineering Task Force, September 2005. http://www.ietf.org./rfc/rfc4210.txt.

[25] Steve Lloyd. Understanding Certification Path Construction. *PKI forum*, September 2002. http://www.oasis-pki.org/pdfs/Understanding_Path_construction-DS2.pdf.

[26] John Linn. Trust Models and Management in Public-Key Infrastructures. November 2000. ftp://ftp.rsasecurity.com/pub/pdfs/PKIPaper.pdf.

[27] Jim Turnbull. Cross-Certification and PKI Policy Networking. *Entrust*, August 2000. http://www.entrust.com/resources/pdf/cross_certification.pdf.

[28] Federal PKI Policy Authority, editor. *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, February 2009.

[29] Helena Rifà-Pous and Jordi Herrera-Joancomartí. An Interdomain PKI Model Based on Trust Lists. In J. Lopez, P. Samarati, and J.L. Ferrer, editors, *EuroPKI 2007*, pages 49–64. Springer-Verlag Berlin Heidelberg, 2007.

[30] Zheng Guo, Tohru Okuyama, and Mrion F. Finley. A New Trust Model for PKI Interoperability. *IEEE Computer Society*, 2005.

[31] Asia PKI Forum. Webpage. http://www.asia-pkiforum.org/.

[32] Russell Housley, Warwick Ford, William Polk, and David Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Technical Report RFC 2459, Internet Engineering Task Force, January 1999. http://www.ietf.org/rfc/rfc2459.txt.

[33] Public Key Infrastructure (X.509) (pkix). Webpage, August 2008. http://www.ieft.org/html.characters/pkix-charter.html.

[34] Santosh Chokhani and Warwick Ford. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Technical report, Internet Engineering Task Force, March 1999. http://www.ietf.org/rfc2527.txt.

[35] LDAP Extension (ldapext). Webpage, March 2008. http://www.ieft.org/html.characters/OLD/ldapext-charter.html.

[36] Kurt Zeilenga. Lightweight Directory Access Protocol (LDAP) : Technical Specification Road Map. Technical Report RFC 4510, Internet Engineering Task Force, June 2006. http://www.ietf.org/rfc/rfc4510.txt.

[37] Blake Ramsdell. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling. Technical Report RFC 3850, Internet Engineering Task Force, July 2004. http://www.ietf.org/rfc3850.txt.

[38] Blake Ramsdell. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification. Technical Report RFC 3851, Internet Engineering Task Force, July 2004. http://www.ietf.org/rfc3851.txt.

[39] Jürgen Brauckmann, Alfred Giessler, Tamás Horváth, and Hans-Joachim Knobloch, editors. *Common ISIS-MTT Specifications for Interoperable PKI Applications*. T7 e.V. i.G. and TeleTrusT e.V., March 2004.

[40] IP Security Protocol (ipsec). Webpage, June 2004. http://www.ieft.org/html.characters/OLD/ipsec-charter.html.

[41] Tim Dierks and Eric Rescola. The Transport Layer Security (TLS) Protocol version 1.2. Technical Report RFC 5246, Internet Engineering Task Force, August 2008. http://www.ietf.org/rfc5246.txt.

[42] Federal PKI Operational Authority, editor. *Federal Public-Key Infrastructure (FPKI) Architecture Technical Overview*, October 2005.

[43] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities, January 2000. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT.

[44] The European Association for e-Identity and Security. Webpage, 2009. http://www.eema.org/.

[45] EEMA PKI Challenge. Webpage, 2009. http://www.eema.org/index.cfm?fuseaction=focus.content&cmid=148.

[46] The pkiC Management Consortium. PKI Challenge Final Report. Technical report, EEMA, 2003.

[47] Harald Baier and Markus Ruppert. Interoperable and Flexible Digital Signatures for E-Government and E-Commerce, March 2004.

[48] *Directive of the European Parliament and the Council on a Community framework for electronic signatures*. Directive 1999/93/EC, 1999.

[49] Interoperability Working Group (IOWG), editor. *Asia PKI Interoperability Guideline (Version 2.0)*. Asia PKI Forum, March 2005.

[50] Yasuo Miyakawa, Takashi Kurokawa, Akihiro Yamamura, and Yasushi Matsumoto. Current Status of Japanese Government PKI Systems. In S.F. Mijølsnes, S.Mauw, and S.K. Katsikas, editors, *EuroPKI 2008*, number LNCS 5057, pages 104–117. Springer-Verlag Berlin Heidelberg, 2008.

[51] Population Statistics in Norway. Webpage, January 2009. http://www.ssb.no/english/subjects/02/.

[52] BBS AS business. Webpage, 2009. http://www.bbs-nordic.com/en/About-BBS/Our-business/.

[53] ZebSign. Webpage, 2004. http://www.zebsign.no/About-ZebSign/.

[54] Buypass. Webpage, 2009. http://www.buypass.no.

[55] European Commission External Relations. Webpage, July 2008. http://ec.europa.eu/external_relations/norway/index_en.htm.

[56] Direktoratet for forvaltning og IKT. Webpage, July 2009. http://www.difi.no/.

[57] William Burr, Donna Dodson, Noel Nazario, and William Polk. Minimum Interoperability Specification for PKI Components, Version 1. Technical report, National Institute of Standards and Technology, September 1997.

[58] Jon Ølnes, Anette Andresen, Leif Buene, Olga Cerrato, and Håvard Grindheim. Making digital signatures work across national borders. In *ISSE/SECURE 2007 Securing Electronic Business Processes*, pages 287–296. Vieweg, December 2007.

[59] VeriSign Thawte Relying Party Agreement Version 4.0. http://www.thawte.com/repository/pdf/cpsrelyingparty.pdf.

[60] Tom Freeman, Russell Housley, Ambarish Malpani, David Cooper, and William Polk. Server-Based Certificate Validation Protocol (SCVP). Technical Report RFC 5055, Internet Engineering Task Force, December 2007. http://www.ietf.org/rfc5055.txt.

[61] Carlisle Adams, Peter Sylvester, Michael Zolotarev, and Robert Zuccherato. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols. Technical Report RFC 3029, Internet Engineering Task Force, February 2001. http://www.ietf.org/rfc/rfc3029.txt.

[62] XML Key Management Specification (XKMS). Webpage. http://www.w3.org/TR/xkms/.

[63] Requirements for Use of Signatures in Public Procurement Processes. PEPPOL deliverable Version 1.2, 2009. http://www.peppol.eu/deliverables/wp-1.

[64] Jon Ølnes, Leif Buene, Anette Andresen, Håvard Grindheim, Jörg Apitzsch, and Adriano Rossi. A General Quality Classification System fo eIDs and e-Signatures. In Pohlmann, Reimer, and Schneider, editors, *ISSE 2009 Securing Business Processes - Highlights of the Information Security Solutions Europe Conference 2009*, pages 72–86, October 2009.

[65] Framework mapping of technical/organisational issues to a quality scheme. STORK deliverable D2, 2009. http://www.epractice.eu/en/library/292314.

[66] Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms. IDABC, December 2007. http://ec.europa.eu/idabc/servlets/Doc?id=29622.

[67] Ascertia. Webpage, 2009. http://www.ascertia.com/.

[68] DNV. *XML Schema Description*, 2008. http://www.dnv.com/binaries/XML_schema%20description_v1.0_tcm4-243234.pdf.

[69] Ascertia. *ADSS Server Admin Guide*, February 2008.

[70] DNV. *DNV VA Quality Parameters, Certificate and Signature Quality*, 2008. http://www.dnv.com/binaries/VA-quality-parameters-v2.0_tcm4-222724.pdf.

[71] Interoperable Delivery of European eGovernment Services to public Administrations, Business and Cditizens. Webpage. http://ec.europa.eu/idabc/.

[72] IDABC European eGovernment Services. *Analysis and Assesment of the solutions. Study on European Federated Validation Service (EFVS) : Analysis and assessment report*. European Communities, July 2009. http://ec.europa.eu/idabc/en/document/7764.

[73] OASIS Digital Signature Service Overview. http://www.oasis-open.org/committees/download.php/22725/oasis-dss-overview.pdf.

.1 List of interviews

Person	Function	Place	Date	Remarks
Bishwajit Choudhary	Senior Vice President BBS eSecurity	BBS	15.07.2009	
Ole Kristian Svendsen	BBS eSecurity Team Manager	BBS	17.07.2009	
Halvor Sakshaug	BBS eSecurity system developer	BBS	21.07.2009	exercise with BBS VA test application
Wenke Skjærve	BBS Identity Manager	BBS	28.07.2009	with participation of Bente A. Alnes
Leif Buene	Senior Principal Engineer, DNV	DNV	04.08.2009	
Anette Andresen	Product Manager BBS Trust Solutions	BBS	03.09.2009	
Ketil Kintel	Security Advisor BBS Trust Services	BBS	04.09.2009	
Jon Ølnes	Senior Advisor, Difi	Difi	10.09.2009	