Secure Vehicular Communication Systems: Cross-Domain VPKI, Design and Implementation

Behrooz Aghakhanian Fereydani

KTH Electrical Engineering

Master's Degree Project

Stockholm, Sweden October 2013

XR-EE-LCN 2013:019

KTH Electrical Engineering

Secure Vehicular Communication Systems: Cross-Domain VPKI, Design and Implementation

Behrooz Aghakhanian Fereydani

Stockholm Oct. 2013

Lab of Communication Networks (LCN)
School of Electrical Engineering
Kungliga Tekniska Högskolan (KTH)
Stockholm, Sweden

Secure Vehicular Communication Systems:
Cross-Domain VPKI, Design and Implementation

Behrooz Aghakhanian Fereydani

Master’s Thesis in Computer Science (30 ECTS credits)

at the Information and Communication Systems Security (ICSS)
Master’s Program
Royal Institute of Technology, year 2010
Supervisor at School of Electrical Engineering at KTH:
Prof. Panagiotis Papadimitratos
Examiner: *Prof. Panagiotis Papadimitratos*
XR-EE-LCN 2013:019
Royal Institute of Technology
School of Electrical Engineering
Osquldas väg 10
SE-100 44 Stockholm, Sweden
URL: http://www.kth.se/ees

Acknowledgement

This master thesis report was written during the period of spring 2012 until October 2013, under the supervision of Prof. Panos Papadimitratos in LCN (Lab of Communication Networks) in the school of Electrical Engineering at KTH. First of all I like to gratefully appreciate my supervisor who consulted me choosing right topic and guided me through this research thesis. Then I would like to thank Mohammad Khodaei for his comments and feedbacks on implementation and proposed model of this report. Moreover, I want to appreciate great help of Thomas Cellerier and Mohammadhadi Misagh - my friends and colleagues at my workplace, Cryptzone – for their feedbacks and useful discussions. Furthermore, I would like to thank my parents Gholamreza and Zahra, and also my brother Farhang who always encourage me through all these years. Last but not the least, I appreciate Swedish educational system for providing free education which make lots of students to follow their dreams in higher education level.

Behrooz Aghakhanian Fereydani

Stockholm, October 2013

Abstract

Enabling communication among vehicles on the road has advantages, but it also introduces a number of security drawbacks. A Vehicular PKI (VPKI) provides an infrastructure that brings security and privacy within the VPKI domain. But when it comes to establishing a trust model among multiple VPKI domains, a new trust model is needed in order to facilitate travelling across domains. This project proposes an approach and partially implements a scalable and efficient Cross-Domain VPKI trust model that, first, enables VPKI domains to establish different levels of trust with each other and, second, it suggests that a Domain CA (DCA) in each domain to evaluate trustworthiness of vehicle's Long Term Certificate (LTC). As result, CAs in VPKI domains will have more granular control over issuing pseudonym Foreign Certificates for a vehicle that travels into their domain.

Keywords: Cross-domain VPKI, Vehicular PKI, LTCA, Certificate policy assurance level, X509v3, CSR, PCA

Contents

List of Figures

List of Tables

List of Notations

NTF	*Non-Trust Factor*
PK	*Public Key*
PKiV	*(i)th Public Key generated for Vehicle*
SK	*Private Key*
PKiV	*(i)th Private Key generated for Vehicle*
CA	Certificate Authority
CN	Common Name
CP	Certificate Policy
CPAL	Certificate Policy Assurance Level
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCA	Domain Certificate Authority
DN	Distinguished Name
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FC	Foreigner Certificate
FPC	Foreign Pseudonym Certificates
FPKID	Foreign PKI Domain
HSM	Hardware Security Module
IEEE 1609.2	Standard for Wireless Access in Vehicular Environments (WAVE), Security Services for Applications and Management Messages
LTC	Long-Term Certificate
LTCA	Long-Term Certificate Authority
NPKID	Native PKI Domain
PCA	Pseudonymous Certificate Authority
PKCS	Public-Key Cryptography Standards
PRA	Pseudonym Resolution Authority
RA	Registry Authority
RCA	Root Certificate Authority
RSU	Road-Side Unit
TTP	Trusted Third Party
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad hoc Network
VC	Vehicular Communication
VPKI	Vehicular Public Key Infrastructure

1 Preliminaries

1.1 Introduction

A number of research and development efforts have been done since 2001 in North America and Europe to provide communication infrastructure for vehicle. These Vehicle communication (VC) projects can be categorized in three major areas: Transportation safety such as Emergency Electronic Break light and Intersection Collision Warning application which protects vehicle against road accidents. Transportation efficiency such as Electronic Toll collect applications and finally, Infotainments which provide user level services like map and media downloads. In spite of introducing new services which solve number of issues, technology give this chance to new threads as well that can explodes systems through their vulnerabilities. VC is also not an exception and developed services should be protected against various adversaries that are already exists and can be adopted for this particular application. Therefore, to address these adversaries, security requirements has been provided. These requirements are message authentication and integrity, confidentiality, non-repudiation, entity authentication, access control, accountability as well as keeping privacy of sender. Digitally signing a messages using asymmetric cryptography algorithms which is proposed by [1] is a solution that provide non-repudiation and entity authentication at the same time. In this way, receiver of the messages which is vehicle in a VC environment would be able to verify authenticity of sender that can be another vehicle or Road-Side Unit (RSU) and also be sure that the sender can't deny sending the message later. To satisfy privacy of sender, signatures are short living with pseudonym identity which makes tracking of a specific sender difficult [1]. Implementing digital signature needs a Public Key Infrastructure which realizes the trust model between sender and receiver of messages. [1] proposed a model for PKI in a single domain in which both parties trust a Certification Authority (CA) so that can easily validate each other's identity. According to [1], this model will address VC security requirement while preserving privacy in an efficient way. When a vehicle wants to move to another domain which controlled by another CA, it needs a Foreign Certificate (FC), which is a pseudonym certificate issued by hosting domain, so that other vehicles or RSUs can trust it. Establishing a cross domain PKI trust model in a VC environment is still a challenge. CAs in different domains should be able to trust each other in an efficient and flexible way. Efficient, so that growing number of CAs will not affect performance of validation of digital certificates dramatically and also flexible, in a way that CAs establish different level of trust with each other. This report tries to propose a model to address this issue and then assess it based on existing PKI trust evaluation models. Finally, a protocol would be introduced and developed with a programmatic language.

1.2 Background

Over the past years, numerous technologies have been developed to provide vehicles, drivers and their passenger with safer, faster and more exciting travel experience. These technologies expand from Automotive Navigation Systems to Electronic Toll Collection and Electronic Parking Systems. As an emerging research area, Vehicular Communication (VC) involves large number of projects both in automotive industry and academic environments [2]. Similar to other computer networks, VC is comprised of number of nodes which here can be divided into mobile vehicles and immobile like RSUs. Therefore, communications are either Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I).

Infrastructure includes collection of all the non-vehicle entities which provide networking services or application services. Networking services are provided through RSUs or other infrastructure (e.g. Base Transceiver Station (BTS)). An emerging example is GeoNet [3] which was a European project that have conducted researches on developing IPv6 networking for VC. Over the established networked various kind of services can be accessed such as Traffic Management systems, Remote Diagnosis systems and media download. In addition to these services that are provided through infrastructure, there are other ones which can be run over V2V network. Emergency Electronic Break Light and Pre-Crash sensing are among of those services to number a few.

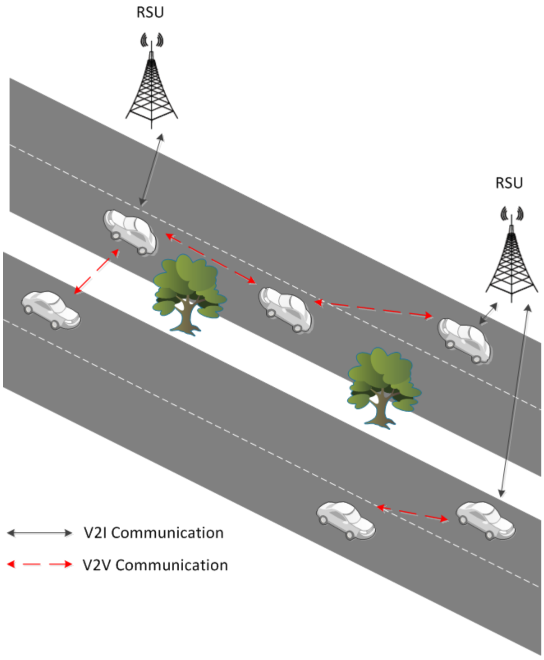


Figure 1.1: Simple illustration of VANETs [1]

Looking at Vehicular Communications (VC) from physical and data-link layer of OSI communication model, specific wireless protocols need to establish connection for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Protocols that have different connectivity ranges and bit rates. IEEE 802.11p or IEEE 1609.2 [2] is a standard that suitable for mobile environment and supports proper connectivity range which can provide connectivity both between vehicles and between vehicle and RSUs.

According to [2], applications that have been provided for VC can be categorized in three areas: Transportation safety, Transportable efficiency and Infotainment. Transportation safety includes ones what try to protect vehicle and passengers such as Lane Change Warning. Transportation efficiency applications mostly help congestion and intersection management systems and finally infotainment which gives user-level services like Map download or update.

Depending on type of application, different security requirements are needed to protect various adversaries against those applications. According to [1] adversaries can be either active like data modification and injection of false messages or passive which generally means capturing messages and reading their data or meta data as attacker such as communication protocols or header information. Therefore, general security protection methods plus privacy should be developed while considering specific characteristics of VC which introduce new limitation in compare to traditional networks such as Local Area Networks (LAN).

As the most prominent project, SEVECOM (Security Architecture for Vehicle Communication) addressed security in VC and developed protocols and mechanism that provide both security protections while considering user privacy. As [1] explains the project address two fundamental issues: 1) Identity, credential and key management 2) Secure communication. As the focus on this report is contributing to the first one, here it will be explained in more detail.

Generally in all secured systems each and every node should have a unique identity in order to be authenticated and later become accountable in the system. Therefore, an authority is needed to be in charge of assigning identity and credential. SEVECOM uses Certification Authorities (CA) in VC infrastructure to play role of these authorities. To provide message confidentiality, integrity, non-repudiation and also entity authentication, the architecture is relay on asymmetric cryptography based on Public Key Infrastructure (PKI). Using this method vehicles and RSUs should first encrypt messages and then sign them using private key. Before accepting it, receiver should validate the integrity of both sender and the messages itself. To perform this action, it needs public key of sender.

This is where digital certificate comes to action which can store identity of each entities plus their public key. These certificates should be signed by a CA which both sender and receiver trust. The CA is responsible with issuing digital certificates, signing them and also managing revocation process if they become compromised.

In SEVECOM security architecture, there are two types of certificate: Long-Term Certificate (LTC) and short-term certificate. LTC contain long-term identity plus public and private key pair of vehicle which is issued by Long-Term Certificate Authority (LTCA) once. Short-term certificate which developed to address privacy of vehicle contains short-term identity in a form of pseudonym. These certificates published in large numbers contain set of public and private keys that are generated in Hardware Security Module (HSM) of vehicle and sent to Pseudonym Certificate Authority (PCA) to get signed. These vehicles use the short term pseudonym certification for signing each message including all certification chain which is needed for receiver to preform validation process. Short term certificate make the vehicle hard to trace and the only entity that bind short term identity to long term identity is Pseudonym Resolution Authority (PRA). More detail about functionally and communication among vehicles, LTCA, PCA and PRA could be found in [4]. These entities would be managed by a Domain CA (Top CA of a domain) which is in charge of providing PKI infrastructure services such as Issuance of certificates and managing revocation plus define and enforcing Certification Policies (CP) which is explained in Chapter 2.

When vehicle wants to travel from Native PKI Domain (NPKID) to Foreign PKI Domain (FPKID) which is under control of another DCA, it should obtain new pseudonym certificate to be still hard to trace in Foreign PKI Domain (FPKID). Otherwise other vehicles or attackers would notice the difference between new foreign and native vehicles. Thus, guest vehicle first should prove to hosting DCA that it is registered by a CA in its NPKID and then hosting DCA will generate and sign pseudonym certificates which are called Foreign Pseudonym Certificates (FPC). Using new certificates, guest vehicle looks like other can in FPKID and therefore it is will be hard to trace.

Here, it comes to question that how its trust should be established between DCAs in different domains. What type of PKI trust model suits for this purpose so that scalability would be considered in future and also what more granular control can be considered while trusting other CA and in time to issuing Foreign Certificates? Rest of the report tries to address this issue of cross-domain PKI trust model for VC and develop a protocol for that.

1.3 Related Works

There have been four projects that mainly proposed solution and architecture regarding security in Vehicular Communication. But none of them have addressed trusting issue between VC infrastructural domains in order to grantee sustaining security and privacy when a vehicle drive in a FPKID and wants to communicate with other vehicles and RSUs. On the other hand, out of scope of VC environment, there are PKI trust models which have been designed to establish trust between Certification Authorities which will be discussed in later Chapter 2. There are also some implementations of these PKI trust models in number countries or regions which lack specific need of VC. Here, some VC and non-VC projects are reviewed and discussed regarding topic of presenting report.

EVITA [5] (E-Safety Vehicle Intrusion Protected Applications) which was started in 2008 and ended in 2011. The project designed and implemented prototype of a secure on-board architecture for vehicle which secure distributed network of ECUs (Electronic Control Unit) in a vehicle. Each of these ECUs is responsible for controlling different functionality in a car such a brake or windows systems. Messages between these ECUs and central unit called

HSM (Hardware Secure Module) which is responsible with managing encryption keys and setting up a secure on-board communication network. Messages are encrypted and get signed to be protected from tampering or generating fake one that may cause malfunctioning of critical components. While it addresses secure communication between vehicle components, EVITA does now discuss about how these architecture could be extended to involve communication between different vehicles. Therefore, it does try to solve trust issues which arise when a vehicle wants to communication with other vehicles which are not managed by different security infrastructure.

NoW [6] (Network on Wheels) is another project started in 2004 and ended in 2008 which designed and implemented a vehicular communication system supporting safety and infotainment applications. They also considered security architecture in the model which provides entity authentication, message integrity and non-repudiation together with privacy using digital signature and certificates. This mechanism that address communication between vehicle and RSUs and also other vehicles, secures both routing information (as it support GeoCast with enable communication based on location on entities) and data messages. In a simple scenario when there are multiple hops between sender and receiver, each hop digitally signs messages in a way that receiver and validate it transmission path. But NoW does not discuss about situation when certification used by these entity are managed by different Certificate Authorities in a cross domain scenario and how these CA can establish trust with each other.

SEVECOM [1] is the biggest project in this research field as it dedicated to design security architecture which also to large extent considers performance overload that this architecture would bring to vehicular communication protocols. Like NoW it is based on digital signature and certification to bring entity authentication, messages integrity and non-repudiation plus confidentially as well as privacy through pseudonym and short-term certificates and. The project addressed cross domain travelling as vehicle with get set of foreign certificates like pseudonym certificates which enable it to keep its privacy in FPKID as the recent identity looks like other vehicle in the domain. But Establishing a PKI trust model which can be used among Certificate Authorities in different domains was not discussed.

D-SPAN [7] which is stand for Data Security and Privacy in Wireless Networks has introduced a multi domain architecture which uses ticket base authentication approach like Kerberos which enables a vehicle to be authenticated in FPKID so that it can leverage VC application in new domain. But this ticketing method whether become implemented using Kerberos, SAML or OpenID, it needs PKI trust model among DCAs to leverage Public Key Cryptography which further can be used in Authentication, Authorization and Accounting (AAA).

Beside above researches in VC, there are some countries or communities which have implemented multi domain PKI trust models. Here some of them are reviewed. EuroPKI [8] is a loose association of organizations and people which use a Public Key Infrastructure (PKI) with hierarchical topology where their Root CA (RCA) is currently located at Politecnico di

Torino, Italy. This association which was born from two European Commission founded research project called ICE-TEL and ICE-CAR uses X509v3 protocol for digital certificate and the RCA as a trust anchor is responsible for establishing trust among other people or CA in this association. EuroPKI is named as a loose association because the RCA does not mandate it conforming CA to apply certain cryptographic algorithm or special hardware or software specification for storing private key in its Certification Policy except some general requirement. Therefore, conforming CA who should mention this certificate policy in issued certificates for their clients may apply their own requirement and detailed policy.

The most pioneer example of multiple domain PKI trust model is US Federal government PKI environment which is managed by Federal Bridge Certificate Authority (FBCA) [8]. This environment consists of few numbers of federal organizations such as Department of Defense (DoD) and some commercial CA such as Verisign. FBCA does not act as a RCA but a hub that other CA establishes cross certificate with under different level of assurance. To become eligible to get each of these levels which are rudimentary, basic, medium, medium commercial best practice, medium hardware, medium hardware commercial best practice, and PIV-I, CA need to comply with related certification policy that is provided by Federal PKI policy authority (FPKIPA). Then FPKIPA map the certificate policy of each CA with one or more level of assurance. Therefore, CAs can establish trust with each other based on these assurance levels which are developed based on enrollment process of certificate requester entity, cryptography algorithm used in each PKI domain and method of storing private keys. From topological viewpoint, FBCA is just a hub (star model) that conforming CAs need to cross certify with. It's not mesh topology as CA does not cross certify with all other CAs in the community. Thus, as FBCA does not issue certificate for other CA and use a strict certificate policy, CA are free to apply their own policy in their domains and its reasonable because federal government does not want to interfere in technical issue and policy that CA use in their organization and does not want to take responsibility of any failure in domain that it has no any control over. The methodology and technical specification in not open for public usage. Canada and Japan governments also use the same method. In Canada case, central bridge is designed and implemented by Entrust as one of the leading companies is PKI and digital certificate technologies. Other countries such as Singapore or China applies a hierarchical PKI which uses an government or stated owned RCA which is responsible to issue certificate for sub-ordinate CA in different domains using specification which is stated in their certification policies.

1.4 Problem Definition

The problem this report considers is the lack of a cross-domain PKI trust model for the VC environment. Proposed model for VC have addressed a single domain solution where sender and receiver of a message are vehicles certified with the same DCA. But when it comes to multi domain Vehicular PKI environments, a new trust model should be design to define PKI relationship among different Vehicular PKI domains. This cross-domain PKI trust model for VC environment should be scalable so that performance in case of issuance and validation of

LTC which is need for issuing FPC would not be affected by growing number of interconnected domains. Moreover, each DCA apply its own CP for which is set of standards such as length of signing keys, algorithms and authentication mechanism. Therefore, establishing trust between CAs of various domains become difficult and complicated. In the other word, using existing PKI models, CA of a domain is not able put different levels of trust on CA of another domain based on CP it applies in its domain. They must either accept or reject CP of a PKI domain. Having different levels of trust gives more granular control over trusting vehicles coming from VPKI domain.

1.5 Research Goal and Contribution

The contribution of the project to preceding research in VC security is designing and implementing a cross-domain PKI trust model as proof-of-concept which enables DCA in each domain to establish different level trust with each other and to have detailed control in issuing FPC for a vehicle that drives into HPKID. Efficiency has been also considered in a scalable way when designing proper trust model topology and certification management procedure so that growing number of domain would not affect the performance in the system dramatically. This detailed limitation control can be applied using number of criteria including CP used in NPKID, vehicle specification (such as brand, model and etc.), and remaining validation period on vehicle’s LTC.

1.6 Methodology

According to [10] there are two research methodologies in Information System discipline: behavioral science and design-science. *"Behavioral science paradigm seeks to develop and verify theories that explain or predict human or organizational behavior"*[10], while design-science *“seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts"*[10]. As the aim of presenting research project is to create a new artifact instead of explain an existing human behavior, it follows design-science phases to some extent which are illustrated below:

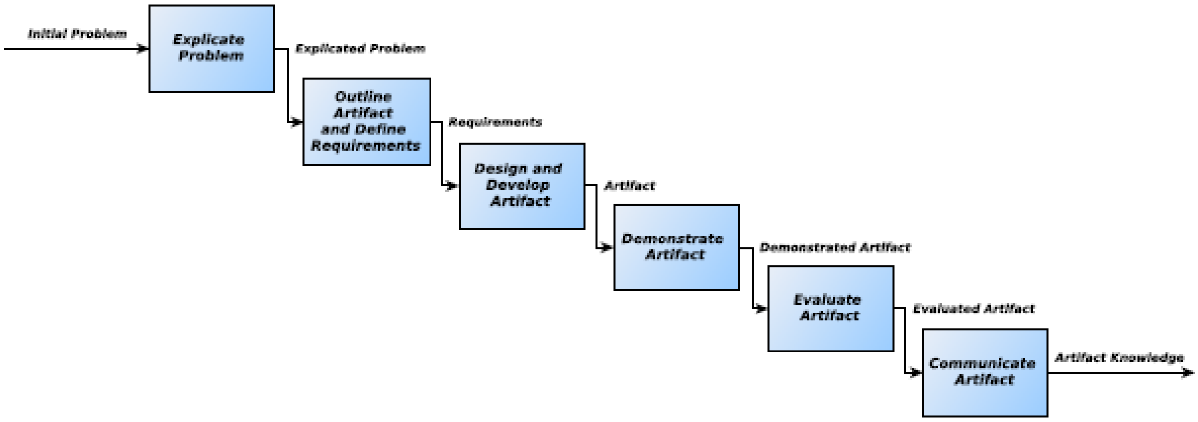


Figure 1.2: Overview of Design-Science Methodology [10]

1.6.1 Explicated Problem

This phase tries to explicate the problem of the project by investigating and analyzing the research area and focus on the points that were not address by other projects and show how solving the problem will contribute to existing field of research. To elaborate the problem other tools such as empirical research, survey, interviews and literature review could be use based on type of research.

In this project, research problem that was stated in preliminary chapter is explicated main chapters. The most related projects which have addressed similar problem and their shortcomings are explained in detail through literature review. Mainly, SeVeCom project is analyzed in a way that how it defines adversary model of VC and how they practically addressed security problem while considering privacy in a single domain. Then they solution for cross domain scenario is stated and we will see why this solution cannot be applied without and efficient and robust PKI trust model for VC.

1.6.2 Outline Artifact and Define Requirements

Following the previous phase, different type of project requirement which are need to solve the problem should be defined. Then list of artifacts such as design, implementation and test artifact are outline.

In this project functional and non-functional requirement for a cross-domain PKI infrastructure in VC will be listed. As an information security project most of non-functional requirements are related to security issues while scalability, reliability and usability and etc. also are considered. Functional requirements address design aspect needed to establish a trust model among loosely coupled functional domain in VC PKI infrastructure. Defining these requirement necessitates study of different PKI trust models involve both topology and certification policies that could be used by Certification Authorities. Then PKI trust model evaluation criteria need to be reviewed in order to find an evaluation method for accessing any cross-domain PKI trust model that is proposed further in the project and if it meets non-functional requirement of the project. Studies continued with reviewing implemented PKI trust models which have addressed cross-domain trust and performance issues. This part of project also elaborate deep into models, protocols and technologies that have been used in Europe, United States, China and etc.

Then project artifact that will be attached to the report in Appendix section such as adversary model, functional and non-functional requirement, UML diagrams regarding design and implementation phase and communication protocols are listed.

1.6.3 Design and Develop Artifact

The third phase in design-science method is to design, develop and implement the proposed artifact based on the explicated problems to thoroughly fulfill the requirements [11]. In project these UML diagrams for design and modeling which follows object orient and component based architecture in software development:

- Component diagram to illustrate which programmatic components (including DCA, Vehicles, and RCA) should be code and what interfaces they should offer to communicate with other components. Using this diagrams the architecture of model and interrelation of component are shown.
- Protocol diagram to show which parameters (CSR, Signed Certificates, X509v3 Certification extensions) should be passed between different component in request and response manner.
- Deployment diagram that shows how component are installed on different nodes including operating systems (Linux), programmatic libraries (OpenSSL, XML-RPC) and communication protocol to set secure channels (SSL/TLS).
- Code base which is implementation on above diagrams which in C++ programmatic language

1.6.4 Demonstrate Artifact

This phase describes the use of developed artifact in the real environment or in other words, in the real-life case to prove its feasibility [11]. In this project, demonstration of developed artifact is limited to running compiled C++ code on independent Linux workstations based on two trust model topologies. Single RCA and Cross Certified CAs in both scenarios are three Linux workstations with different components in each one are needed. Demonstrations involves number of certificate request, response and validations procedures together with digital certificate data extractions and decision logic which are customized to meet requirements of the project. Due to limitations described in the corresponding section, the demonstration of the artifact is dependent on other project being conducted and therefore it is out of scope of this project.

1.6.5 Evaluate Artifact

Artifact evaluation deals with identifying and determining whether the artifact is made up of all the necessary requirements, to determine to what extent this approach has solved the problem [11]. Due to limitation in demonstration of artifacts, evaluation phase is mainly focuses on functional requirement and criteria to meet them in which functionality if developed components independently and in relation to other components are measured based of outcomes and error messages. This method of software testing which is called black-box testing which deal with compiled piece of code rather than reviewing the code base (white-box testing) which is done after code development using debugging and syntax error tools. Furthermore, document review which involves evaluating list of requirement and UML artifacts is done by research field expert before developing the code. Fully evaluations of artifacts necessitates integration to other projects which address security requirement on VC in a single domain and protocols for handling pseudonym certification needed in VC environment. Therefore, evaluating non-functional requirement regarding performance and reliability is depends on deploying vehicle components on a real hardware unit built-in vehicle.

1.6.6 Communicate Artifact

The last phase of design-science methodology is about communication of the artifacts that means making them available to other researchers and experts in VC and especially ones who are conducting research in VC security and trust models. Furthermore, programmatic artifacts of this project will be integrated into already developed solutions about PKI in VC environment.

1.7 Audience

This report targets information security experts and students who work in field of VC and specially those who focus on Public key Infrastructure in this field. Additionally, for researchers who work on PKI trust model in general regardless of VC domain may find this report useful and informative. Reader of the report should be familiar with general information security terms, PKI and digital certificate, VC environment although some basic information is given throughout the report.

1.8 Limitations

The project is about design and implementation proof-of-concept of a Cross-Domain PKI for VC. Therefore, to fulfill all functional and non-functional requirements it needs to be implemented and tested on real life environment which is partially should be deployed on hardware kit on number of vehicle and also at least two CA with proper traffic load regarding certification request, issuance and validation of certificate and also other programmatic logics, to test performance and reliability of communication channels and programmatic modules. Additionally, trust evaluation of certification policy of VC PKI domain results in number of criteria for assigning assurance level to CP of a domain which although make it a very granular and flexible but on the other hand, end with lot of programmatic difficulties in implementation phase. Therefore, this project just addresses some trust evaluation criteria in component design and writing code.

Furthermore, not being familiar with OpenSSL API and C++ language along with allocating part time (instead of fulltime) makes the project take longer for writer of this report to accomplish the project. Of course, turning this proof of concept implementation to an industrial product needs more hours of R&D.

1.9 Thesis Outline

Rest of this report is divided into three chapters which in Chapter two different PKI trust models from topological and certificate policy perspective are described and implemented cross domain model are reviewed and then proper trust model for VC is proposed. Moreover, different approaches in evaluation trust degree of a certificate are explained and based on that, criteria for evaluating trust degree of digital certificate and assigning

Assurance Level to security practices of VPKI domain are listed and formulated. In Chapter tree, the PKI trust model and Assurance Level criteria which were developed based on Cross-Domain VPKI requirement will be turned into design protocols and diagrams. Then designed model and protocols are implemented and tested and last chapter make conclusion of whole project, clarify the contribution and gives some ideas which can be topic of further research projects in field of Cross-Domain VPKI trust model.

2 Cross-Domain PKI Trust Model

This chapter is divided into two parts. First part starts with explicating research problem what was defined in Preliminaries and following that the adversary model and challenges about Cross-Domain PKI trust model for VC are elaborated. Then an introduction is given about Public Key Cryptography and Infrastructure following a review of PKI trust models and numbering their advantage and disadvantages. Afterwards, some real life example of an implemented PKI trust model worldwide is analyzed and finally a model from topological perspective is proposed. In the second part, evaluation of the trust degree of a vehicle's LTC is considered. First security threat to CA and subscriber of PKI domain is explained and then based on that two set of criteria are developed: CP of a VPKI domain and LTC of a vehicle.

2.1 Problem of Trust in Issuance of Foreign Pseudonym Certificate in Cross Domain Scenario

SeVeCom project's solution provides security and privacy for Vehicle Communication have addressed a single PKI domain solution. In that security model which is based on Public Key Cryptography and Infrastructure, they provide Message authentication and integrity, confidentiality, non-repudiation, entity authentication, access control, accountability while keeping privacy of vehicles through concept of pseudonym and short term certificates. To explain SeVeCom model in more detail, here the key concept and overall procedure of acquiring certificate and validation process is explained.

In a VC domain each vehicle (X) has one Long-Term Identification that is similar to Vehicle Identification Number (VIN). This identifier contain a pair of cryptographic key (SK x, PK x) and some attributes like model of vehicle, engine type, year of production, and etc. As stated in [1] the identifier is unique, life time, and registered in offline mode based on agreement between manufacturer and Certificate Authority (CA) of the domain. Vehicle generates bunch of key pair (SK1V; PK1V); :::; (SKiV; PKiV) in its HSM console and sends public keys together with Long-Term Identifier to a configured CA. CA identifies the vehicle and generated and sign pseudonym, puts its own identifier and then send them back to vehicle. Since pseudonyms of other vehicles in the domain is issued and signed with same trusted CA, they have verified identity of each other which provides a base line for other cryptographic operation specified in security requirement during communication among vehicles such as Message authentication and integrity, confidentiality, non-repudiation, entity authentication. In other word, vehicle uses one of temporary and pseudonym identities and key pair to sign messages what they want to pass to other entities. Design and implementation of this procedure is topic of another project by [4] which uses certificates as identifiers and develops LTCA and PCA to handle process of issuing different types of certificates and also PRA which is the authority to perform pseudonym resolution to identify the real identity of a pseudonym certificate.

But what if a vehicle crosses boundaries and drives into domain B from domain A? To preserve privacy SeVeCom suggest a new identifier name Foreign Pseudonym Certificate (FPC). FPC is again a pseudonym certificate which inherits identity of foreign PKI domain B, therefore, vehicle looks like other vehicles in domain B while communication with them and intruder is not able to identify it by format of pseudonym it uses. To do this, vehicle should proves its identity to DCA is domain B and then DCA signs pseudonym key pairs and issue new pseudonym certificates with set of identifies which looks like other identifier in domain B.

But in stated FPC solution there are two aspects that need be addressed. First and main one is that when talking about more than one VC domain, many questions would be aroused about PKI trust model. Each DCA has its own CP which is set of standards such as length of signing keys and algorithms used or Proof of Possession requirements in Certification Requests, where to store keys, request should be offline or online and etc. [12]. Therefore, establishing trust between CAs of various domains become difficult and complicated. Furthermore, another question is that to which level domains can put trust on each other. In real life scenario VC domains can be states or countries. Due to many factors such as diplomatic relationship, industry standard DCA in domain A may highly trust domain B. Therefore, it issue FPC for all categories of vehicle including type (Trucks, cars, motorcycles), importance (VIP, diplomatic, emergency, ordinary cars), manufacturer, year of production and etc. Or domain A put low level of trust on vehicles from domain C, so it just give foreign certificate to emergency and diplomatic vehicles. Making decision about these criteria depends on domains policies but technology should provide tools to realize these policies in practice.

Second aspect that needs to be addressed is the topological design of PKI trust model for VC. Unlike CA in one domain, relation between top CA in each domain (like countries) could be very loose. Is it possible to set up a Top CA for an area like European Union? What are the risks or advantages? Is it possible to establish cross certification between each two domains? What bout scalability of the PKI trust model in future?

Following sections in this chapter answer seconds question about Topology of PKI trust model and then introduce and formulate criteria as an answer the first one.

2.2 Topology of CAs in PKI Trust Model

Since introducing asymmetric cryptography and concept of Public Key Cryptography (PKC) main drawback of symmetric cryptography was solve [13]. The problem was how to share the secret key between security entities. Using PKC each entity needs to have their own private key and public of other entities so that they can leverage it to establish secure communication channels IPSec, SSL/TLS or sending secure messages through SMIME or PGP.

But a new problem aroused which was distribution of public keys. As [13] states *“The goal of a public key infrastructure (PKI) is to enable secure, convenient, and efficient discovery of public keys.”* In PKI concept, digital certificate binds identity of each entity to its public key [13]. To become valid and creditable, these certificates should be signed by another entity that both parties trust in.

There are two approaches for establishing trust between PKI entities: Web of Trust and Certificate Authority (CA). As [13] defines in web of trust approach public key holder *“can make publicly known whose keys they trust to be authentic. As a member of this infrastructure, one can decide whom to trust as an introducer of new keys, to a lesser or stronger degree. If the resulting web of keys and trust relationships allows one to establish a link between oneself and the target identity, then communication can take place.”* In other word, as a non-hierarchical infrastructure authenticity of a public key has a direct relations with authenticity and number of intermediates (or your friends) who introduce you to the other party you want to communicate. Web of Trust like other non-hierarchical structures suffers the problem of scalability beside potential adversary such as impersonation attacks in a way that intruder can pretend to be authentic person and deceive a node in infrastructure. As a result all other parties who trust that node will trust the intruder as well. Web of Trust is a trust model which was introduce with PGP (Pretty Good Privacy) which is a communication security protocol and software mainly designed to protect email communication [15].

But the other approach which more widespread is using CA in PKI. PKI which is uses a synonym to PKI based on CA was introduced to address the problem of securely distribution of public key of principles who want to communicate. As [14] states *“accepted solution is to have trusted nodes known as certification authorities (CAs) digitally sign data structures known as certificates that state the mapping between names and public keys.”* CA as a trusted third party (TTP) proves identity of all principle and signs their certificates. But that solution which is called Single-CA obviously cannot be implemented because of following problems:

- It is inconvenient, insecure, and expensive to get a certificate from a CA in distance.
- In any security policy it is recommended to change the keys after a certain period of time. Of course CA is responsible for signing newly generated keys and also revoking the keys which have been compromised. Depending on key expiration period and compromise of the keys, this put huge amount on overhead on CA
- And as a non-technical issue Single CA model end with a monopolization of information security structure of whole world by a single entity.

To solve these issues there should be more than one Single CA in the world. Each domain (e.g. organization, city, county, state, country or even continent) should have their own CA. Now consider that two principles in two different domains want to have a secure communication. The application used for secure this communication channel could be range from Secure MIME (S/MIME) [16], SSL/TLS [17] in Web application and VPN connection or

IPSec [18] for securing Network layer of ISO model [19] between two network router. This raises the issue of cross-domain trust in PKI. Many models have been introduced by researchers in academies and also more practical ones by major information security trust companies to address this issue. Beside cross-domain PKI trust solution two other principles is PKI are designed which mainly try to help A Single CA with its work load and identity check of certificate requester:

- **Delegated CA:** In order to decrease overload on a CA, it can delegate its responsibility of signing certificate to sub-ordinate CAs. These subordinate CAs are trusted and their certificate is signed by CA. In an organization, CA can give responsibility issuing certificate of organizational units (OU) to CA of that OU. CA here is responsible of certification policy (see Chapter 3) and controlling subordinate CAs.
- **Registration Authority:** Process of issuing certificate can be divided into two steps verifying. Verifying identity of public key holder and issuing digital certificate itself. Registration Authority (RA) gets identity of the principle who requests of certificate. This verification could be though checking email address, home (or office) address or impersonal meeting [14]. If verified, RA send the request to CA and CA signs it and issue a digital certificate for that principle (Note that depend of certificate policy of a domain, key pair can be also generated by CA itself. Moreover, technically issuing a certificate includes signing digital certificate info together with public key which is explained in chapter 3.

While PKI domains can leverage any of above two solutions, when it comes to cross-domain interrelation problem, a number of PKI trust models have been designed. The main practical models that are used in industry are introduced and their specification, advantages and disadvantages are explained.

2.2.1 Direct Cross Certification

As it is shown in figure 2.1, CA 1 trusts principles of domain B by certifying (i.e. signing digital certificate) of CA 2. In this way relying parties is of domain one can trust subscribers of the other domain. In other world as EnTrust explains CA 1 *"acting as an agent for its community of relying parties, evaluates the risk of accepting certificates issued by the other authority, and places the appropriate controls in the cross certificates that it issues"* [24]. As risk assessment process, CA of one domain investigate the CP of other domain and based on that decides which subscribers are allowed on communicate with its relying parties in context of specific business application. An example is that subscribers of Sales department of Organization B are certified to use their cryptographic keys for digitally signing emails when communicating with replaying parties in Organization A.

Direct Cross certification is bidirectional, therefore, CA of domain B also certifies subscribers of domain A by reviewing its certificate policy and then signing digital certificate. In this model there is no trusted third party that acts as a hub and grantees trustworthiness of CAs of different domains. The main drawback of this model, as Entrust states, is that *"cost of the risk assessment associated with entering into the trust relationship is prohibitive when the number of relationships is more than a small number"* [24]. Consider that number of PKI domains increases then CA of each domain should evaluation risk of each and every domain itself which for a Complete Graph:

If graph K has n Verticle then K_n has $n(n-1)/2$ edges which forms a sequence number of 0,1,2,3,6,10,15,21, 28, 36, 45,…. .

That means a PKI with 8 domains should do 28 risk assessments, evaluate the certificate policy, issuing certificates and managing revocation. Here the assumption is that CA itself acts as RA. Figure 2.1 demonstrate Direct Cross Certification:

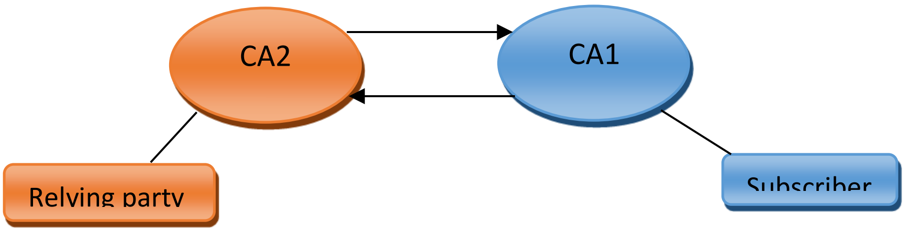


Figure 2.1: Direct Cross Certification

2.2.2 Hub Certification Authority

To overcome the scalability issue of direct cross certification model. A trusted third party (TTP) comes to action. Its responsibility is assessing risk of trusting PKI domains by reviewing certification policies, then checking and validation of identities, signing CAs public key and finally issuing a digital certifications for CAs of all domains. This means that TTP accepted the security risk of subscribers of all domains so relying parties in those domains can start secure communication with them. Of course transferring risk to a third party comes at its cost. These TTP has different name in PKI industry such as Root CA, Hub, trust anchor and Trusted CA. [14] calls them configured CAs as in many application like Web Browser which leveraging SSL/TLS Digital certificate of these CA are stored and configured to be used by Web browser of relating parties. To verify certificate of subscribers which is signed directly or indirectly (with DCA or other sub-ordinate CAs that in the end form a certificate chain) by RCA, Relying parties retrieve RCA certificate and do the actual verification using embedded public key. Something specific about RCAs is that their digital certification is self-signed. This is because they are trust anchors and supposed to be trusted by other PKI domains Worldwide. Therefore there is no governmental or State CA above them to sign their certificates. Mozilla among other Web browser companies publish list of RCA which they configured in their web browser. The list include number of commercial brands such as EnTrust, Verisign and etc. [20]. Figure 2.2 shows the architecture of Hub Certification Authority. In this model Hub act both as CA and RA.

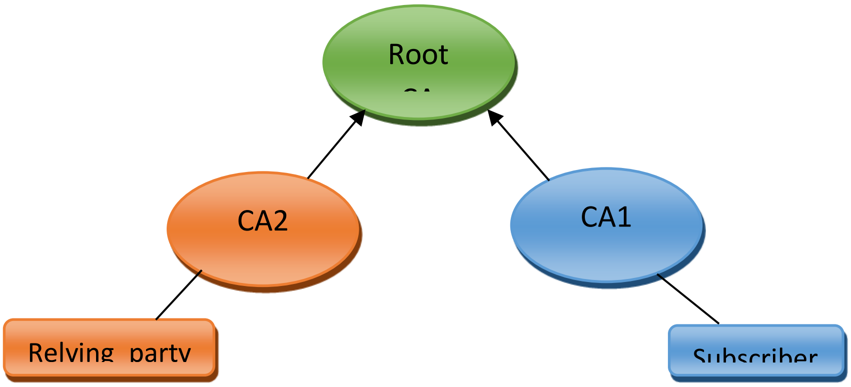


Figure 2.2: Hub Certification Authority

Of course the model solves scalability issue of direct cross certification by proposing a StarGraph concept vs. CompleteGraph in which number of edges is equal to vertices plus 1:

$V = K-1$, Where K is number of edge and V number of vertices.

But as the size of domains and principals who are from various geographical location increase which cause new problems for hierarchical CA model. (Real-World Problems of PKI Hierarchy) categorized real life drawbacks of above this model:

- Technological, which is the distribution of information about certification revocation. Certification Revocation list (CRL) and Online Certificate Status Protocol (OCSP) have been developed to handle revocation problem which put large amount of overload on CAs due to request and response signals. Technically explaining about them is out of scope of this report.
- Administration concerns about including CP under which certificate is issued for CA or subscriber and also evaluation of CPs applied in different domain against each other. These problems have been solved in X509v3 standard which is used for implementation (see Chapter 3). The other administration problems are self-signed certificate of RCA which is still unsolved.

2.2.3 Hub Authentication Authority

Third model is hybrid of two other models in which it separate CA and RA role of hub. Hub acts as RA and after verifying identity of DCAs distribute authentication token. Similar to direct cross functional, this model suffers from scalability issues. Figure 2.3 illustrate this model:

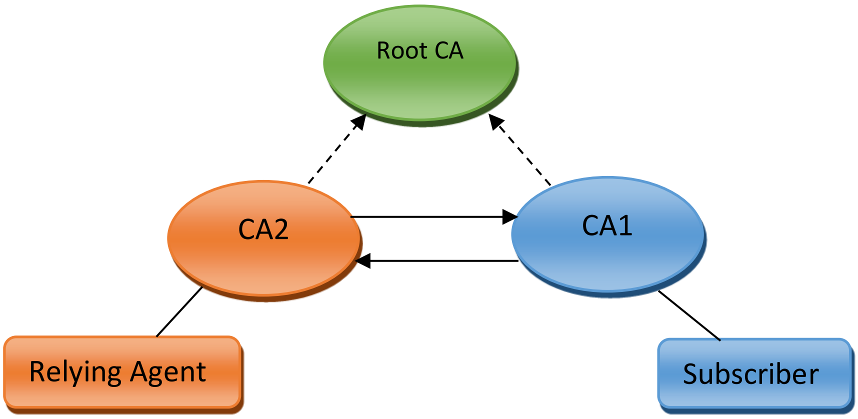


Figure 2.3: Hub Certification Authority

Explained PKI trust models addresses cross domain scenarios. In each PKI domain like an organization, city, state or county any of these models can be implemented which in most cases result in hybrid models. A widespread example is organizations that use hierarchical model in their own domain but CAs directly cross certify each other. This PKI relation could be between two commercial companies that enable their employees to establish secure email communication though S/MIME. In next section some real life example to cross-domain PKI trust model are introduced in which domains ranges from state owned organization to countries.

2.3 Example of Implemented Cross-Domain PKI Trust Model

This section of report review real of example to Cross-Domain PKI trust models. These models are created to orchestrate independent PKI domains which use different CPs that mostly result in loosely coupled architectures.

2.3.1 US Federal Bridge Certification Authority

As Peter Alterman, Senior Advisor to the Federal PKI Steering Committee states, US Government in Paperwork Elimination Act of 1998 mandates all US federal agencies to provide electronic government services by 2003 for citizen. Infrastructural solution to establish secure communication channels to implement services like secure email or digital signature was realized through a Federal PKI. Aim of US Federal PKI is to *"create a cross-governmental, ubiquitous, interoperable Public Key Infrastructure and the development and use of applications which employ that PKI in support of Agency business processes"* [8]. In addition, the U.S. Federal PKI *"must interoperate with State governments and with other national governments"* [8]. Therefore, a cross functional PKI trust model was need to provide interoperation among national government. The first proposed model was a hierarchical Hub Certification Authority which a RCA which is responsible for writing and enforcing CP and implementing digital certificate operations. But there are four arguments against it:

- First is privacy issue in a way that this PKI solution enables the government to aggregate too much personal information of US citizens in a single place and make that information available to Agencies. This concern is not true about private sectors like shopping website where personal information are anonymous, but information stored in governmental agencies unlike commercial website, are not anonymous.
- Second argument is that Federal Agencies concerns about any security agency which is in charge of RCA. They insist that a *"PKI run by another Agency cannot possibly satisfy their unique, mission-based requirements"* [8]. The technical translation of it is that agencies prefer to have their own CP in their PKI domains due to their security concerns.
- Third argument is that in absence of a single dominant PKI solution vendor who would be become in charge of design, implementation and maintenance. Winning invitation to tenders (ITT) would have a huge benefit for any private vendor and of course a massive loss of other ones.
- Finally implementing and managing a new single PKI imply huge cost to government. Therefore, US Congress mandate Federal agencies to implement their PKI solution with their existing budget.

Having all these limitation in mind, US PKI started a project called Federal Bridge Certification Authority (FBCA) which acts similar to authority hub in Hub Authentication Authority. As [9] state *FBCA "does not operate as a root. It does not issues certificates to subordinate CAs or relying parties. Rather, it exchanges a pair of cross-certificates with each participating Federal Agency CA. It has been designed to create trust paths among the individual Federal Agency PKIs".* From technical perspective, there is no online communication between CAs and the Bridge CA and CA cross certify each other (issue certificate) with different security policy and based on information provided by the Bridge CA. These loosely coupled PKI domains which are Federal Agencies have their own CPs. FCBA defines different levels of assurance which are assigned to CP of each domain. This classification has six levels: Rudimentary, Basic, Medium, PIV-I Card Authentication, Medium Hardware, and High. Each PKI domain submit its CP and Certificate Practice Statements (CPS) which is a *"statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements"* [12]. FBCA defined technical and administrational requirements of each assurance level in document called *"X.509 Certificate Policy for the Federal Bridge Certification Authority"* [29]. Based on this directive an assurance level is assigned to a CP of a PKI domain. These domains may have multiple CP for different business applications. Therefore, they may be assigned more than one assurance level. Based on these assurance levels, CA of each domain are able to evaluate level of security practices for each CP applied in a certain domain and choose whether to cross certify with them or not. Through this method security risk of accepting subscribers of a PKI domain is shared between FCBA and other CAs.

From architectural view, this PKI model following Hub Authentication Authority model in which hub create authentication or trust path among PKI domains while Certification path is established between each two CA of different domains.

2.3.2 Canada

Before US, Canada made their strategic decision about implementing PKI enabled technologies in 2003 [21] to secure electronic communication between Government of Canada (GoC) departments. Government On line (GoL) which is responsible for providing network communication for state department asked Entrust – a pioneer in PKI solution – to design and implement and a single unified PKI trust model for all departments.

It seems that unlike US government, Canada did not have problem of choosing a specific private vendor, privacy issue of accumulating information in a single database or heterogeneous certificate policy needs in different departments. Therefore, they choose to create a Single RCA named Canadian Central Facility (CCF)) which manage PKI processes in all domain based on Hub Certification Authority model. CCF issue certificate including four different certification policies for various business application. Each CP is rated based on an assurance level (rudimentary, basic, medium and high). When created, GoC PKI facilitates secure communication only between state departments. But in 2003 secure communication between citizens and government establish through private vendor. In practice, private vendors are cross certified with CCF. Therefore, citizen or commercial sectors that use private PKI vendor are able to use e-Government services. GoC PKI developed a plug-in including its self-signed certificate and configured it into citizen web browsers. In result, citizen and validate certificate of each department that are signed by CCF.

2.3.3 EuroPKI

EuroPKI is successor of two other European projects which first were stared in 1993. *"ICE TEL and ICE-CAR were funded by the European Commission (EC) to promote the development of PKI-based European security technology to protect open networks and advanced network services (such as e-government, e-commerce or e-healthcare)"* [8]. It was an experimental project in 10 European countries which was based on Hub Certification Authority model. As most CAs of PKI domains are located in universities and also certificate are issue to academic center and personnel, it could be concluded that this solution is widely inspired and used in academic environments. RCA was in Denmark and transferred to Politecnico di Torino which was responsible of maintaining it till 2010. On website of RCA [22] there are CA cert and CRLs. It also responsible for publishing CP and CPS, which unlike FBCA and GoC PKI lacks assurance levels. Its policy [23] is also much more flexible than FCBA which result in a loose association as mentioned in the official website.

2.3.4 Other Samples

[21] Provided a survey about PKI trust models implemented in different countries and at time of writing this report website of mentioned countries in were check to see whether any changes in their model has happened or not. Apart from reviewed case studies, Japan and United Kingdom are leveraging Hub Authentication Authority model in which bridge CA act as a trust path and PKI domain (agencies) cross certify each other. Communication Electronic Security Group (CESG) like GoC and FBCA assign different levels of assurance to certificate policy. In Japan, organizations are free in choosing CA product and themselves are responsible of storing key and repositories like CRLs also PKI domain are not restricted to state agencies and it is open to commercial companies.

In Finland and Singapore, on the other hand, Hub Certification Authority model is used. Net trust which is a national PKI solution company is the chosen product for Singapore PKI. As a RCA, it provides online identity and security architecture for both governmental and non-governmental agencies. Also some banks and state organizations act as RA for this RCA to facilitate identification procedure. In Finland, citizens and their own certification embedded in ID card. Väestörekisterikeskuksen (Population Register Office) acts as RCA while police department offices play RA role.

2.4 Proposed Topology for Cross-Domain PKI Trust Model

To propose a topology for PKI trust model for VC, first there is a need to know about principles of this environment, number and density of VPKI domains and interrelation among them. Below is list of the principles in VPKI domain:

- Long-term CA (LTCA): A CA in a VPKI domain that is responsible for issuance of long term certificate (LTC) for vehicles.
- Pseudonym CA (PCA): A CA is VPKI domain that is responsible of issuance of Pseudonym Certificate (PC)
- Pseudonym Resolution Authority (PRA): An entity which responsible for resolution of PC map it to related LTC.
- Road-Side Unit (RSU): Units places on side of a road to transmit data using WAVE (802.11p) protocol from vehicles to PCA and vice versa.
- Subscriber: A vehicle which is registered with an LTCA and has acquired LTC. Based on its LTC it can request PC obtain it from PCA
- Relying party: A vehicle which should validate PC of S form secure communications.
- Domain CA (DCA): A Top CA in a VC PKI domain which is responsible for setting certifications policies, managing certificates operation such as issuing and revocation for LTCA, PCA, PRA

The architecture and protocol for obtaining, validation of and resolution of PC in single VPKI domain is design and implemented in [4].

Purpose of this report is to design PKI trust model between LTCs of different domains. Therefore RSU, PRA are not discussed and Pseudo Certificate is replace with FPC. FPC is pseudonym certificates which are obtained by subscriber from Foreign PKI domain [1]. According to [1] subscriber sends its LTC together with request to PCA of FPKID while passing the domain border. The LTC is signed by LTCA private key which embeds its certificate into it. PCA of foreign domain validates LTCA and LTC, respectively, and then pushes bunch of FPCs to subscriber. Figure 2.4 shows schematic view of Cross-Domain VPKI trust model topology.

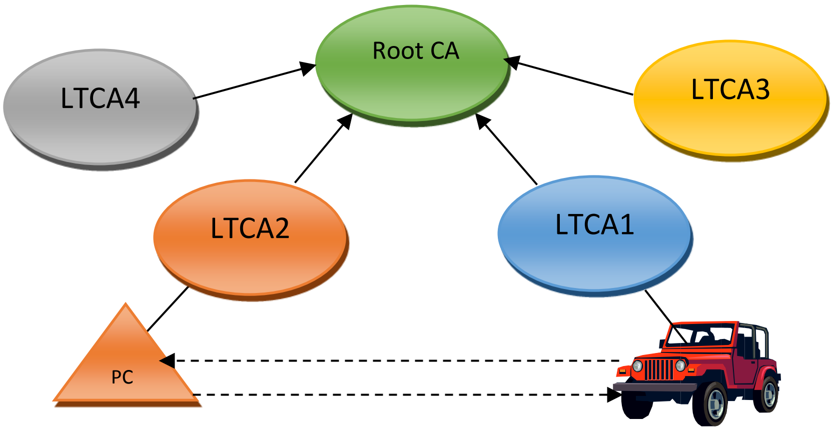


Figure 2.4: Cross-Domain VPKI Trust Model - Topology

Note that inside a VPKI domain there would be CA hierarchy as well. That means LTCA and PCA certificates would be signed by another CA in the same domain that could be named as RCA of specific VPKI domain. As a result, subscriber should have full chain of certificate embedded in this own LTC. In this project assumption is that LTCA is Domain CA (DCA) and responsible for certificate management of a VPKI domain including setting certification policies, issue certificate for subscribers and PCAs. In fact, a VPKI domain is a domain under control of one LTCA which is a RCA of its domain and applies its own CPs.

Here we try to find a suitable PKI trust model considering scalability and performance as non-functional requirement and also Keep It Simple Stupid (KISS) in design. Different PKI trust models which were explained in section 2.1 are reviewed and proper one is selected.

As mentioned before number of VPKI domain CAs is the main issue while choosing a cross domain PKI model. Increasing number of domains mandates CAs to perform risk assessment on each domain they want to certify which means reviewing CP of each and every domain in VPKI environment. This approach in the end forms a CompleteGraph. Moreover, as depicted in Figure 2.5, cross certifying with a PKI domain means that certificate of LTCA1 should be signed by LTCA2. PCA in Domain 2 also needs certificate of its own CA (e.g. LTCA) to validate chain of certificate of subscriber in order to issue FPCs for subscriber. This approach in case of increasing number of PKI domain arise scalability problems.

- First, if Domain 1 cross certify other domains, then subscriber should store a copy of all CA certificates each signed by its own CA. Furthermore, these signed certificates should be embedded in subscriber’s LTC. Therefore, each time it crosses domain border corresponding certificates chain should be sent to PCA of foreign domain.

- Second, storing that many certificate in HSM of subscriber vehicles, choosing the right certificate cause performance overload on subscriber.
- Design and implementation of this solution makes the resulted product complex and hard to maintain.

Considering the above reasons, using Direct Cross Certification is not recommended for Cross-Domain VPKI environment because of scalability, performance and also design and implementation complexity problems. Furthermore, applying Hub Authentication Authority model would result in same problems. Although the risk assessment of VPKI domain certification policies will be transferred to a third party and helps domain CAs about CP evaluation overhead but in the end performance, scalability and complexity issues still remains unsolved.

Therefore, the only remaining model is Hub Certification Authority. Leveraging this model, subscribers just need to store and use one LTC which is signed by LTCA and RCA respectively, forming a certificate chain. Other the validation side, the PCA need to store only RCA certificate to verify the whole certificate chain. Of course, implementing this model has its own drawbacks which were explained in section 2.1. RCA will have to issue certificate for all LTCA in different domains, handling revocation mechanism, accepting security risk of poor certification policies and also being single point of failure.

Now back to nature of VPKI environment, it should be considered that VPKI domains could be cities, states or even countries. Assigning responsibility of writing, supervising correct implementing CP of all domains which already may use different technologies, governmental regulations and political consideration would not be the best practice. Countries may want to have more granular control on vehicle that wants to pass their borders depending on their models, type or manufacturer. Therefore, they need to have their own rule and for a vehicle, just being certified by RCA does not mean that it can necessarily pass FPKIDs border and communicating with other vehicles. In fact, there is a need for a loose cross domain PKI trust model solution to:

- Apply security principle of Separation of Duties [24] in order to perform a double check on identity of a subscriber which wants to pass domain border.
- Distribute security risk of poor certification policy in a certain domain. By this way RCA and DCA both are responsible for authenticity and trustworthiness of a subscriber.

Here, the question is how to apply above solutions. What is responsibility of RCA and DCA? What are the criteria to evaluate trustworthiness of a subscriber? Next section answers these questions. It shows how RCA can evaluate and grade trustworthiness of security practices applied in a VPKI domain. It also explains, based on which criteria, DCA can decide to issue FPC for subscriber and how granular it is.

2.5 Assurance Level of Security Practices and Trust Degree of LTC

Issuing FPCs for a subscriber that enters a foreign VPKI domain can't be simply limited by validation digital signature of RCA and DCA who respectively has signed a digital certificates and form a chain. RCA as hub of a hierarchical structure needs to evaluation all security practices which is used by DCA of VPKI for managing certificate processes such as steps needed for validation certificate request, proofing subscribers identity, issuance of certificate, defining revocation mechanism and etc. Moreover, when PCA of a hosting VPKI domain validate certification of a subscriber it is just sure that current public key is belongs to a principle that its identity and the identity of its VPKI domain CA is approved. But for an independent domain which has its own security principles for VC environment, more granular control should be considered to allow or deny data traffic of a foreign vehicle with other native vehicle in its domain.

A number of research projects have addressed trustworthiness of digital certificates. Carl and Bruce explicate 10 major security risks of PKI [25]. Entrust analyzed trustworthiness of certificate from risk management perspective and listed number criteria to be evaluated in certificate and security policy [26]. David W Chadwick performed a survey among security expert and collected their opinion about criteria which are important for evaluation certificates [27]. Mingde Zhang [34] mathematically formulated evaluation of certificate trust path and listed criteria to compare and grade trustworthiness of subscriber certificate. Based on these researches presenting section categorize security threat types that effect trustworthiness of a certificate and then divides evaluation process of this trustworthiness into two parts: First explain how RCA can evaluate security practices of a VPKI domain and how it can grade them. Then it explicates about criteria that are important for evaluation trust degree of a digital certificate holding by a principle (e.g. LTC in VC). In Cross-Domain VPKI trust model RCA and PCA are responsible for these evaluations, respectively.

2.5.1 Security Threat

As Mingde Zhang [34] defines security thread that trustworthiness of a certificate are listed in three categories:

1. Threats to CA because of poor security practices of a domain:
    a. Threat that targets weaknesses of the private key such as poor algorithm, key length, validity period which may lead to a crack
    b. Stealing or hijacking of private key cause by poor physical or technical design and implementation. Or administrative and management issues.
    c. Certificates might be signed without complying with rules cause by poor authentication and identification regulation.
2. Threat to Subscriber keys because of poor security practices of the domain:

a. Threat that targets weaknesses of the private key such as poor algorithm, key length, validity period which may lead to a crack.
b. Stealing or hijacking of private key cause by poor physical or technical design and implementation. Or administrative and management issues.
c. Certificates might be signed without complying with rules cause by poor authentication and identification regulation.

To address these threats, security practices of VPKI domain should be evaluated. Next section explains about different security practices need to be in place while section 2.5.3 mathematically analyzed criteria that should be develop to judge about trustworthiness of a digital certificate.

2.5.2 Evaluation of VPKI Domain Security Practices

As Entrust defines in its PKI risk assessment document, evaluation of a PKI domain is possible though reviewing two kinds of policies: Certificate Policy (CP) and Security Policy (SP).

2.5.2.1 Certificate Policy

According to RFC 3647 [12], a certificate policy (CP) is *"a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements."* It helps relying party to evaluate trustworthiness of a certification issued for particular application. The important things here is that when CP identification number appears on a certificate, that certificate is only proper to be used in certain business applications and target community stated in CP document. Consider a CA which wants to issue certificate for Sales department and enable them to receive encrypted email in S/MIME format to employees in marketing department. First, it prepares document that explains usage of included public key in certificate and stated that this public key is just for receiving encrypted email to marketing dept. Then include CP document number is certificate (which is an extension in X.509 digital certificate standard) and finally signed the certificate and distribute it to marketing department. Employees of marketing will just use embedded public key of sale department employee to encrypted email is a standard format (S/MIME, PKCS#7). They don’t use public key for encrypting database files or establish SSL session to sales department website.

Not just for subscriber, but CA also have their own certificate policy and part of their self-sign certificate or the one issued by a Trusted CA. RFC 3647 does not stated explicitly what information should be included in CP documents but different PKI vendors and Commercial CA has their own template which they give or organization CAs or subscribers to fill in order to issue certificate for them. There are three extensions in X509v3 standard called: Certificate Policy, Policy-mapping, and Policy-constraint which if their flag CRITICAL is one, then they should contain a value. Necessity of these extensions is based on application which want to use them. If a company uses an eMail client that mandates having certificate policy extensions for using S/MIME then it will just certify CA of an organizations which have CP documents and put its Object Identifier (OID) in X509v3 certificate. This company rejects certificates that lack these extensions and don't send them any encrypted e-mail. To look closer to a CP document here are some of required information that should be field by CA or subscriber which request for certificate signing from a PKI vendor called Entrust [26]:

Field	Mandatory	Description
Issuer	x	Name of CA that issue CP
Subject	x	Name CA (subject CA) or relying party that CP is for
Trust mark		Logo of subject CA
Community		Community of subject CA or S (e.g. Sale dept.)
Hierarchy level		Hierarchy level subject CA in certificate chain
Name		Name space for which subject CA issue certificate for
Key Usage	x	Usage of certified keys (e.g. digital signature)
Policy		Human-readable name of policy
Relying party notice	x	Text to be displayed to the relying party
Certificate access method		The method by which certificates can be obtained from the subject authority's certificate repository.
Revocation access method		The method by which revocation information can be obtained from the subject authority.
Notice registration method		method by which a relying party should register to receive notices issued by the subject CA
Policy authority		The name of the authority which administers the certificate policy.
Notice method		The method by which notices should be sent by the subject authority to the relying party.
Start date	x	The time and date before which the relying party does not qualify as a relying party.
End date	x	The time and date after which the relying party does not qualify as a relying party.

Table 1: Required information for X.509v3 Certificate

According to RFC 3280 [28] this information also appears on X509v3 certificate as extension. Therefore, relying party can see CP information in standard digital file format. These extensions are: Basic constraints, Name constraints, Policy Constraint, Policy mapping, Key usage, Certificate Policy. X509v3 standard and extensions are explained in detail in chapter 3. FBCA [9] and EuroPKI [23] CP document are good examples of real life policies.

2.5.2.2 Security Practices

Since CP is about business application of certificate and its target community, it's not enough to evaluate all security practices of a PKI domain. There are many security considerations in a PKI domain and domain CA should regulate and provide a document for. Certificate Practice Statement (CPS) is a document that mentions all the detail about security practices in a domain. According to RFC 3647 CPS is *"a statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates*" [12]. In one view CPS is an extension to CP. RFC 2527 explains relation between these two artifacts. According to [12] CPS is either a list of CPs issued by a CA, set of provision that is deliberately left by CP to be explained in detail and shows how CP rule should implemented or even statement which does not address anything in CP but certificate practices on CA. In fact, CPS include each and every security practices in PKI domain from key pair generation, principle authentication to air condition specification that needs to be installed in repositories and data centers. A good example of a real life CPS is the one for US FBCA that can be found in here [31].

2.5.2.3 Assurance Level of Security Practices

To evaluation certification policy and security practices RCA of cross domain VPKI needs to review CP document and Certification Practices Statement of each VPKI domain. Then based on this evaluation that can grade them which is called Assurance Level of security practices. Therefore, RCA in Cross-Domain VPKI is responsible for auditing right implementation of stated regulation in CP and especially CPS. Criteria of giving Assurance Level depends on VPKI environment. It could be a state, country or an international community .In Europe, RCA could be an association established by European Commission (EC), there for the criteria should be in compliance with other European security regulations and standards such as Directive 95/46/EC [33] which is out of scope of this project. Furthermore, defining levels of Assurance Level is again based on VPKI regulations and security classifications. FBCA of US Federal PKI has six levels which two of them concerns about Personal Identity Verification Interoperability (PIV-I). As [29] defines these Assurance levels are:

- **Rudimentary**: It concerns primary level of security which is just enough for providing data integrity and signing information.
- **Basic**: It is basic level of security when there is risk of data loss or compromise. Assumption is that user in this level are just normal end-user but not malicious one.
- **Medium:** This level targets transactions that have substantial monetary value or risk of fraud. Using SHA-1 for digital signature is not necessary.
- **PIV-I Card Authentication:** For environment where risk of data compromise in moderate. It targets contactless PIV smart card in which activation of PIN code is not practical.
- **Medium Hardware**: For environment where risk of data compromise and security consequences is high. Using SHA-1 in digital signature is mandatory.

- **High:** *"This level is reserved for cross-certification with government entities"* [29] and suitable for environment which risk of data compromise and security consequences is high.

In FBCA, these Assurance levels are labels on different CPs which are you in different PKI domains. Cross domain VPKI can also define its own assurance level base on existing regulation and security standard label CP and CPS of each VPKI domain with proper level. Chapter 3 shows what is data format of Assurance Level is and how it should be added to subscriber certificate.

2.5.3 Evaluation of Subscriber Certificate

The second step in measuring trustworthiness of a certificate apart from security practices and certificate policies in VPKI domain is to evaluation data that can be extract directly from the certificate itself. There are number researches that have addressed credibility of the certificate, some of their criteria concerns the first step. Mingde Zhang [34] defines and formulates these criteria which can be used by both RCA to evaluate security practices and by relying party to evaluate received digital certificate.

Here Mingde Zhang evaluation method is explained and result is adopted to cross domain VPKI trust model which is aim of this report to develop an evaluation criteria. Mingde introduces a concept of Non-Trust factor (NTF) which is influenced by security risks including crack, forge, leak or hijack of subscribers' certificate and private key. This factor ranges in [0, 1]. Note that less NTF means more trustworthiness of the principle that could be CA, Security Practices or Subscriber. For sake of convenience and formulation, principle are abbreviated and mathematical language is used.

$\mu = NTF(s)$, $\phi = NTF(ca)$, $\varepsilon = NTF(sp)$.

Where S is subscriber, CA is certificate authority of PKI domain who signs certificate of subscriber and SP is security practices applied by in PKI domain. Based on Security Practices defined in CP and CPS, conclude these inferences:

- If SP1 states that CA1 uses RA for identification and authentication of certificate requesters and CA2 process request directly without RA, then: $NTF(SP1) \geq NTF(SP2)$

  Means that using RA because of adding another principle as an intermediate in certification issuance process increases security risk as it there more entities that can be compromised.
- If SP1 allows that private keys if S1 can be stores and software application like browsers and SP2 mandates that private key must be stored in hardware then:
  $$NFT(sp1) \geq NTF(sp2)$$
  Which mean storing private keys in hardware increase trustworthiness of subscriber.

- If SP1 allows that CA1 signs certificate of online which means S1 can remotely apply to certificate signing without coming to CA1 office and SP2 mandate that S2 must come to CA2 in order to get its certificate signed, then:
$$NFT(sp1) \geq NTF(sp2)$$

Apart from evaluation of security practices in a PKI domain, Mingde defines number of quantitative trust degree factor for subscriber's certificate. In case of Cross-Domain VPKI, PCA can use these factor to decide if subscriber is illegible to receive Foreign Certificate or not.

If certification path (CPath) of subscriber can be written in a sequence if would be:

$$CPath = \{c(ca_1), \dots, c(ca_k|ca_{k-1}), \dots, c(s|ca_n)\}$$

In which, ca_1 is trust anchor or RCA. Then trust degree of certificate is:

$$D(s) = \left(1 - \mu^{\lambda(s)\tau(s)}\right) \prod_{k-1}^{n} (1 - \phi^{\lambda(ca_k)\tau(ca_k)})(1 - \varepsilon_k^{\lambda(sp_k)})$$

In which $0 \leq D(s) \leq 1$. Looking this equation value of following parameters affect trust degree:

τ: In this equation τ denote ration of available time and validity period of a public key in certificate. Value of τ is depend of remaining time of validation period called$T_b - T_e$; where, T_b is start date of validity period and T_e denotes end of it. Then:

$\tau = T_{be}^{-1}(T_e - t) \quad if \;\; T_b \leq t \leq T_e$

Therefore, if certificate is closed to be expired trust degree of it declines.

λ: is also denote experience factor. If there is any failed experience in case of validation of subscriber certificate or intermediate CA, then the λ is zero and makes $D(s) = 0$.

Consider two certificate paths:

$$CPath1 = \{c(ca_1), \dots, c(ca_k|ca_{k-1}), \dots, c(s|ca_n)\}$$

$$CPath2 = \{c(ca_0), c(ca_1|ca_0), \dots, c(ca_k|ca_{k-1}), \dots, c(s|ca_n)\}$$

Which means CPath2 is longer than CPath1 and as result $D(s1) \geq D(s2)$. In fact if number of the intermediate CA increases trust degree of certificate declines.

Furthermore, trust degree is also influenced by number of certification path for a certain certificates which means and more than one CA has approved the identity of the key holder.

Following table summarizes evaluation criteria that could be considers either by RCA of cross domain VPKI while evaluating CP and CPS document and also by PCA of FPKID when assessing subscriber certificate before issuing Pseudo Foreign Certificates:

Criteria	RCA of cross domain VPKI	PCA of FPKID
CA delegate to RA responsibility of identification and authentication process before issuance of certificate for subscriber (Not using is RA is an advantage)	x	
Storing subscriber private key is software or hardware (hardware is an advantage)	x	
Applying subscriber certificate request Online or Offline to CA (Offline is an advantage)	x	
Remaining time of certificate validation period (more remained time is as advantage)		x
Fail experience with certification from same subscriber or its CAs in certificate chain		x
Length of certificate path (i.e. number of intermediate CA in certificate chain) of subscriber certificate (shorter length as an advantage)		x
Number of certificate path for a certificate (more paths is an advantage)	Not Applicable	Not Applicable

Table 2: Evaluation criteria for Certification Policy (CP), Certification Practice Statements (CPS) and X.509 certificate

In VPKI environment, PCA can also use other criteria for evaluation trustworthiness of a certificate which is based on their own regulation and standards. X509v3 contains a mandatory data field which is Subject Name. Subject name naming convention is based on distinguish syntax introduced in X.500 standard [30]. As defined in RFC 2253, *"The X.500 Directory uses distinguished names as the primary keys to entries in the directory. Distinguished Names are encoded in ASN.1 in the X.500 Directory protocols"* [30]. Distinguished Name comprised of number of attribute that are supposed to make a Unique Identifier of subscriber. These attribute types are following:

Common Name (CN), Locality Name (L), State or Province Name (T), Organization Name (O), Organizational Unit Name (OU), Country Name (C), Street Address (STREET), Domain Component (DC), User Id (UID)

Examples of Distinguished Name could be:

CN=Behrooz Aghakhanian,O=KTH,C=SE

CN=L. Eagle,O=Sue,C=GB

As a mandatory part of regulation, RCA should define a naming convention for distinguished name for subscriber certificate in cross domain VPKI so that PCA could be able to set and apply their own criteria while evaluation trustworthiness if a certificate. While the serial number of a subscriber certificate is its unique identity, the Subject Name can be defined in from of:

CN= [vehicle model], OU= [Vehicle type], O= [Manufacturer], T= [State], C= [Country]

Where:

- Vehicle model: Model of a car named by manufacturer such as Volvo V70, Bentley Mulsanne
- Vehicle type: public transport, emergency, private, VIP, diplomatic, and etc.
- Manufacturer: Volvo, Saab, Rolls-Royce
- State: Skåne, Västra Götaland, Bavaria, Attica
- Country: Sweden (SE), Greece (GR), Iran (IR)

Therefore, examples of subject name for VPKI environment could be:

- CN= [V70], OU= [private], O= [Volvo], T= [Skåne], C= [SE]
- CN= [Bentley Mulsanne], OU= [diplomatic], O= [Rolls-Royce], T= [Attica], C= [GR]

Each VPKI domain has its own regulation and rules that may not be just related technical security issues but administrative or political. PCA of FPKID is able to evaluation trustworthiness of a subscriber based one either certification trust degree criteria or X509v3 subject name.

To summarize this section, trustworthiness evaluation of a certificate is based one security practices in different VPKI domain which include information stated in CP and CPS. This evaluation is performed by RCA of cross domain VPKI and domain are grade with Assurance Level which is security classification of security practices based on RCA criteria. RCA should also consider criteria stated in presenting chapter under Non-Trust Factors (NTF). Then PCA evaluates issued certificate by a VPKI domain based on criteria of trust degree stated in this chapter plus subject name in X509v3 certificate. Next chapter explains design and implementation of proposed cross domain PKI trust model including the topology, architecture and programmatic modules.

3 Design and Modeling

Having defined topological architecture of Cross-domain VPKI trust model and evaluation method to assess trustworthiness of subscriber certificate, this chapter explains how to develop proposed solution. Frist, scope of design and implementation is defined and it continues with explaining modeling language. Then based on different diagrams used in the modeling language schematic view, communication sequences of components of final product is illustrated. After that standards and protocols leveraged for realizing the models are explained and then reason for using is justified. Finally cryptographic algorithm and libraries, programmatic languages and operating system that developed code needs to complied and executed on is mentioned.

3.1 Scope and Assumptions

This section explains why all proposed solution especially in certification trustworthiness evaluation is not developed in final product. As this project is supposed to be integrated into [4] which is another VPKI project in the LCN research group, it was needed that the writer of this report to be able to develop code in a programming language and uses cryptographic and communication library which he is novice in. Of course, this project also benefits from experience of related project but lack of proficiency in C++, OpenSSL API make it difficult to add additional features.

Here is scope and assumption of this project regarding software development phase:

- In this project, LTCA of a PKI domain is the top CA in the domain (DCA) and issues LTC for vehicles (subscribers) and PCAs. RCA issue certificate for LTCA of each domain so that they could be able to establish trust among each other.
- Software product is consist of three component:
    - Subscriber which request for LTC for LTCA. LTC is issued and embedded in vehicles HSM which has long validation period. But renewal of LTC is needed in case on certificate compromise or changes in certification info like Distinguish Name and Assurance Level of domain. Therefore, there should be a mechanism to generate LTC request.
    - LTCA which issue certificate for subscriber and embed Assurance Level field which is given by RCA, into certificate of subscriber as an X509v3 extension
    - PCA of FPKID which extracts Assurance level flag and SubjectName of subscriber certificate and base of this information decides whether to issue FPC or not.
- Project does NOT development subscriber’s request for FPC from PCA of FPKID which is done by [4]

- Project does NOT consider trust degree criteria stated in section 2.5.3 which are remaining time of validation period, Certificate path length and failed experience of same subscriber or CAs in its certificate chain. This information can be extracted and also customized in other industrial projects.
- Project does NOT develop revocation solution for Cross-domain VPKI.
- Decision that should be made based on extracted information from subscriber certificate which could be issuing FPCs and applying granular customization in certificate information is out of scope of this project because it is different from on VPKI domain to another VPKI domain.

3.2 Design and Modeling

According to [35], since its introduction in 1997 the Unified Modeling Language (UML) is the de facto modeling language for software development. This project used object oriented design and leverages these three diagrams (which is drawn using Microsoft Visio 2007 and could be found in Appendix): Sequence, Component and Deployment.

As described above, Sequence diagram helps developers and customers to understand interaction between different components in a system. Moreover, it shows time sequence of requests and replies signals. Cross-Domain VPKI application is consists of three entities which are subscriber, LTCA and PCA of FPKID.

1. Subscriber generates Elliptic Curve Public Key Pair.
2. Subscriber creates Certificate Signing Request (CSR).
3. Subscriber sends it online to LTCA of its domain.
4. LTCA issues new LTC embeds Assurance Level of its PKI domain.
5. LTCA load its private key and signs LTC and create certificate chain by adding its own certificate.
6. LTCA sends it back to subscriber.
7. Subscriber validate signed LTC.
8. Passing domain border, subscriber sends its LTC to PCA of FPKID.
9. PCA verify certificate chain.
10. PCA extracts assurance level and subject name from LTC and issue and send FPCs to Subscriber

However, issuance and sending FPCs to subscriber is out of scope of this project.

Appendix 1 is Sequence diagram of these steps. In this diagram details about data type and data of CSR, LTC and interfaces of each component is not explained. This information is presented in Component diagram.

Components diagram as stated before, illustrates components and their relationships. Each of these components contains classes of code and interfaces. In Cross-Domain VPKI application each entity in Sequence diagram become one component in Components diagrams. Each component also contains one class of code and interfaces that provide communication between components. In fact, other functions and private which are revoked internally. This report keeps abstraction at components level and does not visualize class diagram because each component just contain one class. Here is list of the components and their interfaces. Appendix 2 shows the actual Components diagram.

Having explained about each component and their relations, Deployment diagram is need to visualize node components should be deployed on. In Cross-domain VPKI application which is a demo software, nodes are host computers with Linux Ubuntu v12.04 as operation systems. In real life scenario, deployments diagram should include specification of HSM of vehicle as subscriber and also PCA and LTCA hardware and software specification like database, repository system, and etc. In demo versions, code of each component is compiled and executed one Linux machine. Linux hosts are virtual machines virtualized and deployed using VMware ESX server v5.1 and are accessible through VMware vCloud Director.

Data files which used to store CSR, LTC, LTCA certificate and RCA public key are in PEM (Privacy Enhanced Mail) format and stored in local file system of Linux hosts. PEM is a Base64 encoded file that store DER certificate and public and private keys. DER specifies a self-describing and self-delimiting format for encoding ASN.1 data structures of certificates. More detail about file format is explained in next section. Appendix 3 shows the actual Deployment diagram of Cross-domain VPKI domain.

3.3 Digital Certificate standard and communication protocol

Having visualized architecture of Cross-Domain VPKI application which describes programmatic components and their relationships, this section explicate standards used for creating certification request and LTC. It also explains communication protocol which is used for communication between components.

3.3.1 Certificate Signing Request

According to Sequence diagram in Appendix 1, first step to communication is between subscriber and LTCA where both are belongs to one domain. As mentioned in section 4.1 in case of any need for LTC renewal which could be any changes in Distinguish Name of subscriber, compromise of keys or change is Assurance Level of VPKI domain, there should be a mechanism to request of LTC again. Subscriber generates a public and private key pair which the algorithm is explained in next section, and then it creates a certificate request which contains subscriber identity in form of X.500 Distinguish Name. Finally, it embeds its public key to certificate request and sends it to LTCA. In fact, as mentioned before, the main purpose of digital certificate is to bind identity of subscriber of its public key.

RFC 2986 defines a standard for creating certificate request which was first introduced by RSA Laboratory as part of Public-Key Cryptography Standards (PKCS) series named PKCS#10.

PKCS is a group of public-key cryptography standards devised and published by RSA Security Inc, starting in the early 1990s. Well-known standards in this series are:

- PKCS#7 which is used to sign and/or encrypt messages under a PKI. In S/MIME for sending encrypted and signed emails and also Cryptographic Message Syntax Standard (CMS) which is used for single sign-on.(SSO) to provide authentication and authorization.
- PKCS#11 which is known as Cryptoki, an API defining a generic interface tocryptographic tokens (see also Hardware Security Module). Often used in single sign-on, Public-key cryptography and disk encryption systems.
- PKCS#12 which defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

PKCS#10 which is known as Certificate Signing Request (CSR) is *"a certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification"* [32]. In Cross-domain VPKI application, Subscriber component instantiates a CSR object though OpenSSL library and add three information to CertificateRequestInfo which an ASN.1 syntax:

- Serial number which is a mandatory unique identifier of CSR
- SubjectName which is in form of DN and just contain CommonName
- Subscriber's public key

Then, CSR library signs CertificateRequestInfo value with subscriber's private key. Finally, CSR is stored in PEM file format which could be send later to LTCA.

3.3.2 X509v3 Certificate

After generating CSR by subscriber component, LTCA performs following steps to issue a LTC:

- Parsing CSR from communication socket and store it in an OpenSSL CSRobject
- Extracting SubjectName data which is an CommonName in DN format and also public key
- Creating an new X509v3 certificate and add information plus subscriber public key
- Adding Assurance Level as X509v3 custom extension to X509v3.
- Loading its private key and signs the X509v3 certificate.
- Sending back signed certificate to subscriber
- Subscriber validated signed certificate with public key of signer

X509v3 standard which is used as LTC, according to RFC 3280 is *"part of the X.500 Directory recommendations, defines a standard certificate format. The certificate format in the 1988 standard is called the version 1 (v1) format. When X.500 was revised in 1993, two more fields were added, resulting in the version 2 (v2) format"* [28]. Purpose of creating X509 is to provide a standard to bind identity of certificate holder to its public key in CA based PKI environment which is widely used on internet. Both CRS and X509 use ASN.1 which is a standard and notation language that describes rules and structures for representing, encoding, transmitting, and decoding data. X509 leverages this standard to define certificate information including identification data, extensions and public key in data structures. These data structures can be encoded in different file formats such as Basic Encoding Rules (BER) and Distinguished Encoding Rule (DER). According to RFC 3280, X509v3 provides number of standard extension to store different data about certificate such as Subject Key Identifier, Key Usage, Policy Mapping, and Basic Constraints. Moreover, it gives developers of X509v3 to define custom extension. In Cross-Domain VPKI application an extension is needed for Assurance Level which its data cannot be added under title of other standard extensions.

List of information which is added in LTC is:

- Version: V3 which is X509 version of LTC
- Serial Number: Unique Identification of LTC
- Validity period:
    - Valid from: Before it date LTC is not valid
    - Valid to: After this date LTC is not valid
- Issuer Name: CommonName of LTCA is DN format
- Subject Name: CommomName of subscriber which is extracted from CSR
- Assurance Level
- Public Key of subscriber

OpenSSL X509v3 library adds signature algorithm and actual signature that it is used to sign LTC at the end of certificate. Appendix 4 shows a sample of and issued LTC.

After receiving LTC by PCA component of FPKID, it performs following actions:

- Loads RCA public key and verifies subscriber certificates chain which store certificate of LTCA and LTC is form of X509 certificate stack. This is done by OpenSSL X509v3 library
- Extracts Assurance Level and SubjectName and store them a variables which can be used by PCA component to decide whether it issue FPCs for subscriber or not.

3.3.3 Communication protocols

As stated before, components pass data to each other. Subscriber sends CSR to LTCA, LTCA send back signed LTC. Then subscriber send LTC to PCA of FPKID to get validated. PCA validate it and sends back a parameter as acceptance or rejection. This implementation leverage XML-PRC [38] which is a remote method revocation protocol that uses XML to send parameters. Moreover, before sending any data, subscriber establish SSL tunnel to LTC and PTC component which are running as CGI script on Linux Apache server.

4 Implementation and Performance Measurement

Having explained about Certification and Communication standards and formats, this section first overview cryptographic library and algorithm and why it is used in developing Cross-Domain VPKI and then explains about programming language and Integrated Development Environment utilized to develop code base of application.

4.1.1 OpenSSL and Cryptographic Algorithm

To develop all three components including Subscriber, LTCA and PCA, there is a need for a cryptographic library. Considering financial limitations of this project this library should be free of charge. Among free cryptographic libraries, there are two well-known and open source providers: OpenSSL and BouncyCastel. Both has libraries that could be used as dependency in C++ and compiled on Linux which is programming language and host computer of the project and also implemented classes which is needed in for developing Cross-Domain VPKI application. But because of following reason OpenSSL v.1.0.1) is chosen for this project:

- OpenSSL v.1.0.1 provides a method to easily define X509v3 custom extension (stated in RFC 3280) which is needed for adding Assurance Level to subscriber LTC. BouncyCastel does not support this feature.
- OpenSSL X509v3 libraries is more mature in compare with BoucyCastle, since is more common among C/C++ developers. So, more contribution has been done in regarding of implementing RFC 3280 features.

It also provides following classes:

Cryptographic Alghrithm: In Cross-Domain VPKI application, generating Public key pairs is for subscriber, RCA and LTCA. Subscribers need to have key pair for signing their CSR request and any other data that is needed for securing communication. RCA needs it to sign LTCA certificates and LTCA uses it for signing subscriber X509v3 certificate. Generally, three main algorithms are supported by OpenSSL: RSA, DSA and Elliptic Curve Cryptography (ECC). For the sake of compatibility with preceding project in VPKI keys are generated with ECC on prime256 curve which will be used in creating CSR, certification signing and verification. Strength and efficiency of ECC over RSA algorithm is proved in [36].

Moreover, as indicated in table 3, ECC shows how ECC has the same level of security as RSA with shorter key sizes, generated keys are smaller which fit low speed networks and signing operation is faster in compare with RSA.

Symmetric	RSA/DSA/DH	ECC	Time to break in MIPS years
80	1024	160	$10^{\wedge 12}$
112	2048	224	$10^{\wedge 24}$
128	3072	256	$10^{\wedge 28}$
192	7680	384	$10^{\wedge 47}$
256	15360	512	$10^{\wedge 66}$

Table 3: Security Level Comparison of Symmetric, RSA and ECC (key sizes in bits) [39]

Signature Hash algorithm: As part of certificate signing process, X509v3 certificate should be first hashed and then get signed by private key. The hash algorithm is recommended by NIST in 'Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths' published on 2011 should not use SHA-1 or weaker algorithms after the end of 2013 [37]. Therefore this project uses SHA-256 for ECDSA signature which is also provided in OpenSSL v1.0.1 and also used by related projects in LCN.

PKCS#10 CSR and X509v3: OpenSSL also provides proper libraries to issuance and verifying X509v3 certificate and certificate chain with support of adding custom extension which is used to embed Assurance Level to LTC. It also has classes to generate PKCS#10 CSR for subscriber components. Moreover, it provide special I/O libraries to read and write PEM file format which is used to store CSR, X509v3 and public key pair.

4.1.2 C++ and IDE

As mentioned in section 3.2, this project uses Object Oriented design for developing Cross-Domain VPKI application. Therefore, it is needed to utilize a programming language which supports writing classes of codes. C++ is the language chosen over Java for developing code of application for the sake of compatibility with previous projects in VPKI. G++ which is an open source compiler is used to compile developed code while NetBean v7.1 with C/C++ workspace is utilized as Integrated Development Environment.

4.2 Performance Measurement

To evaluate scalability and reliability of Cross-Domain VPKI demo tool, a performance measurement test is done which includes following test cases:

- Creating CSR
- Issue and signing certificate
- Validation and information extraction of certificate

Client (CSR component) and CA (signing and validation component) are compiled and run on a Linux Ubuntu 12.04 machine which is virtualized using VMware ESX server 5.1. Here are specification of the machine:

CPU	RAM	OS
Single Core 2GHz	1 GB	Linux Ubuntu 12.04

Table 4: Configuration of systems hosting performance test

Below figures show measured time each component 1, 10, 100, and 1000 LTCs, respectively:

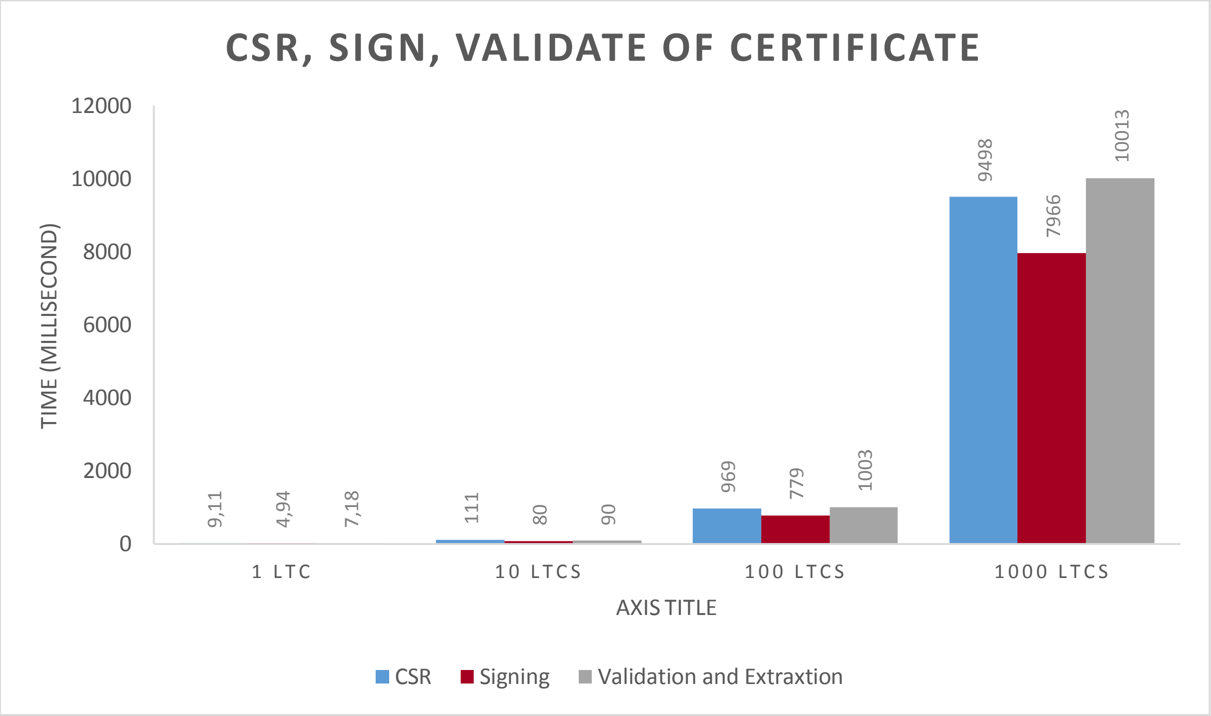


Figure 4.1: CSR, Sign and Validation time of certificate (milliseconds) for 1,10,100,1000 LTCs

Following figures show the average time of performing each step in both LTC obtaining and LTC validation and information extraction test cases after 1000 times of repetition:

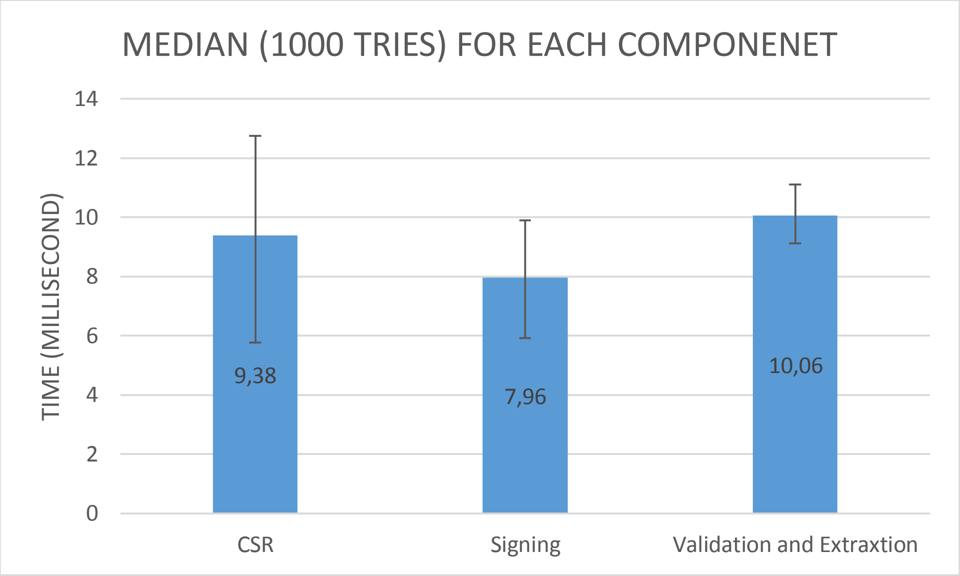


Figure 4.2: Median for CSR, Signing and Validation components

Collected data and analysis shows that the implemented demo tool is scalable as there is no dramatic decrease in response time of CSR, certificate issuance and components. To wrap up Chapter 4, appendix 5 list all standard and software versions which is used to develop Cross-domain VPKI Application.

5 Conclusion and Future Works

This research project proposed a Cross-Domain PKI trust model for VC environment and implemented a proof-of-concept code to demonstrate how the model's features function in practice. Using this model, VPKI domains can establish different levels of trust among each other called Assurance Level through evaluation of PKI security practices in each domain which is done by a Root CA entity in a hierarchical architecture. Moreover, PCA in foreign domain is able to assess validity and credibility of a LTC not just by verifying its signature but leveraging other mandatory fields or extensions such as SubjectName, BasicConstraint beside the Assurance Level which is embedded as a custom extension in LTC of vehicle. Cross-Domain VPKI trust model is scalable since hierarchical PKI model is in used which unlike direct cross certification model, its performance will not decrease dramatically by increasing number of VPKI domains. Also, CAs leverage ECDSA in generating cryptographic key pairs which is faster in signing and verifying in compare with RSA and DSA.

Since the implemented code for CAs and vehicle is a demo to show how proposed model function, it has long way to become a sophisticated CA code base which needs systematic functional and non-functional requirement analysis including all possible security threats.

As future works in Cross-Domain VPKI I would suggest developing a framework for evaluating security practice in VPKI domain including CP and CPS analysis which includes defining multiple categories as Assurance Level. There are number researches for defining evaluation criteria for validity or trust degree of a digital certificate, but it could be narrowed down according to specific use cases of LTC in VC environment and applications.

6 Bibliography

[1] Papadimitratos, Panagiotis, et al. "Secure vehicular communication systems: design and architecture." *Communications Magazine, IEEE* 46.11 (2008): 100-109.

[2] Papadimitratos, Panos, et al. "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation."*Communications Magazine, IEEE* 47.11 (2009): 84-95.

[3] Mariyasagayam, M. N., H. Menouar, and M. Lenardi. "GeoNet: A project enabling active safety and IPv6 vehicular applications." *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*. IEEE, 2008.

[4] Alexiou, Nikolaos, et al. "VeSPA: vehicular security and privacy-preserving architecture." *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy. Budapest, Hungary*. 2013.

[5] Wolf, Marko, and Timo Gendrullis. "Design, implementation, and evaluation of a vehicular hardware security module." *Information Security and Cryptology-ICISC 2011*. Springer Berlin Heidelberg, 2012. 302-318.

[6] Festag, Andreas, et al. "'NoW–network on wheels': Project objectives, technology and achievements." (2008).

[7] Alexiou, Nikolaos, et al. "Towards a Secure and Privacy-preserving Multi-service Vehicular Architecture." 4th IEEE International Workshop on Data Security and Privacy in Wireless Networks: D-SPAN. 2013.

[8] Lioy, Antonio, et al. "The euroPKI experience." *Public Key Infrastructure*. Springer Berlin Heidelberg, 2004. 14-27.

[9] Alterman, Peter. "The US federal PKI and the federal bridge certification authority." *Computer Networks* 37.6 (2001): 685-690.

[10] P. Papadimitratos. IoT Security - Part 1: Secure Vehicular Communication Systems. Networked Systems Security (NSS), Lecture Notes, Slide #32, 2012. [online] Accessed on May 3, 2012. http://www.ee.kth.se/~papadim/nss/nss.html.

[11] Hevner, Alan R., et al. "Design science in information systems research." *MIS quarterly* 28.1 (2004): 75-105.

[12] Chokhani, Santosh, and Warwick Ford. "Internet x. 509 public key infrastructure certificate policy and certification practices framework." (1999).

[13] Adams, Carlisle, and Steve Lloyd. *Understanding PKI: concepts, standards, and deployment considerations*. Addison-Wesley Professional, 2003.

[14] Perlman, Radia. "An overview of PKI trust models." *Network, IEEE* 13.6 (1999): 38-43.

[15] Caronni, Germano. "Walking the web of trust." *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000.(WET ICE 2000). Proeedings. IEEE 9th International Workshops on*. IEEE, 2000.

[16] Ramsdell, Blake. "S/MIME version 3 message specification." (1999).

[17] Freier, Alan, Philip Karlton, and Paul Kocher. "The secure sockets layer (SSL) protocol version 3.0." (2011).

[18] Frankel, S., and S. Krishnan. *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*. RFC 6071, February, 2011.

[19] Recommendation, I. T. U. T. X. "200 (1994)| ISO/IEC 7498-1: 1994." *Information technology–Open Systems Interconnection–Basic Reference Model: The basic model*.

[20] Mozilla. "Included Certificate List," Mozilla.org. [Online]. Available: http://www.mozilla.org/projects/security/certs/included/ [Accessed: April. 30, 2013].

[21] Yildiz, Eedal. “A Proposal for Turkish Government Public Key Infrastructure Trust Model.” Middle East Technical University, 2001.

[22] EuroPKI. “Certificate of the EuroPKI RCA”, europki.org. [Online]. Available: http://www.europki.org/ca/certs/ [Accessed: April. 30, 2013].

[23] Policy, EuroPKI Certificate. "Version 1.1 (Draft 4)." (2000).

[24] Simon, Richard T., and Mary Ellen Zurko. "Separation of duty in role-based environments." *Computer Security Foundations Workshop, 1997. Proceedings., 10th*. IEEE, 1997.

[25] Ellison, Carl, and Bruce Schneier. "Ten risks of PKI: What you're not being told about public key infrastructure." *Comput Secur J* 16.1 (2000): 1-7.

[26] Boeyen, Sharon, and Tim Moses. "Trust management in the public-key infrastructure." white paper, Entrust, available at: www. entrust. com/resources/download. cfm/21126/trustmodels. pdf (2003).

[27] Chadwick, David W., and Andrew Basden. "Evaluating trust in a public key certification authority." *Computers & Security* 20.7 (2001): 592-611.

[28] Housley, Russell, et al. "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile." (2002).

[29] Authority, Federal Bridge Certification. "X. 509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)." *current edition* (2002).

[30] Wahl, Mark, Tim Howes, and Steve Kille. "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names." (1997).

[31] Authority, Federal Bridge Certification. "United States Federal PKI X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI) Trust Infrastructure." current edition (2011).

[32] Nystrom, Magnus, and Burt Kaliski. "PKCS# 10: Certification Request Syntax Specification Version 1.7." (2000).

[33] DATA, MOVEMENT OF SUCH. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." Official Journal L 281.23/11 (1995): 0031-0050.

[34] Zhang, Mingde, et al. "Research on Model of Trust Degrees for PKI."*Information Assurance and Security, 2009. IAS'09. Fifth International Conference on*. Vol. 2. IEEE, 2009.

[35] Lange, Christian FJ, Michel RV Chaudron, and Johan Muskens. "In practice: UML software architecture and design description." Software, IEEE 23.2 (2006): 40-46.

[36] Calandriello, Giorgio, et al. "On the performance of secure vehicular communication systems." Dependable and Secure Computing, IEEE Transactions on 8.6 (2011): 898-912. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5611547 &isnumber=6016569

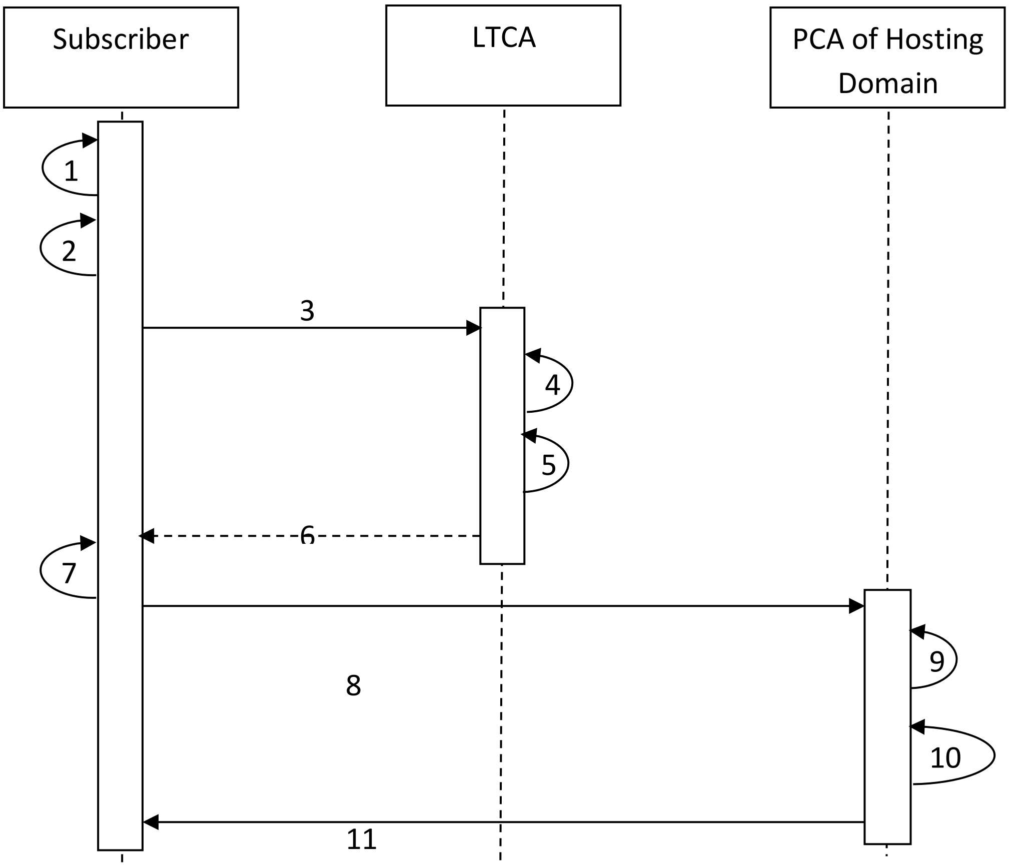
[37] Barker, E., et al. "NIST special publication 800-57: Recommendation for key management—part 1." (2007).

[38] Winer, Dave. "Xml-rpc specification, 1999." *URL http://www. xmlrpc. com/spec*(2003).

[39] Khalique, Aqeel, Kuldip Singh, and Sandeep Sood. "Implementation of elliptic curve digital signature algorithm." *Int J Comput Appl* 2.2 (2010): 21-27.

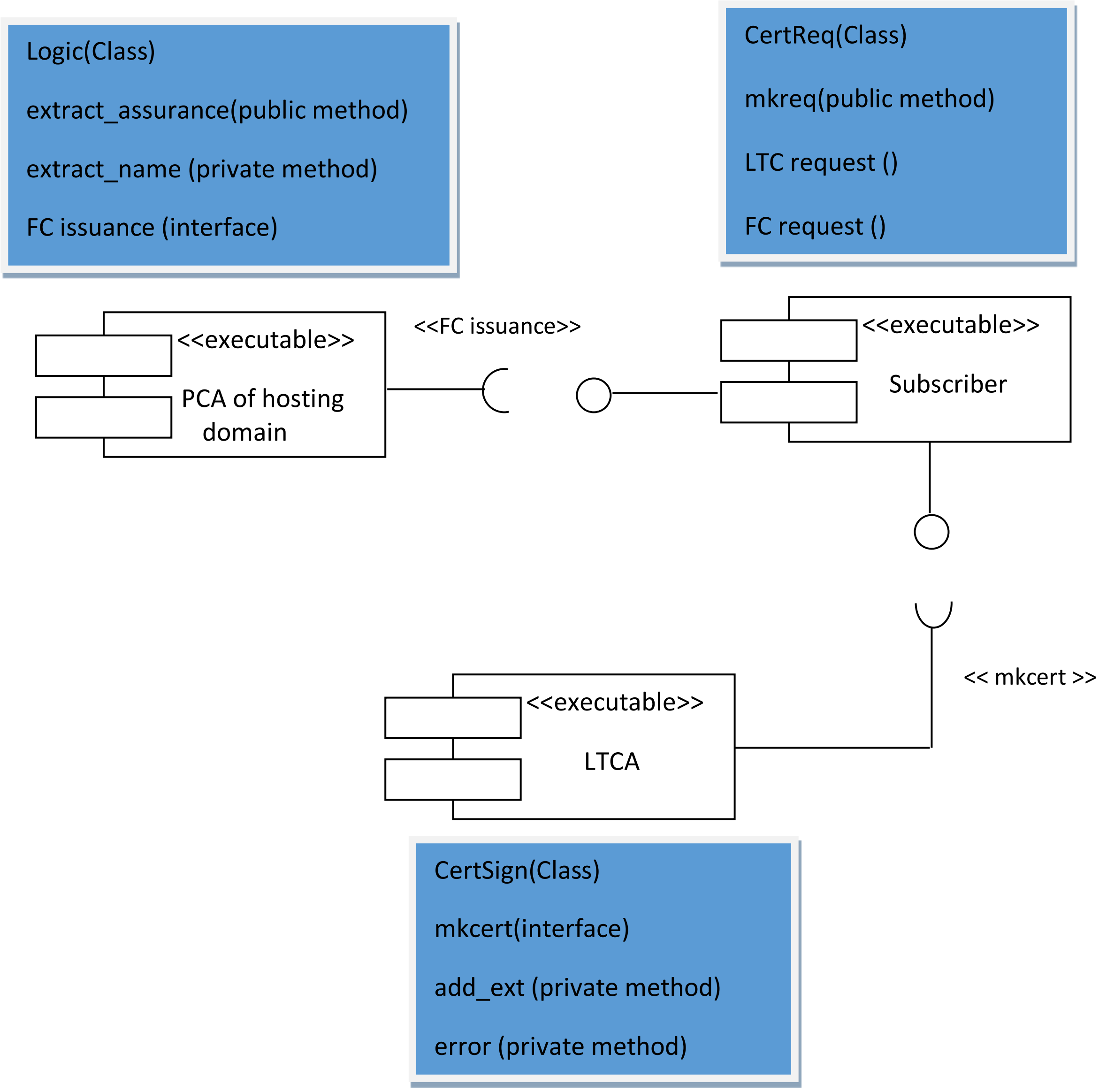
Appendices

A.1 UML Sequence Diagram of Implemented Design

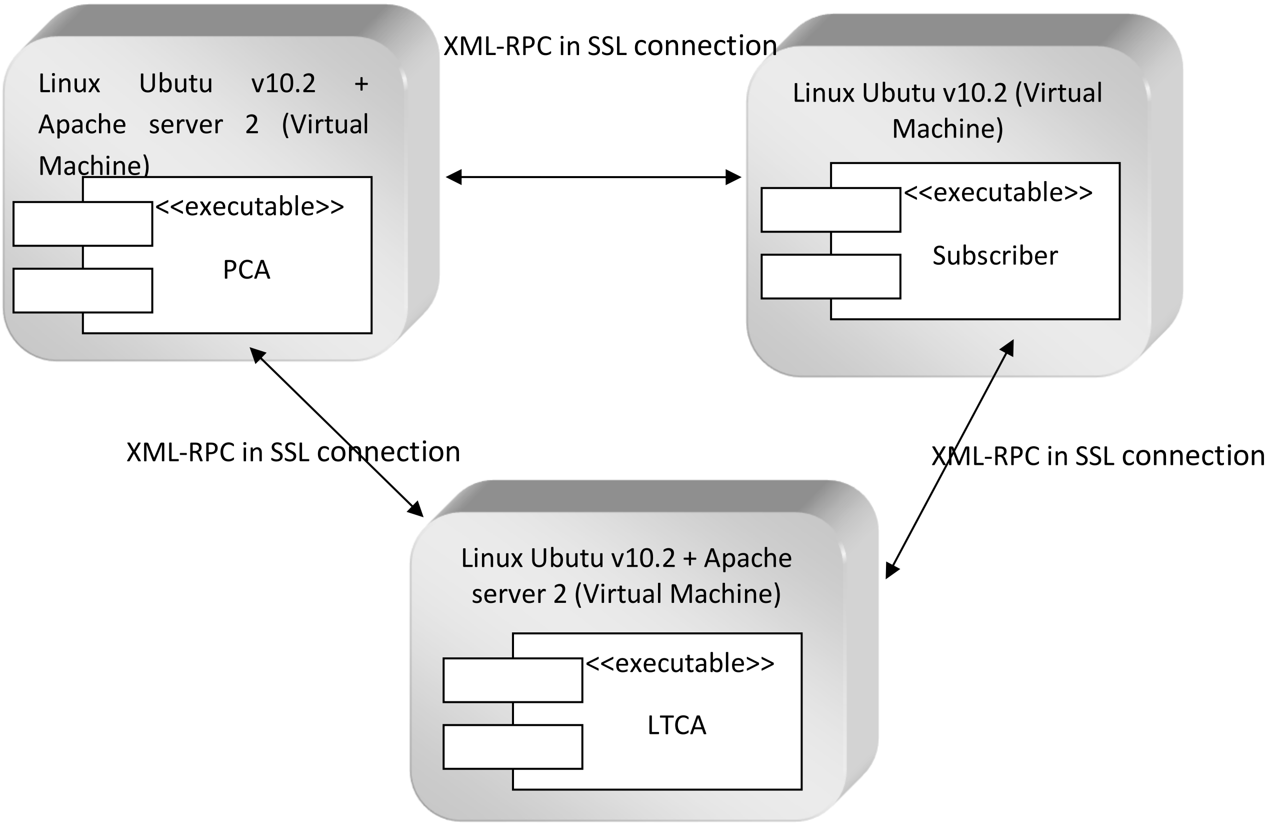


1. Subscriber generates Elliptic Curve Public Key Pair.
2. Subscriber creates Certificate Signing Request (CSR).
3. Subscriber sends it online to LTCA of its domain.
4. LTCA issues new LTC embeds Assurance Level of its PKI domain.
5. LTCA load its private key and signs LTC and create certificate chain by adding its own certificate.
6. LTCA sends it back to subscriber.
7. Subscriber validate signed LTC
8. Passing domain border, subscriber sends its LTC to PCA of FPKID.
9. PCA verify certificate chain.
10. PCA extracts assurance level and subject name from LTC, Perform decision logic
11. PCA issues and send FCs to Subscriber

A.2 UML Component Diagram of Implemented Design



A.3 UML Deployment Diagram of Implemented Design


XML-RPC in SSL connection
Linux Ubutu v10.2 + Apache server 2 (Virtual Machine)
<<executable>>
PCA
Linux Ubutu v10.2 (Virtual Machine)
<<executable>>
Subscriber
XML-RPC in SSL connection
XML-RPC in SSL connection
Linux Ubutu v10.2 + Apache server 2 (Virtual Machine)
<<executable>>
LTCA

A.4 Sample LTC Issued by LTCA

```
Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: ecdsa-with-SHA1
        Issuer: C=SE, ST=Stockholm, O=KTH, OU=EE, CN=RCASE
        Validity
            Not Before: Aug 12 10:32:44 2013 GMT
            Not After : Aug 12 10:32:44 2014 GMT
        Subject: C=sd, CN=sdf
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            EC Public Key: pub:
                    04:a0:4b:59:72:17:45:c9:75:6f:16:46:c9:31:0f:
                    5b:ad:79:8a:65:52:4e:5b:4d:b2:20:e6:ef:f9:26:
                    5e:16:90:cd:9f:60:08:75:47:b5:85:71:44:27:a0:
                    08:6e:31:db:17:6c:3d:05:c9:7b:d6:d7:98:23:a8:
                    36:d9:49:d6:11
                Field Type: prime-field
                Prime:
                    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
                    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
                    ff:ff:ff
                A:
                    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
                    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
                    ff:ff:fc
                B:
                    5a:c6:35:d8:aa:3a:93:e7:b3:eb:bd:55:76:98:86:
                    bc:65:1d:06:b0:cc:53:b0:f6:3b:ce:3c:3e:27:d2:
                    60:4b
                Generator (uncompressed):
                    04:6b:17:d1:f2:e1:2c:42:47:f8:bc:e6:e5:63:a4:40:f2:77:03:7d:81:2d:eb:33:a0:f4:a1:39:45:d8:
                    98:c2:96:4f:e3:42:e2:fe:1a:7f:9b:8e:e7:eb:4a:
7c:0f:9e:16:2b:ce:33:57:6b:31:5e:ce:cb:b6:40:68:37:bf:51:f5
                Order:
                    00:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:ff:
                    ff:ff:bc:e6:fa:ad:a7:17:9e:84:f3:b9:ca:c2:fc:
                    63:25:51
                Cofactor:  1 (0x1)
                Seed:
                    c4:9d:36:08:86:e7:04:93:6a:66:78:e1:13:9d:26:
                    b7:81:9f:7e:90
        X509v3 extensions:
            1.2.3.4:
                ..A...
    Signature Algorithm: ecdsa-with-SHA1
        30:45:02:21:00:c1:2e:33:a7:71:c9:eb:c0:06:f9:ce:ed:b0:30:a1:02:5a:fc:59:ba:f3:fe:cc:26:23:45:25:e3:ef:3c:45:
        f5:02:20:24:89:65:5e:b8:4a:e3:0c:a3:6e:f3:8d:98:b2:4b:18:c1:ff:a2:fd:c7:e6:a0:cf:f2:43:59:69:7c:44:8c:b2
```

A.5 List of Algorithm, Libraries, Tool used in development

Name	Usage
SHA-256	Hash algorithm used for signing LTC by LTCA
ECDSA prime256v2	Public Key pair generation algorithm use by subscriber and LTCA
UML 2.2	UML version used for making Object Orient diagrams
OpenSSL v1.0.1e (Linux source code and libraries)	Cryptographic library use for generating public key pair, CSR, LTC (X509v3)
XML-RPC C/C++ library	Establish connection between components
VM ware ESX server 5	Used for deploying Linux Ununtu 10.2 virtual machines
Linux Ubuntu 12.04	Operating system used for running executive binary of component
vCloud Director 5	GUI for ESX server used for virtualization of Linux hosts
C++ (g++ as compiler)	Programming Language used for developing the code base
NetBean with C/C++ workspace	IDE used for writing C++ code, debugging, compiling and packaging
X509v3 (RFC 3280)	Standard used for creating LTC for subscriber
PKSC #10 (RFC 2986)	Standard used for creating CSR