Secure Vehicular Communication Systems: Cross-Domain VPKI Trust Model

Behrooz Aghakhanian

Under Supervision of Prof. Panos Papadimitratos

LCN , School of Electrical Engineering

KTH

14Oct. 2013

Outlines

- Background and Related Works
- Problem Definition and Contribution
- Cross-Domain VPKI Trust Model
- Design and Modeling
- Performance Evaluation
- Conclusion and Future Works

Outlines

- Background and Related Works
- Problem Definition and Contribution
- Cross-Domain VPKI Trust Model
- Design and Modeling
- Performance Evaluation
- Conclusion and Future Works

Background

- Applications in Vehicular Communication: Transportation Safty and Effeicency, Infotainment
- Security Requirement in VC application
  - Confidentiality
  - Message Authentication and Integrity
  - Non-repudiation
  - Access Control and Accountibility
  - ... While considering **Privacy of vehicles**

Related Works

- SeVeCom project address above security requirement:
  - Assymmetric Cryptography with PKI
  - Encryption and Digitally Signature
  - Long Term Certificate (LTC) and Pseudonym Certification
  - Hardware Security Module (HSM)
- Design and Implementation of LTCA, PCA
- EVITA, NoW, PRESERVE

Outlines

- Background and Related Works
- Problem Definition and Contribution
- Cross-Domain VPKI Trust Model
- Design and Modeling
- Performance Evaluation
- Conclusion and Future Works

Problem Definition

- SeVeCom model addresses single Vehicular PKI (VPKI) domain
- Multiple trust level between VPKI domians
  - Different Security Practices
  - Non-technical criteria regarding esblishing trust with a VPKI domian
- Granular evaluation of vehicle certificate
  - Type, model, manufactures of vehicle
  - Remaining Validity Period on certificate

Contribution and Methodology

- Design a Cross-Domina VPKI trust model
  - Scalable trust topology among VPKI domains
  - Enable VPKI domain to establish different levels of trust
  - Give granular control for evaluation of LTC before issuing Foriegn Pseudonym Certificate(FPC)

- Methodology
  - Studing PKI topology and propose one for Cross Domain VPKI
  - Studing trust evaluation methods for PKI domain and X509 certificate. Proposing a new model for Cross Domain VPKI
  - Design, develope and test a demo code to show how new trust evalation model works in paractice

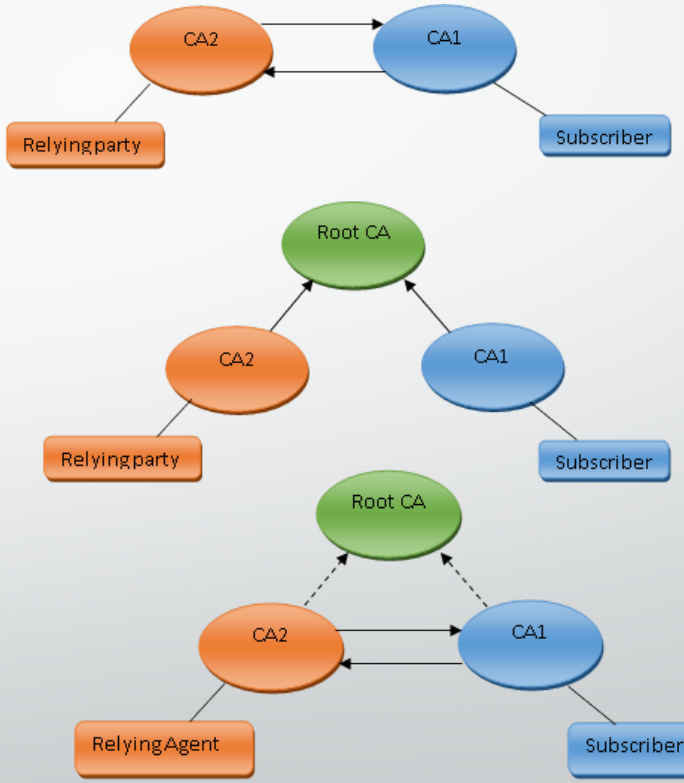
Outlines

- Background and Related Works
- Problem Definition and Contribution
- Cross-Domain VPKI Trust Model
- Design and Modeling
- Performance Evaluation
- Conclusion and Future Works

PKI Trust Models Topology

- Direct Cross Certification
- Hub Certification Authority
- Hub Authentication Authority

Examples: US (FBCA), Canada (CCF), EuroPKI, Japan

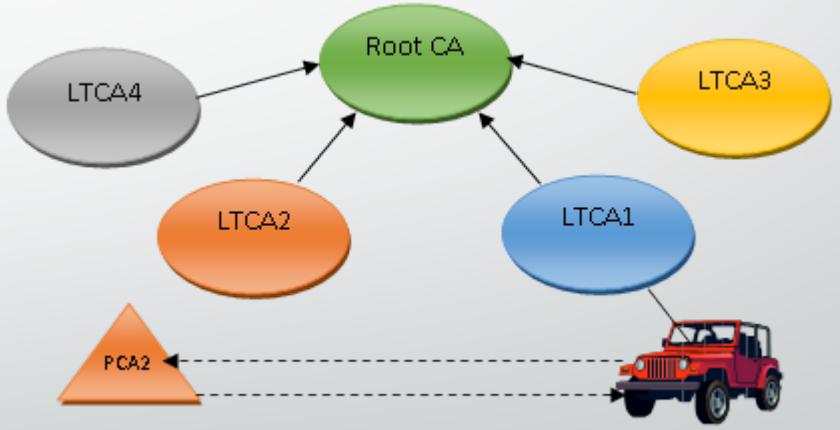


Proposed Topology for Cross-Domain PKI Trust Model

- Hub Certification Authority:
  - Scalability problem with Cross Certification caused by increasing number of VPKI domain
  - Scalability problem with storing large number of Domain CA certificate in HSM
  - Need of Root CA to certify Domains CA certificate which contains Assurance Level

Proposed Trust Evaluation for Certificate

- Security principle of Seperation of Duty
- Sharing the risk of untrusted LTC
- RootCA evalates Security Pactices of VPKI Domain and assign an Assurance Level
- Hosting PCA evaluates Trust Degree of LTC and decide to issue FPC



Assurance Level of Security Practices

- **Certificate Policy**:
  - Specific application public key in certificate
  - Its information appears of certificate (Key usage, Issuer, Subject)
  - Documented by CA with an unique OID
- **Security Practices**:
  - Practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates
  - Subscriber and CA authentication method, technical, physical, procedural and personal security controls
  - Documented by CA as Certification Practices Statement (CPS)

Assurance Level of Security Practices

- Security Practice of VPKI Domain are evaluated including CPS and CP
- Root CA responsibility
- Graded as Assurance Level and embeded in all LTCs of VPKI Domain

Trust Degree of Certificate

- Evaluation of Subscriber Certificate done by PCA of hosting VPKI Domain in Cross Domain VPKI
- Number be researches have be done to evaluated trustworthiness of certificate
- Mingde Zhang evaluation model mathematically formulated results
- …. plus Subject Name of certificate

Criteria	RCA of cross domain VPKI	PCA of FPKID
CA delegate to RA responsibility of identification and authentication process (Not using is RA is an advantage)	x	
Storing subscriber private key (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
Failed experience with certification from same subscriber or its CAs in certificate chain		x
Length of certificate chain (shorter length as an advantage)		x
Number of certificate path for a certificate (more paths is an advantage)	Not Applicable	Not Applicable

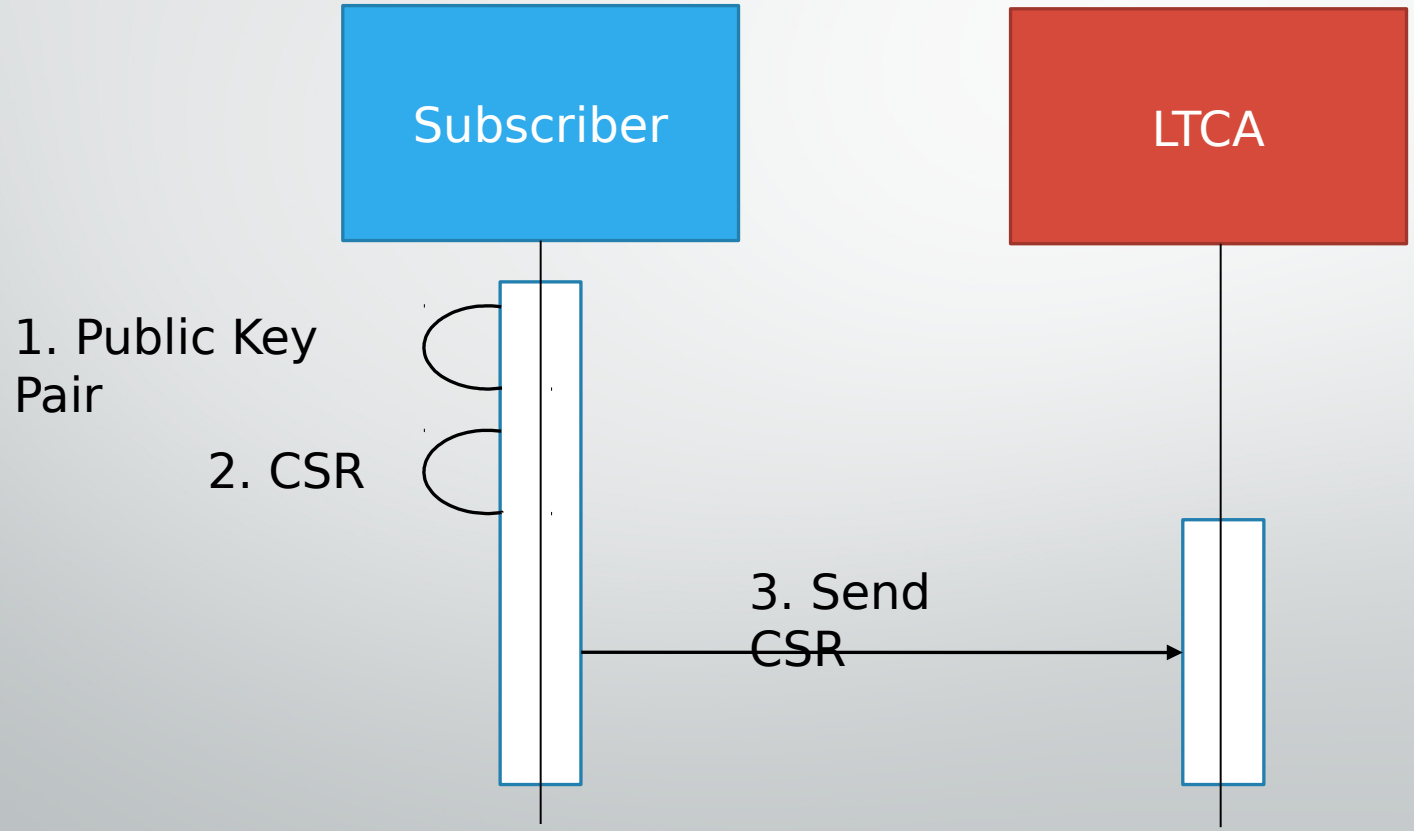
Outlines

- Background and Related Works
- Problem Definition and Contribution
- Cross-Domain VPKI Trust Model
- Design and Modeling
- Performance Evaluation
- Conclusion and Future Works

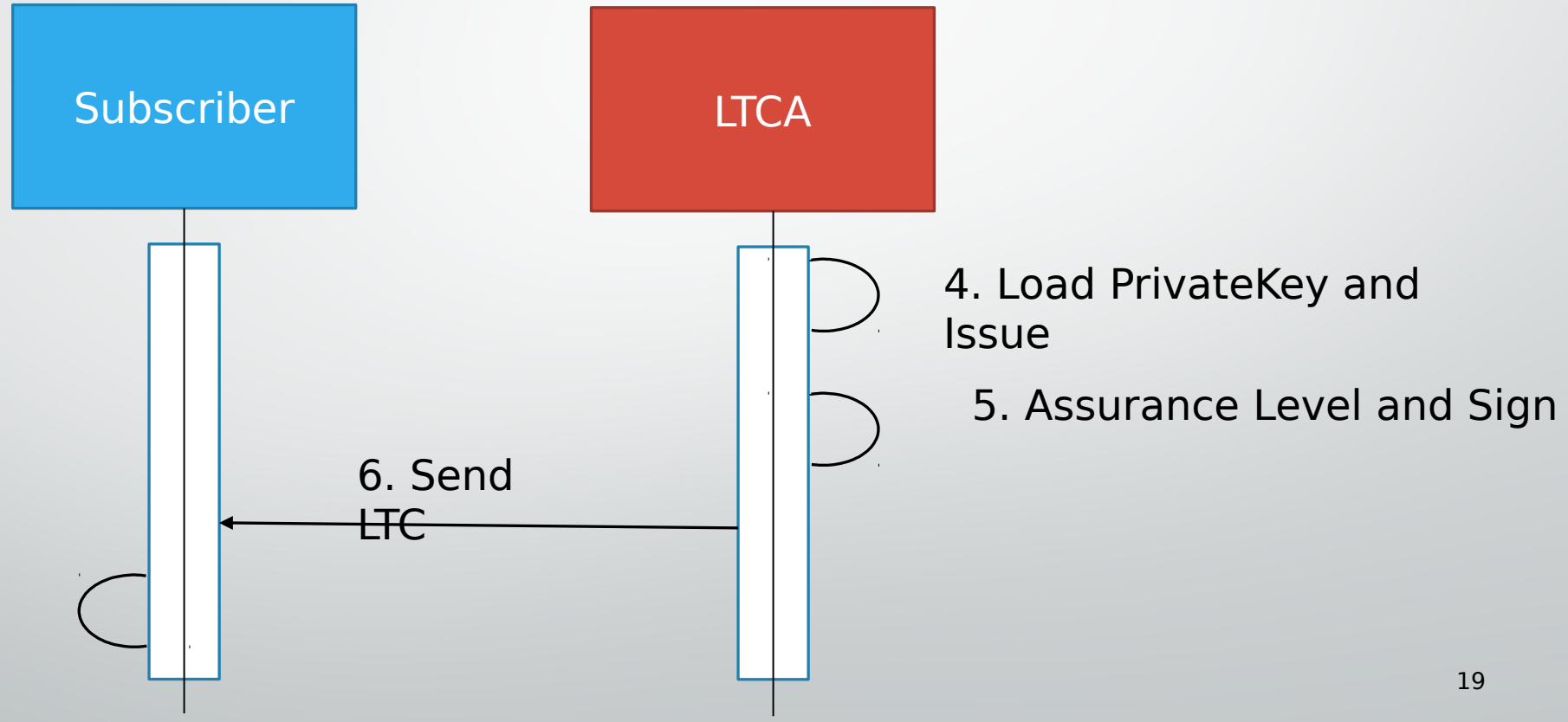
Design and Modeling

- Scope and Considerations:
  - Lack of information about future Cross Domain VPKI environment
  - Proof of concept. Design and implementation of proper CA need more effort.
  - NOT implement all trust degree criteria (Assurance Level, Subject Name in LTC)

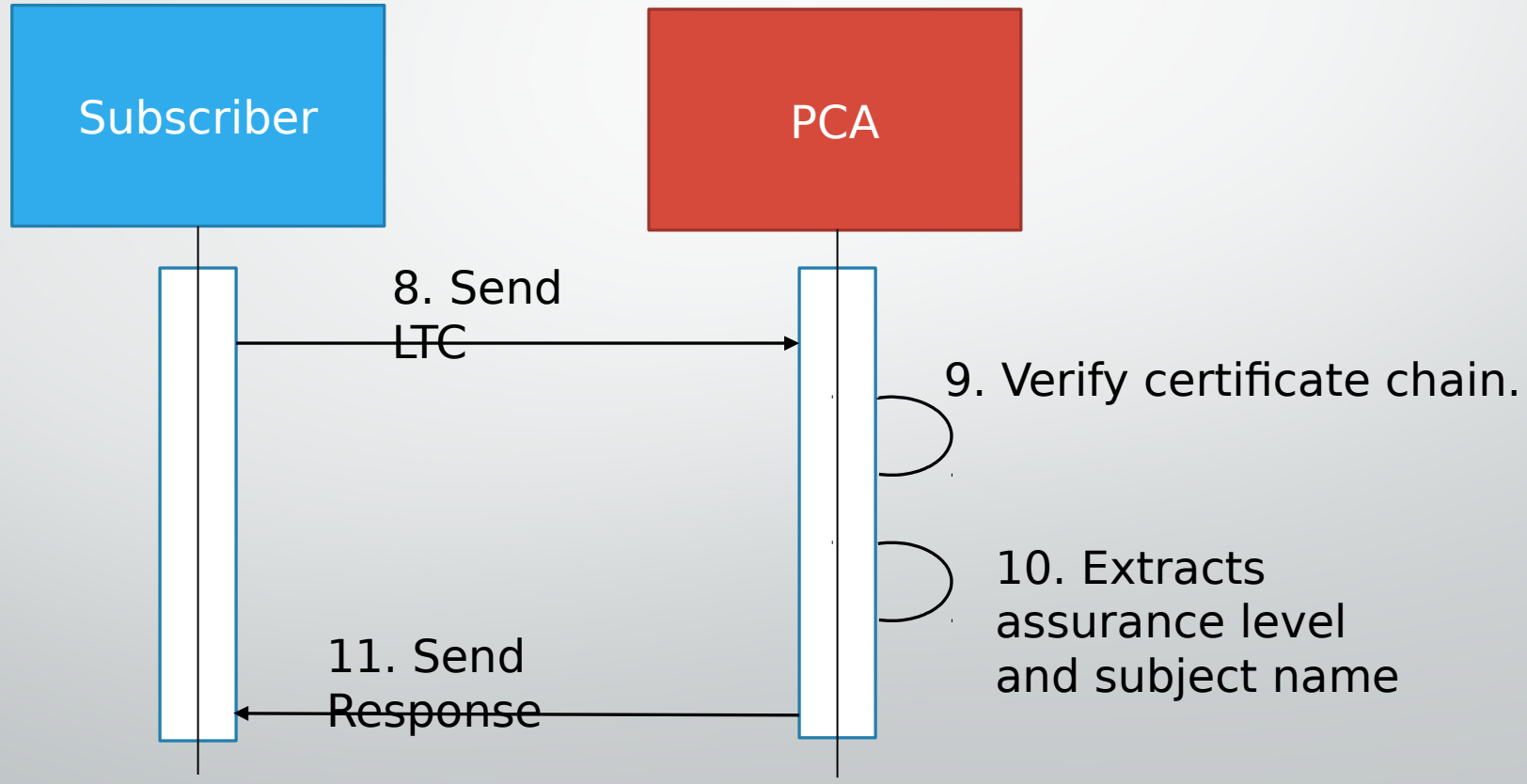
Design and Modeling



Design and Modeling



Design and Modeling



Standards and Protocols

- Elliptic Curve for Public Key Generation (ECDSA prime265v2)
- SHA-256 for signing LTC
- X509v3 (RFC 3280) for LTC creation and validation
- PKSC #10 (RFC 2986) for creating CSR
- OpenSSL v1.0.1e as cryptography library (crypto operations and X509v3)
- XML-RPC as communication protocol
- C++ as programming language (g++ compiler)

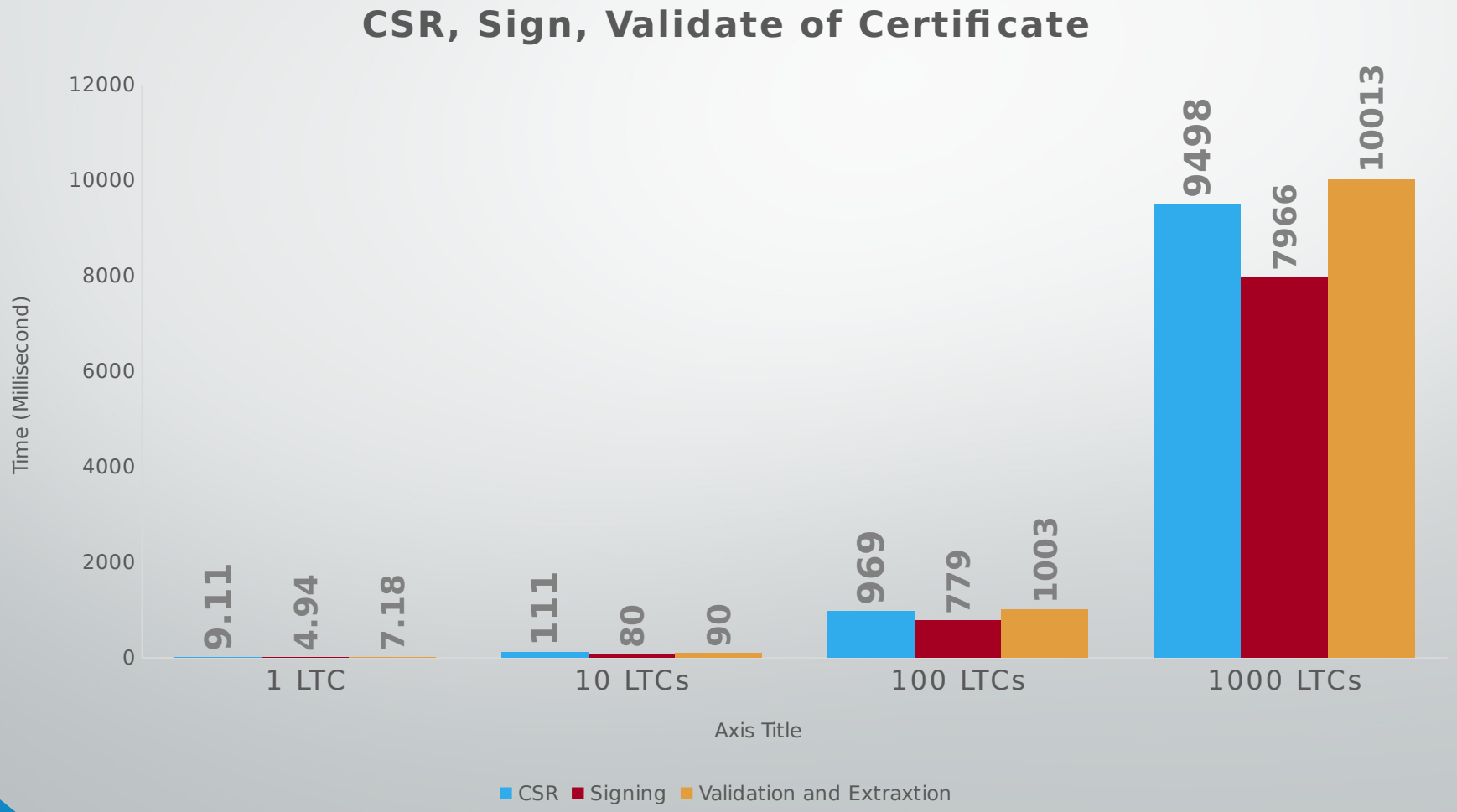
Outlines

- Background and Related Works
- Problem Definition and Contribution
- Cross-Domain VPKI Trust Model
- Design and Modeling
- Performance Evaluation
- Conclusion and Future Works

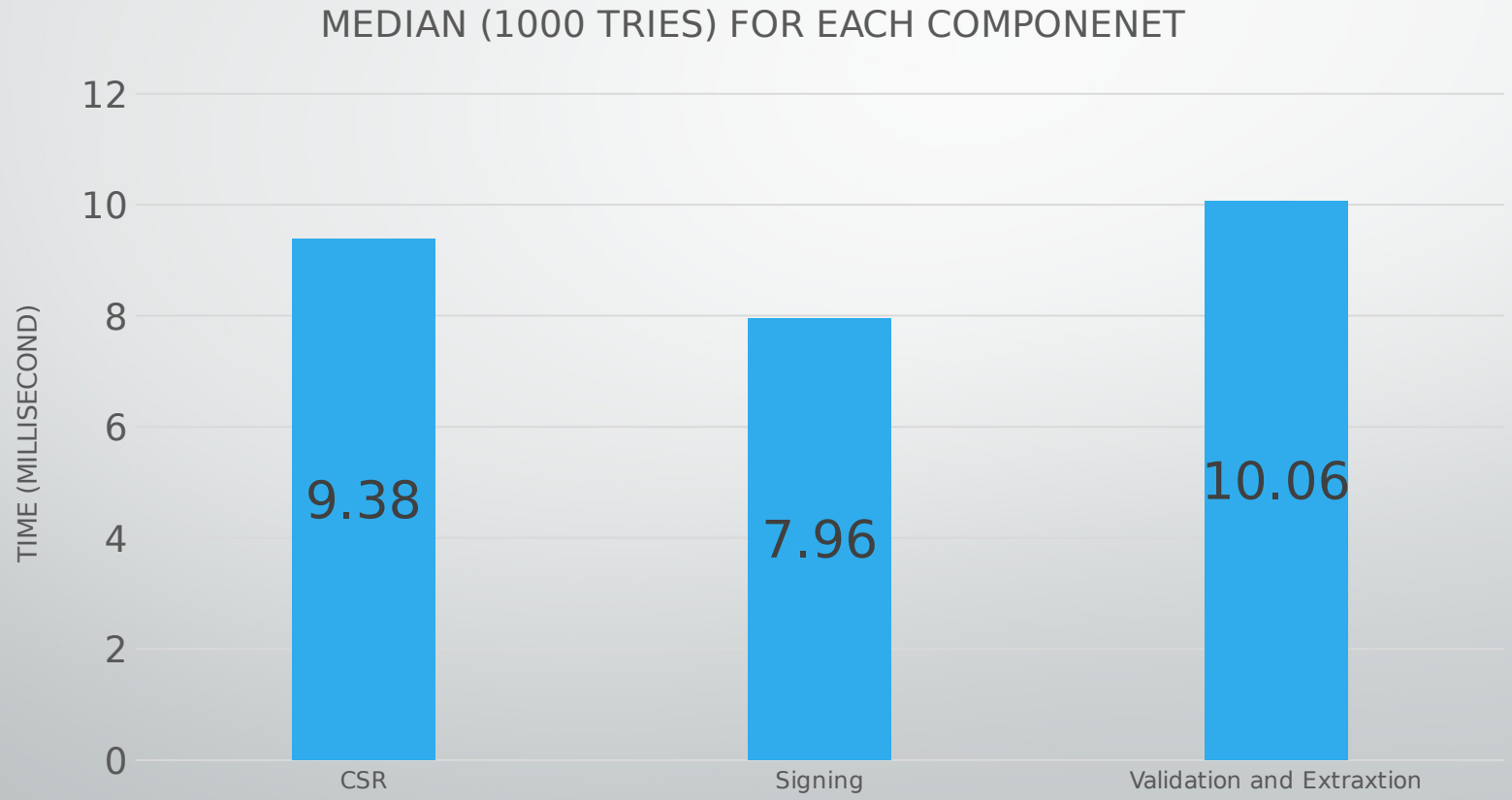
Performance Evaluation

- Virtualized environment using VMWare ESX server
- One linux machine (Subscriber, LTCA, PCA of hosting domain) on virtual LAN: Single Core 2GHz, 1 GB RAM
- Evaluation performance of CSR, Sign, Validation components
  - Average of 1000 times of running earch
  - Summation of 1, 10, 100, 1000 running each

Performance Evaluation



Performance Evaluation



Outlines

- Background and Related Works
- Problem Definition and Contribution
- Cross-Domain VPKI Trust Model
- Design and Modeling
- Performance Evaluation
- Conclusion and Future Works

Conclusion

- Using Cross-Domain PKI trust model , VPKI domains can establish different levels of trust.
- Hosting 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

Future Works

- Framework for evaluating security practice in VPKI domain including CP and CPS analysis which includes defining multiple categories as Assurance Level
- Framework for evaluation of trust degree of LTC specifically.
- Developed software is just a demo. Sophistication and secure LTCA considering functional and non-function requirement

Thanks for your attedtion