



X-Roadと電子署名

電子署名WG春祭り2018
JT2Aリモート署名TFサブリーダー
濱口 総志

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

自己紹介

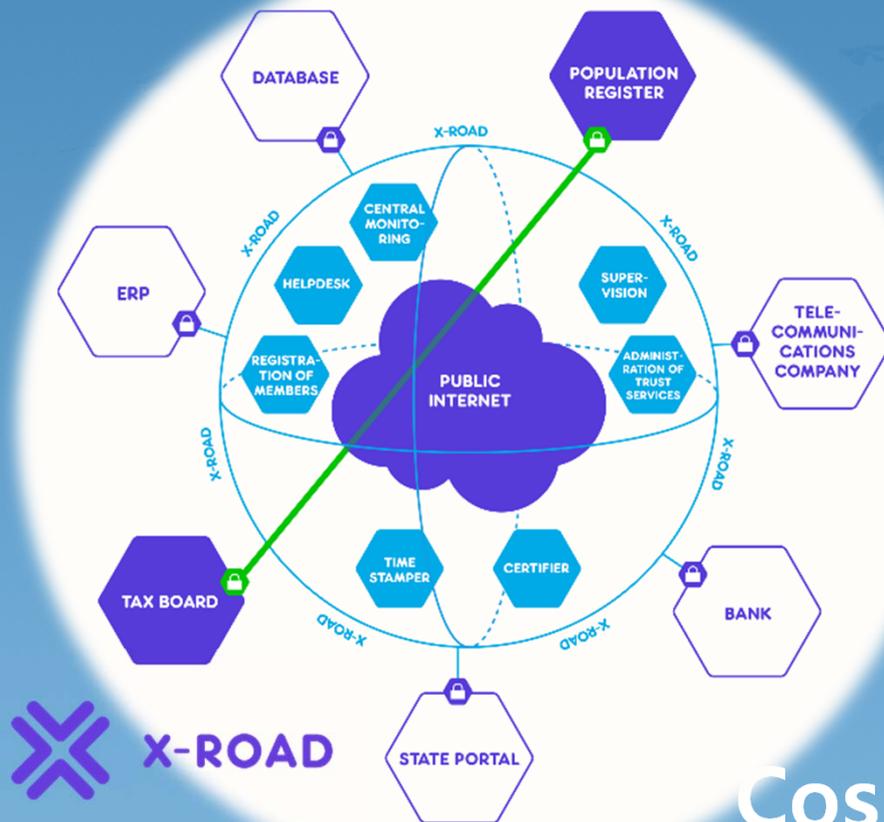
濱口 総志 33歳 三重県伊勢市出身

株式会社コスモス・コーポレイション ITセキュリティ部 責任者
一般財団法人日本情報経済社会推進協会 (JIPDEC) 客員研究員
ISO/IEC JTC1 SC27 WG3 小委員会 委員
NPO 日本ネットワークセキュリティ協会 電子署名WG
タイムビジネス協議会 電子証明基盤WG

Lead Assessor – ETSI TS 102 042, eIDAS
Common Criteria評価者(ドイツ)

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

A long time ago in a galaxy far, far away...



Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

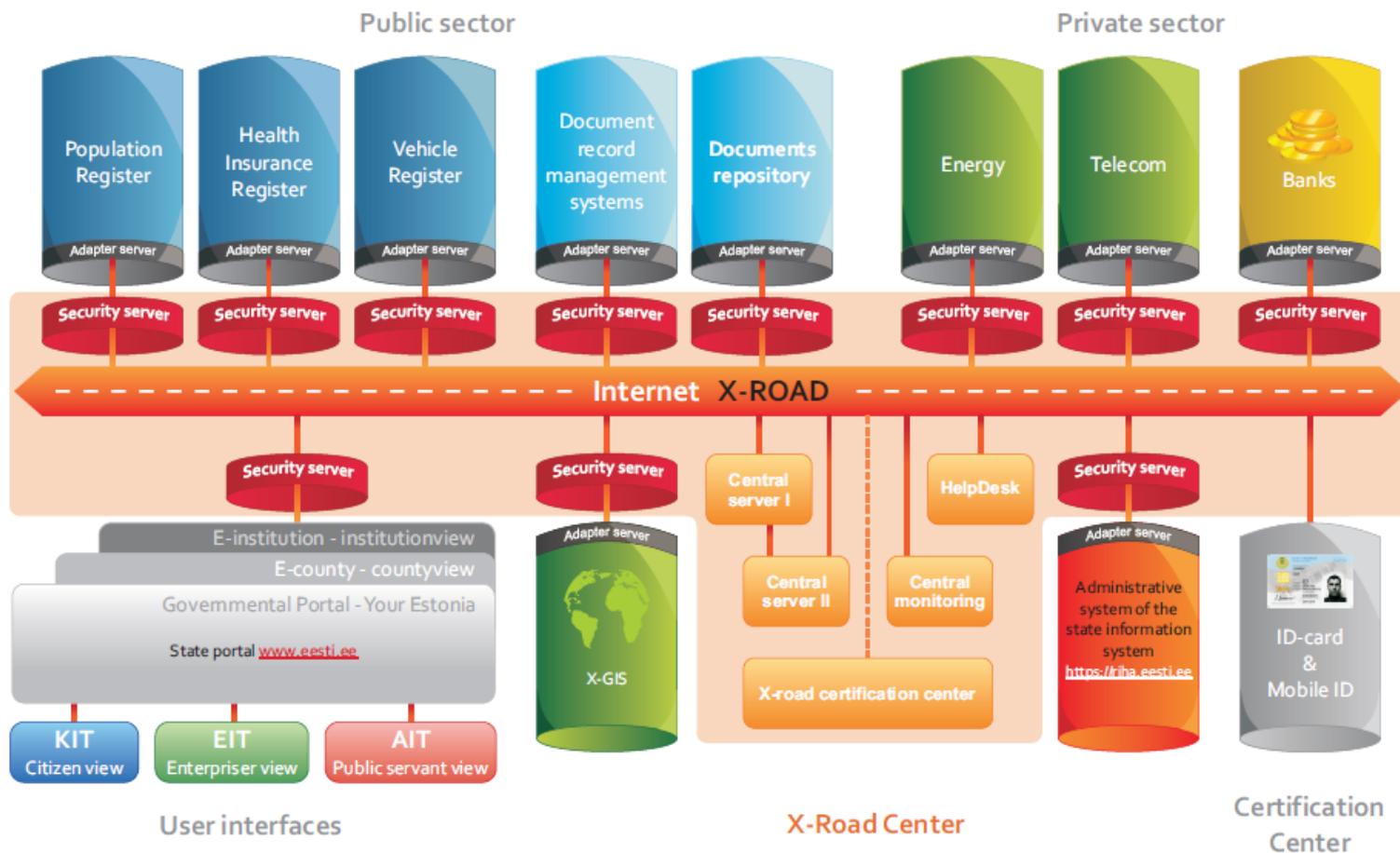
X-Road is;

1. 情報連携基盤
2. 情報システム間のセキュアなデータ交換を実現
3. オープンソース <https://github.com/ria-ee/X-Road>
4. エストニア(X-tee)とフィンランド(Suomi.fi)、キルギスタン(Tunduk)で官民情報連携基盤として採用



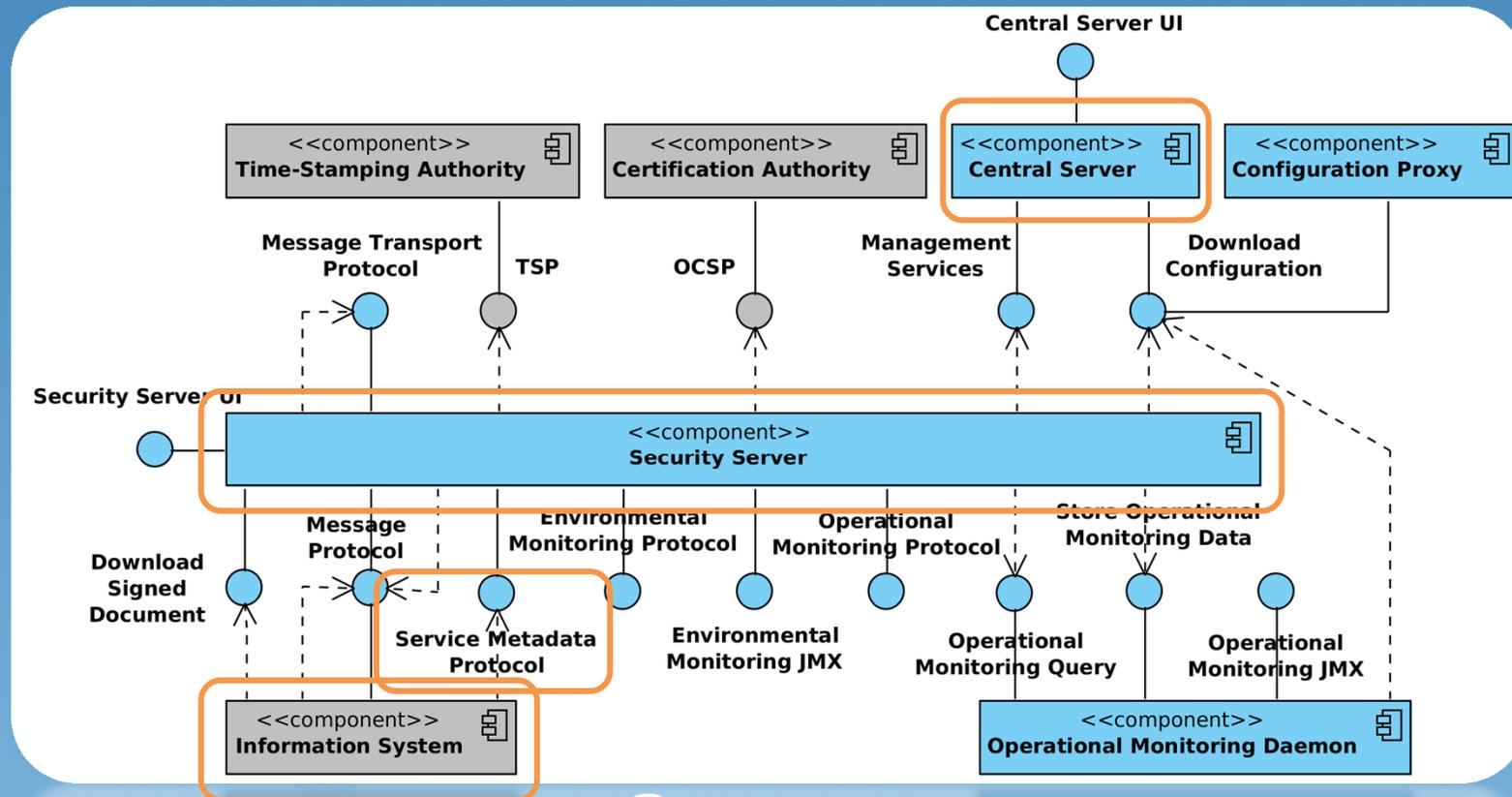
Estonian Informatics Centre

Estonian information system

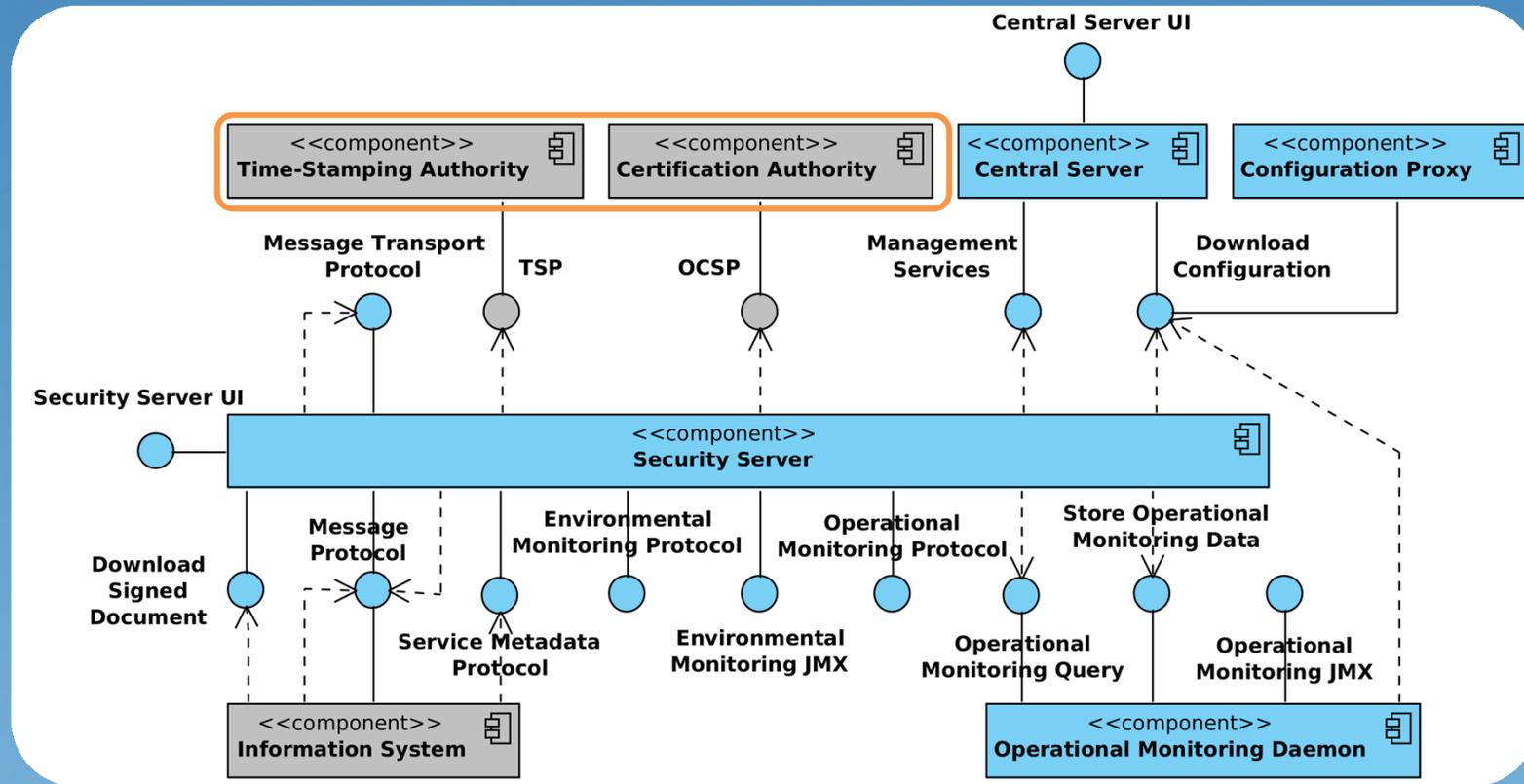


<https://www.x-road.com/>

X-Roadのアーキテクチャ



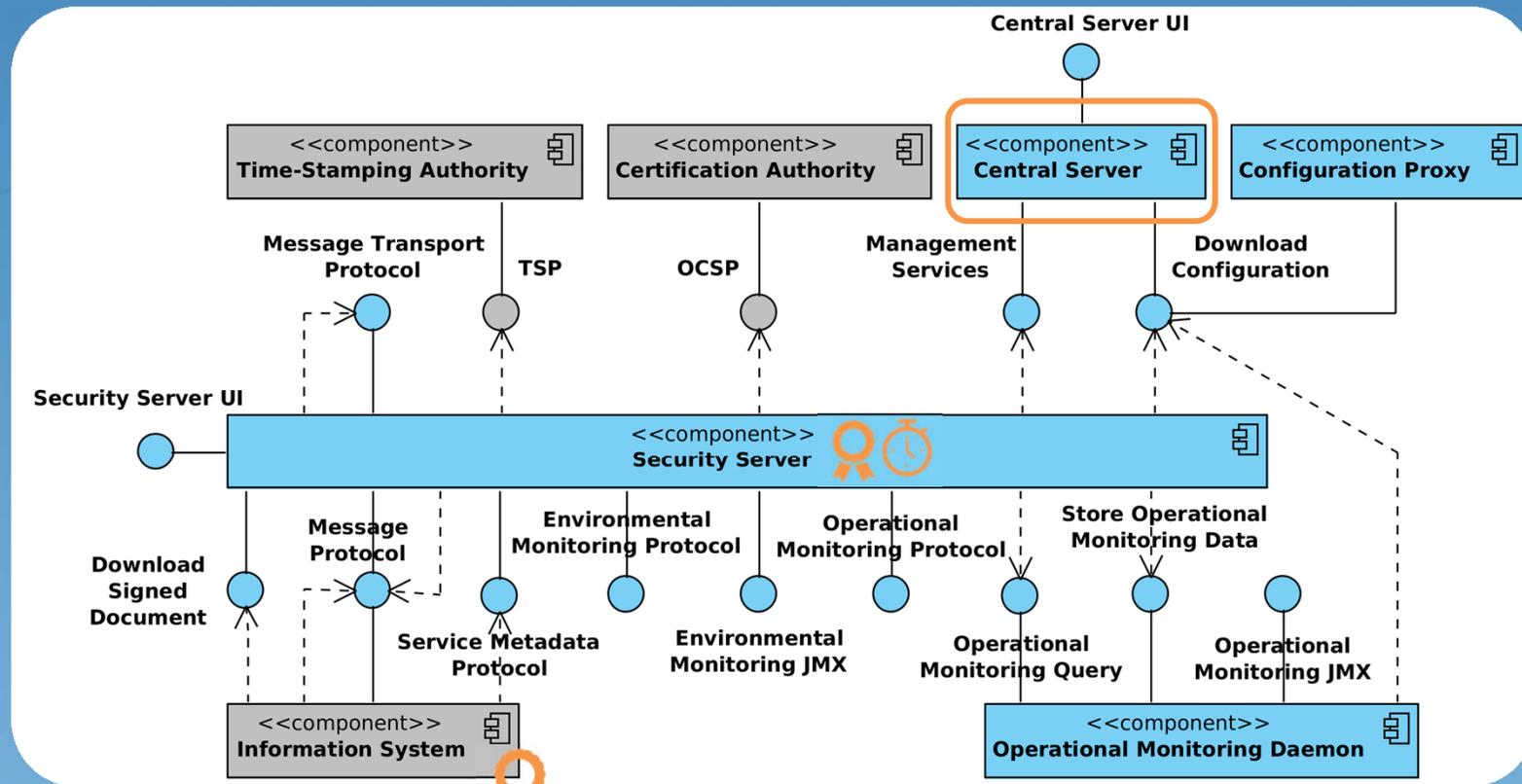
X-Roadのアーキテクチャ



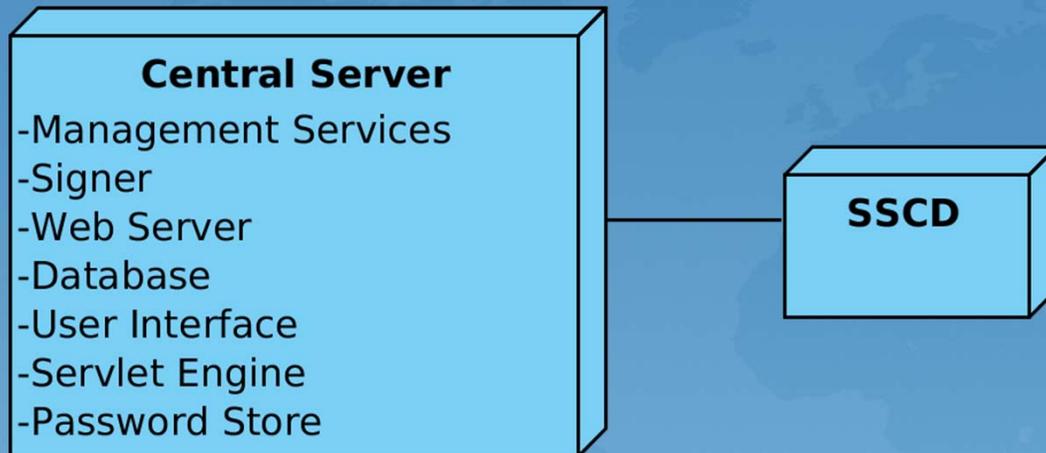
CAとTSA

- CA
 - Qualified Service Provider
 - セキュリティサーバに認証用証明書を発行
 - X-Roadメンバー(情報システム)に署名用証明書を発行
 - 検証サービスの提供(OCSP)
- TSP
 - Qualified Service Provider
 - セキュリティサーバのログにバッチタイムスタンプ(エストニアでは48分毎)

X-Roadのアーキテクチャ



Central server



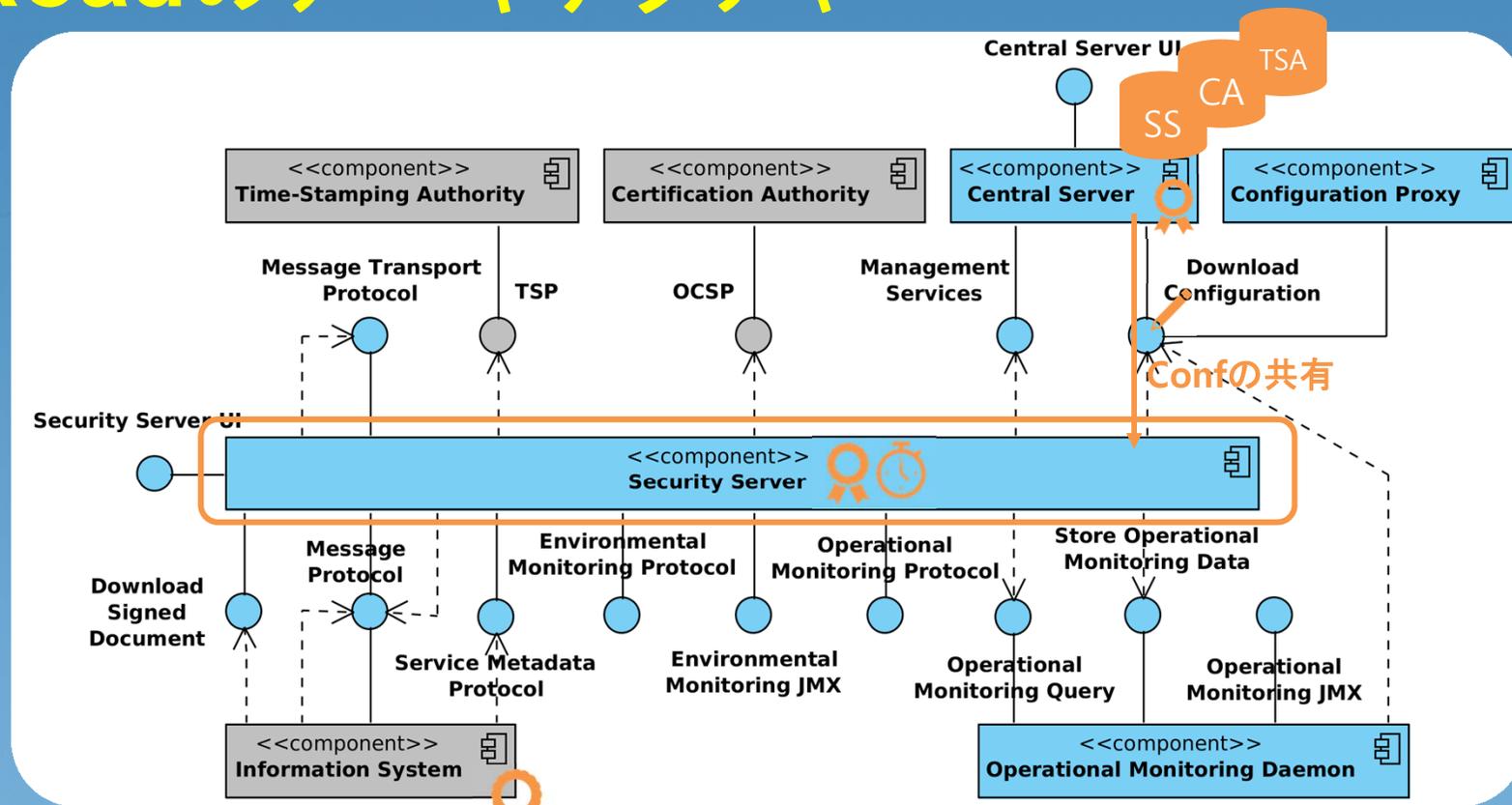
1. X-Roadメンバーとセキュリティサーバのデータベースを管理

- セキュリティサーバリスト
- X-Roadメンバリスト(情報システムのリスト)
- 認証局リスト
- タイムスタンプ局リスト

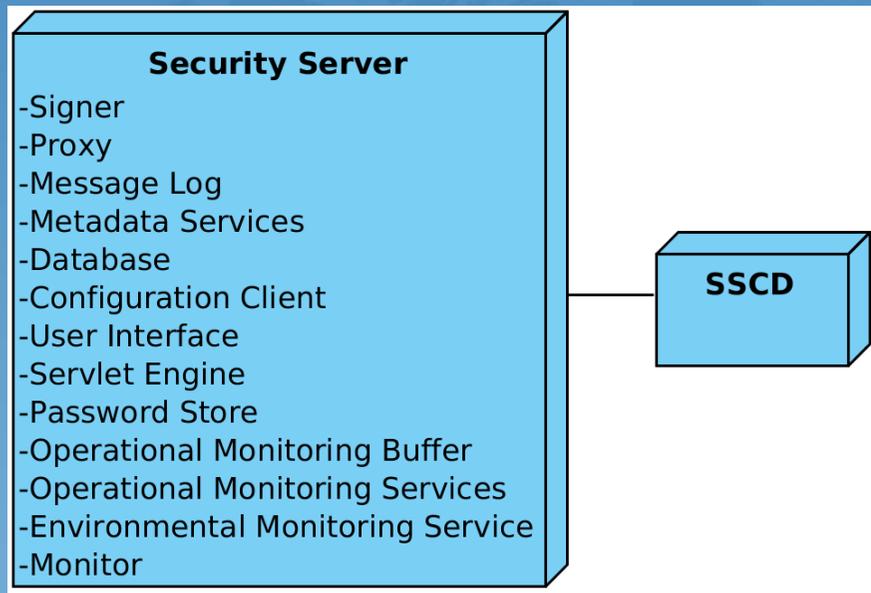
2. 各セキュリティサーバの設定を作成し、各セキュリティサーバに公開

- Confファイルを作成し、セキュリティサーバへ公開(HTTPプロトコル)
- Confファイルへの電子署名(eシール)

X-Roadのアーキテクチャ



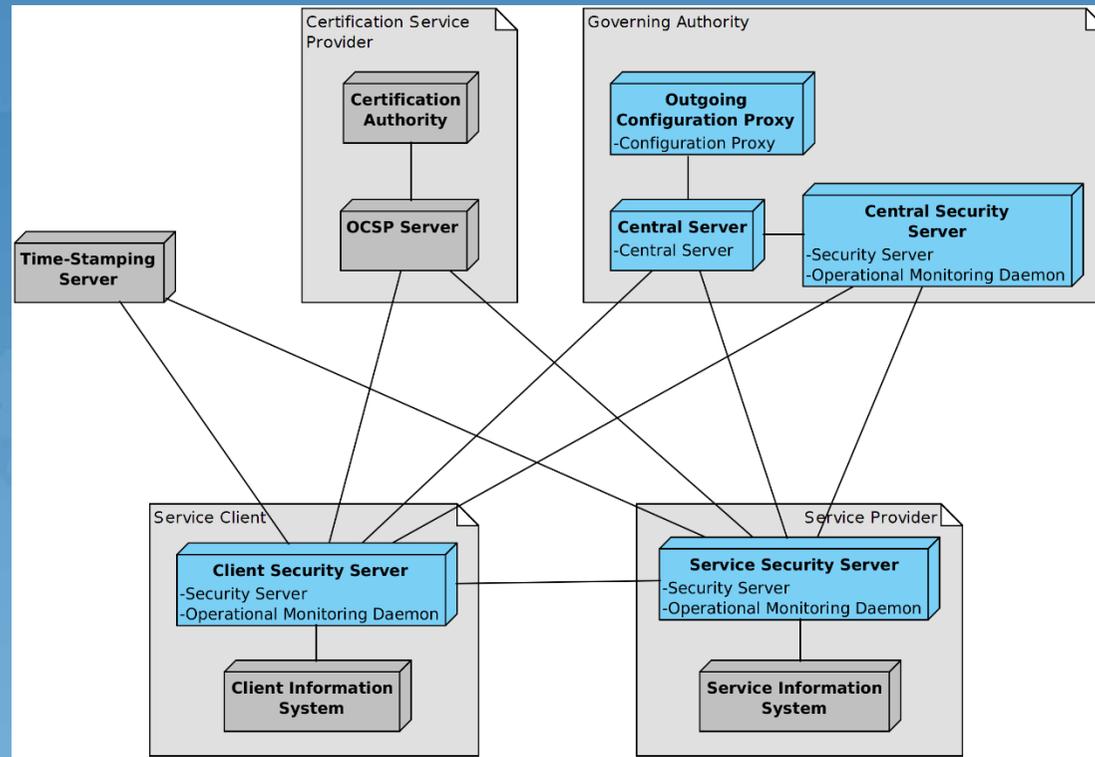
Security Server



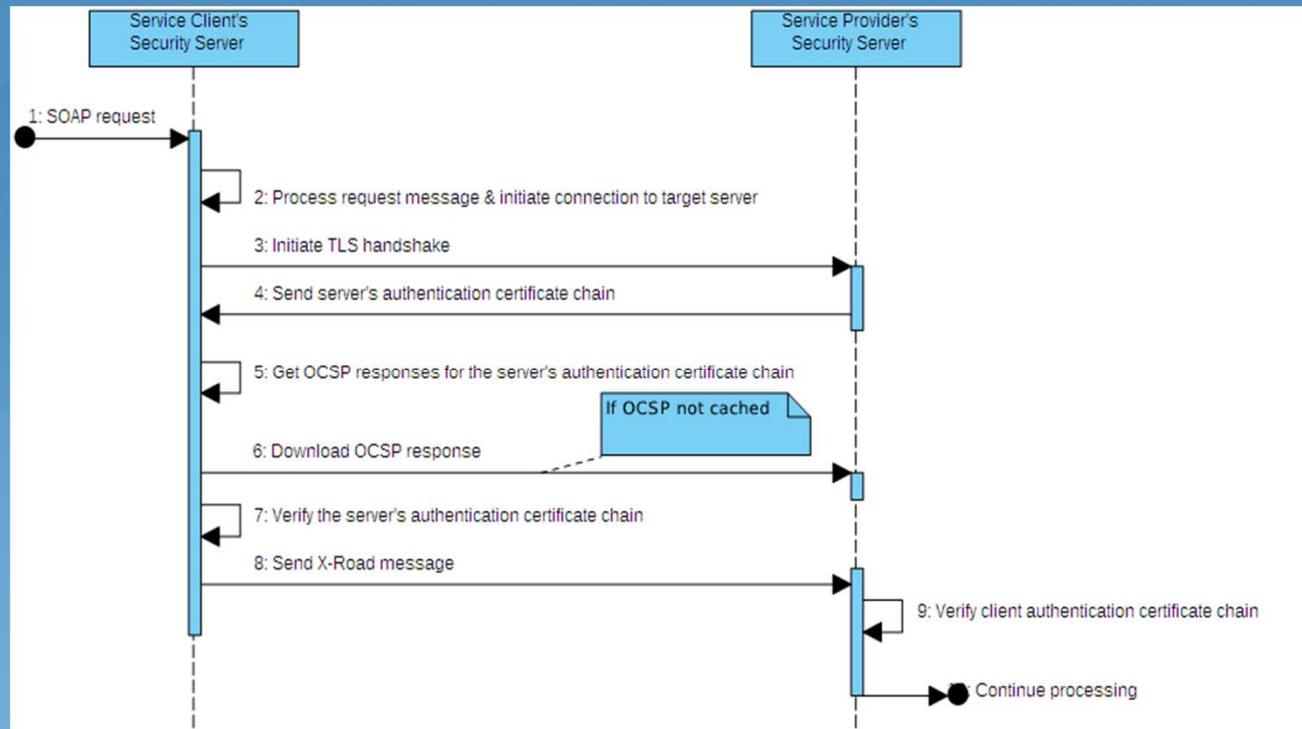
SOAPベースのX-RoadメッセージプロトコルによるSecure Server間の安全なデータ交換を実現

- 署名機能(各送信メッセージに署名)
- タイムスタンプ機能(ログにタイムスタンプ)
- ログ機能
- プロキシ機能(署名と暗号化による他のセキュリティサーバとのセキュアな通信)
- メタデータサービス(他のセキュアサーバに対して、このセキュアサーバがどのようなサービスを提供できるかを開示)
- 監視機能
- Configダウンロード機能(セントラルサーバからの設定ファイルのダウンロード機能)

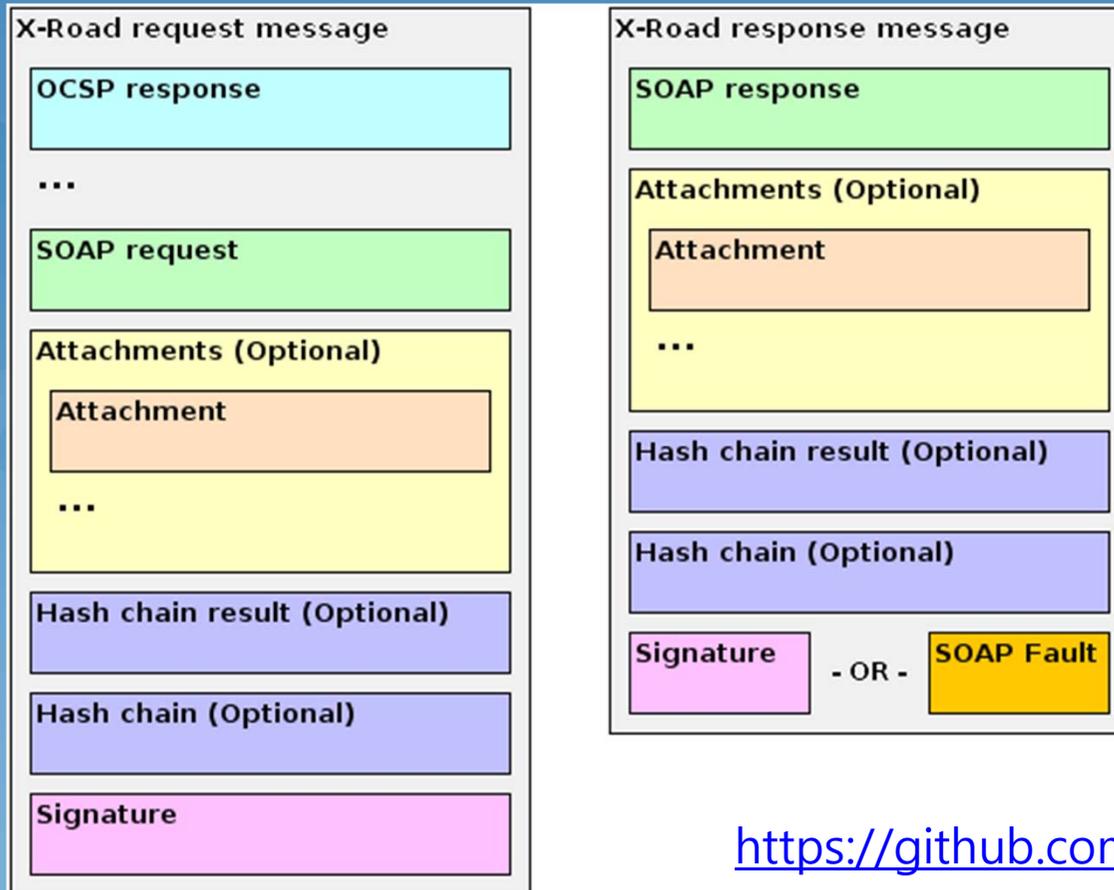
X-Road上での情報交換



TLS認証

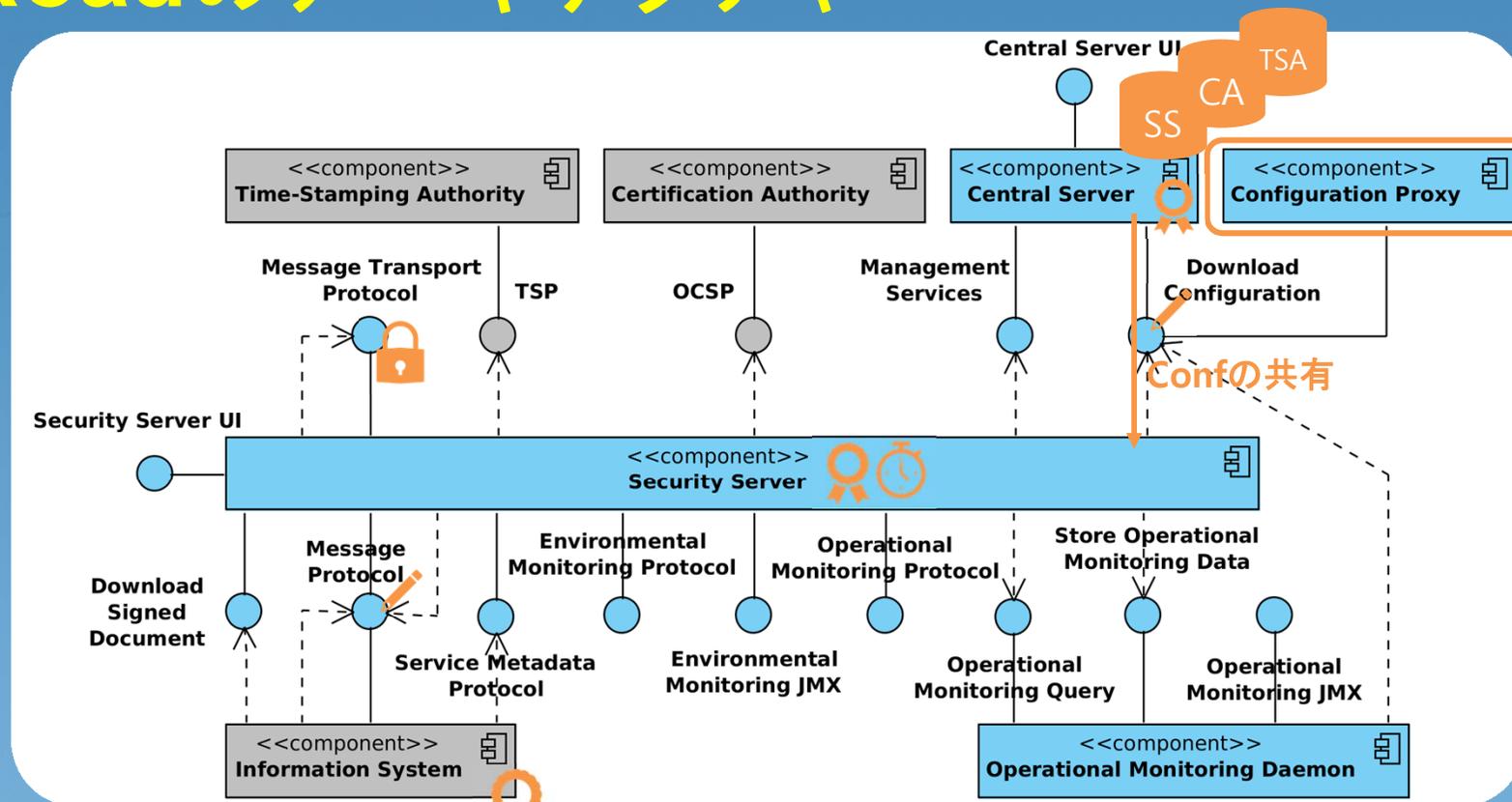


メッセージの構成



<https://github.com/ria-ee/X-Road>

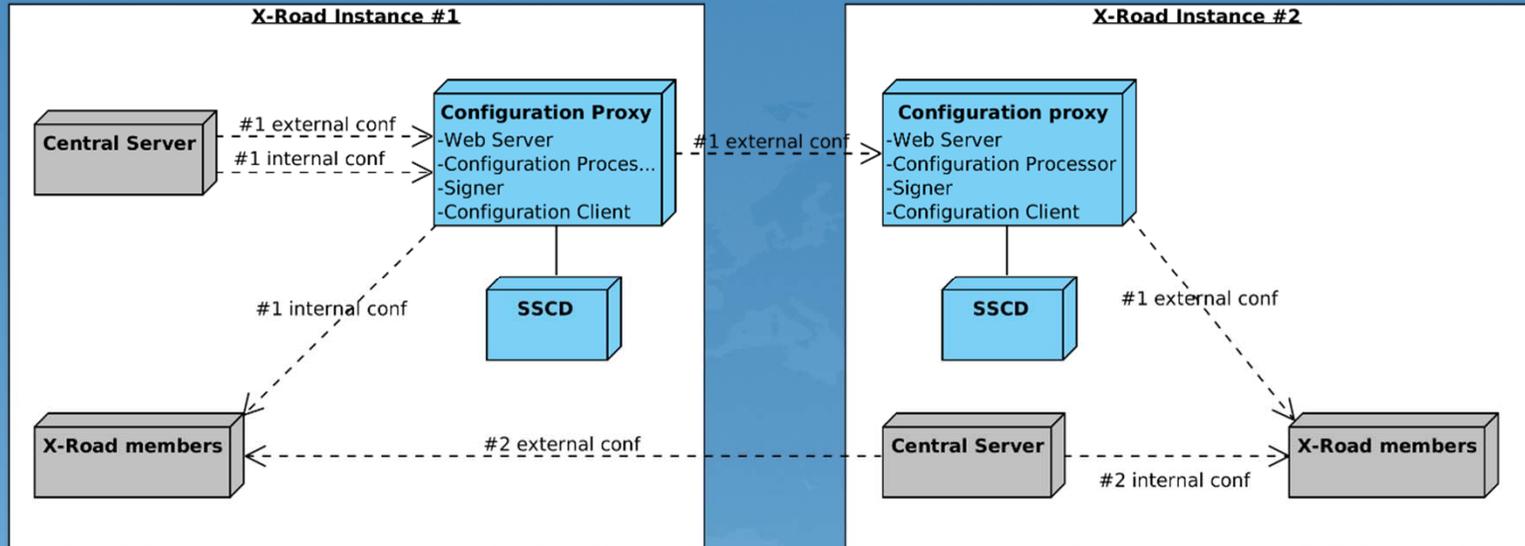
X-Roadのアーキテクチャ



Cosmos <https://github.com/ria-ee/X-Road>

PROFESSIONALS OF SAFETY ENGINEERING

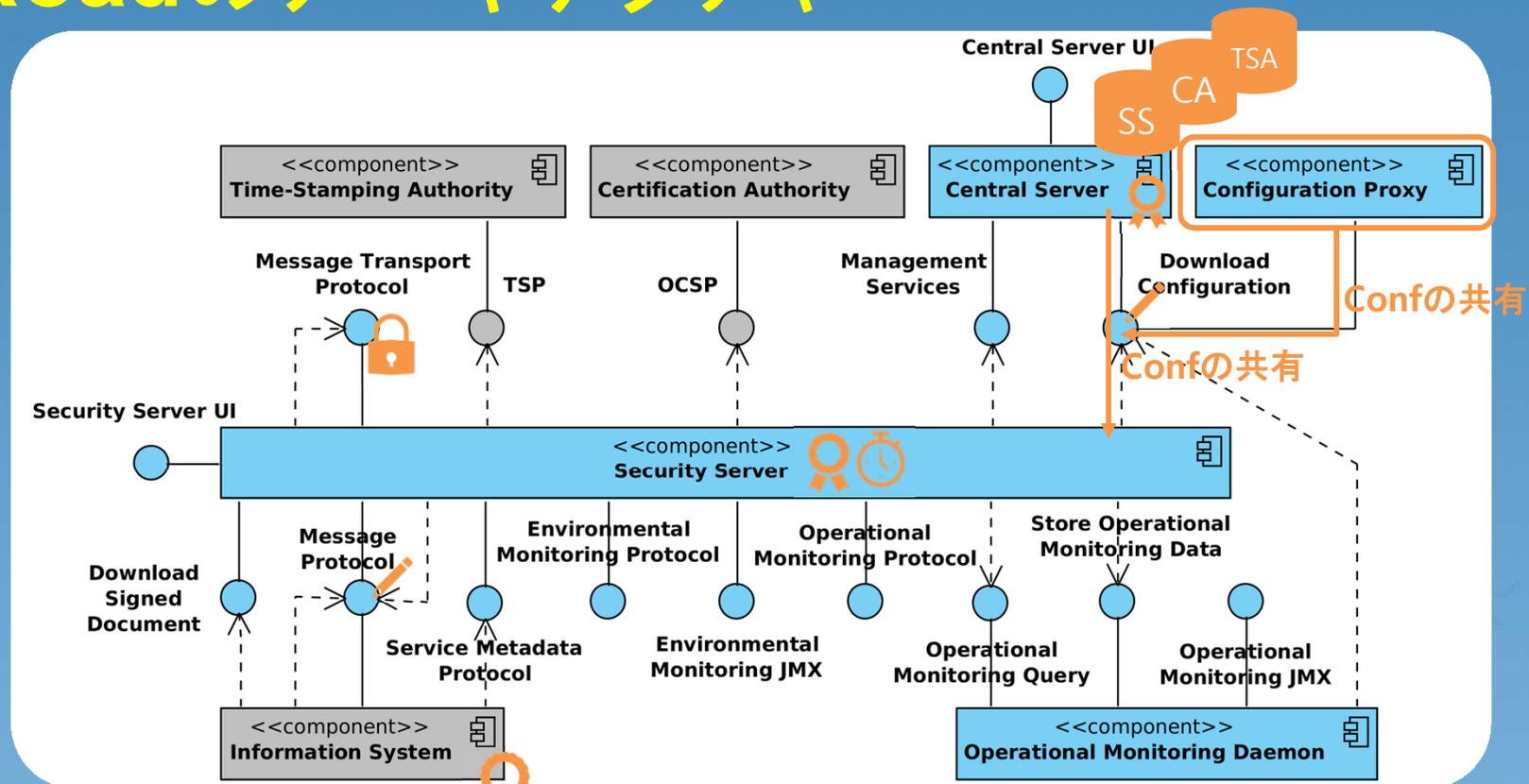
Configuration Proxy



Central ServerからのConfファイルのダウンロードのためのProxy
一分毎にConfファイルをダウンロードし、署名して公開
各セキュリティサーバ内のConfiguration Clientからアクセス可能
X-Road間の設定共有
Central Serverの負荷分散と可用性アップ

Cosmos <https://github.com/ria-ee/X-Road>
PROFESSIONALS OF SAFETY ENGINEERING

X-Roadのアーキテクチャ



Findings

X-Roadを支える仕組み

- Technologies
- 社会基盤

- eID, eIDAS規則、国内法(Regulation No 105 of the Government of the Republic of 23.09.2016)

➔ X-Road上のログは法律的に証拠能力が保証されている

X-Roadはchosen oneか？

- エストニア; 人口130万人、eIDカードの問題、電子投票における問題

- X-Road自体の問題はまだ報告されていない

Estonia freezes resident ID cards due to security flaw

The flaw makes Estonians vulnerable to identity theft.

4 Comments 955 Views



Estonia's residents use their mandatory national ID to access pretty much anything, from online banking to online voting. So, it was a huge blow to the program when experts found a security flaw in the chip the ID used that makes it possible for bad players to impersonate and steal the identities of all 760,000 affected individuals. That might not sound like a huge number, but that's half the small country's population. Now, the country has blocked most of its residents from accessing all its online services for a weekend, so it can go in and fix the vulnerability. All ID cards issued from October 2014 to October 2016, 2017 will be frozen.

Verified Voting Blog: Report on the Estonian Internet Voting System

Sep 3 2011 - Barbara Simons

I visited Estonia in mid-July of this year at the invitation of Edgar Savisaar, the country's first prime minister and current mayor of Tallinn. Mr. Savisaar is the leader of the Centre Party, which placed second in recent national elections. The Centre Party and Mr. Savisaar have been questioning the outcome of the Internet voting portion of those elections. They invited me to Estonia because of a presentation I made at a European Parliament panel on the risks of Internet voting.

I told my hosts that I was happy to discuss the risks of Internet voting, but I would not comment on internal Estonian politics. When asked whether or not I thought the national election was rigged, I refused to comment, aside from saying that no one could prove that it was or was not rigged, because there is no way to conduct a recount of an Internet election.

The Internet portion of the 2011 election lasted from February 24 to March 2, with paper balloting conducted on March 6. The Internet vote was counted the evening of March 6. Estonian law allows complaints to be submitted only during the 3 days immediately following the procedure being challenged. Since Internet voting is considered separate from paper voting, the final day for submitting complaints about Internet voting was March 5. Graduate student Paavo Pihelgas was the only person who submitted a complaint by the deadline. (The Centre Party and independent candidates tried to file complaints, but they did not do so within the required 72 hour time frame).

Pihelgas asked the National Election Commission (NEC) to cancel the election results, since the possibility of election-rigging malware meant that there was no way to be sure that the voters' preferences had been correctly recorded. NEC rejected his complaint the following day, saying that they have all the necessary provisions to detect such cases, without specifying what those provisions are. When Pihelgas resubmitted his complaint, it was forwarded to the Supreme Court. The Supreme Court dismissed the complaint on March 21, say that the voter can file a complaint only when his/her rights have been breached.

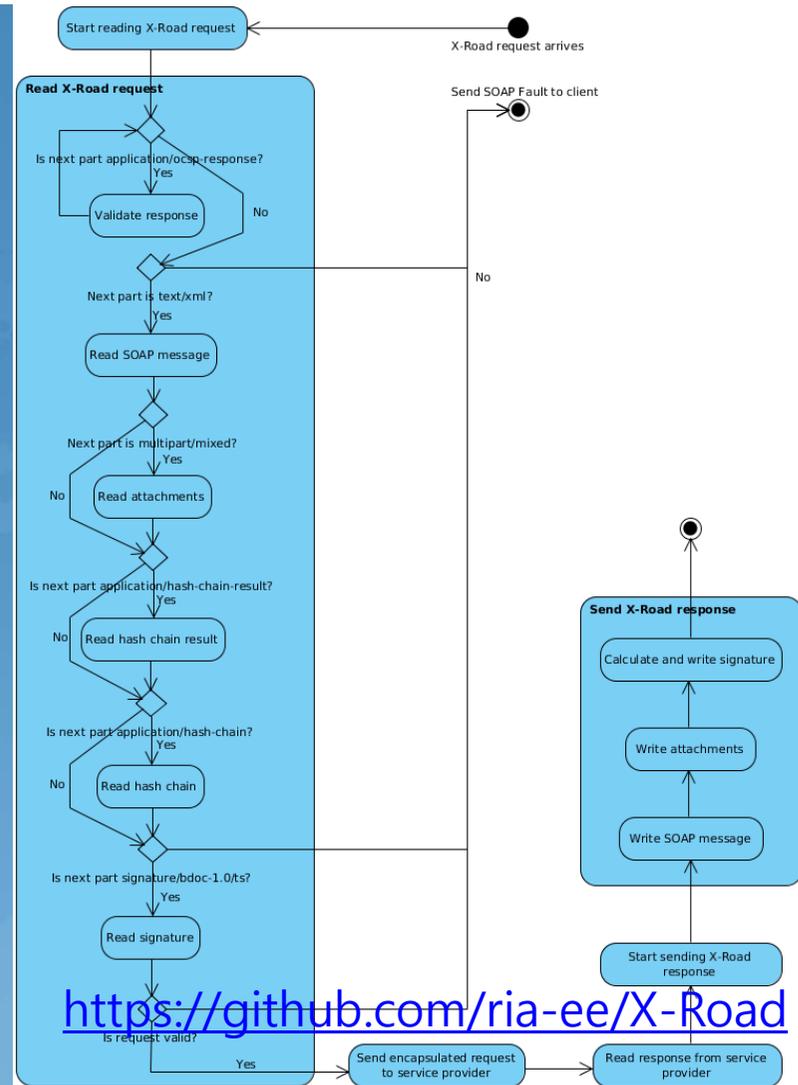
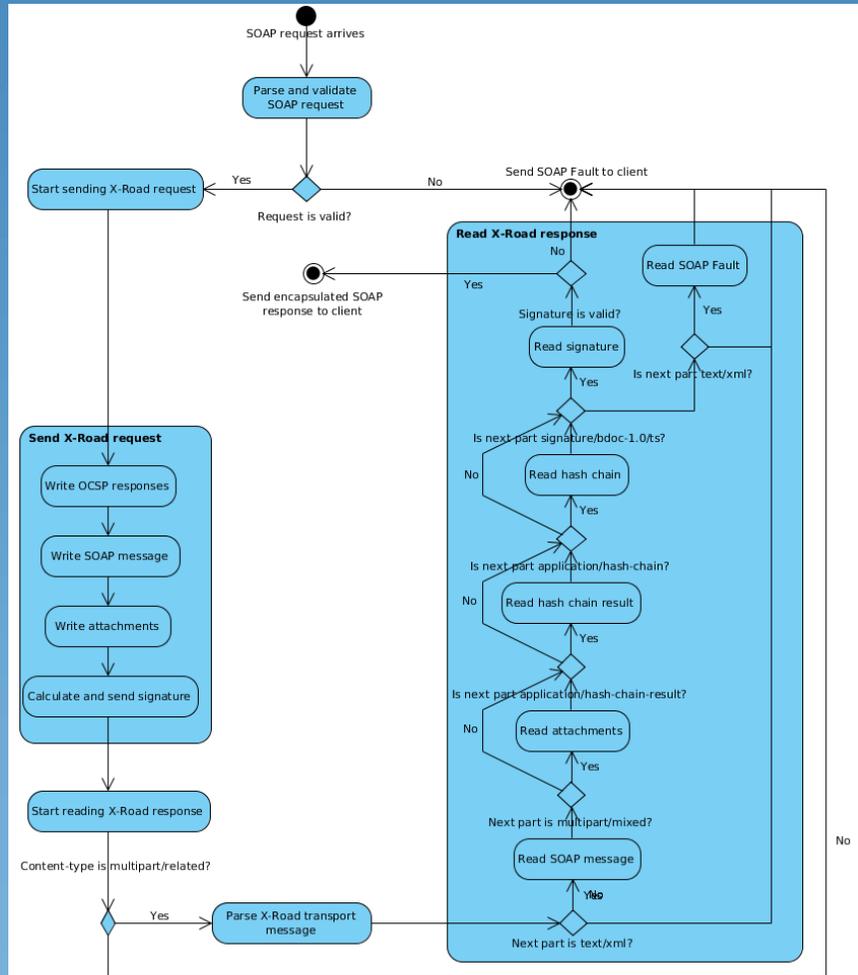
I have communicated with several Estonians before, during, and after my trip. I have also read a report written by a team from the OSCE/ODHR (Organization for Security and Cooperation in Europe/Office for Democratic Institutions and Human Rights) who observed the March 2011 election, and I have talked with a member of the OSCE/ODHR team. Based on the information I have obtained, I have concluded that the Internet voting system used in Estonia is insecure.

1. There are a number of serious problems, as described by the OSCE/ODHR report;
2. The voters' privacy (secret ballot) is vulnerable;
3. The voters' computers are vulnerable to election rigging malware;
4. There is an insider threat;
5. The server is vulnerable to attack from anyone/anywhere;
6. The system is not open or transparent;

Get the power of next-generation verification.

SECURITY ENGINEERING







Central Server Technologies

Technology	Signer	Web Server	Password Storage	Management Services	Database	User Interface	Servlet Engine
Java 8	X			X		X	X
C			X				
Logback	X			X		X	
Akka 2.X	X			X		X	
Jetty 9							X
JRuby 1.7						X	
Javascript						X	
PostgreSQL 9.3					X		
PostgreSQL 9.4					X ^[1]		
nginx		X					
PAM							X
Liquibase					X		
upstart	X	X					X
PKCS #11	X						

Security Server Technologies

Technology	Signer	Proxy	Password Store	Message Log	Metadata Services	Database	Configuration Client	User Interface	Servlet Engine	Monitor	Environmental Monitoring Service	Operational Monitoring Buffer	Operational Monitoring Services
Java 8	X	X		X	X		X	X	X	X	X	X	X
C			X										
Logback	X	X		X	X		X	X			X	X	X
Akka 2.X	X	X		X				X		X	X	X	
Jetty 9									X				
JRuby 1.7								X					
Javascript								X					
PostgreSQL 9.3						X							
PAM									X				
Liquibase						X							
upstart	X	X					X		X				
PKCS #11	X												
Dropwizard Metrics										X			

Operational Monitoring Technologies

Technology	Op. Mon. Daemon Main	Op. Mon. Database	Op. Mon. Service	Configuration Client
Java 8	X	X	X	X
Logback	X	X	X	X
Akka 2.X	X	X		
PostgreSQL 9.3	X	X		
Liquibase	X	X		
Dropwizard Metrics	X	X		
upstart	X			X

Configuration Proxy Technologies

Technology	Web Server	Configuration Processor	Signer	Configuration Client
Java 8		X	X	X
Logback		X	X	X
Akka 2.X		X	X	
nginx	X			
upstart	X	X	X	X
PKCS #11			X	