# 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
POFESSIONALS OF SAFETY ENGINEERING

# 自己紹介

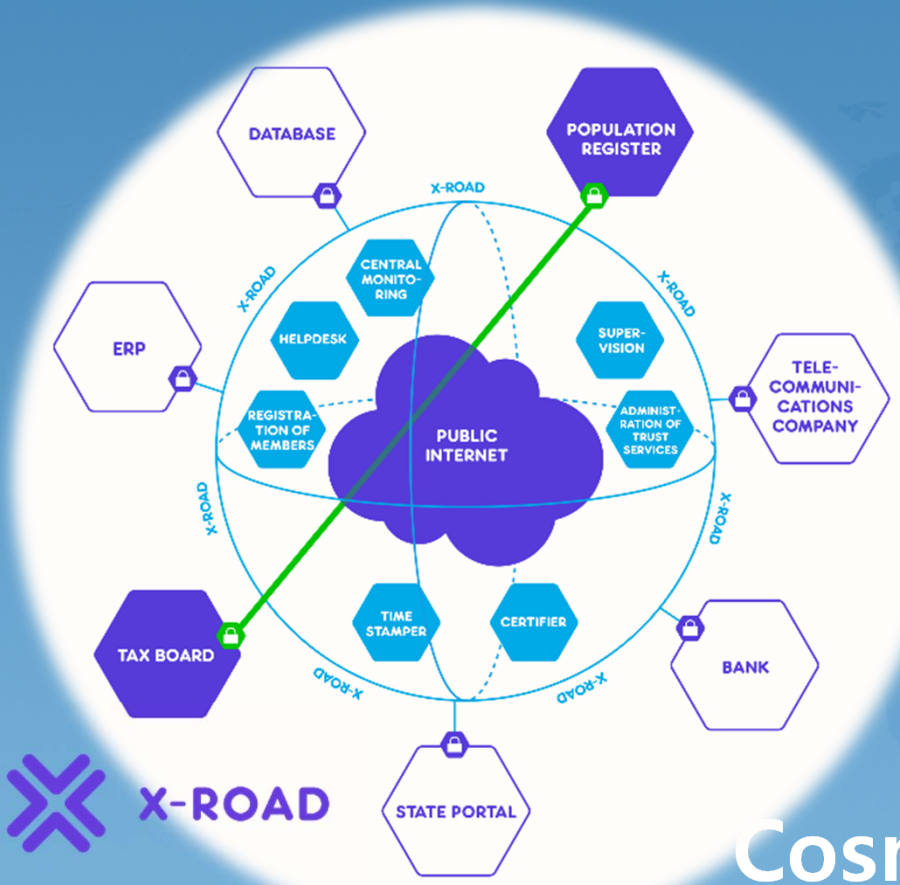
濱口　総志　33歳　三重県伊勢市出身

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
POFESSIONALS OF SAFETY ENGINEERING

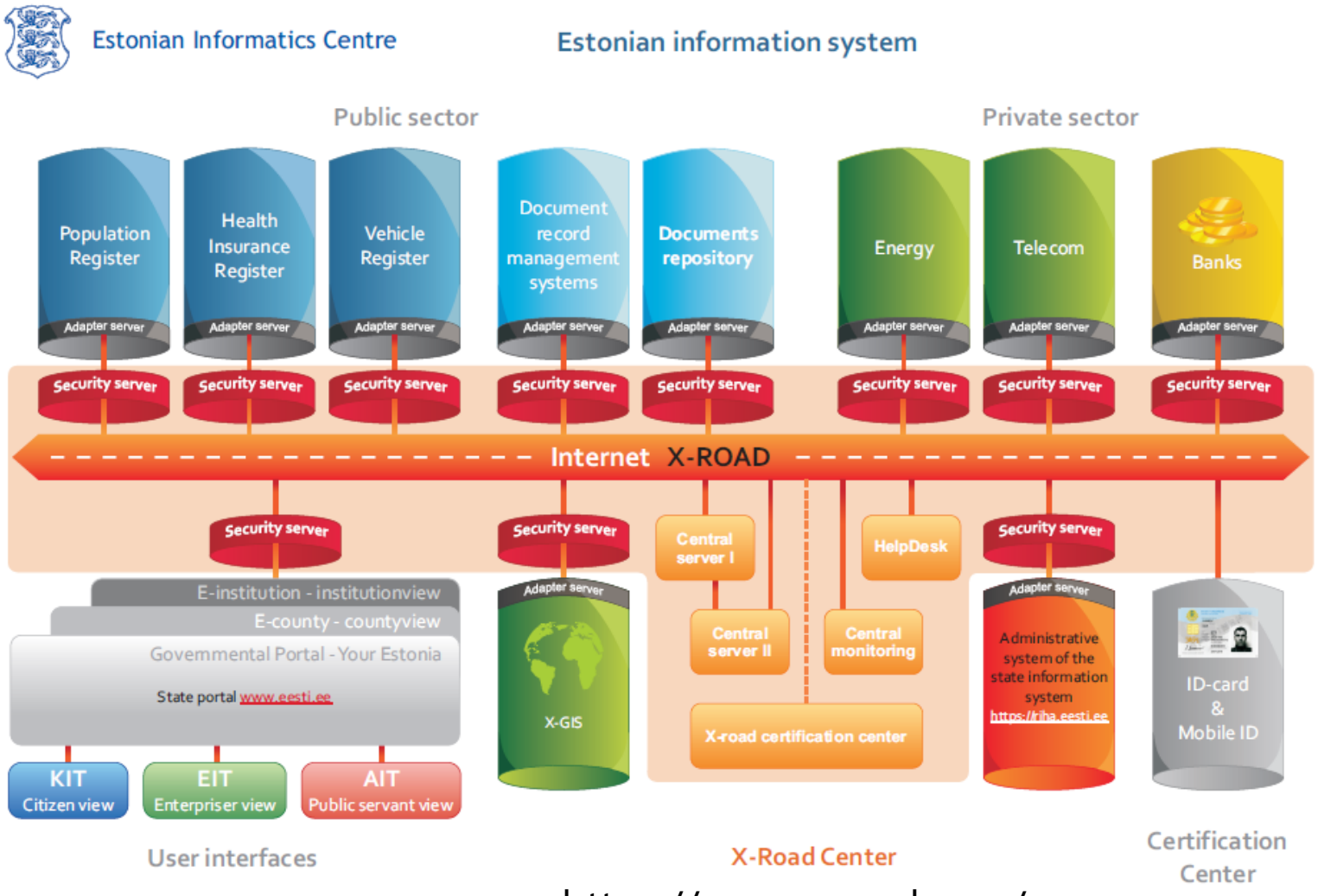
# A long time ago in a galaxy far, far away…




X-Road is;

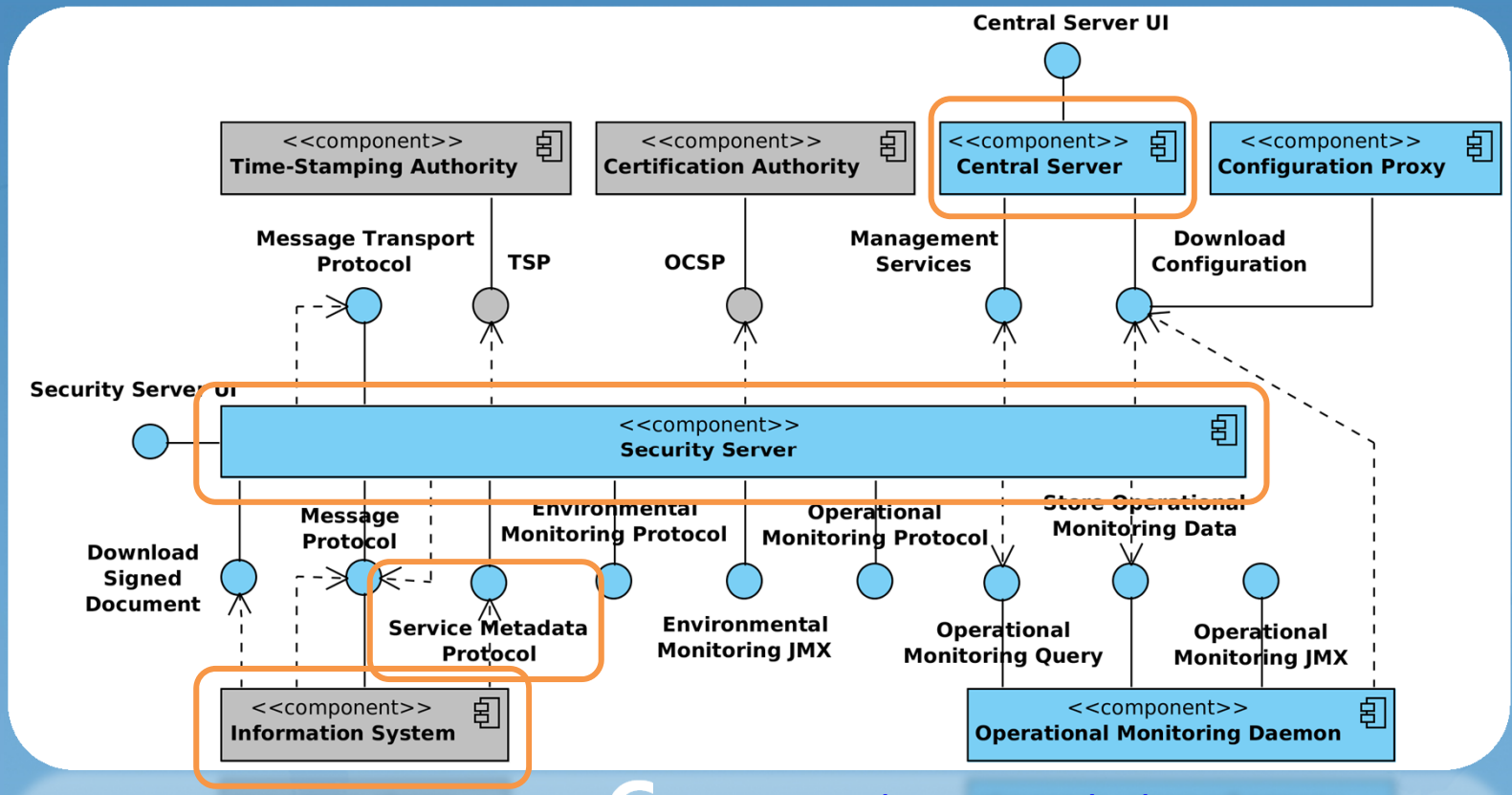
1. 情報連携基盤
2. 情報システム間のセキュアなデータ交換を実現
3. オープンソース https://github.com/ria-ee/X-Road
4. エストニア(X-tee)とフィンランド(Suomi.fi)、キルギスタン（Tunduk）で官民情報連携基盤として採用

Cosmos
POFESSIONALS OF SAFETY ENGINEERING



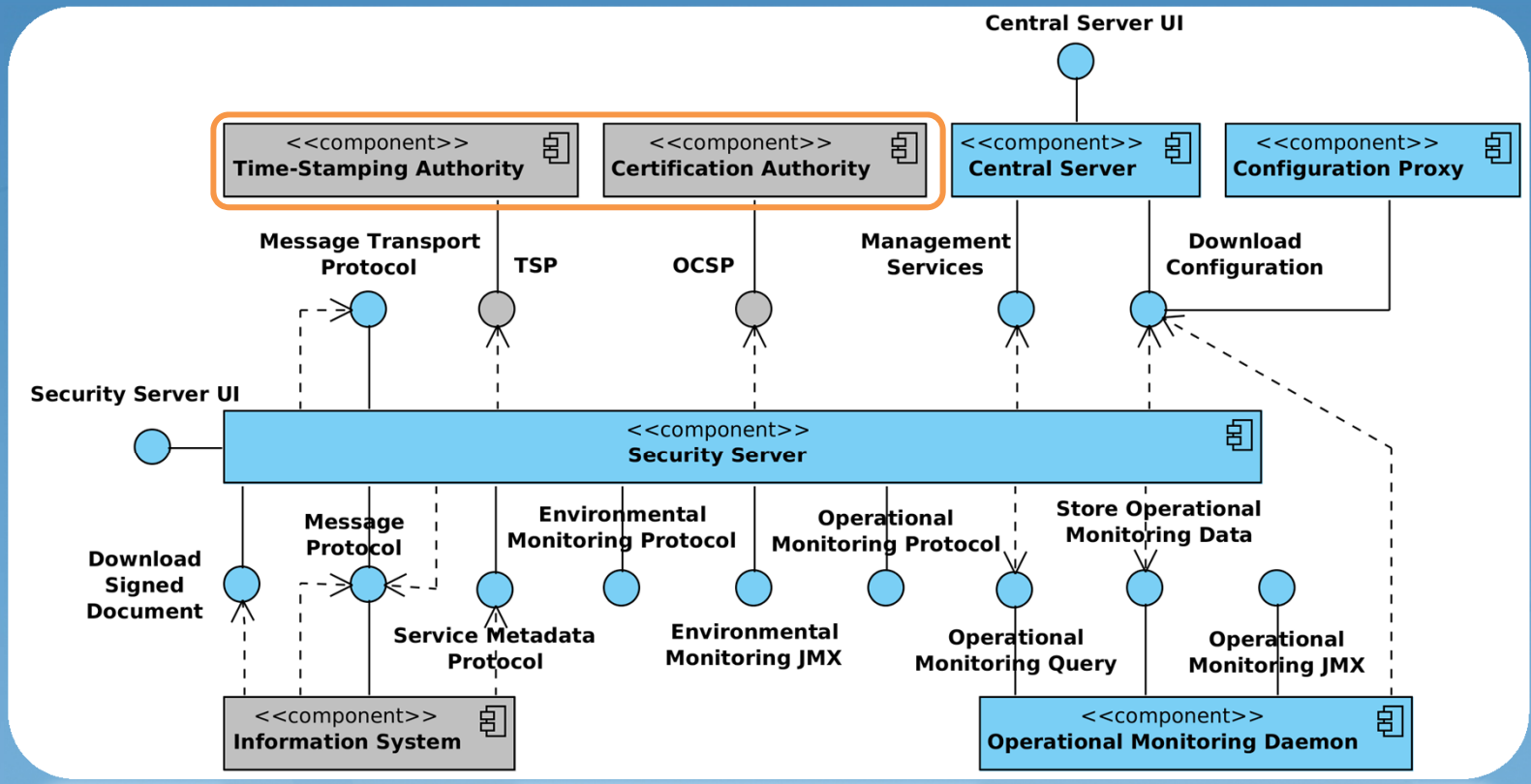

https://www.x-road.com/

# X-Roadのアーキテクチャ




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

# X-Roadのアーキテクチャ



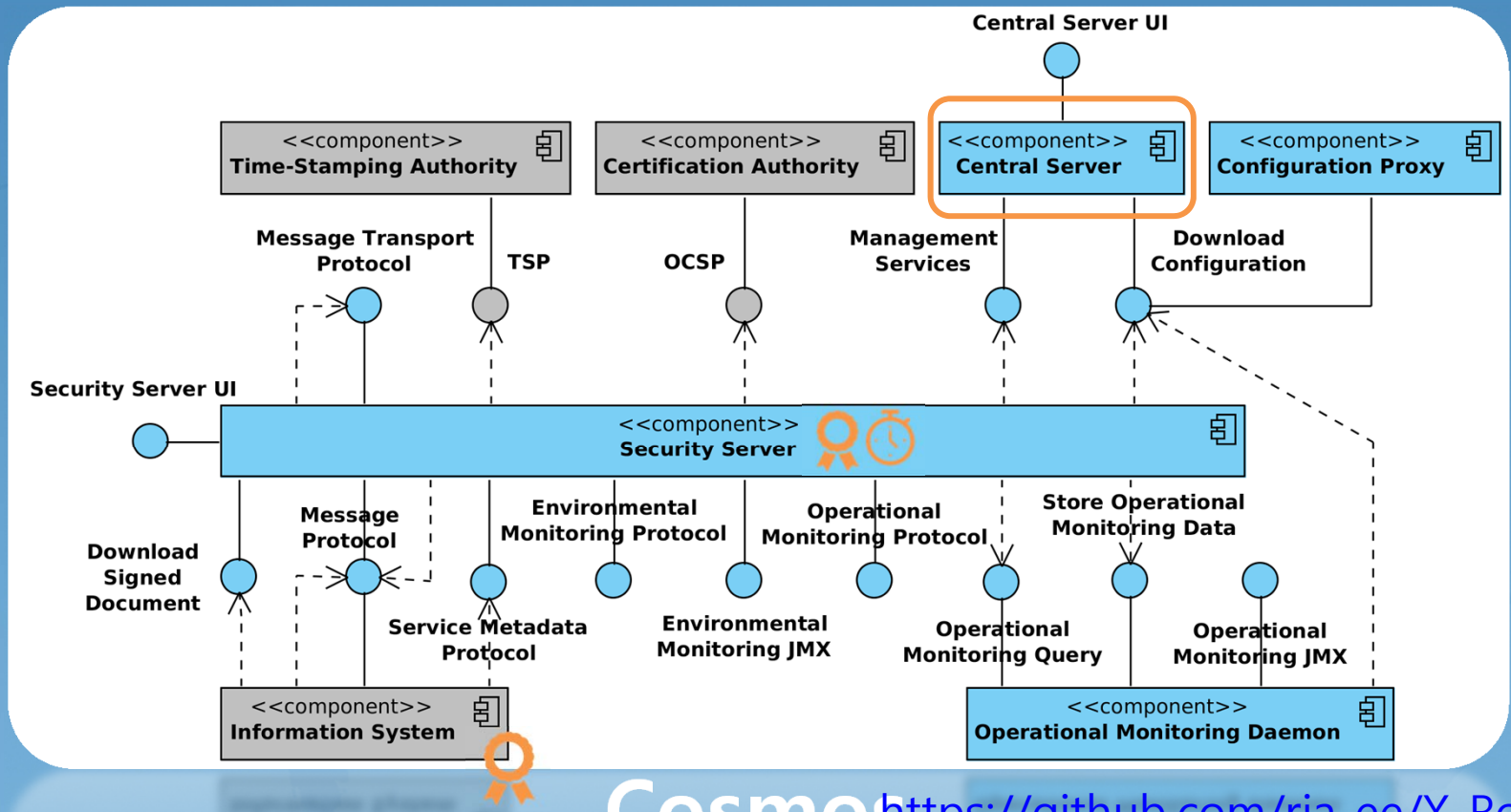

https://github.com/ria-ee/X-Road

# 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）

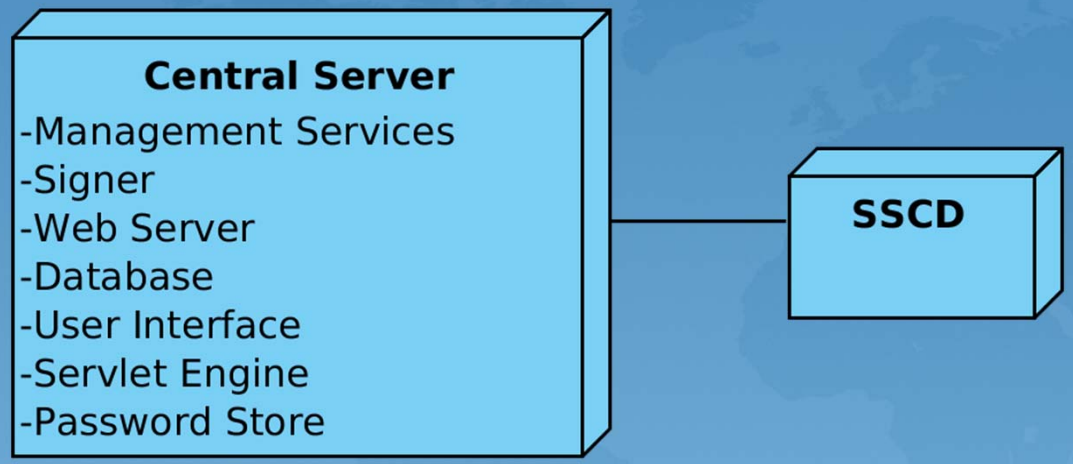
Cosmos
POFESSIONALS OF SAFETY ENGINEERING

# X-Roadのアーキテクチャ




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

# 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

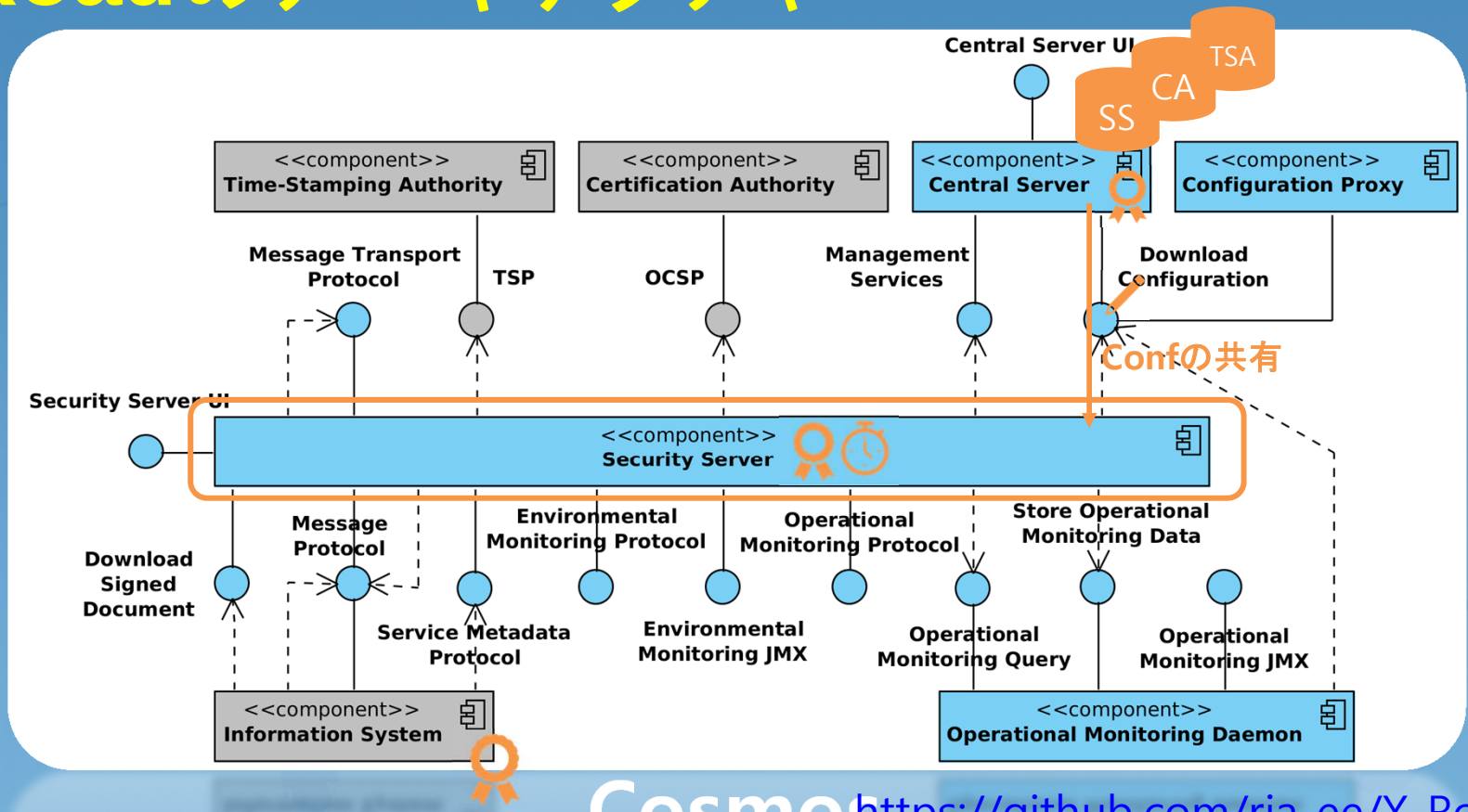
2. 各セキュリティサーバの設定を作成し、各セキュリティサーバに公開

- 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）

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

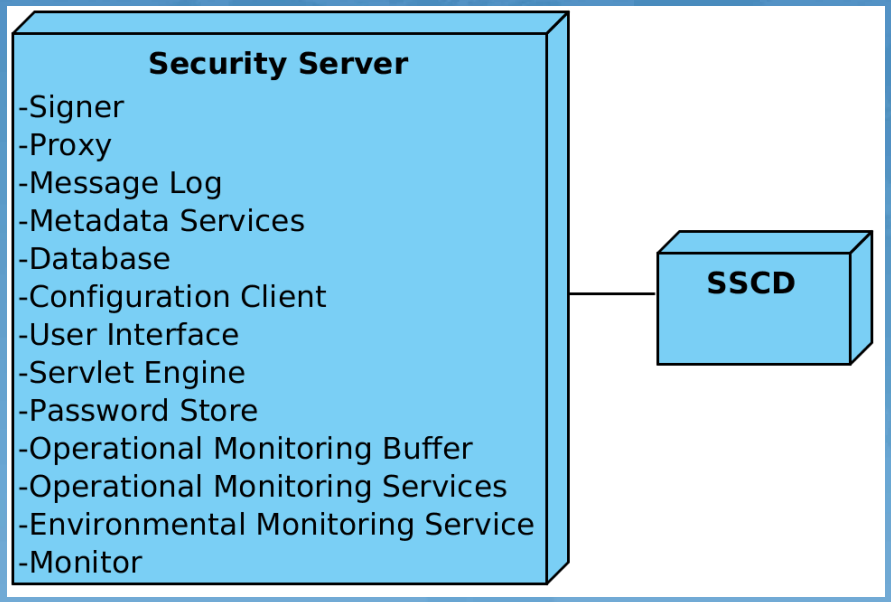
https://github.com/ria-ee/X-Road

# X-Roadのアーキテクチャ




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

# Security Server



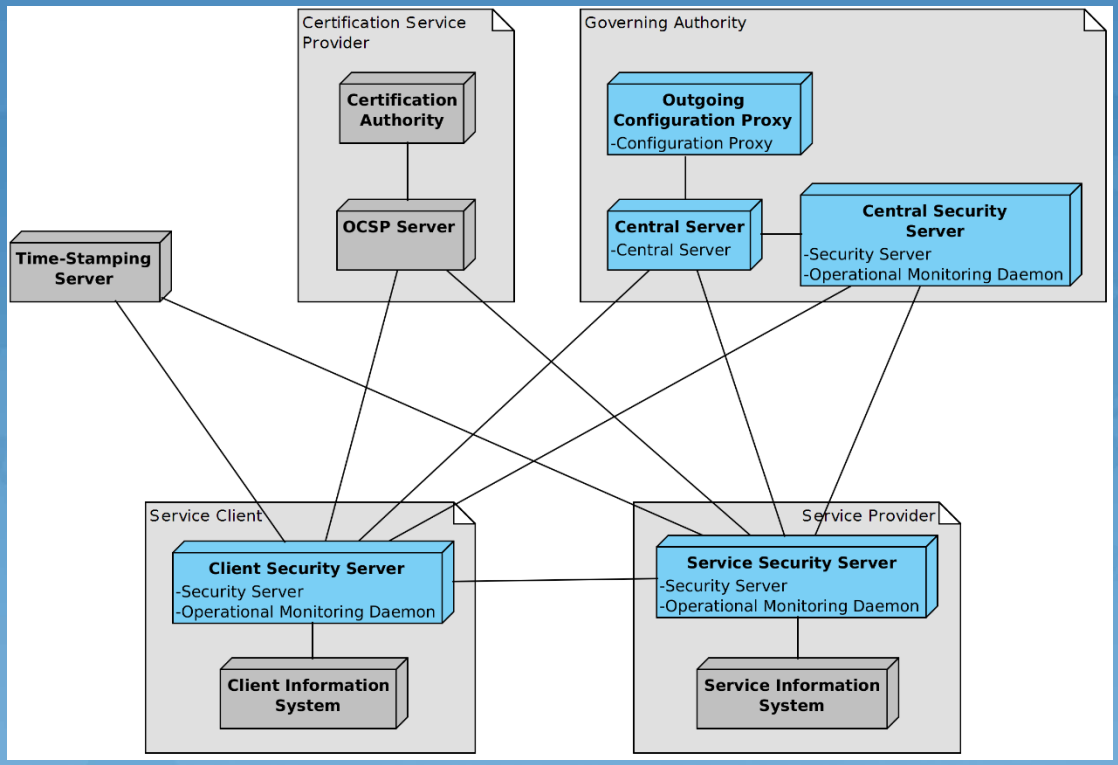

SOAPベースのX-RoadメッセージプロトコルによるSecure Server間の安全なデータ交換を実現

- 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

等。https://github.com/ria-ee/X-Road

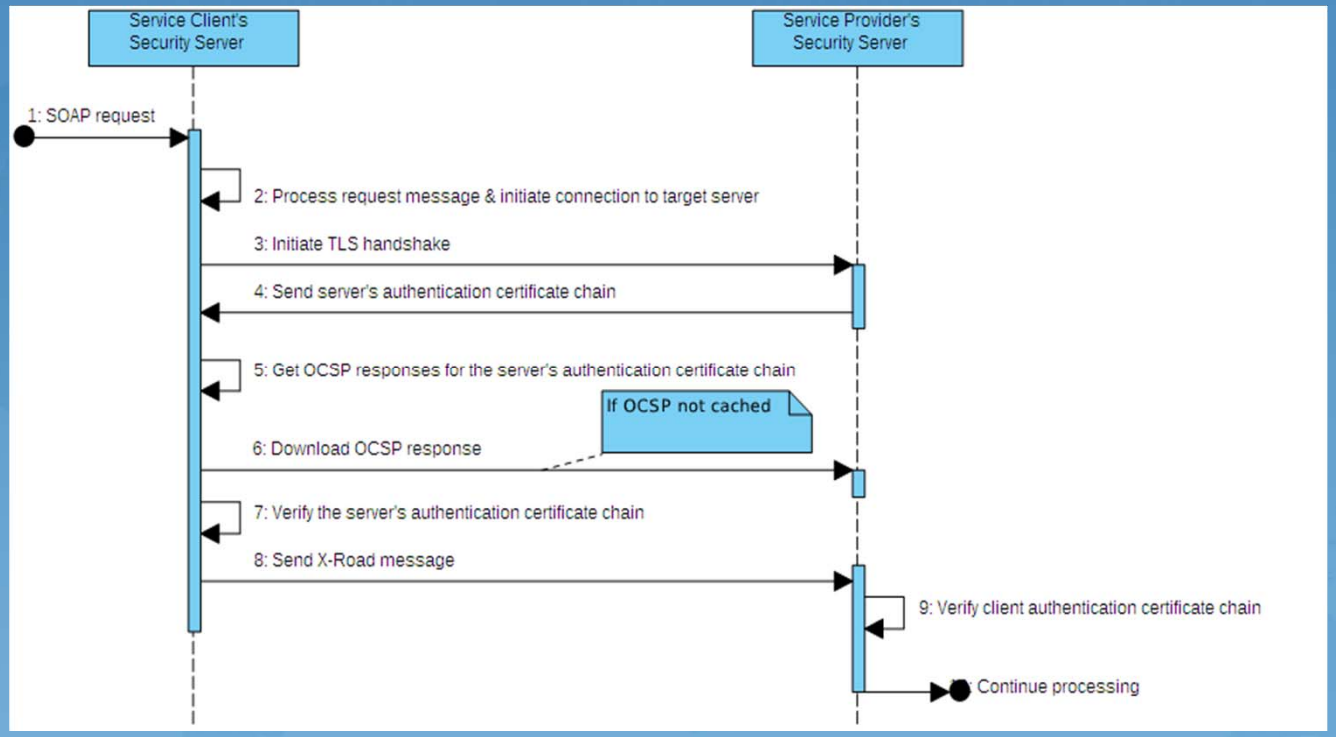
Cosmos
POFESSIONALS OF SAFETY ENGINEERING

# X-Road上での情報交換



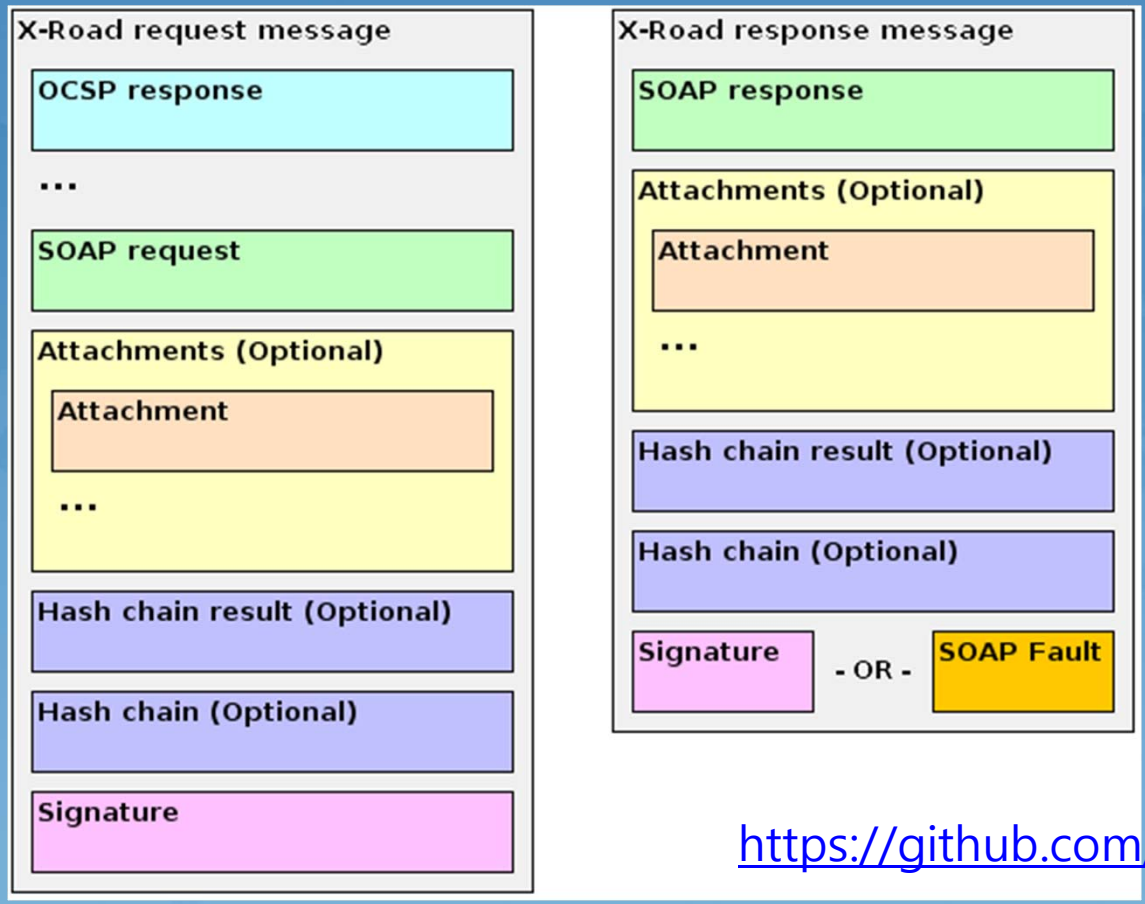

https://github.com/ria-ee/X-Road

# TLS認証



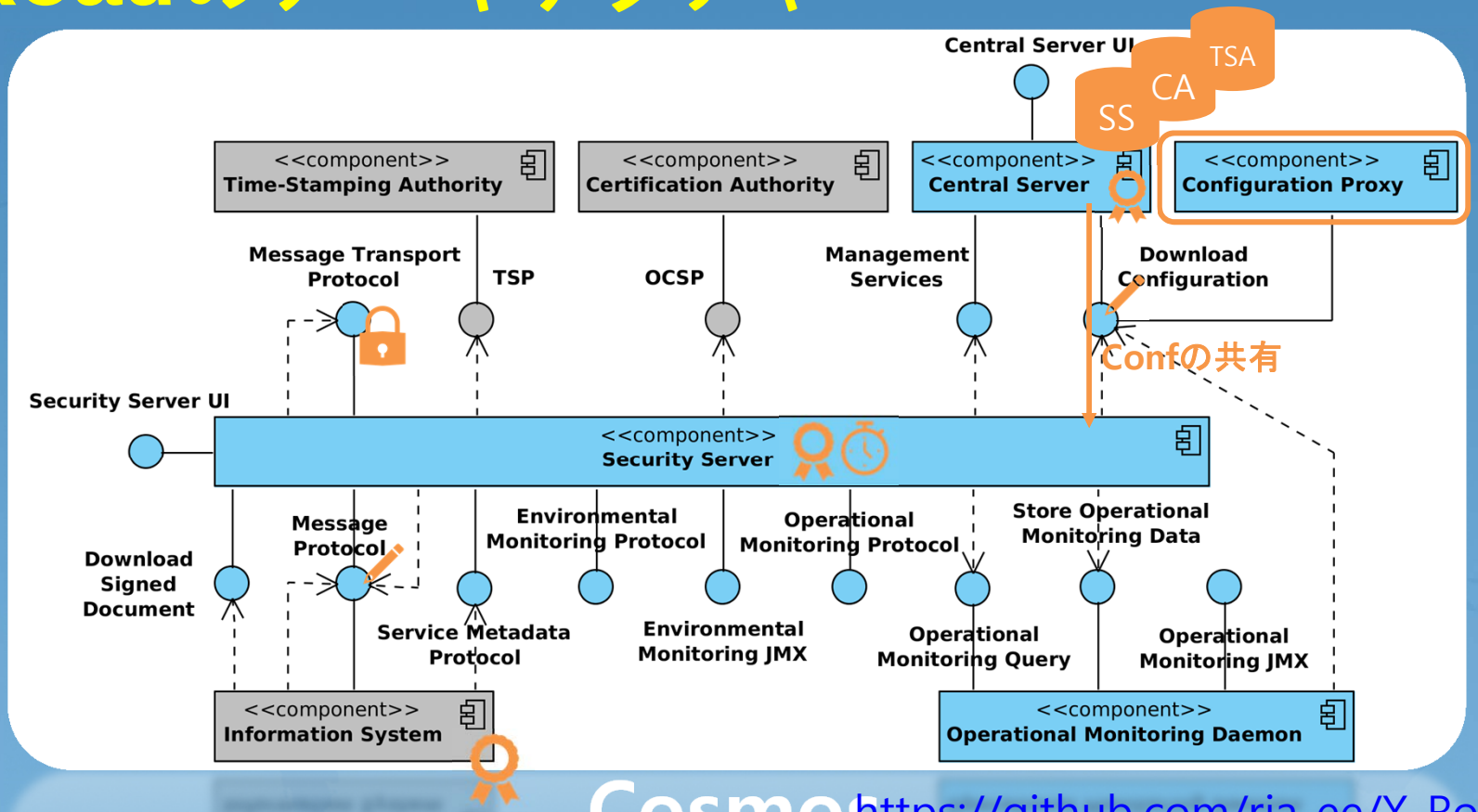

https://github.com/ria-ee/X-Road

# メッセージの構成




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

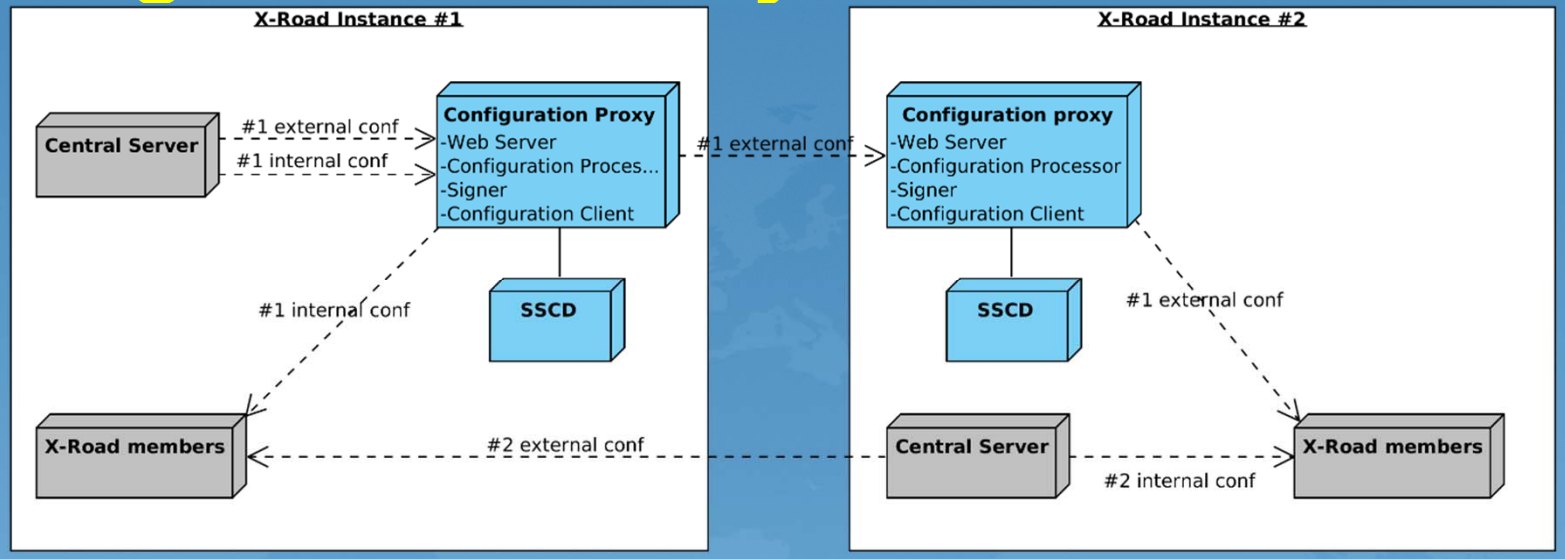
# X-Roadのアーキテクチャ




Cosmos
POFESSIONALS OF SAFETY ENGINEERING

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

# Configuration Proxy

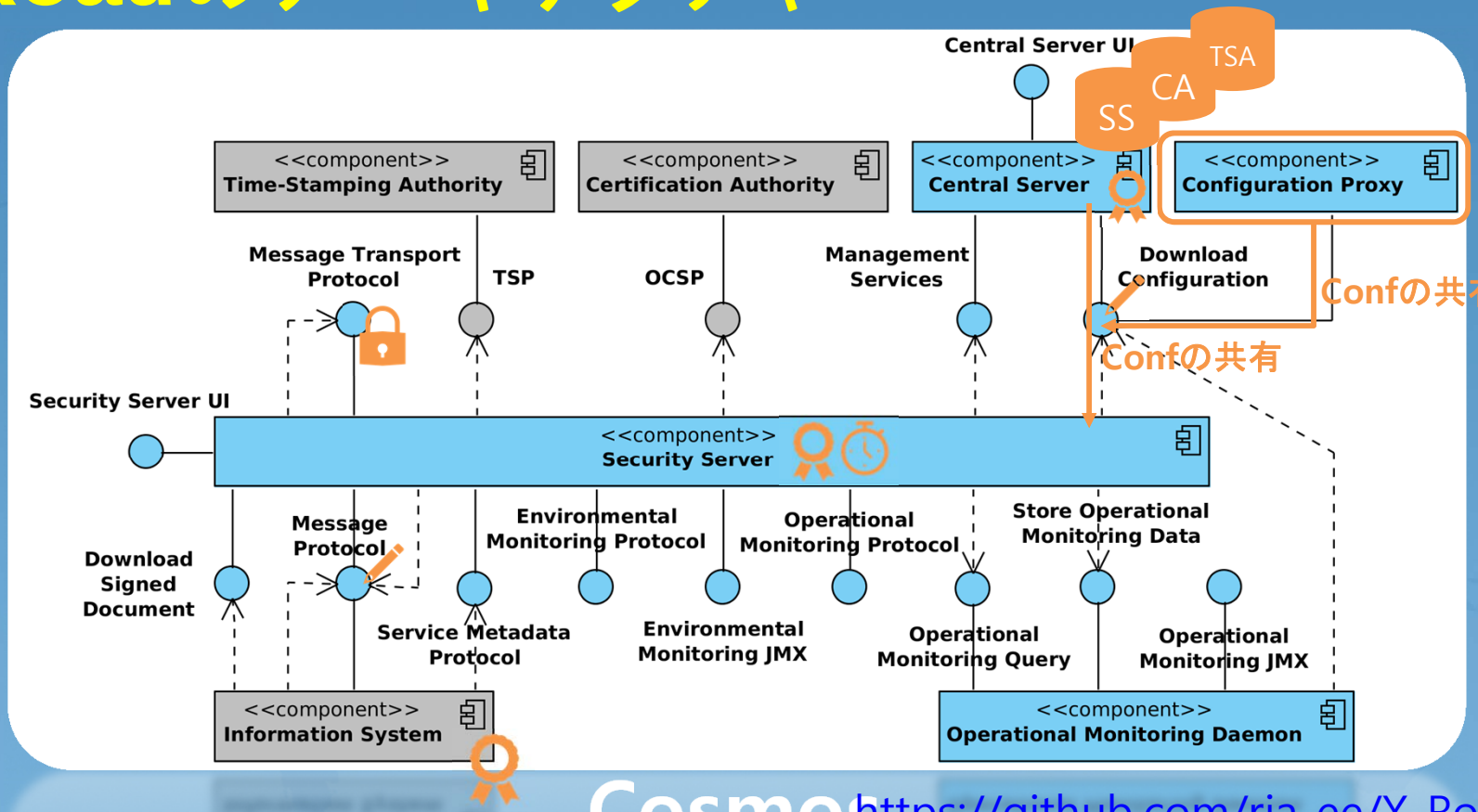



Central ServerからのConfファイルのダウンロードのためのProxy
一分毎にConfファイルをダウンロードし、署名して公開
各セキュリティサーバ内のConfiguration Clientからアクセス可能
X-Road間の設定共有
Central Serverの負荷分散と可用性アップ

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

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

# X-Roadのアーキテクチャ




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

# Findings

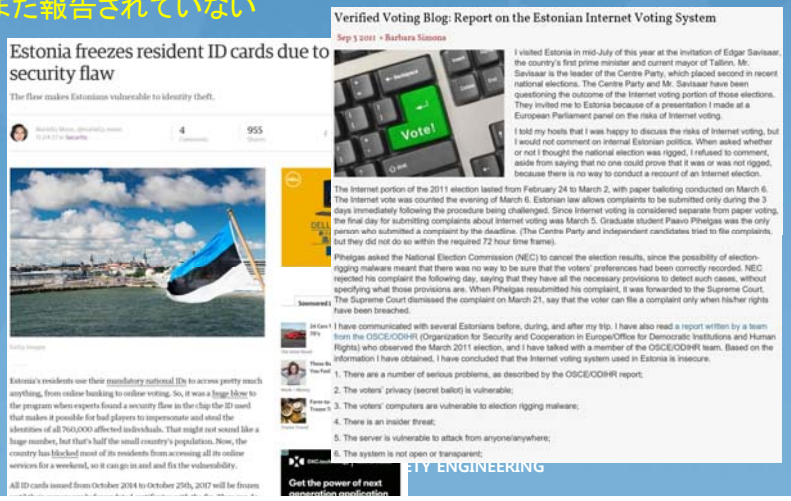
X-Roadを支える仕組み

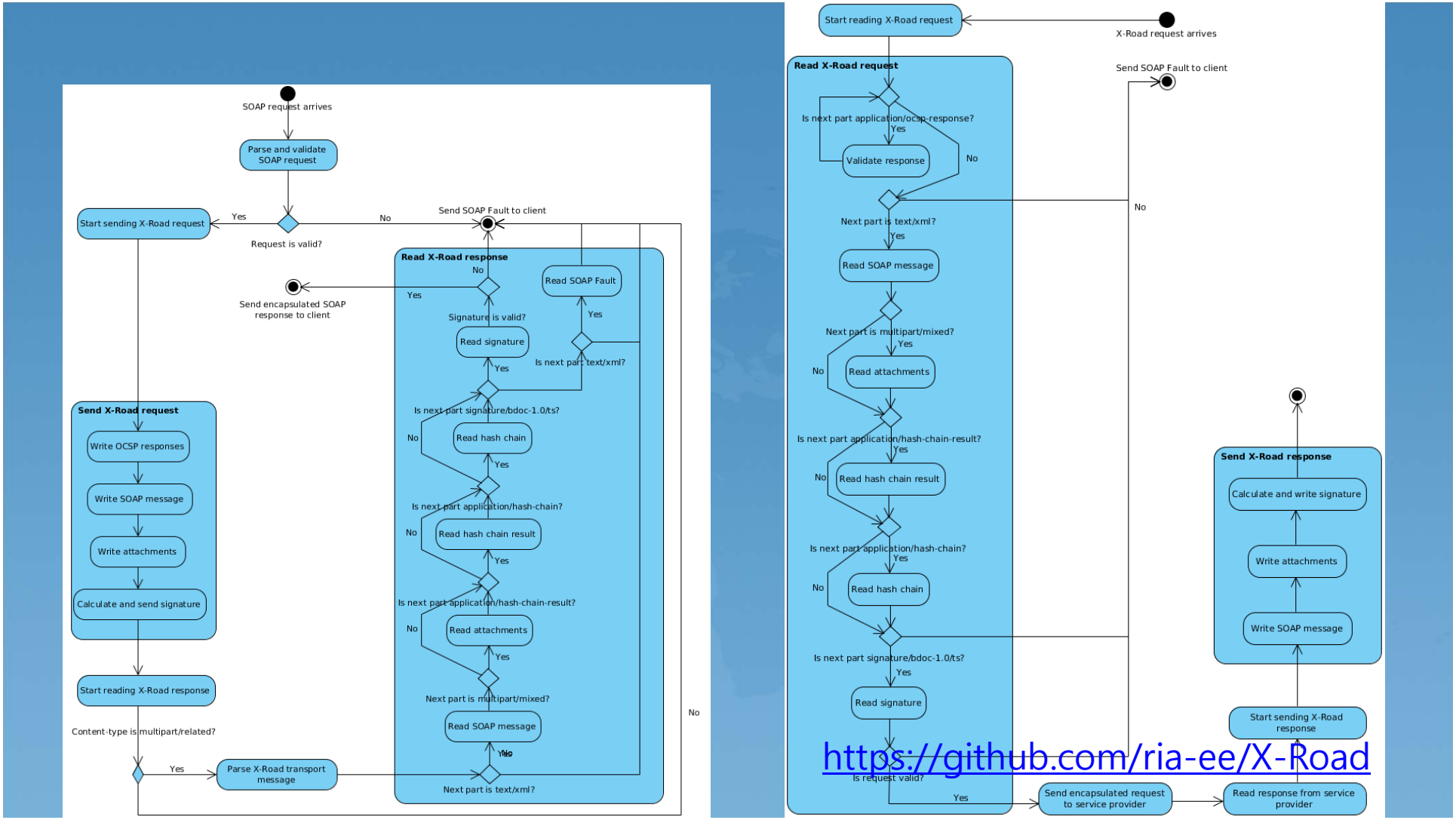
- Technologies
- 社会基盤
  - eID, eIDAS規則、国内法（Regulation No 105 of the Government of the Republic of 23.09.2016）

➡ 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






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

# Central Server Technologies

| Technology | Signer | Web Server | Password Store | 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 | | | | | | |

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

[1] https://github.com/ria-ee/X-Road

# 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 | | | |

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

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

# Operational Monotoring 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 |

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

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

# 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 | |

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

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