OPC Day 2018 in Japan

OPC UA
Global Discovery Serverによる
証明書管理の紹介

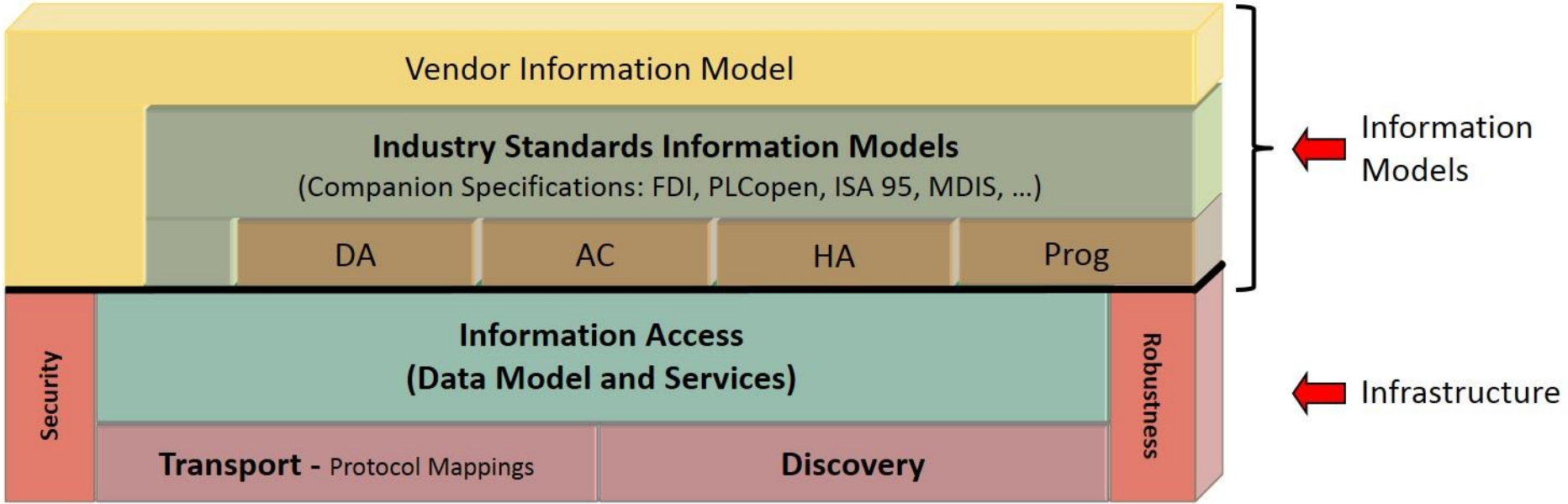
2018年12月14日

日本OPC協議会 技術部会
遠藤 徹 (アズビル株式会社)

Agenda

- OPC UAセキュリティの概要
- 自己署名証明書を使う場合
- 課題 / 解決方法
- CA署名証明書を使う場合
- 利点
- デモ
- まとめ

OPC UAセキュリティの概要



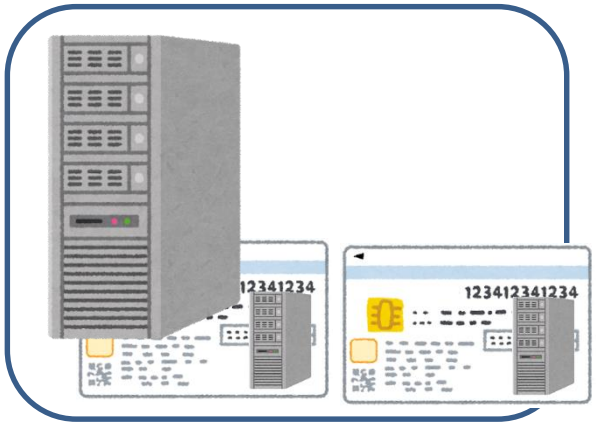
Global Discovery Server

仕様：
OPC Unified Architecture Specification
Part 12: Discovery and Global Services
Release 1.04 February 7, 2018

Global Discovery Server (GDS) ：
a *DiscoveryServer* that maintains a list of OPC UA *Applications* available in an administrative domain.
Note 1 to entry: a GDS may also provide certificate management services.

概要：
OPC UAアプリケーションのリストを管理するサーバ
上記アプリケーションで使用される証明書の管理もおこなう

自己署名証明書を使う場合（準備）

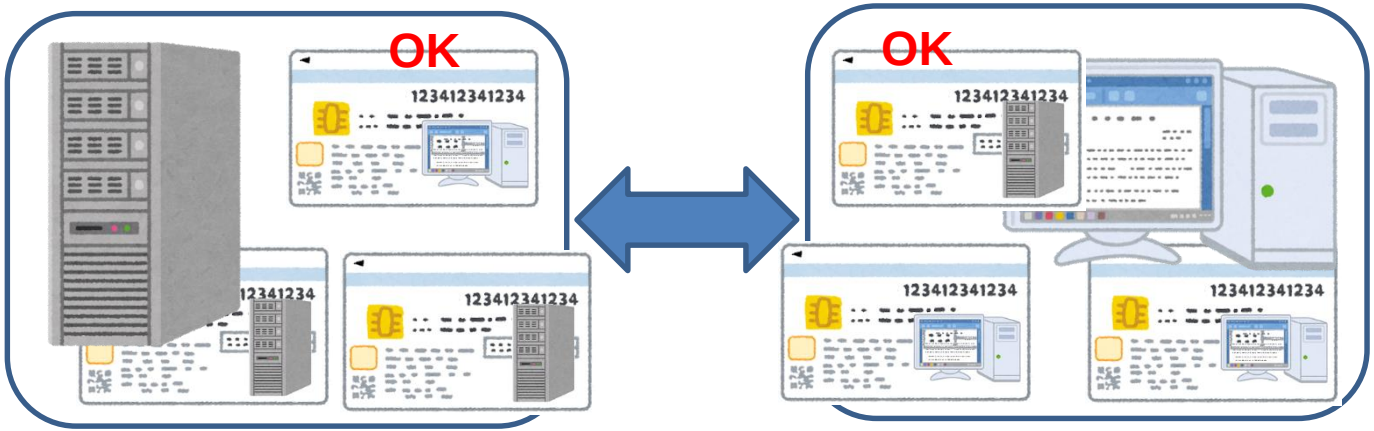


サーバ

クライアント

① 各デバイスに自己署名証明書を作成
② サーバにクライアントの証明書をインポート
③ クライアントにサーバの証明書をインポート

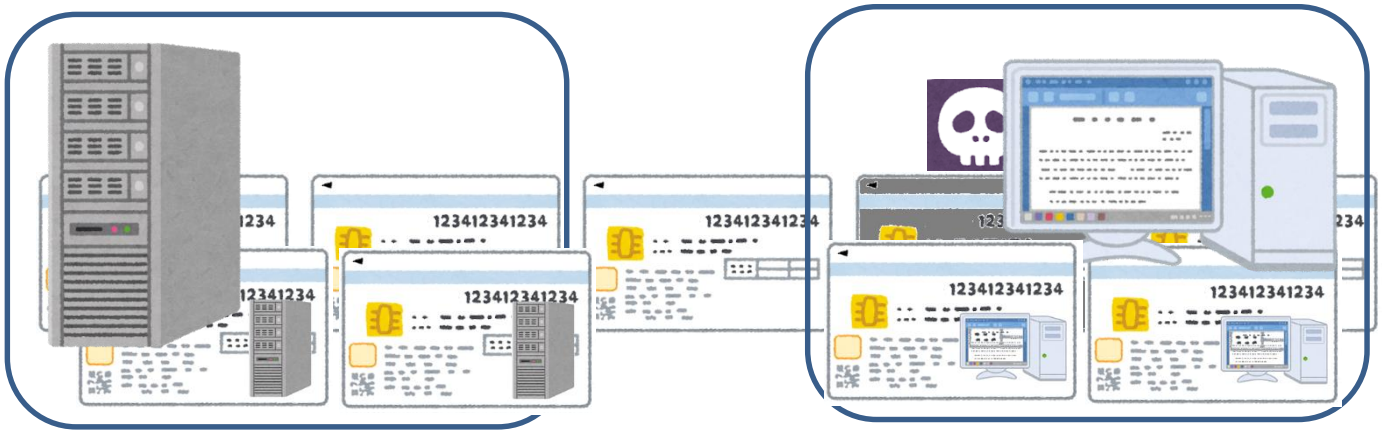
自己署名証明書を使う場合（認証）



① 自身の証明書をお互いに送付
② 送付された証明書とインポート済みの証明書を照合
③ 接続する

課題

- 自己署名証明書は偽造が容易
- サーバとクライアントごとに証明書のペアが必要
- 証明書の作成/インポートが煩雑



サーバ　　クライアント

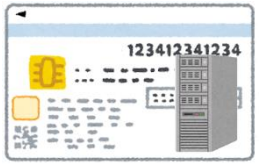
解決方法

- Global Discovery Serverによる証明書管理
  - 証明書の作成をGDSに集約
  - 証明書はCA署名証明書にする
  - 証明書の照合にはCA証明書を使用
  - 証明書の自動インストール機能あり

GDS：Global Discovery Server
CA：Certificate Authority 認証局
CA署名証明書：認証局発行の証明書
CA証明書：認証局自身の証明書

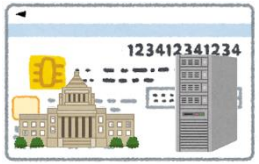
証明書の種類

自己署名証明書



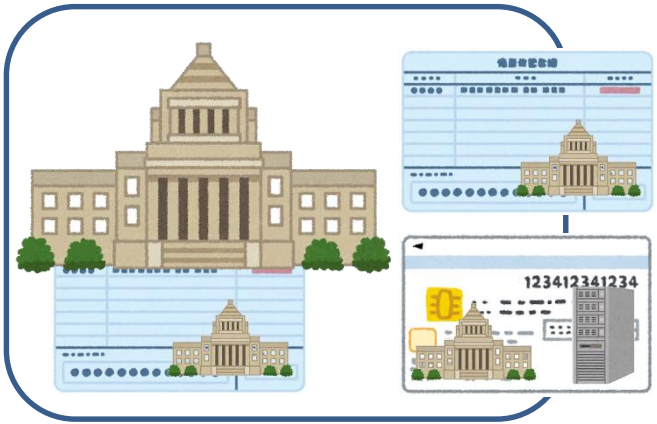
- 自分で作るID
- 名刺のようなもの

CA署名証明書

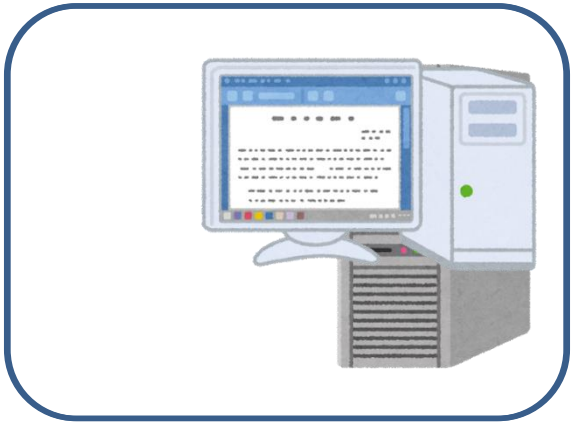


- GDSが発行するID
- 正当性をGDSが担保
- 免許証のようなもの

CA署名証明書を使う場合（準備）



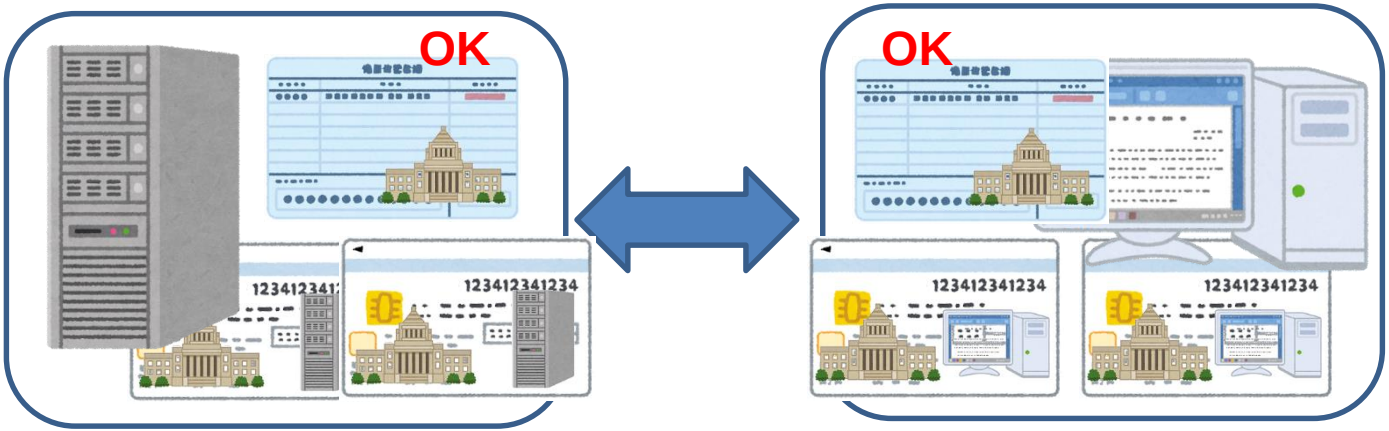
GDS



サブCAオペレータ

① GDSはCA証明書を作成
② GDSはデバイスのCA署名証明書を作成
③ デバイスはCA署名証明書とCA証明書をインポート

CA署名証明書を使う場合（認証）



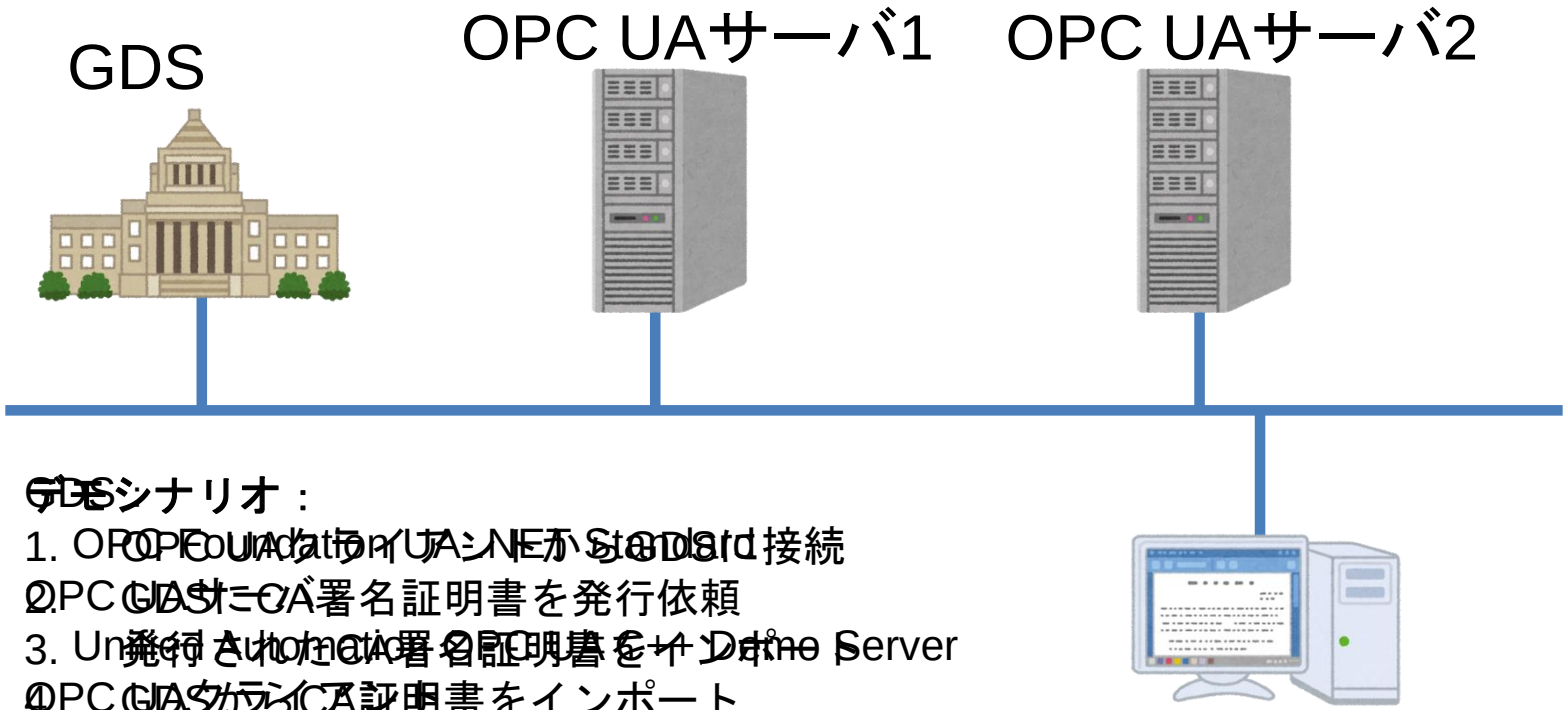
サーバ　　クライアント

① お互いのCA署名証明書を送付
② 送付されたCA署名証明書をCA証明書で照合
③ 接続する

利点

	自己署名証明書	CA署名証明書
証明書の偽造	偽造可能	GDSのセキュリティにより偽造を防ぐ
証明書の枚数	デバイス数の2乗(10000枚） 各デバイスに全デバイスの自己署名証明書が必要	デバイス数の2倍（200枚） 各デバイスにCA署名証明書とCA証明書が必要
証明書の更新	手動	自動化可能
デバイス追加時の既設デバイス変更	新規デバイスの証明書を既設デバイスにインポート	変更なし
設備	デバイスのみ	デバイス ＋ GDS

デモシステムの構成



デモシナリオ：

1. OPC UAクライアントからGDSに接続
2. GDSでOPC UAサーバ署名証明書を発行依頼
3. 発行されたOPC UAサーバ署名証明書をインポート
4. GDSからCA証明書をインポート
5. OPC UAクライアントからOPC UAサーバに接続

デモ（準備）

添付の動画ファイルを参照

デモ（確認）

添付の動画ファイルを参照

デモ（接続）

添付の動画ファイルを参照

まとめ

- Global Discovery Serverによる証明書管理
  - 証明書管理の省力化/自動化
  - 偽造防止によるセキュリティ向上

台数が多くなりがちなIIoTデバイスに効果大

日本OPC協議会

URL: https://jp.opcfoundation.org