
KUKA

Security in OPC UA

Vollversammlung der OPC UA Arbeitskreise im VDMA

2. November 2018

Agenda

- Warum Security?
- Security in OPC UA
- PKI im industriellen Umfeld
- Zertifikate im IoT Umfeld
- Herausforderungen für Verschlüsselung
- Rollen & Rechte

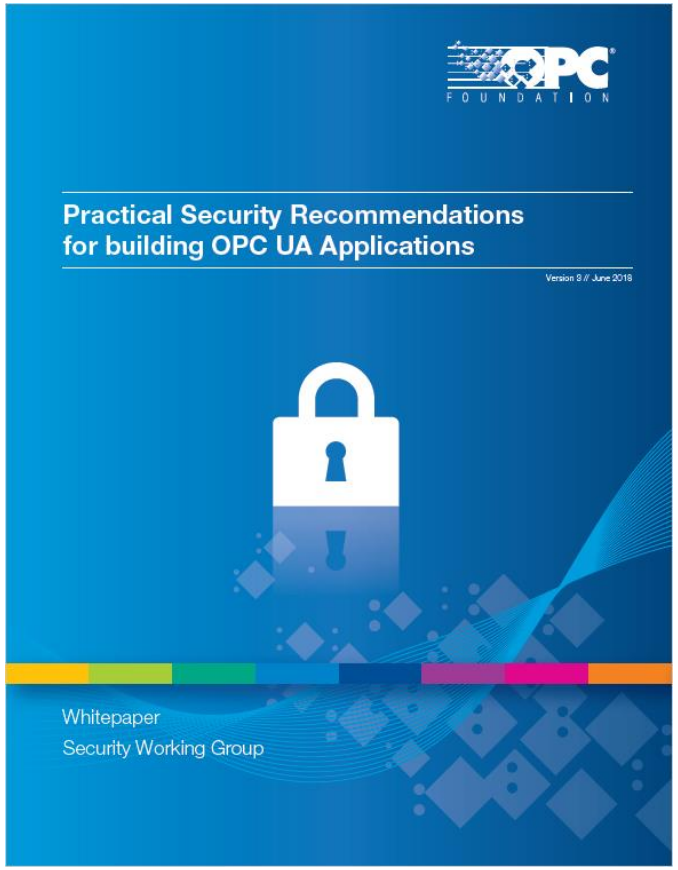
Warum Security?

- Bisherige Feldbusse kommen auch ohne Security aus!
- Hacker schaffen es niemals durch die diversen Firewalls!
- Industrieanlagen sind grundsätzlich mit starken Passwörtern geschützt!
- Security Updates sind völlig überbewertet!

Security in OPC UA

- Security wurde bereits beim Design von OPC UA berücksichtigt und ist Teil des Standards (Part 2 Security Model, Part 7 Profiles, auch in weiteren Teilen berücksichtigt)
- Sicherer Kanal über durch Verschlüsselung auf Transport Layer mit **X.509** Zertifikaten
- Sicher Applikations-Authentifizierung über Application Instance Certificates (**X.509**)
- Benutzerauthentifzierung über Benutzername und Passwort oder **X.509** Zertifikat
- Drei Message Security Modes: None, Sign, Sign & Encrypt

Steht alles hier drin:



… und natürlich hier:

OPC FOUNDATION

OPC Unified Architecture

Specification

Part 2: Security Model

Release Candidate 1.04

May 14, 2018

IDATION

Unified Architecture

Specification

Part 7: Profiles

Release 1.04

November 1, 2017

TION

hitecture

on

files

Release 1.04

November 1, 2017

PKI im industriellen Umfeld

- Publik Key Infrastructures sind im industriellen Umfeld noch nicht etabliert – bei vielen Firmen noch nicht einmal im Office-Umfeld!
- Software für PKI existiert – die Konzeption einer Key Infrastructure und die Einführung ist eine organisatorische Herausforderung
- Global Discovery Server (GDS) von OPC UA übernimmt auch CA-Funktionalitäten – ist aber trotzdem nicht „plug and play“
- Root of Trust?

Zertifikate im IoT-Umfeld

- Gültigkeit: 2 Jahre? 3 Jahre? 10 Jahre? Gerätelebenslang?
- Schlüssellängen müssen wegen steigender Rechenleistung eines potentiellen Angreifers erhöht werden
- Hash-Algorithmen müssen durch neue Verfahren ersetzt werden
- Neue Verschlüsselungsverfahren werden etabliert (Leightweight Crypto, z.B. PRESENT)
- Widerruf von kompromittierten Zertifikaten über CRLs
- CRLs müssen aktualisiert werden
- CRLs „wachsen“ mit der Zeit und der Anzahl verbreiteter (und damit potentiell zu widerrufender) Zertifikate
- Wo werden Zertifikate bzw. der zugehörige private key auf einem IoT-Device **sicher** gespeichert?
- Verwendung von OCSP? (online!)

Herausforderungen für Verschlüsselung im IoT

- OPC UA verwendet hybrides Verfahren: asymmetrisches Verfahren, um einen Sitzungsschlüssel für ein symmetrisches Verfahren auszuhandeln
- Asymmetrische Verfahren sind rechenaufwändig und erzeugen größere verschlüsselte Nachrichten als symmetrische Algorithmen
- Zufallsgenerator:
- IoT-Device muss für symmetrischen Session-Key Zufallszahlen generieren können
- Zufallszahlen (Nonce) werden auch für die Authentifizierung mittels Challenge-Response benötigt
- IoT-Devices und embedded Betriebssysteme sind oft nicht in der Lage **gute** Zufallszahlen zu erzeugen → schwache Session-Keys
- Forward Secrecy?

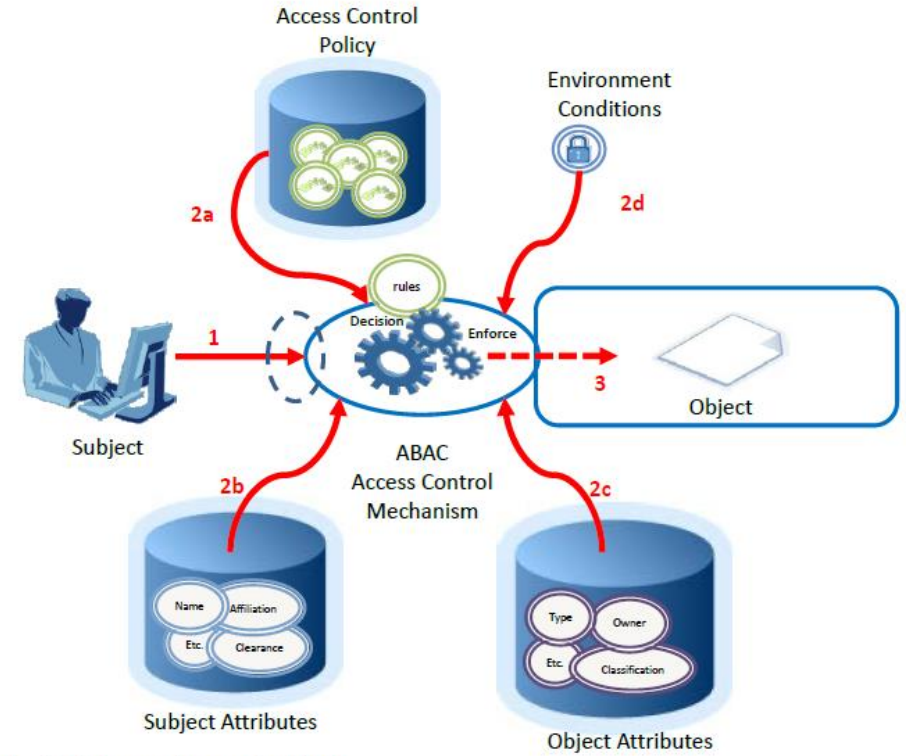
Die Landtechnik kann PKI:

- Aber:
  - Zertifikate sind unbegrenzt gültig
  - Nach dem Erstkontakt (zw. Traktor und Anbaugerät) wird nur noch ein symmetrischer Schlüssel verwendet (der nicht erneuert wird?!)

Rollen und Rechte

- UPC UA verwendet rollenbasierte Zugriffskontrolle (RBAC – Roll Based Access Control)
- Mehr Möglichkeiten, aber auch eine höher Komplexität ergeben sich mit ABAC – Attribute Based Access Control – siehe NIST SP 800-162
- Attribute erweitern dabei die Rollen um eine zusätzliche Dimension, z.B.:
  - Zeit
  - Ursprung einer Verbindung
  - Zustand einer Maschine
  - …
- Die AG 3 der Plattform Industrie 4.0 wird zum Digitalgipfel im Dezember ein Diskussionspapier zum Thema ABAC veröffentlichen

Attribute Based Access Contol – Basic Scenario



1. Subject requests access to object
2. Access Control Mechanism evaluates a) Rules, b) Subject Attributes, c) Object Attributes, and d) Environment Conditions to compute a decision
3. Subject is given access to object if authorized

Figure 2: Basic ABAC Scenario

Quelle: NIST SP 800-162

ABAC – Enterprise Scenario

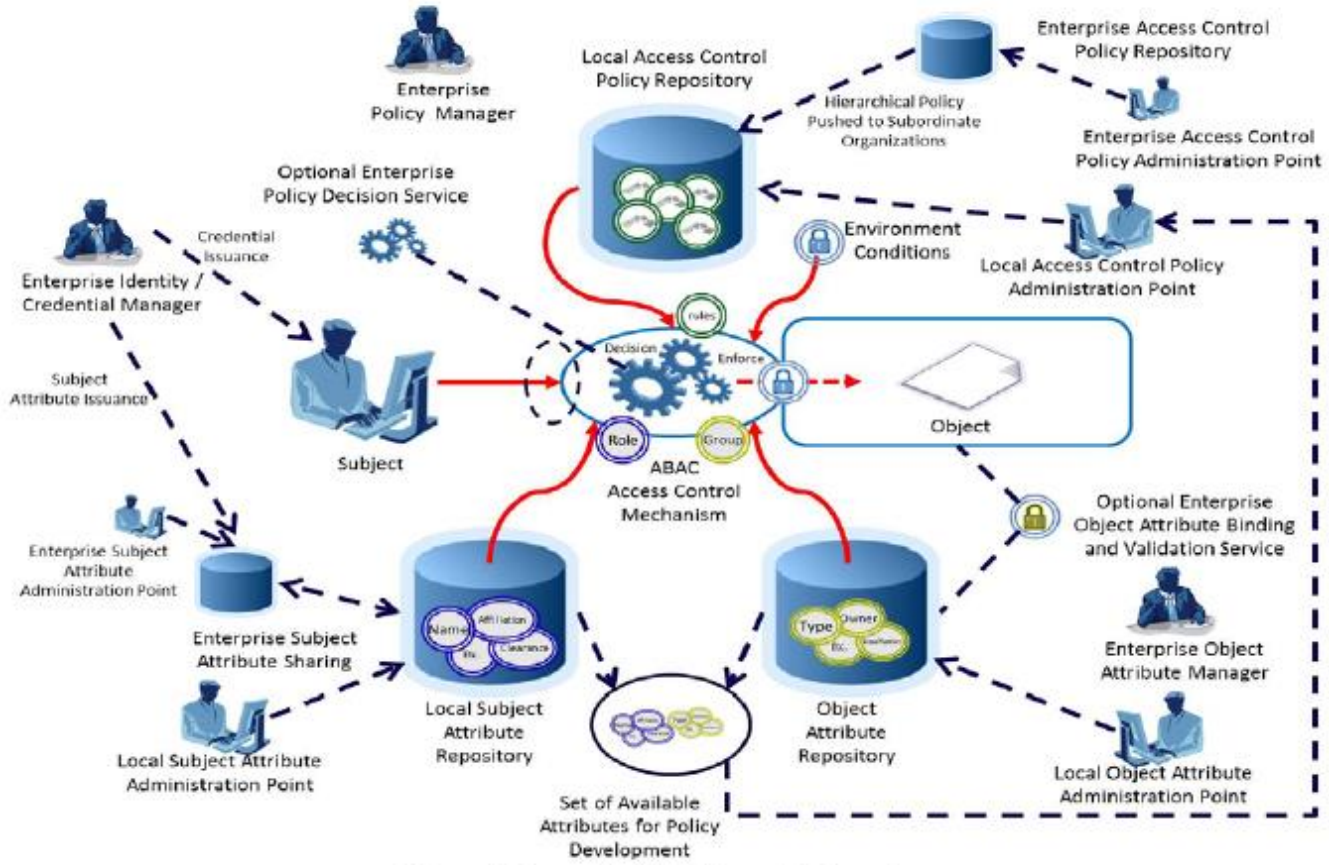


Figure 4: Enterprise ABAC Scenario Example

Quelle: NIST SP 800-162

KUKA

Vielen Dank! Fragen?