OPC UA Security – How It Works

MatrikonOPC

OPC FOUNDATION

Information Revolution 2014

Microsoft Conference Center,

Redmond, WA

August 5th – 6th

Nathan Pocock
Technical Director
OPC Foundation

Darek Kominek
Strategic Marketing Manager
MatrikonOPC

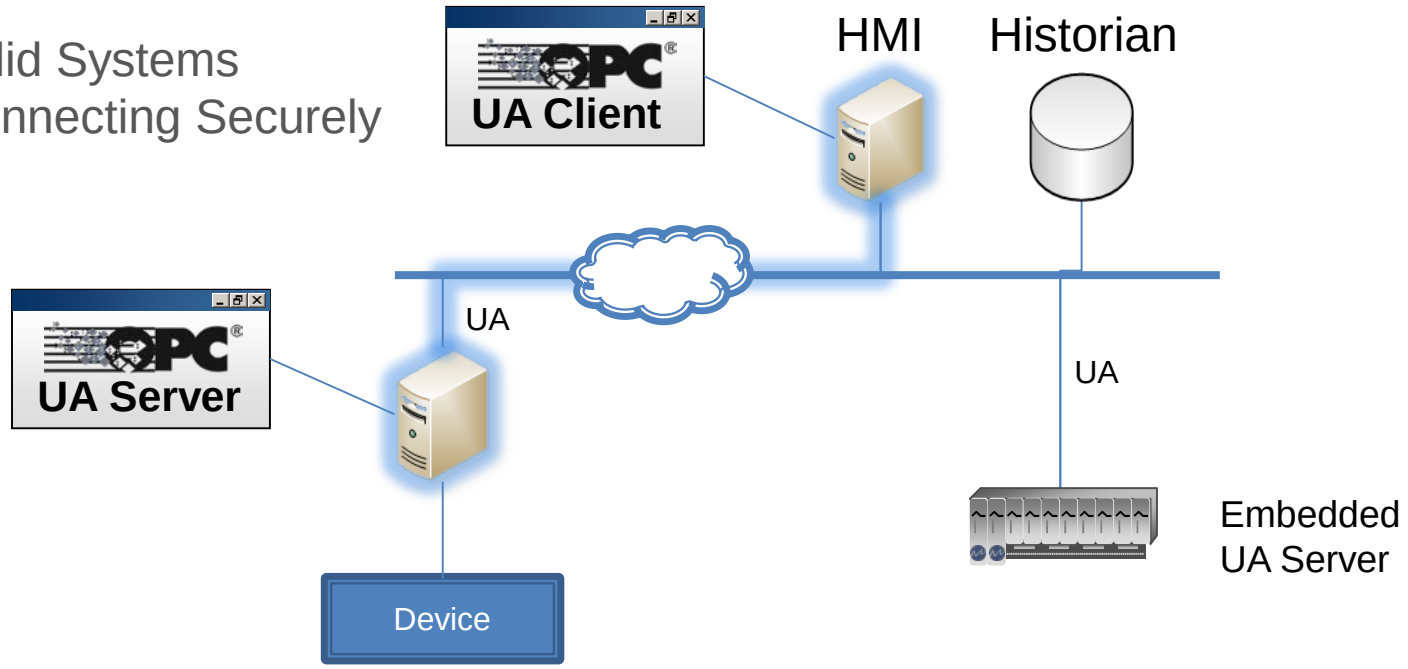
Paul Hunkar
Technical Director
DS Interoperability LLC

Agenda

- Security Backgrounder
- OPC UA Security Overview
- Questions

OPC UA Goal: Secure Data Connectivity

Valid Systems
Connecting Securely



Authorized Users
Gaining Access

Challenge: How To Keep It Secure

Must uphold:

How?

- Build standard with security in mind
- Use industry accepted standards & best practices (Ex. WS-*,NERC, ISA99, NIST…)
- Keep it flexible: Account for evolution

Key Security Factors

1. Should the Client and Server trust each other?
2. Should the Server trust the current user of a trusted application?
3. How can the data be protected?

Secure Communications

Backgrounder

Security Backgrounder

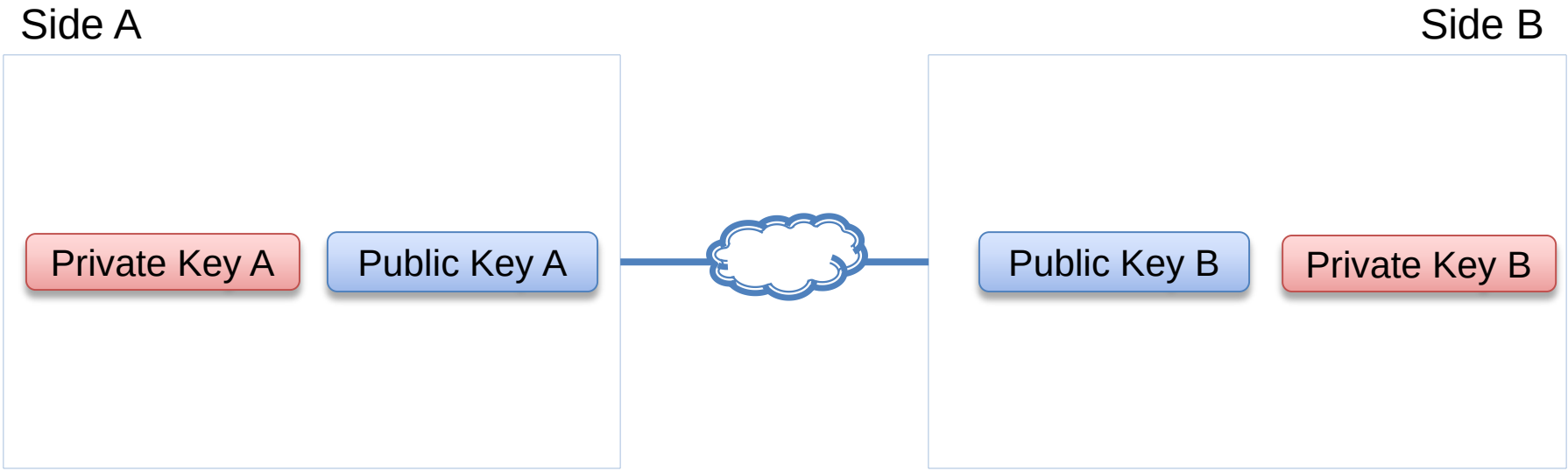
Physical Security

Digital Security

Physical Keys & Locks	Cryptographic Keys & Algorithms
Keys - Physical Locks - Physical	Keys - Large Prime numbers (hard to guess) Locks - Cryptographic Algorithms
Lock & Unlock	Encrypt & Decrypt
Block Access, protect contents	Block Access, protect contents, prove identity

Topic 1: Establish Secure Communication

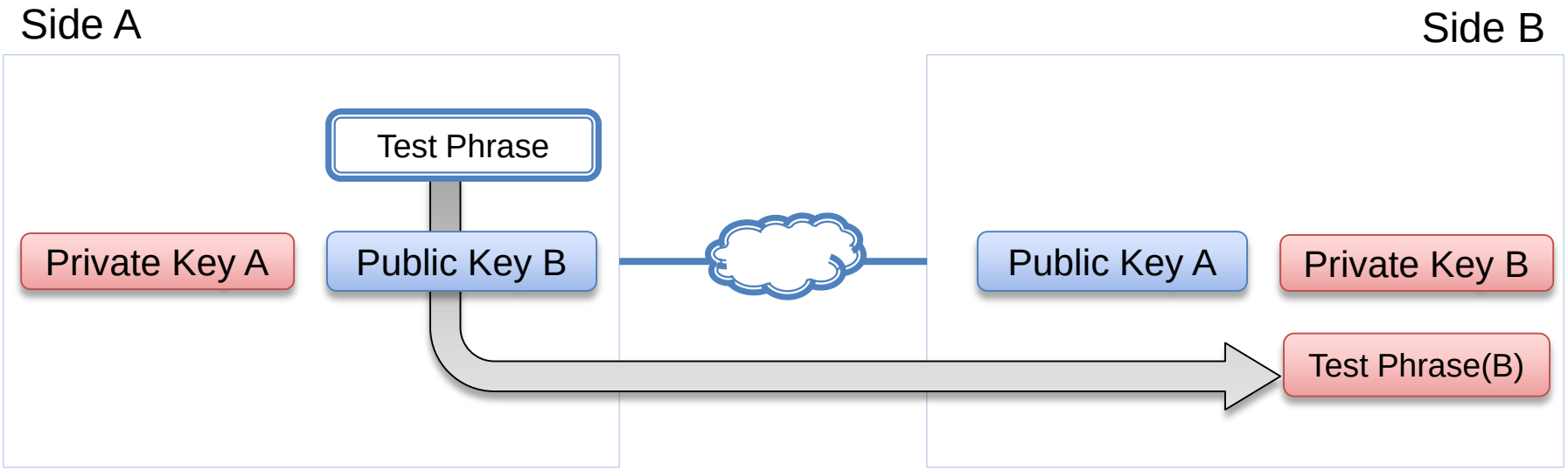
Focus: Mechanics



Sides A & B: Exchange Public Keys

Topic 1: Establish Secure Communication

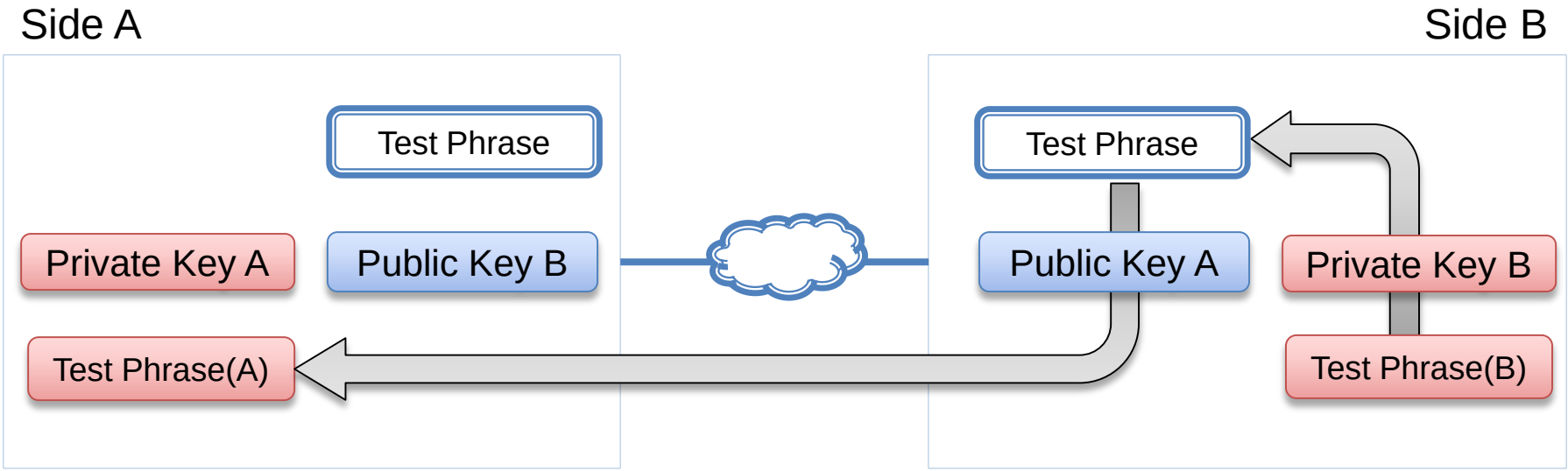
Focus: Mechanics



Side A: Encrypt “Test Phrase” with Public Key B, send to B

Topic 1: Establish Secure Communication

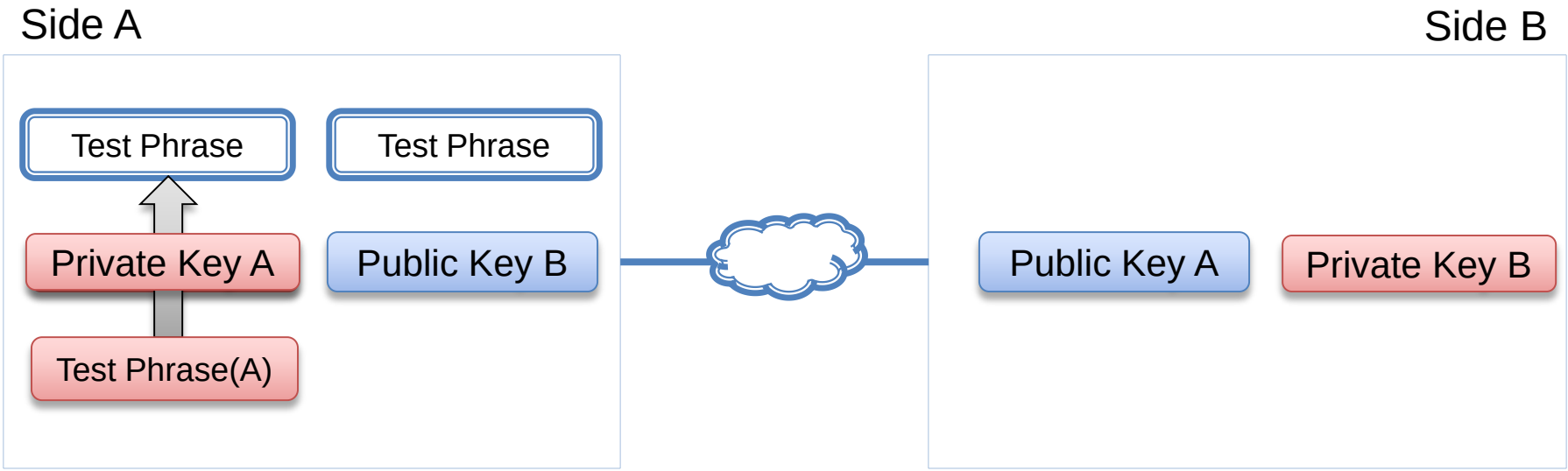
Focus: Mechanics



Side B: Decrypt with Private Key B, then Encrypt with Public Key A, send to A

Topic 1: Establish Secure Communication

Focus: Mechanics



Side A: Decrypt with Private Key A – ensure both sides can process message

Asymmetric Encryption: Each side uses different key to encrypt messages.

Symmetric Encryption: Both sides use agreed to key for encrypt/decrypt

Topic 1: Establish Secure Communication

Focus: Signing vs. Encryption

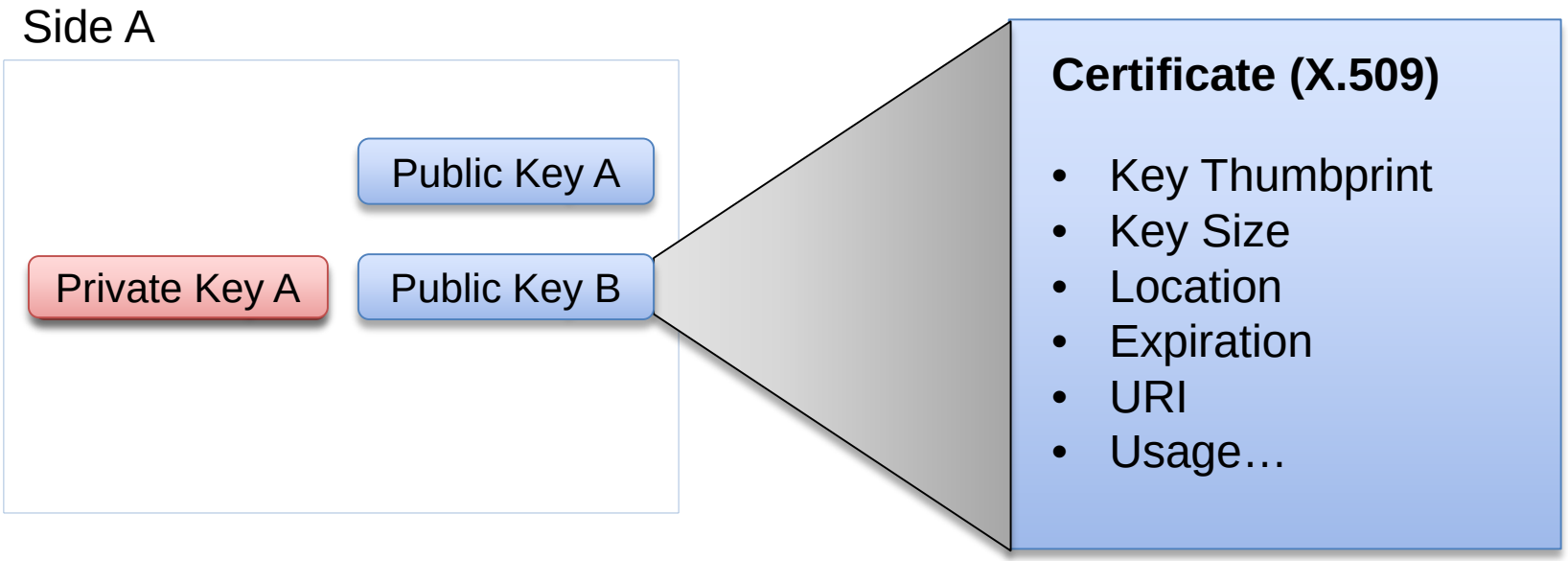
Private and public keys can be used for both functions:

- **Signing:** Proving you are who you say you are
- **Encrypting:** Protecting the data being sent so only receiver can read

Operation	What's Generated	Generated Using	Consumed Using
Signing	CRC / Hash	Sender's Private Key	Sender's Public Key
Encrypting	Scrambled Message	Receiver's Public Key	Receiver's Private Key

Topic 2: Certificates

Focus: What is a Certificate



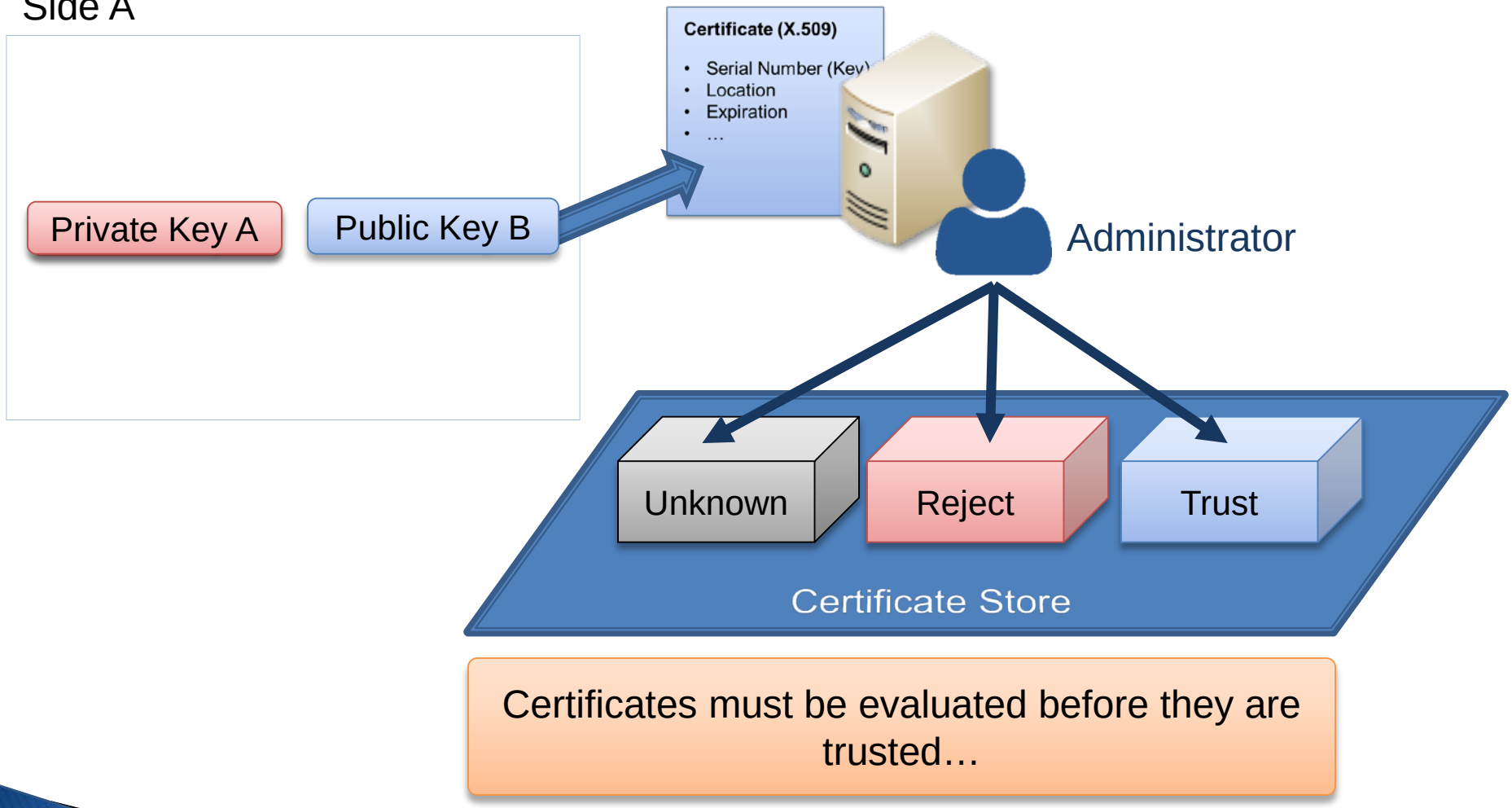
Certificates provide:

1. standardized key encoding format
2. additional context (expiry date)

Topic 2: Certificates

Focus: Trusting Certificates

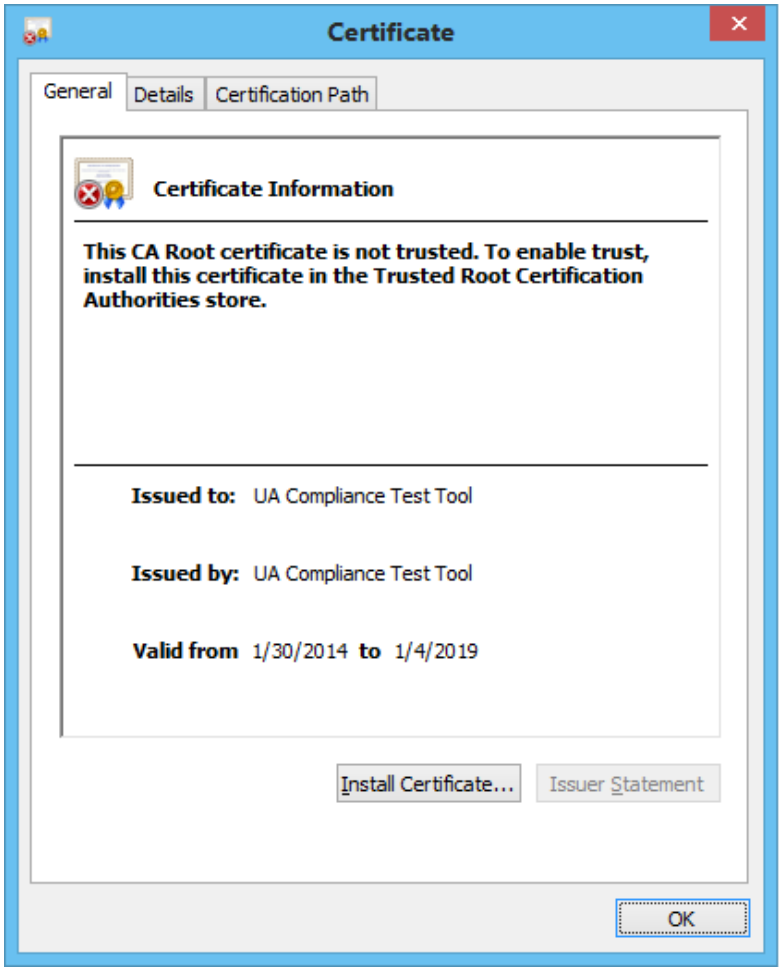
Side A



Certificates must be evaluated before they are trusted…

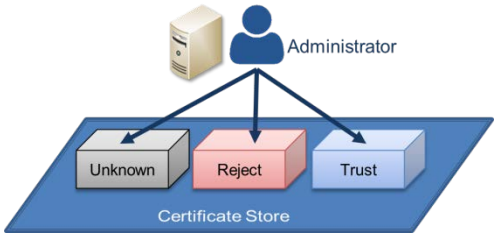
Topic 2: Certificates

- Example: Not Trusted Certificate



Topic 2: Certificates

Focus: Certificate Management



- Public Key Infrastructure (PKI)
  - System for managing certificates
  - Management options:

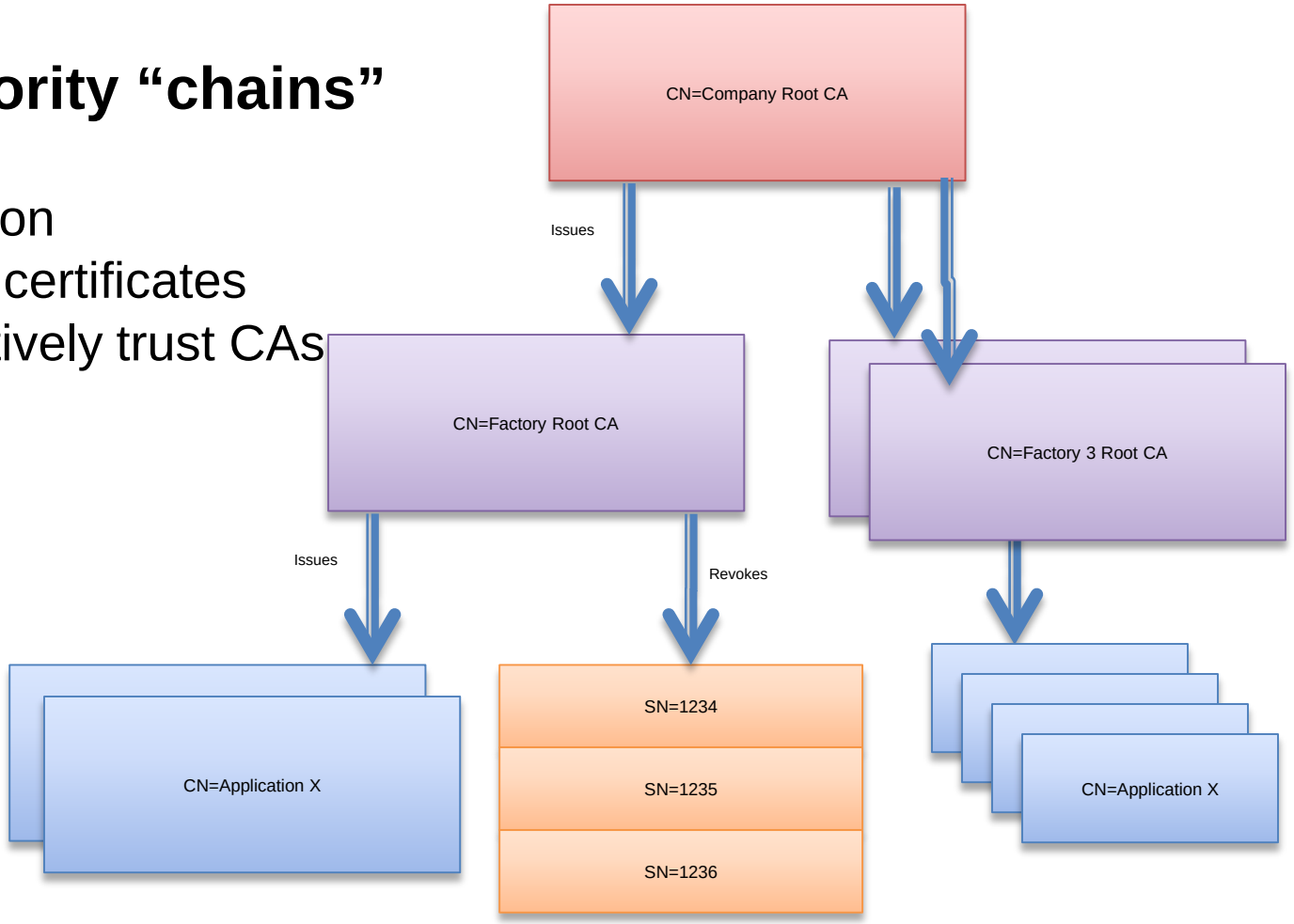
Self-Signed (Manual Process)	Local Certificate Authority (CA)	External Certificate Authority (CA)
Pro: - Low infrastructure cost **Con:** - work intensive - does not scale well	**Pro:** - Medium/Large installations - Local trust - Chaining **Con:** - Medium cost	**Pro:** - Large installations - Multiple CA's **Con:** - Medium/high cost - 3rd Party trust

Topic 2: Certificates

Focus: Scalable Certificate Management

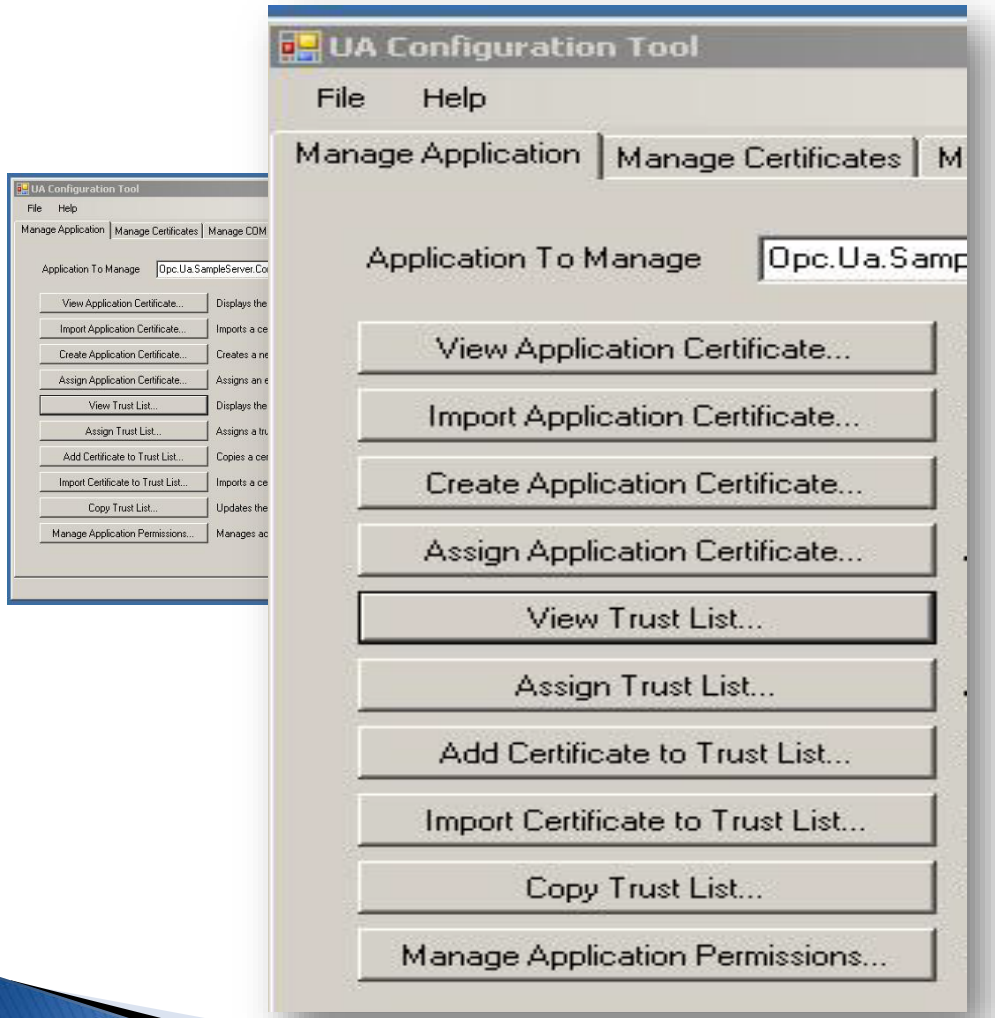
Certificate Authority “chains”

- Create hierarchy
- Improve organization
- CAs issue/revoke certificates
- Applications selectively trust CAs



Topic 2: Certificates

Focus: Example Certificate Management Utility (OPC Foundation)



Available for OPC Foundation members

OPC UA Security

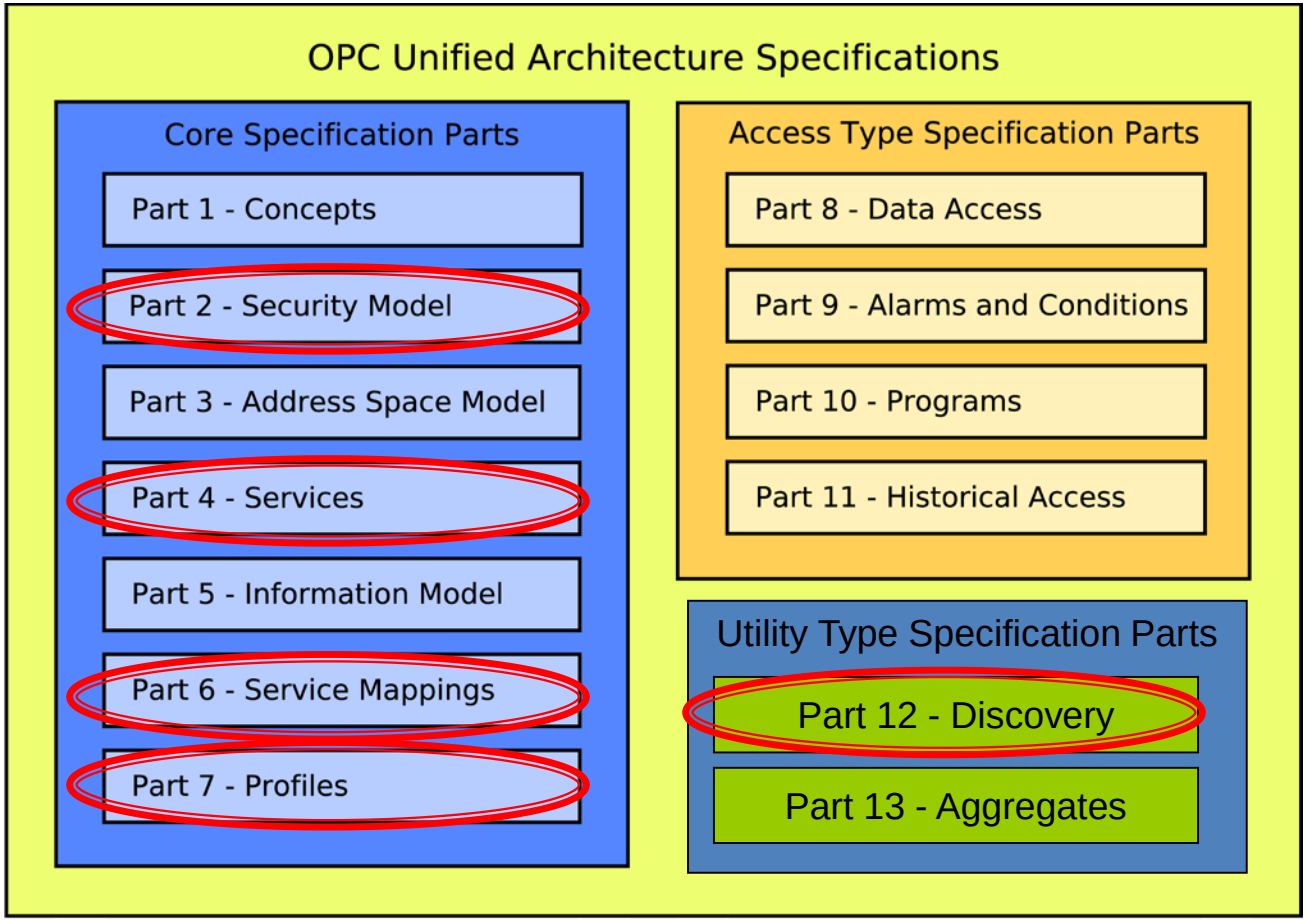
High Level Overview

MatrikonOPC

OPC FOUNDATION

OPC UA Security: Overview

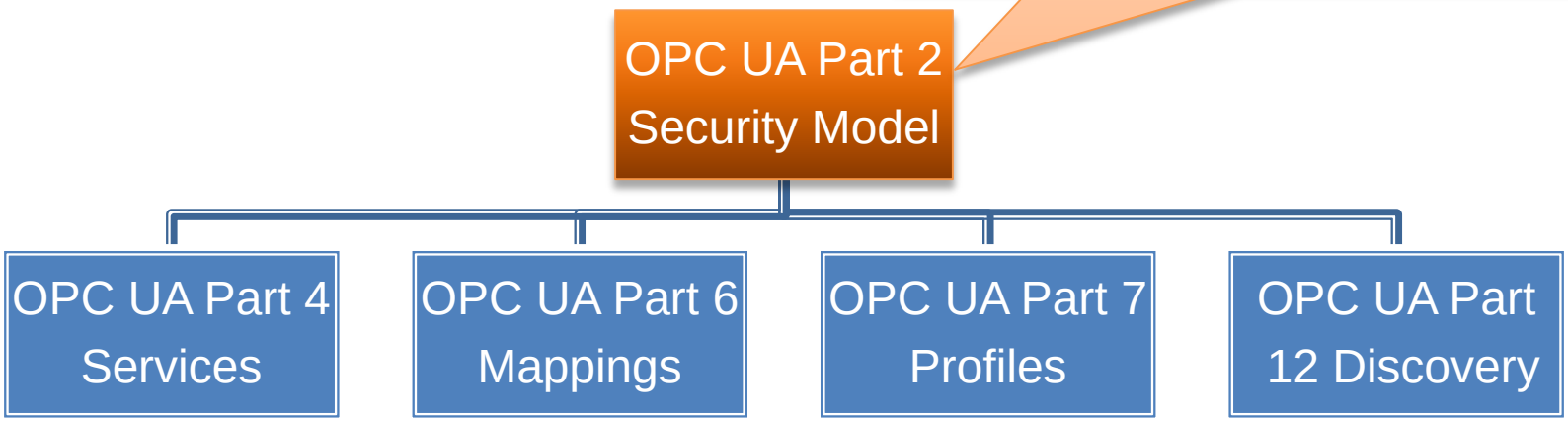
Security built into specification from ground up.



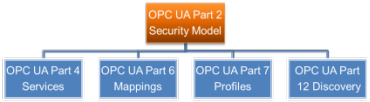
20

OPC UA Security: Highlights

- Objectives, Threats, & Mitigations
- Secure Infrastructures
- Secure Applications



OPC UA Security: Objectives



- **Application Authentication**
  - All application must have a unique Application instance Certificate
  - URI should identify the instance, vendor and product

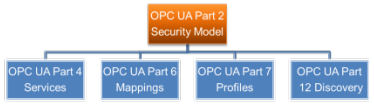
- **User Authentication**
  - Username / password, WS-Security Token or X.509
  - Fits into existing infrastructures like Active Directory

- **User Authorization**
  - Granular control over user actions: read, write, browse, execute

- **Server Availability**
  - Minimum processing before authentication
    - Restricting message size
    - No security related error codes returned
    - …

- **System Auditability**
  - Generating audit events for security related operations

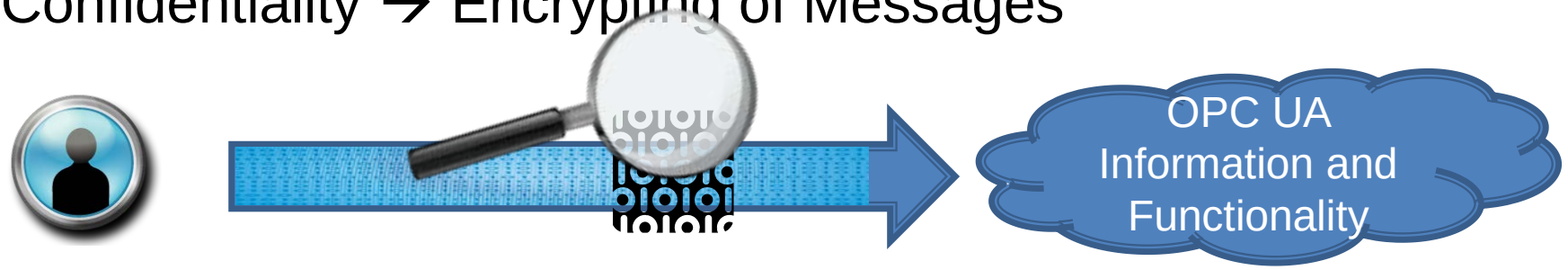
OPC UA Security: Objectives



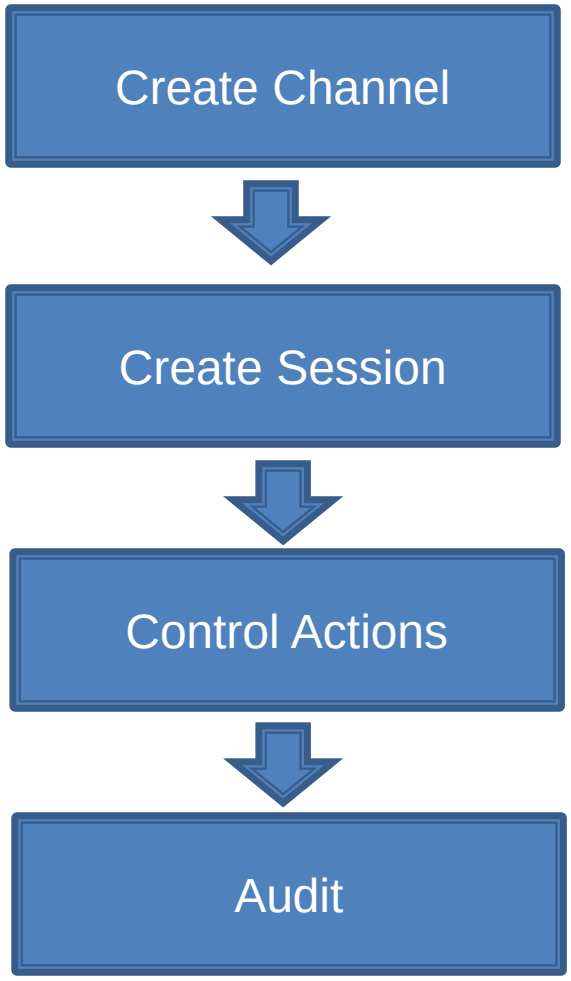
- Availability → Fast & Efficient Authentication

- Integrity → Signing of Messages

- Confidentiality → Encrypting of Messages



OPC UA Security: Step-by-Step



- Trusted applications
- Communication Setup

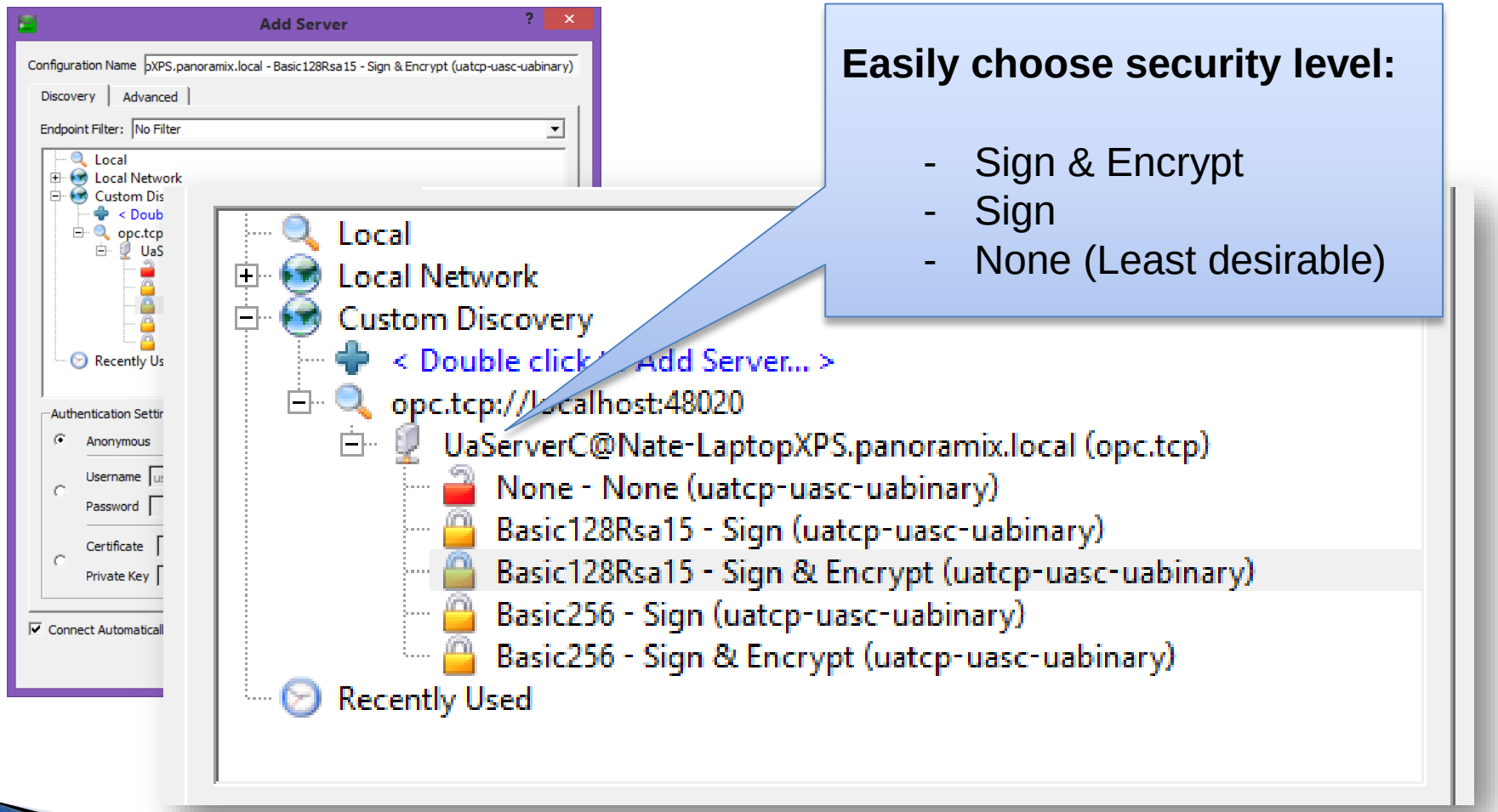
- User Authentication

- User Authorization

- Traceability via logging

OPC UA Security: Channel Creation

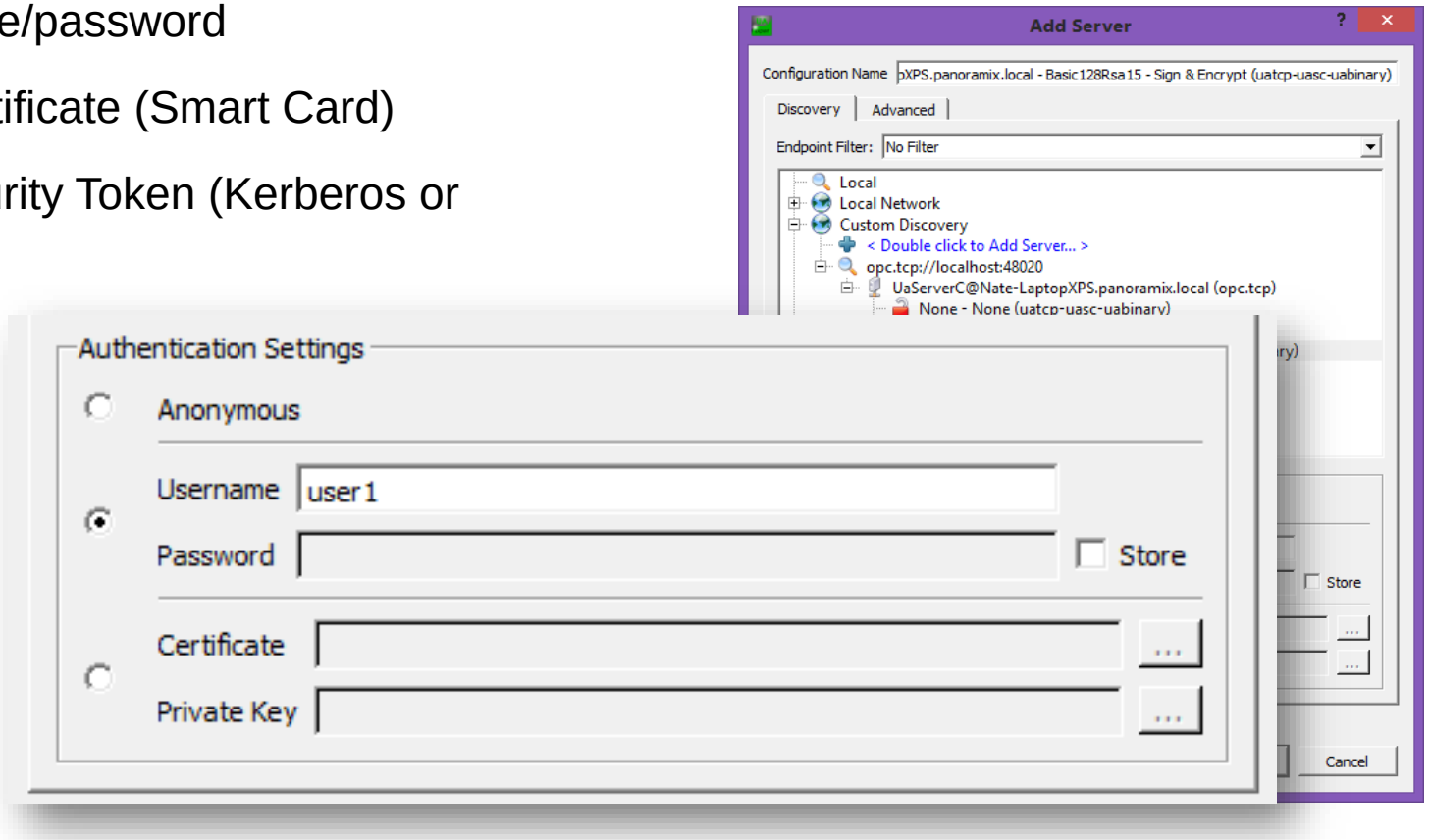
End-User: Select needed security level, then connect. Easy.



OPC UA Security: User Authentication

End-Users: Have a choice on how to best identify self. Easy.

- 3 user login types (Token types):
  1. Username/password
  2. X509Certificate (Smart Card)
  3. WS-Security Token (Kerberos or SAML)

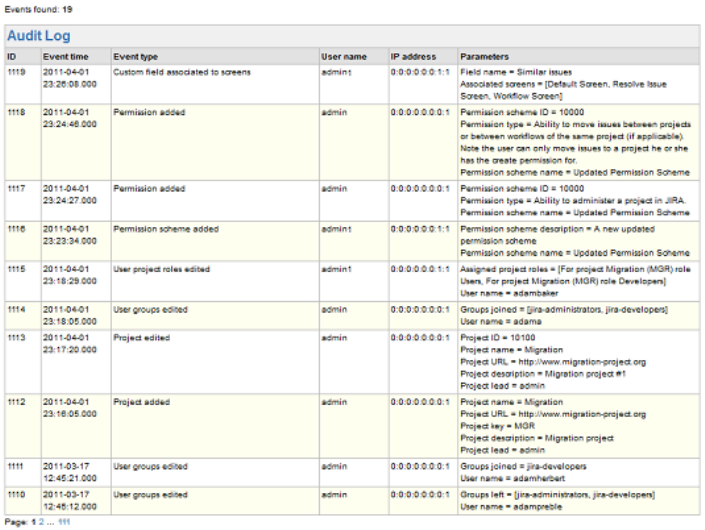


OPC UA Security: User Authorization

Operation	User 1	User 2	User 3
Browse	✓	✗	✓
Read	✓	✗	✓
Write	✓	✗	✗
Execute	✗	✗	✓

OPC UA Security: Auditing

- Log all actions
- Audit regularly as required
- Act on suspicious activity
- Integrate with IDS/IPS



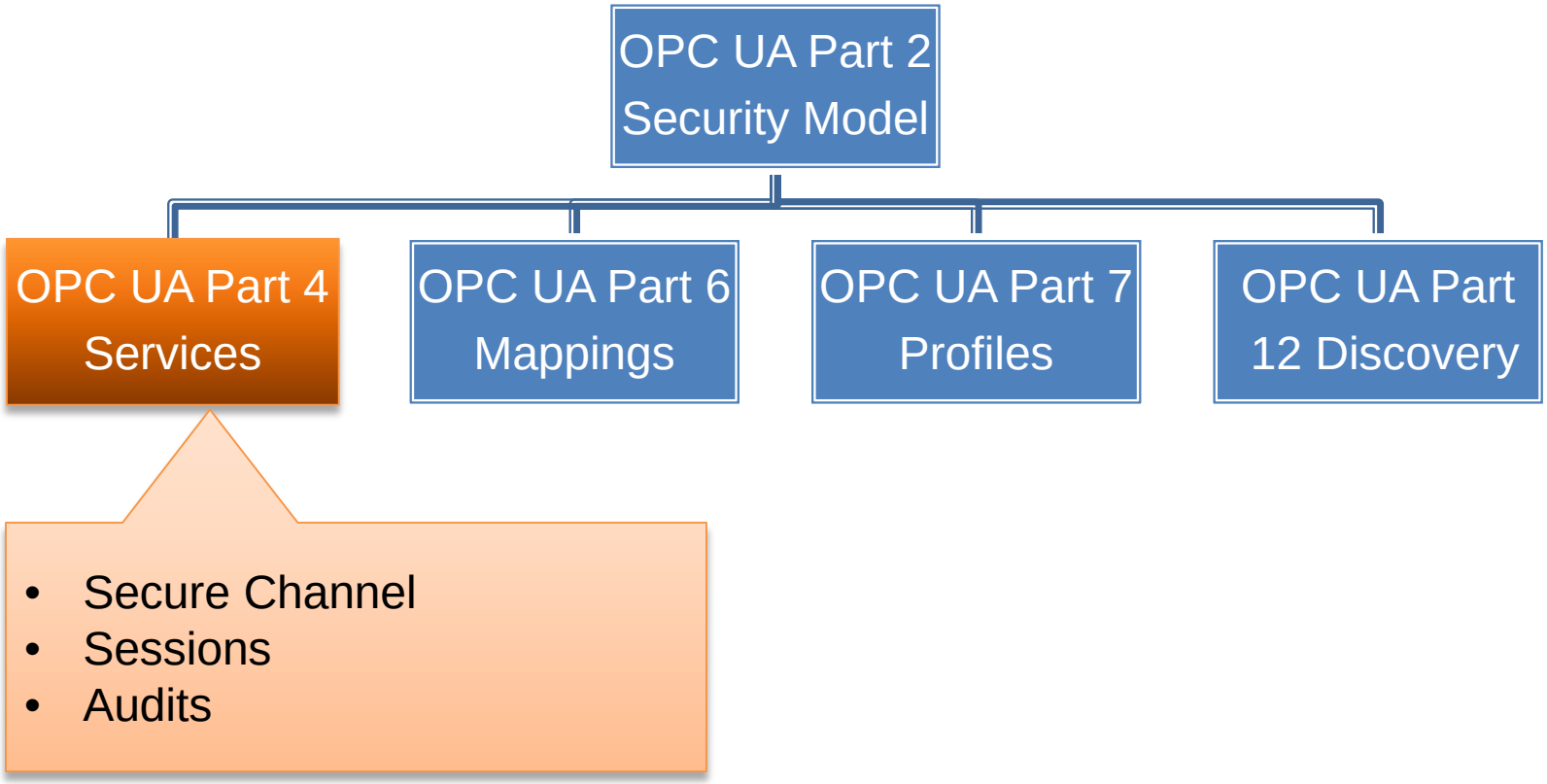
Events found: 19

Audit Log

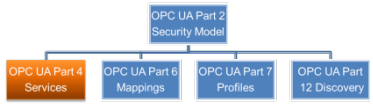
ID	Event time	Event type	User name	IP address	Parameters
1119	2011-04-01 23:26:08.000	Custom field associated to screens	admin1	0:0:0:0:0:0:1:1	Field name = Similar issues Associated screens = [Default Screen, Resolve Issue Screen, Workflow Screen]
1118	2011-04-01 23:24:46.000	Permission added	admin	0:0:0:0:0:0:0:1	Permission scheme ID = 10000 Permission type = Ability to move issues between projects or between workflows of the same project (if applicable). Note the user can only move issues to a project he or she has the create permission for. Permission scheme name = Updated Permission Scheme
1117	2011-04-01 23:24:27.000	Permission added	admin	0:0:0:0:0:0:0:1	Permission scheme ID = 10000 Permission type = Ability to administer a project in JIRA. Permission scheme name = Updated Permission Scheme
1116	2011-04-01 23:23:34.000	Permission scheme added	admin1	0:0:0:0:0:0:1:1	Permission scheme description = A new updated permission scheme Permission scheme name = Updated Permission Scheme
1115	2011-04-01 23:18:29.000	User project roles edited	admin1	0:0:0:0:0:0:1:1	Assigned project roles = [For project Migration (MGR) role Users, For project Migration (MGR) role Developers] User name = adambaker
1114	2011-04-01 23:18:05.000	User groups edited	admin	0:0:0:0:0:0:0:1	Groups joined = [jira-administrators, jira-developers] User name = adama
1113	2011-04-01 23:17:20.000	Project edited	admin	0:0:0:0:0:0:0:1	Project ID = 10100 Project name = Migration Project URL = http://www.migration-project.org Project description = Migration project #1 Project lead = admin
1112	2011-04-01 23:16:05.000	Project added	admin	0:0:0:0:0:0:0:1	Project name = Migration Project URL = http://www.migration-project.org Project key = MGR Project description = Migration project Project lead = admin
1111	2011-03-17 12:45:21.000	User groups edited	admin	0:0:0:0:0:0:0:1	Groups joined = jira-developers User name = adamherbert
1110	2011-03-17 12:45:12.000	User groups edited	admin	0:0:0:0:0:0:0:1	Groups left = [jira-administrators, jira-developers] User name = adampreble

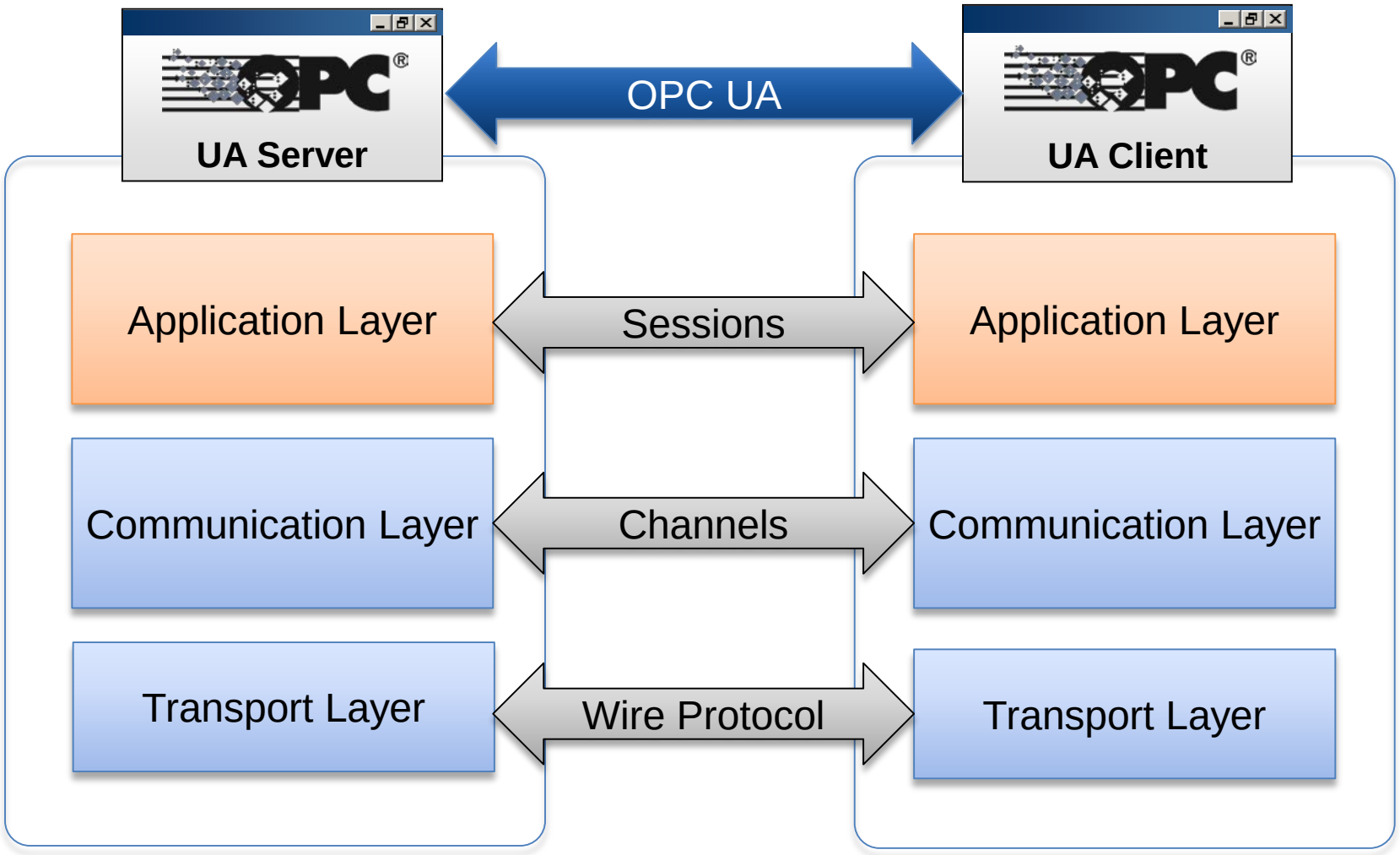
Page: 1 2 ... 111

OPC UA Security: Services

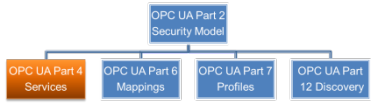


OPC UA Security: Services





OPC UA Security: Services



OPC UA Server

Get Endpoints

End Points & Security Info

OPC UA Client

Certificate Valid?

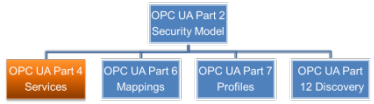
Operation	TRUSTED	NOT TRUSTED
CERT 1	✓	
CERT 2	✓	
CERT 3		✗
CERT X		✗

DSInteroperability

MatrikonOPC

OPC FOUNDATION

OPC UA Security: Services



OPC UA Server

Open Secure Channel

Secure Channel Open

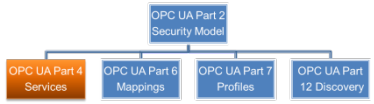
OPC UA Client

Certificate

Valid?

Operation	TRUSTED	NOT TRUSTED
CERT 1	✓	
CERT 2	✓	
CERT 3		✗
CERT X		✗

OPC UA Security: Services



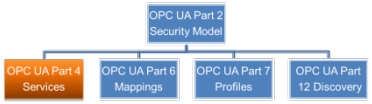
OPC UA Server

Create Session

Session ID

OPC UA Client

OPC UA Security: Services

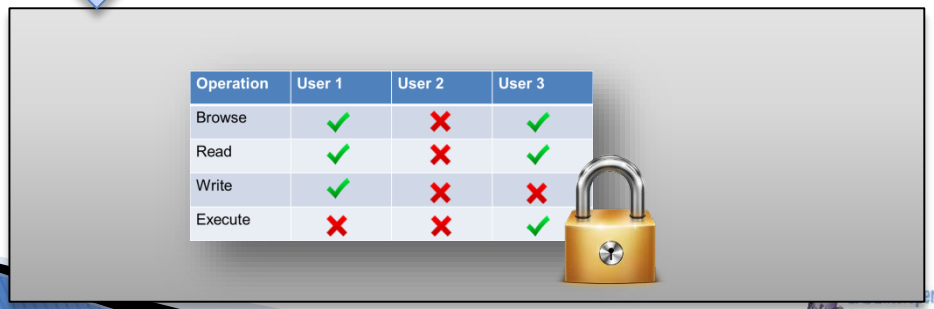


OPC UA Server

Activate Session

Session Activated

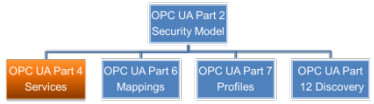
Token Authentication



MatrikonOPC

OPC FOUNDATION

OPC UA Security: Services



Symmetric Security

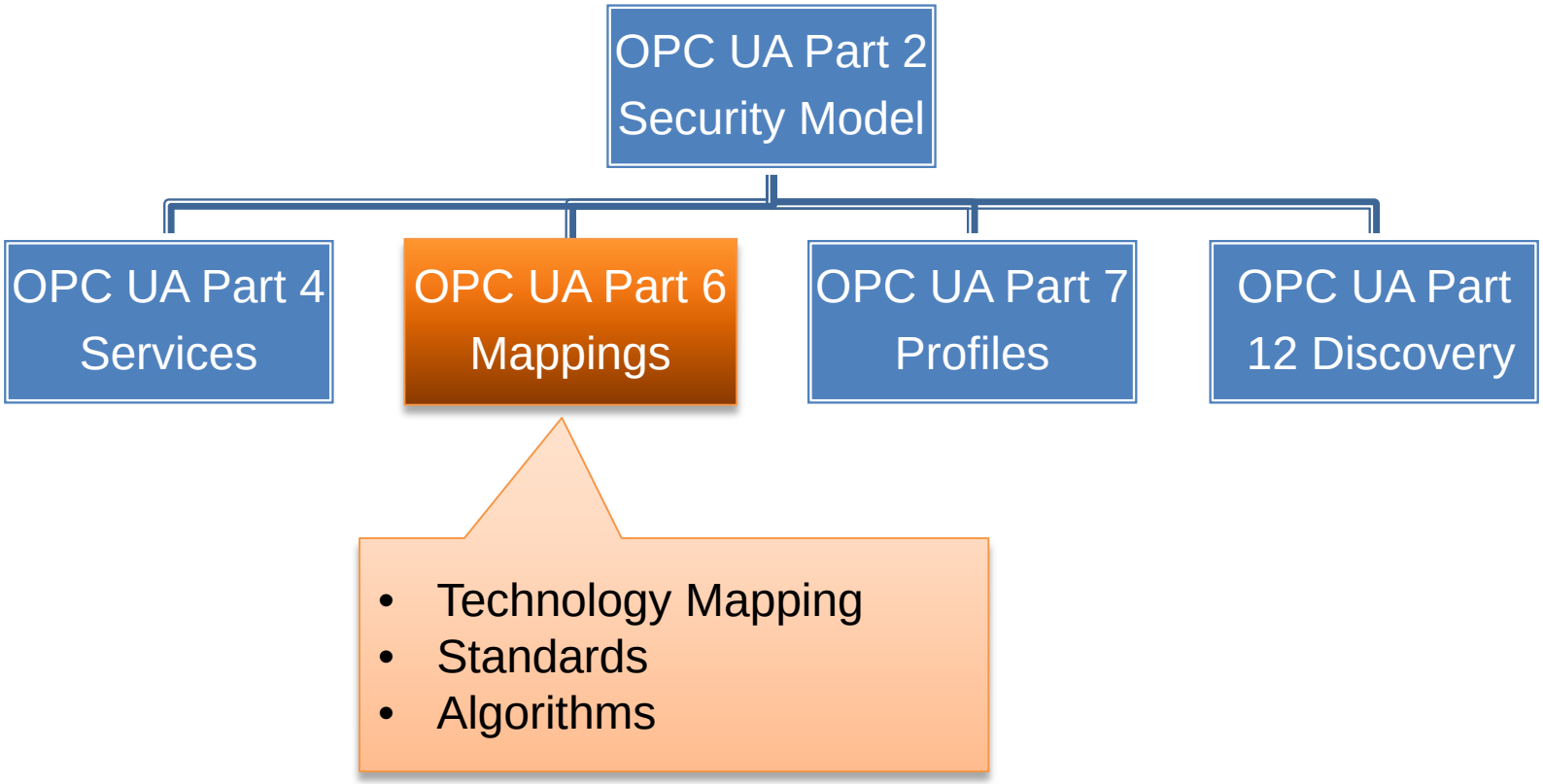
OPC UA Server

Session established!

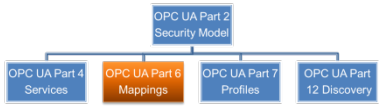
OPC UA Client

Routine Communication

OPC UA Security: Services

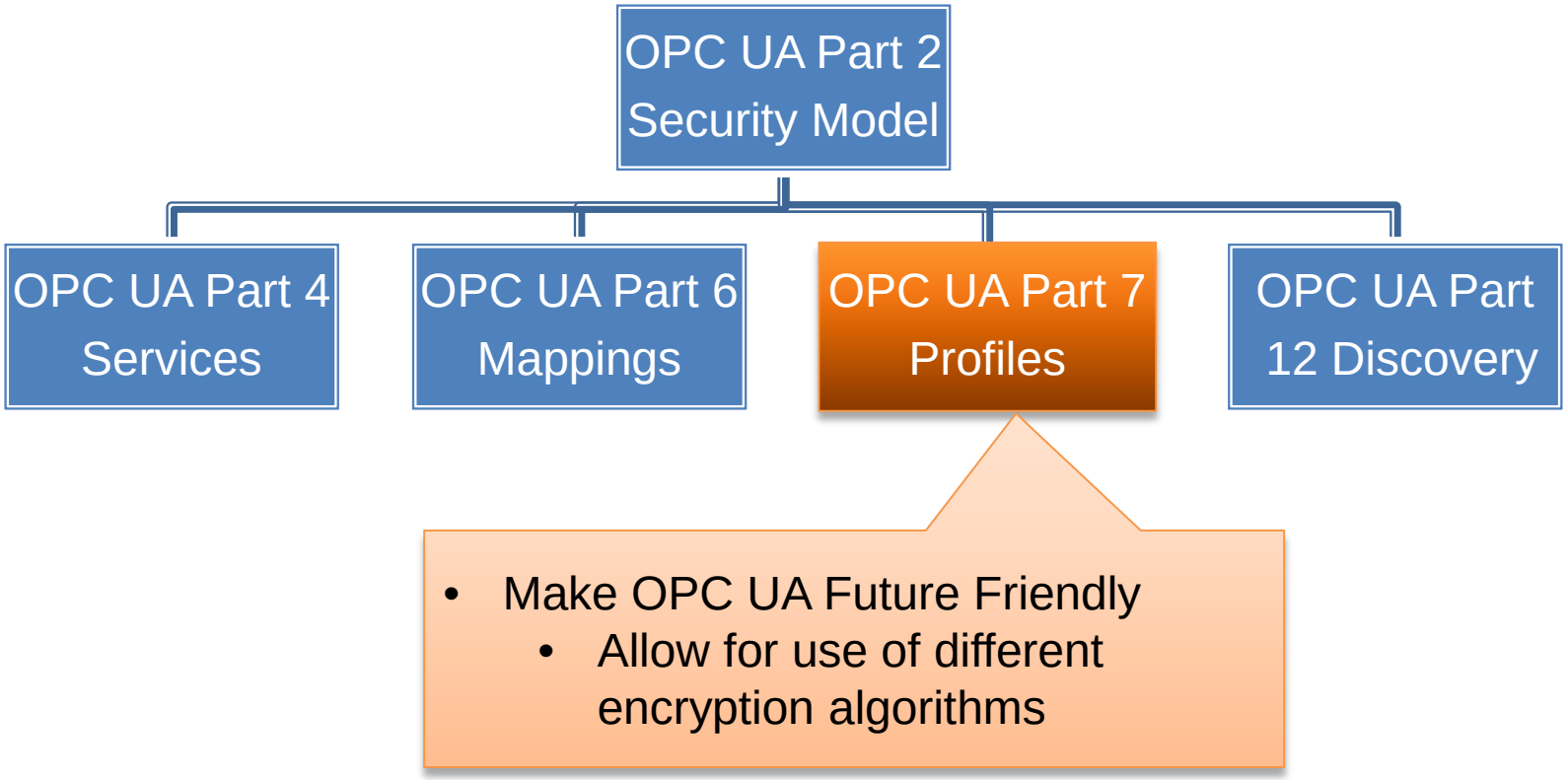


OPC UA Security: Standards Based

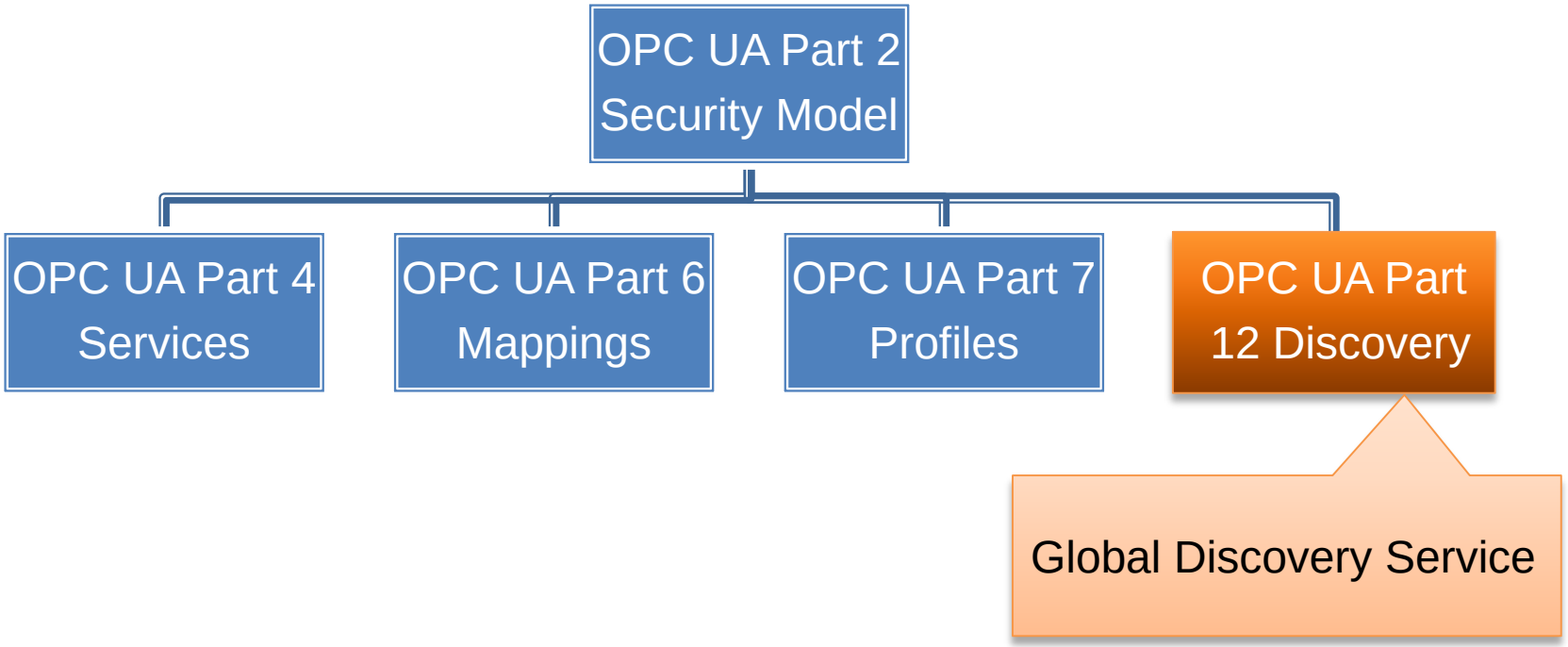


- OPC UA relies upon approved security standards
  - WS-Security
  - WS-Trust
  - WS-Secure Conversation
  - Public Key Cryptography Standards (PKCS)
  - Digital Signature Standard (DSS)
  - Advanced Encryption Standard (AES)

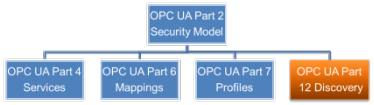
OPC UA Security: Services



OPC UA Security: Configuration



Global Directory Service (GDS)



OPC UA Client | OPC UA Client | OPC UA Client

NEW

GDS Features:

- Certificate creation / management
- Certificate Authority (CA)
- Management of Certificate Revocation Lists (CRL)
- Push / Pull of Certificates / CRL
- Network wide server registry

- Security Config
- Find Servers

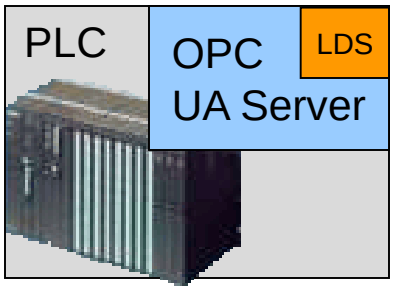
- Security Config
- Register Server

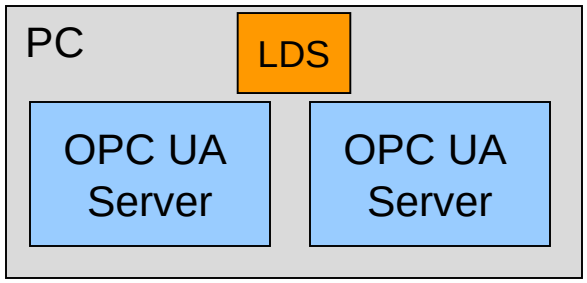
Central Server

GDS (Port:4840)

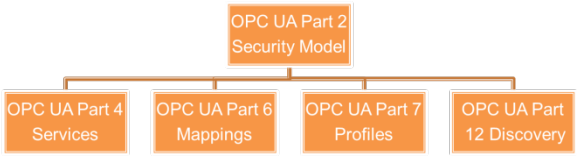
Pull / Push Certificates | CA

List of registered UA Servers





Conclusion



- OPC UA security should be part of a security management system
- OPC UA is secure-by-design addressing security concerns by providing:
  - Authentication of Users, Application instances (Software)
  - Confidentiality and integrity by signing and encrypting messages
  - Availability by minimum processing before authentication
  - Auditability by defined audit events for OPC UA operations
- OPC UA allows different levels of security
- OPC UA certificate management can be retrofitted or new!

Questions?

Nathan Pocock
Technical Director
OPC Foundation

Darek Kominek
Strategic Marketing Manager
MatrikonOPC

Paul Hunkar
Technical Director
DS Interoperability LLC

Thank You

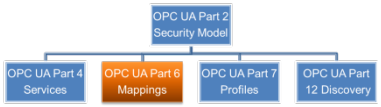
Nathan Pocock
Technical Director
OPC Foundation

Darek Kominek
Strategic Marketing Manager
MatrikonOPC

Paul Hunkar
Technical Director
DS Interoperability LLC

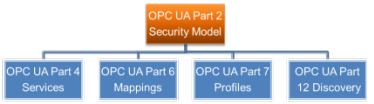
Slide Store Not part of Presentation

OPC UA Security: Technologies



	Main goal(s)	Algorithm(s)/ Standard(s)	Usage
MACs	**Authentication, Integrity**	► **HMAC-SHA1** ► **HMAC-SHA256**	► **Message authentication**
Signature	**Authentication, Integrity**	► **RSA-SHA1**	► **Signing certificates, security handshaking**
Symmetric Encryption	**Confidentiality**	► **AES-128-CBC** ► **AES-192-CBC** ► **AES-256-CBC**	► **Message encryption**
Asymmetric Encryption	**Confidentiality**	► **RSA-PKCS1** ► **RSA-OAEP**	► **Security handshaking**
Key Generation	**Confidentiality**	► **P-SHA1**	► **Session key generation (for message encryption)**
Certificates	**Authentication, Authorization**	► **X.509** ► **X.509v3 (Extensions)**	► **Application authentication, user authentication, key exchange**

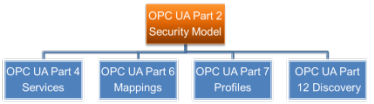
Subject Names



- Subject names identify the holder of the certificate
  - Structured value with multiple fields
  - Common Name (CN)
  - Organization (O)
  - Country (C)
  - Domain (DC)
- String syntax for display purposes
  - CN=UASampleServer,O=MyCompany,DC=MyComputer
- Subject names are not guaranteed to be unique
  - Thumbprints better choice when a unique id is required
  - Thumbprint is the SHA1 digest of the DER encoded certificate

46

Subject Alternate Names



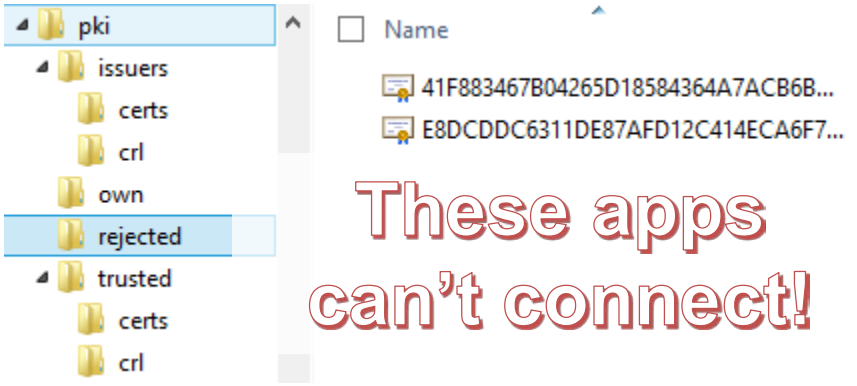
- Specify additional names for the certificate
  - Used for validation purposes
  - Domain Name, IP Address, Application URI
- The alternate name binds the certificate to a context
  - Domain/IP address must match the host in the Endpoint URL
  - The URI must match the URI in the Application Description
- Helps prevent spoofing

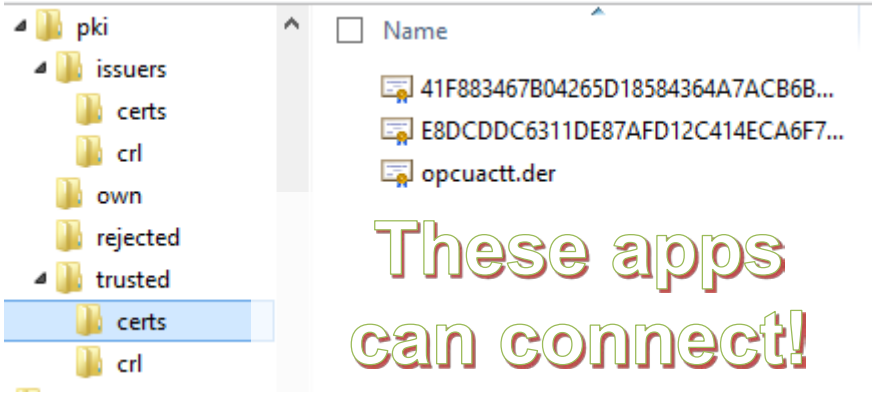
47

Administrator Perspective: Certificates

Certificates | Authorities | Auditing

- Certificates stored in a “trust list”:
  - File structure
  - Windows Certificate Store
- Application’s certificates must be trusted, to connect
- Move certificates from “rejected” to “trusted”





DSInteroperability

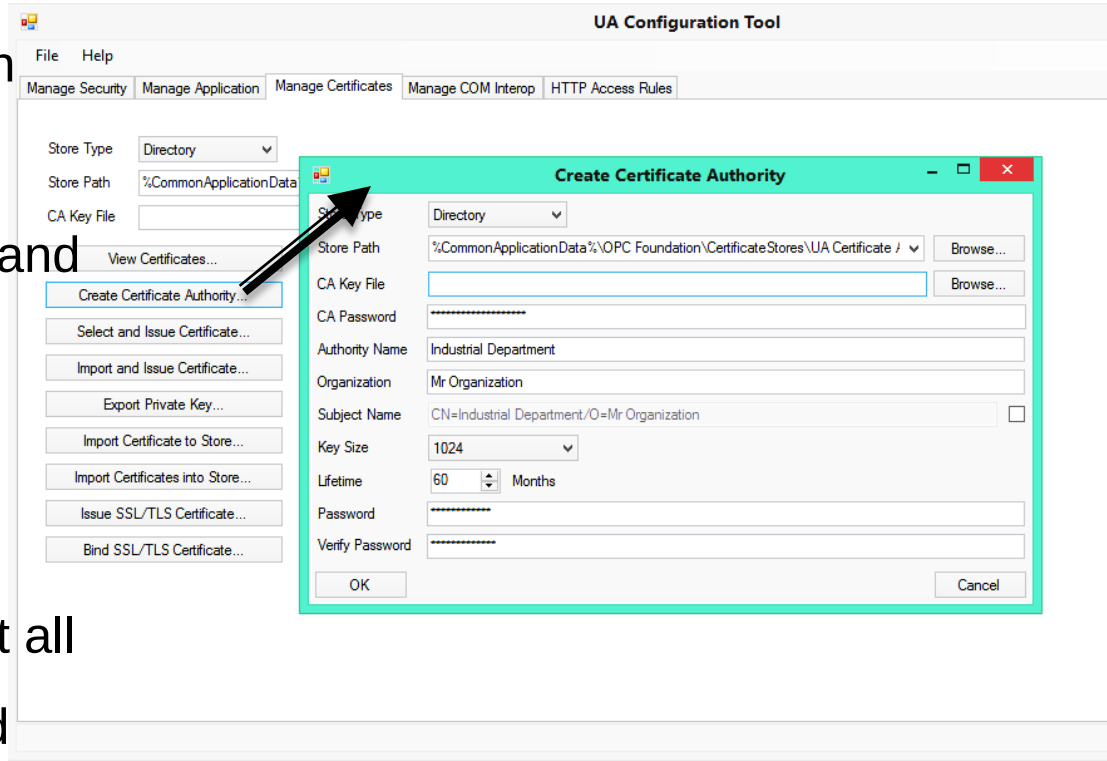
MatrikonOPC

OPC FOUNDATION

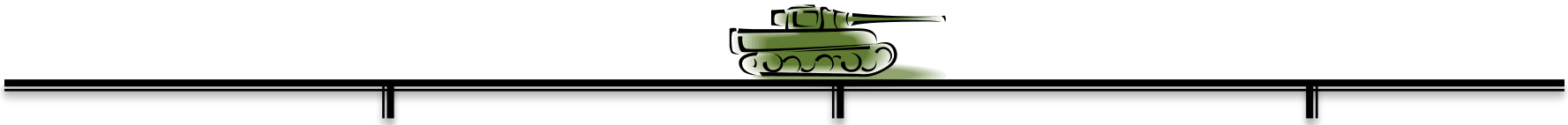
Administrator Perspective: Certificates

Certificates | Authorities | Auditing

- Certificate stores scale poorly in large environments.
- Administrative burden of trusts and no-trusts etc.
- Certificate Authorities (CA) can issue certificates.
- Trust the CA, and implicitly trust all apps who certificate was issued

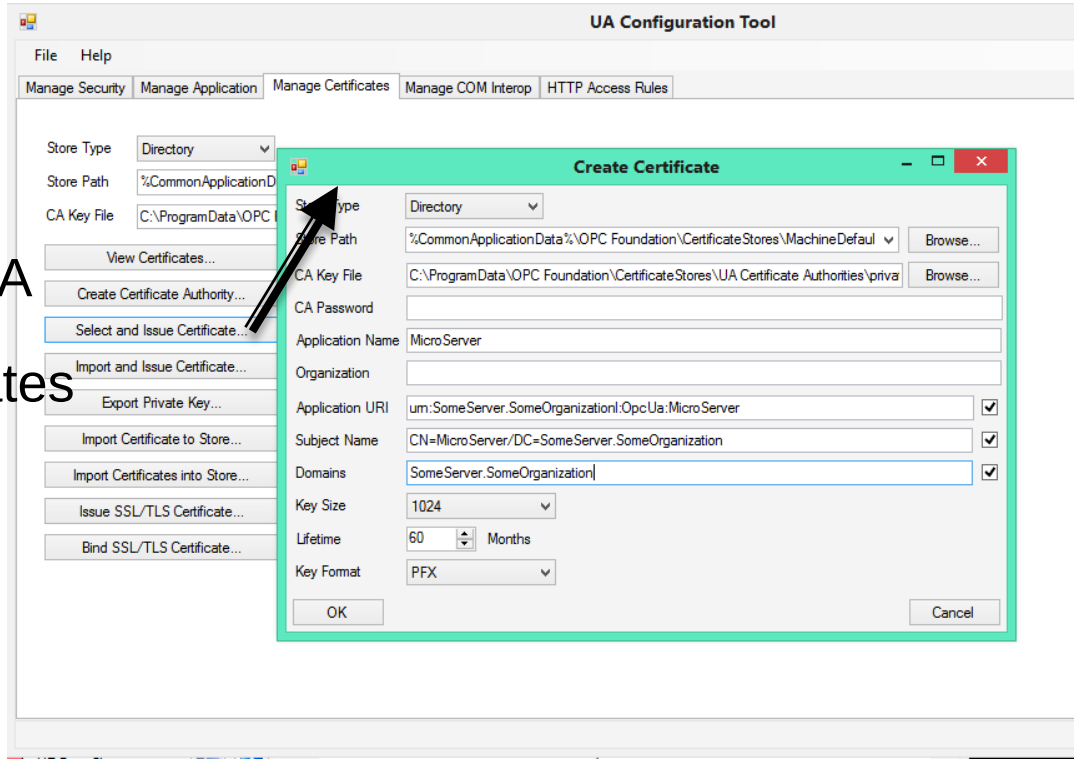


Administrator Perspective: Certificates

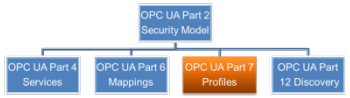


Certificates | **Authorities** | Auditing

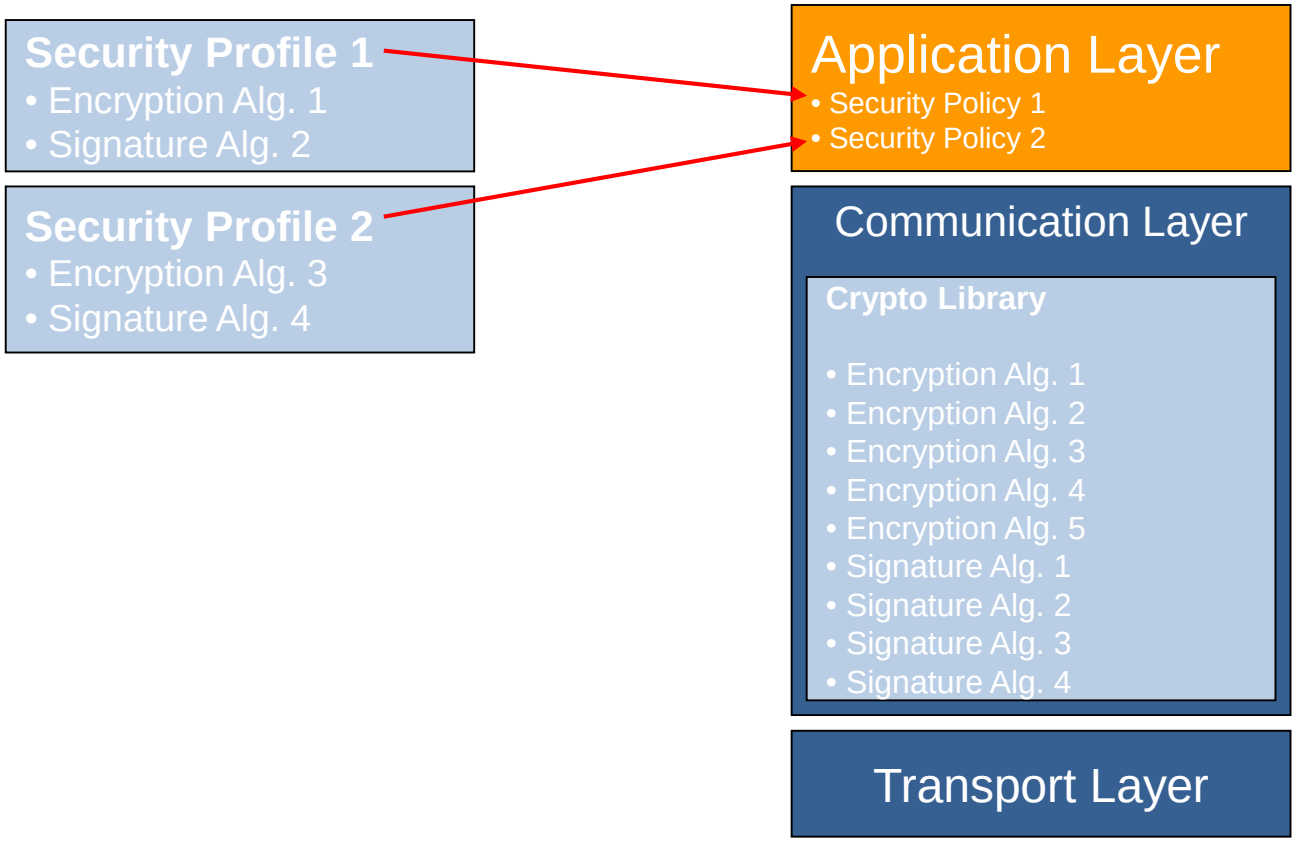
- CA issues App Certificate
- Easier to maintain
- Organization create have >1 CA
- CA's can also "revoke" certificates that have been compromised.



OPC UA Security: Flexibility

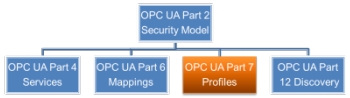


- Flexibility and Extensibility
  - Profiles and Policies
    - Profiles list various functionalities of UA applications

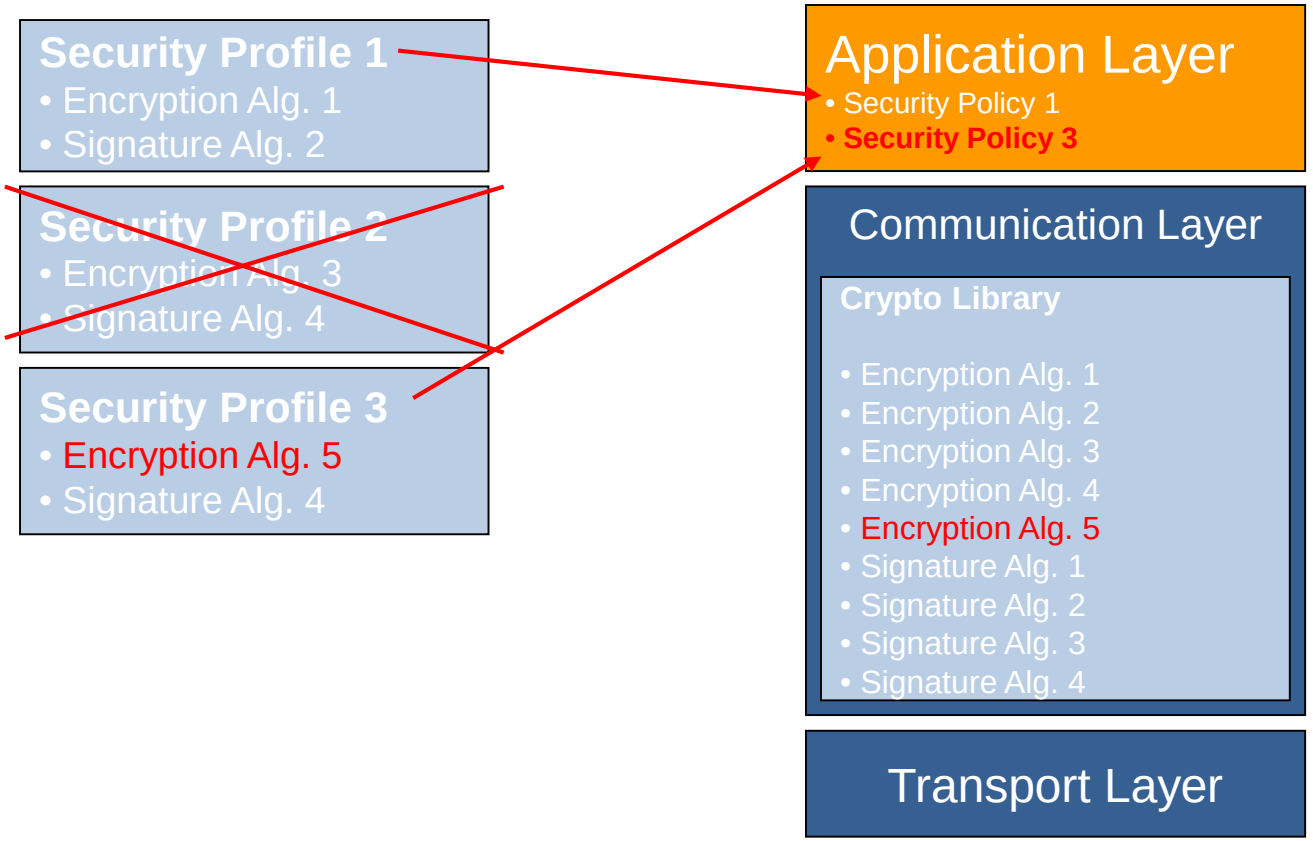


51

OPC UA Security: Flexibility

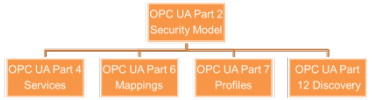


- Flexibility and Extensibility
  - Profiles and Policies
    - Profiles list various functionalities of UA applications



52

Provisioning / Setup - Server



MyServer

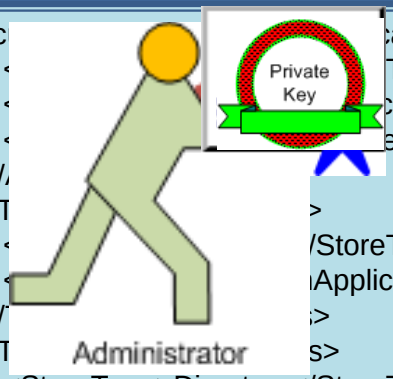
EndPoints

Security Policies

User Token Policies

Security Configuration

MyDevice



Must be kept secure

Password Protect

Provisioning / Setup - Client