OPC UA security management with GDS

OPC UA Application Discovery
OPC UA PKI Certificate Management
User Management
PubSub Security Key Management
Unified Automation SDK Products

> Largest OPC UA SDK & Toolkit Vendor
> All Languages available
> Scaling on all Targets

High Performance SDK

.NET SDK
JAVA SDK
C++ SDK
ANSI C SDK

bare metal, FreeRTOS, Euros, QNX, embedded Linux, VxWorks, WinCE, Win32, Win64, Linux, Solaris
Agenda

> PKI / Certificate Management Basics

> Centralized Security Configuration

> GDS from Unified Automation

> Future GDS Features
Application Authentication (PKI)

Can I trust my communication partner?

Client
- Trust List
- Public Key

Server
- Trust List
- Public Key

Client
- Key
- Server

Server
- Key
- Client

© Unified Automation GmbH – All rights reserved.
Message Privacy (PKI)

Can I make information private?

Client

Trust List

Encrypt

Decrypt

Server

Trust List

Public Key

Private Key
Message Integrity (PKI)

Can I check whether information has been changed?

Client
- Trust List
  - Sign
  - Check Signature

Server
- Trust List
  - Sign
  - Check Signature

Public Key
- Client
- Server

Private Key
- Client
- Server
Agenda

> PKI / Certificate Management Basics

> Centralized Security Configuration

> GDS from Unified Automation

> Future GDS Features
Enhanced Application Authentication

Client A

Client B

Client C

Server

Trust List

© Unified Automation GmbH – All rights reserved.
CA Based Application Authentication

Client A

Client B

Client C

CA

Sign

Server

Certificate Authority
CA Based Application Authentication

- Client A
- Client B
- Client C

CA

Server

Trust List

Trust
CA Based Application Authentication

- Client A
- Client B
- Client C

CA

Server

Trust List

© Unified Automation GmbH – All rights reserved.
CA Based Application Authentication

- Client A
- Client B
- Client C

CA

CRL

Server

Trust List
Global Discovery Server (GDS)

GDS as Certificate Authority
- Central CA
- Full OPC UA Server
- CertificateDirectoryType is interface with UA Methods

CertificateDirectoryType
- StartSigningRequest
- StartNewKeyPairRequest
- FinishRequest
- GetCertificateGroups
- GetTrustList
- GetCertificateStatus
Application Setup

- Application registration with GDS during setup
- Signing of application certificate
- Setup requires security
GDS – Application Security Update – Pull

**Pull**
- Applications are clients for GDS

**Application Security Update**
- Frequent update of trust list and CA revocation list
- Update requires security

![Diagram](image)
GDS – Application Security Update – Push

- Client gets trust list from GDS
- Server implements `ServerConfigurationType` and `TrustListType`
- Client updates server trust list with latest setting from GDS
Global Discovery Server (GDS)

Find Servers

Application Registration
Initial Configuration/Certificate Generation
Update Trust List/Revocation Lists

OPC UA Client

OPC UA Client

OPC UA Client

OPC UA Server

OPC UA Server

OPC UA Server

OPC UA Server

Central Administration

GDS

Pull

Pull or Push

Pull/Push Certificates

List of registered UA Servers

CA
Agenda

> PKI / Certificate Management Basics

> Centralized Security Configuration

> GDS from Unified Automation

> Future GDS Features
Unified Automation GDS Components

GDS Tooling
- GDS Administration GUI
- GDS Client Proxy

GDS Administration
- GUI
- Client Proxy

OPC UA Client
- Server
- Application

Managed OPC UA Applications

Unified Automation GDS Central Component

GDS Server
- CA
- UA App Registry

GDS Client
- Certificate DirectoryType
- Server ConfigurationType

Pull
- DirectoryType
- Certificate

Push
- Server ConfigurationType
- Certificate
PULL configuration Server / Client Applications

Application Setup
- Application registration with GDS during setup requires GDS admin rights
- Signing of application certificate
- Setup requires security

Application Security Update
- Frequent update of trust list and CA revocation list
- Update requires security
PUSH with GDS Client Proxy

GDS Tooling

GDS Client Proxy

Unified Automation GDS Central Component

GDS Server

Certificate DirectoryType

CA

UA App Registry

GDS Client

DirectoryType

Update TrustList

GetTrustList

OPC UA Server

ServerConfigurationType TrustListType

Used if OPC UA server is not directly reachable by central GDS client
Agenda

> PKI / Certificate Management Basics

> Centralized Security Configuration

> GDS from Unified Automation

> Future GDS Features
User Authorization with GDS / JWT

- JWT = JSON Web Token

Central Server
  - GDS
    - User Management
    - Authorization ServiceType
  - Admin Client

OPC UA Client
  - GetEndpoints() returns Token Provider

OPC UA Server
  - RequestAccessToken
  - ActivateSession()
  - Signature check with public key of Token Provider

Trust Token Provider
Security Key Server for OPC UA PubSub

Publisher

Security Key Server

DataSet

Registration

Messages

Transport

Subscribers

Security Key Server

GetSecurityKeys

Message Oriented Middleware

DataSet Metadata

Directory

Query

Exchanged independent of messages

© Unified Automation GmbH – All rights reserved.
Unified Automation GDS – Feature Complete

**Managed OPC UA Applications**

- OPC UA Client
- OPC UA Server
- OPC UA Publisher
- OPC UA Subscriber

**Unified Automation GDS Central Component**

- GDS Server
- CA
- UA App Registry
- User Management
- Security Key Server

**DirectoryType**

- Certificate

**Certificate DirectoryType**

- Authorization ServiceType

**Authorization ServiceType**

- PubSubKey ServiceType

- Security Key Server