Information Revolution 2014

OPC UA Discovery

Matthias Damm
Executive Director ascolab GmbH
Consultant Unified Automation GmbH
matthias.damm@ascolab.com
Agenda

> OPC UA Discovery and Security Configuration

> Network Wide Discovery

> Centralized Security Configuration
OPC UA Server Initial Configuration

PC 1: MyServer

OPC UA Server

- opc.tcp://MyServer:48001
  - Basic128Rsa15
  - SignAndEncrypt
  - Username/Certificate

- opc.tcp://MyServer:48001
  - Basic256
  - SignAndEncrypt
  - Username

Endpoints
- Endpoint URL
- Security Policy
- Message Security Mode
- User Token Type

Server configuration by administrator

Trust List
List of trusted application instance certificates

Rejected List
List of rejected application instance certificates

Application Instance Certificate
Public and Private Key
Generated by server or provided by admin
Local Discovery Server (LDS) – Registration

Servers register with LDS

Registration requires security
OPC UA Client Configuration

- **PC 2: MyClient**
  - **OPC UA Client**
  - **Server Connection List**
  - **Trust List**

**List of selected Server Endpoint(s)**

**Trust List**
List of trusted application instance certificates

**Application Instance Certificate**
- Public and Private Key
- Generated by client or provided by admin
Local Discovery Server (LDS) – Discovery

Client need to know server host

**FindServers**
- Called on known LDS port 4840
- Returns a list of servers

**GetEndpoint**
- Called on server
- Returns server security config
Connection Configuration

PC 2: MyClient

OPC UA Client

Server Connection List

Trust List

PC 1: MyServer

OPC UA Server

opc.tcp://MyServer:48001
- Basic256
- SignAndEncrypt
- Username/Certificate

opc.tcp://MyServer:48001
- Basic128Rsa15
- SignAndEncrypt
- Username

UA Call to get Endpoints

© Unified Automation GmbH – All rights reserved.
Connection Configuration

Manual accept on client
Connection Configuration

PC 2: MyClient

OPC UA Client

- Server Connection List
  - opc.tcp://MyServer:48001
    - Basic256
    - SignAndEncrypt
    - Username

PC 1: MyServer

OPC UA Server

- opc.tcp://MyServer:48001
  - Basic256
  - SignAndEncrypt
  - Username

Client configured
Connection Configuration

Client connect rejected
Connection Configuration

Manual accept on Server
Connection Configuration

PC 2: MyClient
OPC UA Client
- Server Connection List: opc.tcp://MyServer:48001
- Trust List:
  - Basic256
  - SignAndEncrypt
  - Username

PC 1: MyServer
OPC UA Server
- opc.tcp://MyServer:48001
- Trust List:
  - Basic128Rsa15
  - SignAndEncrypt
  - Username/Certificate

Secure Connection
Agenda

- OPC UA Discovery and Security Configuration
- Network Wide Discovery
- Centralized Security Configuration
Ad-Hoc Discovery/Multicast DNS (mDNS)

**Features provided:**
- Host name resolution without central DNS server
- Find OPC UA servers with feature list in local network

**Advantage:**
No central infrastructure required

**Limitation:**
Works only in local subnet
LDS-ME – Announcing Servers

LDS-ME on Server
- Servers are registered with local LDS
- **LDS with Multicast Extension (LDS-ME)** announces servers

Embedded Server
- Announce themselves in the network
LDS-ME on Client

- LDS-ME provides cache of servers announced in the network
- Client can access list through OPC UA Service from LDS
LDS-ME – Discovery

FindServersOnNetwork
- Called on local LDS
- Returns a list of servers in the network

GetEndpoint
- Still called on server – returns server security configuration
Global Directory Service (GDS)

GDS
- Central discovery server
- Full OPC UA Server
- DirectoryType is discovery interface with UA Methods

DirectoryType
- RegisterApplication
- UpdateApplication
- UnregisterApplication
- QueryServers
GDS – Server Registration

Server Setup
- Server registration with GDS during setup
- Registration requires security
GDS – Client Discovery

Client Discovery
- QueryServers used to find servers
- Filter (LIKE string filter) for
  - ApplicationName/ApplicationURI
  - ProductURI
  - Server Capabilities

Central Server
- List of registered UA Servers
  - DirectoryType
GDS – How to Find GDS

Client Discovery
- Local LDS-ME delivers GDS location (capability filter)
- QueryServers used to find servers
Server Discovery URL for GetEndpoints

- **Server Discovery URL from**
  - GDS QueryServers
  - LDS FindServers
  - LDS-ME FindServerOnNetwork

**GetEndpoints**
Discovery – Big Picture

**LDS-ME – mDNS**
- Ad-Hoc discovery
- Local Subnet

**GDS**
- Network wide discovery
- Security can be applied
Agenda

> OPC UA Discovery and Security Configuration

> Network Wide Discovery

> Centralized Security Configuration
Global Directory Service (GDS)

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

CertificateDirectoryType
- RequestCertificate
- SignCertificate
- RenewCertificate
- CheckRequestStatus
- GetTrustList
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
Push

- Client gets trust list from GDS
- Server implements TrustListType
- Client updates server trust list with latest setting from GDS
Global Directory Service (GDS)

- OPC UA Client
  - Pull
- OPC UA Client
  - Pull
- OPC UA Client
  - Pull

Central Administration

GDS

- Pull/Push Certificates
- List of registered UA Servers

Find Servers

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

Pull or Push

OPC UA Server

© Unified Automation GmbH – All rights reserved.
Global Directory Service (GDS)

GDS is OPC UA wrapper around any directory or CA
Summary

> Discovery used to
  > Find servers
  > Get security configuration

> Discovery options
  > Discover on known port 4840 of a network node
  > Use mDNS for ad-hoc discovery in local network
  > Use GDS as central discovery server

> GDS for central certificate management