Information Revolution 2014

OPC UA Discovery

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

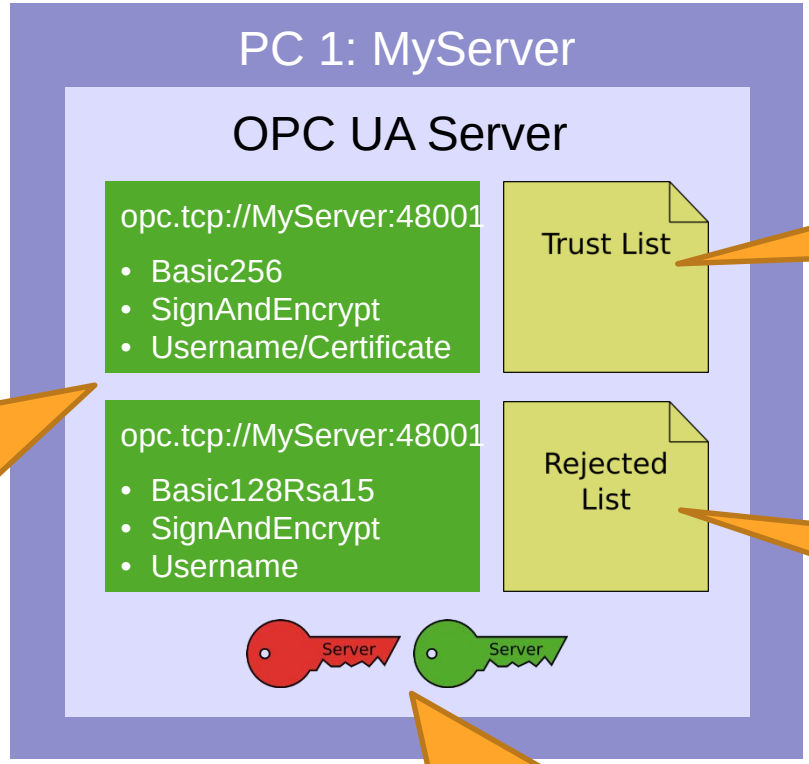
Agenda

> OPC UA Discovery and Security Configuration

> Network Wide Discovery

> Centralized Security Configuration

OPC UA Server Initial Configuration



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

Server configuration by administrator

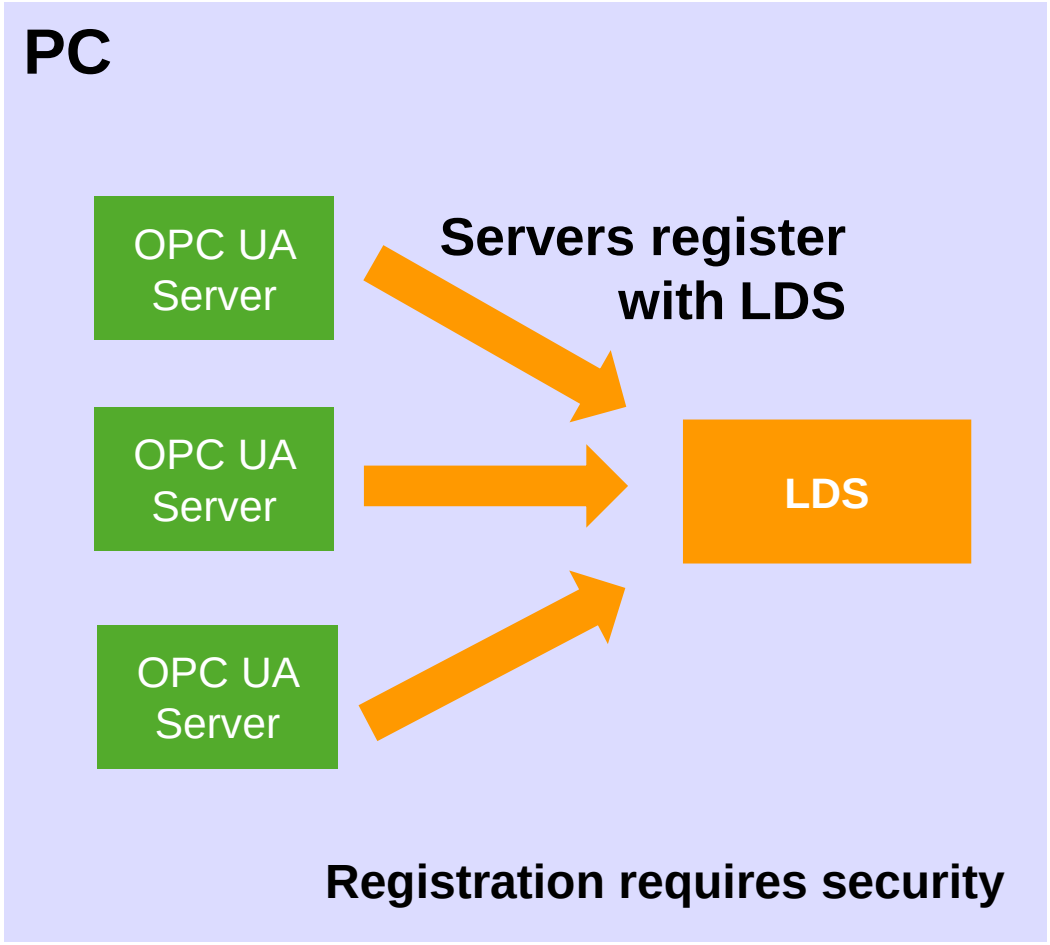
Trust List
List of trusted application instance certificates

Rejected List
List of rejected application instance certificates

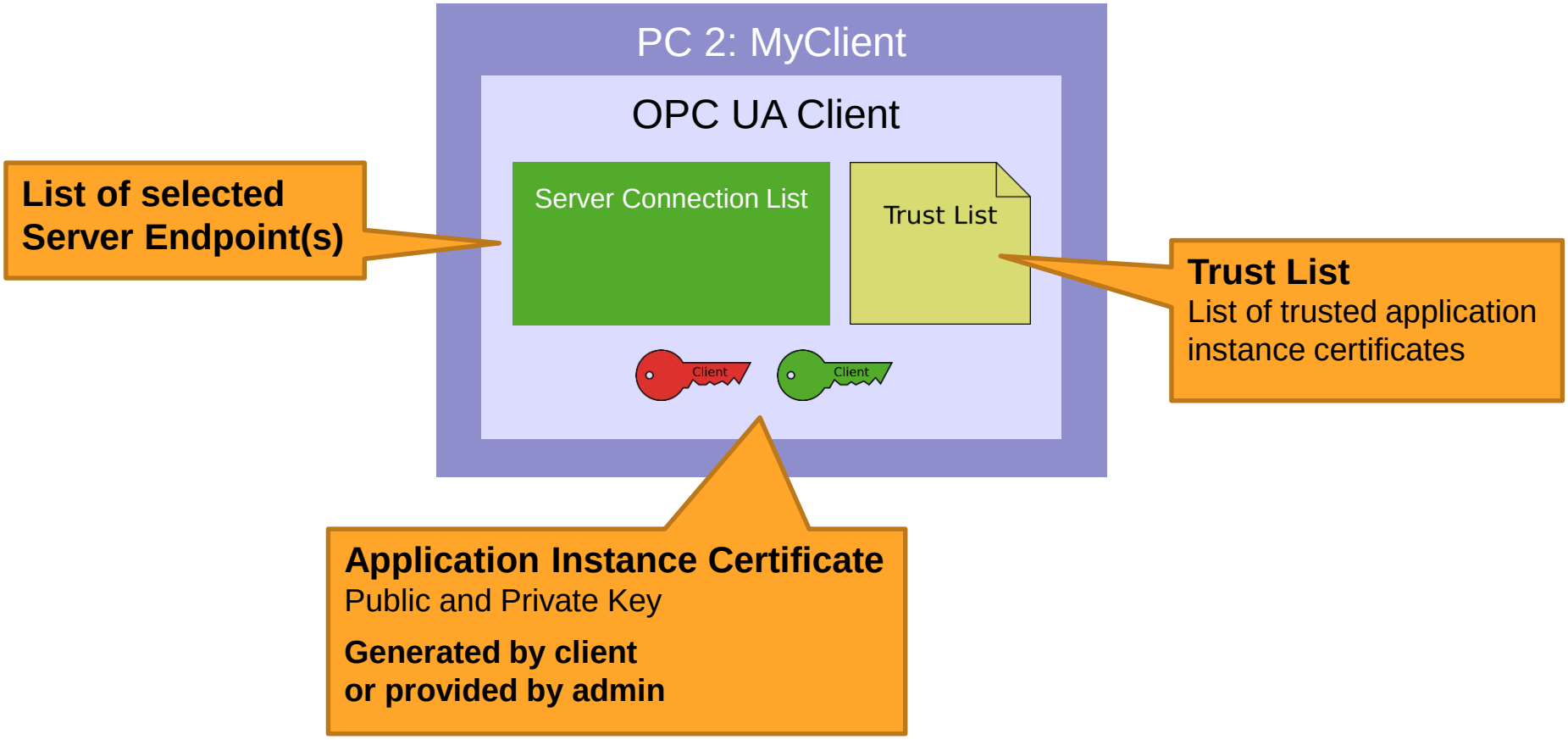
Application Instance Certificate
Public and Private Key

Generated by server or provided by admin

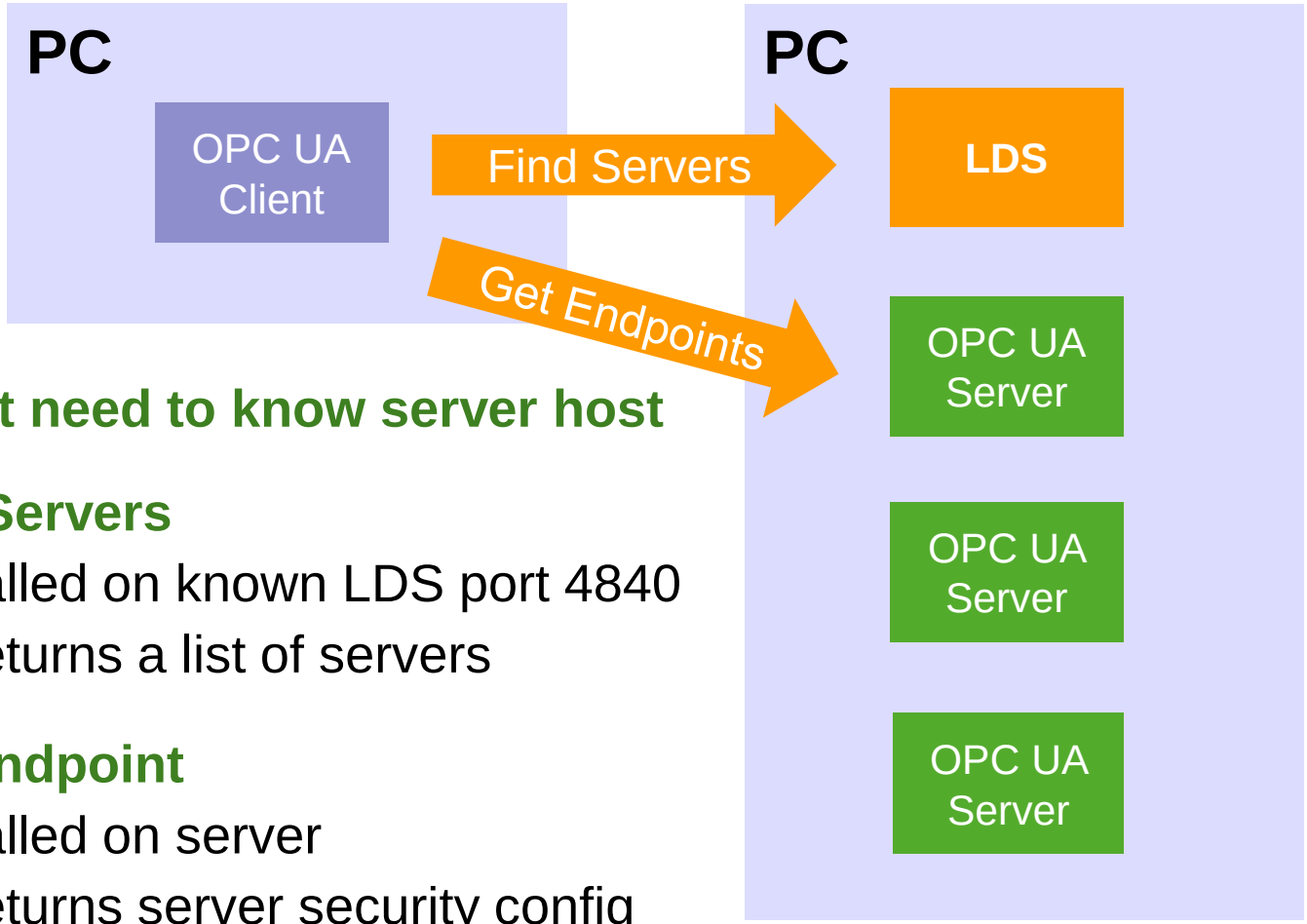
Local Discovery Server (LDS) – Registration



OPC UA Client Configuration



Local Discovery Server (LDS) – Discovery



Client need to know server host

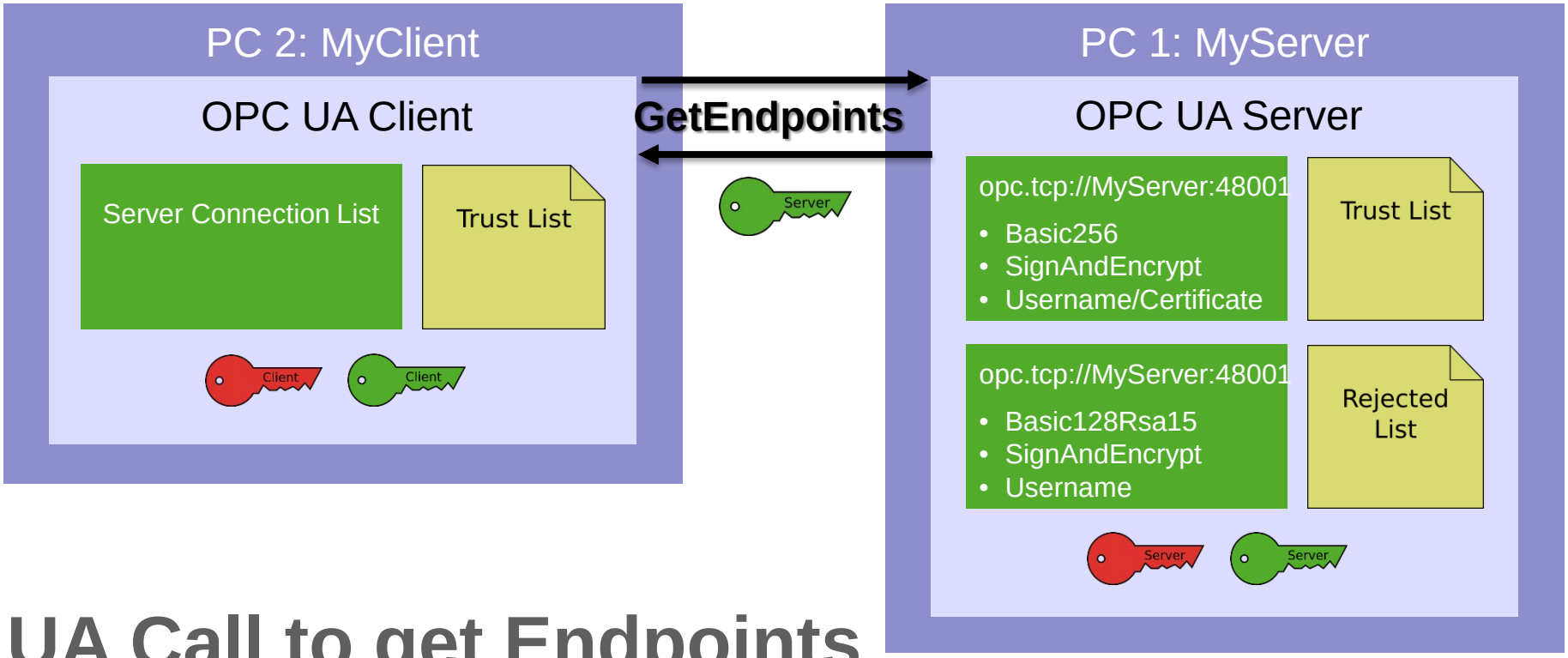
FindServers

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

GetEndpoint

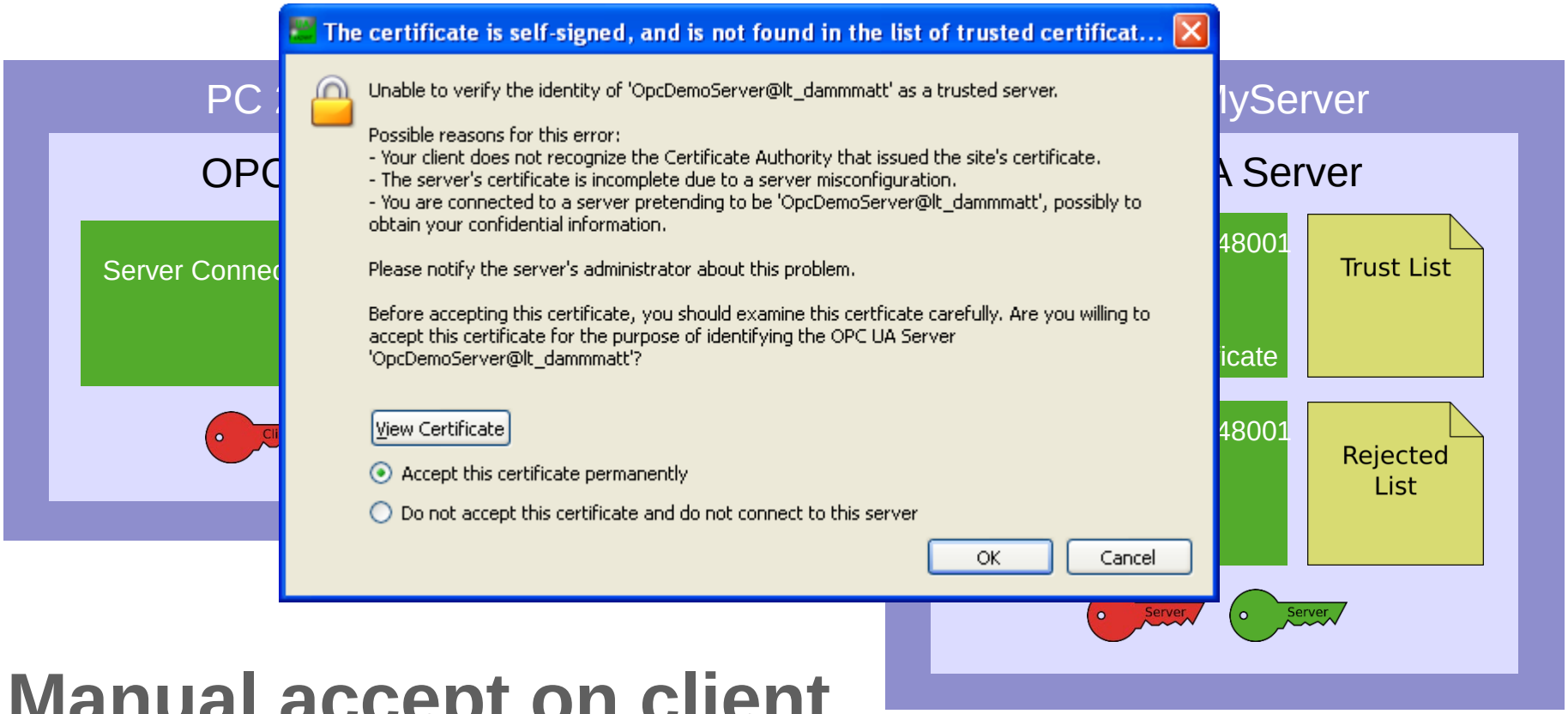
- Called on server
- Returns server security config

Connection Configuration



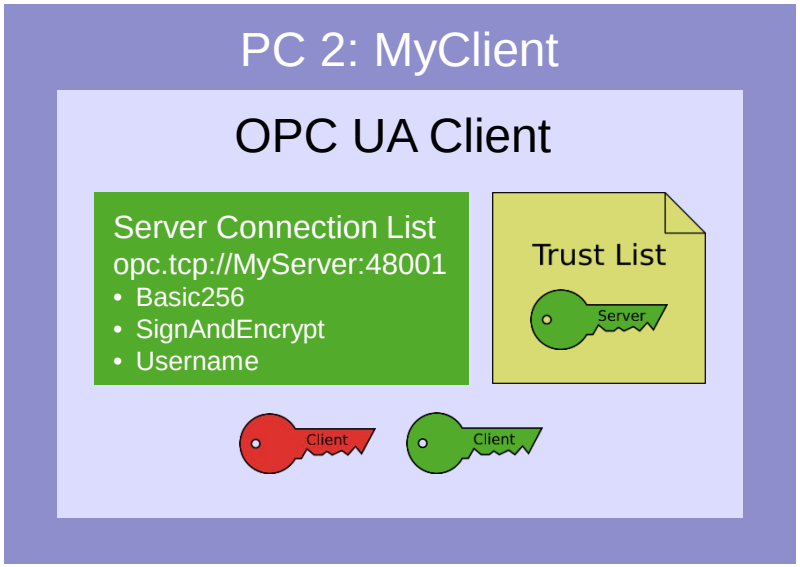
UA Call to get Endpoints

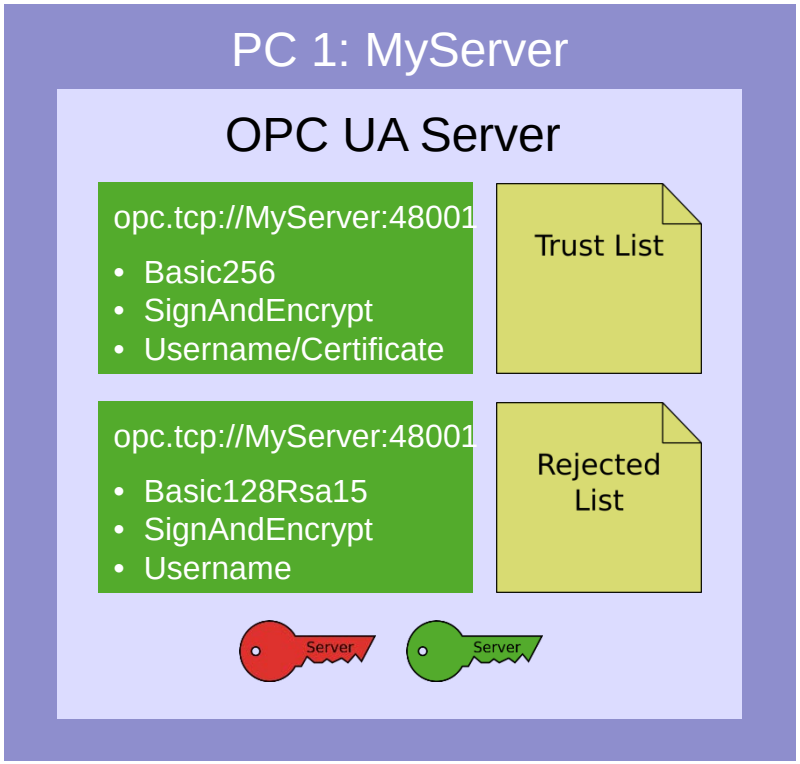
Connection Configuration



Manual accept on client

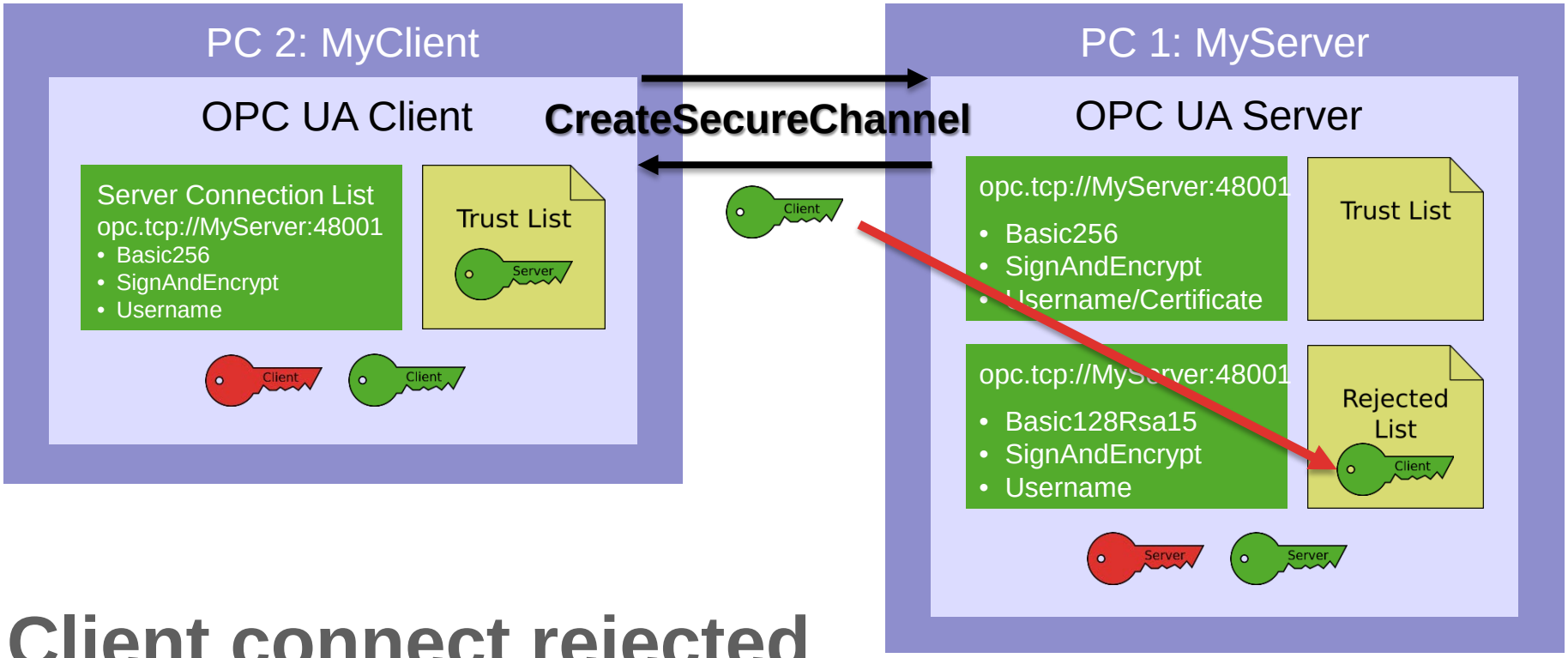
Connection Configuration





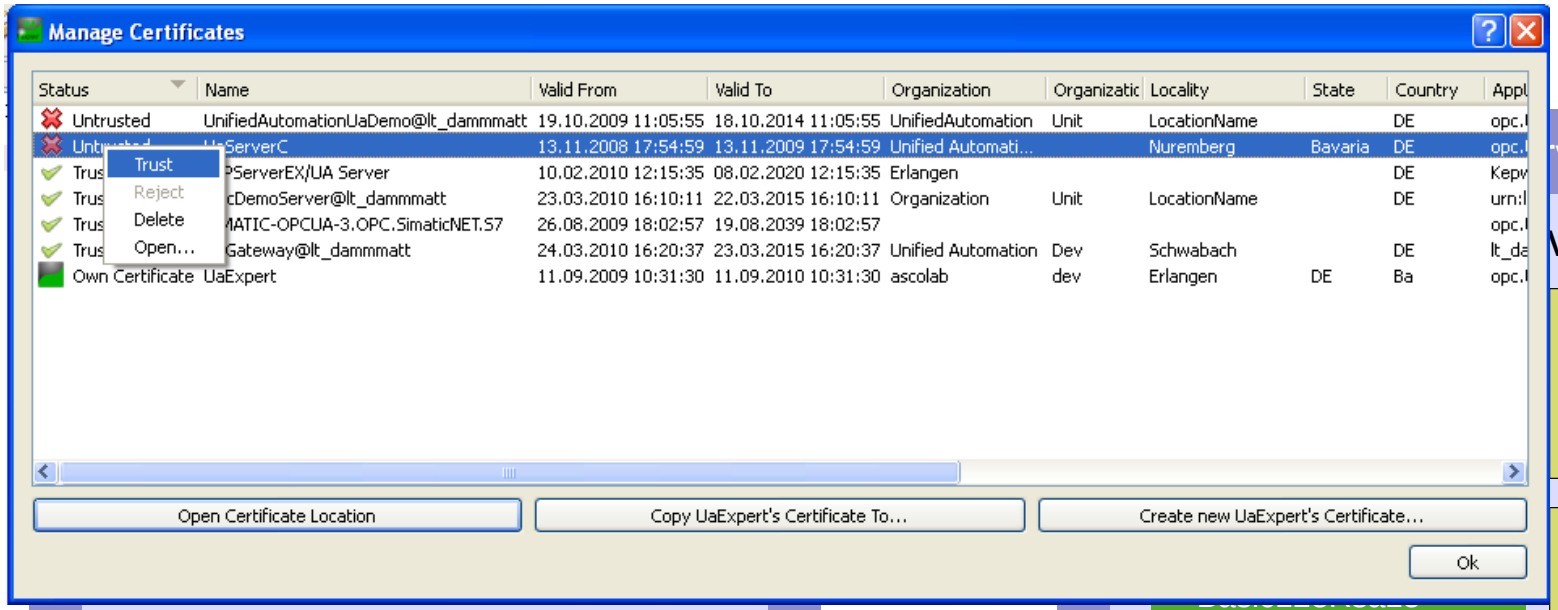
Client configured

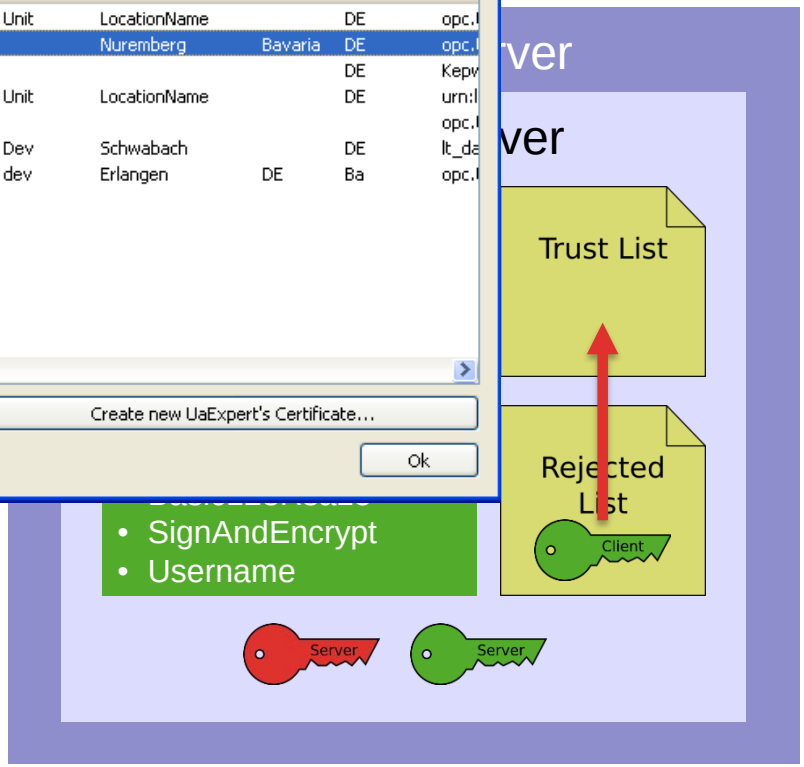
Connection Configuration



Client connect rejected

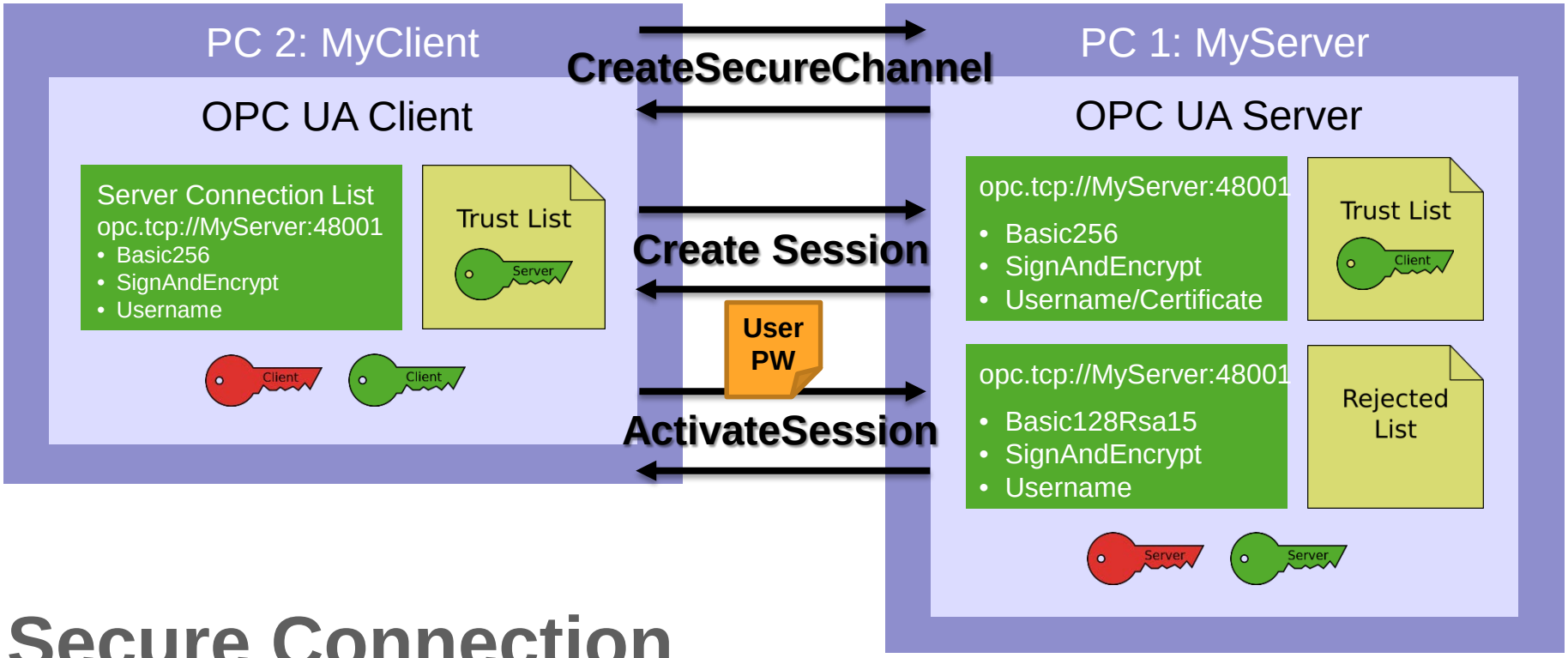
Connection Configuration





Manual accept on Server

Connection Configuration



Secure Connection

Unified Automation

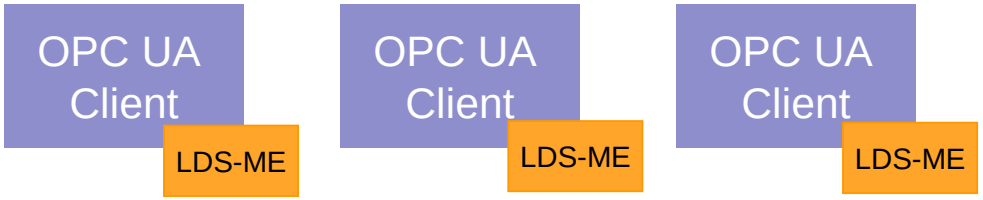
Agenda

> OPC UA Discovery and Security Configuration

> Network Wide Discovery

> Centralized Security Configuration

Ad-Hoc Discovery/Multicast DNS (mDNS)



Features provided:

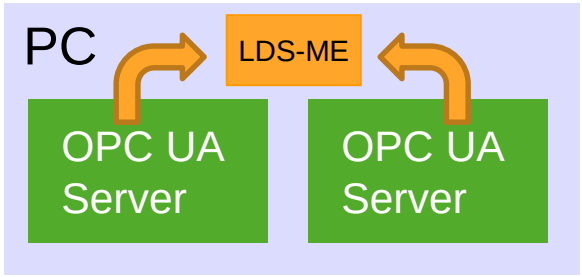
- Host name resolution without central DNS server
- Find OPC UA servers with feature list in local network

Advantage:

No central infrastructure required

Limitation:

Works only in local subnet



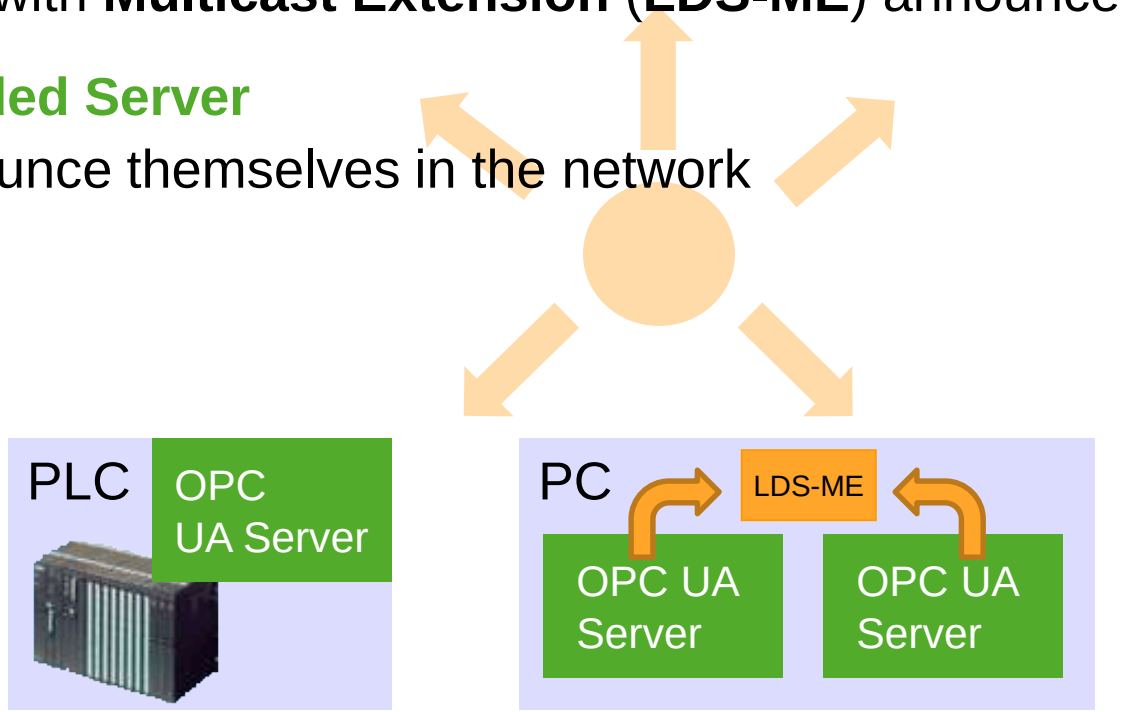
LDS-ME – Announcing Servers

LDS-ME on Server

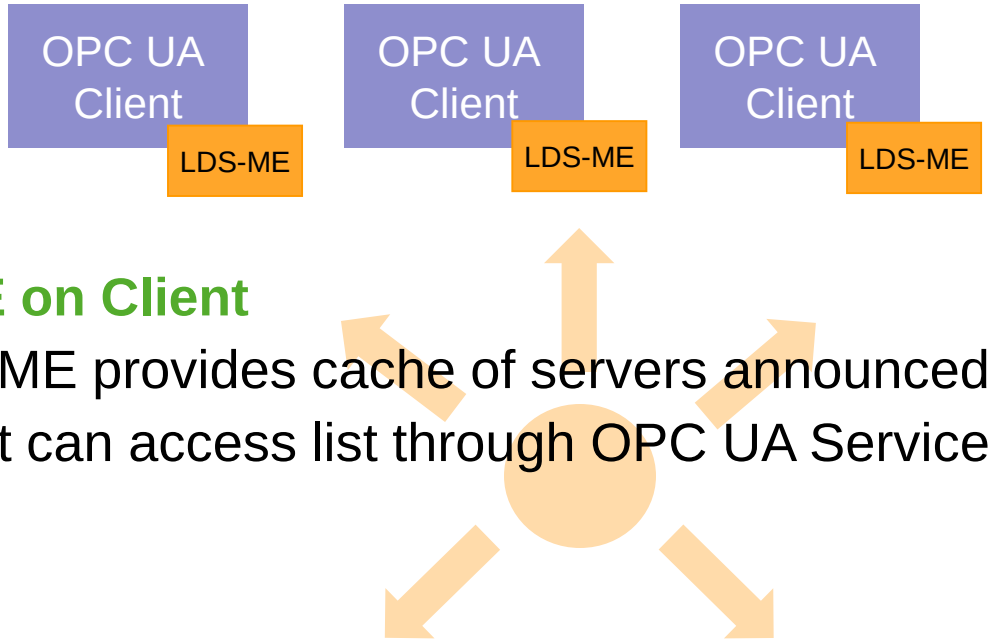
- Servers are registered with local LDS
- **LDS** with **Multicast Extension** (**LDS-ME**) announces servers

Embedded Server

- Announce themselves in the network



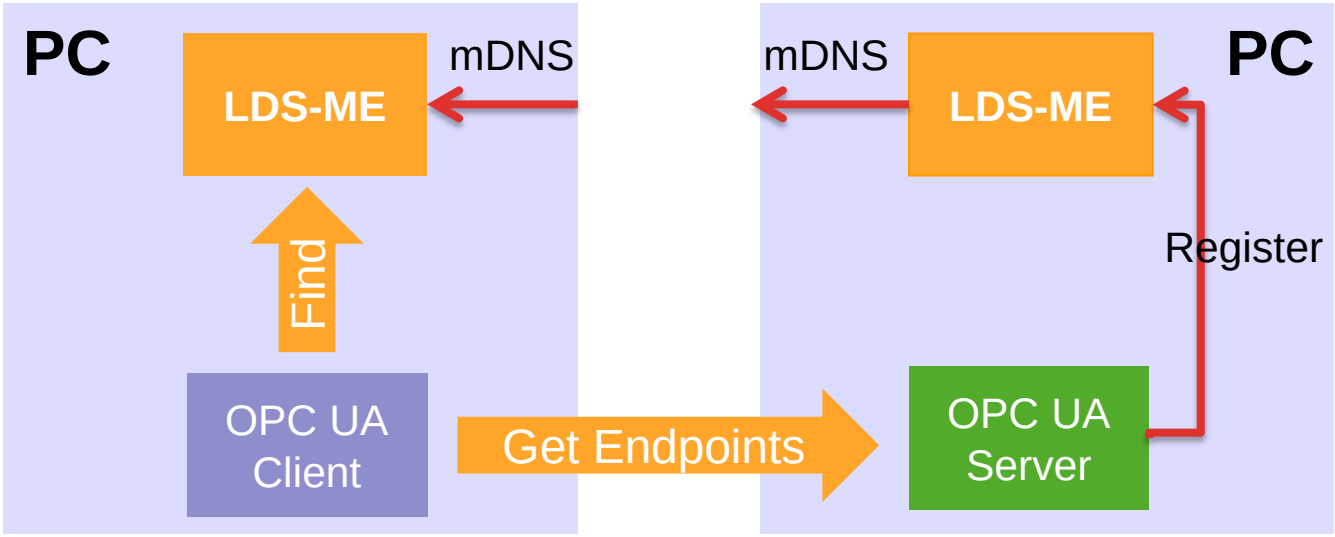
LDS-ME – Provide Server List to Client



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

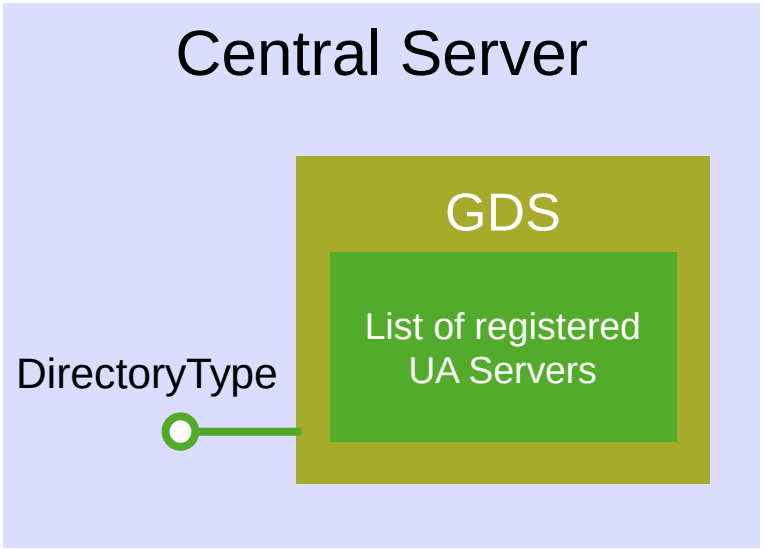
Global Directory Service (GDS)

GDS

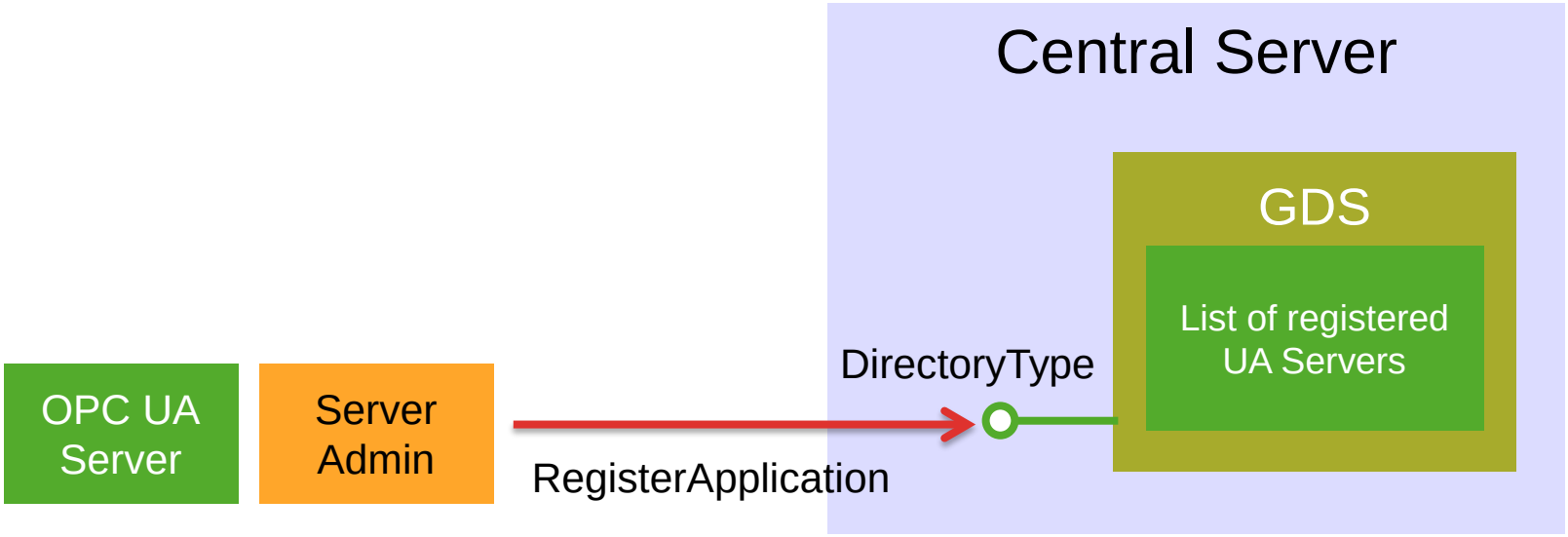
- Central discovery server
- Full OPC UA Server
- DirectoryType is discovery interface with UA Methods

DirectoryType

- RegisterApplication
- UpdateApplication
- UnregisterApplication
- QueryServers



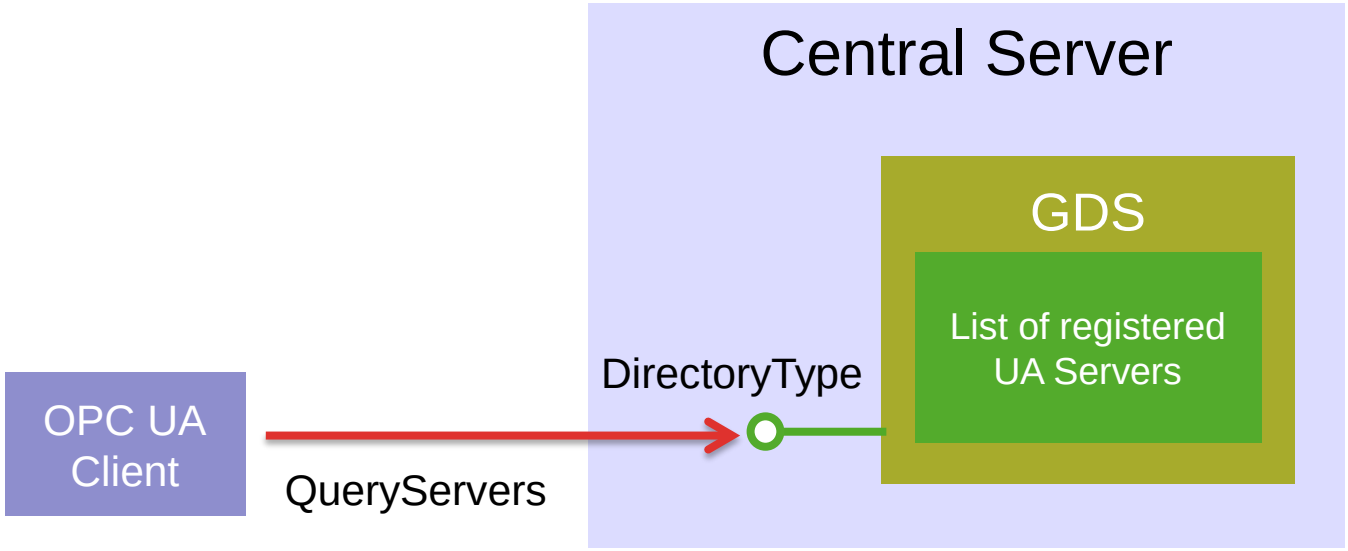
GDS – Server Registration



Server Setup

- Server registration with GDS during setup
- Registration requires security

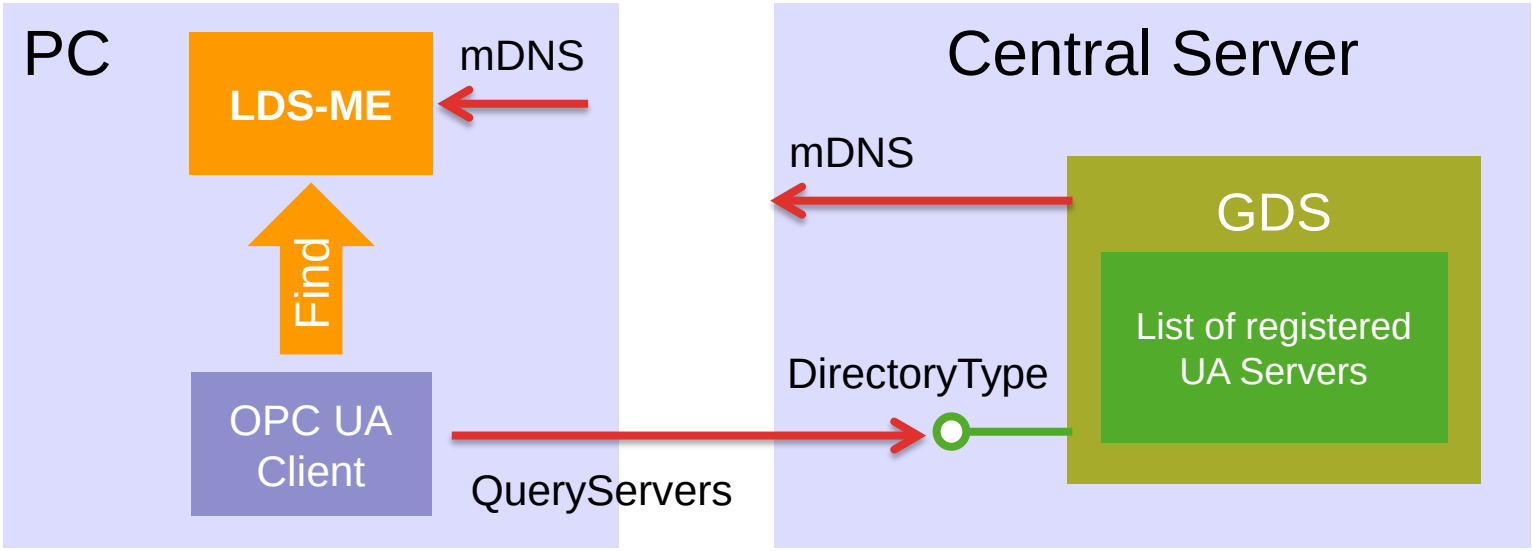
GDS – Client Discovery



Client Discovery

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

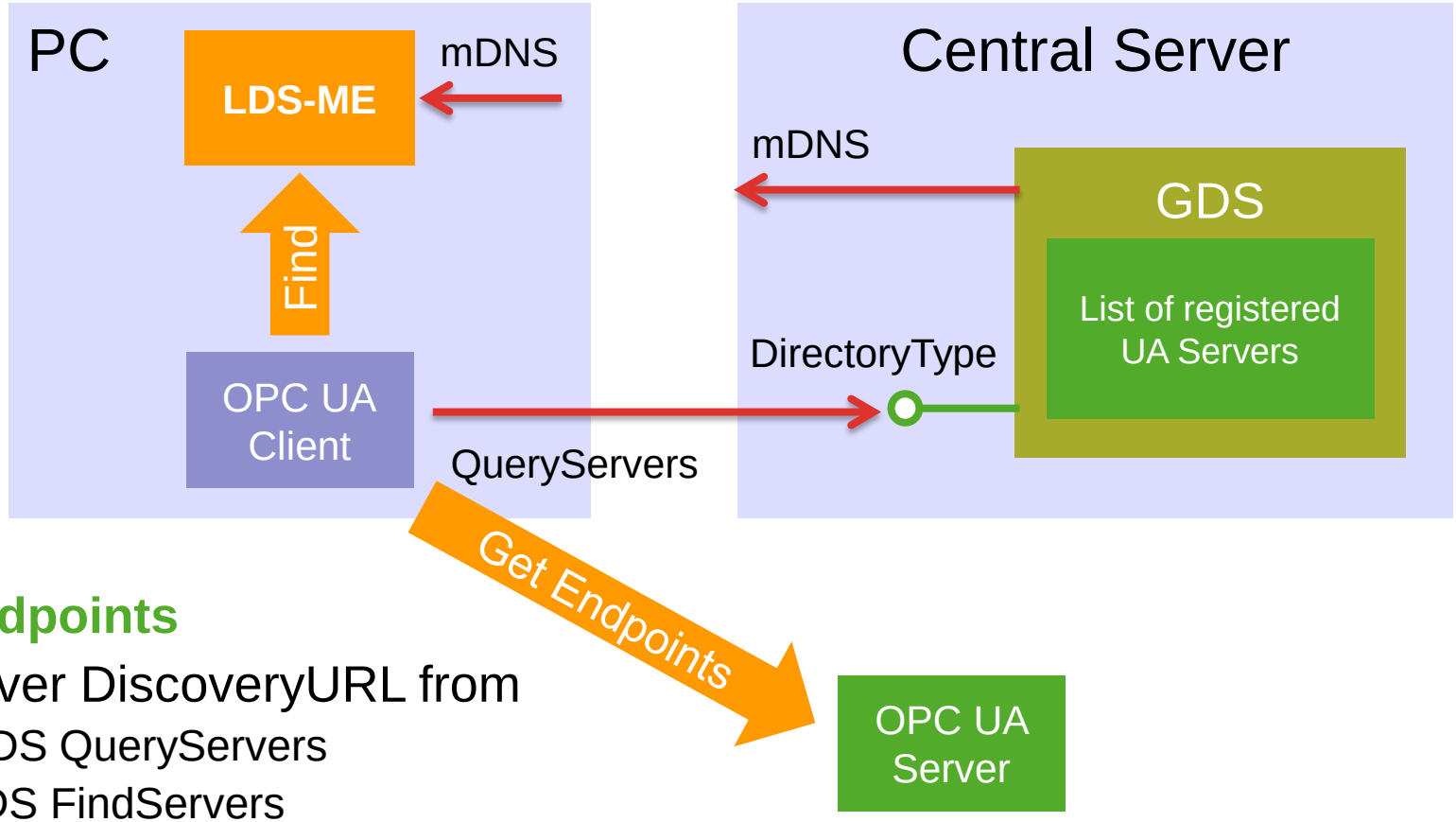
GDS – How to Find GDS



Client Discovery

- Local LDS-ME delivers GDS location (capability filter)
- QueryServers used to find servers

Server Discovery URL for GetEndpoints



GetEndpoints

- Server DiscoveryURL from
  - GDS QueryServers
  - LDS FindServers
  - LDS-ME FindServerOnNetwork

Discovery – Big Picture

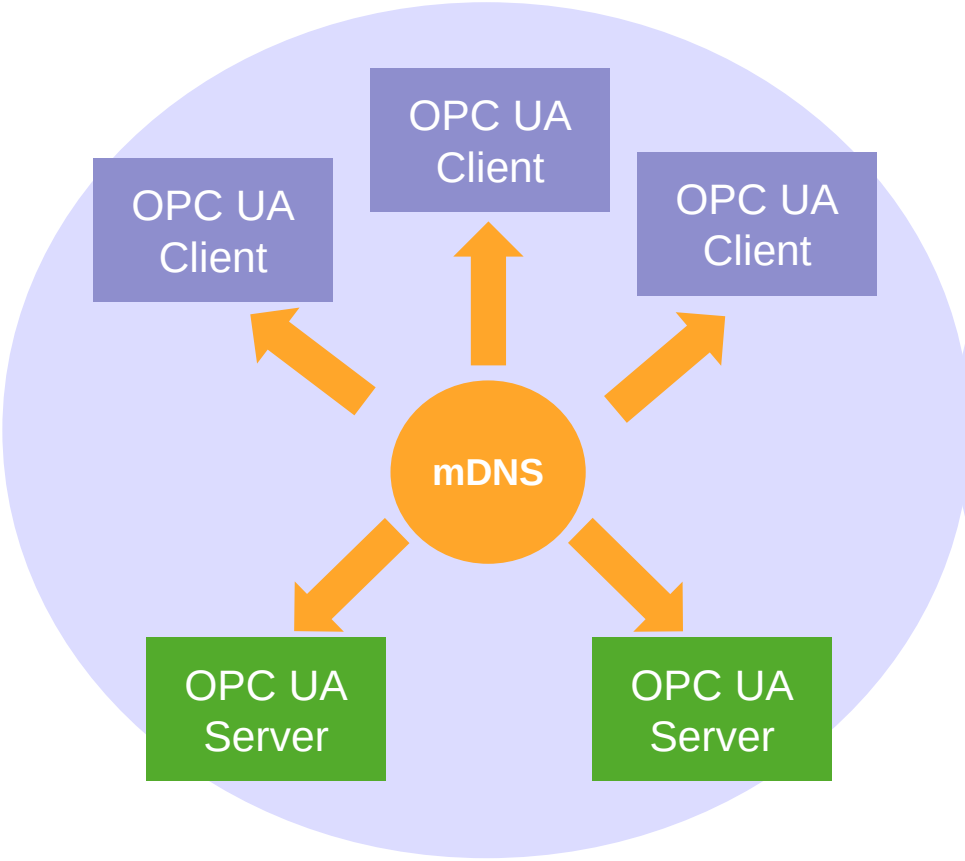
LDS-ME – mDNS

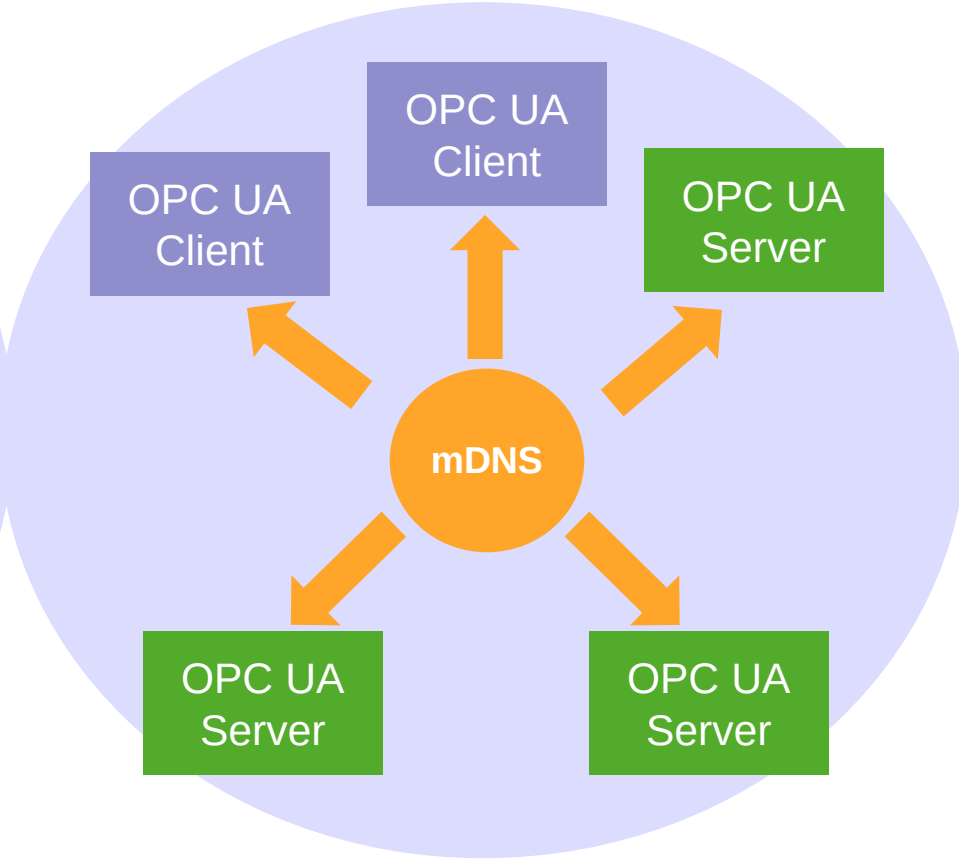
- Ad-Hoc discovery
- Local Subnet

GDS

GDS

- Network wide discovery
- Security can be applied





Agenda

> OPC UA Discovery and Security Configuration

> Network Wide Discovery

> Centralized Security Configuration

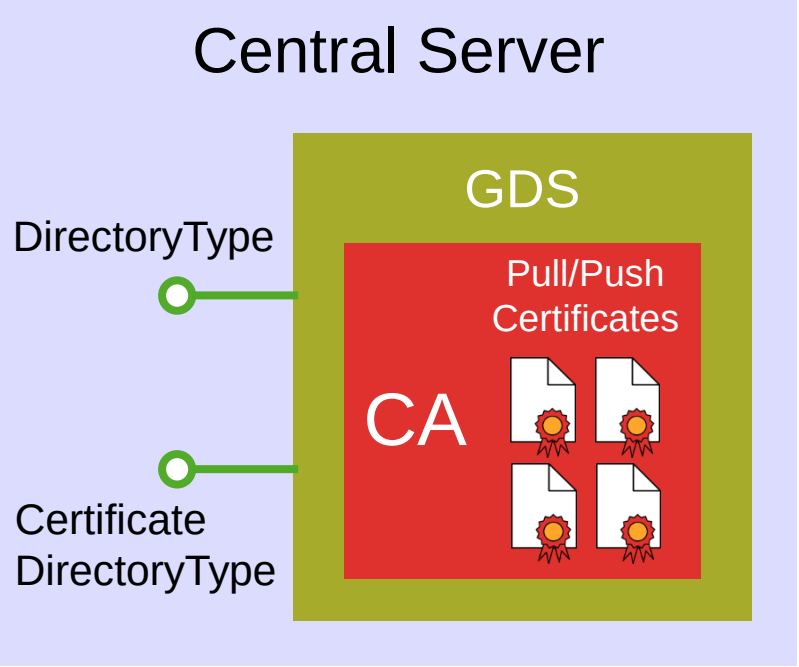
Global Directory Service (GDS)

GDS as Certificate Authority

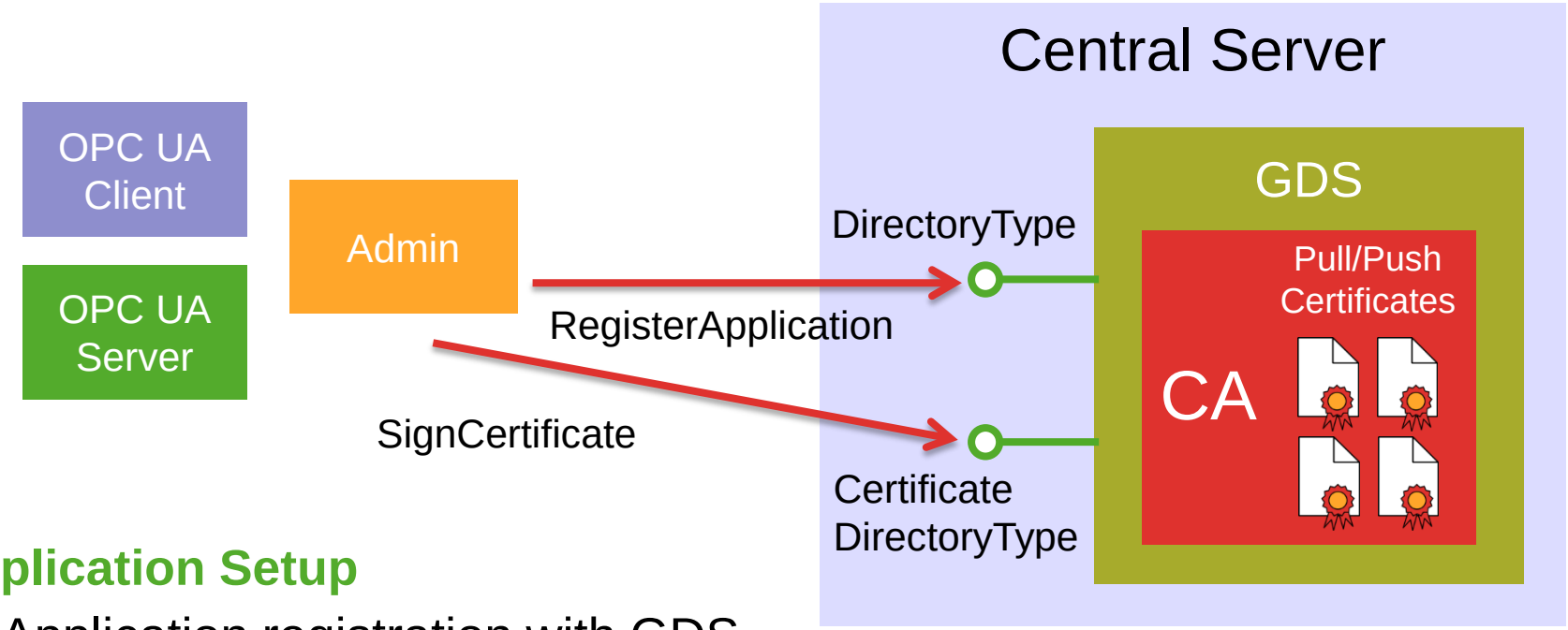
- Central CA
- Full OPC UA Server
- CertificateDirectoryType is interface with UA Methods

CertificateDirectoryType

- RequestCertificate
- SignCertificate
- RenewCertificate
- CheckRequestStatus
- GetTrustList



GDS – Application Setup



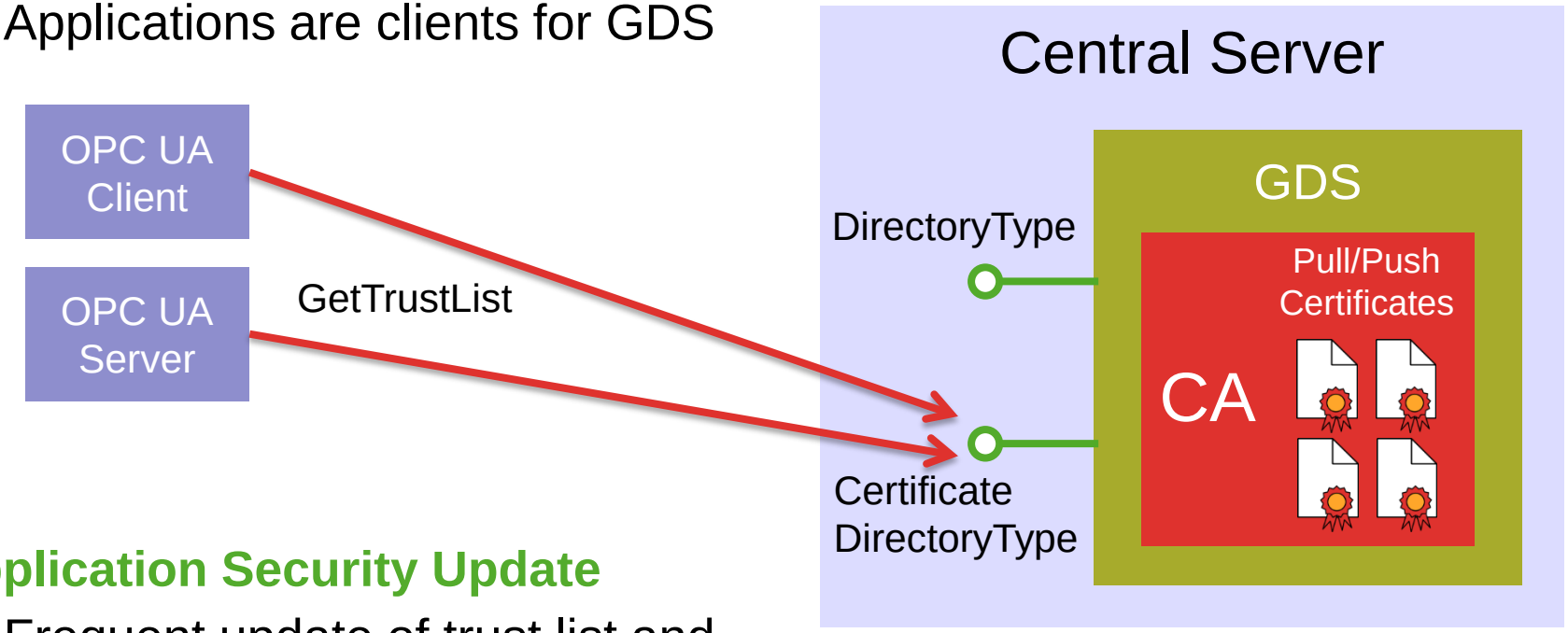
Application Setup

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

GDS – Application Security Update – Pull

Pull

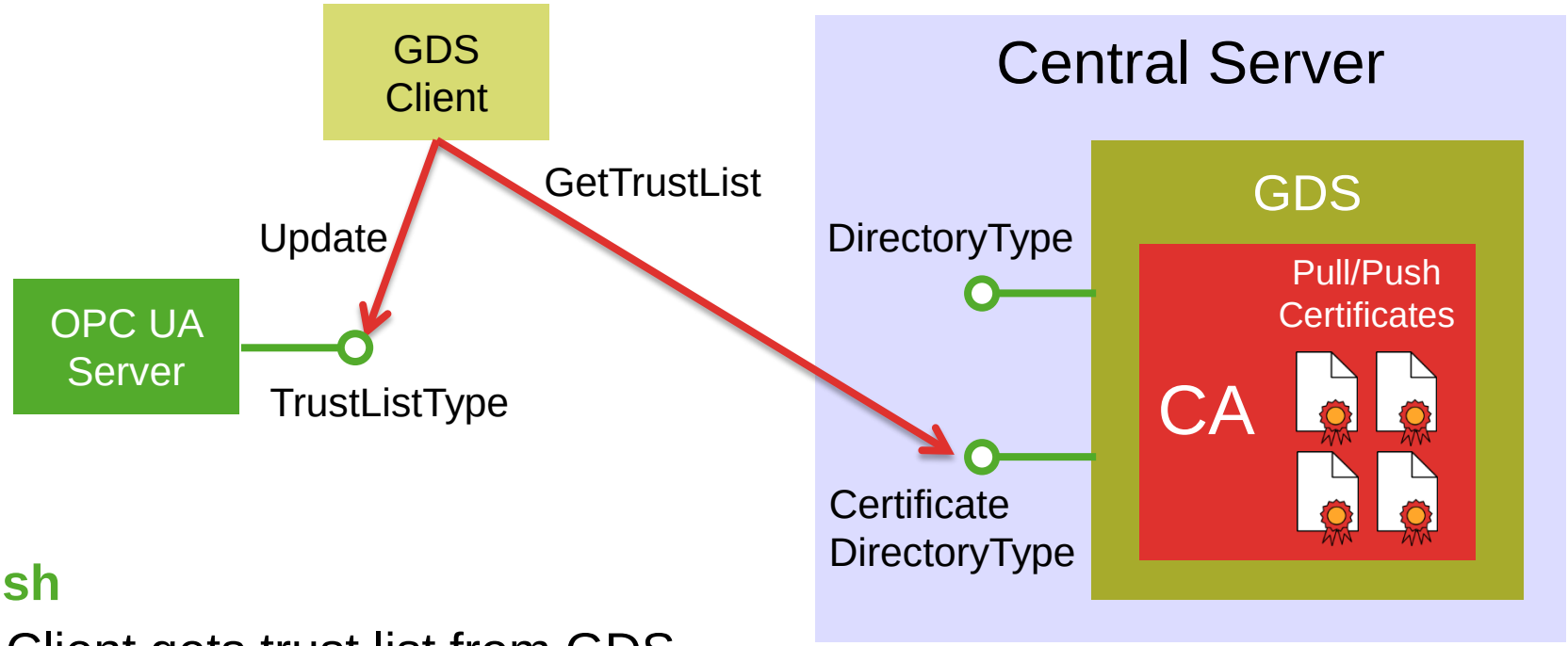
- Applications are clients for GDS



Application Security Update

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

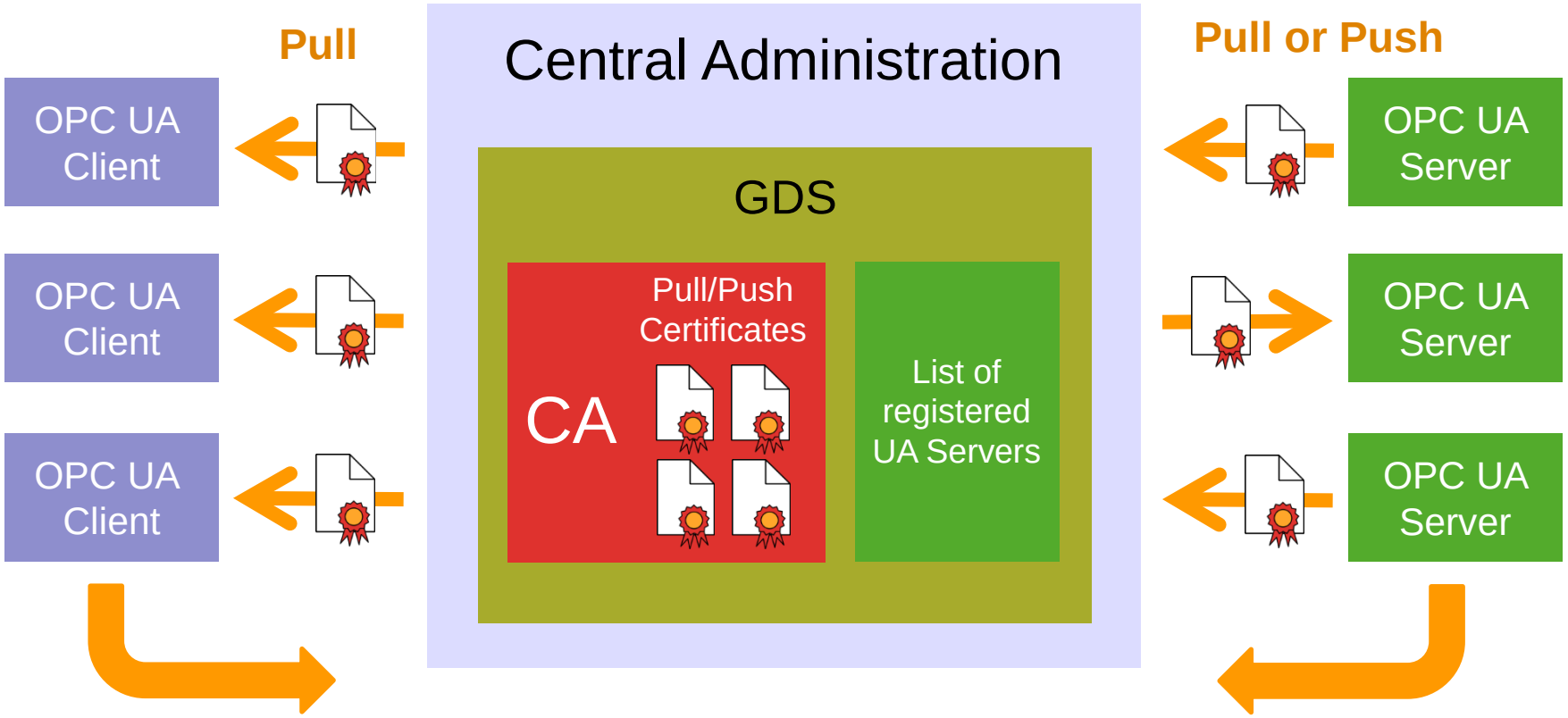
GDS – Application Security Update – Push



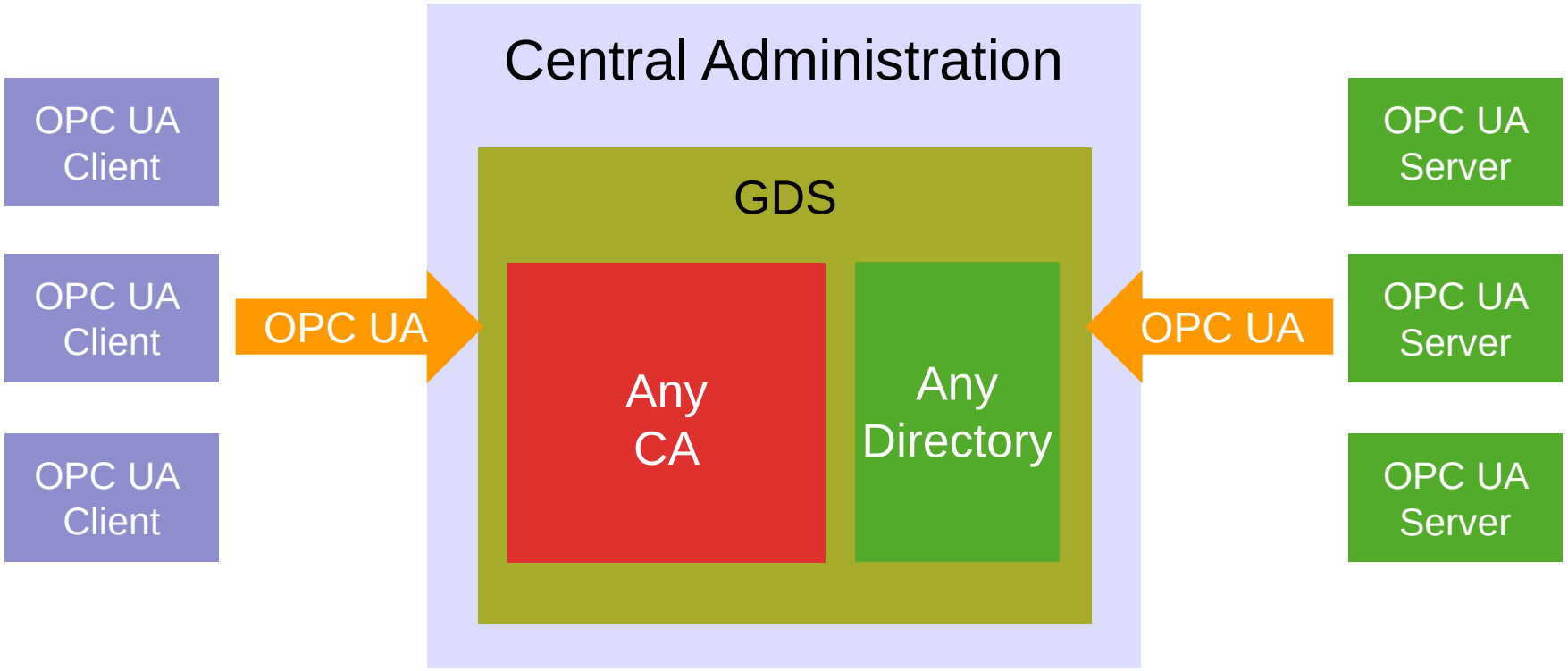
Push

- Client gets trust list from GDS
- Server implements TrustListType
- Client updates server trust list with latest setting from GDS

Global Directory Service (GDS)



Global Directory Service (GDS)



GDS is OPC UA wrapper around any directory or CA

Unified Automation

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**