No more excuses: Use OPC UA Security!

Erich Barnstedt

Microsoft Corporation

erichb@microsoft.com

Our Business Principles

- **Modular Industrial IoT PaaS platform**
  Managed and hyper-scale
-
- **Scales through Ecosystem**
  World's largest partner network to solve any complex problem
- **Largest hardware OEM ecosystem for gateways**
- **Most certified/compliant cloud**
- **Partnership with OT companies**
  Creating a win-win for IT/OT merger
- **Most datacenter regions & world's largest network**
  plus sovereign clouds in US, Germany & China

Our Technology Principles

- **Open Source**
  No proprietary solutions,
  Support for Micro-Services and managed container services on the edge and in the cloud
- **Protocol independent, platform independent**
  Works just as well with AMQP, MQTT and HTTPS as well as Linux and Windows
- **Uses an open data/information model**
  along with open-source tools
- **Based on Open Industrial Interoperability Standards**
  Compatible with the Plattform I4.0's Reference Architecture Model Industrie (RAMI) 4.0 and using OPC UA
- **Non-intrusive**
  Connected your machines without modifying them

The Industrial Interoperability Standard

Microsoft is a member of the OPC Foundation since 1996
Microsoft supports OPC UA on Azure since 2016

Interoperability

Vendor, Platform and OS Independent

Open Source on GitHub (Many Microsoft contributions)

Discoverable Services Oriented Architecture (SOA) independent of the transport method

Owned by a Non-Profit (OPC Foundation)

50M installed base and exponential growth

Data Modelling

Rich data modeling preserves source context

Vendors can extend the data model of each product (Companion Specification)

Maps to field bus protocols, e.g. BACNet | PLCopen | MTConnect | …

Security

Secure Design from group-up

Based on **open security standards**

Authentication | Encryption

Evolves as security technologies evolve

Vendors/Users can choose level of security

Easily acceptable by IT departments

Azure IoT: **Industry leading** OPC UA Support

github.com/Azure?q=OPC

1. OPC Publisher

- OPC UA PubSub telemetry data to the cloud
- non-intrusive data collection via UA Client/Server I/F

2. OPC Proxy plus OPC UA Client in the cloud

- OPC UA Client/Server communication to the cloud **and back**
- Reverse-proxy for service-assisted communication
- Firewall remains closed

3. OPC Twin

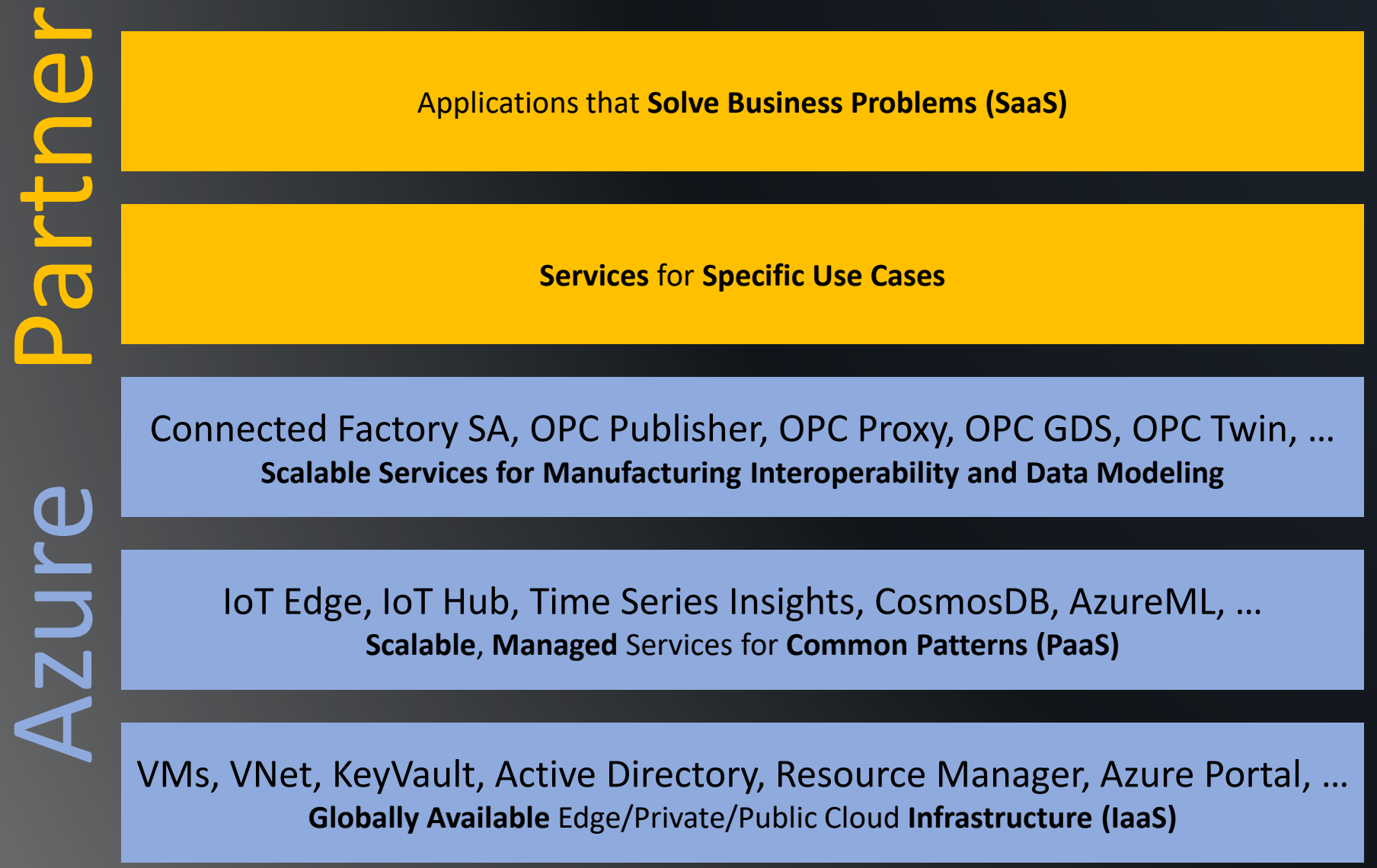
- REST I/F in the cloud
- browsing UA data models
- command execution
- Read & Write data

4. OPC Vault

- Certificate Management for UA
- REST I/F in the cloud
- Private CA
- Based on HSM Key Vault

ISO/OSI Model	OPC UA Client/Server		OPC UA PubSub	
Application	UA Application		UA (Cloud) Application	
Presentation	UA Binary		UA Datagram	JSON
Session	UA Secure Channel	HTTPS		MQTT / AMQP
Transport	TCP		UDP	TCP
Network	IP		IP	
Data Link	Ethernet		DSL/5G/TSN/Ethernet/etc.	
Physical	CAT5/6/etc.		CAT5/6/etc.	

The Industrial IoT Stack



OPC UA Security

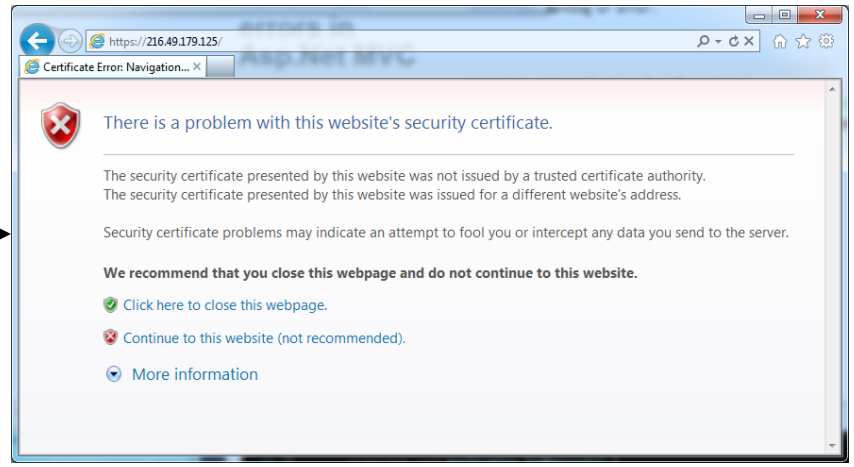
OPC UA is secure **by design**,
you need to make it secure **by default**!

Rule #1 – “Don’t talk to strangers”!

Enabling <SecurityMode>None_1</SecurityMode> is the **same thing**!

Rule #2 – “Don’t accept gifts from strangers!”

Accepting self-signed certificates is the **same thing**!



Rule #3 – “Don’t leave your secrets lying around!”

Storing your private keys on the (unencrypted) file system (in .pfx files) is the **same thing**!

The Big Problem

- Need a shopfloor X.509 Certificate Management Solution
- OPC UA specifies a Global Discovery Server for this in part 12
- Handles **discovery** of **registered** OPC UA Servers
- …but also handles **certificate management**
- It’s complicated… but there is hope! ☺

Timeline

- First on-prem GDS released by GE in May 2015
  - http://www.geautomation.com/news/ge-first-implement-and-release-new-opc-ua-standard-launch-global-discovery-server
- First cloud-based GDS demoed by Microsoft at OPC Day Europe in June 2017
- First on-prem open-source version contributed by Microsoft to OPC Foundation in December 2017
  - https://github.com/OPCFoundation/UA-.NETStandard/tree/master/SampleApplications/Samples/GDS
- First cloud-based GDS released by Microsoft *soon*. ☺

“Plug ‘n’ Deploy” IIoT Experience Walkthrough

Auto-deploy Connected Factory

- Customer deploys Connected Factory solution accelerator through single click in azureiotsolutions.com

Auto-deploy IoT Edge

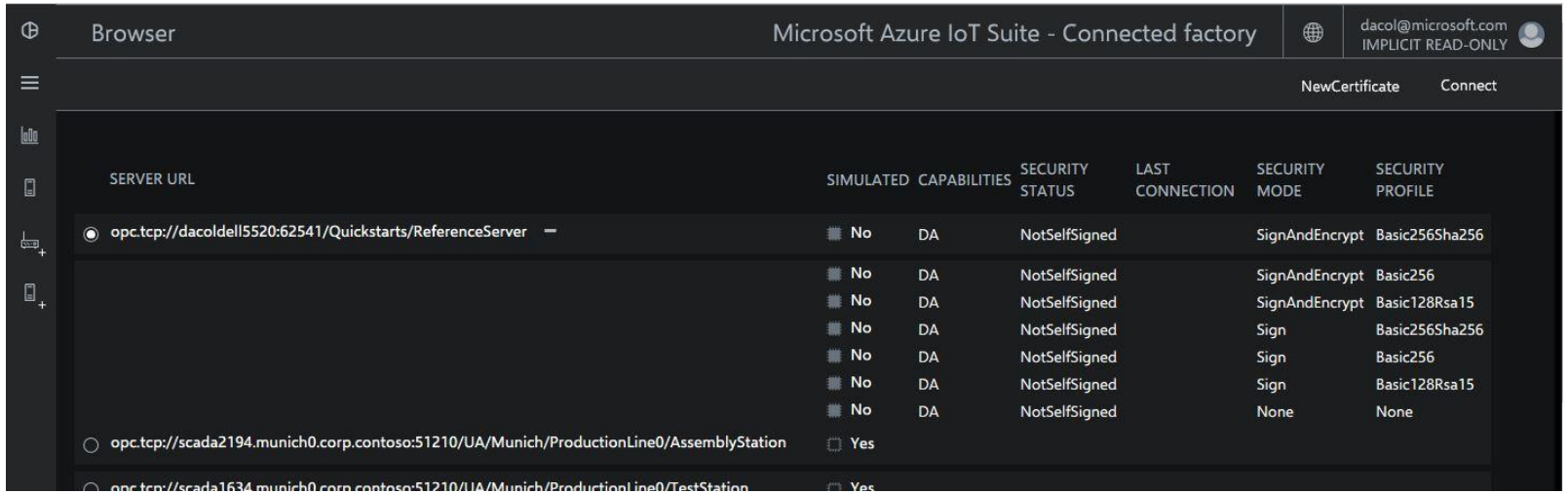
- Customer deploys Edge device in local network (factory floor)
- Registers Edge with IoT Hub/Connected Factory (e.g. through DPS)

Auto-deploy OPC modules

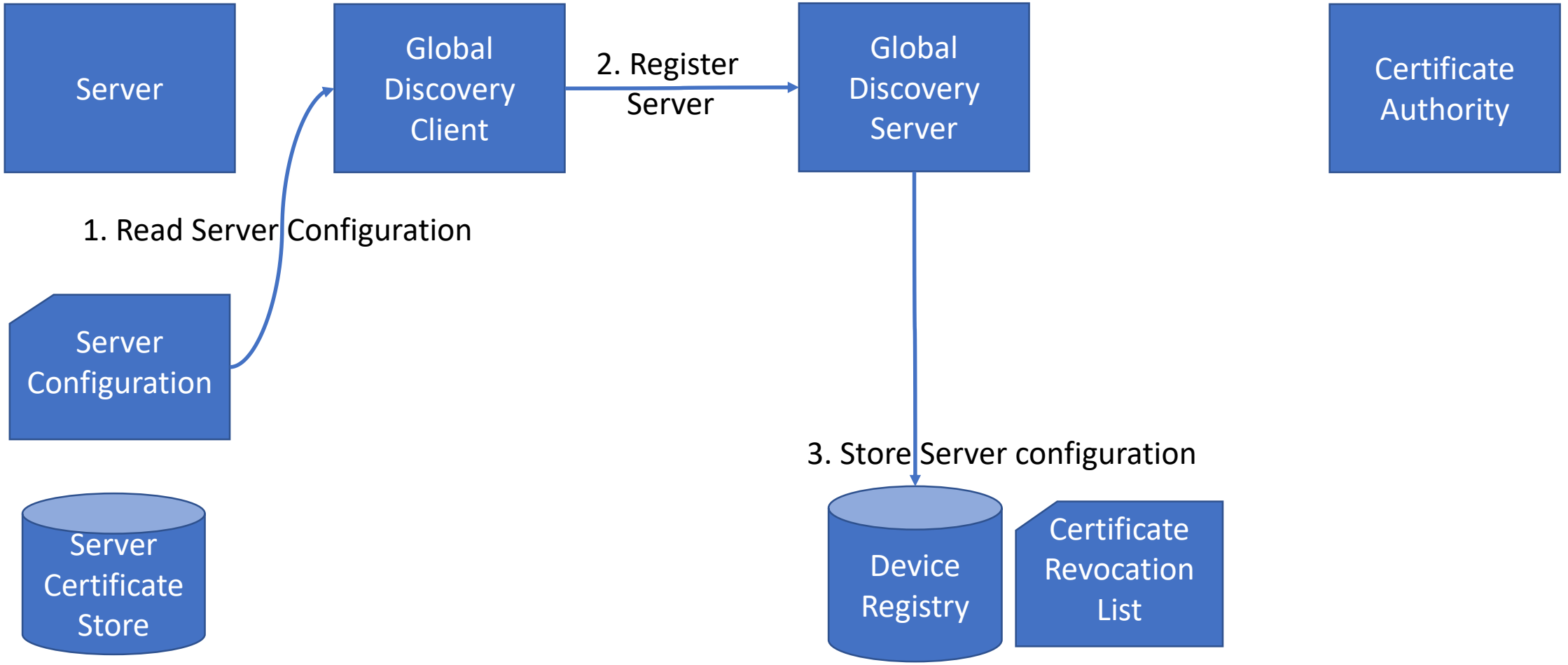
- Customer deploys OSS modules to the Edge via the standard module deployment process
- Modules are auto-configured

Auto-register OPC servers with CF

- Newly discovered devices will **automatically** appear in the CF device registration list
- Administrators can pick and choose devices and initiate the security audit
- Machines can be secured **automatically**

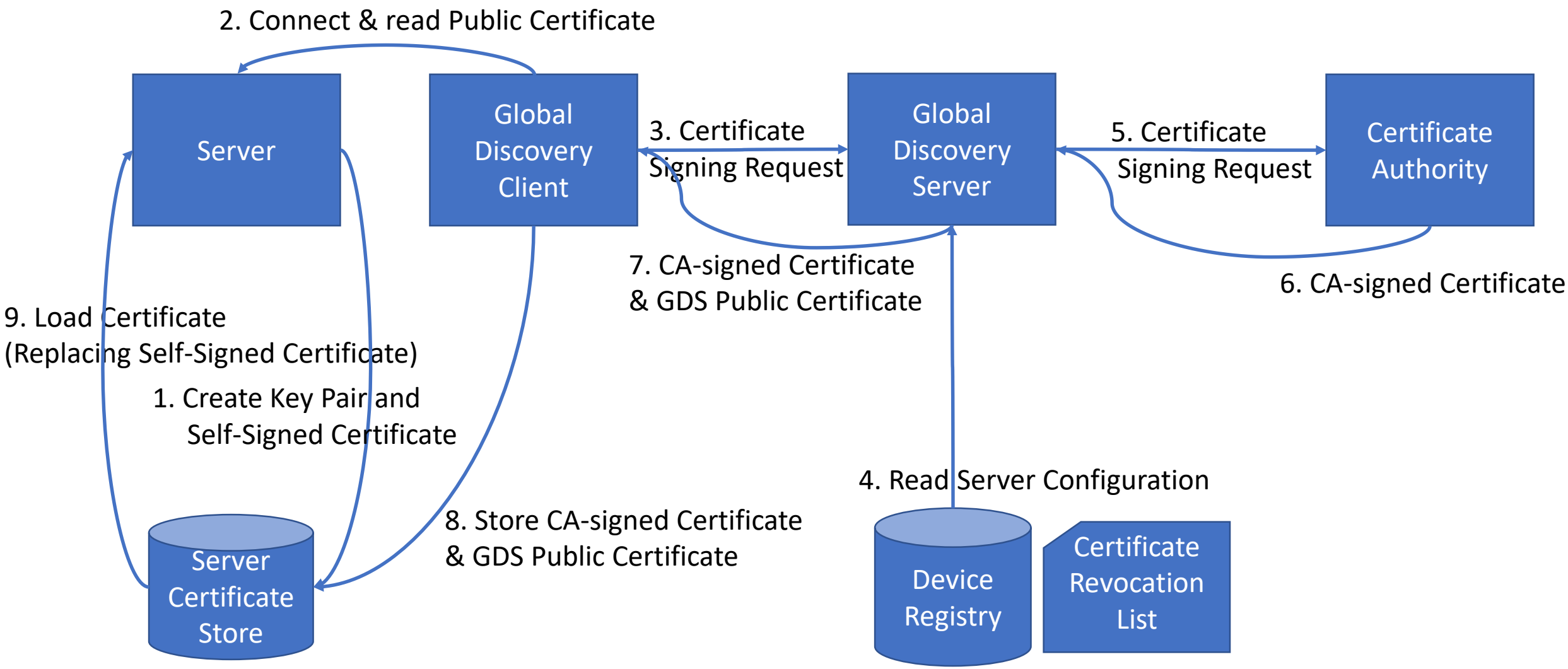


GDS deep dive: Registration (always needs to happen first)



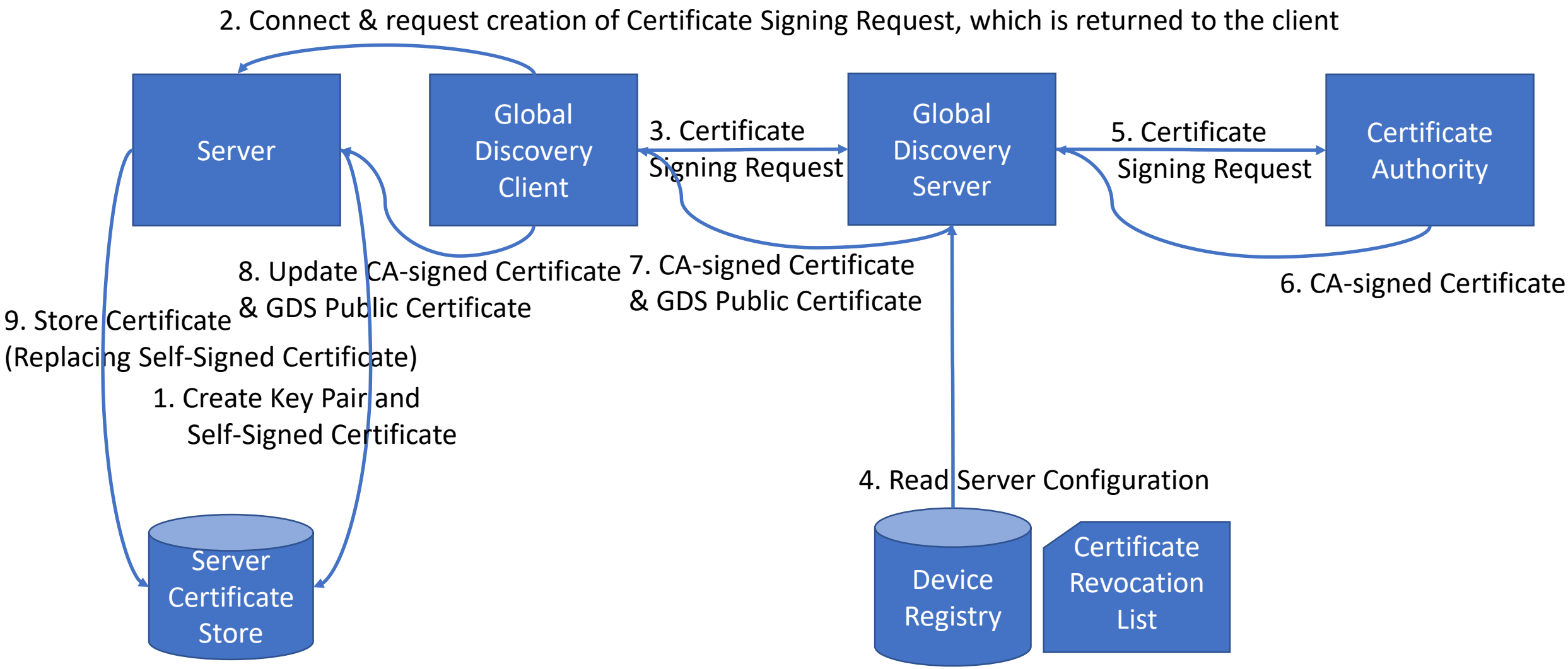
GDS deep dive: Client Pull Certificate Request

Disadvantage: GDC needs access to Server's private key in step 3!

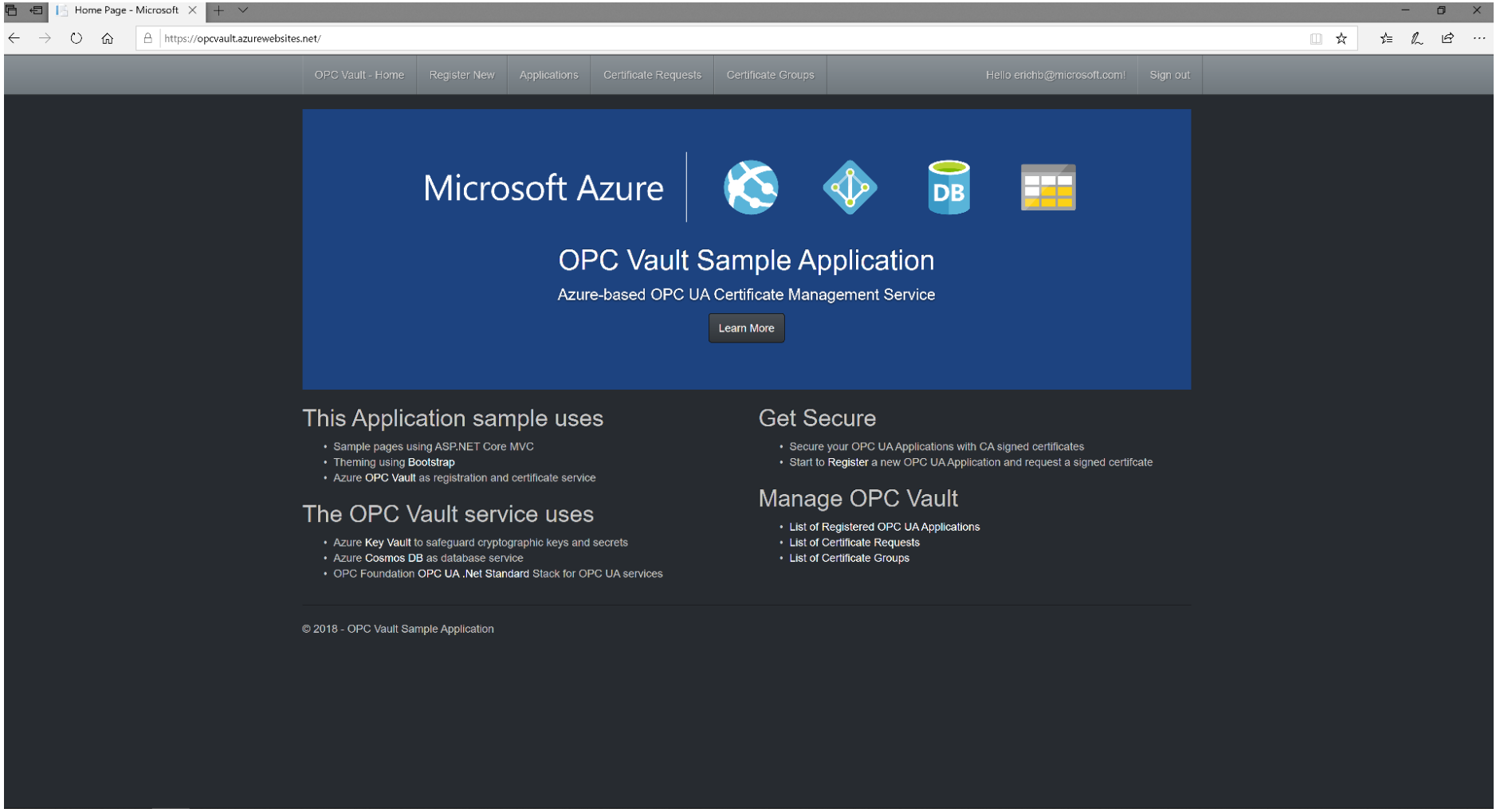


GDS deep dive: Server Push Certificate Request

Advantage: Global Discovery Client does not need physical access to server certificate store!



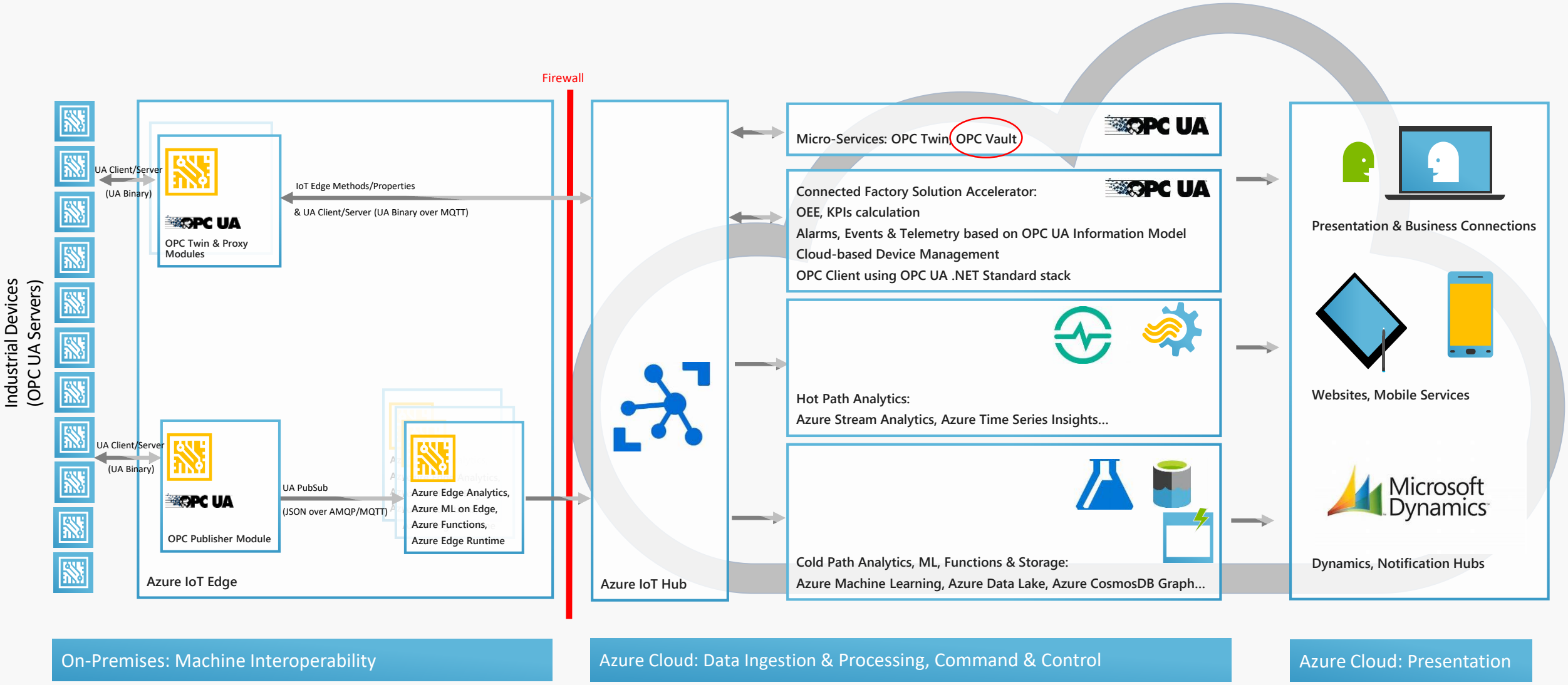
Where is the hope?



OPC Vault

- Combines GDC and GDS certificate functionality into a single cloud REST-based micro-service
- Open-source on GitHub
- Open-source sample app on GitHub
- Uses OPC Proxy/Twin for communicating with on-prem OPC UA Servers (or makes certificate available for download)
- Uses Azure Key Vault for storing root CA private key an certificates

Azure Industrial IoT Cloud Platform



Please enable GDS Server Push!

- All commercial OPC UA stacks support it
- …but not enabled in most PLCs ☹

Thank you.