Solving PKI in OT

Slowly but surely

Wapice

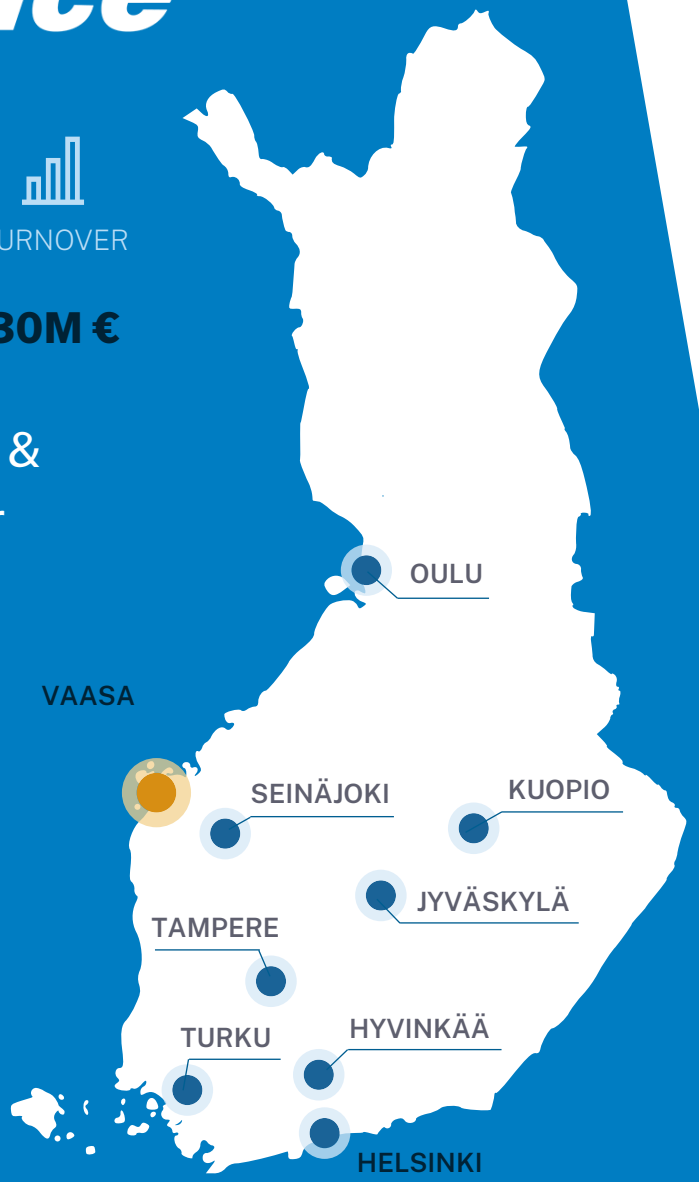
CREATING A SMARTER
FUTURE TODAY

Wapice

EMPLOYEES	R&D SPEND OF TURNOVER	TURNOVER
~350	7%	30M €

- Industrial Software & Electronics partner
- Cutting-edge IoT & AI

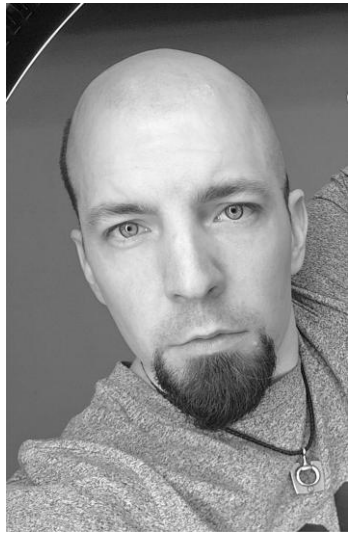
Energy
Logistics
Construction
Public Sector
Manufacturing
Moving Machinery



Lassi Niemistö

Head of DevOps, Security & Quality Solutions

- **MSc. in Automation Technology**
- **Embedded SW developer background**
- **15 years a Wapicean 💙**
- **Forever a tech hobbyist**



TAMPEREEN TEKNILLINEN YLIOPISTO

Jurva

@brainmademedoit

lassi.niemisto@wapice.com
www.linkedin.com/in/lassi-niemistö-45711051

PKI

Simon says you are trustworthy

- Normal people cannot be expected to grasp all nuances of PKI
  - Certificate, key, X.509, public, private, CA, root, intermediate, attestation, DER, PEM … 👀
- Think it simple:
  - Prepare all devices / entities to trust Simon
  - Simon says another entity is trustworthy → trust it
  - No need to establish 1-on-1 trust relations

Trust purposes

- User trusts a web service (most common)
- Industrial devices trust:
  - Remote **management** system to control it
  - Vendor-assigned human users for **maintenance**
  - A software **update** package
  - Product specific **cloud** backends
- And..
  - **Device-to-device communication**
  - **Device-to-scada communication**
  - **On-site human users**
  - Device/scada-to-cloud

Trust purposes

- User trusts a web service (most common)
- Industrial devices trust:
  - Remote management system to control it
  - Vendor-assigned human users for maintenance
  - A software update package
  - Product specific cloud backends

Vendor PKI works

- And..
  - **Device-to-device communication**
  - **Device-to-scada communication**
  - **On-site human users**
  - Device/scada-to-cloud

Compatibility bottleneck!

IT world practices

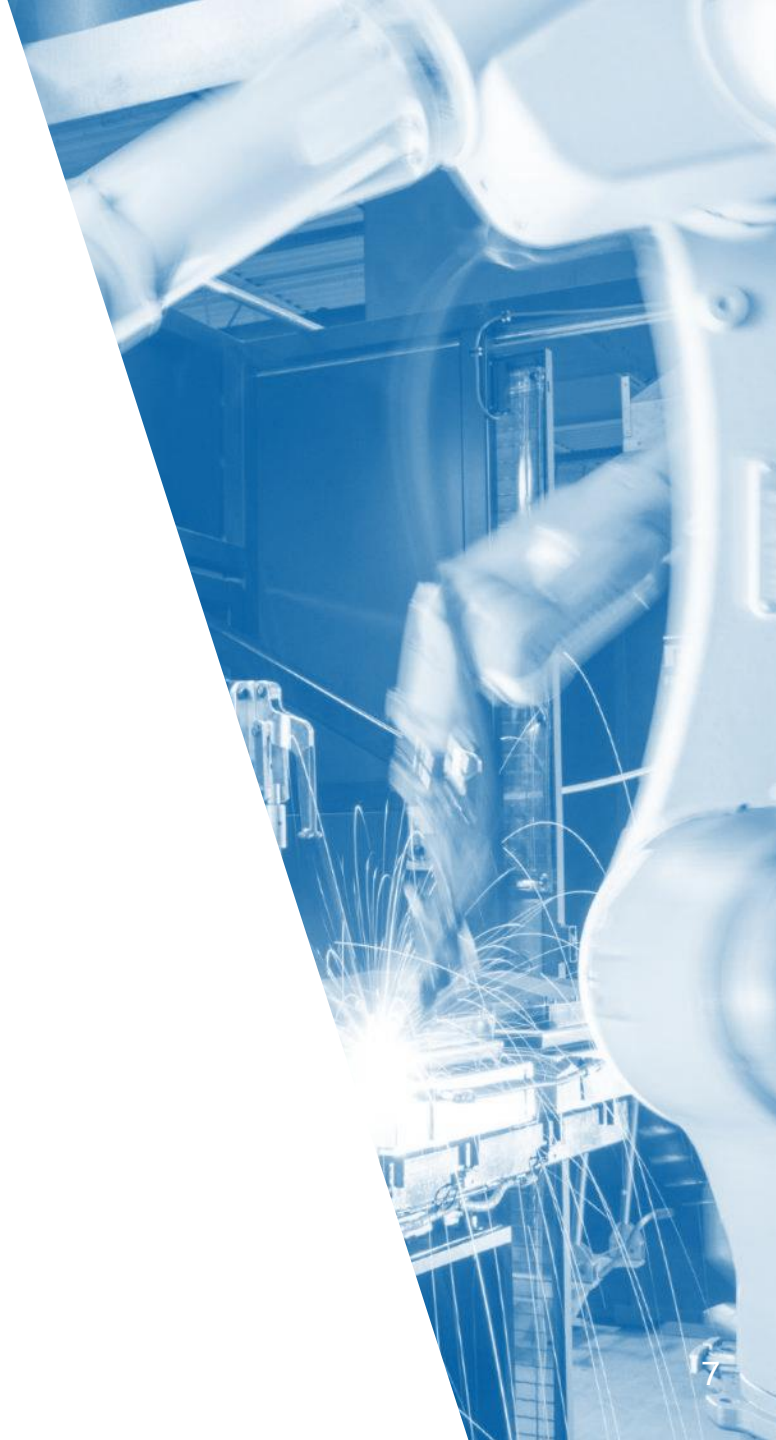
Status of web PKI

- Root trust is bundled with browsers
  - Long validity, 8..25 years
  - Updated via browser updates
- Server side certs are supposed to be rotated
  - 2029: rotate every 47 days
  - Everything is online
    → Easy to accomplish with **automation**

- **No direct impact to OT if private PKI chains used**

Industrial protocols

- Certificate based security is a typical solution
  - OPC UA
  - MQTT
  - AMQP
  - DDS (with DDS Security)
  - Modbus TCP (with TLS extensions)
  - PROFINET (Security Class 3)
- Unprotected protocols are still out in the wild
  - Add-on VPN style security → certificates



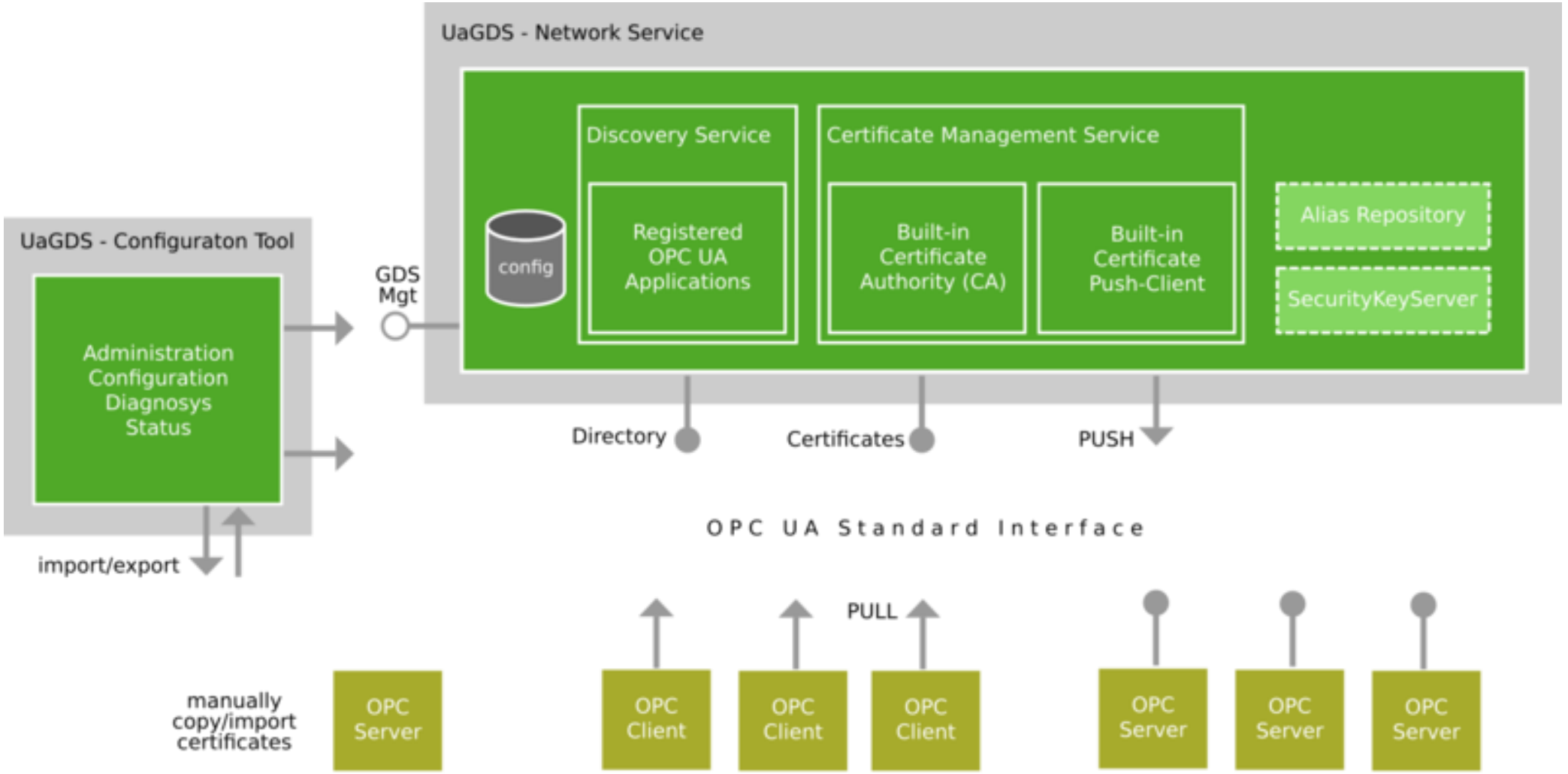
What we need

- Local CA that works in airgapped environments
  - But binds to cloud side roots for convenience and compatibility
- Generic and manufacturer independent site certificates management
  - With the necessary rotation and revocation processes
- Strong device identities
- A reasonable commissioning & permissions process
  - Complete plants
  - Added functionalities and replaced devices

Device identity certificates

- A standard model is now available by IEEE 802.1AR
  - Crafted to OT purposes, finally
- **IDevID** (Initial Device Identity)
  - Globally unique ”birth certificate” by manufacturer
  - Long lived by definition
- **LDevID** (Local Device Identity)
  - Issued by Site PKI
  - Purpose or role assigned to a specific device
  - Can be used for communications

OPC UA GDS

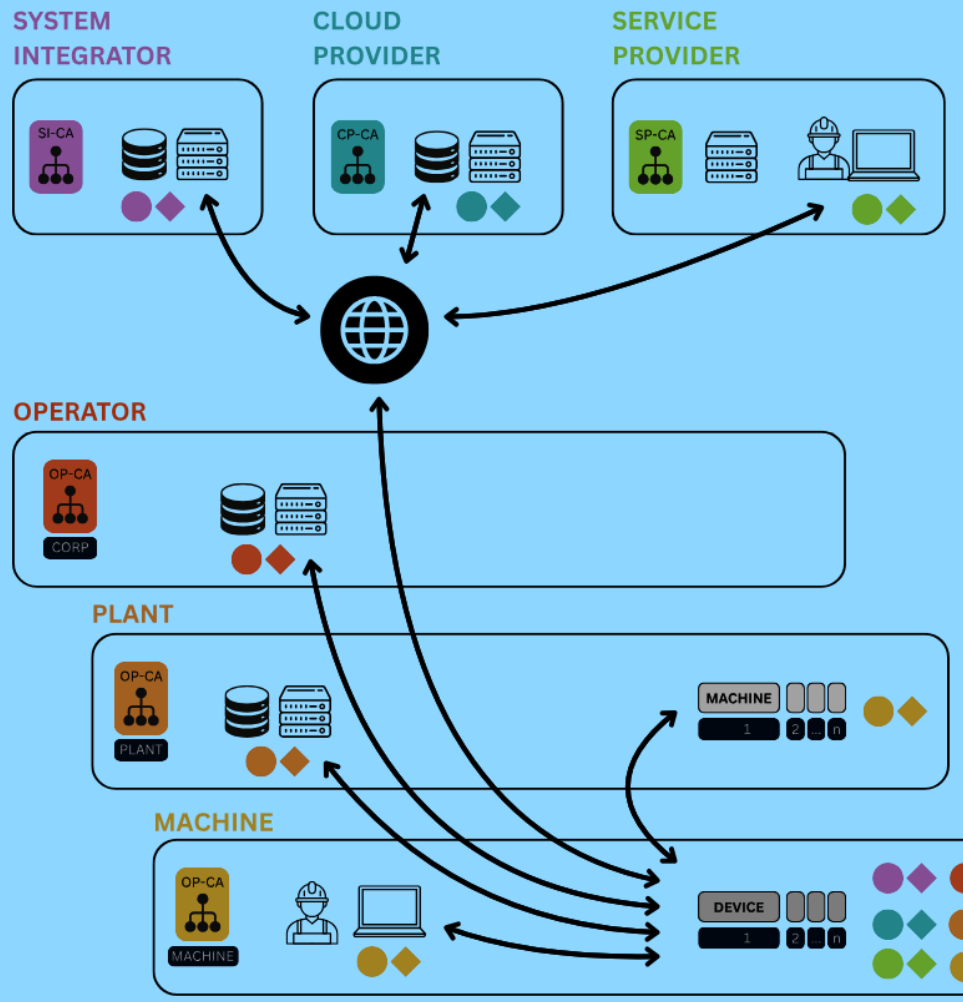

UaGDS - Network Service
Discovery Service
Registered OPC UA Applications
Certificate Management Service
Built-in Certificate Authority (CA)
Built-in Certificate Push-Client
Alias Repository
SecurityKeyServer
config
UaGDS - Configuraton Tool
Administration
Configuration
Diagnosys
Status
GDS Mgt
Directory
Certificates
PUSH
import/export
OPC UA Standard Interface
PULL
manually copy/import certificates
OPC Server
OPC Client
OPC Client
OPC Client
OPC Server
OPC Server
OPC Server

OPC UA GDS

- Solves following in the OPC UA scope
  - Local CA, suitable for airgapped environments
  - Automatic rotation of client and server certificates
  - Centralized management of application registrations / commissioning
- Does not provide
  - General purpose PKI features for non- OPC UA devices/apps
  - Global trust anchors for establishing initial trust automatically
  - HW-bound trust (device identity, signed software)

Trustpoint Emerging Open Tech

- Standard / open protocols for
  - Enrollment over Secure Transport (EST, RFC 7030)
  - Certificate Management Protocol (CMP, RFC 9483)
- OPC US GDS Push support
- IDevID/LDevID support
- AOKI Zero Touch Onboarding
- **Open and OT-oriented**



Commissioning

- Complex configuration won’t fly
- Pre-shared trust vs. Trust-on-First-Use
- Innovations are necessary
  - Trusted commissioning gateway devices
  - Smart devices + QR codes
  - Device identity + join voucher
  - Physical access as a permission

Why are we not there yet?

- Backwards compatibility allows insecure fallbacks..
  - ...which become permanent way-of-working
- Parallel PKI systems cause confusion
  - Manufacturer and site owner PKIs cannot be fully merged
- Lack of openness in contrast to web world
  - No manufacturer shall own the solution
  - Only open PKI standards/stacks can bring compatibility
- Security is not the #1 purchase criteria
  - Support for site-owned PKI and easy commissioning costs in R&D

Wapice

CREATING A SMARTER FUTURE TODAY

Visit **wapice.com**