Certificate Management for Cloud-Hosted Digital Twins

Nikos Fotiou
ExcID

Chalima Dimitra Nassar Kyriakidou, Athanasia Maria Papathanasiou, Iakovos Pittaras, Yannis Thomas, George Xylomenos
Mobile Multimedia Laboratory, AUEB

https://mm.aueb.gr/projects/snds

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Motivation

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Why Certificates for DTs?

- What is a Digital Twin (DT)?
  - Virtual representation of physical IoT device
- How can we trust a cloud-hosted DT?
  - Is it authorized to represent the IoT device?
- Our scheme: short-lived certificates
  - Quick rotation of certificates
  - Resilience against malicious CAs
  - No IoT device secrets kept at the DTs
  - Low overhead and standards-based

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

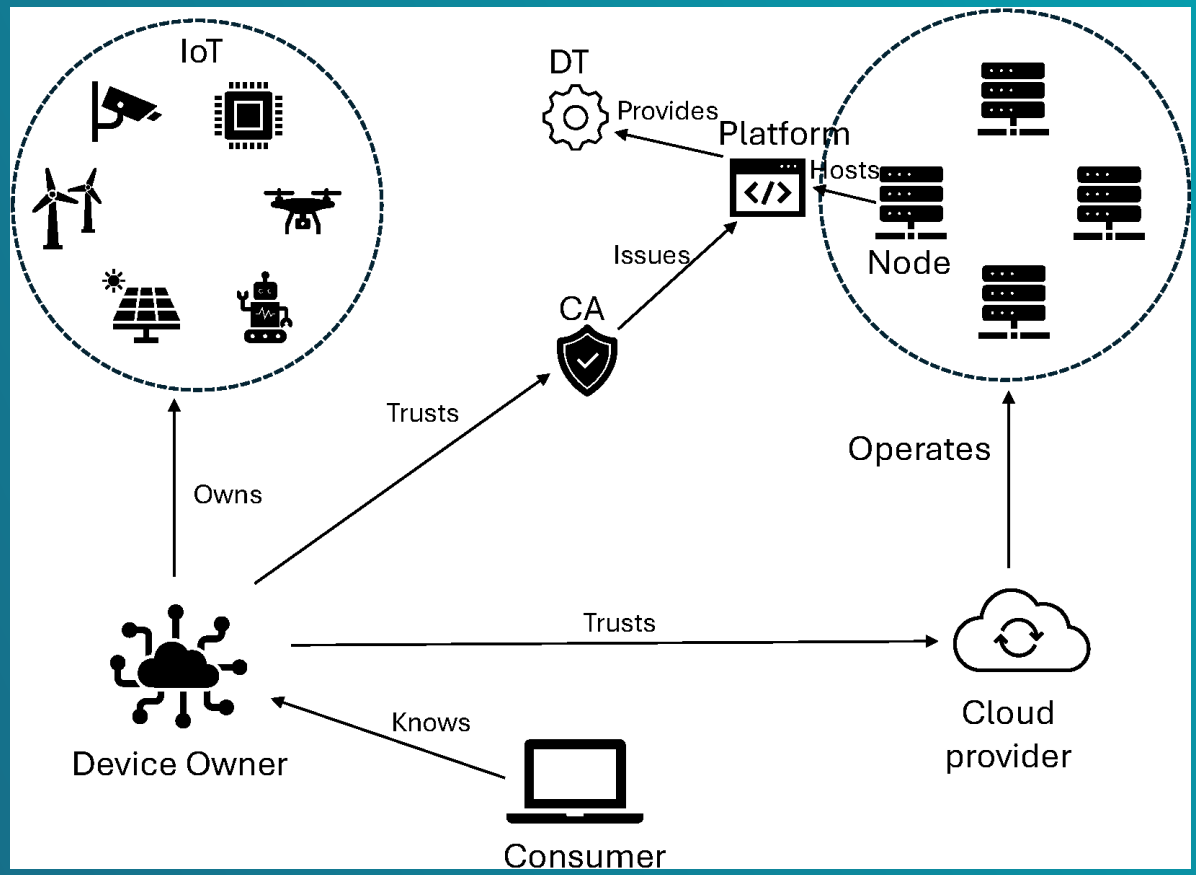
Design

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ  ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

THE UNIVERSITY OF MEMPHIS

System Model

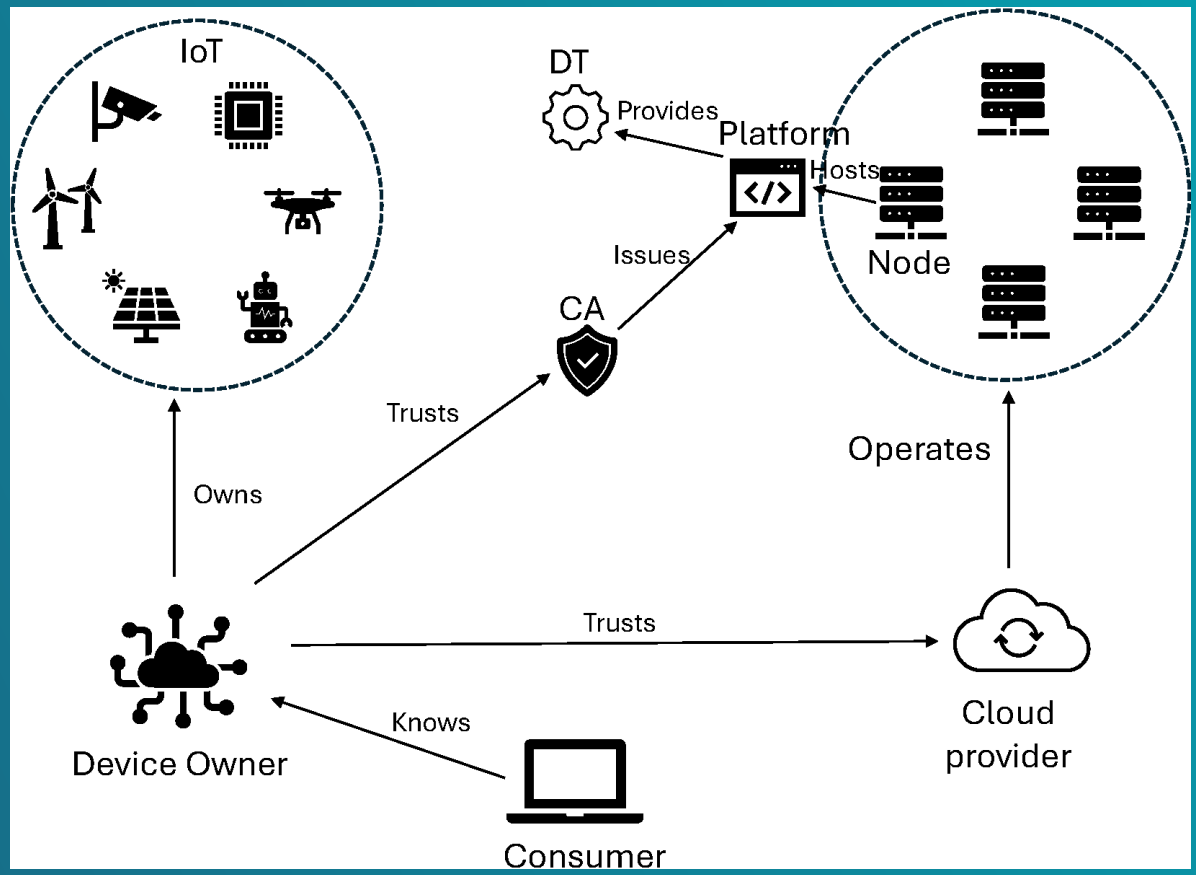
- (IoT) Device owner
  - Identified by $Owner_{URL}$
- Content consumer
- Cloud provider
- Certificate Authority
  - Identified by CA_{URL}
- DT platform
  - Offers DT instances
  - Identified by $Instance_{ID}$
  - Implementing API (NGSI-LD)



NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Trust Relationships

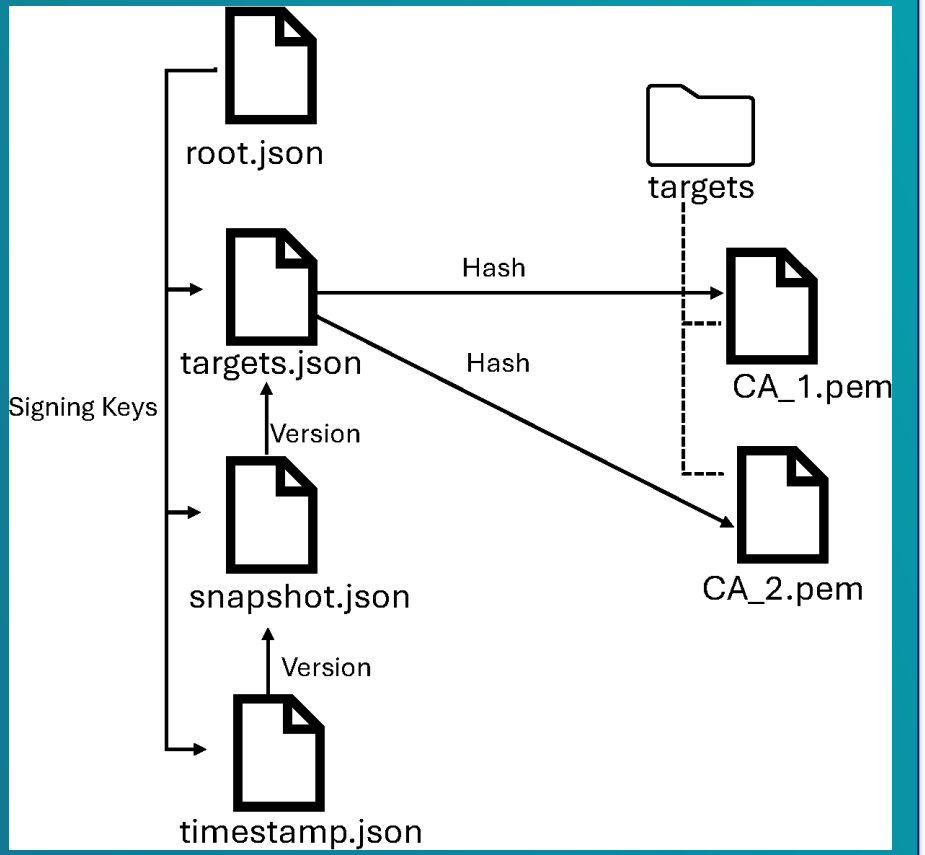
- Consumers know $Owner_{URL}$
- Owners know $Instance_{ID}$
  - Attested by cloud provider
  - Example: digest of binary
- Instances get certificates
  - From CA trusted by owner
  - Binding owner to instance
- Consumers will learn
  - The CAs trusted by owner
  - The instance's certificate



NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Trusted CA Management

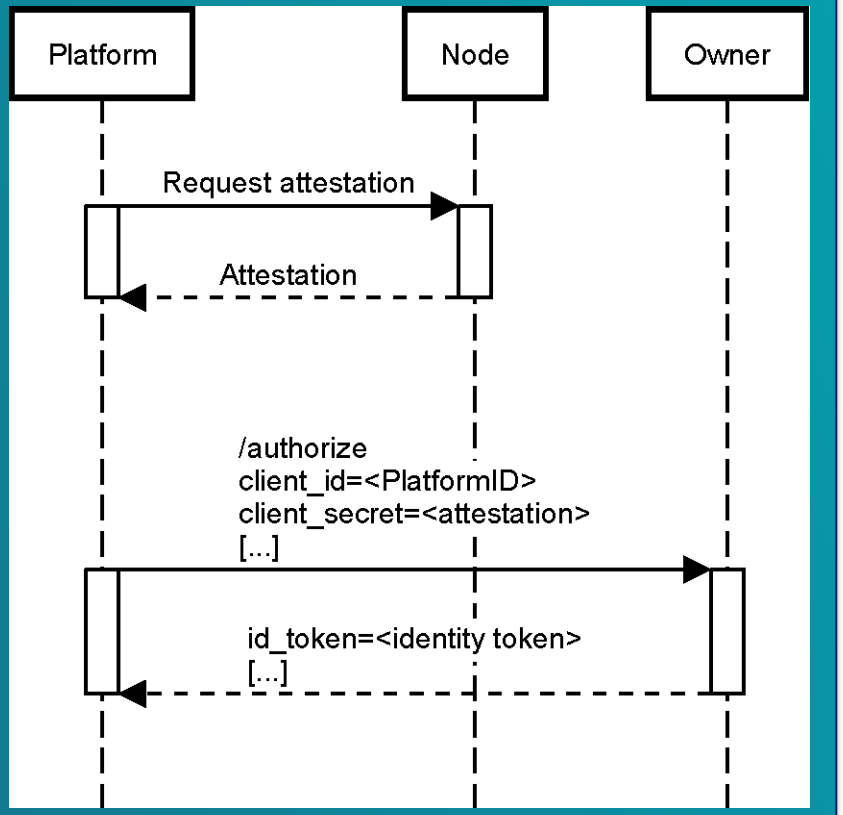
- The Update Framework (TUF)
  - Disseminates PKs to consumers
  - PKs stored in target files
- Device owner defines four roles
  - Root: PKs for other roles
    - Its PKs transmitted out-of-band
  - Timestamp: hashes of snapshot
    - Periodically refreshed and signed
  - Snapshot: versions of root and targets
  - Targets: hashes of target files



NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Platform Bootstrapping

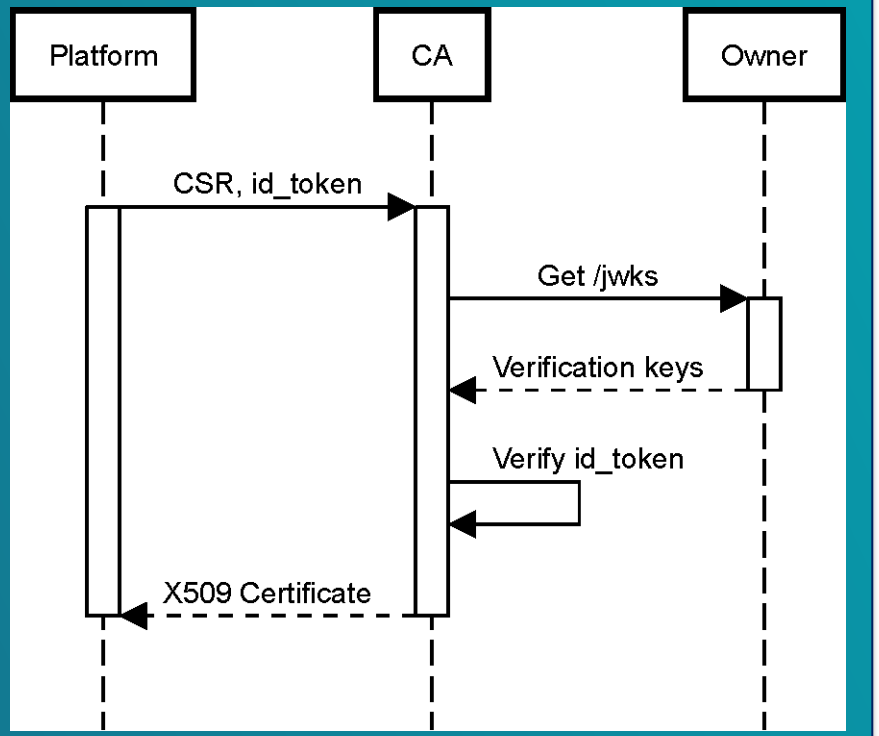
- DT instance requests attestation
  - Proves $Instance_{ID}$ is legit software
  - Signed by cloud provider
- DT instance asks for identity token
  - Uses OpenID connect with owner
  - Sends its attestation as proof
- Owner generates OpenID token
  - Binds $Instance_{ID}$ to owner and CA
  - Token can be used to get certificates



NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Certificate Issuance

- DT instance asks for certificate
  - Using its OpenID token
  - Creates new key pair and CSR
  - CA uses OpenID to get owner keys
  - Checks token is signed by owner
  - Checks token is new and not expired
- CA issues certificate
  - Indicates $Instance_{ID}$ and $Owner_{URL}$
  - Certificate is short-lived (10 min)



NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Signing and Verification

- Consumers ask DT instance for data
  - DT responds with IoT device's state
  - Responses are signed with key corresponding to certificate
- Consumer uses owner as root of trust
  - Uses TUF to get PKs of CAs trusted by owner
  - Uses CA PKs to verify DT instance's certificate
  - Uses DT's PK to verify responses
- The process is completely automated
  - New certificates issued every few minutes

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Evaluation

NGI

ExcID

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

THE UNIVERSITY OF MEMPHIS

Implementation & Performance

- Publicly available prototype in github
  - https://github.com/mmlab-aueb/certificate-management
  - DT instance implements NGSI-LD API
  - Platform identified via SPIFFE
  - Attestations use SPIRE
  - Custom OpenID provider for owners
- Performance evaluation
  - Owner and DT in same cloud provider
  - Public instance of Fulcio as CA
  - Measurements on i5 CPU in Ubuntu 22.04

Process	Time (ms)
Attestation issuance	1
Identity token issuance	4
Certificate issuance	390

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Security Evaluation

- Man-in-the-Middle attacks
  - DT – consumer: cannot create valid signature
  - DT – owner: use nonces to avoid CSR replay attacks
- DT platform compromise
  - Only already verified instance are susceptible
- OpenID provider compromise
  - Certificate Transparency to detect third party certificates
- Malicious CA
  - TUF only allows trusted CAs, multiple root keys used

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Conclusions

NGI

ExcID

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

THE UNIVERSITY OF MEMPHIS

Summary

- Certificate management solution for DTs
  - Automated certificate issuance
  - Securely binds DTs to IoT devices
  - Frequent certificate issuance
  - No IoT device secrets maintained at DT
  - Uses existing protocols and mechanisms
- Future work: integrate transparency services
  - Prevent fake certificates or attestations
  - Enable certificate verification after keys expire

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS

Thank you

https://mm.aueb.gr/projects/snds

NGI ExcID ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS THE UNIVERSITY OF MEMPHIS