Digital Certificates for IoT

a cooperation between RISE SICS and Nexus Group

Nexus Group
Martin Furuhed – Product Manager
Secure access control

Enable e-commerce and online banking

Enable e-services in the public sector

Provision your access cards

Protect communication between things

Manage physical and digital access
eID’s for people and computers are used daily, enabling trusted services.
Both sides authenticate using keys and certificate - eID

- the certificate contains information that identifies the individual and the service
- the certificate is issued by a party trusted by both sides
- end-to-end encrypted channel between known parties enables trusted services
Equipment identified similarly

To protect a private network, only identifiable equipment is allowed to connect

- certificates are used for identifying equipment in networks
- essentially the same type of certificates as for individuals
- administrators typically create keys and install certificate in a partly manual process
  - enrollment: the process of certifying digital keys/certificates
Billions of things – the same principles

Certificates scales well for enabling secure connection to many devices, but...

- Smallest devices, e.g. sensors, lacks a user interface
- Mostly resource-constrained devices, low-end CPU
- May operate in unreliable wireless network environments
- Unattended battery powered devices
- There has been no suitable automated certificate enrollment protocol
IoT security

Transport protection
- Encryption
- Mutual authentication

Device security and integrity
- Tamper proof or tamper resistant
- No default passwords
- Secure update mechanism

Accumulated data
- Encrypt data according to policies and external requirements
- Enforce data access policies
- Monitor for unusual activity
- Strong authentication
Constrained devices

Minimize data and power consumption

Autonomous operation

- CoAP instead of HTTP
- UDP/DTLS instead of TCP/TLS
- Slow wireless connectivity
- Device must request certificate in an automated way
- ECC keys instead of RSA

Contiki OS - client side work by RISE SICS
Certificate Management

Role of the CA

- Support enrollment protocols
- Approve request
- Issue certificate
- Revocation handling
- Short-lived certificates
- Key life-time
- etc
CEBOT
Certificate Enrollment in Billions of Things

Cooperation between RISE SICS and Nexus

Equip IoT devices with capabilities to obtain certificate(s) in a secure and automated way and by using the communication protocols that these devices speak.

Based on the EST standard for issuing certificates is a new standard needed, suitable for battery powered devices, slow networks, and support unattended operation over years.
CEBOT
Making a lightweight version of EST

Enrollment over Secure Transport (EST)

- HTTP based EST standardized in 2013 (RFC 7030)
- Suite more powerful devices
- Combines functions from earlier protocols and with better security
- EST supports for example:
  - CA certificate download
  - Initial certificate and renewal
  - Key pairs can be requested from CA
  - Encryption algorithms RSA and ECC
CEBOT Results

Client side implementation in the Contiki OS for automated enrollment of certificates using EST over CoAPs

Server side support in Nexus Certificate Manager for issuing certificates using EST over CoAPs

IETF draft prepared together with Philips and CISCO
https://www.ietf.org/id/draft-vanderstok-ace-coap-est-02.txt
The SecureIoT project

Eurostars approved project
- Sweden and South Korea
- Nexus, RISE SICS, Ajou University, KAIST University, Apros, Lily

Continues where CEBOT ended
- How the first certificate can be issued automatically to a device, without human intervention, and how the device can be identified in that process.
- Reduce size of certificates by profiling content and by compression while in transfer
- Revocation management for IoT environments
- Standardization, new functionality in products
Current result SecureIoT project

The lightweight version of X.509 certificate for IoT by profiling on a reduced content.

Compression of and encoding schemes for the profiled certificate to reduce certificate size while in transfer over 6LowPAN.

Result: low memory footprint, low computational complexity and minimising of data in transfer.
A possible project for investigating and bringing secure communication to environments consisting of many and different types connected entities, for example within and among autonomous vehicles.