A new Authorization Framework for Internet of Things

Ludwig Seitz
ludwig@sics.se

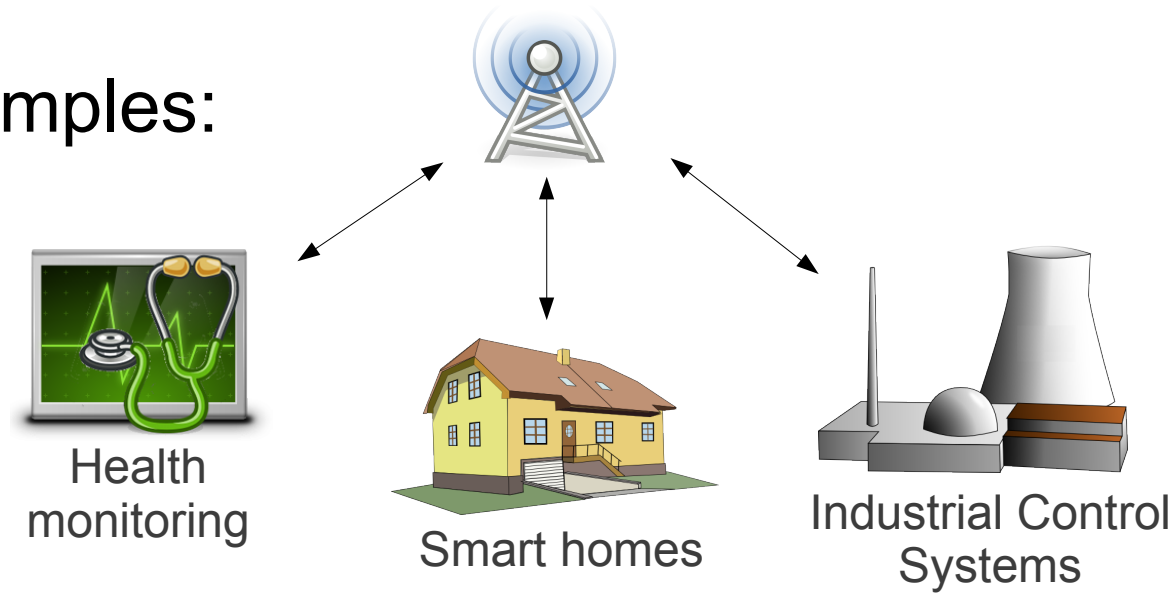
ERICSSON

SWEDISH ICT SICS

Introduction – Internet of Things

Everything that benefits from Internet connection gets connected

Examples:



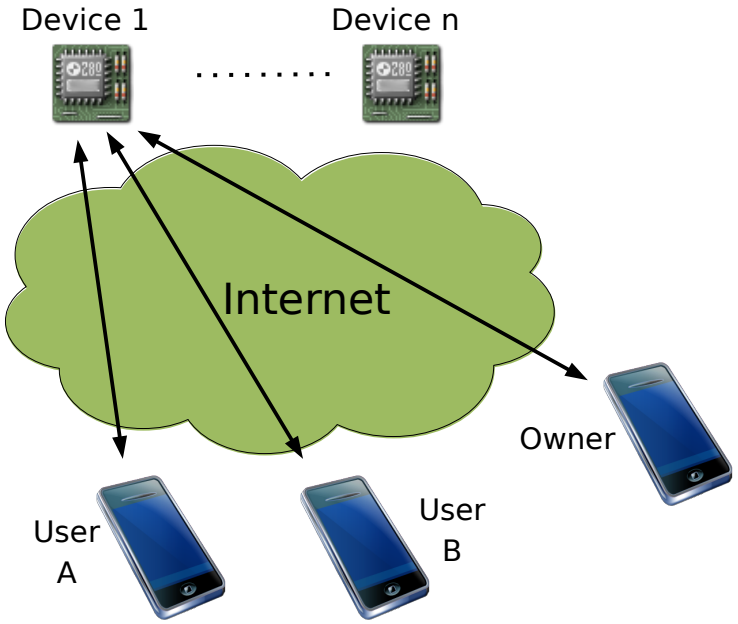
Introduction – Security Issues

- Devices previously in closed environments become globally accessible
  - e.g. Industrial Control Systems
- Devices can handle very sensitive data
  - e.g. Medical sensors
- Novel business models need new access modes
  - Currently: all or nothing (root access)
  - Needed: e.g. pay-by-use, limited anonymous access

Overview

Scenario:

- Network of devices (sensors, actuators)
  - Little memory, small processor
  - Resource owner controls access
  - Users access resources on device



Our goal:

- Provide fine-grained access control
  - Multiple users with different rights
  - Decisions per user, resource and action
  - Based on dynamically changing parameters

ERICSSON SWEDISH ICT SICS

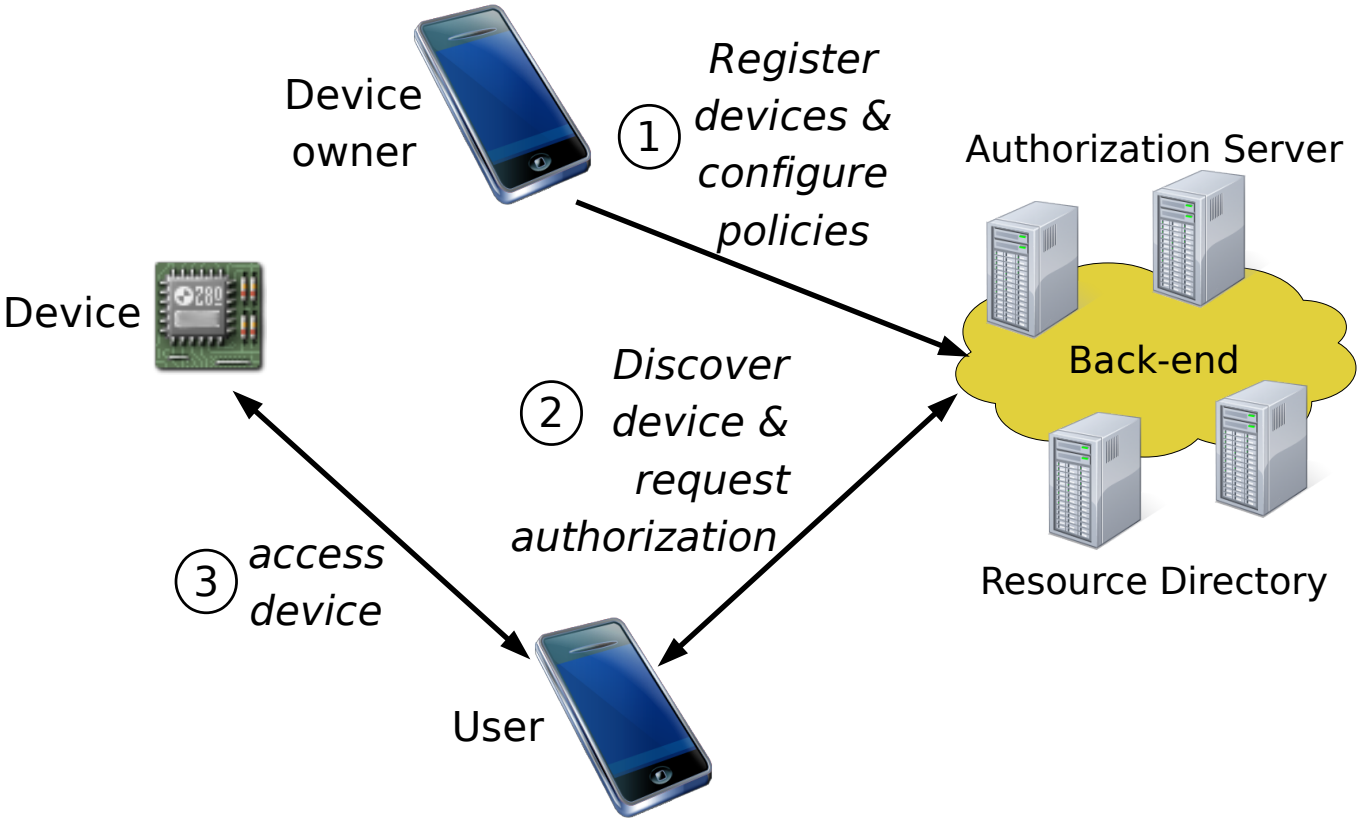
Assumptions and Prerequisites

- Communication Channel: CoAP
  - Lightweight, UDP-based alternative to HTTP
  - Developed by the CORE group at IETF
- Communications security
  - Secure channel or Object security
- Authentication
  - Pre-shared keys or Public Key Infrastructure

Requirements

- Differentiated access control rules for different requesting users
  - Local enforcement of certain conditions (e.g. on device-state, position, time)
- Minimal communication requirements and low computational overhead
- Protect access control information itself
- Dependent on a minimum of other functions
- End-to-end protection of protocol messages

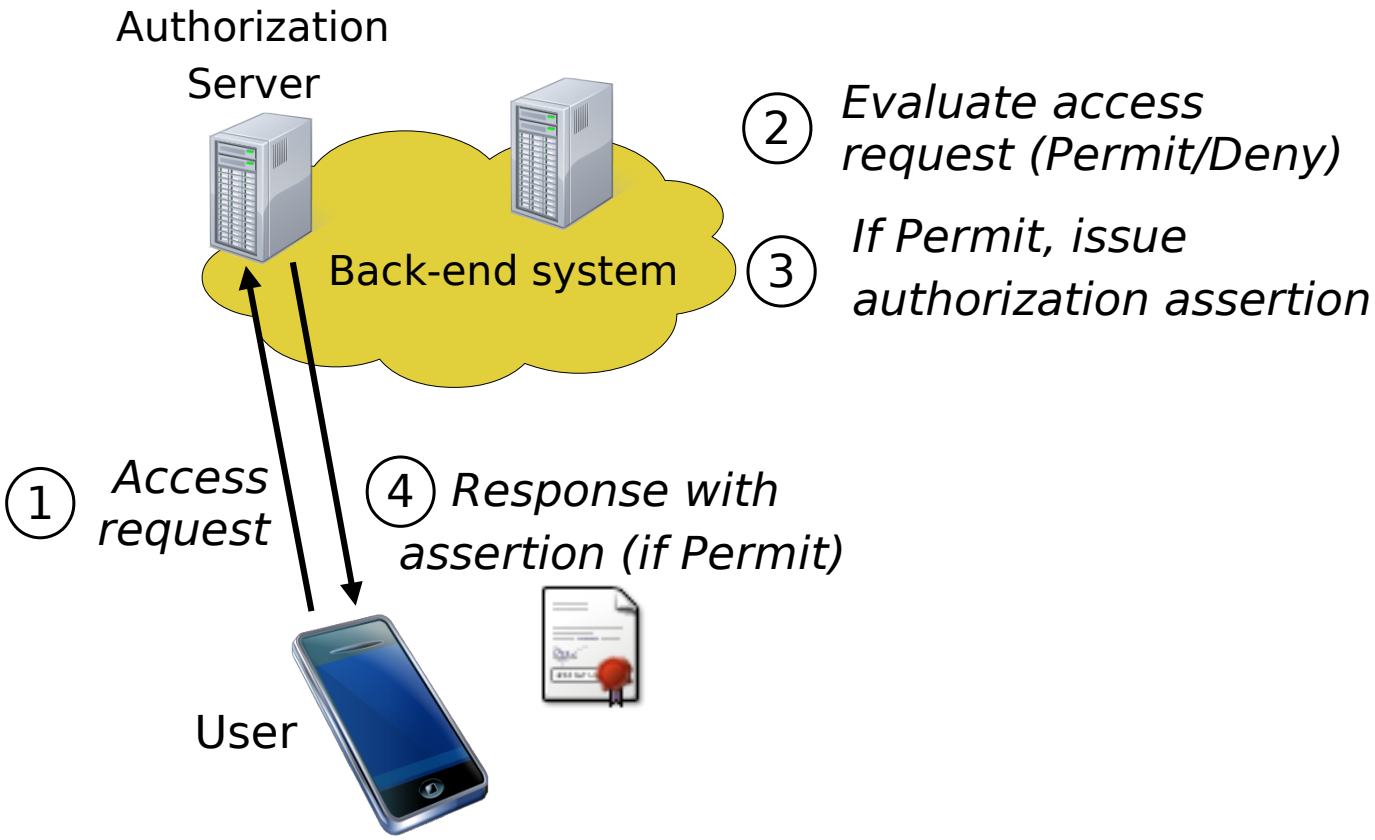
Our Architecture



ERICSSON

SWEDISH ICT SICS

Access procedure



Assertion format

- Based on XACML and SAML
  - Standards for access control and security assertions (OASIS)
- Subsets of the full standards
  - Reduce processing overhead & libraries on device
- Compact representation in JSON

  ~ 250 bytes JSON vs ~ 2500 bytes XML

Conclusion

- Authorization framework for IoT
  - Standards-based, but adapted to IoT
- Key components:
  - Authorization Server
  - Assertion format
- Future work:
  - Communications security alternatives
  - Usability for policy administration

WWW.SICS.SE

Assertion format example

	01 {
Assertion Identifier	02 "ID": "ID_ffda55f9...097bdd21e6",
Issue instant	03 "II": "2013-02-15T10:02:52Z",
Issuer	04 "IS": "AAA-Server",
Subject (key)	05 "SK": "BvDgLAXSHe...0RLhfwS1fue",
Statement	06 "ST": {
Obligation	07 "OB":{
Not before	08 "NB":"09:00:00Z",
Not after	09 "NA":"17:00:00Z"
	10 }
Action	11 "ACT": "GET",
Resource	12 "RES": "coap://node346/tempSensor"
	13 }
	14 }

ERICSSON

SWEDISH ICT SICS

Securing communication

- DTLS
  - TLS over UDP
  - Problem: session establishment time
- Object security
  - Based on JOSE standard drafts at IETF
  - Problem: Key establishment

Authentication

- Pre-shared keys between Device and Authorization Server
  - High setup cost
- Public Key Infrastructure
  - Heavyweight management, e.g. distributing CRLs, installing root certs
- SPKI-like approach
  - Public keys function as identifiers