Smartie

A secure IoT integrating platform for data dissemination will benefit all stakeholders and citizens of Smart Cities

Secure and sMARrter ciTIes Data ManagEment

A European Project

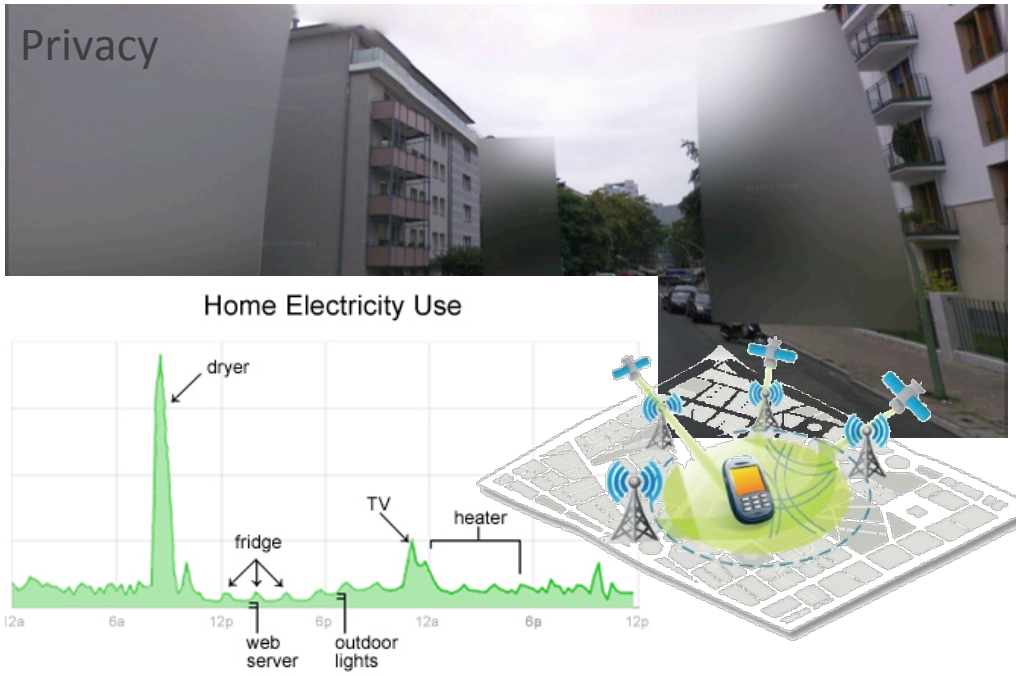
Outline

- Introduction to SMARTIE
- SMARTIE authorization perspective
- Conclusions

IoT for Smarter Cities

- Future technology ecosystem
- Challenging
  - Big scale
  - Security
  - Interoperability

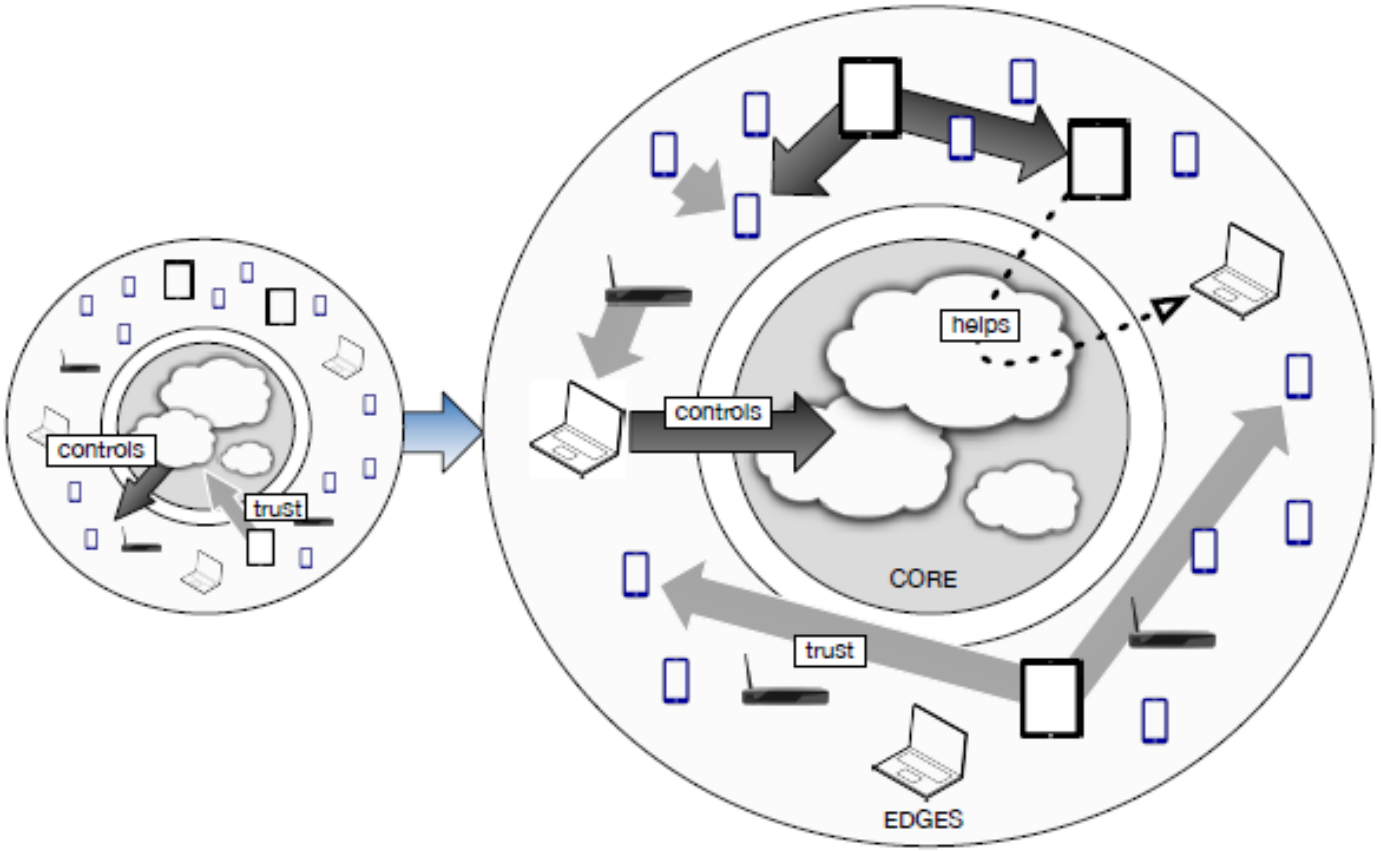
SMARTIE Project's perspective



- User-centric privacy & security for keeping citizens' trust on the IoT
- Security poorly applied
  - Lack of interoperability

SMARTIE Project's perspective

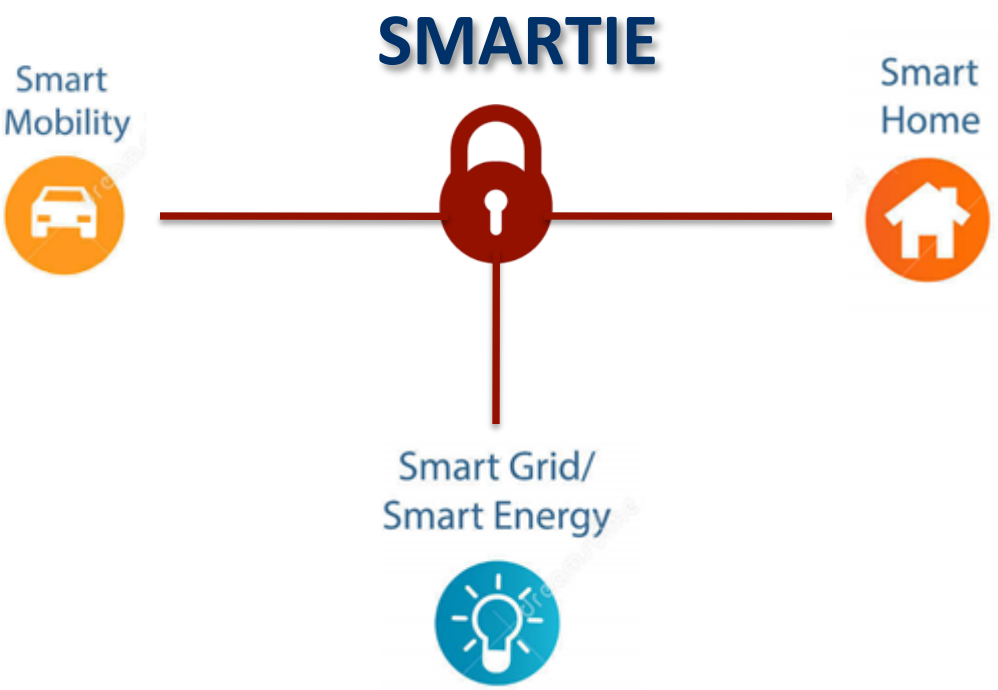
- For the incoming era of Fog/Edge computing, interoperability and (interoperable) security is one of the key enablers



From "Edge-centric computing: Vision and Challanges", ACM SIGCOMM Computer Communication Review, Oct. 2015

SMARTIE Project's perspective

- Prototype, integrating platform for efficient and secure dissemination of city data
  - Lightweight security
    - ECC, PANA
  - Decentralized authorization models
  - User-centric policies
  - Secure data storage
- Architecture generated under the guidelines of the IoT Arquitecture Reference Model (IoT-ARM)



SMARTIE Consortium

World-wide telco (64%, 19% and 17% of PT Innovaçao market set in Europe, Southamerica and Africa, respectively), based in Lisbon

World-wide research center (Europe, North America and Asia). In Heidelberg (Germany), more than 100 employees, focus on security and IoT

Research center based in Frankfurt (Oder)

Startup for ITS solutions, funded in 1998, based in Frankfurt (Oder)

Startup establish in Serbia (Novi Sad) in 2006, around 40 employees, focused on research on IoT

Public University in the Region of Murcia, founded in 1272

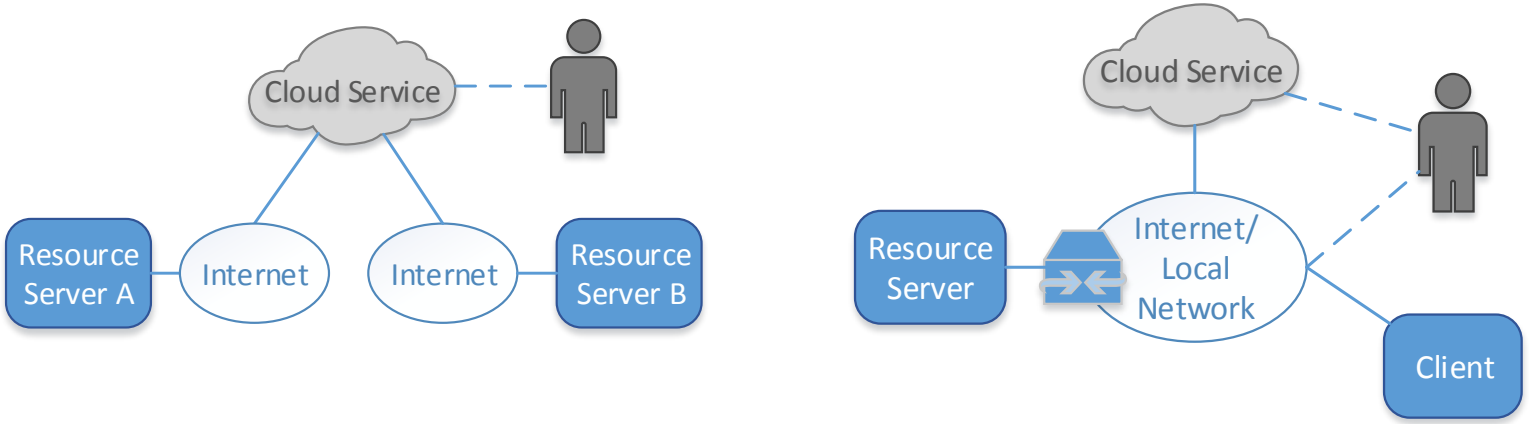
Governmental institution for the development of Region of Murcia

Outline

- Introduction to SMARTIE
- SMARTIE authorization perspective
- Conclusions

IoT Access Control

- Typical IoT communication relies on cloud services and application-level GWs

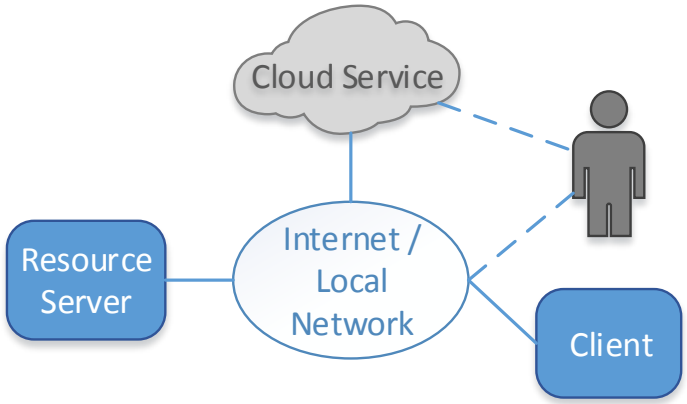


RFC 7452: Architectural Considerations in Smart Object Networking

- Lack of standardization and research on decentralized access control
  - IoT providers generally rely on Access Control Lists
  - Flexible solutions are necessary for device-to-device interoperation

IoT Access Control

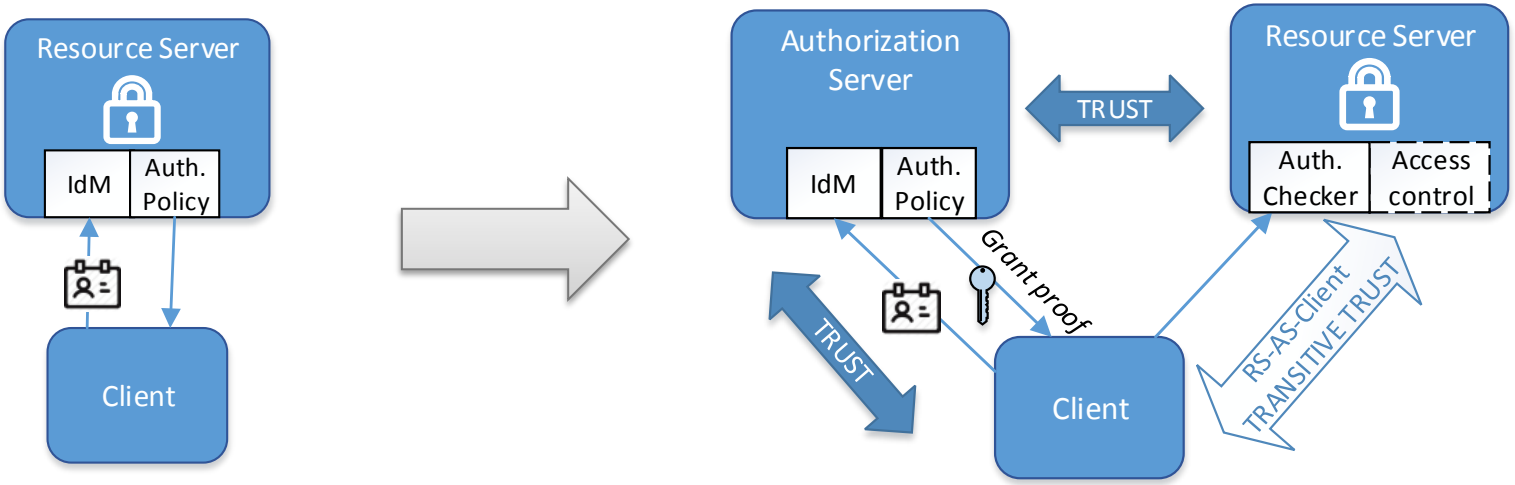
- Massive scale of smart cities require decentralized access control
  - Scalability, constrained devices
- Standardization will promote interoperation
  - Separation between the application logic (done by less-constrained servers) and access control (done by more-constrained devices)
- Assurance of security



- SMARTIE aims at deeply analyzing the impact of access control
  - Implementation of token-based decentralized access for CoAP
  - Encryption-based access control

IoT Delegated Authorization

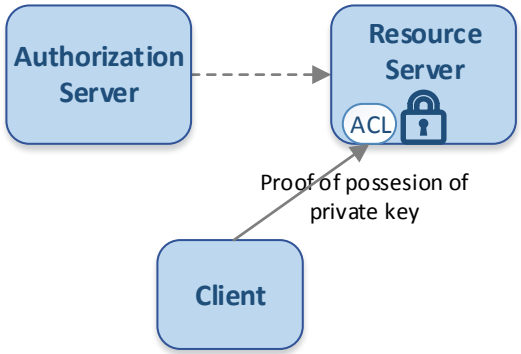
- Device-to-device access control with security…



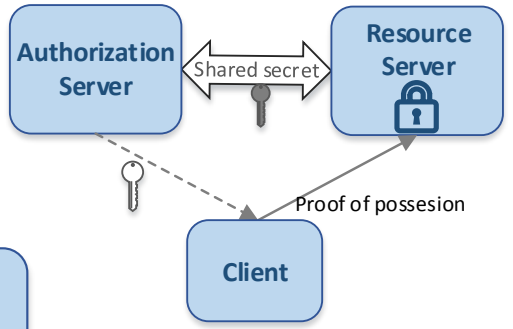
- Client authentication is essential for the IoT
  - Bearer tokens must be avoided
  - It relies on the confidentiality of cryptographic material between clients, RSs, and ASs.
- Application-level authentication is gaining ground

IoT Delegated authorization

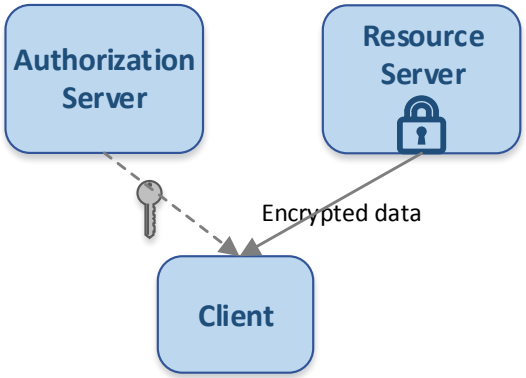
- Cryptograhpic identities pre-configured at the RS
  - AS-to-All model
  - Clients sign the request to the RS
    - Public or symmetric key



- Client identities are not known in advance
  - AS-to-client model
    - Client's symmetric key derived from the AS-RS shared secret

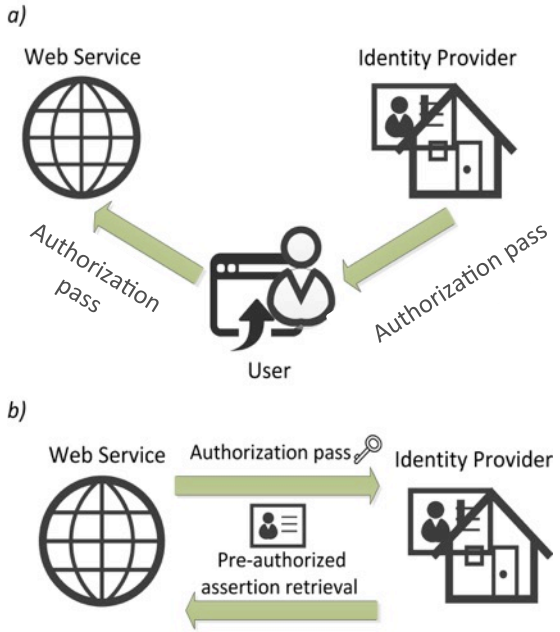


  - Decryption-based authorization
    - RS does not verify authorization
    - Group communciation



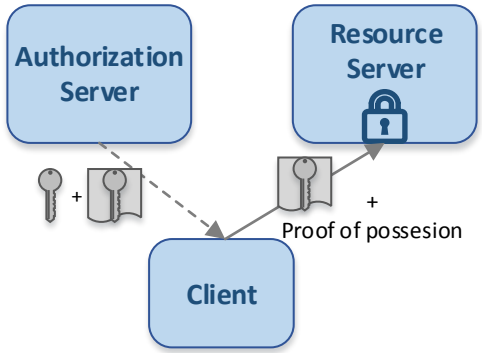
IoT Delegated Authorization

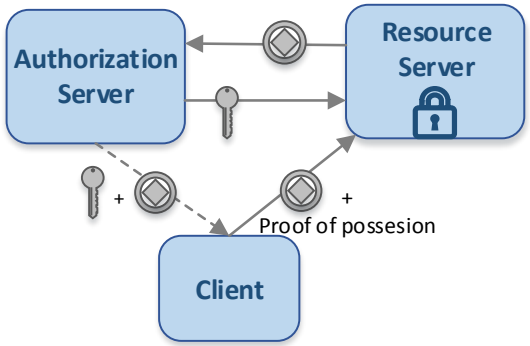
- IETF proposal for Authentication and Authorization for Constrained devices (ACE)
- Based on Proof-of-Possession (PoP) tokens
  - Improve client authentication in OAuth (bearer tokens) by adding proof-of-possession
- OAuth: Delegated Authorization for the Web
  - Extensively used as authentication protocol for Web Single Sign On (SSO)
  - Still, a generic delegated authorization protocol
  - Access token for resource retrieval
    - Bearer token approach → only possession of the access token is enough to grant the holder access



IoT Delegated Authorization

- IETF proposals:
  - Self-contained authorization pass consumed by the RS
    - With the client's symmetric key
      - Encrypted with the AS-RS secret key
    - With the client's public key
      - Signed by the AS's public key
    - Client proves possesion of the token's key
      - DTLS
      - Object security
  - Introspection method when the RS is not able to evaluate the token





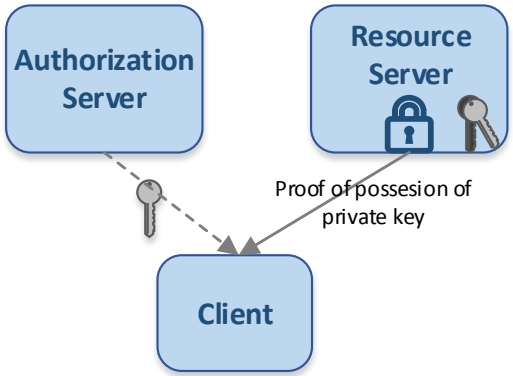
Client Authentication in IoT access control

- Relevant security features should be considered
  - Authorization scope limitation
    - AS should be able to limit the scope of authorization grants
    - The RS should be able to verify the grant scope
  - Access revocation
    - AS should be able to revoke a client's authorization grant
  - Secure access when the AS is offline may be a requirement (offline AS-RS and offline AS-client)

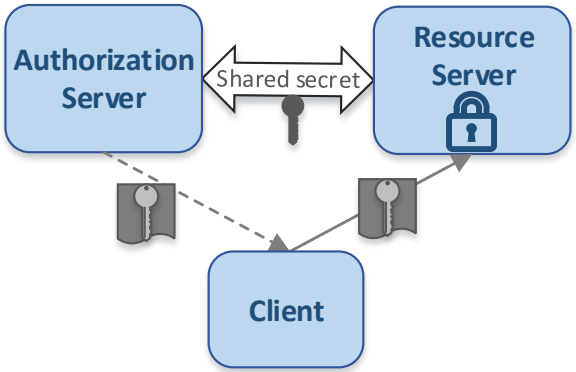
	Scope limitation	Authoriz. Revocation	Offline AS-RS	Offline AS-client
Authorization pass	OK	After pass' lifetime	OK	During pass' lifetime
AS-to-client	Client request	X	OK	OK
Content decryption	Key scope	Group key update	OK	OK
AS-to-All (ACL)	OK	OK	OK if no auth. changes	OK
Introspection	OK	OK	X	During token lifetime

Server Authentication in IoT access control

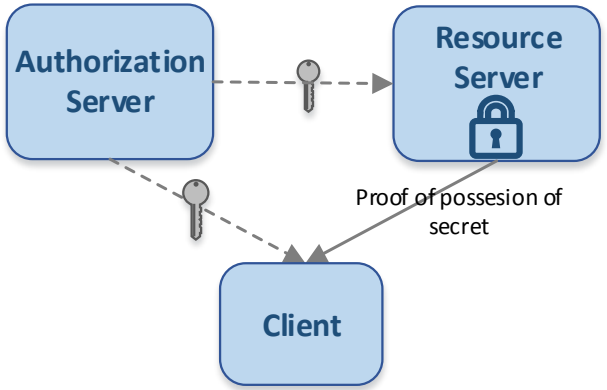
- Server authentication is mainly done by proof-of-possession of a private key



Public key



Decryption-based



Key-possession

SMARTIE authorization & authentication

- Pass-based delegated authorization
  - With fine-grained rules, validity period.
- Implicit authorization for highly-efficient data dissemination
  - CP-ABE encryption for notifying (delay intolerant) data consumers
  - Data is encrypted with specific attributes that have been associated to the consumers
  - Only consumers holding the correct attributes can decrypt the data
  - Sub/pub through the IoT broker
    - Decryption keys are delivered to subscribers when they ask for authorization (i.e., they get a capability token)
    - IoT broker and AS synchronize encryption attributes
    - IoT broker receives data from sensors and encrypts it with the appropriate attributes before notifying consumers
  - Very efficient for data distribution to groups
    - No need for individual authorization, the IoT broker does not consume capability tokens

Outline

- Introduction to SMARTIE
- SMARTIE authorization perspective
- Conclusions

Conclusions

- SMARTIE is an integrating platform for secure data dissemination
  - Developed under the guidelines of the IoT-ARM
- Scalable decentralized authorization models
- The best delegated access control method depends on the system's needs
- Further analysis of the methods' overhead on IoT devices is needed
- The next step will be to analyze inter-domain authorization

Thank you for your attention!