Outline

- Context of the work
- The problem addressed
- Credentials distribution vs data distribution
- Security architecture
- Possible evolutions
- Conclusion
Projets introduction

- SUNSEED: Fp7 EU funded project; Smart grids communications involving Data acquisition nodes spread over the electrical grid.
  - Nodes based on Intel Edison board Embedded secure elements on devices for enhanced credential protection
  - Communications via PLC, fiber, or 4G networks
  - Use of publish/subscribe protocols: MQTT and XMPP
  - Authentication via client certificates and PKI
  - Real life deployment in Slovenia
  - http://sunseed-fp7.eu

TILAS: celtic funded project; communications for smart cities applications. Nodes are spread in the cities
  - Tiny nodes (esp8266) using wifi communications
  - Use of MQTT publish subscribe protocol
  - Authentication via userID/password
  - http://www.tilas.eu
IOT applications; heterogeneity is the Rule

IOT applications often involve several communication hops
Intermediate nodes may be controlled by different entities

Object 1

Object 2

Goals:
- Authenticate entities and secure every single hop of the communication path
- Possibly secure communication from source to destination with a single set of credentials
- Manage authorizations (fine grain) in every node

Application A
Application C
Application C
Real case exemple

IOT applications often involve several communication hops
Not all controlled by the same entity
Delegated security management

Principle: separate data and credentials distribution paths

Benefits:
- The business entity distributing data may be different from the business entity distributing credentials
- Possibility to outsource security
- True end to end security is possible (single set of credentials from Source to Destination)
Building on the UMA idea

User-Managed Access (UMA) from Kantara Initiative is an OAuth-based protocol designed to give a web user a unified control point for authorizing who and what can get access to their online personal data, content, and services, no matter where all those things live on the web.

My Pictures somewhere on the web

My Pictures somewhere else on the web

My Pictures in a 3rd place on the web

Centralized access control system; single place to define access control to all of my pictures
UMA Principle

1. Publish resources description

2. Resource access without Access Token redirects the client to the authorization server

3. Client request Access Token to the authorization server

4. With Access Token, client will be granted access to resources
Extending UMA idea

1. Publish resources
   - Publish Clients
   - Publish rights

2. Resource access without Access Token redirects the client to the authorization server

3. Client request Access Token to the authorization server

4. With Access Token, client will be granted access to resources
Exemple Application for a smart city use case

MQTT broker

middleware

Authorization server

Esp8266 client

Web application

1. Request resource access

2. Obtain Access token (mqtt credentials)

3. Publish

Resources management
Client management
Right management

Publish resources
Publish clients
Publish rights

Obtain Access token (mqtt credentials)

Subscribe

Publish

Request resource access
The programmer perspective

 Traditionnal code:

```
mqttBroker=my.mqttbroker.com
mytopic=« helloTopic »;

UserID=XXX;
Password=YYY;

Handle=
    Mqtt_Connect(userID,password, mqttBroker);

Handle.publish(myTopic, »hello World »);
```

Delegated code:

```
mqttBroker=my.mqttbroker.com
mytopic=« helloTopic »;

(UserID,Password)=getCredentials();

handle=
    Mqtt_Connect(userID,password, mqttBrkAddr);

If( getPermission(MyTopic, »publish »)) {
    handle.publish(myTopic, »hello World »);
}
```
Benefits/Possible evolutions

- **Benefits**
  - Credentials are distributed dynamically; they may be updated periodically
  - Possibility to synchronize credential provisionning in multiple resource servers
  - Centralized management of authorization in multiple systems

- **Possible development tracks**
  - Use lightweight Oauth (Oauth for IOT based on Coap)
  - Use data management protocols (such as LWM2M) for credentials provisionning
Conclusion

- Systems heterogeneity is the rule and not exception in IOT applications

- Credentials and authorization management in heterogeneous system may become very complex

- Delegated credentials and authorization management may simplify the problem

- A security architecture has been described and implemented in proof of concept prototypes.