OAuth/UMA for ACE

draft-maler-ace-oauth-uma-00.txt

Eve Maler, Erik Wahlström, Samuel Erdtman, Hannes Tschofenig

24th March 2015

Motivation

1. Need security and privacy in web. Authentication and authorization become an important component of Web security today.
2. Providing the same level of security functionality to the Internet of Things (IoT) environment.
3. IoT devices, however, have limitations.
4. Web and IoT is a continuum rather than an either or.
5. Would like to use the same approach for managing services, user accounts as well as devices.

1. Need security and privacy in web. Authentication and authorization become an
important component of Web security today.
2. Providing the same level of security functionality to the Internet of Things (IoT)
environment.
3.
IoT

Extract from IETF ACE Charter

specifications.”

Door Lock Use Case

Players in this Scenario

Joe works for a maintenance company and is specialized in installing physical access control systems

Alice is the owner of the small but widely known company example.com. She wants to deploy a new physical access control system in her office building.

Tom is employed by Alice at example.com.

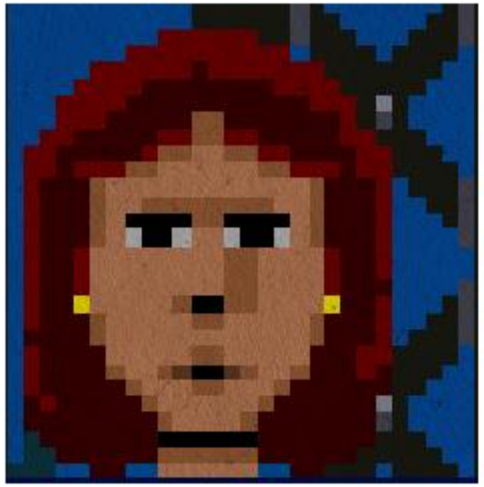
Installing Door Locks

Joe works for a maintenance company and is specialized in installing physical access control systems

Joe configures the door lock with

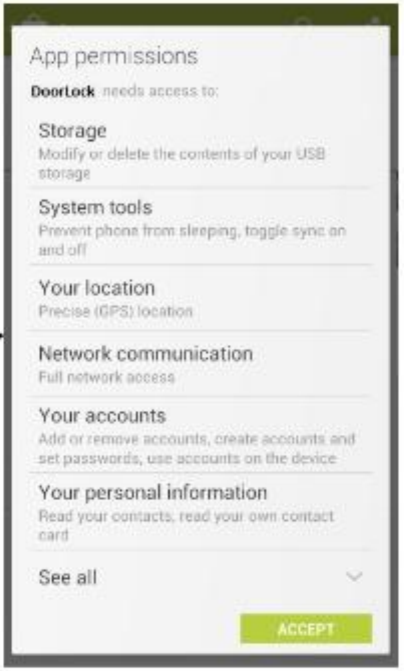
Joe configures the door lock with

server.



Alice is the owner of the small but widely known company example.com. She wants to deploy a new physical access control system in her office building.

(1) She downloads the DoorLock app to her phone.



App permissions

DoorLock needs access to:

Storage
Modify or delete the contents of your USB storage

System tools
Prevent phone from sleeping, toggle sync on and off

Your location
Precise (GPS) location

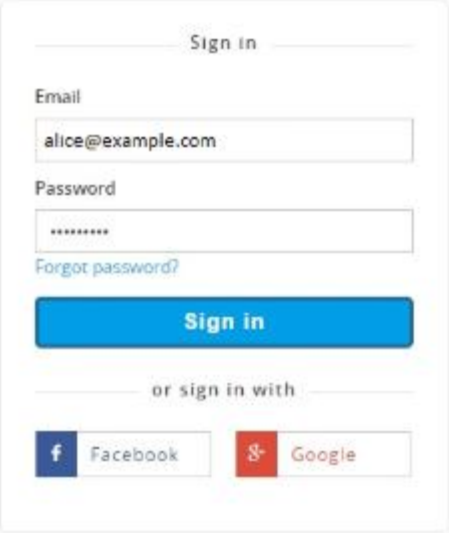
Network communication
Full network access

Your accounts
Add or remove accounts, create accounts and set passwords, use accounts on the device

Your personal information
Read your contacts, read your own contact card

See all

(2) The app needs to be configured for use with the enterprise access control system. Since the app knows nothing about her enterprise identity management system she has to login first.



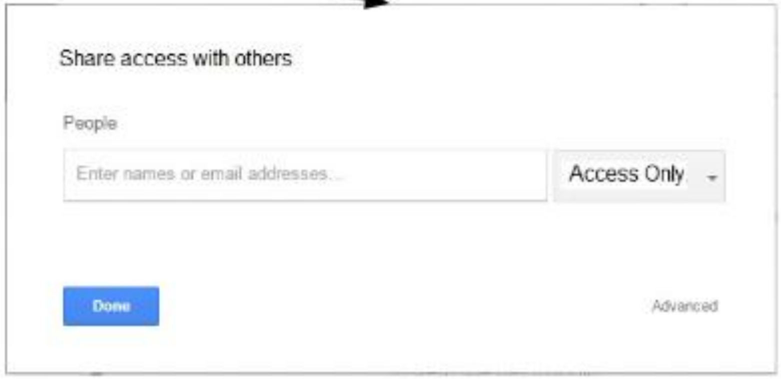
Sign in

Email: alice@example.com

Password: ••••••••••

(3) The DoorLock app uses OAuth 2.0 and no long-term credentials are visible to the app itself.

(4) Alice, as the admin, is now able to configure access policies for her five employees.



Share access with others

People

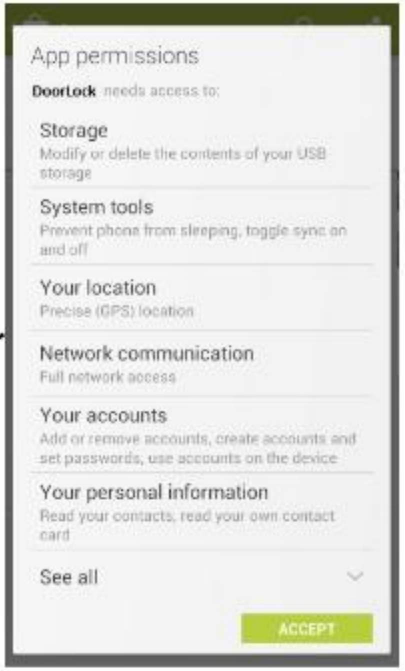
Enter names or email addresses...

Access Only

(5) Configuration completed. Access to all employees granted.

Tom is employed by Alice at example.com.

(1) Tom downloads the DoorLock app to his phone.



App permissions

DoorLock needs access to:

Storage
Modify or delete the contents of your USB storage

System tools
Prevent phone from sleeping, toggle sync on and off

Your location
Precise (GPS) location

Network communication
Full network access

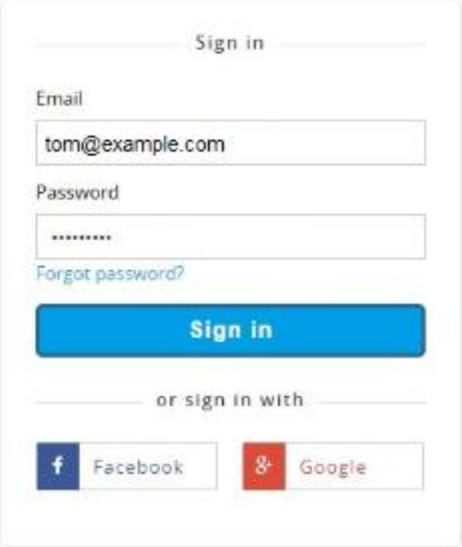
Your accounts
Add or remove accounts, create accounts and set passwords, use accounts on the device

Your personal information
Read your contacts, read your own contact card

See all

ACCEPT

(2) The app again needs to be configured. Tom logs into the enterprise identity management system. The DoorLock app uses OAuth 2.0 and no long-term credentials are visible to the app itself.



Sign in

Email: tom@example.com

Password: ·········

Forgot password?

Sign in

or sign in with

Facebook

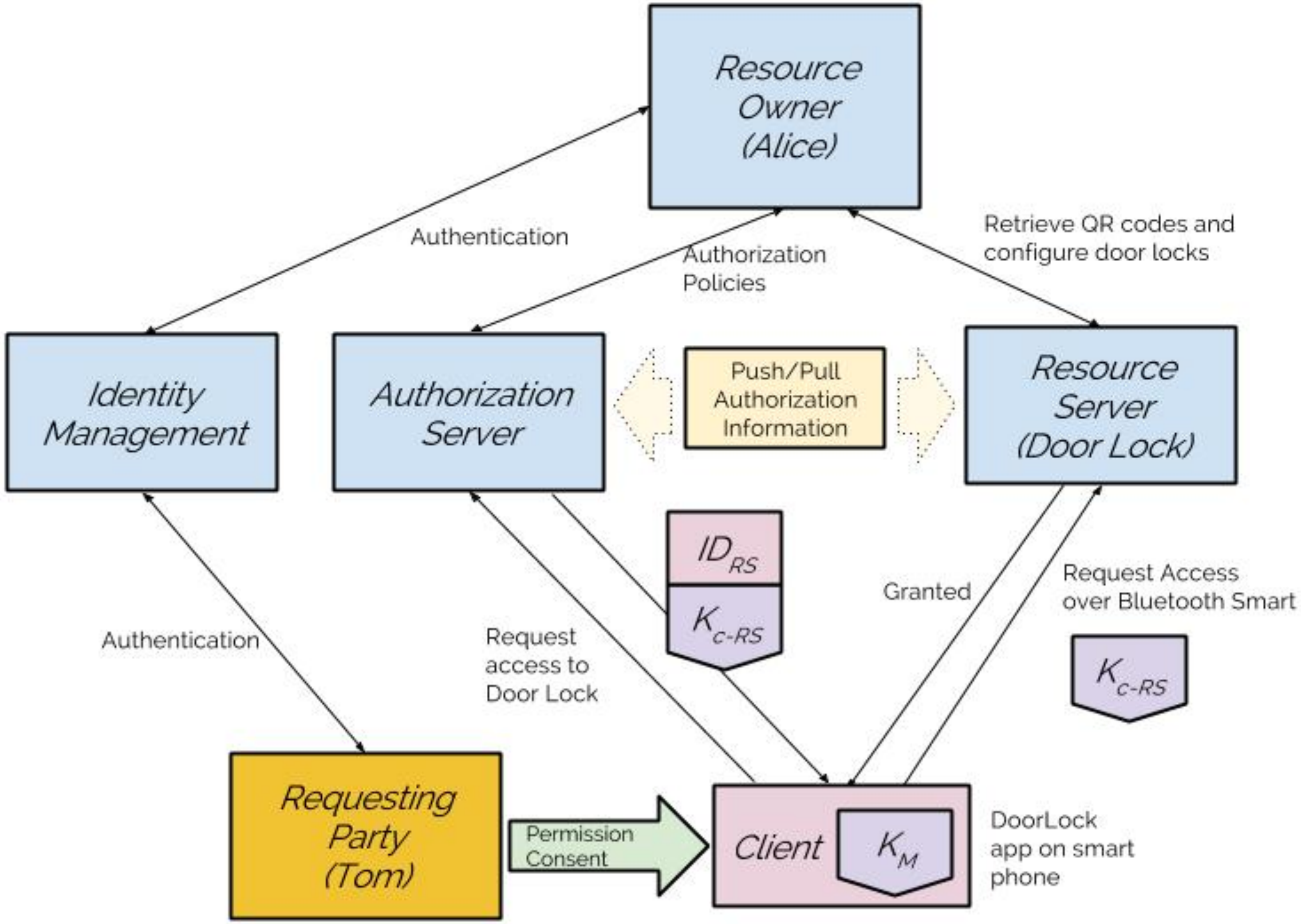
Google

(4) When Tom approaches the office with his newly installed DoorLock app for the first time the app talks to the authorization server and obtains an access token. Alice does not need to grant the request since Tom is already pre-authorized.

(5) The obtained access token is presented to the door.

(6) Tom is granted access.

Architecture for IoT with User Identity Management



Remarks

- … not the most complex scenarios but we need to pick others up where they are today.
- The presented scenario does not require many new extensions.
  - Mostly the communication between client and resource server.

What's Next?

- Technical solution details are available with UMA/OAuth/OpenID Connect specifications but optimizations are possible.
    - OAuth over CoAP profiles.
    - More compact token encodings
    - Ongoing work on PoP tokens and token binding.
- Looking for other interested parties to work on prototypes to gain more experience.