ForgeRock

The leading, next-generation, identity security software platform, driving digital business.

2010 Founded
10 Offices worldwide with headquarters in San Francisco
400+ Employees
600+ Enterprise Customers
50% Americas / 50% International commercial revenues
30+ Countries
With IoT, Identity Is Everywhere...
But So Is Risk.
IoT Challenges

- Security concerns
- Privacy
- Lack of a compelling business case
- Obtaining staff and skills to create the IoT strategy and systems
- Risks associated with business change and new business models
- Dealing with new and untried technology and service providers
- Workforce resistance to new technologies, practices or processes
Device created with some unique, immutable identifier – MAC, certificate

Synchronized and activated in central store

Device authenticates - to download API details, client credentials
Device Pairing Requirements

- Revoke device access when device is lost, stolen or sold
- Bind a token to a device – reduce impact of token theft from MITM
- Device should have scoped permissions
- Device needs to represent user to APIs & services
- Need to pair a device to a person
Device often has limited input capability and UI

“Pin & Pair” - user enters a unique device code out of band on their laptop/tablet

Device receives scoped access, with simple revocation

Simple out of band pairing

Device accesses services on users behalf

© 2017 ForgeRock. All rights reserved.
OAuth2 Device Pairing Flow - “Demo”

1 - Start registration
2 – Device gets code
3 – User enters code out of band on web page
4 - Device polls AS then pairs
5 - Device gets access token
6 - Device uses token against service
7 - Device can be revoked via end user dashboard

Images courtesy of Jon Knight, UK Customer Engineering

OAuth2 Proof-of-Possession Token Safety

Protect access_token through device binding

Device may not use HTTPS or a secure token storage area – need a method to protect hijacking or MITM

Use proof-of-possession with public key being baked into the access_token

Provides the RS an ability to initiate challenge-response to prove correct owner

Token request with pub key

Resource server uses key for challenge response
IoT Data Sharing Requirements

- Ability to share arbitrary data from a device to other users or services
- Ability for authorization policies to be created by end user not an admin
- Ability for end user to perform simple approval
- Ability to perform simple revocation
- Leverage simple standards for fast integration
# User-Managed Access

## My devices

<table>
<thead>
<tr>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>eHealthKit</td>
</tr>
<tr>
<td>Smartee Ehealth 1</td>
</tr>
<tr>
<td>e-Health Sensor Platform V2.0 for Raspberry Pi</td>
</tr>
<tr>
<td>Smartee Body</td>
</tr>
<tr>
<td>Smarthee Body 1</td>
</tr>
<tr>
<td>CardioTrack</td>
</tr>
<tr>
<td>Smartee Cardiotrack 1</td>
</tr>
<tr>
<td>Smartee Glucose Meter 1</td>
</tr>
<tr>
<td>Smartee Connected Glucose Meter</td>
</tr>
</tbody>
</table>

## Smartee Health Watch 1

<table>
<thead>
<tr>
<th>Heart Rate</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>4812</td>
</tr>
</tbody>
</table>

Devices make data! Needs protecting...

Devices registered & managed
User-Managed Access

- Ability for data owner to make easy access revocation decisions across

- Ability for data owner to make well informed and consent driven decisions
End-to-end IoT Identity Platform

FROM DEVICE TO CLOUD

Edge

IoT Services

Enterprise

Solutions

• Consumers
• Customers
• Partners
• Contractors
• Employees
• …

IP and Web to the edge

FORGEROCK Identity Platform

Little Data

End-to-End Security, Web, Data Objects & Management

BIG DATA

© 2017 ForgeRock. All rights reserved.
Thank You

Ludovic Poitou
Director Product Management, General Manager France, ForgeRock

Ludovic.Poitou@ForgeRock.com
@ludomp