IoT, Identity Management & UMA

Cyril Grosjean

Forgerock

CONSTAT: la sécurité dans l'IoT est relativement faible

- Capacité de calcul limitée, énergie limitée, donc pas de logiciel type anti-malware ou autre

- Beaucoup de fabricants ont peu d'expérience en sécurité, la sécurité prend du temps et a un coût, des solutions propriétaires, ou non éprouvées, ou mal implémentées sont ainsi déployées. Des mots de passe sont parfois codés en dur ou faciles à trouver

- Le manque de standards entre les réseaux (cloud public, privé, intranet) et les APIs ouvre des brèches. Certains objets « transitoires » ne sont pas détectés tout de suite.

- Patches difficiles à appliquer (car absence d'écran ou d'interface, bande passante limitée ou bien l'opération est perçue comme une contrainte par l'utilisateur)

- Des données sont parfois stockées dans les objets non chiffrées, idem pour les communications

- Certains objets diffusent des informations sans restriction, elle deviennent alors librement accessibles

CONSEQUENCES: des failles de sécurité avérées et inégales

- Prise de contrôle à distance:
    - Webcams
    - Véhicules
    - Eclairage domestique ou urbain
    - Thermostats
    - Portes
    - Appareils médicaux (pacemaker, pompe à insuline, ..)
- Code d'accès WIFI domestique ou public découvert
- Accès à des informations privées

SOLUTIONS: un ensemble de mesures à différents niveaux

- Penser et embarquer la sécurité dès la conception:
  - empêcher l'analyse statique/dynamique du code,
  - détecter les modifications à l'exécution

- Adopter le principe d'immunité collective: plus une protection est déployée, plus le risque de propagation diminue

- Mettre en œuvre une plate-forme de gestion des objets et des identités:
  - Centralisée pour permettre une gestion et un contrôle global des objets, des utilisateurs, de leurs relations, de leurs données, un contrôle des échanges entre eux, un contrôle de l'authentification et des autorisations (par exemple le provisioning des clés de chiffrement)
  - Reposant sur des standards pour faciliter l'interopérabilité et ainsi limiter les risques
  - Scalable et performante: d'ici 2020, l'IoT comptera de l'ordre de 25 milliards d'objets à minima
  - Evolutive et agile, car l'IoT est en pleine effervescence, il faut être réactif pour être compétitif

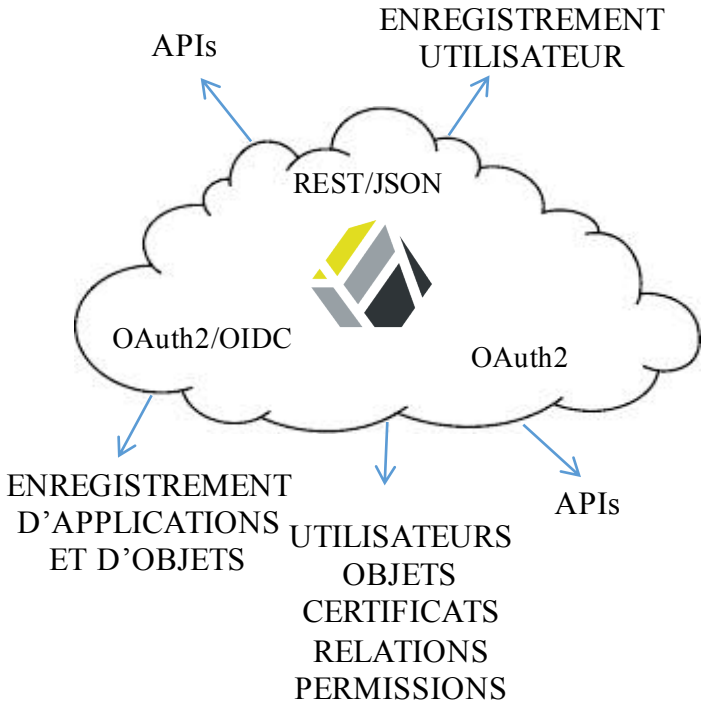
ACCES DIRECT AU CLOUD

Enregistrement d'objets ou d'utilisateurs

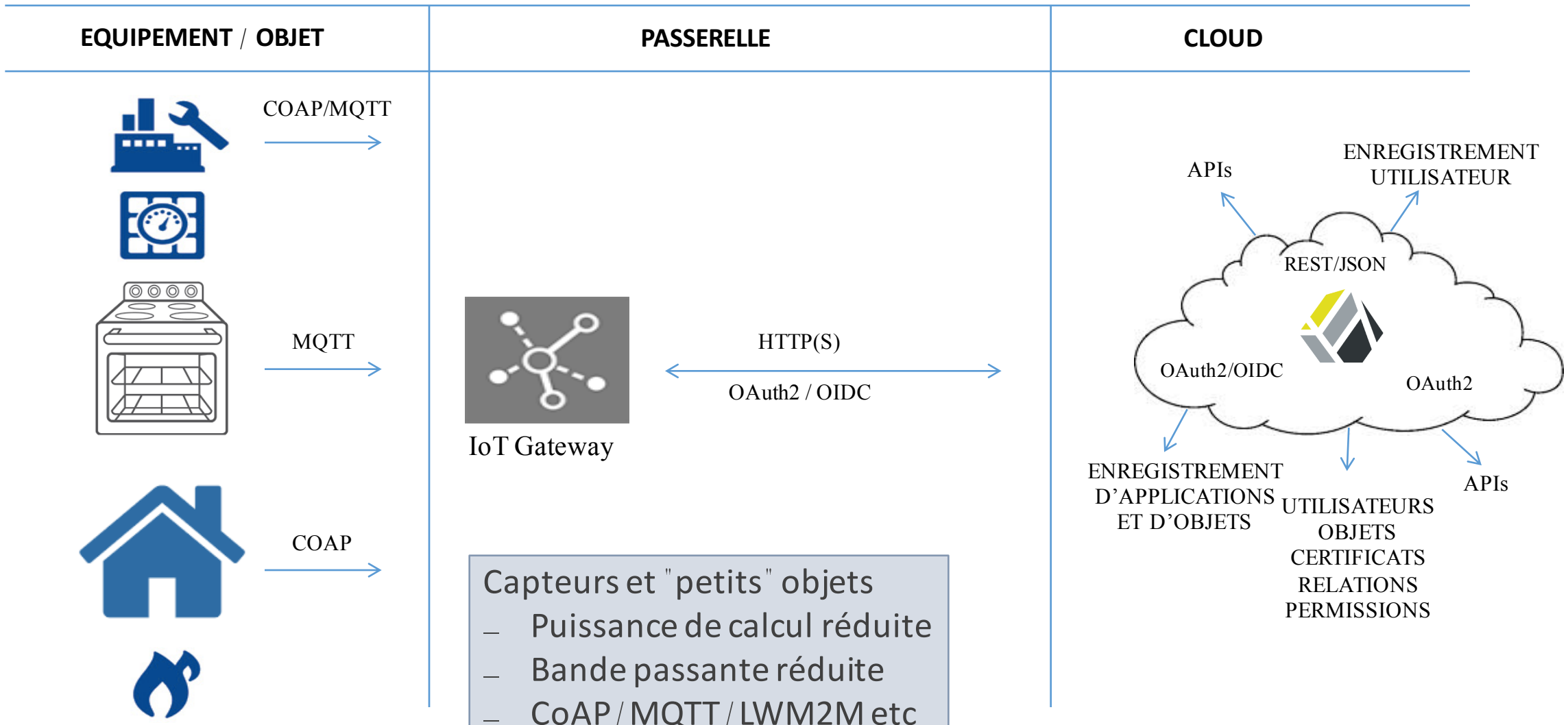
Liaison des utilisateurs aux objets ou des objets entre eux

Transmission d'informations sur l'utilisateur / l'objet

Objets connectés intelligents
- Puissance de calcul
- Bonne connexion réseau
- Supportent HTTPS



ACCES (BIDIRECTIONNEL) VIA PASSERELLE/PROXY IoT



Et UMA dans tout ça ? Consentement 2.0

- 2 cas d'usage évolués de l'IoT impliquant plusieurs utilisateurs et où UMA apporte une solution:

- Projet pilote DHL / Amazon / Audi: donner un accès temporaire au coffre pour le retrait ou le dépôt de colis
- Permettre l'usage temporaire d'éléments de cuisine (ou autre) par des locataires AirBnB

- Mais UMA couvre des cas d'usage plus larges et améliore les fonctionnalités de partage: la granularité, la standardisation (permet de centraliser la gestion), le mode déconnecté, la gestion des consentements

- Partage de documents personnels entre ma banque et des services publics, éventuellement à l'étranger
- Partage de mes dossiers médicaux entre professionnels de santé
- Permet de proposer une offre de type « Authorization as a Service »
- Permet aux utilisateurs de partager des ressources: le bouton « **Partager** » de votre site Web

UMA par rapport à OAUTH2/OIDC

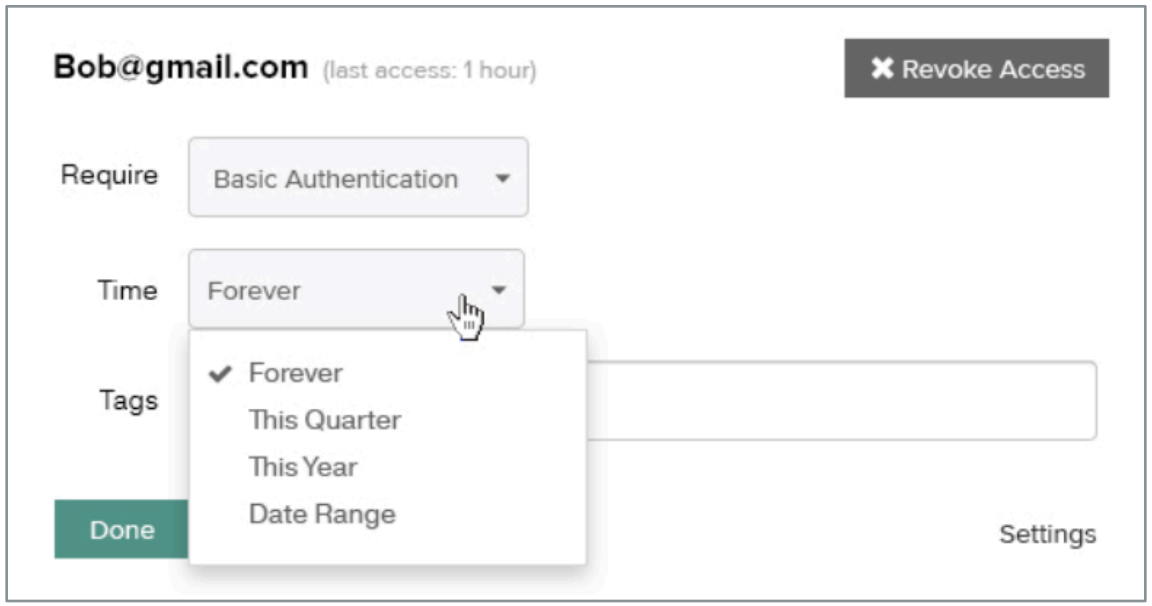
OAUTH 2 permet l'accès à des ressources d'une application à une autre:

- avec mon consentement
- à partir d'une application à laquelle je suis connecté
- la ressource accédée contrôle l'accès à sa façon, localement généralement (et donc pas via un serveur d'autorisation centralisé)

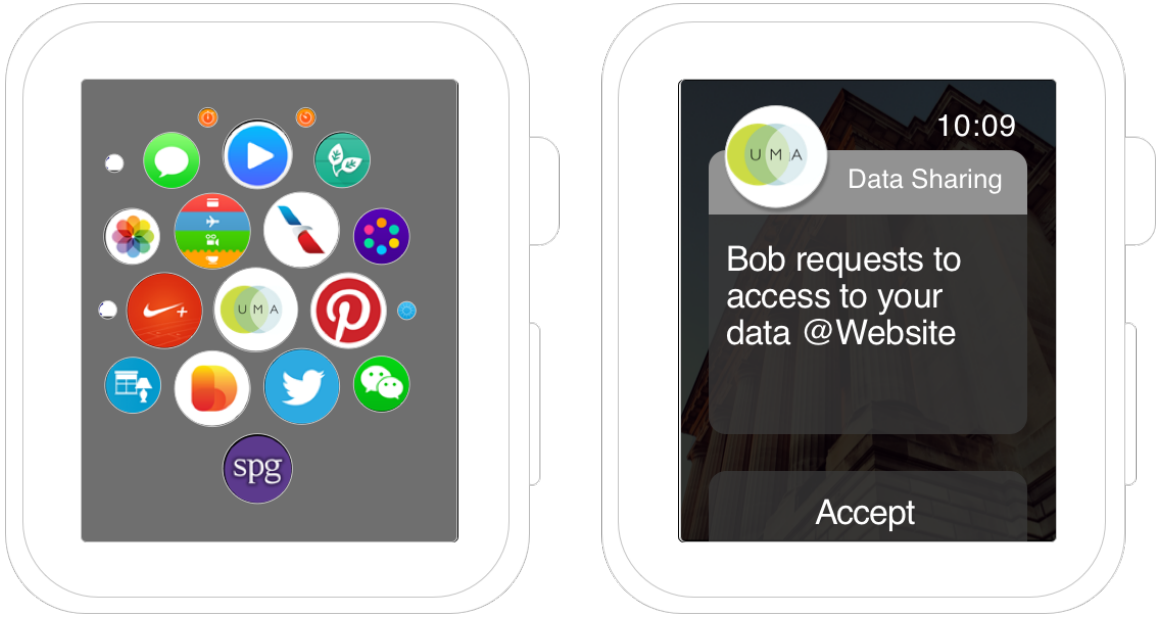
Qu’ apporte UMA ?

La capacité à partager des informations avec d’autres utilisateurs, avec des applications, sous mon contrôle, de façon centralisée et standardisée

Qu’ apporte UMA ?

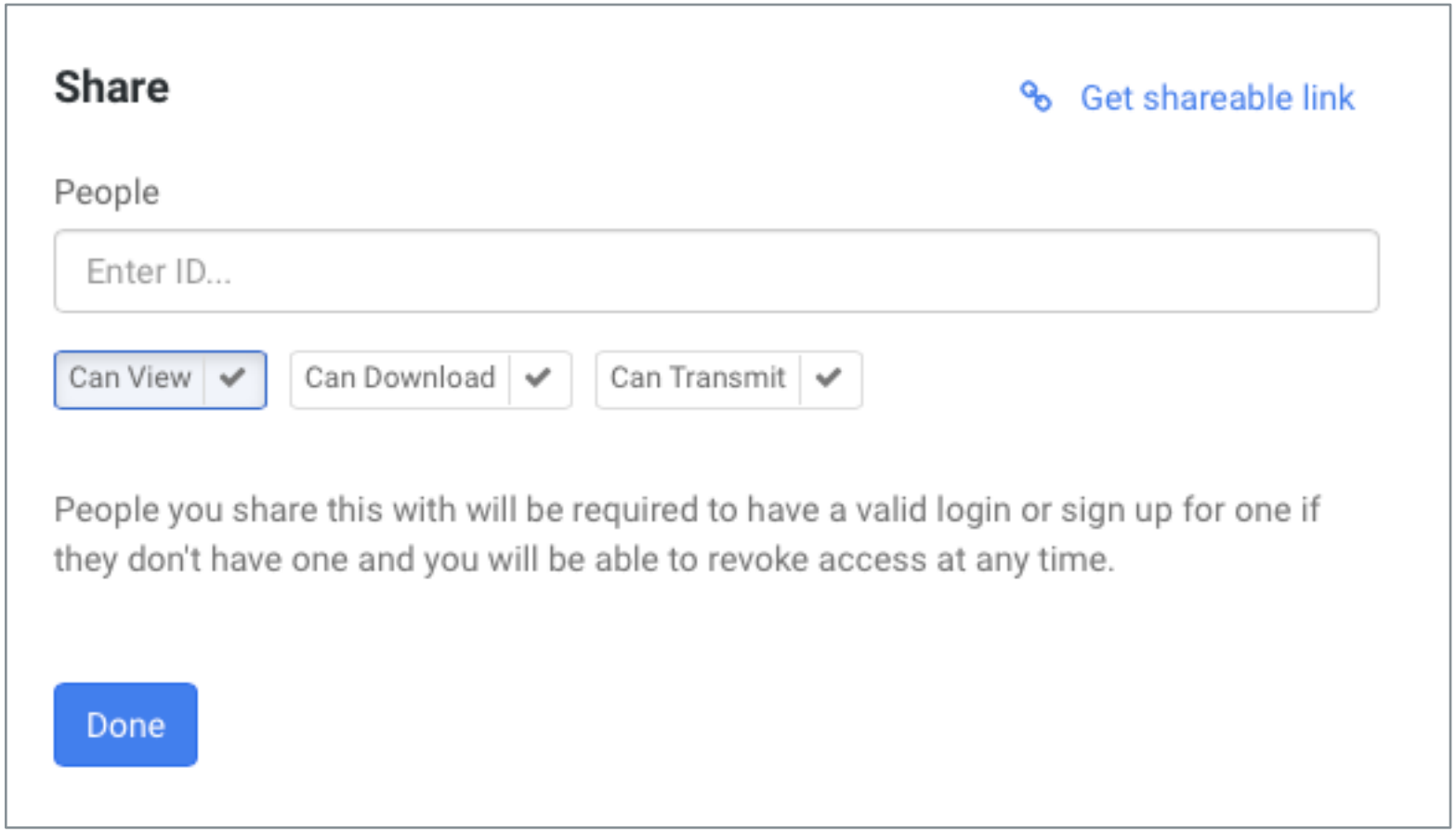


Un contrôle fin sur l’authentification requise et les droits accordés, par exemple la capacité à définir une politique d’accès, des termes et conditions d’accès en fonction du profil de l’utilisateur



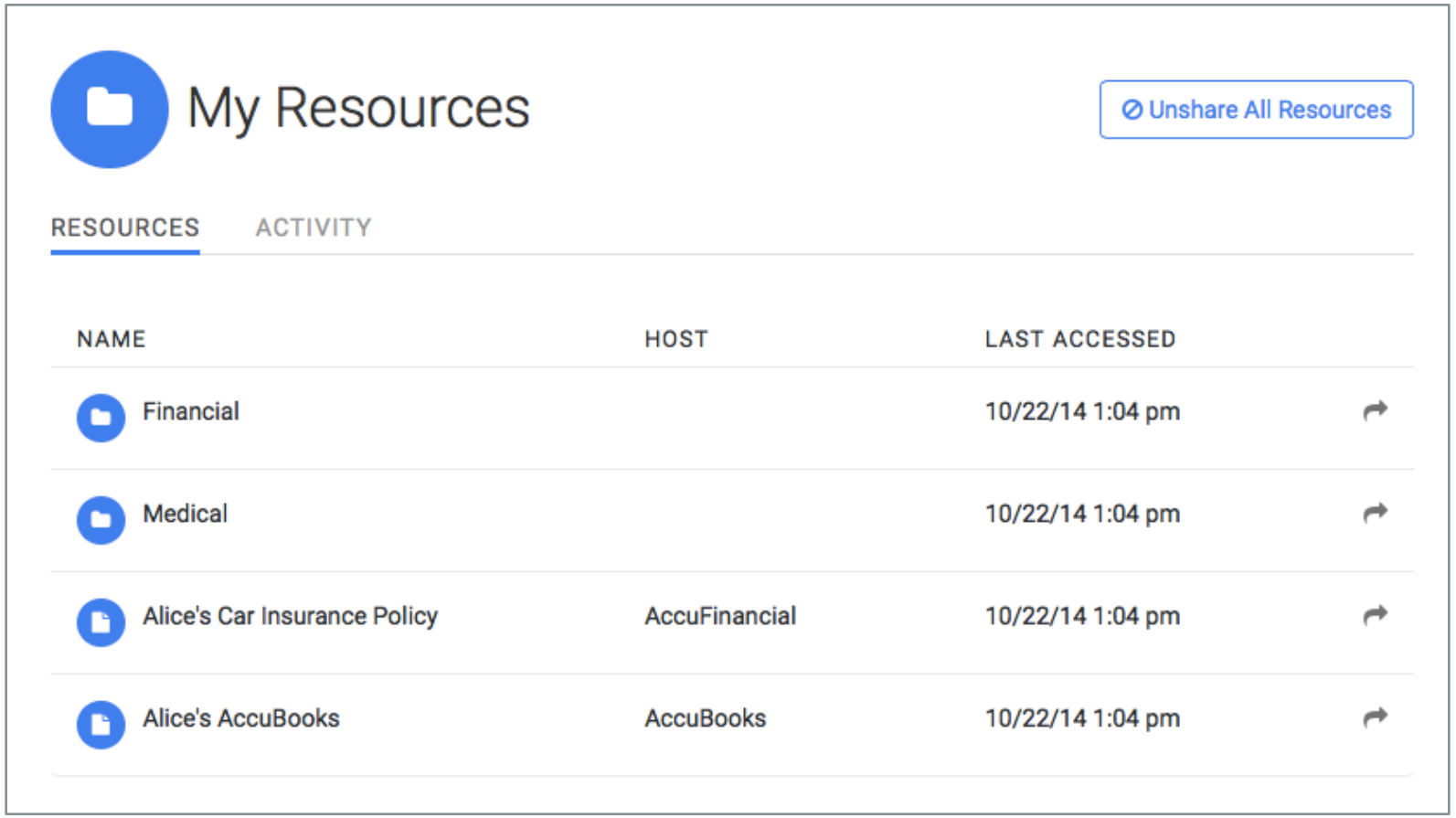
La possibilité de notifier l’utilisateur lorsqu’une nouvelle demande d’accès aux ressources qu’il partage survient

Qu’ apporte UMA ?



UMA étend le spectre des autorisations possibles via les “scopes” – Lire, Télécharger, Transmettre

Qu’ apporte UMA ?



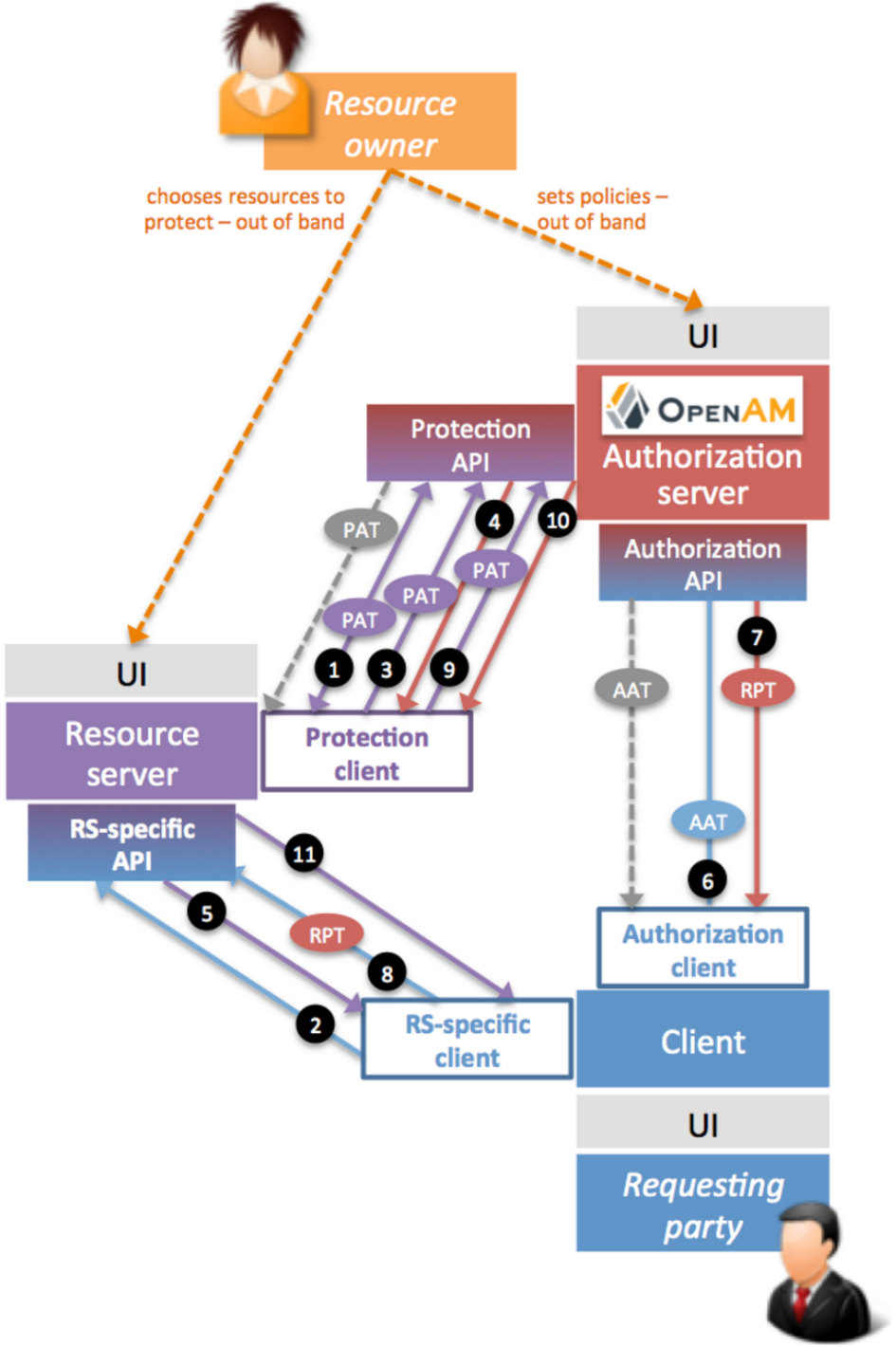
Externalisation de la gestion des autorisations vers une console unique
=> améliore la confiance et donc favorise l’adoption

Qu’ apporte UMA ?

- **Pour l’utilisateur**
  - Rend l’ingérable gérable
  - Donne un contrôle sur ses partages
  - Permet une gestion très fine
  - Rend l’utilisateur plus autonome

- **Pour un fournisseur de service**
  - Perception comme tiers de confiance
  - Données utilisateur précises et à jour
  - Confidentialité et partage mieux contrôlés: un avantage compétitif
  - Service d’autorisation valorisable: Authorization as a service
  - Ouverture à de nouveaux partenariats
  - Techno. facile à intégrer, consentements et partages basés sur des standards, scalable et applicable au delà de l’entreprise

Un peu de technique ..



RS needs OAuth client credentials at AS to get PAT
C needs OAuth client credentials at AS to get AAT
All protection API calls must carry PAT
All authorization API calls must carry AAT

1. RS registers resource sets and scopes (ongoing – CRUD API calls)
2. C requests resource (provisioned out of band; must be unique to RO)
3. RS registers permission (resource set and scope) for attempted access
4. AS returns permission ticket
5. RS returns error 403 with as_uri and permission ticket
6. C requests authz data, providing permission ticket
7. (After claims-gathering flows not shown) AS gives RPT and authz data
8. C requests resource with RPT
9. RS introspects RPT at AS (if using default “bearer” RPT profile)
10. AS returns token status
11. RS returns 20x

Démos IoT, IDM & IAM: http://forgerock.fr

Ressources UMA: http://forgerock.org/openuma

Merci !