SÉCURITÉ POUR LES ENTREPRISES DANS UN MONDE NUAGEUX ET MOBILE

JANUA

OPEN SOURCE & OPEN STANDARDS

Sophia-Antipolis 01/07/2013
Cyril Grosjean
cgrosjean@janua.fr
0950 677 462

Cyril Grosjean

- Directeur technique de Janua depuis 2004

  · Expert en gestion des identités
    · Contrôle d'accès, sécurité, PKI
    · SSO, Fédération
    · Provisioning
    · Annuaires

- Consultant des services professionnels chez Netscape puis Sun pendant 6 ans

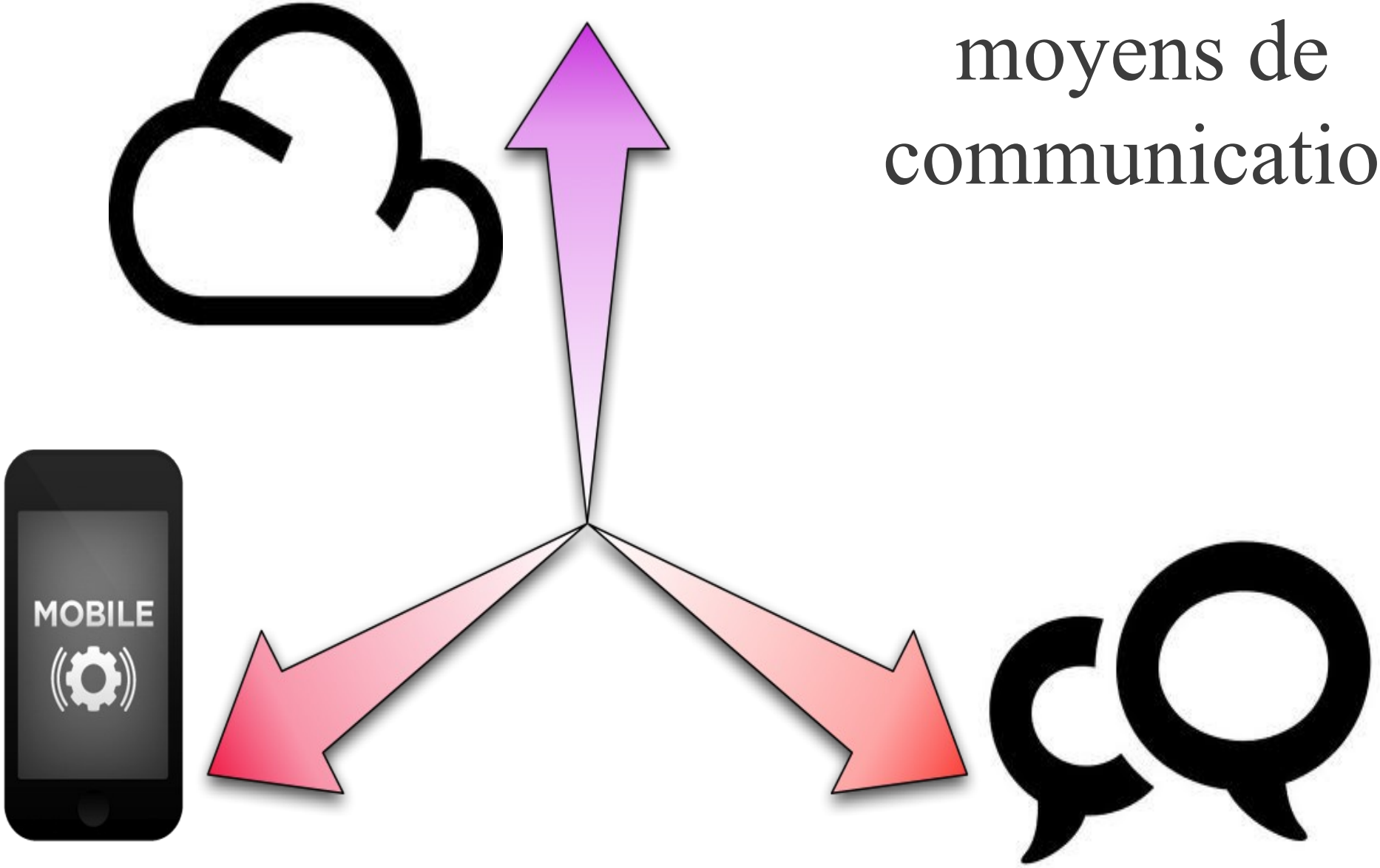
Agenda

- Un monde qui bouge
- ForgeRock Open Identity Stack
- Les standards qui émergent
- Une vision d'architecture

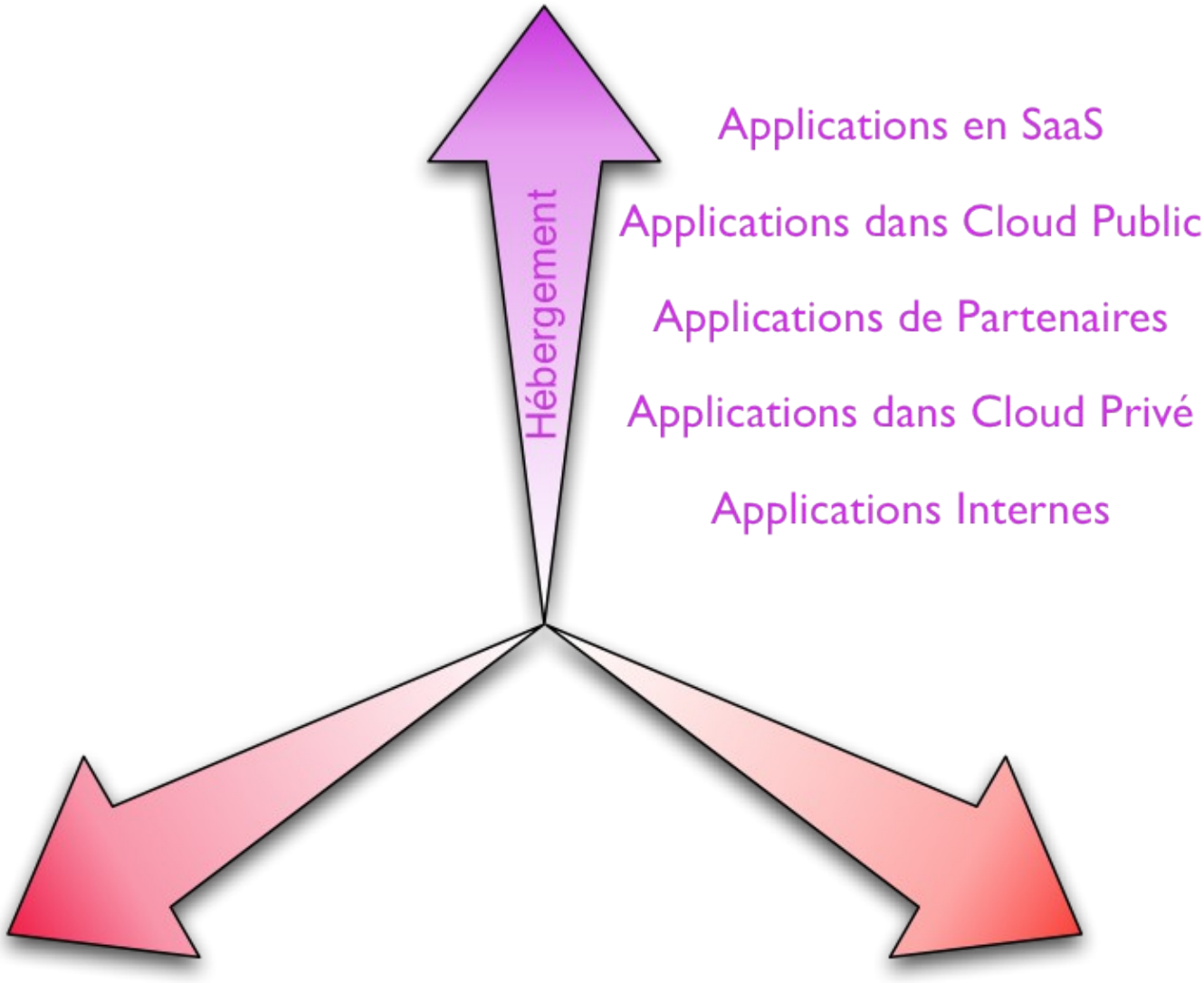
Avant: une sécurité monolithique

Aujourd'hui: des besoins d'accès multiples

Accélération des moyens de communication

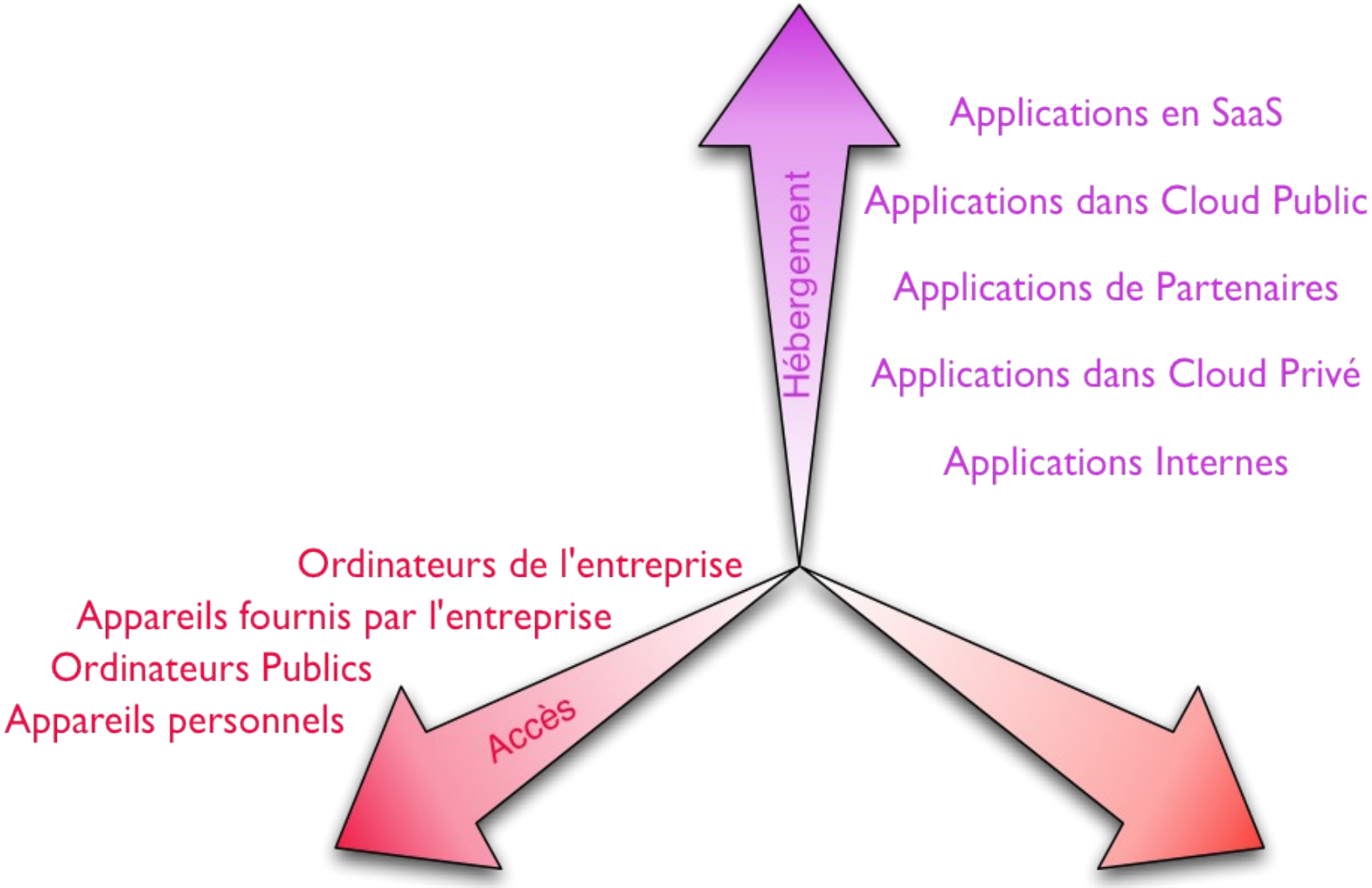


Le cloud



Source: Rapport Forrester "Navigate the future of Identity and Access Management" 2012

La mobilité



Source: Rapport Forrester "Navigate the future of Identity and Access Management" 2012

Le social

Hébergement

Applications en SaaS

Applications dans Cloud Public

Applications de Partenaires

Applications dans Cloud Privé

Applications Internes

Accès

Ordinateurs de l'entreprise

Appareils fournis par l'entreprise

Ordinateurs Publics

Appareils personnels

Utilisateurs

Employés

Sous-traitants

Partenaires

Membres

Clients

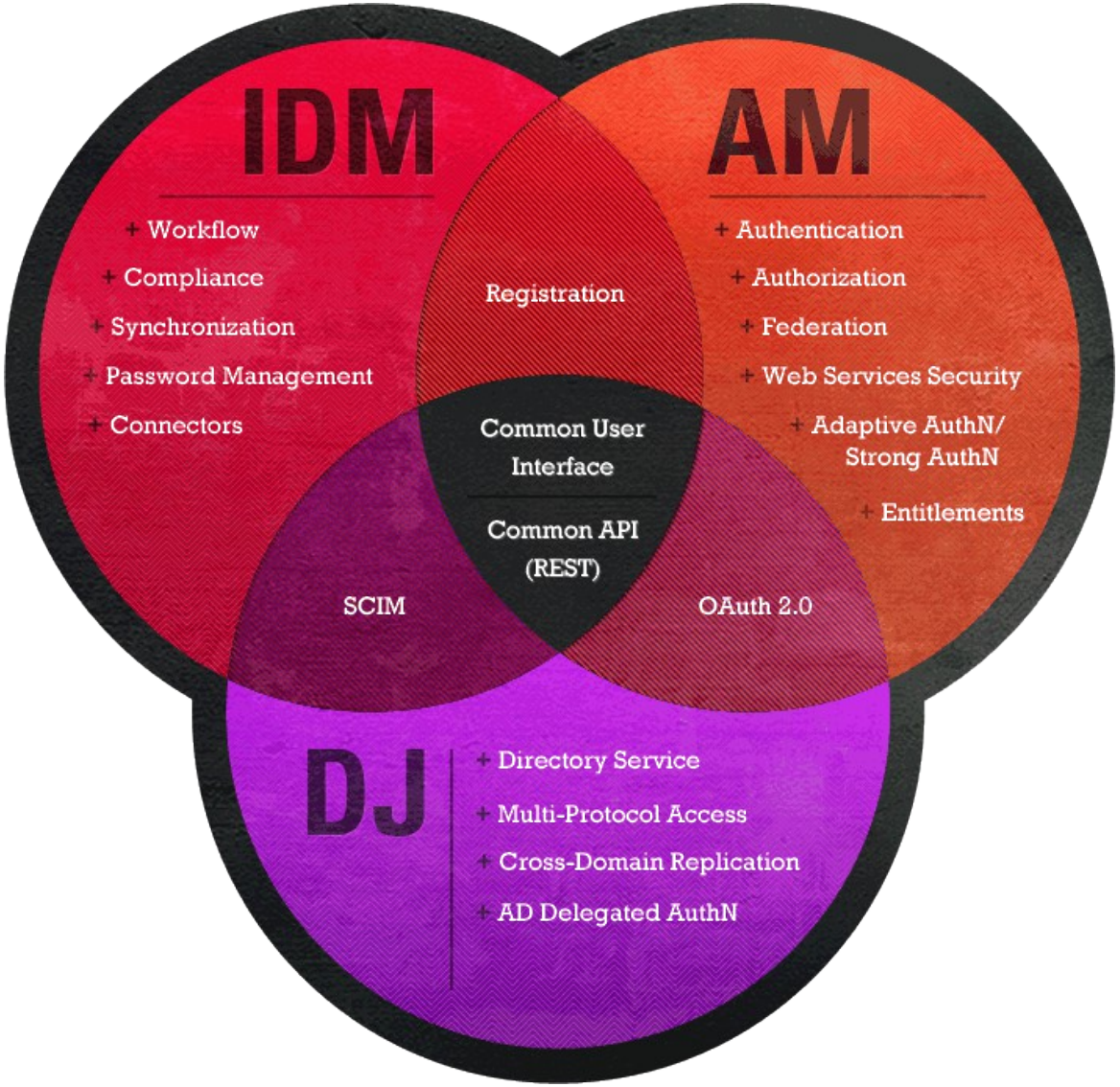
Revoir l'infrastructure de sécurité

- Besoin d'une gestion des identités distribuée, dynamique et capable d'une grande échelle.
- Peut-on faire confiance:
  - à un utilisateur ?
  - à un appareil ?
- Arrêter la prolifération des mots de passe.

Les solutions existent

- ForgeRock Open Identity Stack
  - Une solution open source
  - Ecrite en Java
  - Issue des projets de Sun Microsystems
- Janua: partenaire de Forgerock
  - Conseil
  - Expertise
  - Intégration, développement

Open Identity Stack

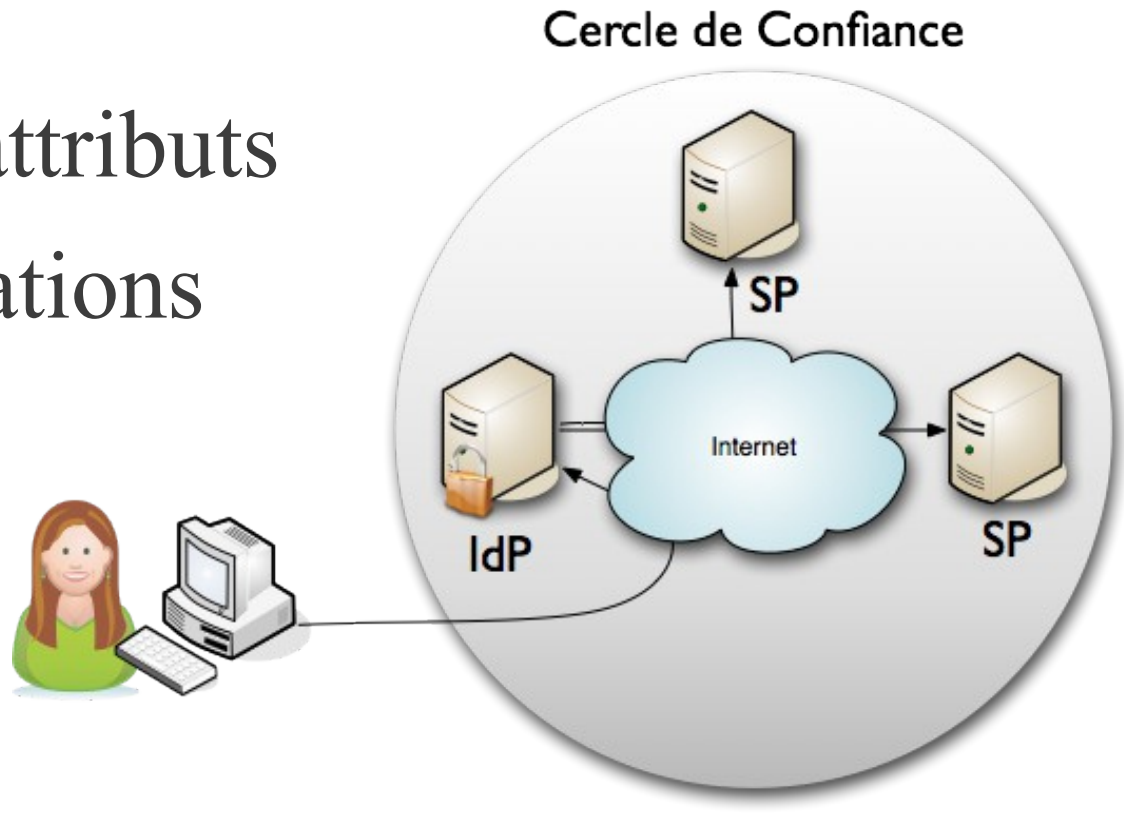


OpenAM: Authentification et contexte

- Qui est qui ?
- Authentification
  - simple
  - à facteurs multiples
  - variant en fonction du contexte
- Une application ne peut pas tout prévoir.
- Autant déléguer à un service d'authentification:
  - OpenAM : 19 modules d'authentification disponibles

OpenAM: SSO et fédération

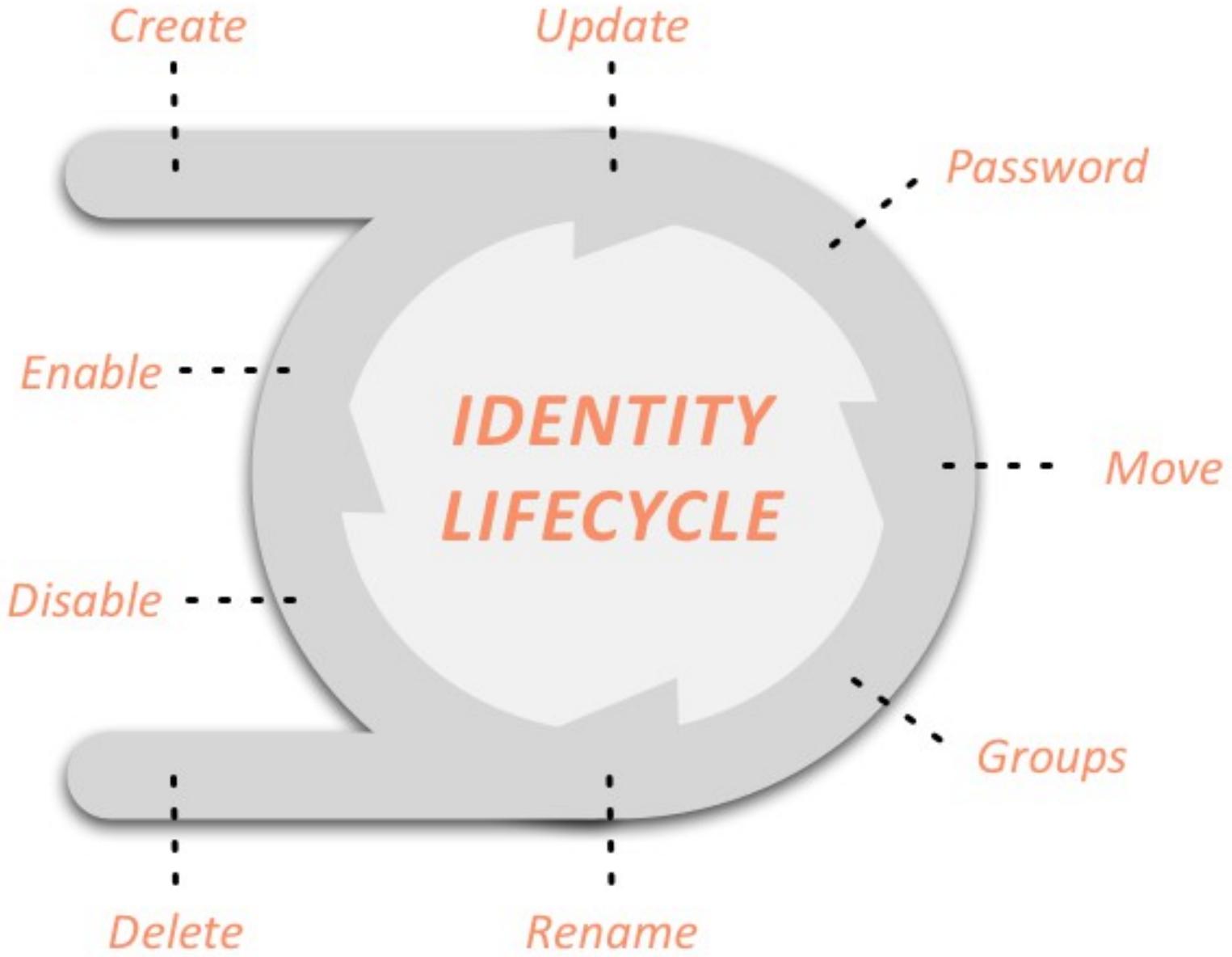
- Une fois authentifié, on peut:
  - Réutiliser le cookie
  - Faire de la fédération entre sites
- SAMLv2
  - Permet l'échange d'attributs
  - Véhicule les autorisations
  - Anonymité possible
- WS-Federation
- Single Sign Out



OpenAM: Autorisations

- Qui peut faire quoi ?
- Centralisée :
  - L'entreprise établit des règles sur qui peut faire quoi
  - XACML
- Déléguée:
  - Le proprietaire d'une ressource, autorise une application à y accéder.
  - RBAC
  - OAuth2

OpenIDM: Gestion des identités



OpenDJ: Stockage des identités

- LDAP, standard de facto
- Capacité en volume et en performances
- Haute disponibilité
- OpenDJ 2.6 proposera un service “REST to LDAP”
- Nombreuses fonctionnalités
- Support des derniers standards LDAP
- Evolutif (architecture modulaire, développé en Java)

Des standards emergent

OpenID Connect

OAUTH 2

SCIM
System for
Cross-domain
Identity
Management

- Système d'autorisation déléguée
- Authentification à 3 tiers
- Protection des ressources REST
- Pour le mobile, autoriser une application à accéder à un service.
- Persistent

OpenID Connect

- Basé sur OAuth2
- S'inspire de SAMLv2 mais
  - REST / Json vs SOAP / XML

SCIM

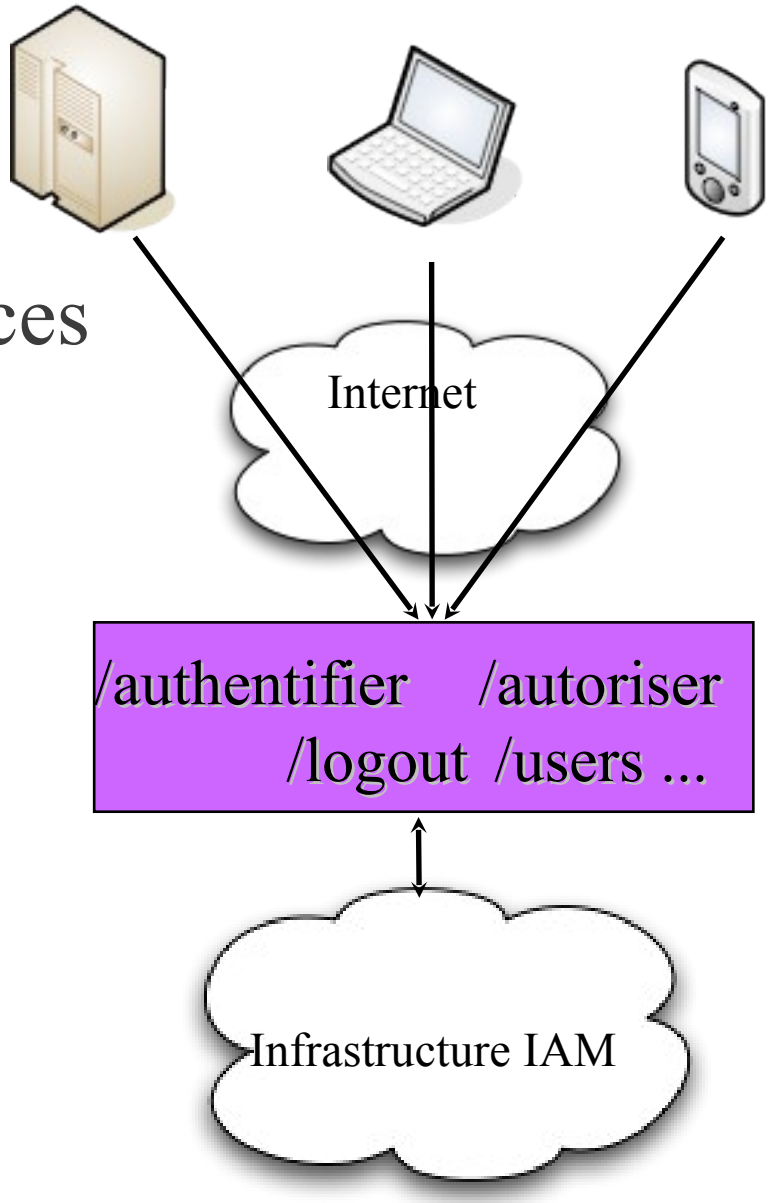
- Standard de gestion d'identité pour les applications cloud, les services
- Schéma standard de représentation des utilisateurs, des groupes et des opérations de provisioning (CRUD)
- Les plateformes SaaS:
  - Besoin de provisionner les utilisateurs et leurs roles
  - Des fois automatiquement
  - Par des interfaces propriétaires
- Maintenant à l'IETF, supporté par OpenIDM et OpenDJ

Services REST

- Representational State Transfer
- Modèle d'architecture logique
- Les Services Web / SOAP
  - Problèmes de performance
  - Problème de SPOF (Single Point of Failure)
- Focus sur REST
- Une approche plus “Internet”
- Supportés par de nombreux langages

IAM sous forme d'API

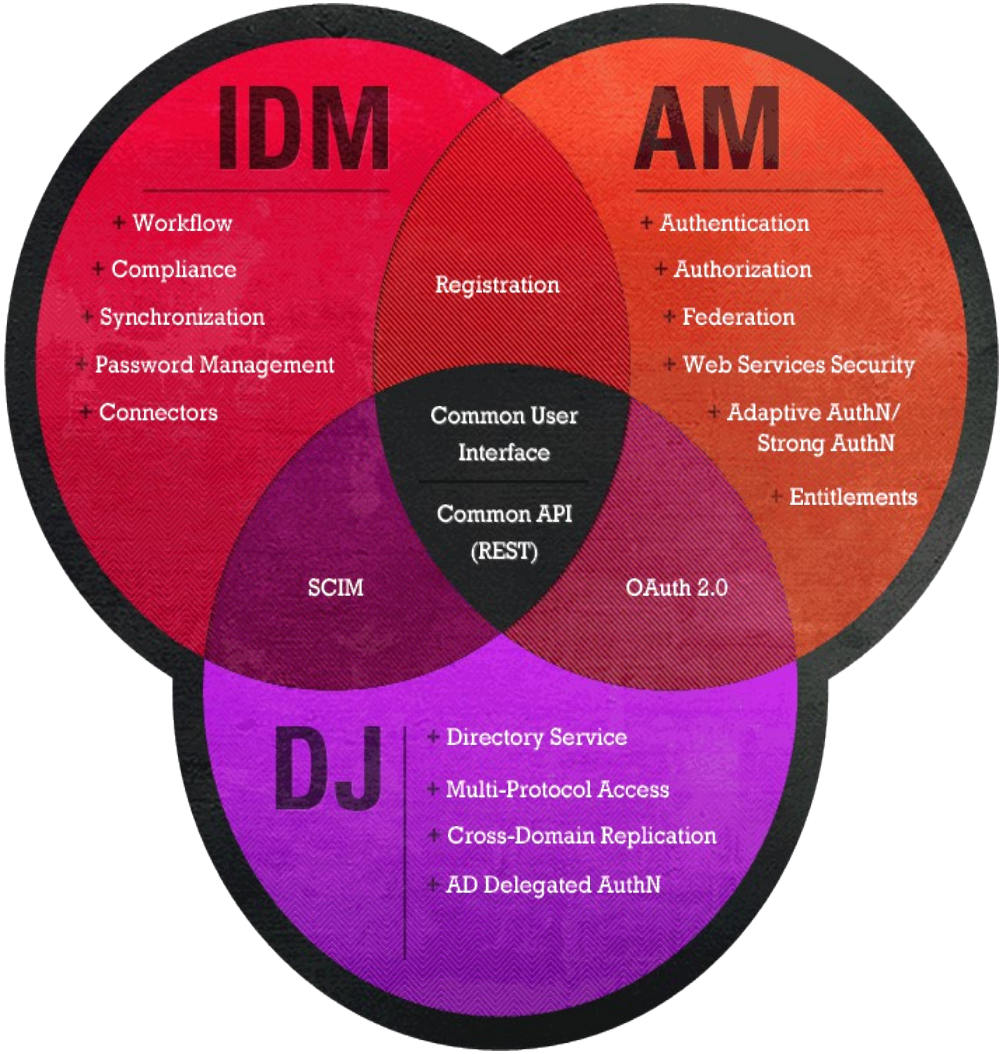
- Couche d'API REST pour les services IAM
- Applicable à toutes les applications
- Découplage quoi / comment
- OAuth2 pour protéger l'accès



Conclusion

L'architecture de sécurité des entreprises doit évoluer:

- Un service IAM
- Accessible par API REST
- Avec OAuth2



Qui sommes nous ?

- Société de consulting et de services en logiciels libres (SS2L) fondée en 2004 à Sophia Antipolis après 15 ans chez Sun
- Notre métier : l'Expertise
- Nos domaines techniques de prédilection : Gestion des identités (IAM) en Open Source, Open Data et couches basses des infrastructures DataCenter.
- Nos prestations : Consulting, Intégration, Accompagnement et développement au forfait.
- Notre approche : les processus itératifs, les maquettes (POC) et l'utilisation des méthodologies dites "Agiles".
- Notre « philosophie/éthique » : l'Open Source et l'humain..