IAM PSA : 16 ans déjà

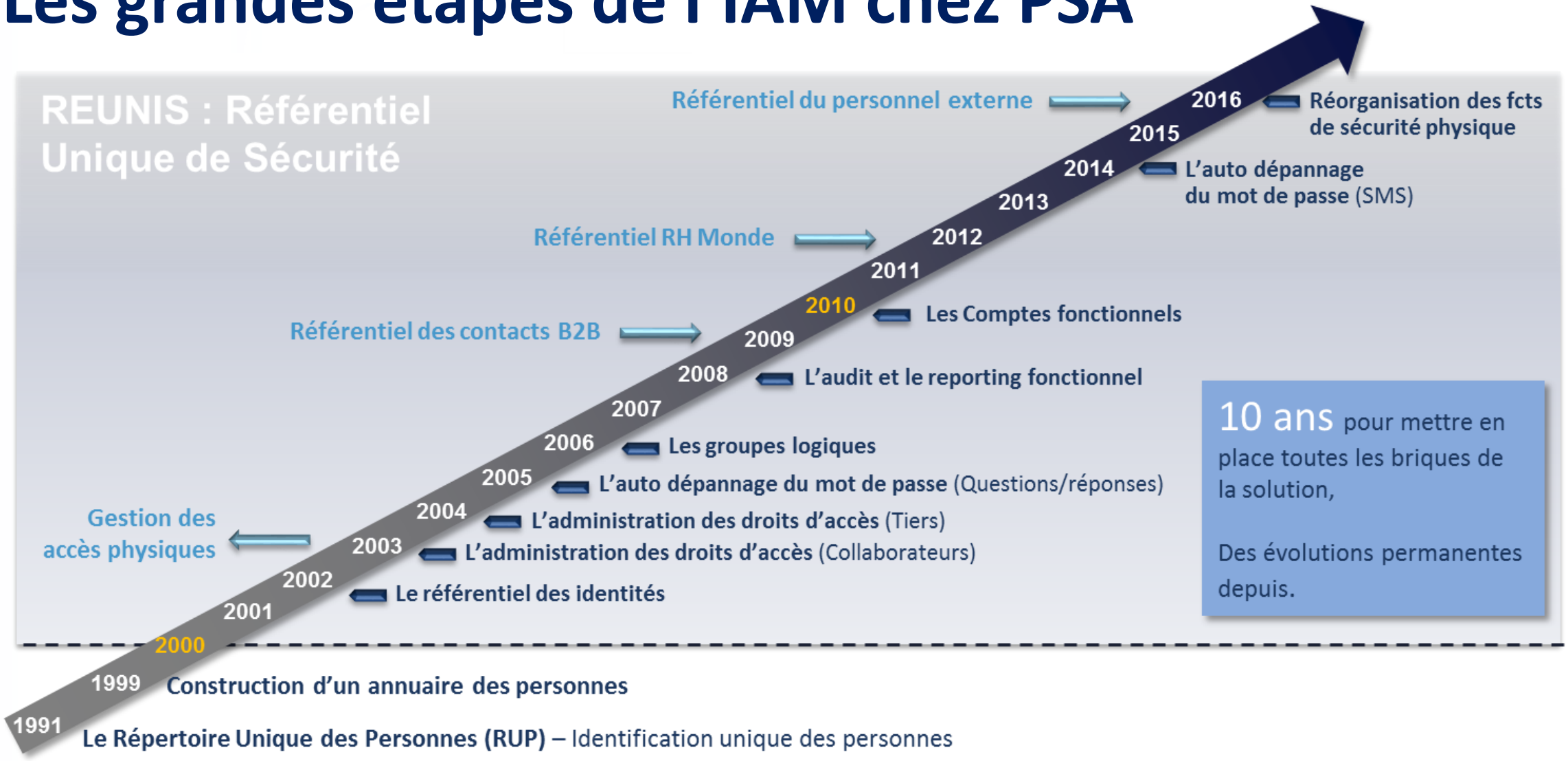
Valérie CHASSAING

Sommaire

- Le contexte PSA
  - Les grandes étapes de l'IAM chez PSA
  - Les principaux objets de la gestion des identités et des droits
  - Les principaux acteurs de l'administration des droits
  - Les identités actuelles et à venir
- Le bilan, 16 ans après
  - Les atouts
  - Les limites du modèle actuel
  - Les enjeux pour la suite
  - Les facteurs de succès et les difficultés

Le contexte PSA

Les grandes étapes de l'IAM chez PSA



Les principaux objets de la gestion des identités et des droits

L'identité Numérique

Toute personne devant accéder au SI de PSA ou aux locaux du Groupe doit posséder une identité numérique.

A une identité numérique correspond une seule personne.

Sauf contrainte technique, chaque personne ne dispose que d'une seule identité numérique.

445 000 Identités dont :
- 115 000 Internes
- 43 000 Externes*
- 244 000 Tiers **
- 43 000 Comptes fonctionnels

(*) Externes = Prestataires + Partenaires
(**) Tiers = Réseau commerce et Fournisseurs

Le rôle applicatif

Les applications gèrent leurs droits d'accès au travers du système centralisé de gestion des droits de PSA.

Un rôle contient :
- une description fonctionnelle
- une ou plusieurs cibles techniques
- une valorisation qui définit le périmètre d'application du service (optionnel).

Un rôle peut être attribué :
- Unitairement aux utilisateurs autres que les Tiers
- A un groupe d'utilisateurs partageant des critères communs
- Au travers de « Métiers » pour les populations Tiers

17 800 Rôles applicatifs
3 000 Applications

Le groupe logique

Un groupe est un ensemble d'identités qui ont en commun un ou plusieurs critères (métier, projet, organisation,..)

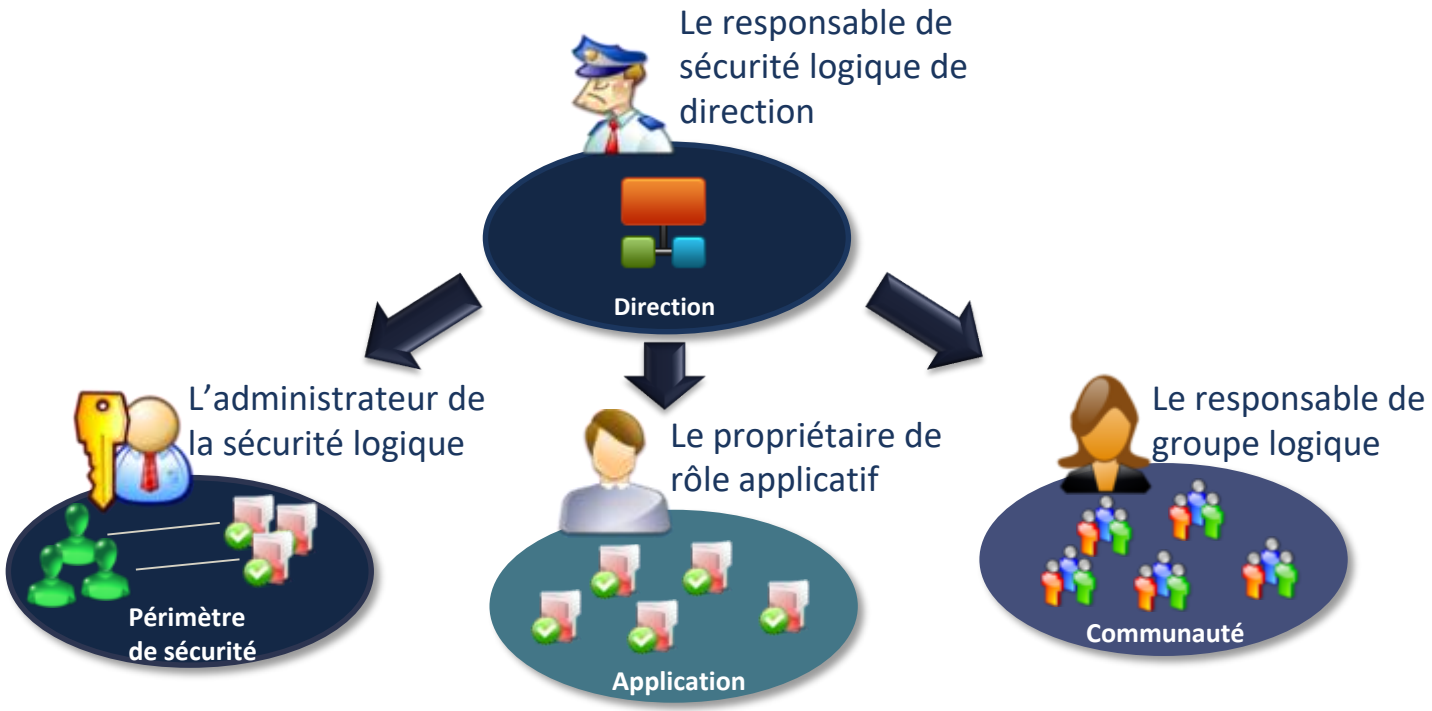
Ils sont utilisés :
- comme listes de diffusion dans la messagerie,
- pour gérer l'accès à des documents,
- pour attribuer des droits d'accès à un ensemble d'identités ayant le même métier.

Lorsque les référentiels associés existent (organigramme, référentiel des activités, Référentiel fournisseur,…) les groupes sont automatiques.

30 400 Groupes Logiques dont 20% sont automatiques

Les principaux acteurs de l'administration des droits

- L'administration des droits d'accès est une administration déléguée et repose sur une organisation « monde »
- Les principaux acteurs sont :



1300 Administrateurs de la sécurité logique PSA

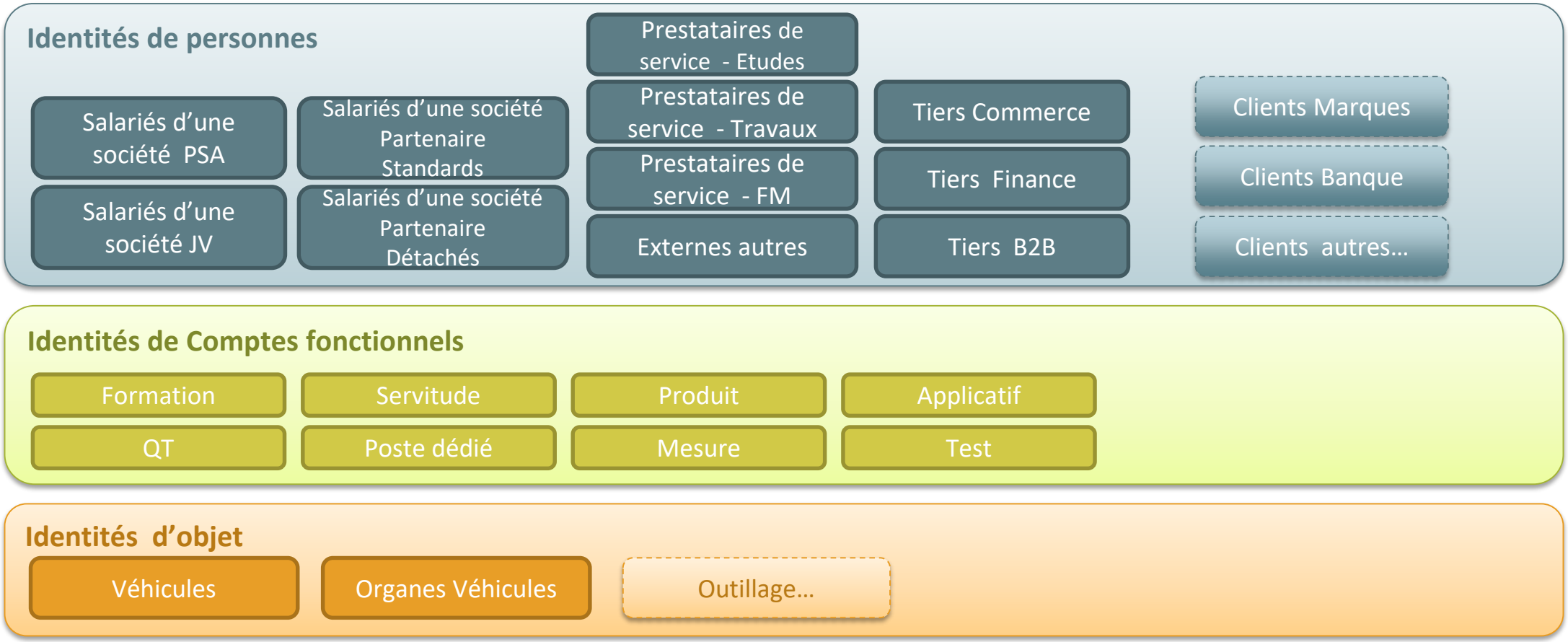
23 000 Administrateurs Tiers

3600 Propriétaires de rôles applicatifs

9000 Responsables de groupes logiques

15 Responsables de sécurité logique de Direction

Les identités actuelles et à venir



Le bilan, 16 ans après

Les atouts

Un outil d'administration de sécurité **unique** pour toutes les applications.

Une administration qui peut être **déléguée** à des utilisateurs métiers.

Une **automatisation** des mises à jour techniques dans les cibles (AD, SAP, TSS, LDAP, …) .

L'IAM PSA est un des piliers majeurs de la sécurité.

C'est un point de passage incontournable pour tout utilisateur devant accéder à notre SI.

Une attribution et un retrait des accès en **quelques minutes**.

La **traçabilité** des actions d'administration des identités et de leurs habilitations.

L'interfaçage de la solution avec les **référentiels RH** et de **sécurité physique**

Les limites de la solution

Une solution conçue sur des principes qui ne sont plus vrais aujourd'hui

Dans les années 2000…

Un collaborateur travaille pour **une seule marque**, dans un seul point de vente…

L'organisation du Groupe est **stable** …

Tous les collaborateurs travaillent **dans** les locaux de PSA…

Les administrateurs de sécurité sont **proches** des utilisateurs…

Les types de populations sont **simples** : interne, externe ou tiers…

Des évolutions fonctionnelles limitées au strict nécessaire

- Une application développée en interne sur une technologie vieillissante
- Un niveau d'abstraction fonctionnelle qui engendre une complexité technique de la solution

Les enjeux d'aujourd'hui

- Etre plus agile pour accompagner la transformation du Groupe :
  - Répondre aux besoins d'administration des populations non hébergées sur des sites PSA.
  - Gérer le changement de statut des utilisateurs .
  - Définir le niveau de confiance à accorder par défaut aux différentes populations d'utilisateurs.

- Adapter le modèle d'administration :
  - Une administration déléguée (proche des utilisateurs) ou une administration centralisée ?
  - Quel niveau de self-service mettre à disposition des utilisateurs ?
  - Quel niveau de granularité des droits gérés dans l'IAM ?
  - Comment régler le curseur entre le contrôle à priori et le contrôle à posteriori ?

- Intégrer les nouvelles typologies d'identités :
  - Les objets connectés
  - Les usagers des objets connectés
  - Les clients

Facteurs de succès et difficultés

Les facteurs de succès

- Une DSI centralisée pour l'ensemble du Groupe
- Un IAM proposé comme un service d'infrastructure « gratuit » et « obligatoire »
- Un chef de projet MOA impliqué et charismatique
- Une collaboration MOA/MOE très étroite (capacité de chacun de comprendre le domaine de l'autre)
- Un développement en mode « Agile »
- Prise en compte importante du contexte des métiers de l'entreprise

Les difficultés

- Maintenir l'intérêt des sponsors pour le projet dans la durée
- Faire comprendre les enjeux du projet et les coûts associés
- S'adapter en cours de projet à l'évolution de l'écosystème

CLUSIF

Vos questions ?