Acsel ASSOCIATION DE L'ECONOMIE NUMÉRIQUE

Commission Identité Numérique

Groupe de travail Gestion des identités

12 mars 2009
Baker & McKenzie,
Paris

Les technologies de gestion de l'identité

ATELIER 1

Paul TREVITHICK, CEO de Parity– Responsable projet Higgins – Président Fondation Infocard (en anglais)
InfoCard / Higgins

Fulup AR FOLL, Sun – Master Architect
Liberty Alliance
Christophe BOUTET, Entr'ouvert – PDG
Point de vue d'un intégrateur de solution Liberty Alliance

Sébastien BRAULT, **Karim SBATA**, Orange
OpenID et solutions Orange

Pierre COUZY, Microsoft France - Architecte en système d'informations
Philippe BERAUD, Microsoft France
Cardspace et autres solutions Microsoft

Identité numérique
SSO, Personal APIs

Atelier Les technologies de gestion de l'identité

Orange – S.Brault, K.Sbata

12 mars 2009

Introduction

- **Orange est actif depuis plusieurs années dans le domaine de l'identité, des services liés à l'identité:**
  - Au travers de sa participation à divers groupes de normalisation (OMA, GSMA, Liberty, etc.) et projets internationaux
  - De part les expérimentations et trials lancés durant les 10 dernières années

- **Aujourd'hui, Orange propose notamment deux offres liées à l'identité numérique :**
  - Le Single Sign On (SSO)
  - Les Personal APIs où comment partager ses données/services Orange avec un site tiers, s'appuyant soit sur le SSO/Fédération, soit l'authentification

- **Orange a lancé en février 2008 son SSO, et en Avril 2008 son programme d'APIs, dont les Personal APIs**

SSO

- **Orange opérateur Fixe Internet et Mobile**
  - Authentification / Identification principalement faite via des composants réseaux et serveurs.
  - Pas de composants clients, les composant clients exploitent l'identification réseau.
  - Remontée des infos réseau au niveau services.

- **Maturité industrielle:**
  - + de 8M de clients ADSL France (+12M en Europe)
  - + de 24M de clients mobile en France (+117M en Europe).

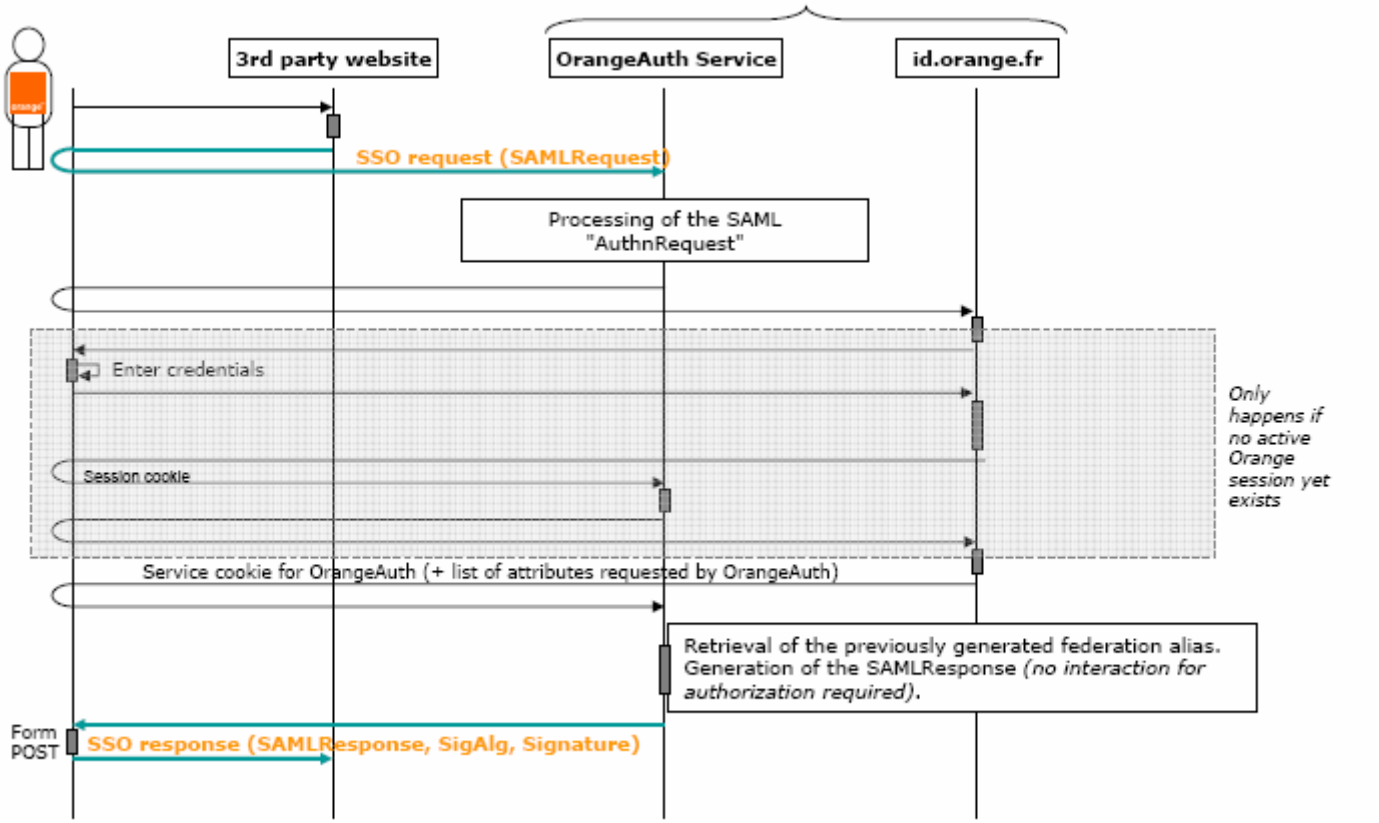
- **open ID V1, SAML, Open ID V2**
  - Différences, Avantages, inconvenients

SSO
Composants technologiques

- **Délégation d'authentification chez Orange avec SAML et OpenID**

  Offre d'authentification pour site tiers à travers des protocoles standard.

  Mécanique de redirection

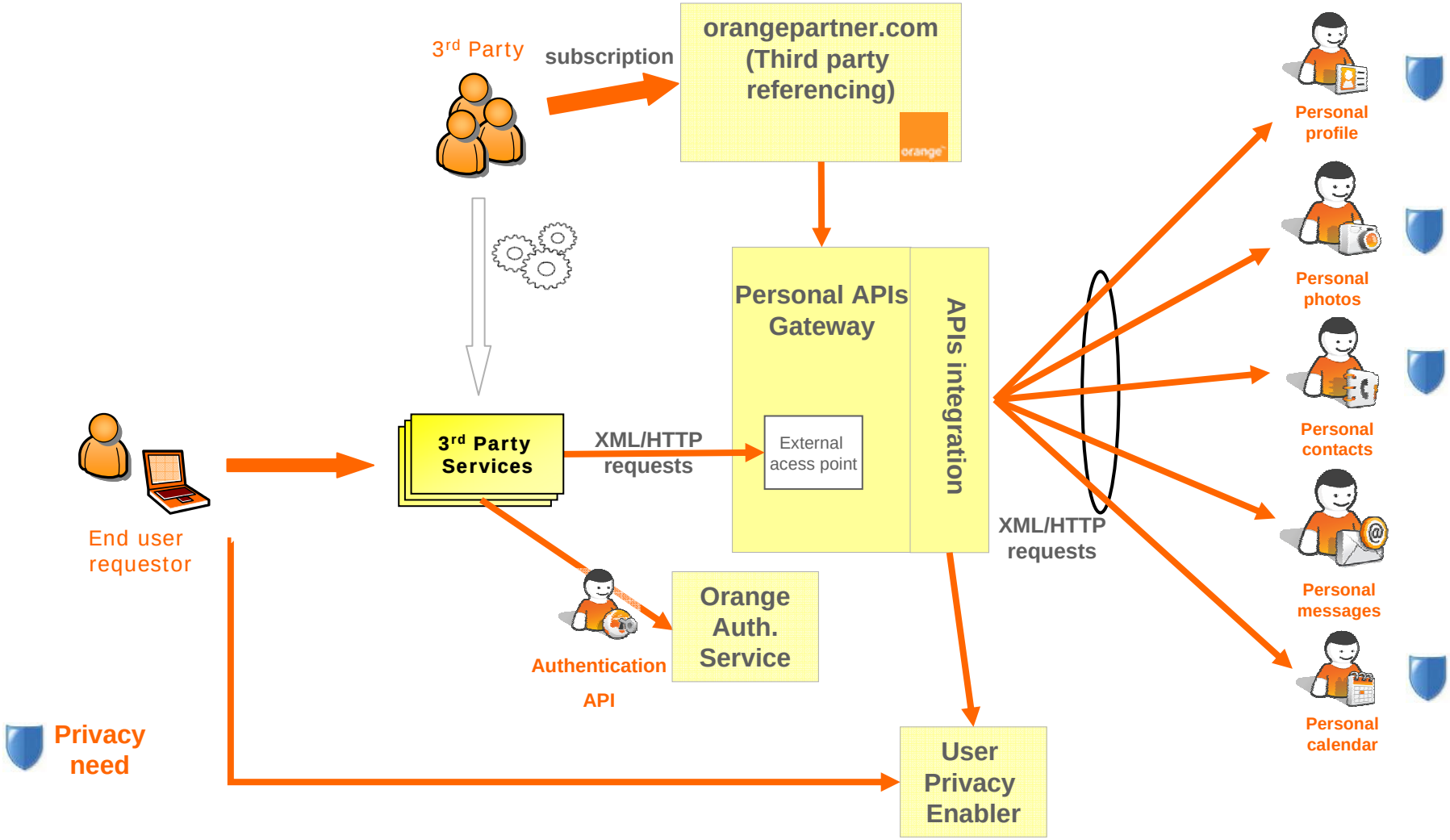


Personal APIs
Composants technologiques

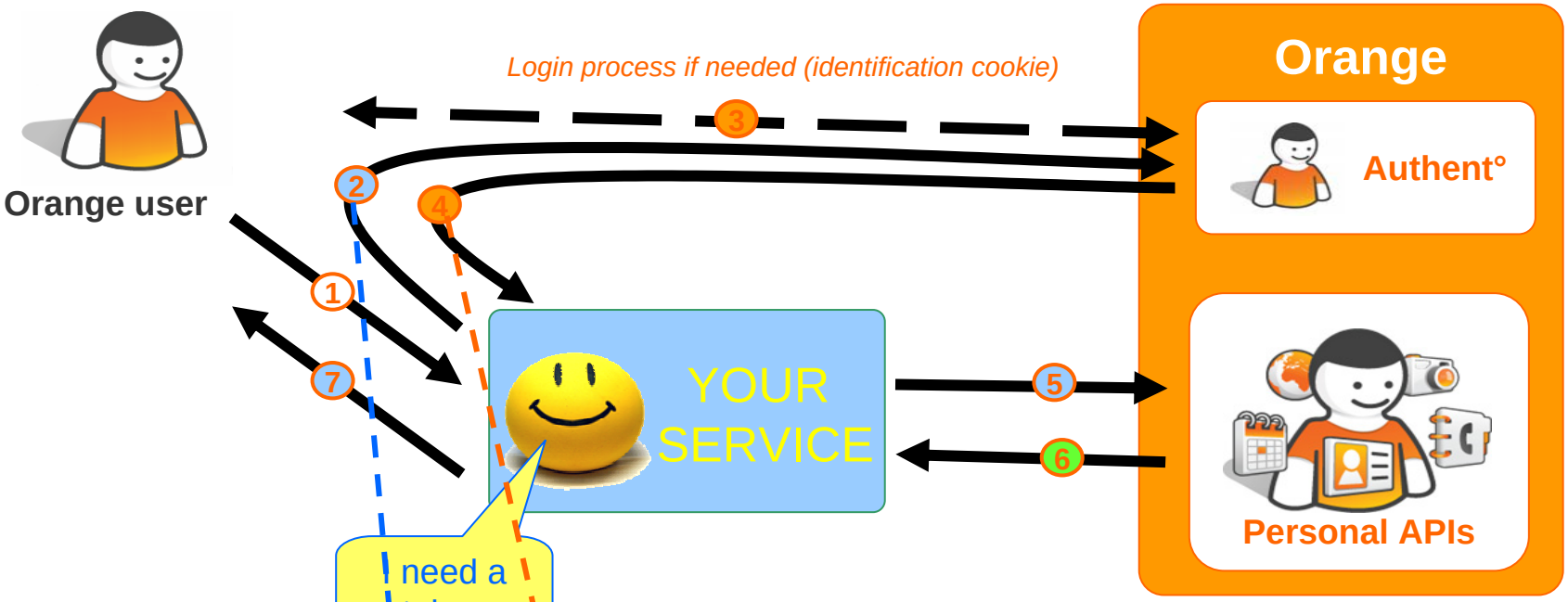
- **Éléments “propriétaires”**
  - APIs et la gestion des autorisations d’accès aux services
  - Standards peu matures/peu adoptées sur les services (contacts, calendrier, etc.)
  - Complexité de gérer les services existants

- **Basés sur :**
  - Des protocoles standard (REST)
  - Le SSO
  - Une plate-forme de médiation
  - Une plate-forme de Privacy
  - Un site d’enregistrement www.orangepartner.com
  -

Personal APIs
Composants technologiques



Scenario



Decoded extract of the SAML response:

...

<Attribute Name="**OrangeAPIToken**" NameFormat="urn:oasis:names:tc:SAML:2.0:profiles:attribute:basic">

<AttributeValue xsi:type="xs:string">

Redirect to: http://auth.orange.fr/sso?SAMLRequest=[SAML_request_zipped_base64encoded]

[returned token]

</AttributeValue>

</Attribute>

...

```
<AuthnRequest xmlns="urn:oasis:names:tc:SAML:2.0:protocol"  ID=[random_id] Version="2.0" IssueInstant=[date] >
    <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
      [your_serviceid]
    </Issuer>
</AuthnRequest>
```

Solutions d’interoperabilité

- SSO :
  - **SAML** : principe des cercles de confiance
  - **Openid** : découverte des fournisseurs d’identité dynamique. Systèmes de whitelist / blacklist
  - Problématiques des niveaux de sécurité et gestion des cookies et de la confiance
  - Plusieurs dizaines de milliers de sites qui acceptent openid. Les limites du systèmes sont qu’il y a plus d’acteurs majeurs fournisseurs que consommateurs. Orange propose les deux aspects en France.

- Personal APIs :
  - Compatibilité des Personal APIs avec SAML v2 et OpenID Orange.
  - Aucune interopérabilité aujourd’hui. Réflexions en court à la GSMA, en particulier au niveau du profil
  - Difficulté d’aligner les architectures de part la diversité des services
  - OAuth est une première piste pour l’autorisation d’accès aux APIs
  - One API (Open Network Enabler) GSMA : initiative opérateurs visant à standardiser l’exposition de services opérateurs dont la localisation, et le user profile

- L’interopérabilité peut toujours être faite par des acteurs tiers aggrégateurs : Rpxnow (SSO) ou AddThis (social Bookmarking)

Architectures régalienne

- Mon.service-public.fr :
  - Lancement 15 décembre 2008
  - Objectif 10 M citoyens 2011
  - Issu d’un pilote de faisabilité entre 2004 et 2006
  - Co-développement Orange/Cap Gemini

  - Identification via protocole Liberty IDFF 1.2+ composants identités

Mobilité et nomadisme

Accès via mobile

- SSO :
  - Authentification implicite via MSISDN/Alias
  - Possibilité pour les clients I et M de fusionner leurs comptes, et de gérer le cycle de vie des utilisateurs. Dans ce contexte, fluidité et optimisation des écrans/pages intermédiaires et saisies.

- Personal APIs :
  - Même ergonomie qu'en web. Ecrans de confirmation adaptés au mobile. Gestion de la privacy accessible en Web seulement.

Nomadisme

- SSO :
  - Authentification implicite sur Livebox et forcer l'authentification explicite. Différencier un client Orange chez lui et un client qui a un accès anonyme, et donc les services peuvent profiter, en fonction de leur niveau de sécurité nécessaire.
  - Ergonomies orientées pour éviter la gestion de session longue sur les postes qui ne sont pas ceux de l'utilisateur. ("me connecter automatiquement" disponible qu'en deuxième accès). > Juste milieu à trouver pour allier sécurité et ergonomie

- Personal APIs :
  - Accès similaire en nomadisme.

Formes et usages de l'authentification

- **OpenID** :
  - Contextes d'authentifications (possible aussi en SAML).
  - Quelques fournisseurs d'authentification forte :
    - trustbearer, avec dongle, smartcard ou biométrie
    - Option myopenid.com

- **Authentification forte et les difficultés de mise en place**
  - Nombreux travaux par le passé et encore plusieurs en cours sur l'authentification out of band : SMS, Bluetooth avec mobile, GBA, etc.
  - Niveaux d'authentification Réseau (MSISDN et Livebox) et Logiciel (login/pass)
  - Pas d'authentification forte prévue dans le cadre des services Grand Public nécessité de déployer du hardware (lecteur de carte, biométrie, etc.).

- Si demain l'internet se fusionne avec l'internet mobile, les problématiques de déploiement de hardware se reposeront même si elles sont résolues sur PC.

- L'authentification mobile offre une bonne alternative car à mi chemin entre l'authentification faible et l'authentification forte.

orange

Collecte et archivage des données personnelles

SSO :

Conforme à la législation en rigueur

OpenID / SAML offrent la possibilité d'exporter son profil

Possibilité pour l'utilisateur de modifier la plupart de ses données

Principe de base : ne rien envoyer sans que l'utilisateur donne son accord explicite

Et tracer les usages qui sont faits des données partagés.

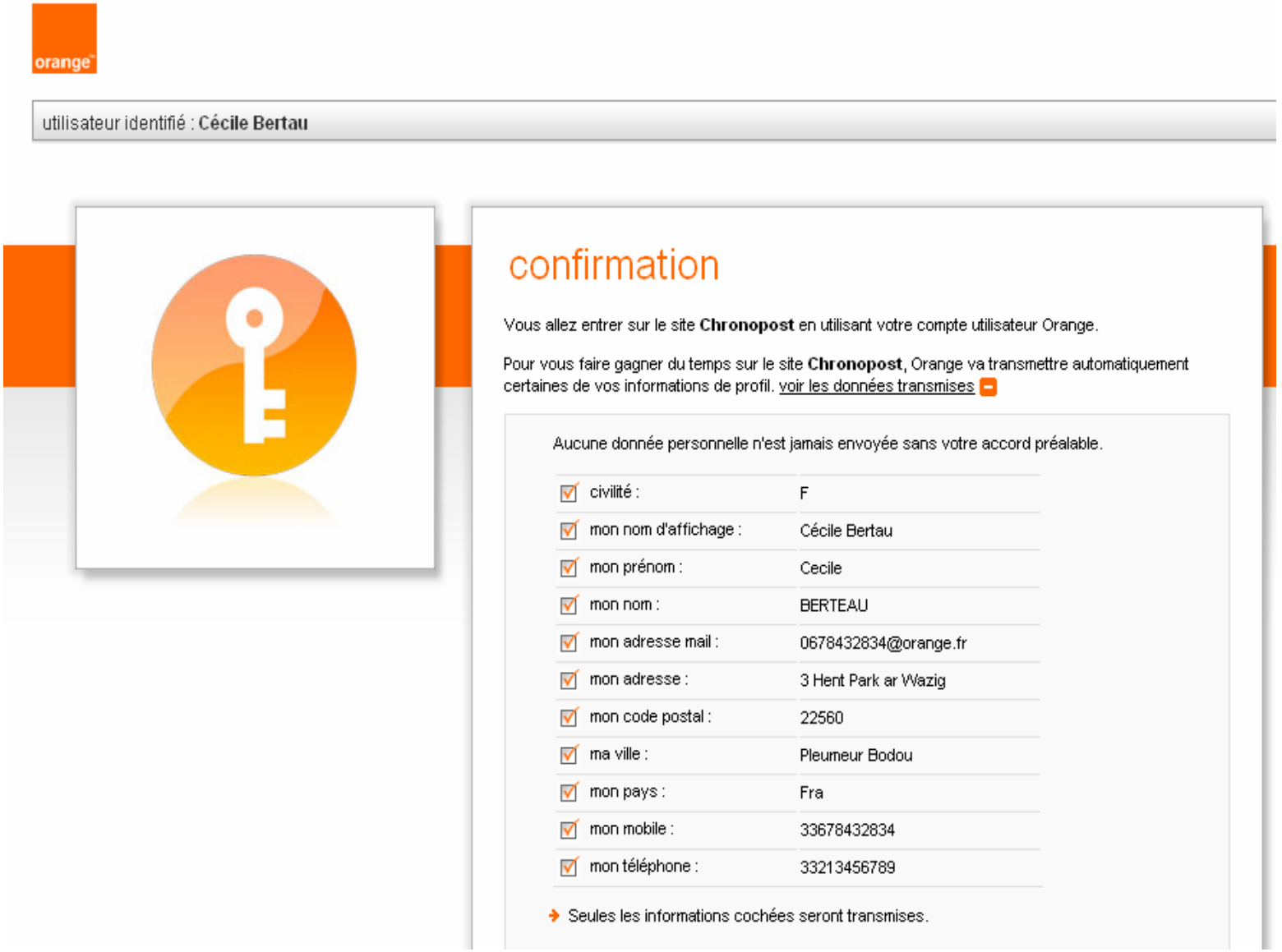
Personal APIs :

Gestion fine de la privacy : Moteur de règles de partages avec règles permanentes ou temporaires.

Possibilité pour le client de sélectionner les actions autorisées

Tableau de bord utilisateur pour contrôle des partages d'informations et de services

Besoin de plus en plus important de contrôler le type d'information/les éléments en amont pour éviter les manipulations parfois pernicieuses et peu explicites des sites


orange
utilisateur identifié : Cécile Bertau
confirmation
Vous allez entrer sur le site Chronopost en utilisant votre compte utilisateur Orange.
Pour vous faire gagner du temps sur le site Chronopost, Orange va transmettre automatiquement certaines de vos informations de profil. voir les données transmises
Aucune donnée personnelle n'est jamais envoyée sans votre accord préalable.
civilité : F
mon nom d'affichage : Cécile Bertau
mon prénom : Cecile
mon nom : BERTEAU
mon adresse mail : 0678432834@orange.fr
mon adresse : 3 Hent Park ar Wazig
mon code postal : 22560
ma ville : Pleumeur Bodou
mon pays : Fra
mon mobile : 33678432834
mon téléphone : 33213456789
Seules les informations cochées seront transmises.


Orange user
Privacy interaction form
Orange
User Privacy
5
4
6
Redirect to your_return_url
orange
Utilisateur identifié : John DOE
Partage de mes informations
YOUR SERVICE
Je souhaite :
Ajouter des évènements à mon agenda Orange
Annuler
Autoriser
Mémoriser ce choix
Accéder à l'espace de gestion des partages de mes informations personnelles
Redirec
<?xml v
<error>
<cod
-3
</cod
<deta
Priv
</det
<url>
htt
</url
</error>
Publicité | A propos d'Orange | Signaler un contenu illicite | AFA protection de l'enfance | Prévention et protection | Informations légales
orange

Privacy

- Un dashboard, disponible sur Orange offre à l'utilisateur un point central de gestion et contrôle des règles d'accès à ses données personnelles :
  - Liste des règles mises en place
  - Vue sur l'historique d'accès à ses données
  - Liste des partenaires

Partage de mes informations

avec Orange, je me facilite la vie

en partageant mes informations en toute sécurité avec les sites de mon choix :

je gagne du temps quand je m'identifie
ou quand je remplis des formulaires

j' accède à mes services Orange depuis ces sites,
comme mon **agenda** ou mon **carnet d'adresse**,
mes **messages**, et bien plus encore....

je modifie à tout moment la gestion de mes services personnalisés.

Cet espace vous permet de gérer le partage de vos informations personnelles selon vos besoins et de visualiser l'historique de vos partages.

› Mes services › En savoir plus

Découvrez les avantages de ce service chez nos partenaires

› afficher tous les partenaires

Orange s'engage à protéger votre vie privée

Vos informations personnelles ne seront en aucun cas transférées à des tiers sans votre accord.

Anonymat, zero knowledge

SSO

- Comportement par défaut de l'implémentation d'OpenId V2: donner des alias différents pour les différents sites pour éviter les mises en commun de bases

Personal APIs

- basé sur l'anonymat du SSO Orange
- Anonymisation des statistiques d'usage pour les tiers

Merci