Orange Authentication API
Using Liberty’s **SAML Simple Sign Binding**

ID-CONF MUNICH, Liberty Alliance workshop, April 2008

Philippe Clément  Head of Identity Enabler, Group Strategic Marketing  philippe.clement@orange-ftgroup.com
Orange / FT Group Worldwide

• **Worldwide:**
  - 220 countries, 170M customers
  - 109M mobiles, 11.6M ADSL, 49M landlines subscribers
  - Leading Telco on fixed/mobile convergence (multiple-play offers, Unik, Livebox)

• **Europe:**
  - 78 million mobile subscribers (#3 in Europe)
  - 47.5 million PSTN landlines (#1 Europe)
  - 11.6 million broadband ADSL lines (#1 Europe)
  - 4.8 million VoIP lines (#1 Europe)

• **France:**
  - 40M active identities in France
  - 185 services federated to Identity Platform covering:
    - Web portal services, Widgets, desktop applications, VoIP, IPTV
    - WAP and Mobile applications
    - Other device-based applications around the Livebox® home gateway
  - SSO and APIs for internal use (based on Liberty Alliance principles)
The Orange Personal API Value Proposition

• Orange is a major provider of online identities
  – In France, Orange manages 23 million mobile users and 15 million individuals with Internet access accounts. 7 out of 10 in France have an Orange Identity
  – Because of network-based authentication mechanisms, Orange delivers enhanced user experiences
    • On mobile: SIM cards → fully transparent authentication
    • On web: DSL-based implicit authentication + multi-level “last known users” management
    • 90% of Orange users do not need to enter a user name/password to access their accounts because of these advanced identification mechanisms based on device recognition
    • When introduced in France, this feature doubled service usage of the Orange communication services

Orange is now opening authentication and authenticated APIs to partners
  – Partners can provide services that are easier to access from Web and Mobile devices
  – Partners can leverage Orange service features via APIs to enhance the customer promise and sales conversion rate for their services
Developer’s journey

- APIs are available via our Partners' website (www.orangepartner.com)
- Partners register to use APIs, receive toolkits, code examples and guidelines
- Partners install Orange’s sign-in functionality on their website

Protocols supported:
- Open ID v1 (Sept 07)
- SAML Simple Sign Binding (Feb 08)
- Open ID v2 (2008)
End users' journey

• User Journey #1: registering on Partner's site with Orange ID

User is already authenticated by Orange (e.g. connects behind home DSL connection)
  – User chooses to access partner's site with his Orange ID
  – User is redirected to Orange IdP; no sign-in page is displayed as there is an existing user session
  – Orange prompts user for authorization before establishing federation and sharing attributes
  – User is redirected to the partner's site, where he continues his journey (typically, 1st time access wizard)

  demo

• User Journey #2: authenticating on Partner's site with Orange ID

The user may be connecting from anywhere
  – User chooses to sign-in on partner's site with Orange ID
  – Partner site "remembers" the previous Orange authentication and proposes immediately to sign-in with Orange (partner site behaviour)
  – User is redirected to the Orange IdP which displays a sign-in page. Typically, user selects his account and types his password
  – User is then redirected to the partner site

  demo
Orange Authentication API: SSO flow

1. The user accesses the site of the service provider.

2. The user clicks on the button "Sign in with an Orange user account" and is redirected to the Orange Authentication service (identity provider).

3. Orange authenticates the user (this stage is transparent for the user if a valid Orange authentication session already exists or if the user can be authenticated implicitly).

4. Orange Authentication service redirects the user to the service by providing an assertion of authentication (SAML Response). The service provider can therefore personalise a service on the basis of the user identifier provided by Orange Authentication service.
Orange Authentication API: SSO flow

"orange.xx" DNS domain

3rd party website
OrangeAuth Service
id.orange.fr

SSO request (SAMLRequest)

Processing of the SAML "AuthnRequest"

Enter credentials

Session cookie

Service cookie for OrangeAuth (+ list of attributes requested by OrangeAuth)

Form POST

SSO response (SAMLResponse, SigAlg, Signature)

Retrieval of the previously generated federation alias. Generation of the SAMLResponse (no interaction for authorization required).

Only happens if no active Orange session yet exists.
Detail of SAML implementation

• Protocol details :
  – SAMLRequest :
    <AuthnRequest xmlns="urn:oasis:names:tc:SAML:2.0:protocol" ID="_b050e0f4c673ec2572fc65d95359afe6"
      Version="2.0" IssueInstant="2007-12-21T19:54:07Z" >
      <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">third-party service ID provided at registration</Issuer>
    </AuthnRequest>
  – SAMLResponse (XML content) :
    • Status
    • NameIdentifier (one-time federation alias)
    • Authentication context class
    • Identifier of the IDP
    • Identifier of the SP
    • Timestamps (for the validity of the response)
    • Other core profile attributes
    • "OrangeAPIToken"
      – To be used for subsequent access to APIs (calendar, photos, contacts, messages etc. )

• Simple Sign Binding
  – Use of plain text signature instead of XML-Signature for easier integration at partner's site
  – Integration into ipernity.com by non identity expert achieved in a few days !
thank you

Please visit www.orangepartner.com for more details on Orange's authenticated APIs