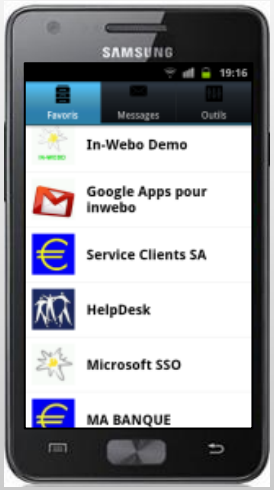
IN-WEBO
Mobile & Web Strong Authentication

De l'authentification au hub d'identité

si simplement…

Présentation OSSIR du 14fev2012



Olivier Perroquin
In-Webo Technologies

Mission et solutions d'In-Webo

- Apporter aux Entreprises et Opérateurs de Services des solutions de sécurisation des accès et des transactions

- Notamment, là où les solutions de sécurité traditionnelles ne se déploient pas, pour des raisons
  - de *faisabilité* : sécurisation des nouveaux terminaux, Cloud
  - de *coûts* : équipement des utilisateurs et partenaires, SMS
  - de *complexité* : intégration laborieuse, gestion des cycles de vie
  - ou d'*usage* : mise en œuvre de certificat, connexion d'équipement, etc.

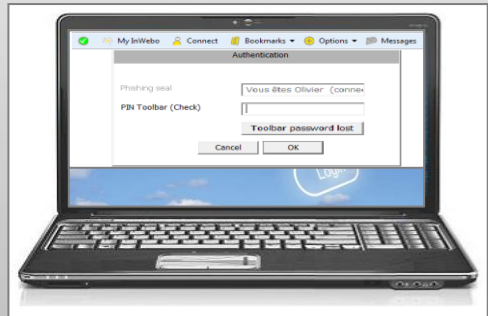
- Grâce à des solutions d'authentification forte
  - simples d'usage
  - dématérialisées et hautement sécurisées
  - sans adhérence IT ni investissement (moyens gratuits)
  - universelles et compatibles avec des solutions d'identité numérique

Authentification forte ++ !

- Sécuriser les applications en ligne, les applications mobiles, les accès distants, les paiements, par une authentification forte intégrée au navigateur, au téléphone ou aux applications.

- Permettre enfin l'accès d'une authentification forte et sécurisée au plus grand nombre.

- Créer grâce à une authentification forte 'démocratisée' de nouveaux usages à valeur ajoutée (paiement sécurisé, dématérialisation des souscriptions, protection des données des applications en mode Cloud…)



Prouver l'identité

IN-WEBO
Mobile & Web Strong Authentication

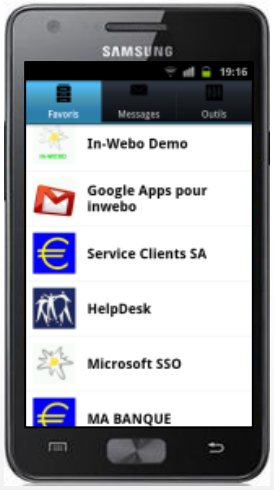
- m-banking
- Extranet
- pari en ligne
- paiement 3D secure
- e-gouv
- Authentification applicative
- smart app sécurisée
- vote électronique
- jeux en ligne
- e-santé
- TV media box
- helpdesk authentifié
- web mail
- VPN
- signature d'opération de maintenance
- e-digicode
- groupware

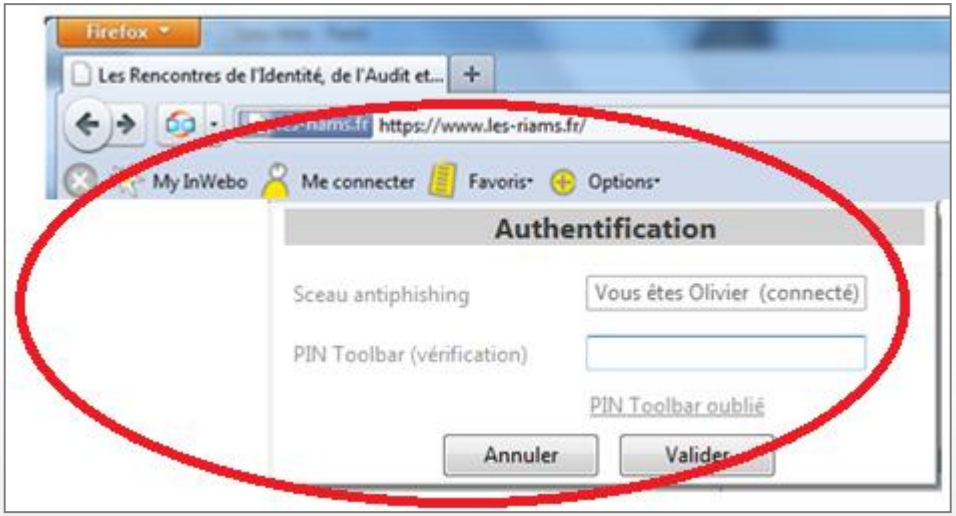
Propositions de valeur

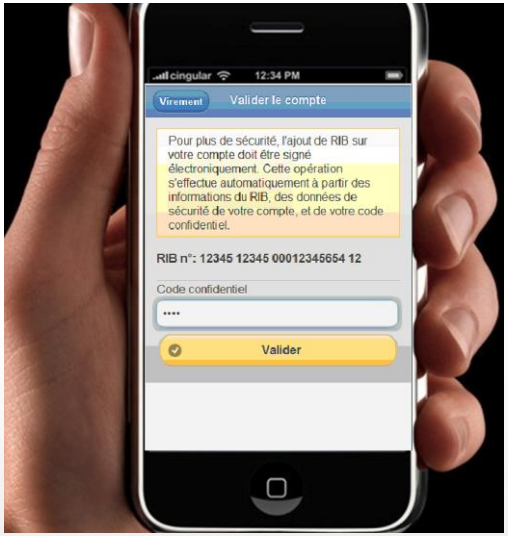
- **Permettre des déploiements massifs et simplifiés**
- **Réduire le TCO global de l'authentification forte existante**
  - **Dématérialisation du token, tout en maintenant sa sécurité**
  - **Externalisation avec des moyens répondant aux contraintes règlementaires (SOX, PCI, …) et business (sécurité, disponibilité)**
  - **Pas d'investissement (outils gratuits, pas de FAS), facturation à l'usage**
  - **Effort d'intégration minimal, pas d'équipement à administrer**
  - **Selfcare pour la gestion des équipements permettant l'authentification forte**
- **Sécuriser les nouveaux usages de l'Entreprise (applications mobiles / tablettes, applications SaaS, B2B)**

Simplifier …

- **Simplifier l'usage en mettant l'outil au cœur du parcours client.**





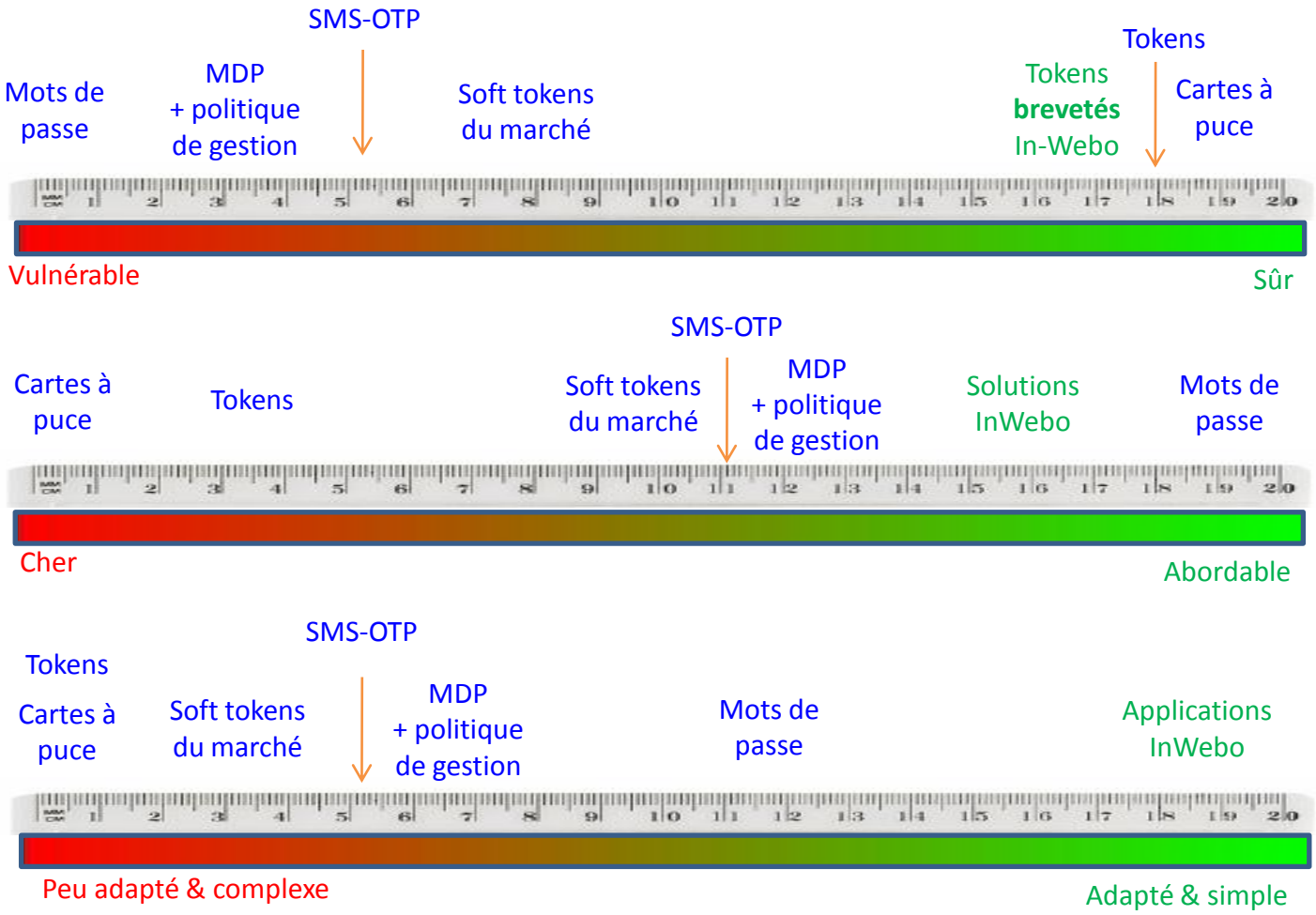


⇒ sur le téléphone dans le navigateur intégré aux applications

- **Fonctionnement SSO-like vu des utilisateurs**
- **Permettre un enrôlement simple compatible avec les exigences métiers**
- **Réduire la lourdeur de gestion des tokens**

Positionnement des solutions

IN-WEBO
Mobile & Web Strong Authentication



Authentification forte sécurisée

Une authentification forte **sécurisée** doit répondre à plusieurs critères :

- Doit être multi-facteur (ce que j'ai, ce que je sais, …)
- Ne doit être valide **qu'une seule fois,** si possible pendant **un laps de temps limité**
- Doit être **non-prédictible,** même en cas de **compromission d'un des facteurs**

  ! Les solutions dématérialisées du marché ne remplissent pas ce critère

Sécurité : Eléments différenciateurs des tokens logiciels

IN-WEBO
Mobile & Web Strong Authentication

OTP = Fonction (Clé secrète perso , PIN , Compteurs)



✓

Token SW

OTP = Fonction (Clé secrète perso , PIN , Compteurs)



✗

En cas de reverse-engineering du token SW, la connaissance d'un OTP valide permet de calculer le code PIN par recherche exhaustive

IN-WEBO

OTP = Fonction (Clé secrète perso, PIN, Compteurs,



Clé service, clés dynamiques.)


✓

En cas de reverse-engineering du token SW, les clés dynamiques empêchent le calcul du PIN en cas de connaissance d'un OTP

⇒ augmente sensiblement la complexité de la fonction de synchronisation

Code PIN non stocké, recherche exhaustive de l'OTP impossible

In-Webo - Architecture

Moyens d'authentification forte

Toolbar dans navigateur
Appli dans téléphone
Librairie pour application

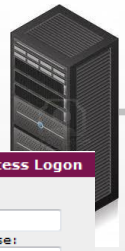
Génèrent des mots de passe à usage unique

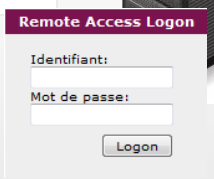
Activation et gestion de moyens d'authentification forte

IN-WEBO

HSM

Connexion aux applications





Application
(Web, portail, VPN, Mobile, Cloud, etc.)

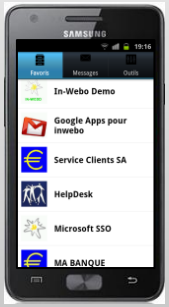
Connecteurs d'authentification
Web services,
Radius,
SAMLv2

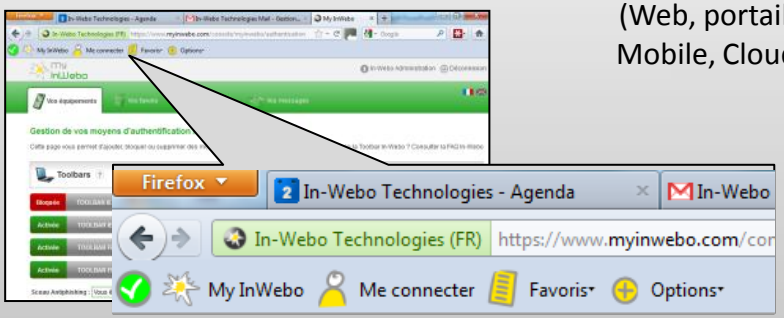
API

API

Web Console

Administration & config
Gestion utilisateurs
Support utilisateurs
Selfcare utilisateurs





La protection ultime des identités numériques

Usages

Générateur universel d'OTP sur téléphone

Générateur universel d'OTP

- Pas de sms ni de connexion, fonctionne sans couverture radio
- Administration de la politique, du format de l'OTP
- Ajout de nouveaux 'Favoris' indépendants à la volée
- Basé sur un protocole bien mieux sécurisé qu'OATH pour les environnements sans « Secure Element »
- Fonctionne également en mode défi/réponse ou scellement
- Disponible pour Androïd, iOS, Blackberry, j2me, Windows Mobile,
- Certification prévue pour Q1 2012

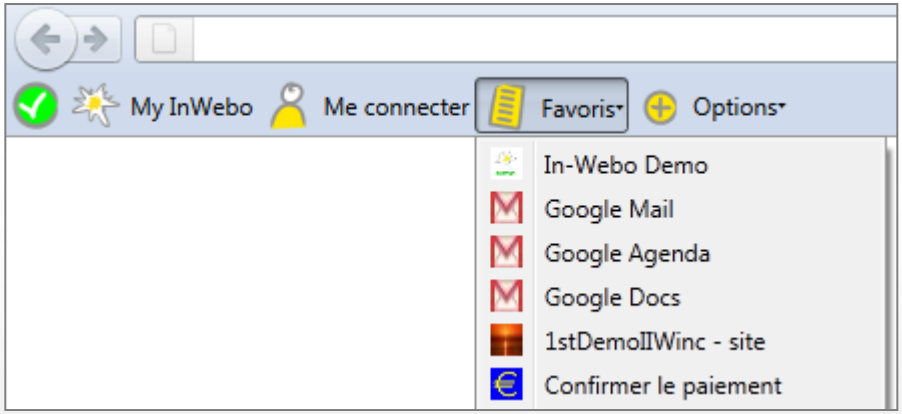
Usages dans tous environnements

- Applications web professionnelles et Grand Public
- Clients applicatifs (VPN IPSec, SAP, Citrix, …)
- Call centers
- …

Accès sécurisé depuis un ordinateur personnel

Connexion sécurisée et automatisée aux applications web

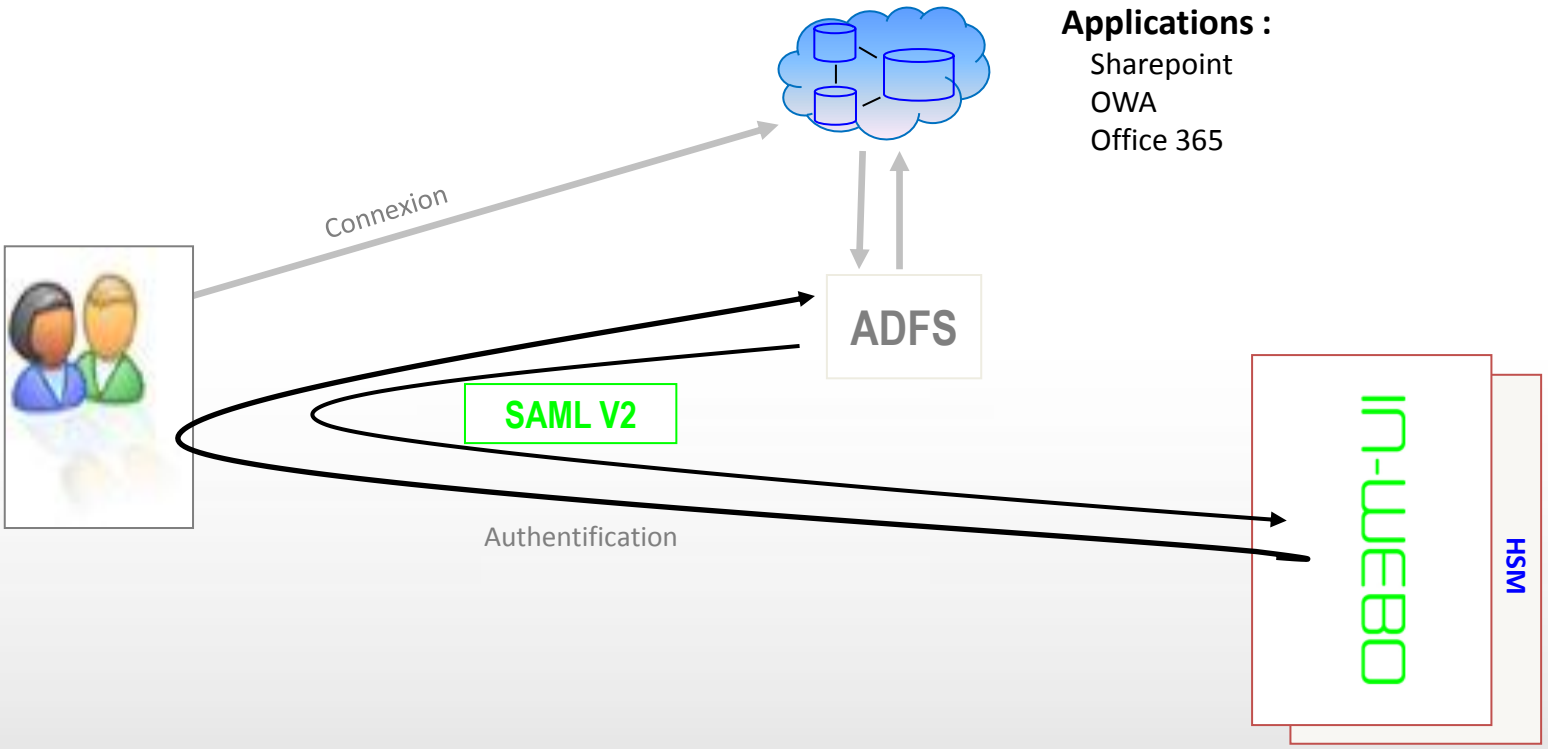
- Outil intégré, ergonomie optimale
- Vérifications de sécurité (phishing, MITM, html injection, …)
- Génération de l'OTP et interaction avec la page d'authentification (pas d'intégration)
- Administration de la politique, du format de l'OTP
- Ajout de nouveaux 'Favoris' indépendants à la volée
- Disponible pour IE, Firefox, Chrome, Safari



Usages depuis un (ou plusieurs) ordinateurs personnels

- Applications web professionnelles et Grand Public
- Services web B2B
- Clients applicatifs

In-Webo – Microsoft ADFS – Fédération d'identité

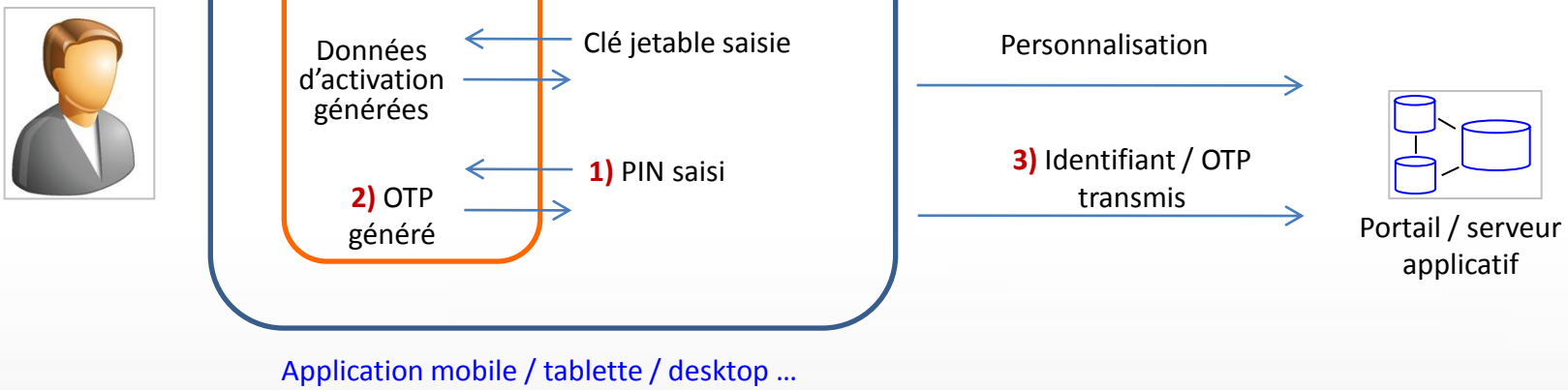


Solutions démontrée au Microsoft Technical Center

- ✓ Sharepoint, OWA on premise
- ✓ Office 365 : OWA et Sharepoint online

CRM Dynamcis

Authentification forte d'application embarquée



Sécurisation de l'accès via les applications embarquées

- SDK permettant d'embarquer l'authentification dans toutes les Apps
- Parcours client transparent, inséré dans l'existant
- Principes de sécurisation brevetés

Usages depuis un smartphone, une tablette, une TV connectée …

- Applications métier
- Mobile banking
- …

Plateformes supportées

IN-WEBO
Mobile & Web Strong Authentication

Téléphones et smartphones

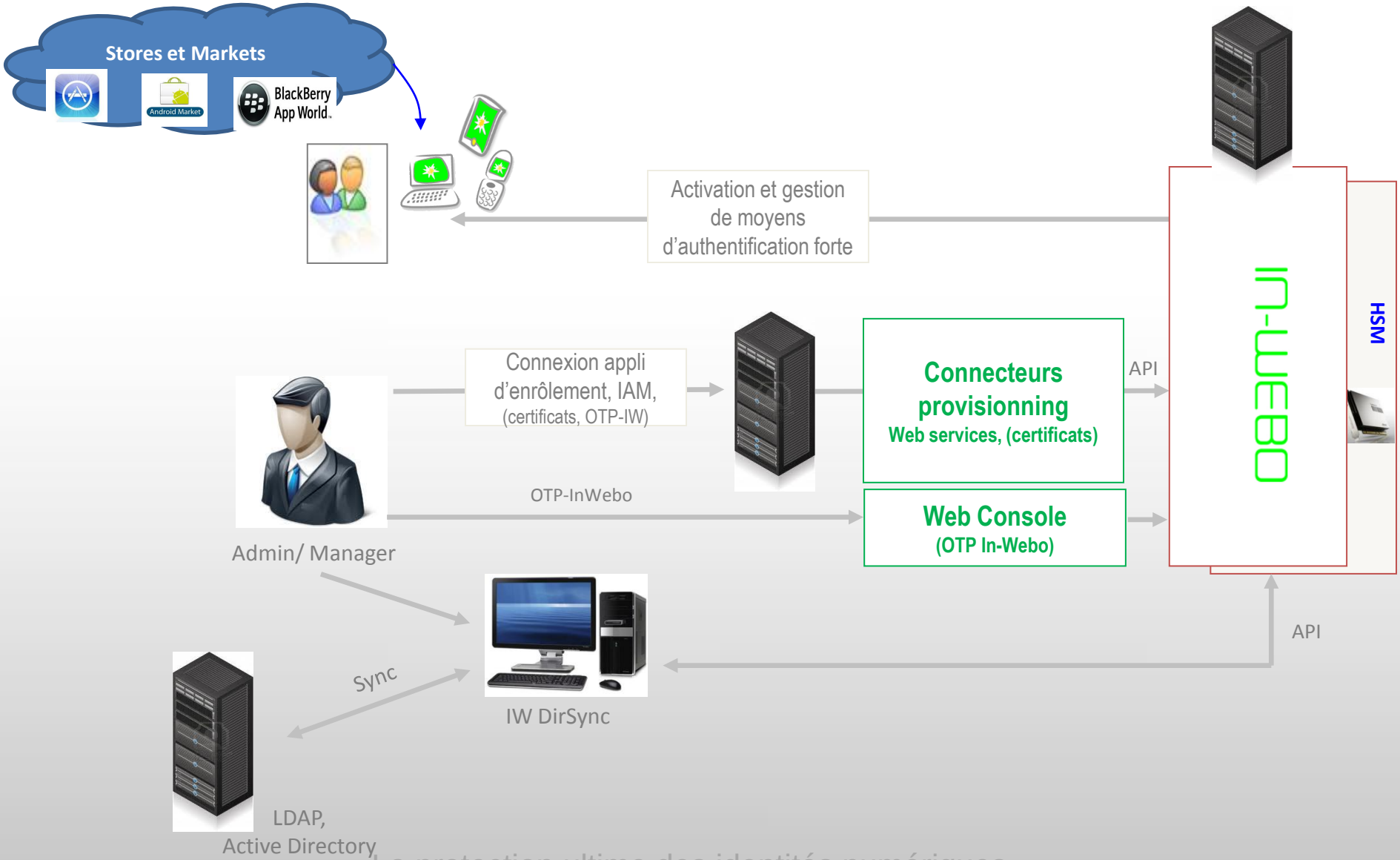
OS et navigateurs

symbian OS … et tout téléphone Java MIDP 2.0

Pâques 2012

Mise en œuvre et gestion

Enrôlement des utilisateurs



Intégration

Intégration du serveur d'authentification

Intégration d'un webservice
(exemples de code fournis)

Site Web, Portail mobile, Extranet

Web Services validation

API

validation

Paramétrage de l'interface d'administration
(**pas d'intégration !**)

SaaS

SAML

API

validation

Configuration d'une politique Radius
(**pas d'intégration** !)

VPN, accès distant

Radius

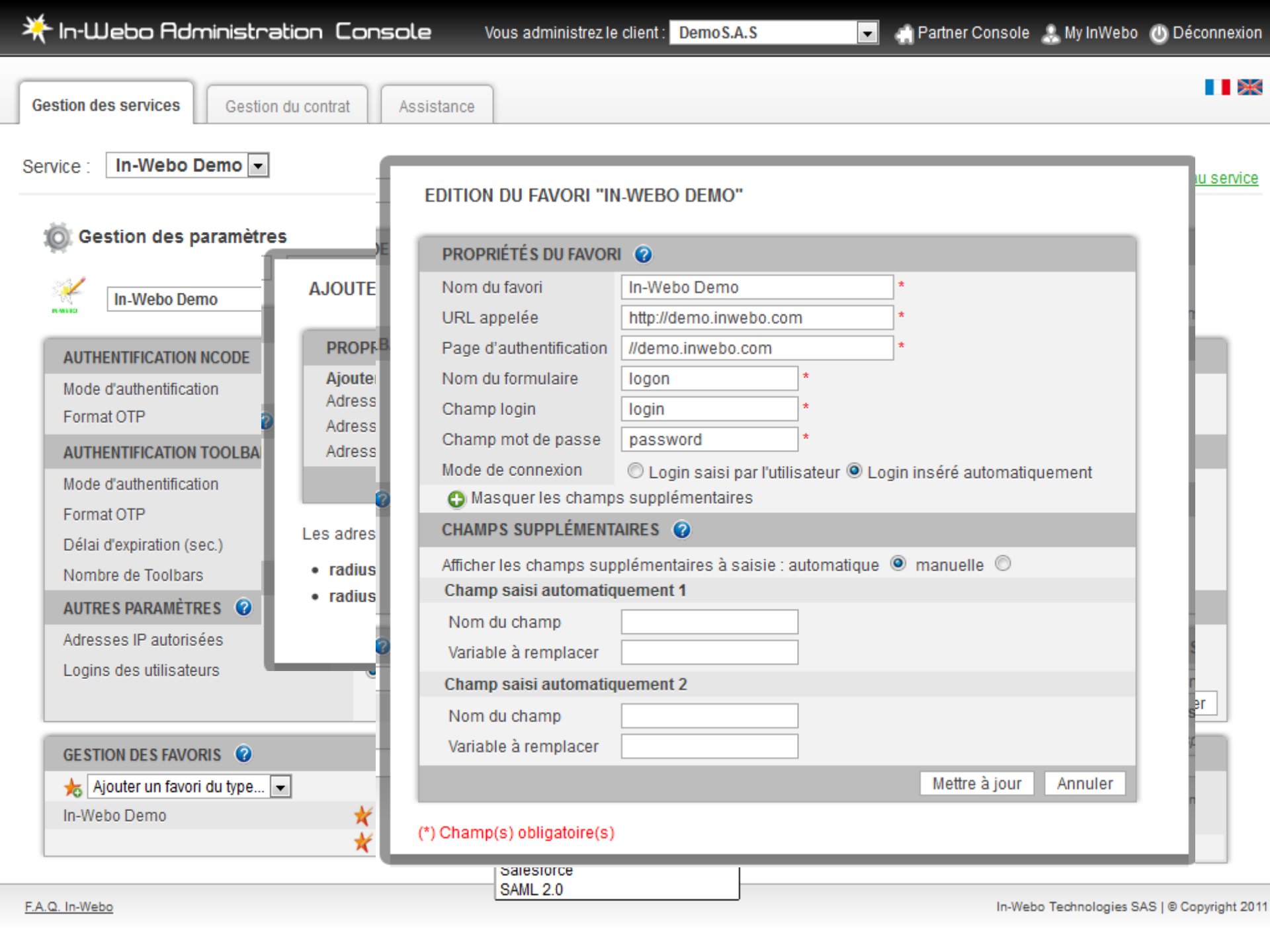
API

validation

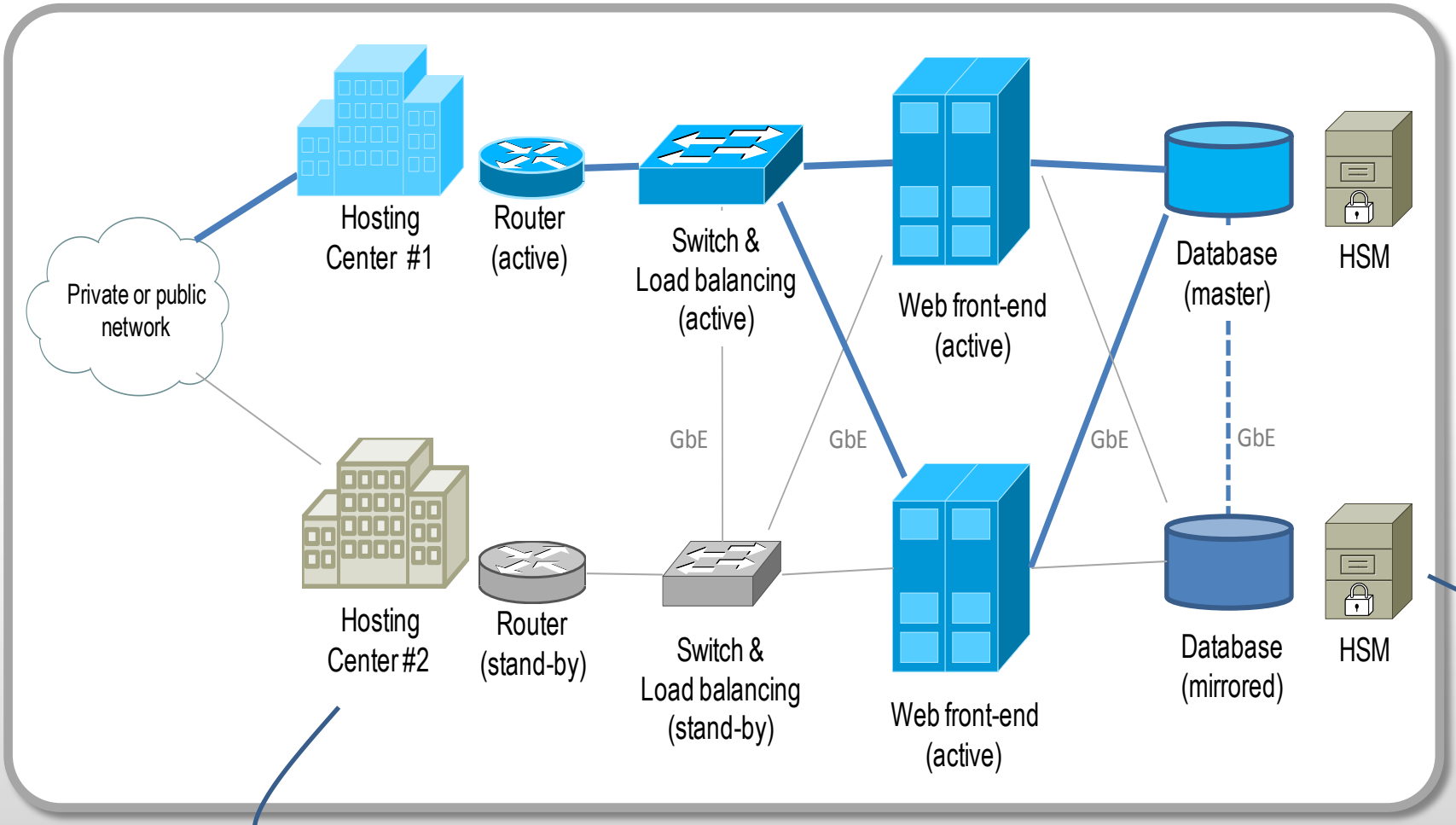
IN-WEBO

HSM

Gestion en selfcare du service d'authentification


In-Webo Administration Console
Vous administrez le client : DemoS.A.S
Partner Console
My InWebo
Déconnexion
Gestion des services
Gestion du contrat
Assistance
Service : In-Webo Demo
Gestion des paramètres
In-Webo Demo
AUTHENTIFICATION NCODE
Mode d'authentification
Format OTP
AUTHENTIFICATION TOOLBA
Mode d'authentification
Format OTP
Délai d'expiration (sec.)
Nombre de Toolbars
AUTRES PARAMÈTRES
Adresses IP autorisées
Logins des utilisateurs
GESTION DES FAVORIS
Ajouter un favori du type...
In-Webo Demo
AJOUTE
PROPR
Ajoute
Adress
Adress
Adress
Les adres
radius
radius
EDITION DU FAVORI "IN-WEBO DEMO"
PROPRIÉTÉS DU FAVORI
Nom du favori
In-Webo Demo
URL appelée
http://demo.inwebo.com
Page d'authentification
//demo.inwebo.com
Nom du formulaire
logon
Champ login
login
Champ mot de passe
password
Mode de connexion
Login saisi par l'utilisateur
Login inséré automatiquement
Masquer les champs supplémentaires
CHAMPS SUPPLÉMENTAIRES
Afficher les champs supplémentaires à saisie : automatique
manuelle
Champ saisi automatiquement 1
Nom du champ
Variable à remplacer
Champ saisi automatiquement 2
Nom du champ
Variable à remplacer
Mettre à jour
Annuler
(*) Champ(s) obligatoire(s)
Salesforce
SAML 2.0
F.A.Q. In-Webo
In-Webo Technologies SAS | © Copyright 2011

Disponibilité – architecture logique



2 hébergeurs distincts « Tier 3 » ou « Tier 4 »
(Telecity / Equinix)

Hardware Security Modules