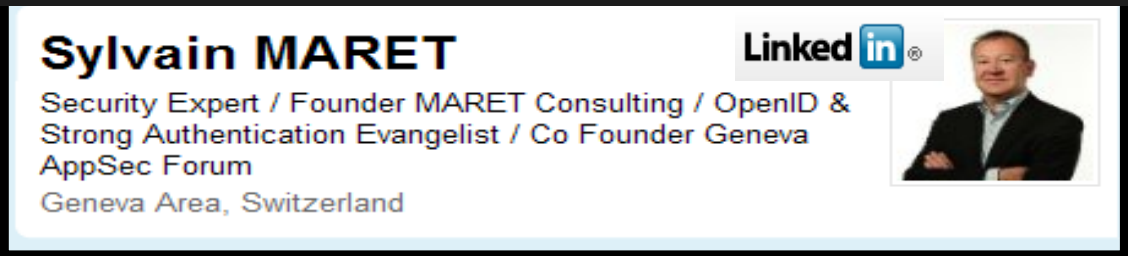
# *Comment protéger de façon efficace son/ses identité(s) numérique(s) sur le Web 2.0?*

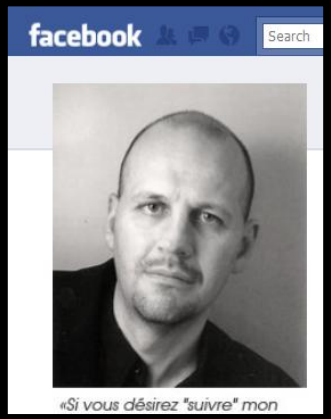
Sylvain Maret

Workshop der SATW ICT Commission
20./21. Mai 2010, Parkhotel Schloss Münchenwiler

# Identité(s) numérique(s)

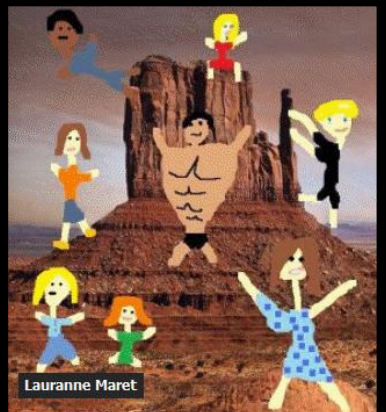












Physical world

Virtual world (abstract layer)

Sylvain Maret
Edit My Profile

virtual person — identity

virtual person — identity

virtual person — identity

one physical person


**Authentication Link**

http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.13_Virtual_Persons_v1.0.pdf

# Réalité ou fiction ?

# Les menaces…


ID Theft costs users $500 and 30 hours per incident (US FTC, 2003)
70% of users would trade their password for chocolate
Demonize-T Trojan Horse forwards password keystrokes to hacker websites
Identity Theft
Password Sniffers
Wireless LAN's and VPN's eliminate the security perimeter
On-line Commerce fastest growing method and twice the cost of in-person payment
Remote Workers
On-line Commerce
$3B in remote payment fraud
Phishing
Crack once, spoof everywhere (my bank password is also my Yahoo! Mail password)
In 2005, liability can be shifted to issuing banks… how will they pass-on the losses?
Phishing successful 5-10% of the time

# Impact ?

LinkedIn Home Profile Contacts Groups Jobs Inbox (2) More... People Advan

College & University Jobs - 10,000+ faculty and staff jobs. Don't just search. Connect. - From HigherEdJobs

Edit My Profile | View My Profile

Sylvain MARET (you)

Security Expert / Founder MARET Consulting / OpenID & Strong Authentication Evangelist / Co Founder Geneva AppSec Forum

Geneva Area, Switzerland | Computer & Network Security

**Sylvain MARET** Is installing BackTrack Live on USB

14 days ago · Comment · See all activity »

**Current**
- **Co Founder** at **Geneva Application Security Forum**
- **Swiss French Area delegate** at **OpenID Switzerland**
- **Founder & CEO** at **MARET Consulting**

see all...

**Past**
- Founder & CTO at e-Xpert Solutions SA
- Lecturer at University of Applied Sciences, Canton de Vaud
- Security Architect at Dimension Data

see all...

**Education**
- University of applied sciences, Geneva

**Recommendations** 37 people have recommended Sylvain

**Connections** 500+ connections

**Websites**
- My Company
- My Blog
- Folow me on twitter

- smaret

Add Sylvain to your network

Forward this profile to a connection

LinkedIn Feature

LinkedIn Stellenmarkt

Finden Sie über Ihr Netzwerk neue Mitarbeiter

Geben Sie heute eine Stellenanzeige auf.

Jetzt beginnen

**Sylvain's Activity**

**Sylvain MARET** Is installing BackTrack Live on USB

14 days ago · Comment

**Sylvain MARET** is interested in OWASP AppSec Research 2010 on June 21, 2010 RSVP

# Réalité !

## Facebook: des mots de passe dans la nature

**Publié le** 25-05-2009 **à** 07:29:26 **dans le thème**
**Pays :** France - **Aute**



Note des lecteurs: **3.6**/5

**Un internaute francophone aurait trouvé une faille qui lui per aux identifiants de connexion des utilisateurs Français de Faceb nous a communiqué 4.000 comptes. Êtes-vous dans la liste ?**
translation available.

Il se nomme HatXwhiTe, un jeune internaute Français de 18 ans. S invisible. Un web que personne ne regarde vraiment dans les yeu grattouille, le chatouille jusqu'à en extirper des données qui n'aura de leur espace alloué.

Parmi ces informations, HatXwhiTe aurait mis la main sur un m comptes des membres Français de Facebook. Inquiétant ? La réda le pense car pour prouver ses dires, le jeune hacker nous a comm près de 4.000 comptes [liste compléte à la fin de notre re identifiants, emails et mot de passe.

Nous avons pu tester la chose avec l'aide de 10 personnes tirées liste. Sur 10 comptes, sept mots de passe étaient encore valide jamais été utilisé par son propriétaire (ce qui éliminerait le phishing NDR), Un de passe avait été changé depuis deux ans (Ce qui tendrait à dire que la base données interceptée par HatXwhiTe cour sur une période de plus de deux ans, NDR).

**Rencontre du 3ème type**
Jeudi 07 mai, il est 19h30. Le soleil se couche lentement sur la capitale Flamande. rédaction de ZATAZ.COM commence à ranger ses papiers, son fouillis, ... Soudain, son d'une connexion MSN coupe le silence du bureau. "Salut, je me nomme HatXwhiT je viens de mettre la main sur une faille visant Facebook. Ça vous intéresse ?". Aut le dire de suite, ce genre de proposition fond sur la rédaction comme neige printemps. Sauf que dans ce cas, nous connaissons un peu cet internaute. Il n arrive de converser avec lui sur la toile. [*Lire son Interview*].

HIGH TECH, INFORMATIQUE, LOGICIELS

## Facebook, vol de mot de passe

Publié le 04 juin 2009 par Idrso

Un internaute francophone aurait trouvé une faille qui lui perme d´accèder aux identifiants de connexion des utilisateurs Français **Facebook**. Pour preuve, il a communiqué 4.000 comptes identifiants, emails et mot de passe. Êtes-vous dans la liste ? Révélati

Il se nomme passion, l'Int dans les ye extirper des

# Et s'il y avait

# le vôtre ?

# Authentification forte

## Authentifieur

Quelque chose
Que l'on possède

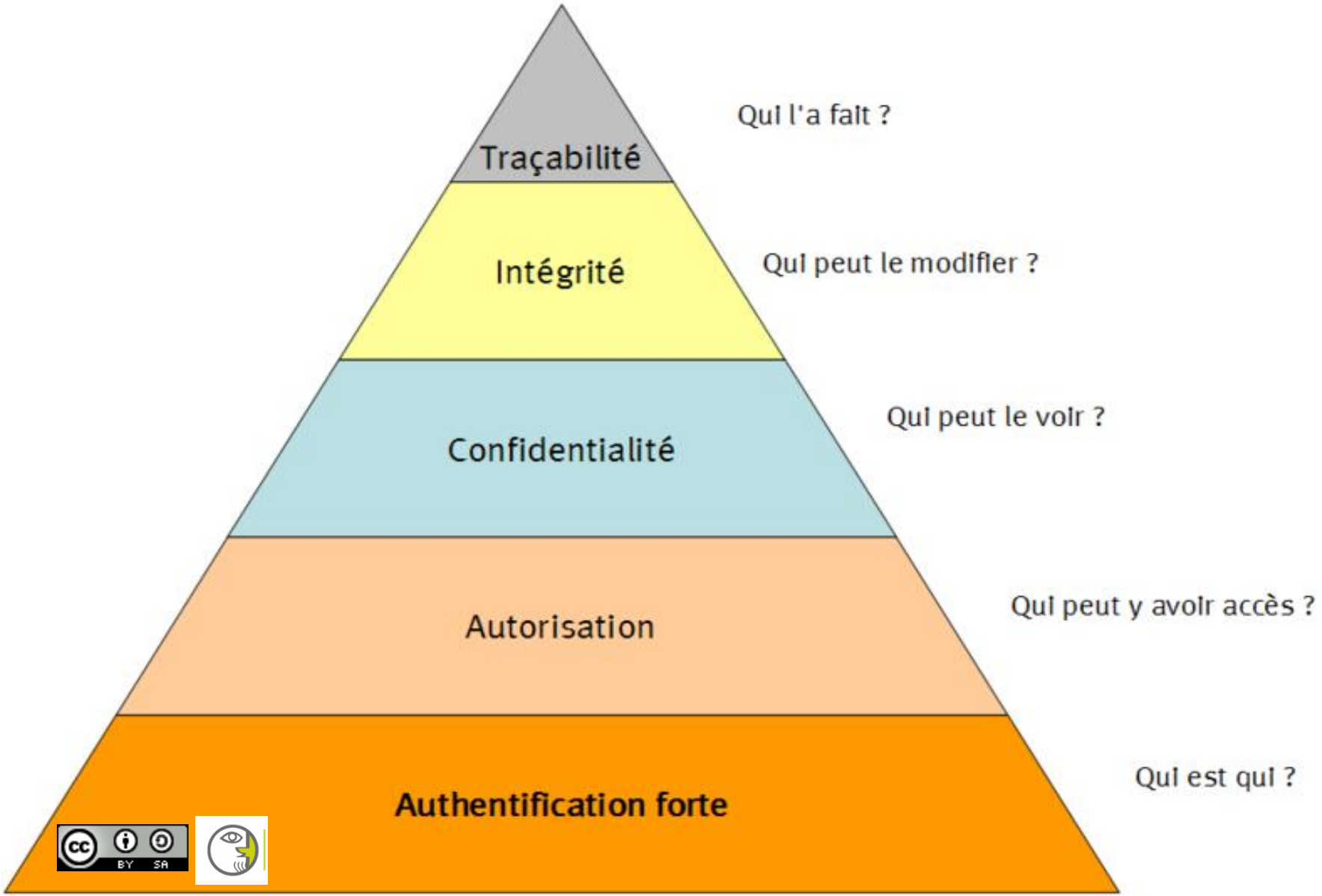
## Secret


Quelque chose
Que l'on connaît

## Biométrie

Quelque chose
Que l'on est ou fait

# La pierre angulaire



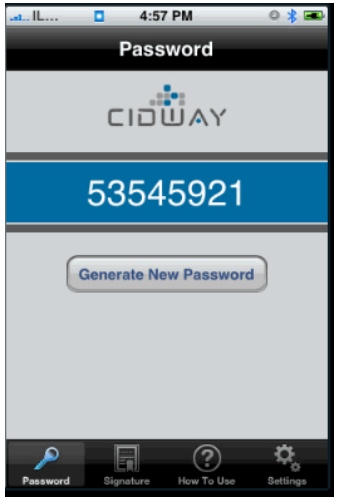
# Que choisir ?

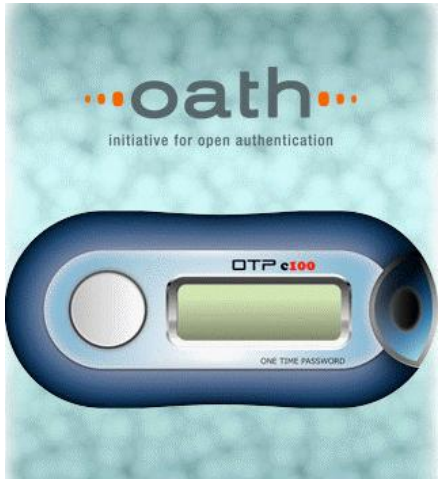

| | OTP | PKI （HW） | Biométrie |
|---|---|---|---|
| Authentification Forte | | | * |
| Chiffrement | | | |
| Signature numérique | | | |
| Non répudiation | | | |
| Lien fort avec l'utilisateur | | | |

* Biométrie type Fingerprinting

# Tendances 2010

# OTP Software SmartPhone





**OTP pour Iphone: un retour d'expérience**
**Software OTP pour l'Iphone**
**Mobile One Time Passwords**

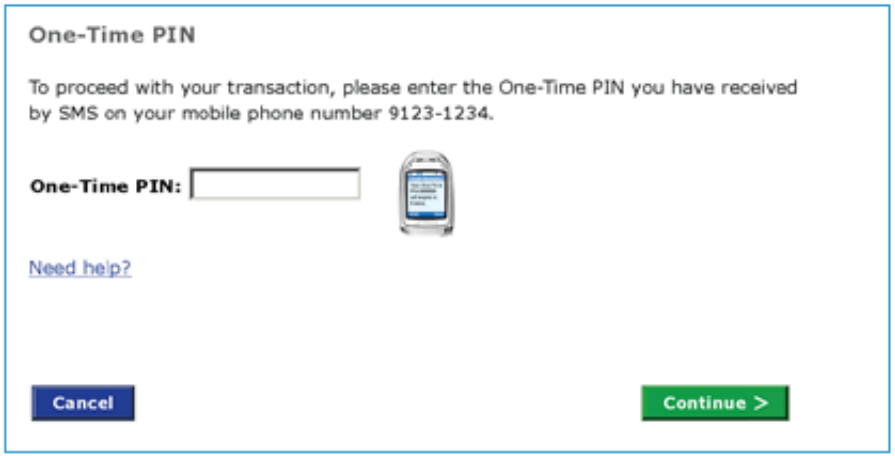


oath
initiative for open authentication

# OTP via SMS


OTP via SMS

Enter OTP



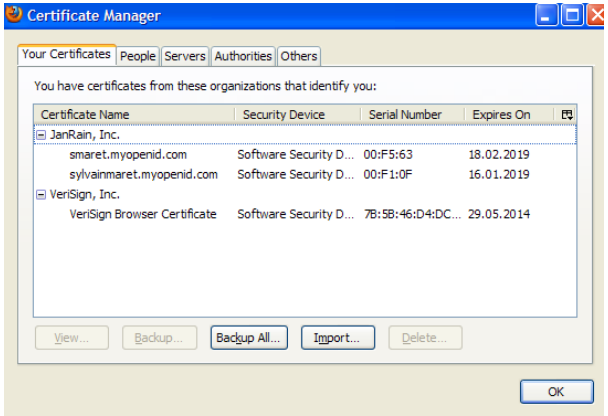
# OTP avec un authentifieur USB



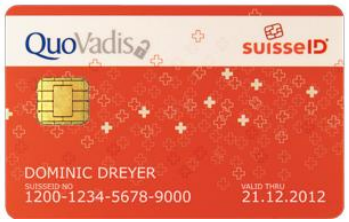
oath
initiative for open authentication

# PKI: Certificat numérique X509

## Software Certificate



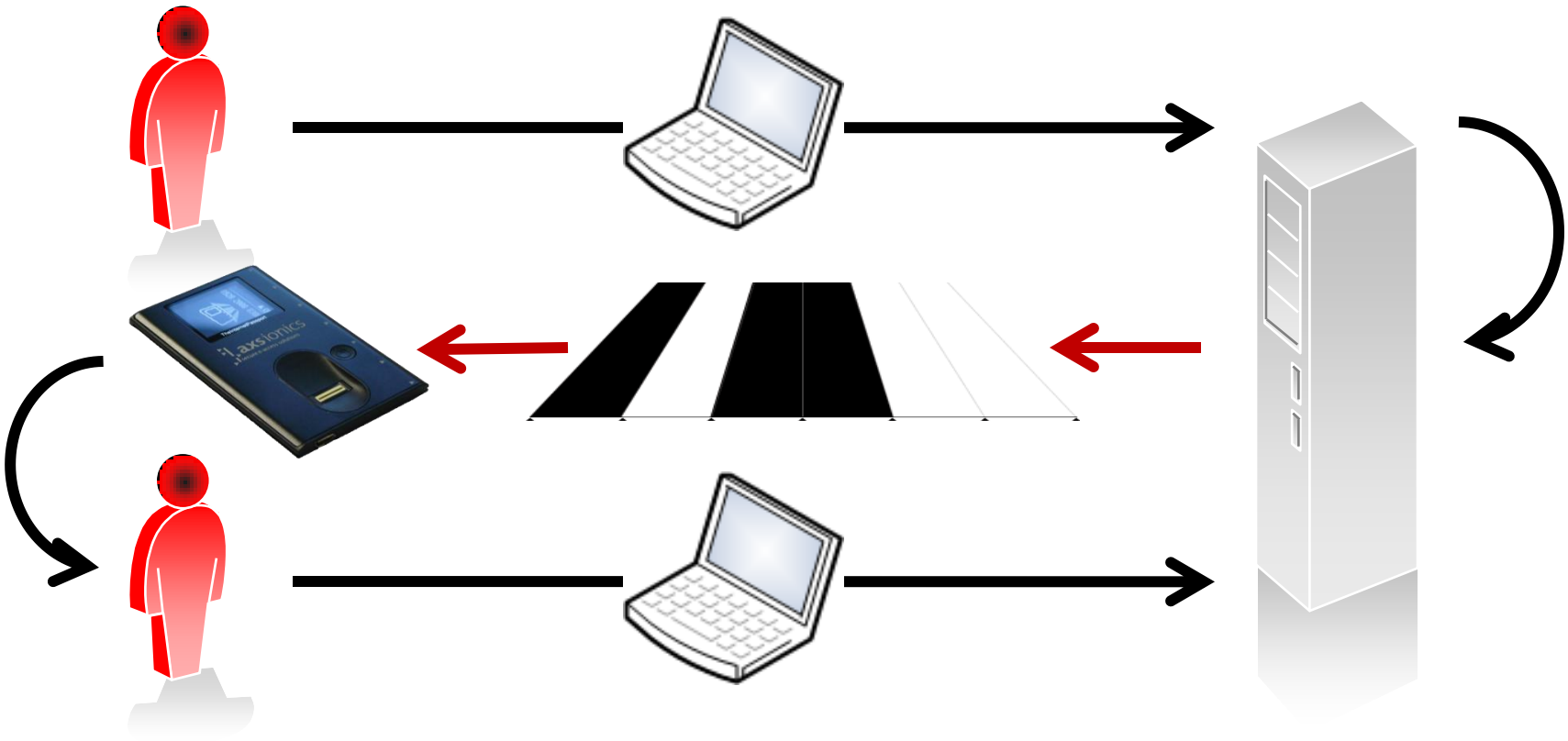

## Hardware Certificate






suisseID

# Passeport Internet



# Biométrie Match on Card

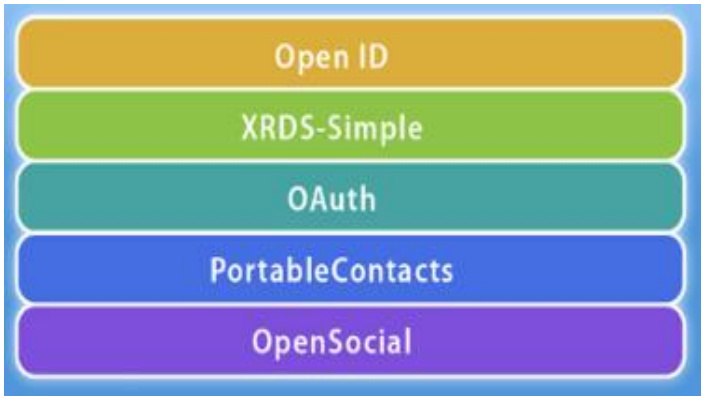
- Utilisation certificat numérique
  - PKI (X509)
- Biométrie
  - Lecture des empreintes
- Match on Card
  - Carte à puce
  - Crypto Processeur


**Retour d'expérience sur le déploiement de biométrie à grande échelle**

# La mire d'authentification biométrique


Technologie accessible à tout un chacun

- Des standards
  - Open Authentication (OATH)
    - OATH authentication algorithms
      - HOTP (HMAC Event Based)
      - OCRA (Challenge/Response)
      - TOTP (Time Based)
    - OATH Token Identifier Specification
- Solution Open Source
  - Mobile One Time Passwords
    - strong, two-factor authentication with mobile phones



# SAML vs OpenID ?

**SAML**

business + IT

**OpenID**

new age + IT

**Liberty Alliance**

IT + legal + business

**WS-Trust**

IT + IT

**Shibboleth**

academia + IT

**Cardspace**

IT + business

# OpenID & Strong Authentication: the future for Digital Native ?

"Enabling Strong Digital Identity Services for a Secure Digital World"


OpenID
Switzerland
Non-Profit Organization

Strong Authentication

# OpenID Switzerland

OpenID is a free and easy way to use a **single digital identity** across the Internet.

With one OpenID you can login to all your **favorite websites** and forget about online paperwork!


Now, you get to choose the login that's right for you. **Get an OpenID** today!

- Internet SingleSignOn
- Relatively Simple Protocol
- User-Centric Identity Management
- Internet Scalable
- Free Choice of Identity Provider
- No License Fee
- Independent of Identification Methods
- Non-Profit Organization

# Surprise! You may already have an OpenID !

Google

ook for the "Sign in with a Google Account" button or use our Google Profile URL.

YAHOO!

Look for the "Sign in with Yahoo" button.

YAHOO! JAPAN

Look for the "Yahoo! JAPAN ID でログイン" button.

LiVEJOURNAL

Enter "username.livejournal.com"

Hyves

Click the "Sign in with Hyves" button.

Blogger

nter your blog URL: blogname.blogspot.com"

flickr™

Look for the "Sign in with Yahoo" button or enter "www.flickr.com/username"

orange™

Click the "Sign in with Orange" button or enter "orange.fr"

mixi

mixi is a web service that allows users to communicate with their friends and acquaintances.

myspace

Look for the "Login with MySpaceID" button or enter "www.myspace.com/username

WordPress.com

Enter your Wordpress.com URL, for example: "username.wordpress.com"

AOL

Look for a "Sign in with AOL" button or enter "openid.aol.com/screenname"

# Other Well Known
# &
# Simple Providers

myOpenID

claimID

myID.net

VeriSign Labs
Personal Identity Portal Beta

TrustBearer openID

http://en.wikipedia.org/wiki/List_of_OpenID_providers


homepage en | de

**Login** clavid - one key, all access

**Strong Authentication**

You must sign in to authenticate to:
**https://www.clavid.com/portal/index.jsp**

Username: **smaret.clavid.ch**

Authentication type: YubiKey + Password

Password

YubiKey

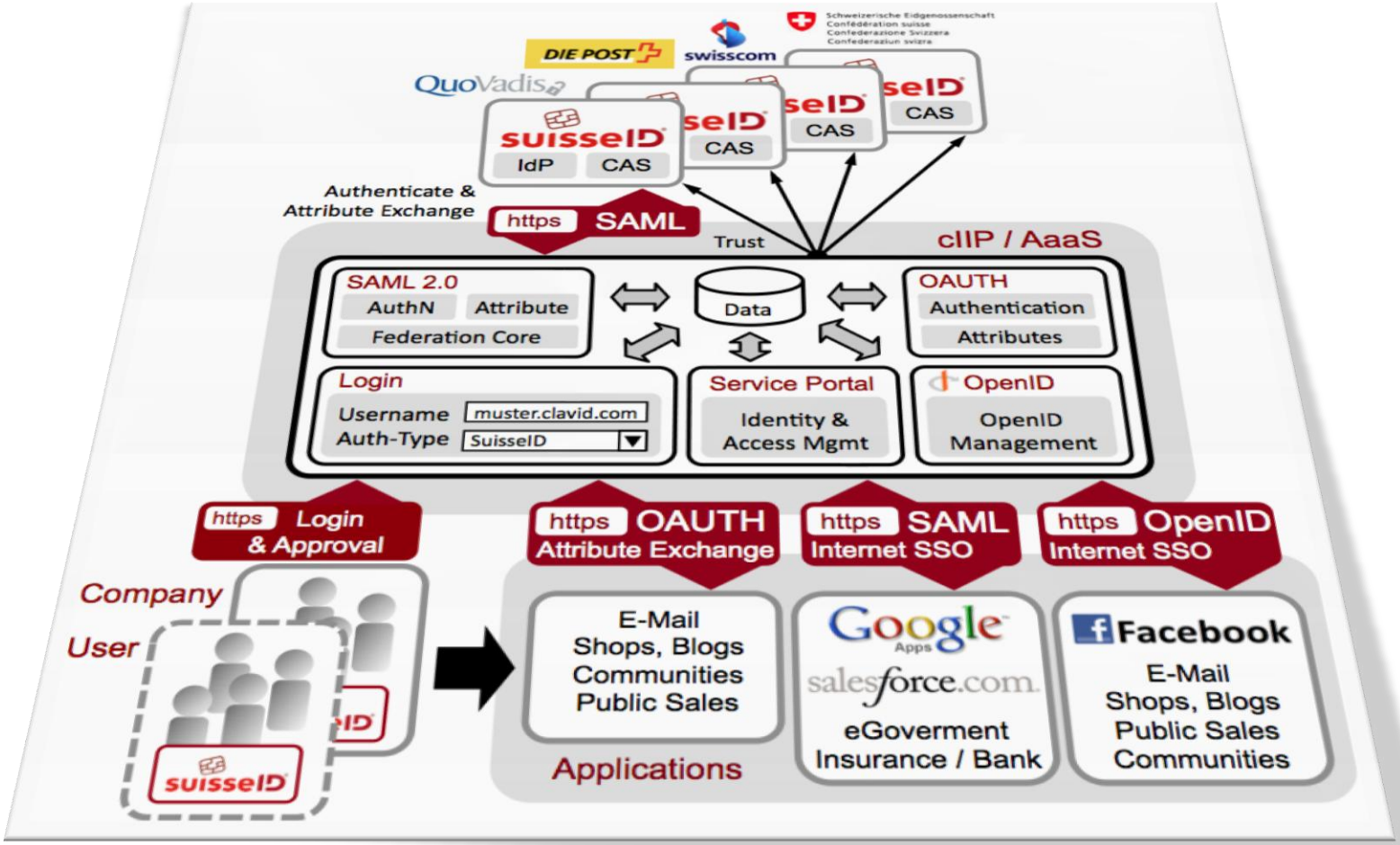
Login

I forgot my login information

Back

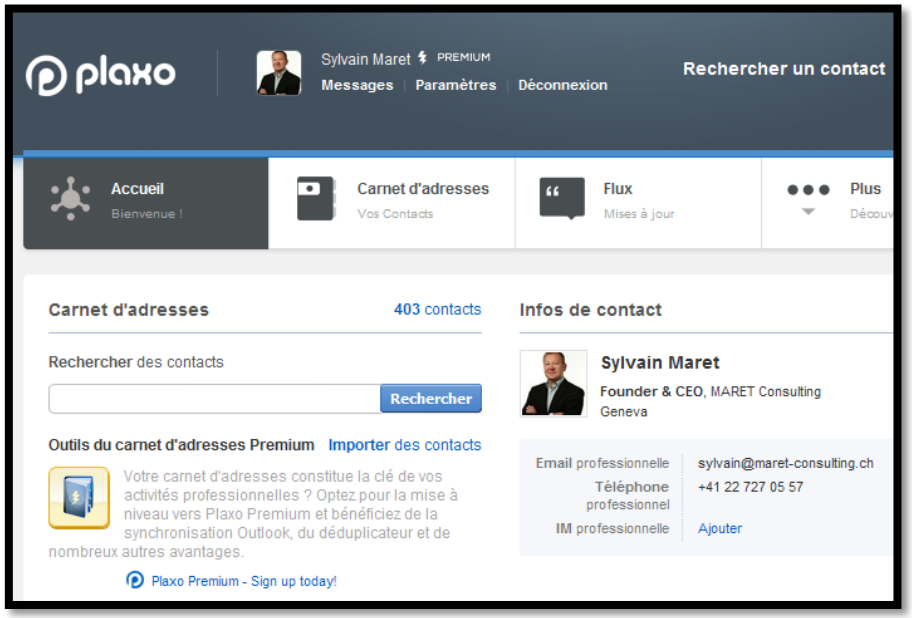
yubico
trust the net

OpenID Switzerland & SuisseID




OpenID
plaxo
Connexion à Plaxo à l'aide d'OpenID
smaret.clavid.ch
Se connecter
par ex. http://nomutilisateur.myopenid.com
Connexion à l'aide d'un Yahoo! ID
Connexion à l'aide d'un compte Google
clickpass enter


Login
clavid - one key, all access
You must sign in to authenticate to:
http://www.plaxo.com/openid?actionType=complete&r=%2F
Username:
smaret.clavid.ch
Authentication type:
YubiKey + Password
Password
YubiKey
Login
I forgot my login information
Back
yubico
trust the net
copyright © 2007-2010 clavid ag, all rights reserved.


plaxo
Sylvain Maret PREMIUM
Messages | Paramètres | Déconnexion
Rechercher un contact
Accueil
Bienvenue !
Carnet d'adresses
Vos Contacts
Flux
Mises à jour
Plus
Carnet d'adresses
403 contacts
Rechercher des contacts
Rechercher
Outils du carnet d'adresses Premium
Importer des contacts
Votre carnet d'adresses constitue la clé de vos activités professionnelles ? Optez pour la mise à niveau vers Plaxo Premium et bénéficiez de la synchronisation Outlook, du déduplicateur et de nombreux autres avantages.
Plaxo Premium - Sign up today!
Infos de contact
Sylvain Maret
Founder & CEO, MARET Consulting
Geneva
Email professionnelle
sylvain@maret-consulting.ch
Téléphone professionnel
+41 22 727 05 57
IM professionnelle
Ajouter


émergence d'une
entité juridique?

# Qui suis-je ?

- Expert en Sécurité
  - 15 ans d'expérience en Sécurité des Systèmes d'Information
  - CEO et Fondateur de MARET Consulting
  - Expert Ecole d'Ingénieurs d'Yverdon & Université de Genève
  - Délégué pour la Romandie du OpenID Switzerland
  - Co-fondateur du Geneva Application Security Forum
  - Auteur Blog: la Citadelle Electronique

- Domaine de prédilection
  - Digital Identity Security

# Quelques liens pour aller approfondir le sujet


- MARET Consulting
  - http://maret-consulting.ch/
- La Citadelle Electronique (le blog sur les identités numériques)
  - http://www.citadelle-electronique.net/
- Articles banque et finance:
  - Usurper une identité? Impossible avec la biométrie!
    - http://www.banque-finance.ch/numeros/88/59.pdf
  - Biométrie et Mobilité
    - http://www.banque-finance.ch/numeros/97/62.pdf
- Présentations publiques
  - OSSIR Paris 2009: Retour d'expérience sur le déploiement de biométrie à grande échelle
    - http://www.ossir.org/paris/supports/2009/2009-10-13/Sylvain_Maret_Biometrie.pdf
  - ISACA, Clusis: Accès à l'information : Rôles et responsabilités
    - http://blog.b3b.ch/wp-content/uploads/mise-en-oeuvre-de28099une-solution-biometrique-de28099authentification-forte.pdf


OpenID
Switzerland
Non-Profit Organization
http://www.openid.ch/