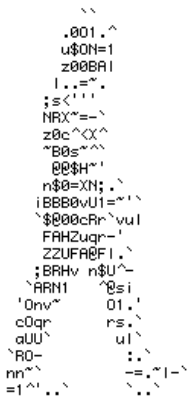
axsionics
The Internet Passport Company

AXSionics – La compagnie du passeport internet

Concept – Produit – Modèle économique

OSSIR **12 Mai 2009**

AXSionics AG, Neumarktstrasse 27, 2503 Bienne, Suisse.



Information:
Martine Reindle, Directrice des ventes
martine.reindle@axsionics.ch
téléphone: +41 79 203 6548
www.axsionics.com

axsionics
The Internet Passport Company

La compagnie AXSionics

- **S.A. Suisse, fondée en 2003, basée à Bienne**
- **Issue de l'Université de Berne pour les Sciences Appliquées**
- **13 brevets internationaux**
- **Financement privé**
- **Partenariat avec Siemens, Sun Microsystems et autres**
- **Récompensée par différents prix d'innovation technologique**

- **NOTRE MISSION: RENDRE INTERNET SÛR!**

axsionics
The Internet Passport Company

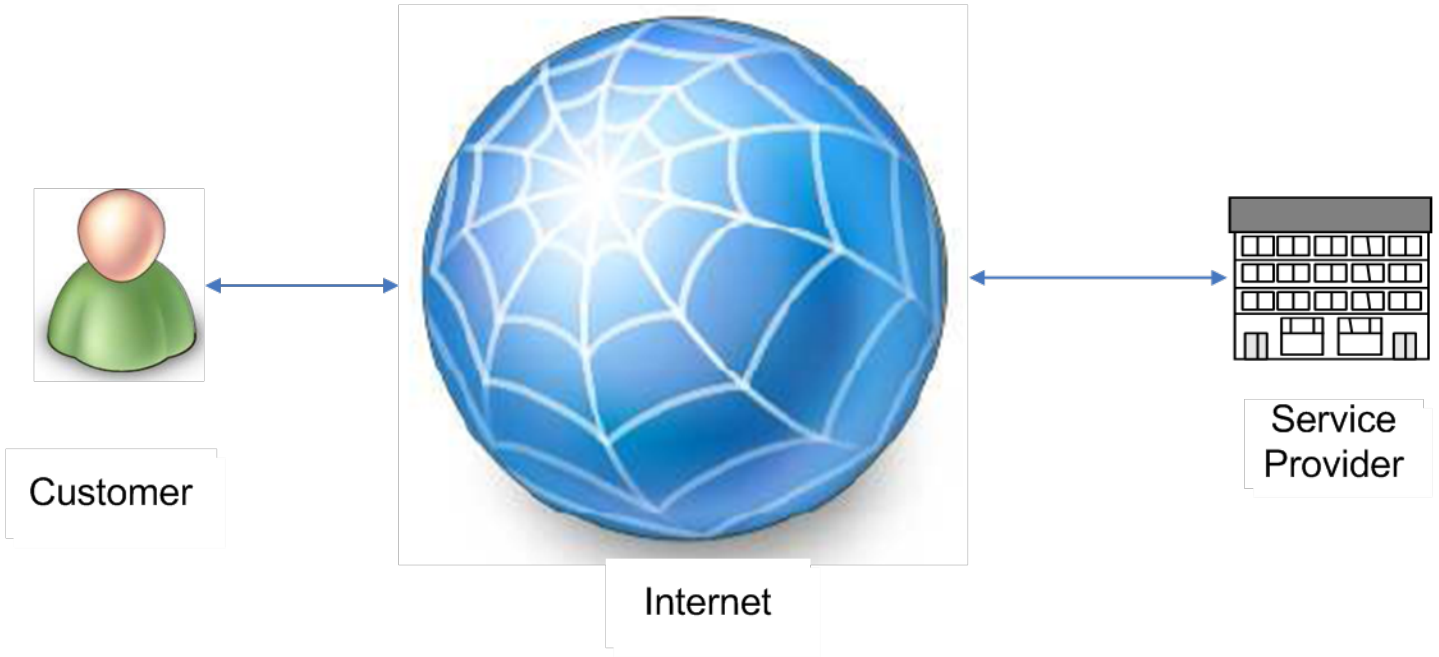
Utilisation

sur un iPhone

sur un PC

axsionics
The Internet Passport Company

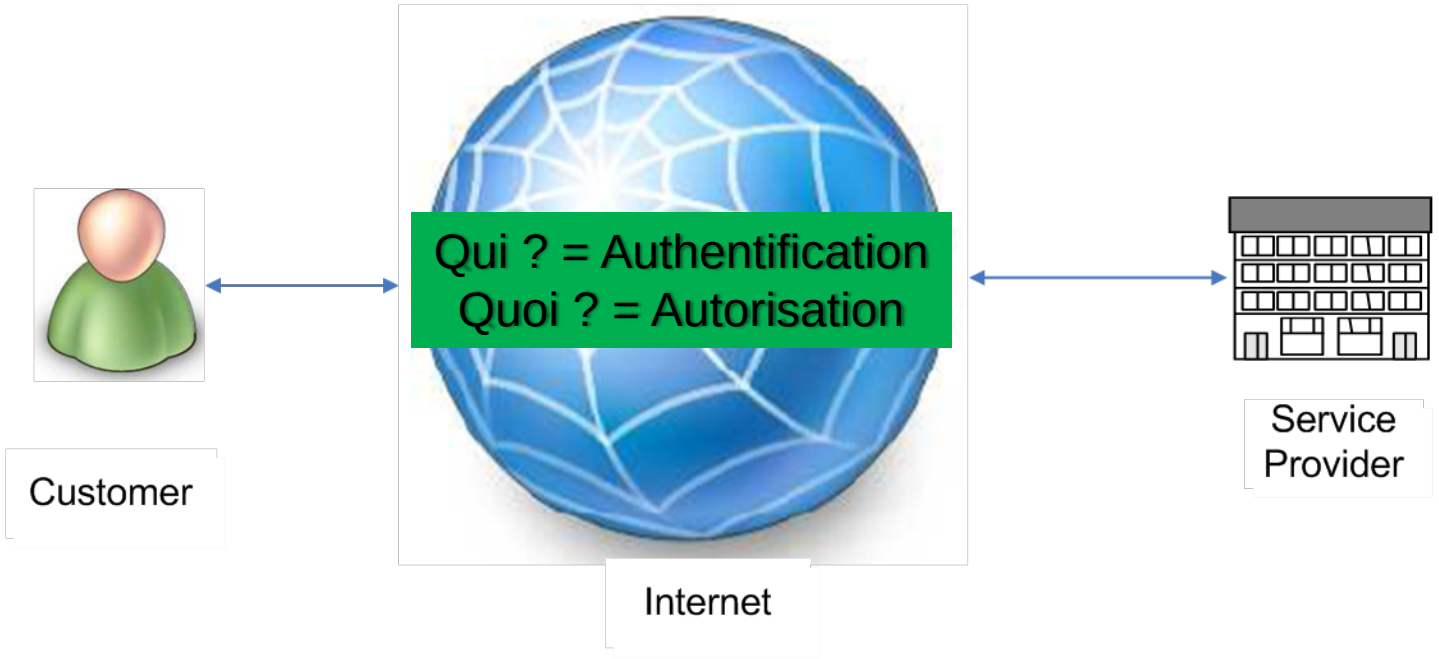
Les entreprises encouragent le e-process
→ accroitre l'efficacité des services et réduire les coûts



Peut-on faire confiance à Internet?

axsionics
The Internet Passport Company

2 questions essentielles



axsionics
The Internet Passport Company

2 questions pour examiner la sécurité d'une e-transaction

QUI?

Vérification **mutuelle** des identités (**authentification**) – être sûr que

- Le Service Provider A (Banque A) parle vraiment avec **Mr** Dubois et non **Mme** Dubois

ET

- Que Mr Dubois parle vraiment au Service Provider A (Banque A).

„What you see is what you get"

QUOI?

Vérification de l'intention (**validation**) – être sûr que

- C'est vraiment l'intention de Mr Dubois de transférer x € de son compte vers le compte xyz de Mme Dupont dans la Banque B

ou par exemple.

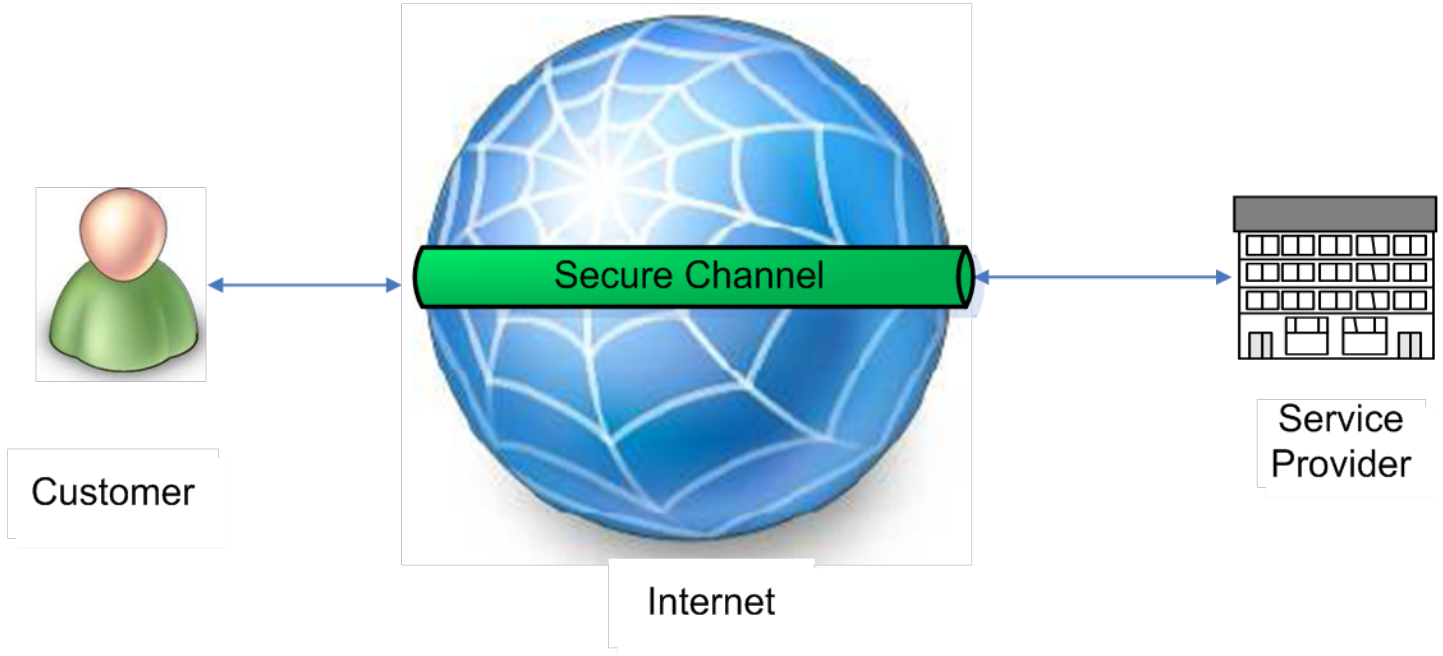
- C'est vraiment l'intention de Mr Dubois de changer les conditions de son contrat de banque en ligne

ou encore

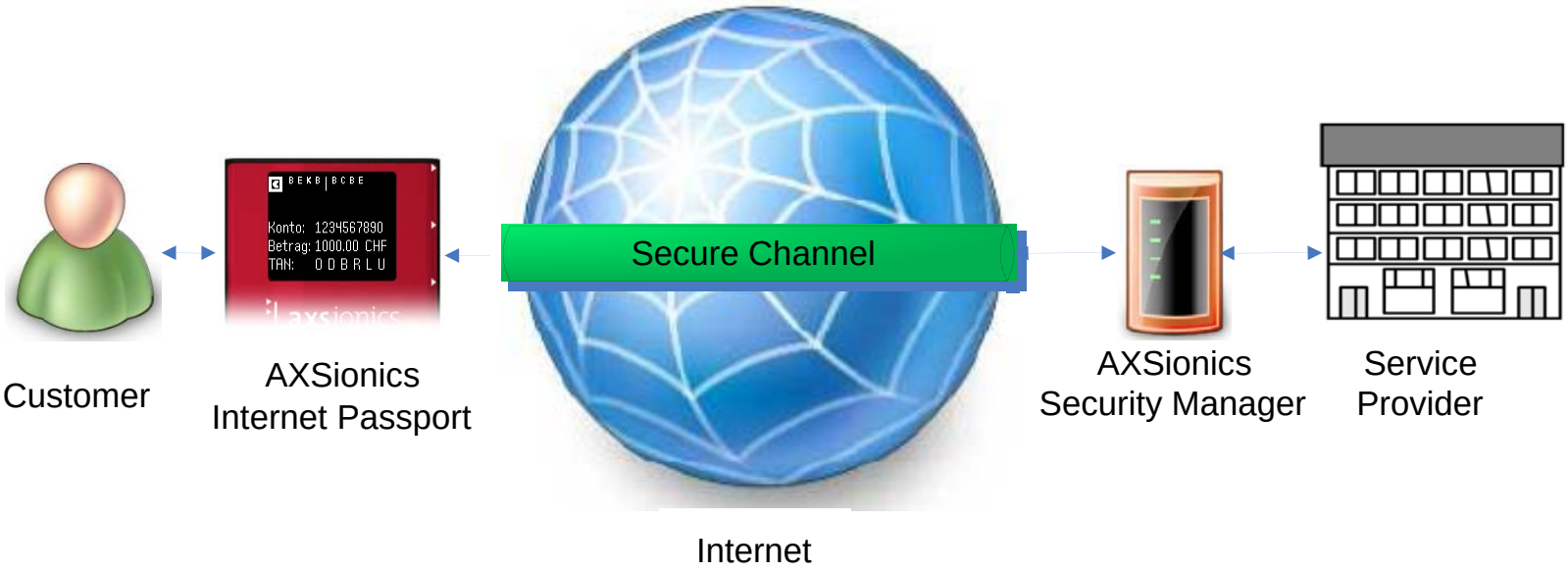
- Son intention de télécharger un document ou de l'imprimer…

axsionics
The Internet Passport Company

La solution d'AXSionics: un canal sécurisé



La solution d'AXSionicsn – les composants

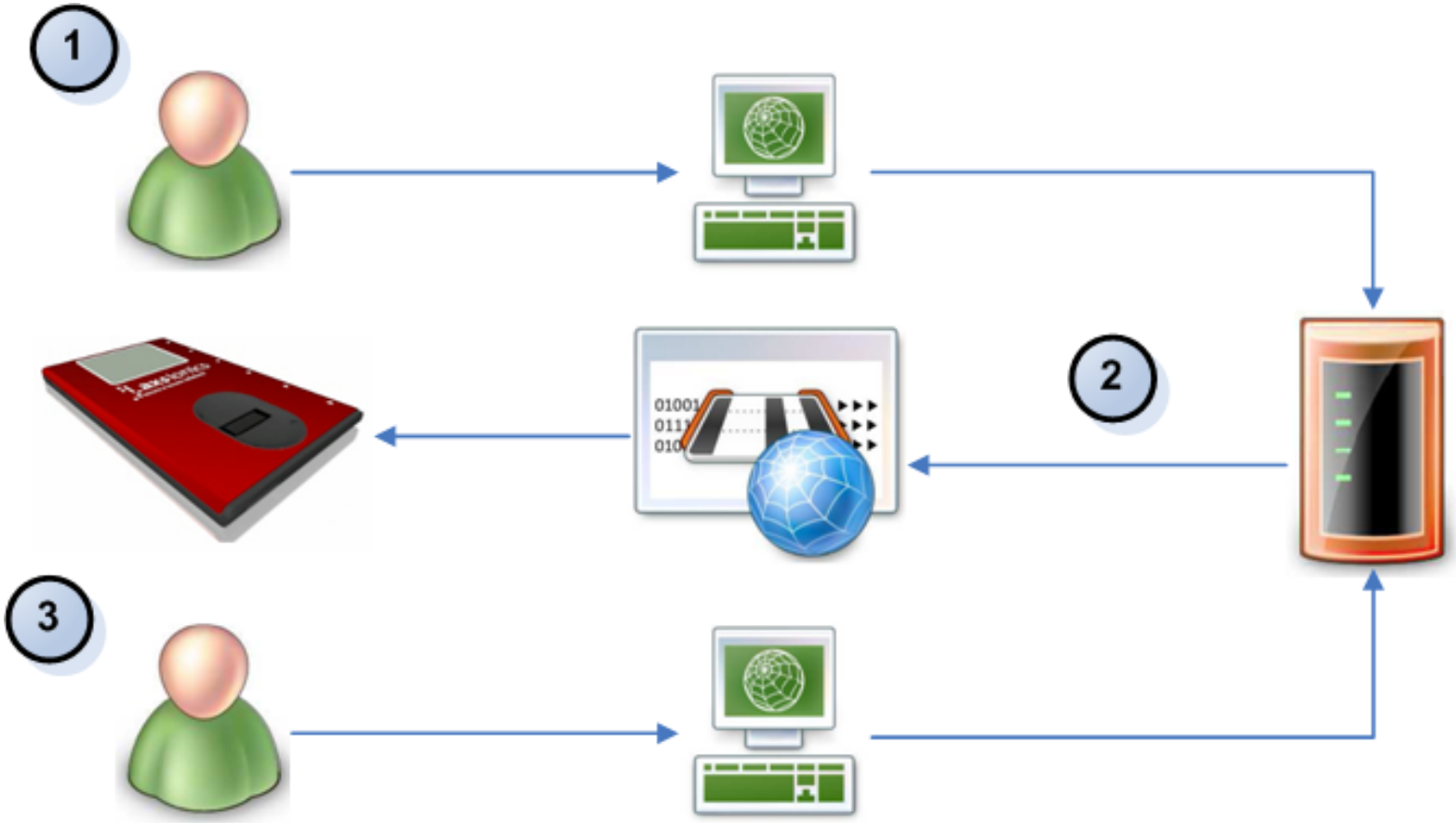


Authentification
3 facteurs

Connexion sécurisée de bout en bout

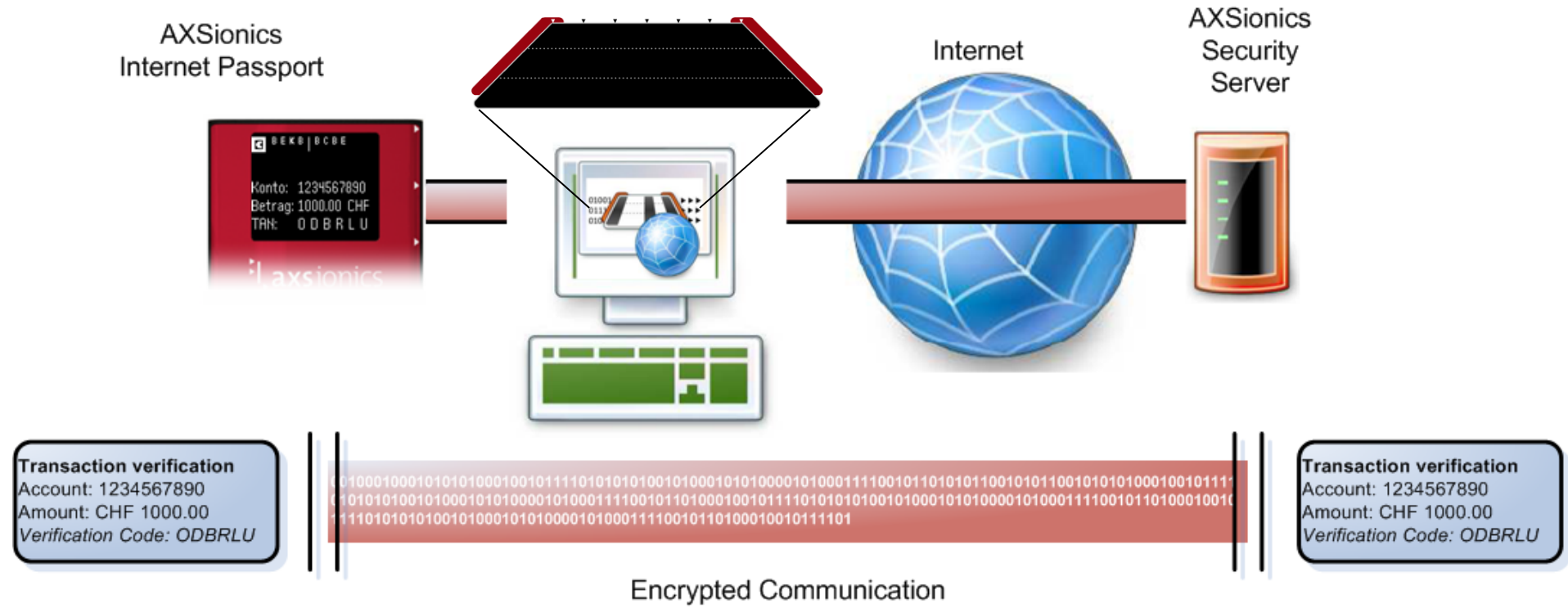
axsionics
The Internet Passport Company

AXS Principe de base: challenge response



axsionics
The Internet Passport Company

Le canal sécurisé – encrypté et toujours disponible



axsionics
The Internet Passport Company

La carte AXSionics – En pratique 1

- La carte reçue par l'utilisateur est « vide », l'utilisateur enregistre ses empreintes digitales sur sa carte qui devient dès lors utilisable que par lui

- Elle permet de travailler sans rien installer et en toute sécurité dans l'infrastructure la plus"pourrie" (Internet, PC, laptop, iPhone) car Internet et le terminal d'accès ne sont utilisés que comme transporteurs d'informations encryptées.

- Son utilisation est très simple et l'utilisateur a la certitude qu'il est en communication avec le service provider. **Elle peut contenir 112 relations**

- La carte reçoit des informations mais ne peut pas émettre = aucun risque de contaminer l'équipement de l'utilisateur

axsionics
The Internet Passport Company

La carte AXSionics – En pratique 2

- **Elle remplace UserName et Password et contient 112 relations sur une seule carte…**

- Chaque Acceptor gère ses certificats absolument indépendamment et demande les informations qu'il souhaite
  - Je veux bien donner des info personnelles pour pouvoir voter mais pas pour faire un achat sur Amazon.com).

- La solution d'AXSionics garantit la présence "physique" de l'utilisateur et de l'Acceptor / Service Provider durant toute la transaction et leur accord:
  Mr Dubois (oui), Banque A (oui), Compte de Mr Dubois (oui), montant x € (oui) pour le Commerçant B (oui) à la Banque C(oui)

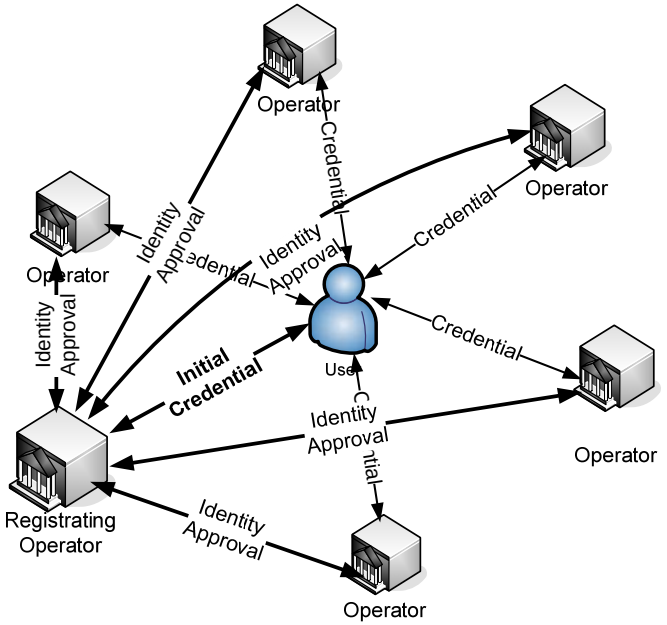
axsionics
The Internet Passport Company

La fédération centrée sur l'utilisateur (user centric)

Une solution facile à utiliser pour gérer de multiples identités

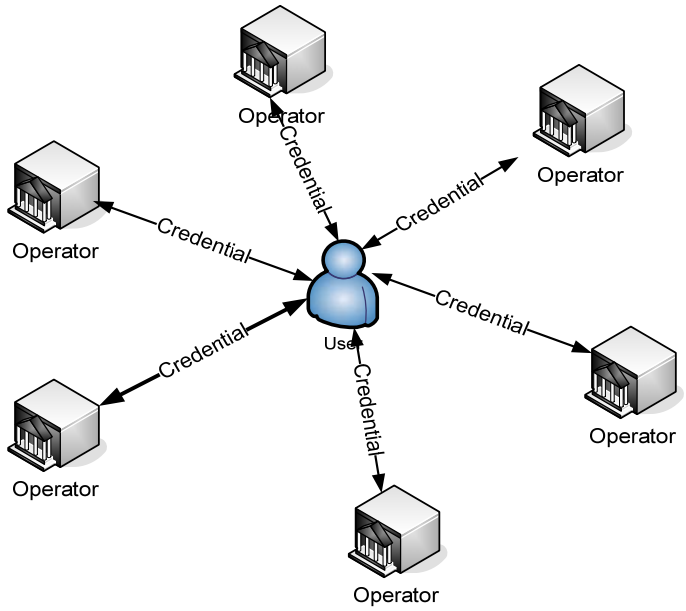
Modèle classique de fédération

- Basé sur l'Opérateur
- *Master Trust Model (PKI)*



Le modèle d'AXSionics

- Basé sur l'Utilisateur
- *Peer Trust Model*

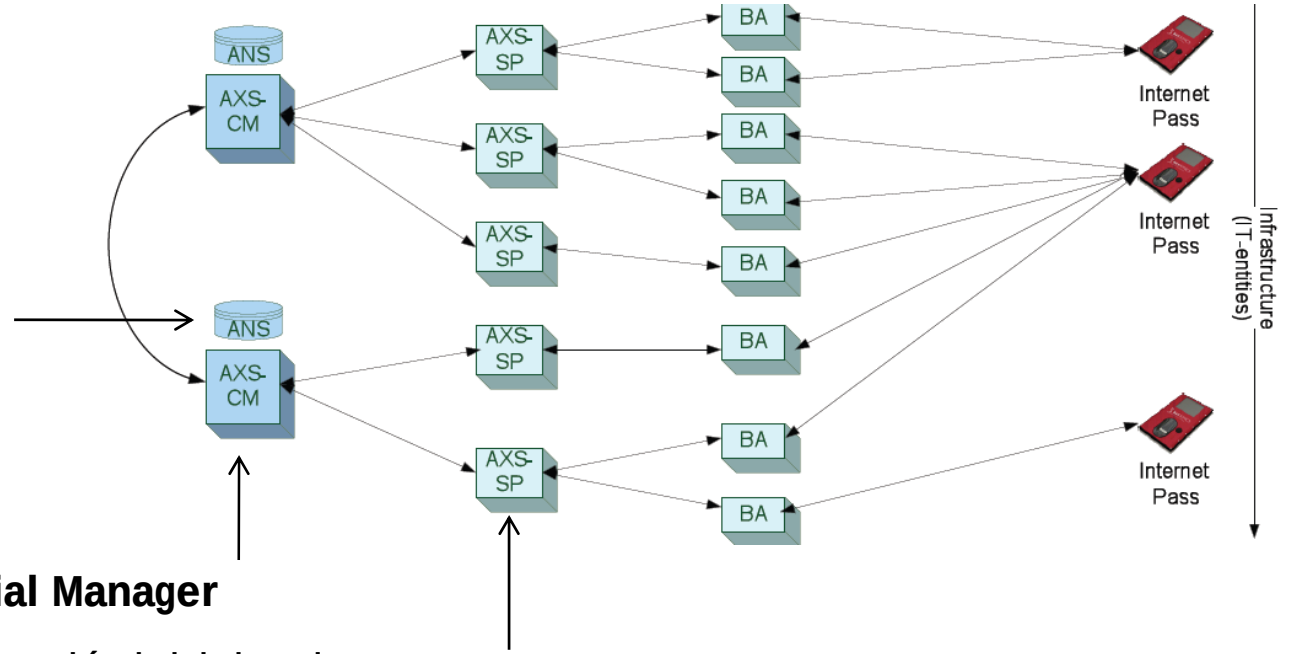


axsionics
The Internet Passport Company

L'architecture du Serveur de Sécurité d'AXSionics

AXSionics Domain Router

Système distribué pour trouver dans quel domaine un certain passeport AXSionics a été émis



AXSionics Credential Manager

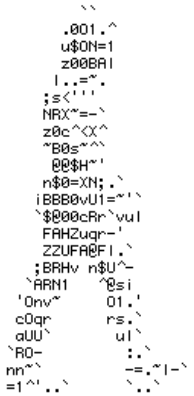
Serveur où toutes les clés initiales de tous les passeports AXSionics pour ce domaine sont hébergées, permettant d'initialiser un nouveau canal de communication sécurisé

AXSionics Security Manager

Serveur qui traite toutes les requêtes (call) et où les clés sont enregistrés et gérées

axsionics
The Internet Passport Company

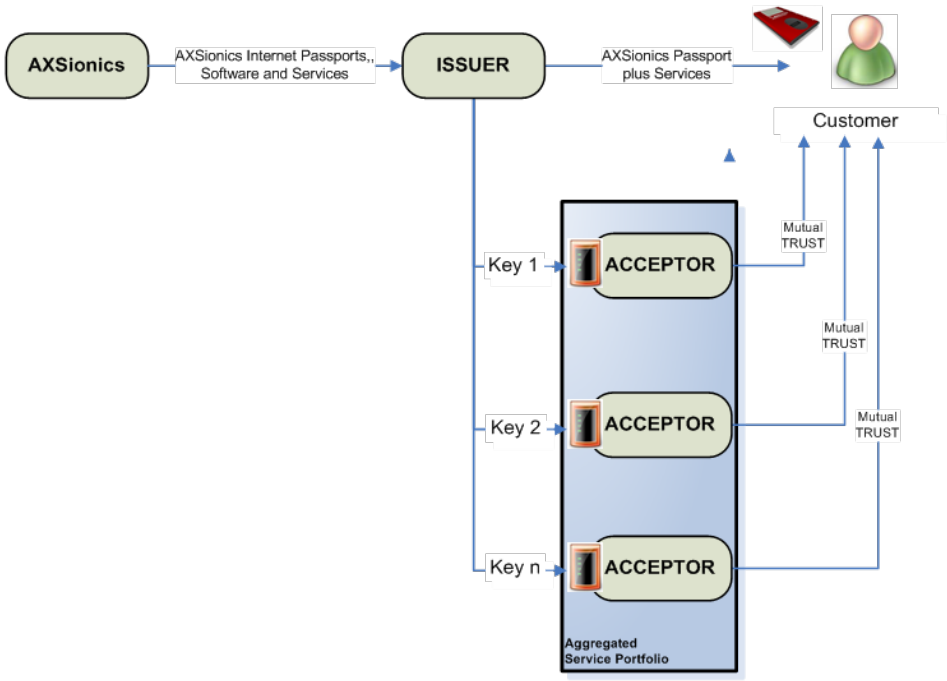
Business Model



La solution AXSionics – Vue économique

- La carte AXSionics **gère 112 relations différentes** (Acceptors/Service Providers/Applications) : **elle remplace 112 tokens** “calculette”
- Sa distribution est très économique car la carte est « sans dénomination » et « vide d’informations utilisables»
- Le meilleur Total Cost of Ownership du marché
- **La solution AXSionics est la plus économique pour toutes les parties Emetteur, Utilisateur, Acceptors indépendants et Service Providers**.

La solution AXSionics - Business Model overview



- Séparation du HW (carte) et du SW
- L'émetteur (issuer) apporte la carte à son marché et participe aux revenus générés par la carte

  Préalable – l'émetteur a une forte pénétration de son marché
- L'acceptor bénéficie d'un modèle "pay as you go" et n'a plus à distribuer, et gérer une carte de sécurité personnalisée
- Fidélisation des clients qui apprécient la simplicité d'utilisation et font désormais confiance aux transactions électroniques

axsionics
The Internet Passport Company

Applications dans différents domaines

- **E-banking et confirmation d'ordres boursiers**
- **E-payment sans lecteur de carte**
- **Sécurisation forte des accès aux informations sensibles (dossier médical, fiscal etc.)**
- **Accès à distance à applications sensibles**
- **Accès pour employés externes et temporaires**
- **E-mails sécurisés lisibles seulement par leur destinataire**
- **Vote électronique**
- **Compliance (qui fait quoi)**
- **Accès physique (salle informatique, coffres)**

axsionics
The Internet Passport Company

Applications en interne – département informatique

- **Sécurisation forte des accès aux données sensibles, local ou à distance**
- **Compliance (qui a fait quoi?)**
- **Confirmation d'ordres (j'ai bien lu et j'accepte)**
- **Pseudo single sign on: un seul token et une seule manière d'accéder à toutes les applications autorisées (autorisation et révocation facile)**
- **Distribution de passwords**
- **E-mails sécurisés lisibles seulement par leur destinataire**
- **Accès physique à certains locaux**

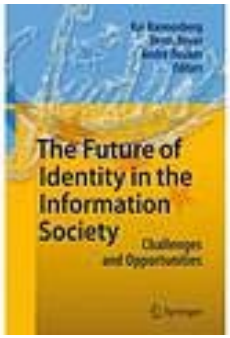
N.B. Informations biométriques sous le contrôle du propriétaire de la carte uniquement

axsionics
The Internet Passport Company

Sources de réflexion et initiatives

- Depuis sa création AXSionics appartient au consortium universitaire européen Fidis **www.fidis.net**

Publication interessante
http://fidis.net/fileadmin/fidis/deliverables/booklet2/Fidis_booklet_web.pdf



Prochaine publication:
The future of identity in the information society

- AXSionics soutient l'initiative OpenID et est membre de son chapitre suisse **www.clavid.com**

OpenID Switzerland

clavid
one key, all access

axsionics
The Internet Passport Company

AXSionics concurrence – comparaison 1

Le Passeport Internet d'AXSionics fonctionne comme

un passeport: authentifie son propriétaire

un notaire: authentifie les 2 parties et valide une transaction

La concurrence propose une des 2 fonctions, pas les 2

Le Passeport d'AXSionics ne nécessite pas d'installation sur le terminal de son utilisateur, n'a pas de connexion physique, peut agréger de multiple "credentials"…

axsionics
The Internet Passport Company

AXSionics concurrence - comparaison 2

AXSionics – concurrence en tant que passeport:

- **Challenge response (ex. token de type Vasco, Xiring)**
- **One time password (ex. token de type RSA):**

- **Pas plus de 2 facteurs:**
  - L'utilisateur physique n'est pas authentifié
  - L'authenticité du service demandé n'est pas prouvée dans tous les cas (pas exempt de Man In The Middle)
  - Le code PIN reste le même (on peut l'observer)
  - Un seul service: un token par banque/institution
  - Nécessite parfois une personnalisation avant distribution
  - Affichage fixe (en général numérique et sur une seule ligne)

axsionics
The Internet Passport Company

AXSionics concurrence – comparaison 3

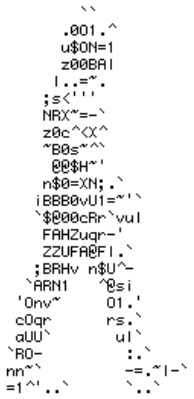
AXSionics – concurrence en tant que notaire

- **Hardened USB tokens (ex. IBM ZTIC)**
- **Smart cards avec lecteur connecté**

- **Mobilité limitée:**
  - Une connexion physique avec le PC est toujours nécessaire
  - Drivers locaux et maintenance du logiciel - sûre?
  - Ports USB pas toujours disponibles
  - Affichage limité
  - Pas toujours trusted display (exception IBM ZTIC)
  - Pas d'agrégation de services (1 service – 1 token par banque/institution)
  - Peut nécessiter une personnalisation avant distribution
  - L'acte "intentionnel" de l'utilisateur n'est pas clairement marqué

axsionics
The Internet Passport Company

Résumé Technique



axsionics
The Internet Passport Company

Le Passeport Internet: la taille d'une carte de crédit!

Un écran graphique qui affiche le logo et jusqu'à 4 lignes de 18 caractères

6 senseurs optiques, dans l'épaisseur de la carte, pour capturer les "images flickering" affichées sur l'écran du PC

Un scanner d'empreintes digitales pour une authentification biométrique et/ou avec un code PIN

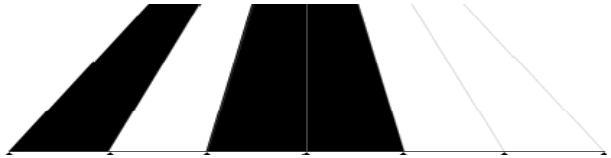
Microprocesseur de sécurité EAL4+/CC qui stocke les éléments biométriques et les clés

Connexion USB pour recharger la batterie

axsionics
The Internet Passport Company

Les composants de la solution AXSionics

AXS-InternetPassport™
une carte personnelle



Le générateur de “Flicker code”
un logiciel qui convertit des données encryptées en une image animée

La plateforme AXS ou le Security Manager:
un serveur qui encrypte les messages et gère les certificats

axsionics
The Internet Passport Company

FLICKER CODE

Le Flicker code fonctionne avec différentes technologies/plug-ins de tout web browser:

- Java
- Adobe Flash
- JavaScript / Active Scripting
- Animated GIF

axsionics
The Internet Passport Company

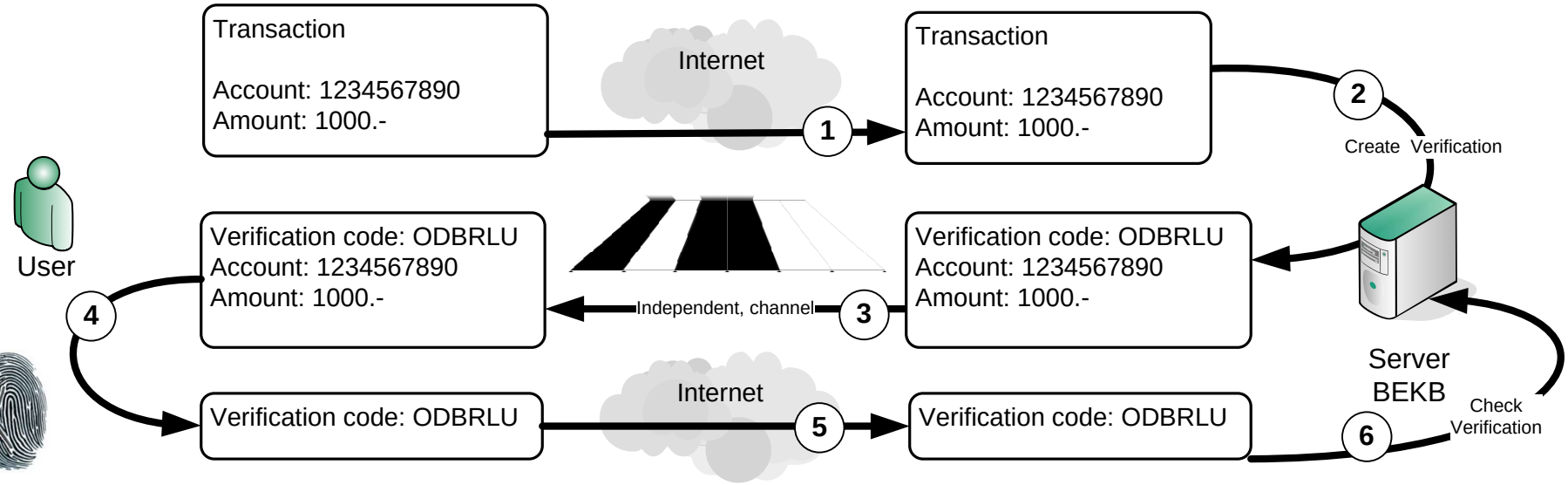
Fonctions et principes de la solution

- **Trusted display:** les détails de la transaction proposée sont encryptés par 1 clé partagée (origine et destination) et seulement affichés après authentification réussie du propriétaire de la carte

- ✓ **Authenticité**, les détails de la transaction ne peuvent être envoyés que par un émetteur authentifié préalablement et identifié par son logo
- ✓ **Integrité / Discretion / Confidentialité**, les détails de la transaction sont envoyés encryptés, lisibles seulement par le destinataire
- ✓ **Fraicheur**, la transaction ne peut pas être rejouée
- **Canal de communication:** sous le contrôle exclusif des 2 parties (jamais de tiers)

axsionics
The Internet Passport Company

Work flow pour internet banking (ex. Banque Cantonale de Berne)



axsionics
The Internet Passport Company

Contenu d'une image flickering (simulation)

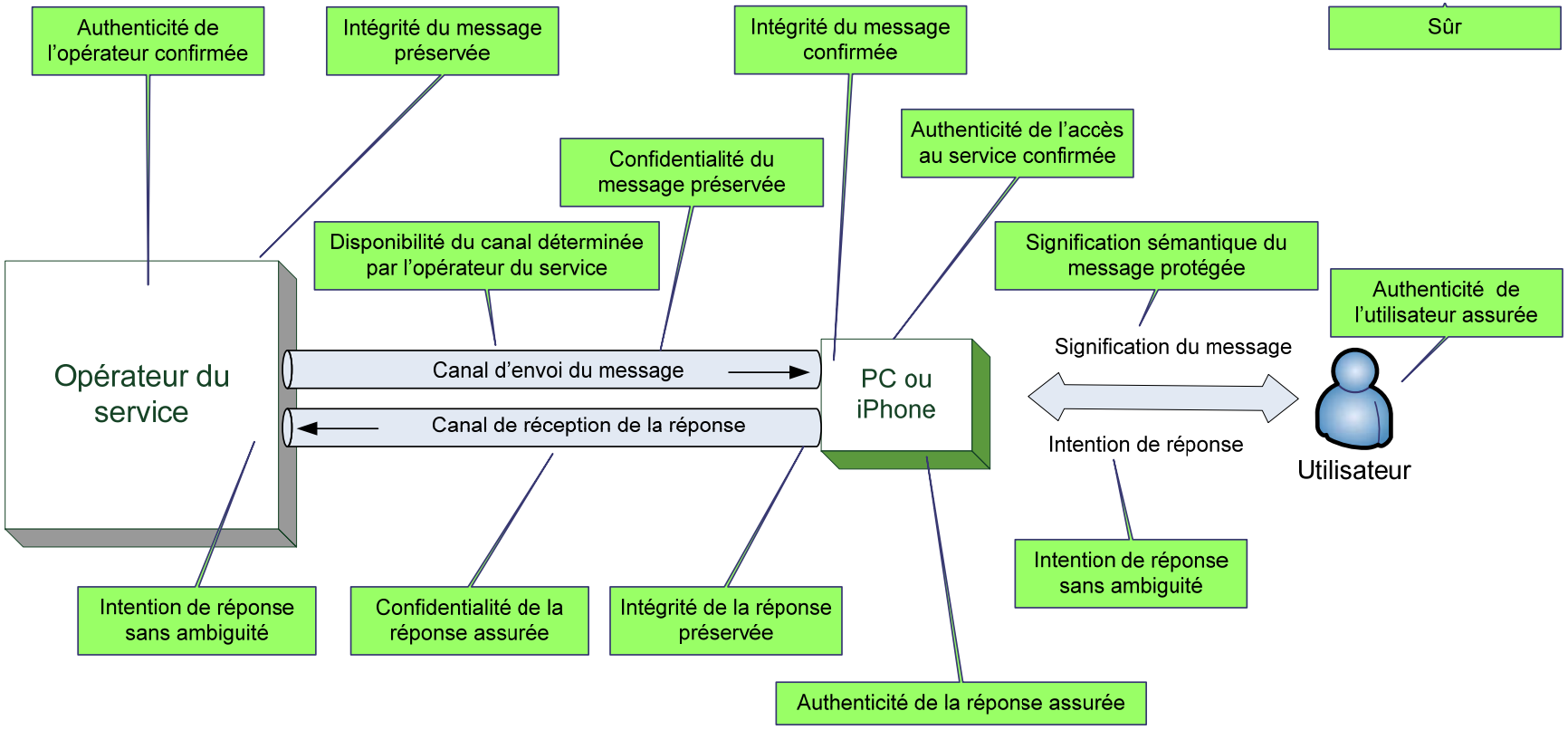
- Datum: 12. 11. 2007**\n**Konto: 1-23104-3**\n**Betrag:123.50 CHF**\n**TAN**$c**
- Output du server avant conversion:
  - 0018081c2c0c2c002418200020002c1c3a0d3f073c0a27112a0c3c1431043b00180c1f2c0a3d023c1b3809281e2d0f361636103905321d3a1c2b122f1538001c08173e0c210737133d03381130003b123b0c381e3c013b0227043d0c27001c0c143e063c1f24182010271f27172618301a381e351b210c340238033c00180a143a053905341b3517371a23133516291f38183b1a2b04341d3f003200180e1d3b152518271d35053b163315260d2d1f2e1c241a340f291b2c132e001d0b162216240933182619270520041d0e103a002d0e2b1623113c192602220a2601330b2316351539062 80d24
- L'instruction "**$c**" demande de produire un One Time Password alphanumérique à 6 caractères
- Contient l'adresse du canal, compteur de session, authentification de l'émetteur (affiche la clé graphique qui correspond au logo), le niveau d'authentification, le message et le MAC

Authentification visuelle du service provider

Un code sécurisé par cryptographie active le branding (ici le logo de la banque cantonale de Berne) qui apparait sur le passeport internet de l'utilisateur lorsqu'il est en connexion avec cette banque.

axsionics
The Internet Passport Company

Solution AXSionics - Gestion des risques



axsionics
The Internet Passport Company

Key length (AXS choice highlighted)

Secure until	Security (bits)	Symmetric	DLOG		EC	HASH	
			Field size	Sub field		Signature	HMAC
1982	56	56	640	112	112	SHA-1	SHA-1
1992	64	64	816	128	128	SHA-1	SHA-1
2012	80	80	1248	160	160	SHA-224	SHA-1
2030	112	112	2432	224	224	SHA-224	SHA-1
>2030	**128**	**128**	**3248**	**256**	**256**	**SHA-256**	**SHA-1**
>2050	160	160	5312	320	320	SHA-384	SHA-224
?	192	192	7936	384	384	SHA-384	SHA-224
?	**256**	**256**	**15424**	**512**	**512**	**SHA-512**	**SHA-256**

axsionics
The Internet Passport Company

Security requests and Crypto - Primitives

Requests

- Secrecy of message → Encryption of payload
- Authentication of sender (AuXX) → Verification of sender identity (knowledge of credential)
- Authentication of receiver (Token) → Verification of token credential (identity)
- Integrity of message → Verification of footprint (checksum)
- Non-Repudiation → Signature code application (optional)
- Provability → Certificates for each token, message log

Crypto technology (similar to Suite B, NSA recommendation)

- Key length equivalent to 2^{255} – complexity for ”brute force” attacks
- Symmetric cipher: AES (128)
- Hash, MAC: SHA 256 / SHA 256, HMAC (RFC2104)
- KDF: KDF1 (IEEE1363:2000)
- Asymmetric cipher: (future impl.) ECDH (NIST 256), (ECDSA)

axsionics
The Internet Passport Company

Crypto primitives and Crypto schemes

For the BAC Protocol the following "crypto primitives" with key sizes, at least at the length recommended as Suite B from NSA and declared as "state of the art" by the ECRYPT Consortiums (IST-2002-507932)

- AES 128 as block cipher in the CTR mode (FIPS 197; RFC3686-IPSEC ESP)
- SHA-256 as hash function for HMAC (NIST FIPS 180-2; RFC 2104, RFC 3174)
- SHA-256 as hash function for digital signatures (FIPS 180-2)
- Elliptic curve with a 256-bit prime module for digital signatures (FIPS-186-2; ANSI X9.62))
- X509.3 Certificate with signature Suite (ECDSA ,SHA-1), (RFC 3280,RFC3279)
- The used key length are based on the recommendations for the amount of security bits by NIST, NSA, ECRYPT and others **(see http://keylength.com)**

Exemple votation 15 questions

Identifiant du vote: 090312HJUGGV

Je suis d'accord avec ces choix = ok:
Je saisis C0B1DU sur le clavier de mon PC

Questions 1 à 15

- **J'ai répondu aux questions suivantes**

Question 1 =yes,

Question 2 = no

Question 3 = no

Question 4 = no

Question 5 = Abstention

Question 6 = no

etc..