

**NEXIMS** présente

# L'authentification forte

Un enjeu majeur pour tous les secteurs de l'économie.

Comment le téléphone mobile  
devient une clé de sécurité incontournable.

## Programme de la matinée :

- NEXIMS Les nouveaux enjeux de l'authentification forte
- SFR Fraude et ROI de l'authentification forte
- AESMA Sécurité des réseaux de télécommunication
- PERICLES Enjeux et pratiques de l'authentification forte pour les banques, les compagnies d'assurances, les acteurs du e-Commerce
- KEYNECTIS Signature électronique et dématérialisation
- DGME Enjeux de l'authentification forte dans l'usage des services publics en ligne

Echanges & Questions

# Présentation des nouveaux enjeux de l'authentification forte

David Bozio-Made

Président, NEXIMS France

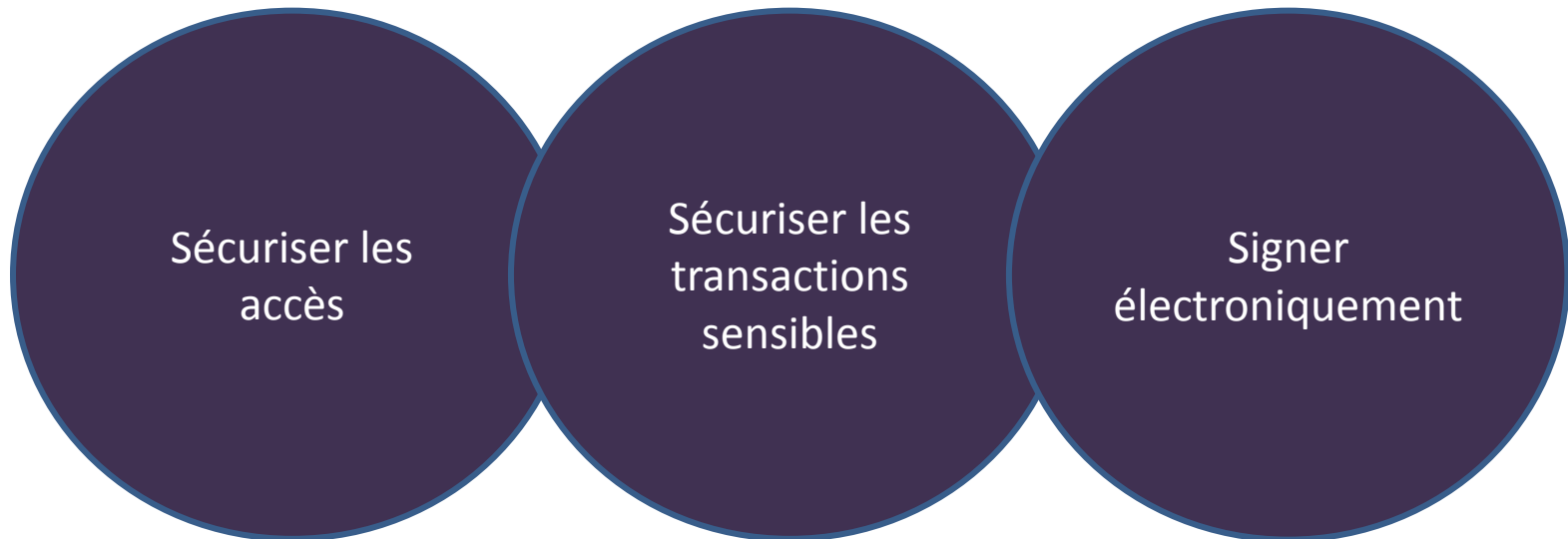
## Authentification forte... Une sécurité **pour qui / pour quoi ?**

### Pour les **EDITEURS DE SERVICES EN LIGNE** :

Lutter contre l'usurpation d'identité  
Proposer de nouveaux services  
Dématiser en toute sécurité



Diminuer les coûts de la fraude  
Générer de nouveaux revenus  
Responsabiliser les clients



## Authentification forte... Une sécurité **pour qui / pour quoi** ?

### Pour les **UTILISATEURS DE SERVICES EN LIGNE** :

Gérer ses données en toute sécurité

Gérer son argent en toute sécurité

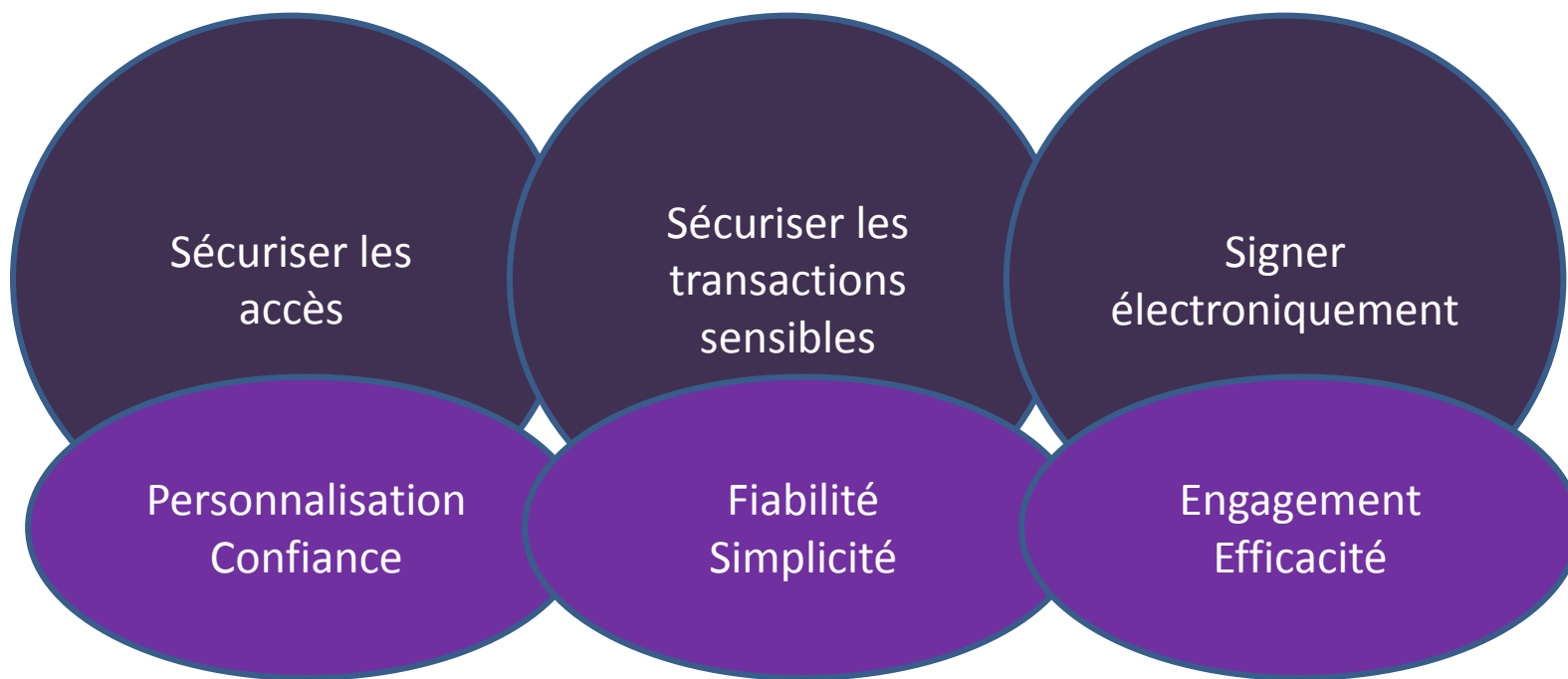
Disposer de nouveaux services



Vivre la sécurité sans contrainte

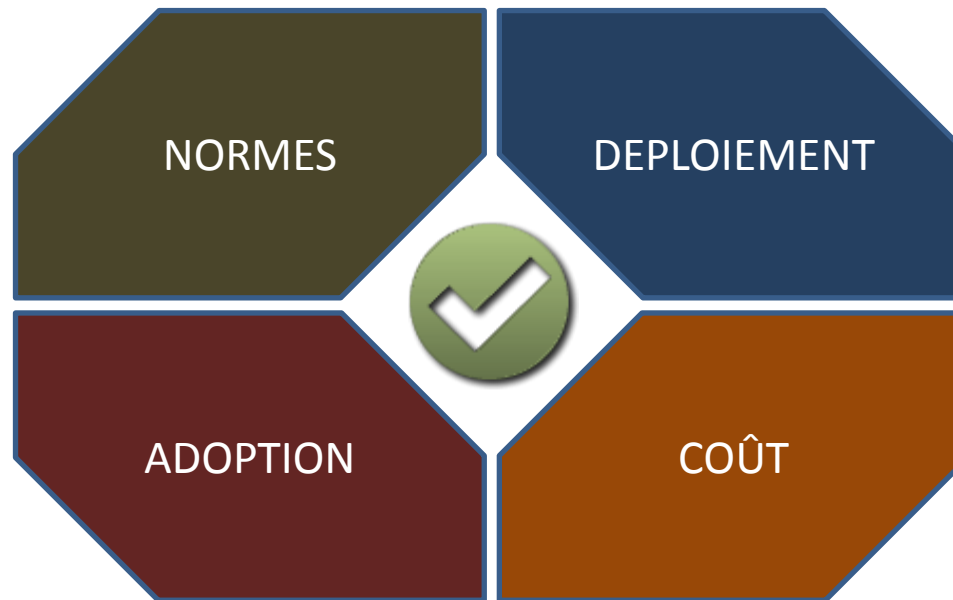
Accélérer ses démarches personnelles

Réduire et simplifier les papiers



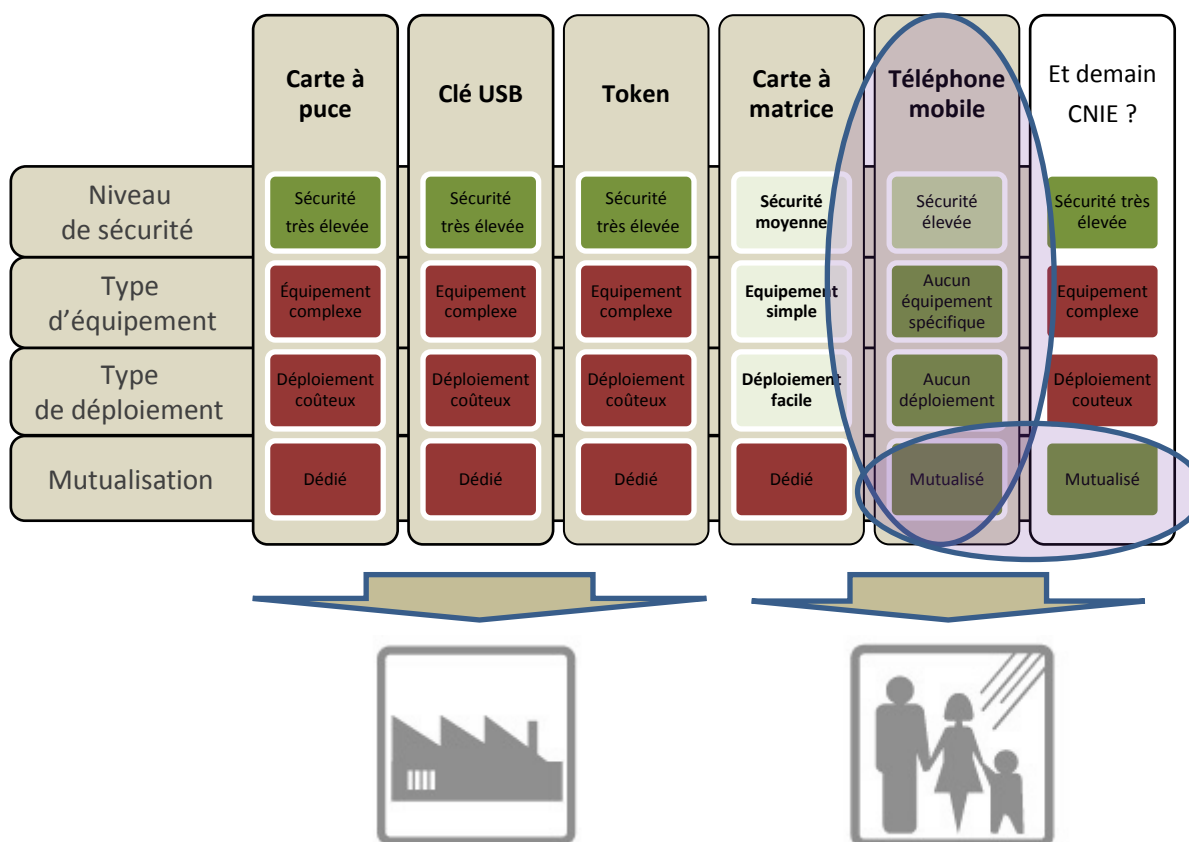
## Authentification forte... Une sécurité **pour qui / pour quoi** ?

Les 4 CLES de REUSSITE de l'authentification forte :



# Authentification forte... Une sécurité **pour qui / pour quoi** ?

## Les différents SUPPORTS de l'authentification forte :



# Authentification forte... Une sécurité **pour quels usages** ?

Web grand public  
Portails opérateurs



Transactions sécurisées  
Banque en ligne



Signature électronique  
Contrats en ligne



Poste de travail distant  
Extranet



Transactions au guichet  
Paiement de salaires



Services publics en ligne  
e-Gouvernement



Transactions entre utilisateurs  
Cash collect, transfert



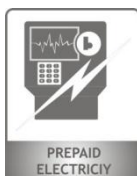
Paris et jeux en ligne  
Jeux d'argent



Transports & Loisirs  
e-Ticket



Rechargement / Paiement  
e-Load, e-Wallet



SaaS & Cloud computing  
Accès sécurisé



SSO, fédération d'identité  
Webmail

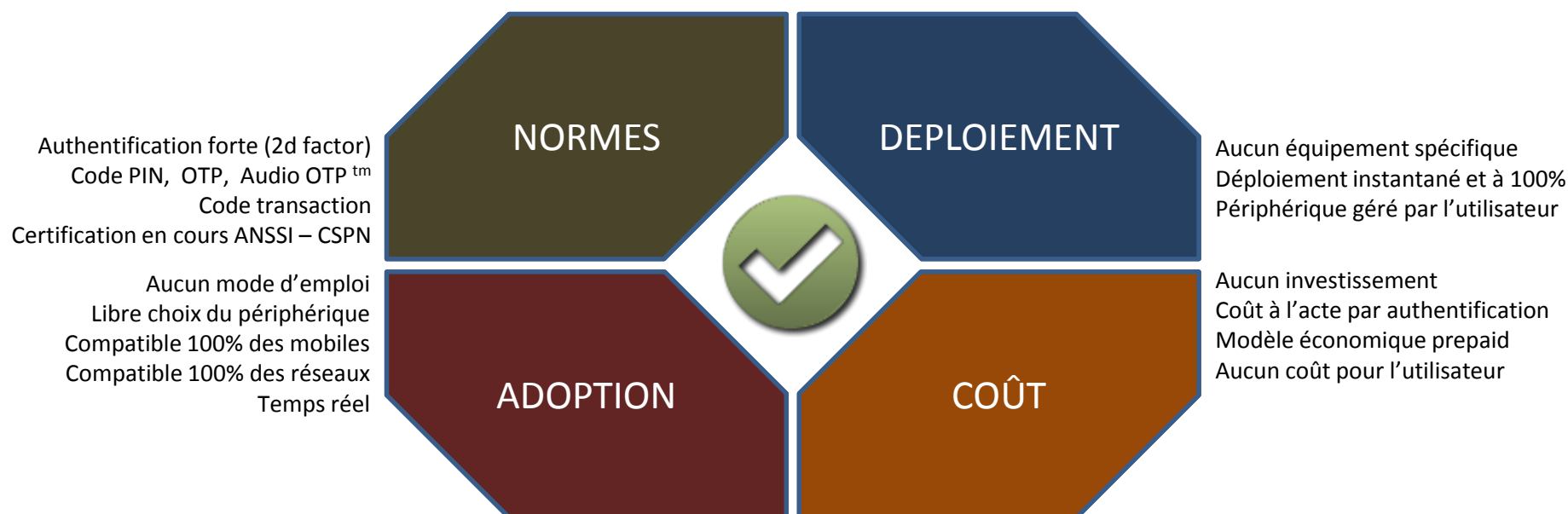


# Authentification forte par téléphone mobile : CertifiCall



**CertifiCall** transforme le **téléphone mobile** de l'utilisateur en **clé de sécurité**

- En phase avec les clés de réussite dans la mise en œuvre de l'authentification forte



# Authentification forte par téléphone mobile : CertifiCall



**CertifiCall** transforme le **téléphone mobile** de l'utilisateur en **clé de sécurité**

- En phase avec les clés de réussite dans la mise en œuvre de l'authentification forte
- Scénario adapté au niveau de sécurité recherché et au contexte utilisateur

## Etape 1 Identification

- Saisie login / mot de passe
- Vérification du profil utilisateur, récupération des infos

## Etape 2 Authentification **CertifiCall**

- **CertifiCall** appelle immédiatement l'utilisateur
- Echange des informations de sécurité (PIN, OTP, ...)
- Fin de la procédure d'authentification

## Etape 3 Certification

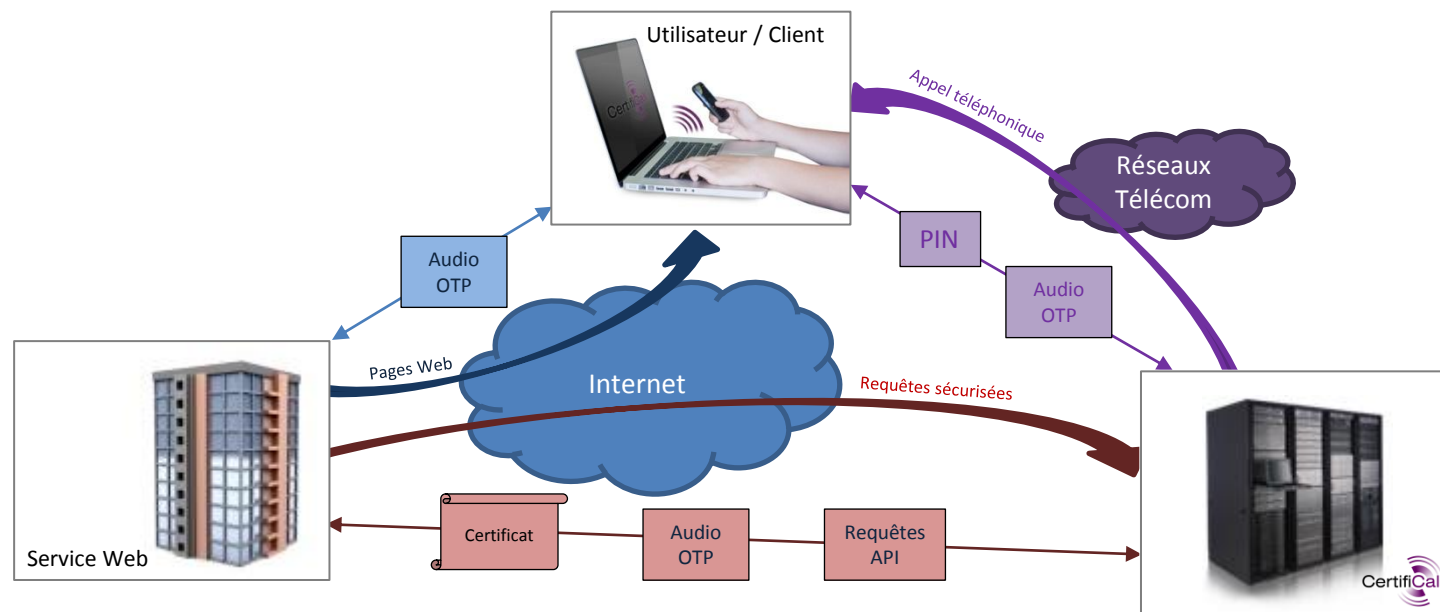
- **CertifiCall** génère le certificat de cette authentification
- Envoi du certificat à l'éditeur du service

# Authentification forte par téléphone mobile : CertifiCall



**CertifiCall** transforme le **téléphone mobile** de l'utilisateur en **clé de sécurité**

- En phase avec les clés de réussite dans la mise en œuvre de l'authentification forte
- Scénario adapté au niveau de sécurité recherché et au contexte utilisateur
- Intégration normalisée, solution haute disponibilité en mode SaaS, couverture mondiale

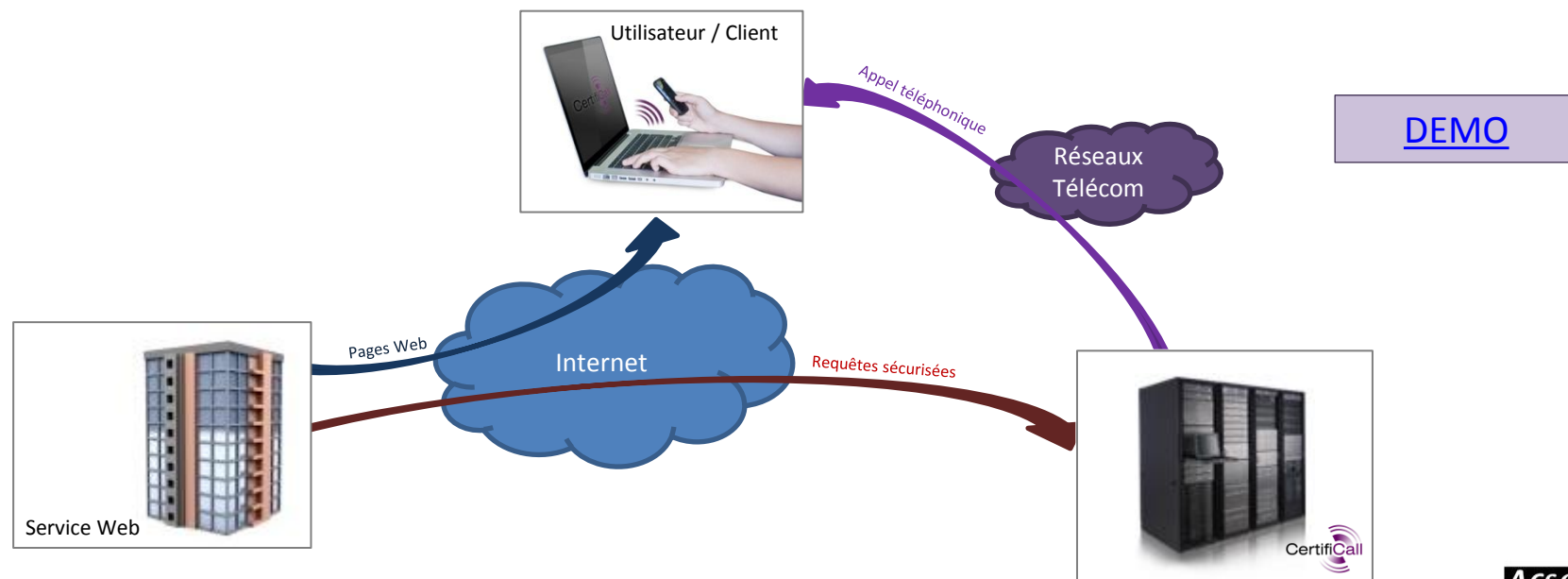


# Authentification forte par téléphone mobile : CertifiCall



**CertifiCall** transforme le **téléphone mobile** de l'utilisateur en **clé de sécurité**

- En phase avec les clés de réussite dans la mise en œuvre de l'authentification forte
- Scénario adapté au niveau de sécurité recherché et au contexte utilisateur
- Intégration normalisée, solution haute disponibilité en mode SaaS, couverture mondiale



## Merci



**David Bozio-Made**

Président, **NEXIMS** France

[dbozio@nexims.com](mailto:dbozio@nexims.com)

Tel : +33 1 7431 1170

Cel : +33 6 6200 9412

# Fraude et ROI de l'authentification forte

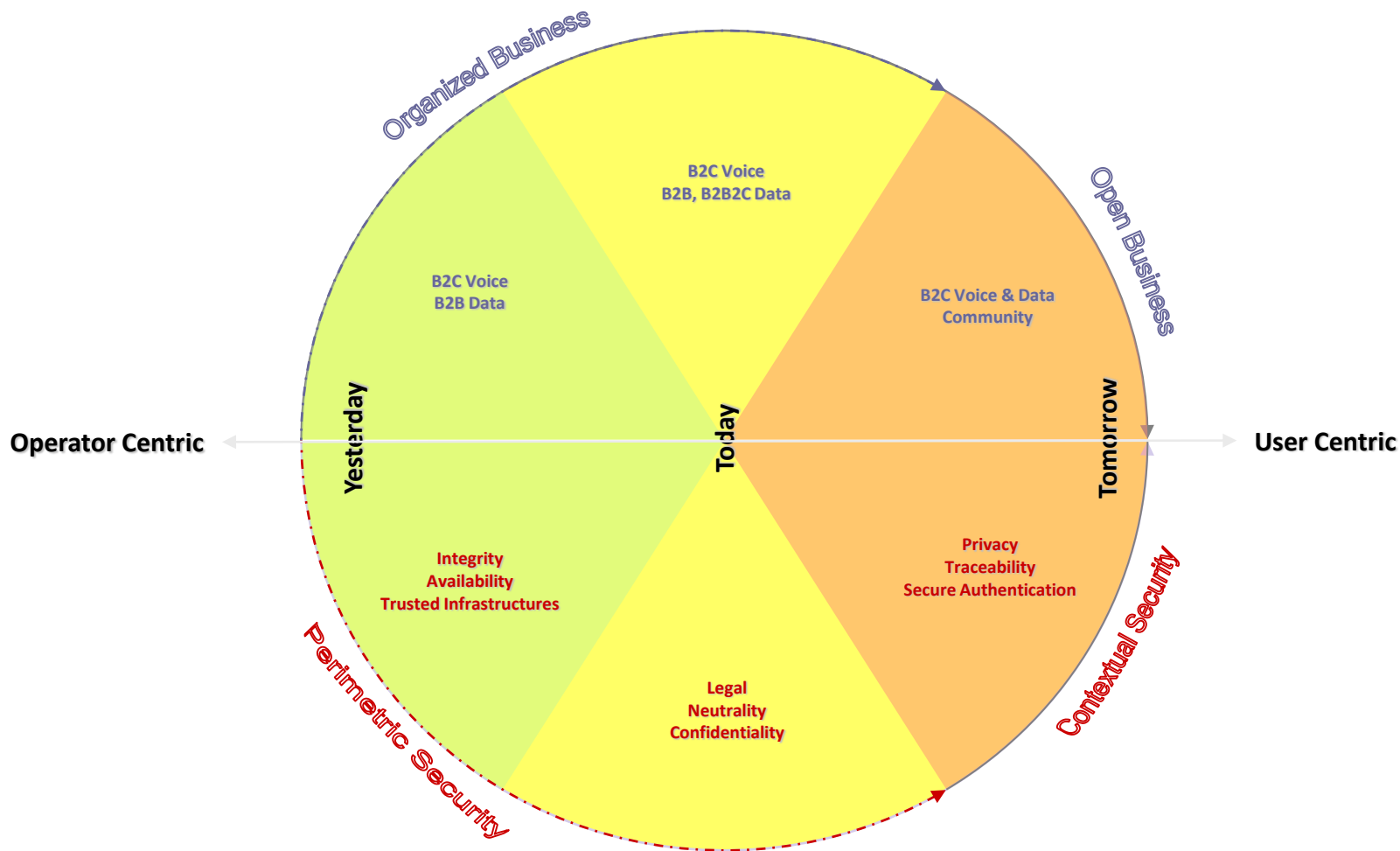
Kourosh Teimoorzadeh

Fraud and Information Security Intelligence

SFR

*SFR Opérateur de Confiance*  
**Core Business Evolution vs New Security Challenge**

SFR Carrément vous



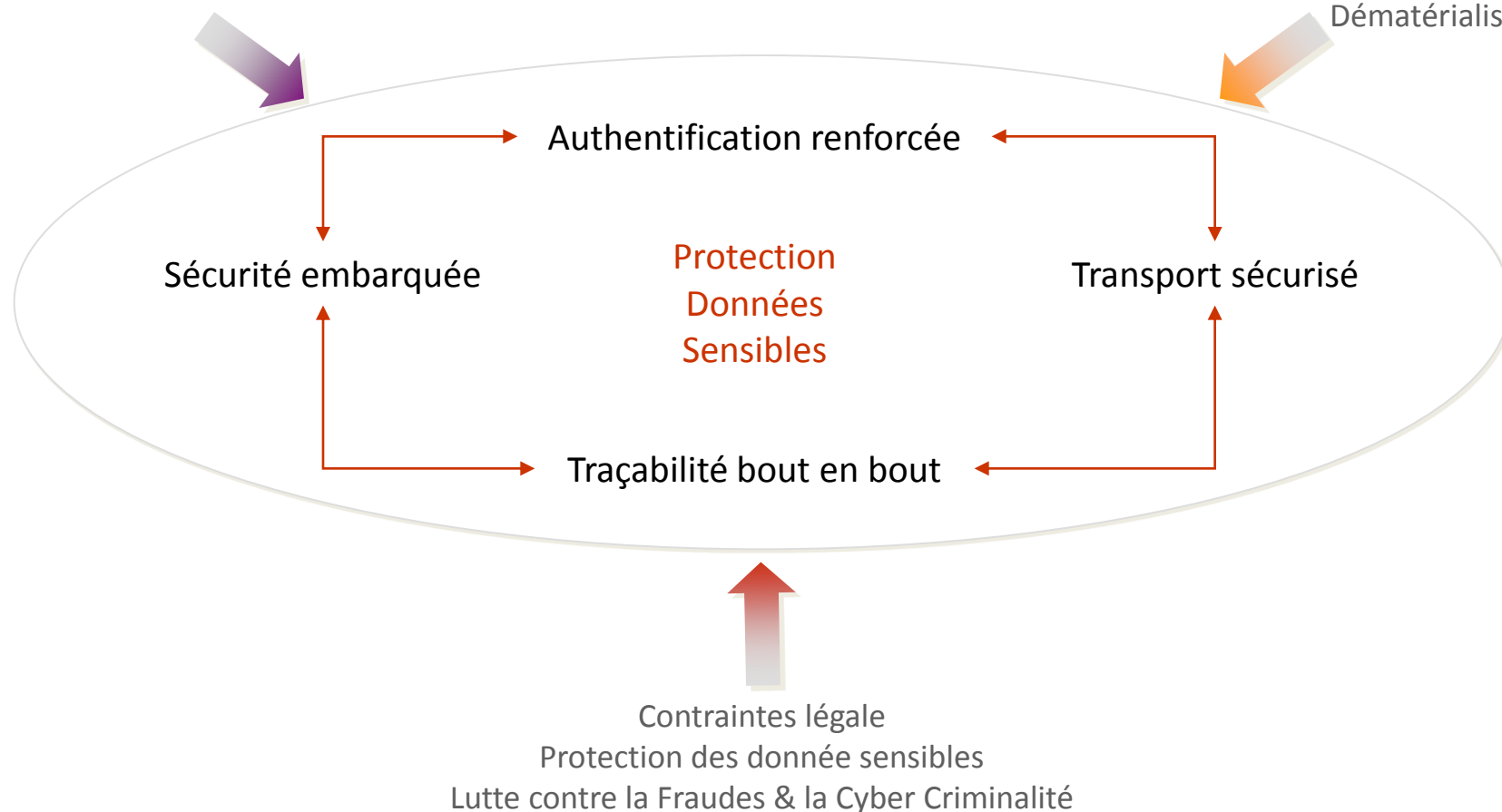
SFR Opérateur de Confiance

Trusted Business → Trusted Technology

SFR Carrément vous

Evolution du marché  
Economie numérique  
Evolution d'usages

Smartphone  
Open Source  
Dématérialisation



SFR Opérateur de Confiance

Smart Authentication → Secure Element

SFR Carrément vous

## Contexte

### Authentification Renforcée

- Technologie permettant le renforcement du niveau de sécurité d'accès aux services et la **simplification du parcours client**
- Solution **User Centric** basée sur l'usage d'une carte SIM afin d'assurer une Identification / Authentification forte de l'utilisateur de façon **transparente** (éviter des authentifications multiples)
- Solution applicable à différents cas d'usage : applications bancaires et transactionnelles (ex. m-payment, M2M, sans contact), Santé, Défense, Peer2Peer, etc

## Enjeux

### Acteur majeur → Confiance Numérique

- Contribuer aux perspectives de business orientées «Opérateur de Confiance » et au positionnement de **SFR** comme **fournisseur naturel d'Identité Numérique**
  - Maîtrise des infrastructures
  - Protection et des biens numériques des usagers
  - Prévention contre la fraude (traçabilité, répudiation d'actes, etc)

## Parcours Client

### Usage opportuniste du contexte réseaux 2G/3G

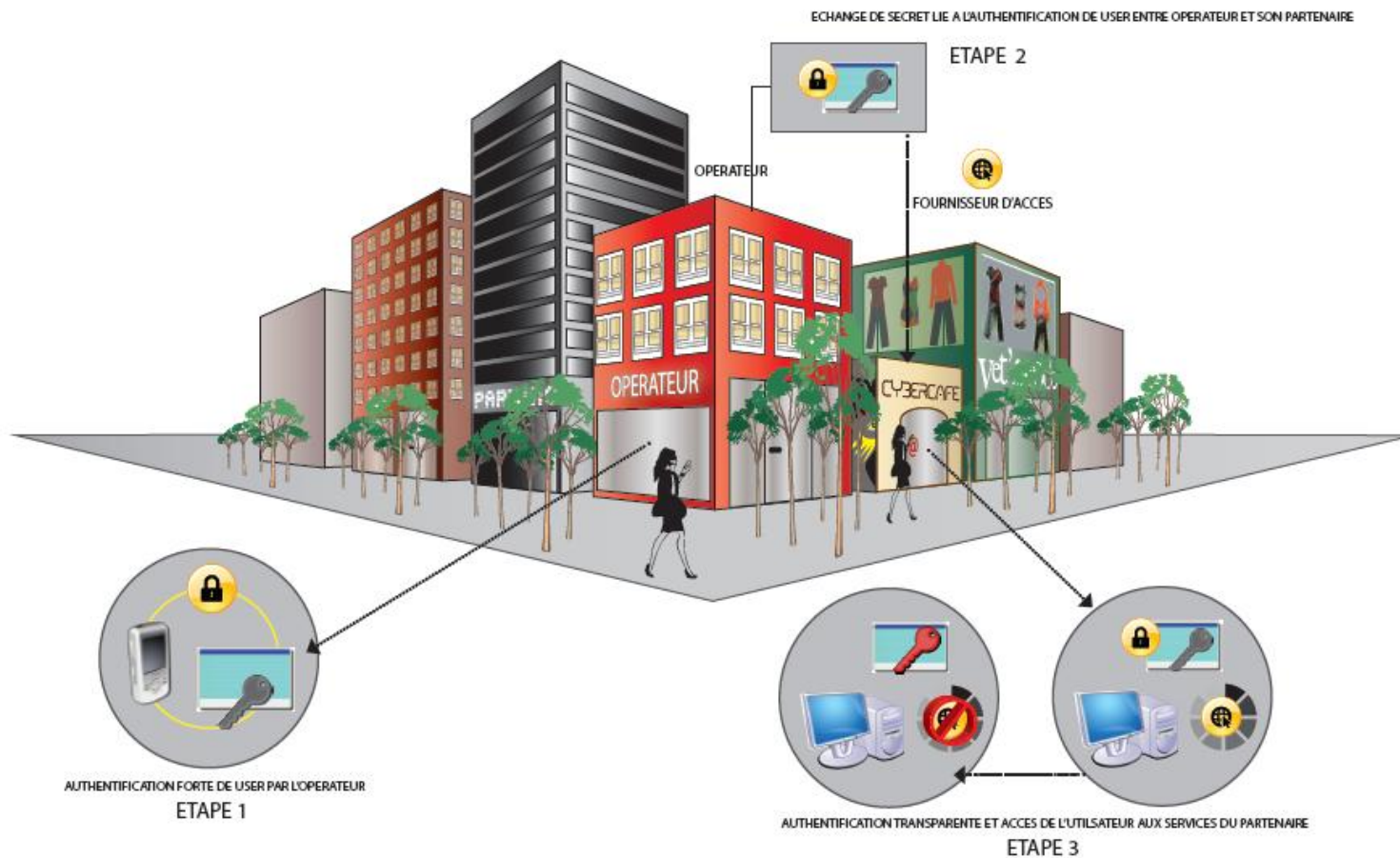
- Une fois connecté au réseau 2G/3G l'utilisateur se connecte à un service sans identification et authentification explicites
- Expérience de connectivité de l'utilisateur au réseau 2G/3G et de son **authentification grâce à sa carte SIM** sera exploitée de façon transparente comme un facteur d'authentification pour accéder à d'autres Services
- Impacts négligeables coté réseau et du coté client (Applets dédiées)

SFR Opérateur de Confiance

SFR Carrément vous

## Smart Authentication → Contextual Authentication

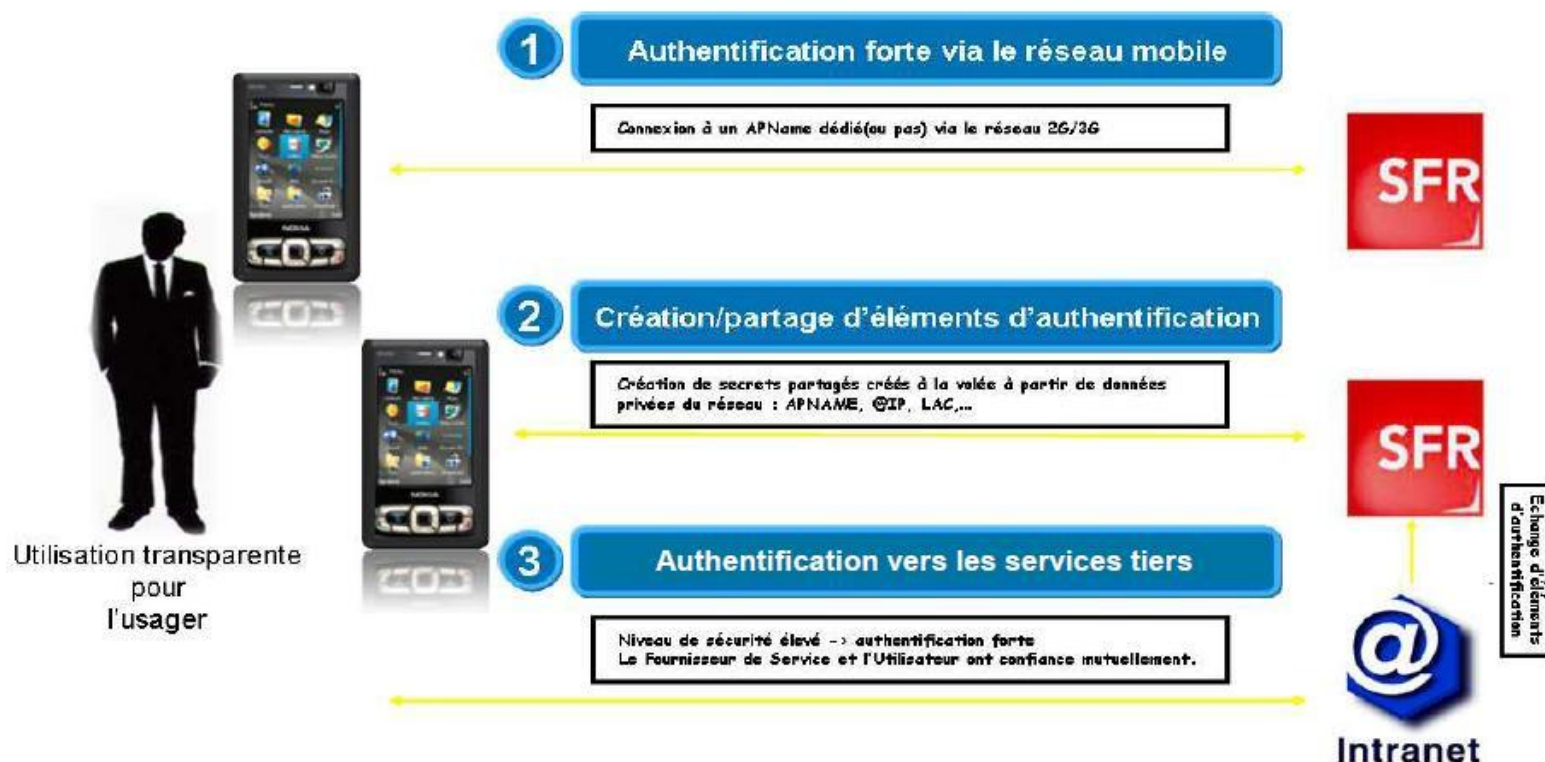
Smart Authentication réutilise de manière *sécurisée* et *transparente* l'authentification mobile du contexte GSM



SFR Opérateur de Confiance

SFR Carrément vous

Smart Authentication → Secure, Transparent, Multiplatform, Multi-bearers



**MERCI**

**kourosh Teimoorzadeh**  
[kourosh.teimoorzadeh@sfr.com](mailto:kourosh.teimoorzadeh@sfr.com)

# Enjeux et pratiques pour les banques, assurances, e-commerce

**Sébastien Inghels**

Supervising Manager

**Périclès Consulting**

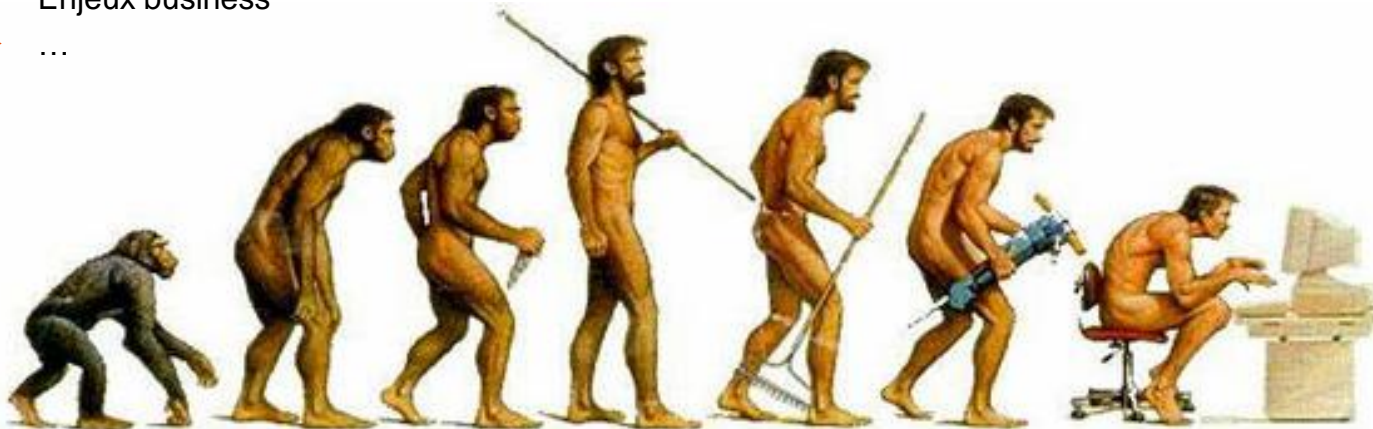
# Le développement de la dématérialisation

## ■ Depuis toujours, l'homme utilise la dématérialisation pour simplifier son quotidien

- ▶ La naissance de l'écriture, premier outil de la dématérialisation
- ▶ Du troc à l'argent
- ▶ Le fax ou la dématérialisation du courrier
- ▶ Le minitel et les premiers services de dématérialisation à la française
- ▶ Internet ou la dématérialisation sans frontières

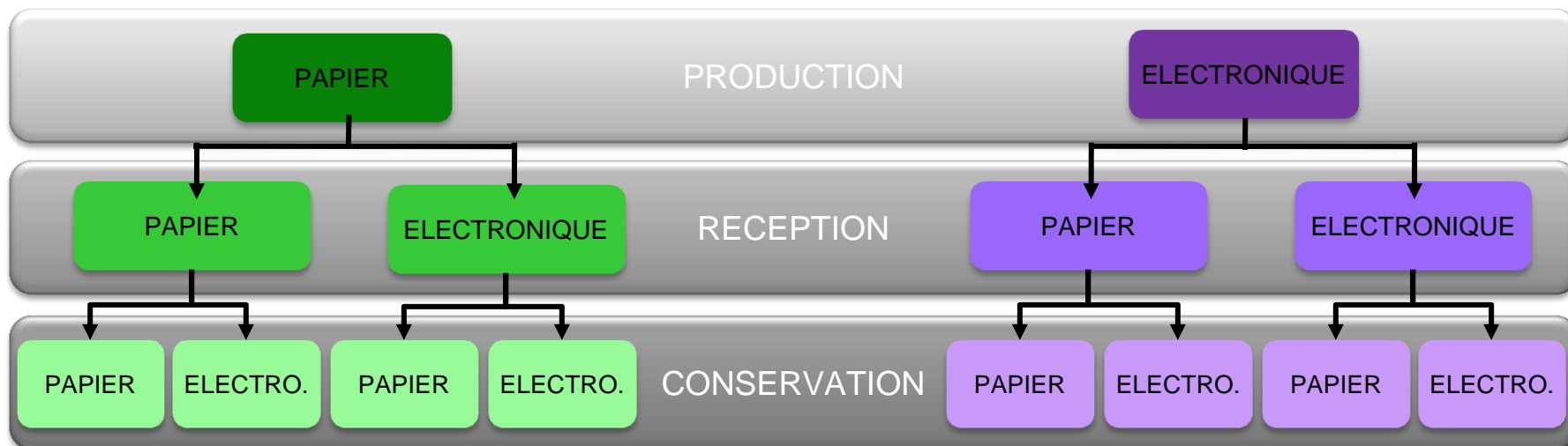
## ■ Le développement de la dématérialisation s'accélère depuis 50 ans

- ▶ Développement des technologies
- ▶ Maturité du cadre juridique
- ▶ Enjeux business
- ▶ ...



## La sécurité, le frein majeure au développement de la démat ?

- Actuellement, le traitement des données se fait de façon hétérogène



- ➔ Quel est l'impact de la circulation et de la transformation du document sur sa valeur juridique ?
- ➔ Comment faire en sorte qu'à minima l'écrit électronique = l'écrit papier ?

## Rappel du rôle de l'écrit en droit français

- **L'établissement d'un écrit est nécessaire pour :**
  - ▶ Former un **CONTRAT**
  - ▶ Établir une **PREUVE**
  - ▶ Satisfaire à une **FORMALITE** légale ou réglementaire (fiscalité, comptabilité, société, droit du travail, etc.)
- **Pour la défense de ses intérêts, l'entreprise doit établir et conserver des preuves :**
  - ▶ De faits (événement susceptible de produire des effets juridiques)
  - ▶ Des engagements qu'elle a souscrits (actes juridiques dont elle est créancière ou débitrice)
- **Les faits peuvent être établis par tous moyens de preuve**
- **Les engagements ne peuvent être établis que par certains moyens de preuve hiérarchisés :**
  - ▶ **L'écrit** (moyen privilégié)
  - ▶ L'aveu
  - ▶ Les témoignages
  - ▶ Les présomptions...

➔ **Comment transposer cela dans le monde dématérialisé ?**

## La preuve « Littérale » en droit

- La preuve des engagements est définie à l'Article 1341 du Code civil (1804)
- La preuve « littérale », écrit sous seing privé, est nécessaire :
  - ▶ Pour prouver un engagement dont la valeur est supérieure à **1 500 €** (décret 20/08/2004)
  - ▶ Si la valeur de l'engagement est *indéterminée*
- Il est impossible de prouver par témoignage « contre et outre» le contenu de l'écrit : l'écrit fait foi entre les parties
- La signature est nécessaire à la perfection de l'acte
  - ▶ Identification du signataire
  - ▶ Adhésion au contenu de l'acte
- ➔ La preuve est « libre» entre commerçants (L.110-3 du Code de commerce)



## La construction du cadre réglementaire

- **Directive du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques**
  - ▶ Favoriser les échanges commerciaux au sein de l'union
  - ▶ Instaurer une certaine confiance dans ces transactions
  - ▶ Conférer à l'ensemble une valeur juridique équivalente à celle de la signature manuscrite
- **Loi n° 2000-230 du 13 mars 2000 : la signature électronique (l'écrit ad probationem)**
  - ▶ La preuve écrite est valable *quel qu'en soit le support* (papier, électronique, microfilms, etc.)
  - ▶ L'écrit électronique à la même force probante que l'écrit papier sous conditions
- **Loi n° 2004-575 du 21 juin 2004 LCEN : l'écrit électronique *ad validitatem* et l'acte authentique électronique**
- **Ordonnance n°2005-674 du 16 juin 2005 : les formalités contractuelles par voie électronique**
  - ▶ « des contrats sous forme électronique »
  - ▶ « l'échange d'informations en cas de contrat sous forme électronique »
- **Les autres textes**
  - ▶ Loi pour l'orientation et la programmation pour la sécurité intérieure (Loppsi I et II)

## La loi du 13 mars 2000

### ■ Article 1316 du Code civil

« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, **quels que soient leur support et leurs modalités de transmission.** »

### ■ Article 1316-1 du Code civil : conditions d'admissibilité de l'écrit électronique à titre de preuve

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être **dûment identifiée la personne** dont il émane et qu'il soit **établi et conservé** dans des conditions de nature à en **garantir l'intégrité.** »

### ■ Article 1316-3 du Code civil

« L'écrit sur support électronique a la **même force probante** que l'écrit sur support papier. »

### ■ Article 1316-4 du Code civil : la signature

« La signature nécessaire à la perfection d'un acte juridique **identifie** celui qui l'appose. Elle manifeste le **consentement des parties** aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

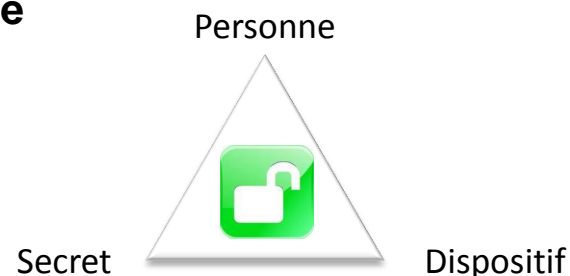
Lorsqu'elle est électronique, elle consiste en l'usage d'un **procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.** La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et **l'intégrité** de l'acte garantie, dans des conditions fixées par décret en Conseil d'État. »

## De l'authentification forte à la signature électronique

- S'identifier, c'est communiquer une identité préalablement enregistrée
- S'authentifier, c'est apporter la preuve de cette identité

- Moyens : les facteurs pour une authentification forte

- ▶ Un support personnel, associé à la personne
- ▶ Disposant d'un dispositif crypté
- ▶ Avec un secret connu de la personne



- La signature électronique qualifiée doit répondre aux contraintes suivantes

- ▶ **Authentique** : l'identité du signataire doit pouvoir être retrouvée de manière certaine
- ▶ **Infalsifiable** : la signature ne peut pas être falsifiée. Quelqu'un d'autre ne peut se faire passer pour un autre
- ▶ **Non réutilisable** : la signature fait partie du document signé et ne peut être déplacée sur un autre document
- ▶ **Inaltérable** : une fois signé, le document ne peut plus être modifié
- ▶ **Irrévocable** : la personne qui a signé ne peut le nier

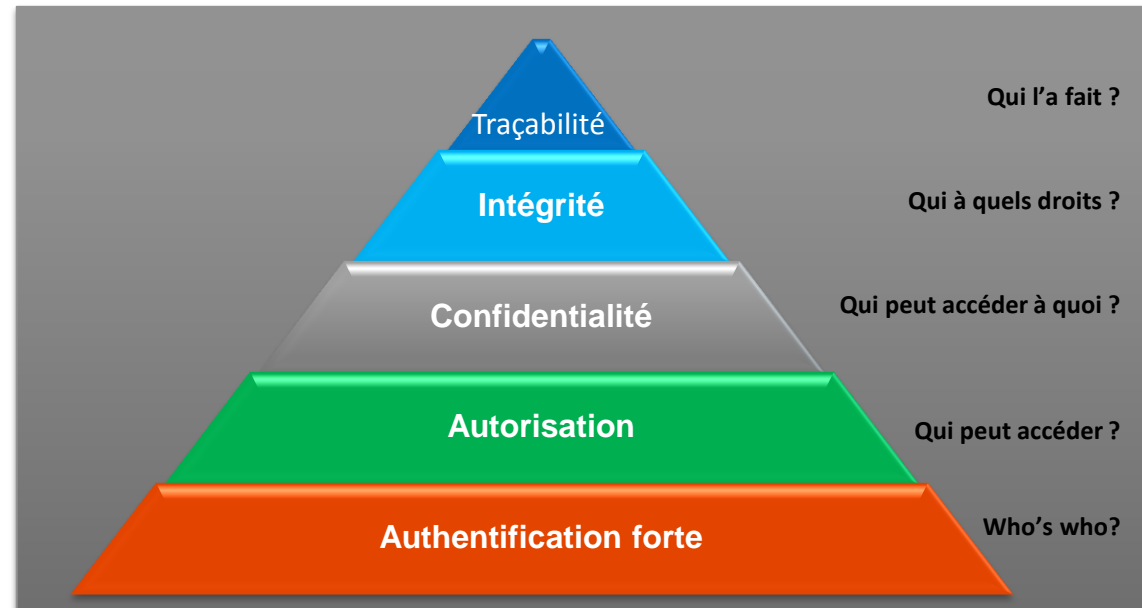
**NB** : La carte bancaire utilisée dans un TPE est un dispositif d'authentification fort



## La pyramide de l'authentification forte

### ■ L'authentification forte est une des fondations essentielles pour garantir :

- ▶ L'identité de parties
- ▶ L'autorisation ou contrôle d'accès
- ▶ La confidentialité
- ▶ L'intégrité
- ▶ La traçabilité



## Les enjeux business

### ■ Pour ce qui concerne le grand public en 2010 *(source ARCEP)*

- ▶ **1 français sur 2** achète par internet
- ▶ Le CA du e-commerce dépasse **31 milliards d'€** et plus de 278 millions de transactions
- ▶ Le commerce électronique est aujourd'hui principalement national (à plus de 90%)

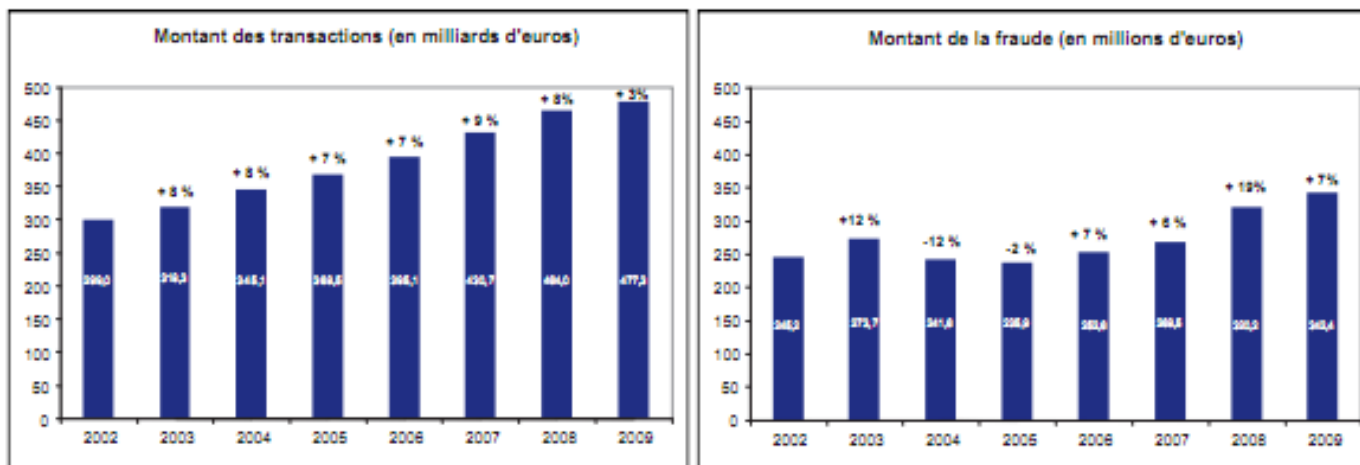
### ■ Pour ce qui concerne les entreprises de plus de 10 salariés *(source INSEE)*

- ▶ 60 % des sociétés échangent par voie électronique de l'information dans un format permettant son traitement automatique
- ▶ **26 %** des sociétés **achètent en ligne** pour un CA de 237,5 milliards d'euros
- ▶ La **presque totalité** des entreprises ont des **accès télématiques bancaires**, EDI et/ou de services en lignes « transactionnels », la **généralisation** d'une **authentification forte et de signature électronique** est en cours



## Le développement de la fraude

### ■ La fraude sur carte de crédit *(Comité de la médiation bancaire – bilan annuel 2009)*



NB : Pour la première fois en 2008, le taux de fraude national pour le canal MO/TO dépassait le taux de fraude sur Internet

### ■ La fraude à l'identité *(Rapport du Credoc) :*

- ▶ Plus de **200 000 victimes** par an d'usurpation d'identité en France
- ▶ Un préjudice de près d'environ **4 milliards d'€**
- ▶ Un coût moyen de **2 229 € par personne**
- ▶ Près d'une victime sur deux avoue être «*incapable de savoir comment le fraudeur a réussi à obtenir ses données personnelles alors que 86 % des victimes estiment faire le nécessaire pour se protéger des risques*»

# Les solutions déployées par les établissements bancaires

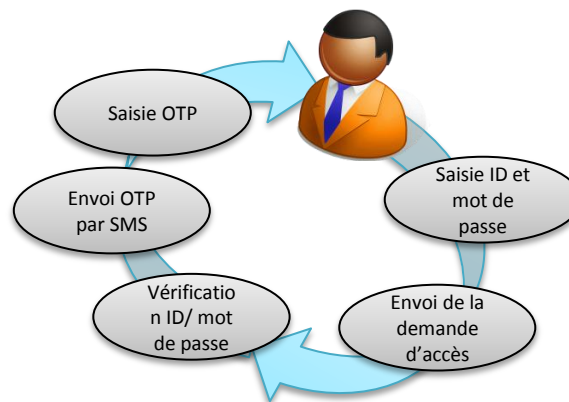
## ■ Les outils d'identification

- ▶ Couple login / Mot de passe



## ■ Les principaux outils d'authentification déployés

- ▶ Certificat logiciel
- ▶ Couple login / Mot de passe avec code de vérification sur carte matricielle (bataille navale)
- ▶ Couple login / Mot de passe avec SMS
- ▶ Token
- ▶ Carte CAP spécifique
- ▶ Certificat X509 sur support matériel : clé USB, Carte à puce, etc.



# Les contraintes et stratégie de déploiement sur le grand public

## ■ La contrainte volume : nombre de client à équiper

## ■ La contrainte coût

- ▶ Coût d'équipement
- ▶ Coût d'utilisation
- ▶ Coût de gestion des identités numériques

## ■ La contrainte adoption client

- ▶ Accompagnement au changement des clients

	Facilité d'utilisation		Efficacité perçue		Souhait d'utilisation
Saisie de la date de naissance	90 %	↑	35 %	↓	45 %
Réponse à une question	85 %		54 %		54 %
Saisie d'un code unique reçu sur le téléphone mobile	71 %		70 %		64 %
Saisie d'un code unique généré par un mini-lecteur	60 %		76 %	↓	69 %

▲ Tableau 9 – Les solutions d'authentification proposées par les banques :  
des perceptions contrastées  
(en pourcentage des payeurs par carte sur Internet)

(Comité de la médiation bancaire – bilan annuel 2009)

# Illustration : ouverture d'un compte : La NetAgence

1

Connexion au site de la Net Agence

2

Remplir un formulaire sécurisé en ligne  
Saisie des informations personnelles

3

Choix des moyens de paiement

**LA NETAGENCE**  
La nouvelle agence sur Internet de BNP Paribas

**Coordonnées** Moyens de paiement

**Ouvrez votre compte dans notre agence sur Internet**

- 1 Complétez en quelques clics le formulaire.
- 2 Obtenez votre convention de compte au format papier (impression en ligne ou envoi par courrier postal) ou signez-la directement en ligne.
- 3 Envoyez-nous les pièces justificatives demandées.

Votre type de compte  
Sélectionnez le type de compte ☒ Individuel ☐ Joint

Vos coordonnées

Nom Martin  
Prénom Jean  
Civilité ☒ M. ☐ Mme ☐ Mlle  
Date de naissance 10/03/1981  
Lieu de naissance ☒ France ☐ Autre pays  
Département de naissance 94  
Commune de naissance Champigny Sur Marne  
Nationalité (Pays) France

Pays de résidence fiscale France  
N° libellé de vote 10 rue de la chance  
Code postal 75000  
Ville PARIS

Email jmartin@chance.fr  
Confirmez votre email jmartin@chance.fr  
Téléphone mobile 0645656667  
et/ou Téléphone fixe  
Être contacté ☒ En semaine le matin

Je souhaite recevoir les meilleures offres de BNP Paribas (actualités commerciales, bons plans, offres promotionnelles, ...) ?  
Par email ☐ Oui ☒ Non Par SMS / MMS ☐ Oui ☒ Non  
Par courrier ☐ Oui ☒ Non Par téléphone ☐ Oui ☒ Non

Les champs marqués d'une \* sont obligatoires.

**LES + DE LA NETAGENCE**

**Exclusivités Internet**

- Votre compte chèques et vos services bancaires **GRATUITS** pendant 1 an <sup>(1)</sup>
- Vos comptes et virements en France sur mobile et Internet **gratuits**
- Vos frais de dossier offerts pour votre prêt personnel souscrit en ligne
- Votre prêt immobilier en ligne : une réponse de principe **immédiate**
- - 50 % sur vos frais d'entrée standards pour toute souscription en ligne d'une **assurance vie**

Profitez de vos exclusivités Internet  
En saisissant : **NET10**  
dans le champ "Code promo" sur la page "Récapitulatif"

**Conseiller personnel**

Votre Conseiller personnel joignable **6 jours/7** (de 8h à 20h du lundi au Vendredi et jusqu'à 18h le samedi)

- Par Webcam rendez-vous
- Sur sa ligne directe
- Sur son e-mail personnel

**Mobile et Internet**

- Vos comptes sur iPhone, iPad, Android et mobile
- Des services et des applications gratuites

BNP Paribas :  
Eu Service Client de l'Année 2011  
Une offre de qualité récompensée en 2010

LES CHAMPS MARQUÉS D'UNE \* SONT OBLIGATOIRES.

**Revenir à l'étape précédente** **Valider et finaliser son ouverture de compte**

## Illustration : suite

4

Valider le récapitulatif

5

Choix du mode de signature de  
la convention : papier ou électronique

### Choix 1 :

- ✓ Impression chez le client de la convention pré remplie,
- ✓ Signature manuscrite, envoi avec pièces justificatives

### Choix 2 :

- ✓ Envoi par BNP de la convention pré remplie,
- ✓ Signature manuscrite, envoi avec pièces justificatives

### Choix 3 : solution dématérialisée

- ✓ Signature vocale sur un serveur vocal,
- ✓ Signature électronique et dépôt en ligne des pièces justificatives

**LA NET AGENCE**  
La nouvelle agence sur Internet de BNP Paribas

**RECAPITULATIF**

Votre compte individuel

Monsieur Martin Jean Email : jmartin@chance.fr Mobile : 0645656667 Date de naissance : 10/03/1981	Adresse : 10 rue de la chance 75000 - PARIS
--	---

Code promo : NET10

[< Précédent](#)

☒ Je certifie que les informations fournies sont exactes.

Pour finaliser votre demande d'ouverture de compte, vous pouvez :

**Imprimer immédiatement votre convention de compte !**

- Validez vos conditions générales
- Imprimez votre convention de compte pré remplie
- Signez et envoyez-la avec vos pièces justificatives

Imprimer sa convention de compte

**Recevoir votre convention de compte par courrier**

- Recevez par courrier votre convention de compte pré remplie
- Signez et envoyez-la avec vos pièces justificatives

Recevoir sa convention de compte par courrier

**Signer en ligne votre convention de compte**

- Validez vos conditions générales
- Donnez votre accord sur notre serveur vocal et signez en ligne votre ouverture de compte
- Déposez en ligne vos pièces justificatives

Ouvrir son compte avec la signature en ligne

## Assurance en ligne...

### ...Vers une généralisation de la signature électronique ?

#### ■ En matière de contrat, on distingue

- ▶ Le contrat desynallagmatique qui est **unilatéral**
- ▶ Le contrat **synallagmatique** ou bilatéral



#### Assurance de personne

- **Cause de l'obligation**
  - ▶ Conduit par les **obligations** de l'assureur
- **Nécessité de formalisme**
  - ▶ Contrat **oral ou écrit**
  - ▶ Date de **début** d'obligation
- **Contrôles à effectuer**
  - ▶ IBAN
  - ▶ Justificatif de domicile
- **Moyen à mettre en œuvre**
  - ▶ Horodatage
  - ▶ Enregistrement vocal



#### Epargne/ prévoyance

- **Cause de l'obligation**
  - ▶ Conduit par les obligations réciproque
- **Nécessité de formalisme**
  - ▶ Contrat **écrit**
  - ▶ Date de **prise d'effet** du contrat (incidence fiscale)
- **Contrôles à effectuer**
  - ▶ Contrôles métiers
  - ▶ Lutte anti-blanchiment
- **Moyen à mettre en œuvre**
  - ▶ Horodatage
  - ▶ Authentification forte
  - ▶ Outil de signature

**MERCI**

**Sébastien Inghels**

[singhels@pericles consulting.com](mailto:singhels@pericles consulting.com)

# Sécurité des réseaux de télécommunication

Frédéric Crestin

AESMA



ANALYSIS ETHICS SECURITY MANAGEMENT ASSESSMENT

- Cabinet de Conseil fondé en 2009 sur le principe de « partnership »
- 2 entités:
  - **AESMA:** conseiller et accompagner le développement international de nos clients dans les pays et environnements dégradés ou complexes
  - **AESMA Engineering:**
    - Conseil et Audit en Sécurité des Systèmes d'Information
    - Ingénierie de Sûreté

# Sommaire

- Les besoins en termes de Sécurité
- Historique
- Un réseau mobile
- Principaux mécanismes Sécurité
- Autres risques
- Cas particulier - Le Blackberry
- Précédents événements Sécurité

# Introduction

- Croissance permanente des terminaux mobiles à travers le monde
  - notamment dans les pays émergents où c'est souvent le seul moyen de télécommunication incluant Internet
- Terminaux de plus en plus versatiles
  - Progression exponentielle des transactions effectuées sur les réseaux mobiles:
  - Exemple: environ 1,5 milliard d'euros de transactions effectuées via l'application eBay sur iPhone

*La Sécurité des réseaux mobiles est donc un enjeu vital pour l'économie mondiale et pour les populations*

# Historique des réseaux mobiles

Année de mise  
en production

1978

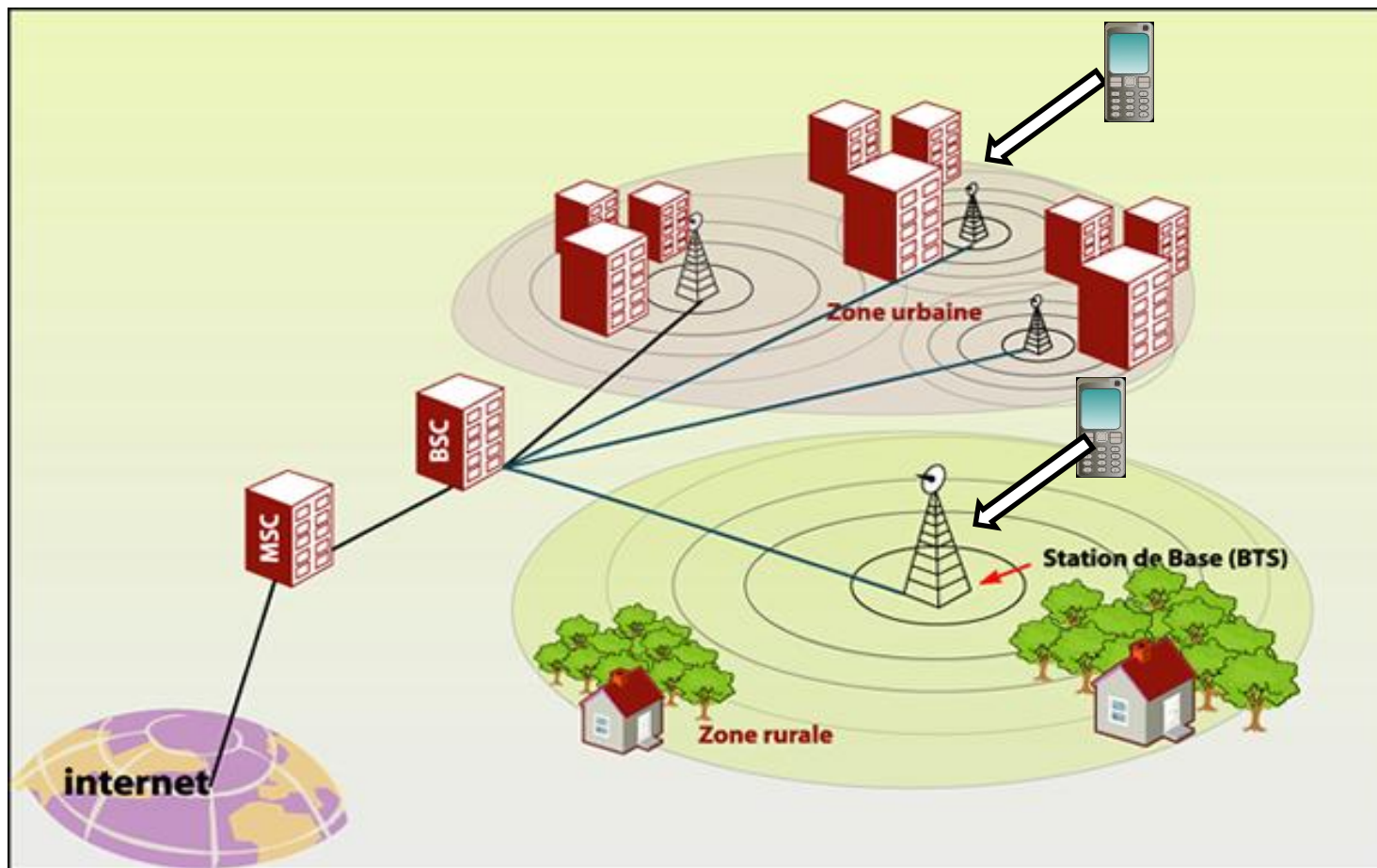
1991

2001

2009

Version	Nom	Sécurité ?
1G	Radiocom 2000 NMT AMPS	Authentification de l'abonné
2G	GSM	Authentification et chiffrement
2.5G	GPRS	Id.
3G	CDMA UMTS	Id. + authentification du réseau par le terminal + qualité de service
3.5G	HSDPA	Id.
4G	LTE WIMAX	Id. + qualité de service

# Schéma de principe d'un réseau mobile



# Principaux mécanismes de sécurité

- **Code PIN:** authentification de l'utilisateur par la carte SIM
- **Authentification de l'abonné:** enregistrement de la carte SIM sur le réseau
- **Chiffrement du flux Voix ou Données**
- **4 adressages liés à l'abonné et au terminal:**
  - **IMSI:** identité unique de l'abonné
  - **TMSI (Temporary Mobile Subscriber Identity):** identifiant aléatoire du terminal sur le réseau
  - **MSISDN:** numéro de téléphone de l'abonné
  - **MSRN:** utilisé pour le routage des appels

# Carte SIM

- L'utilisateur doit s'authentifier à l'aide d'un code PIN
- La carte SIM contient les données permettant d'authentifier l'abonné sur le réseau

# Authentification de l'utilisateur

## Algorithmes utilisés: A3 et A8

Le réseau mobile authentifie et contrôle principalement, lors de l'enregistrement de l'abonné:

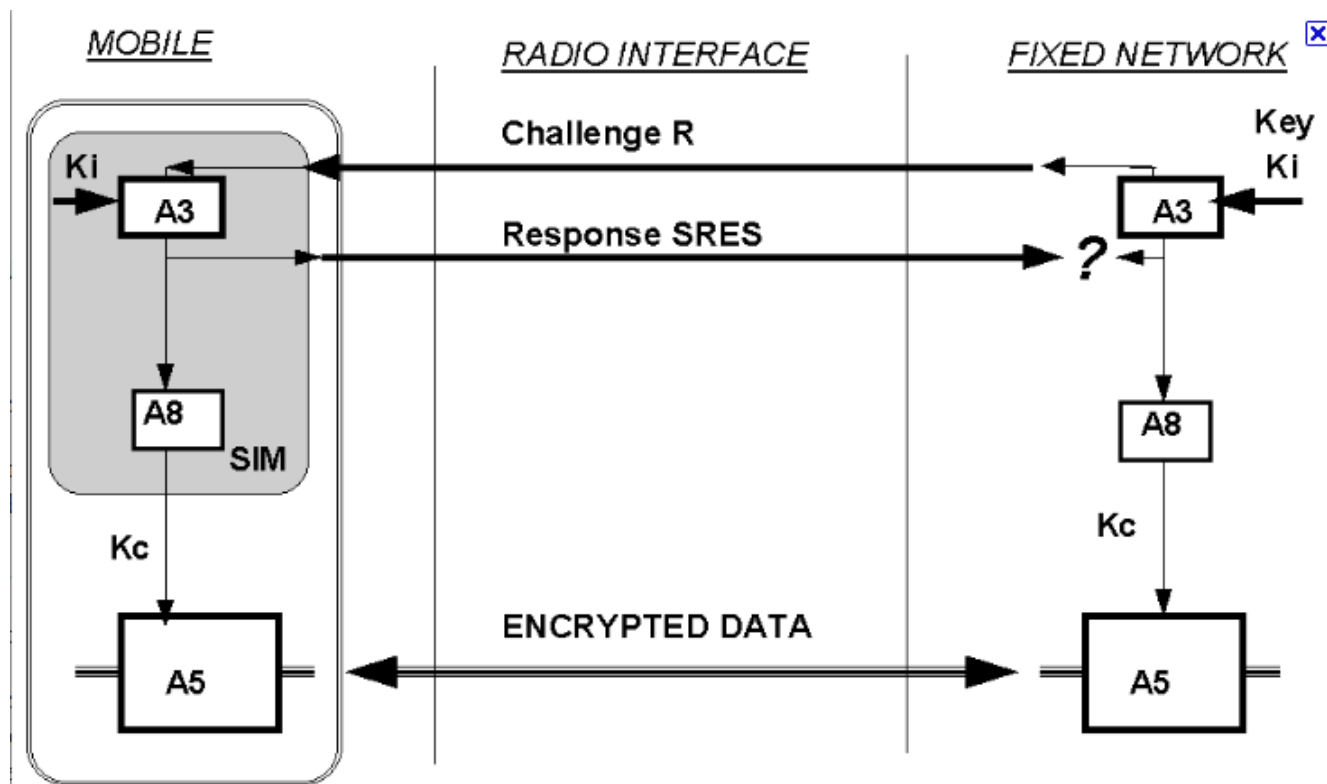
- La validité de la carte SIM
- La validité du terminal (no IMEI)

Un identifiant temporaire est alors attribué au terminal (TMSI).

Ce schéma d'authentification est le même pour tous les opérateurs des réseaux mobiles interopérables et est contrôlé par l'association GSMA:

Security Accreditation Scheme

# Schéma Authentification de l'utilisateur



Une clé est générée par ce biais pour chaque appel passé.  
La clé d'authentification  $K_i$  ne passe jamais sur le réseau !

# Chiffrement des flux

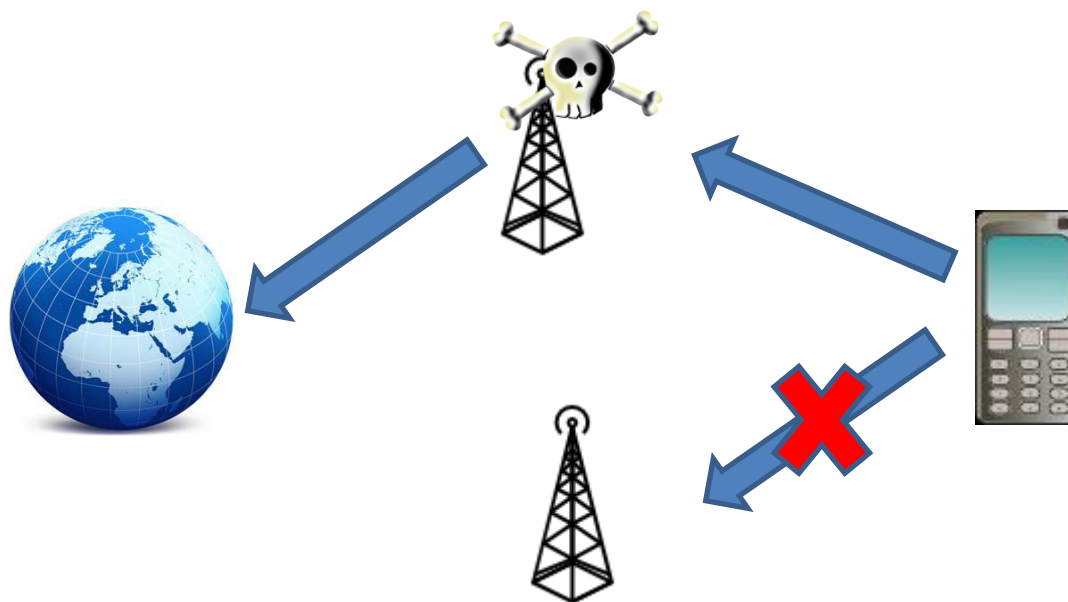
- Algorithmes de chiffrement utilisés:
  - A5/1 (le plus courant), utilise des clés de 54 bits
  - A5/2, dans certains pays soumis à restriction sur l'utilisation de certains algorithmes de chiffrement
  - A5/3, pour le chiffrement des données sur les réseaux 3G et +

# Les bases de données d'une infrastructure GSM

<b>HLR</b> (Home Location Register)	<ul style="list-style-type: none"><li>• Contient toutes les données d'identification d'un abonné</li></ul>
<b>VLR</b> (Visitor Location Register)	<ul style="list-style-type: none"><li>• Contient les données des abonnés se connectant à un réseau étranger</li></ul>
<b>EIR</b> (Equipment Identity Register)	<ul style="list-style-type: none"><li>• Contient les données sur les terminaux et les autorisations (« White », « Grey » et « Black » List)</li></ul>
<b>AUC</b> (Authentication Center)	<ul style="list-style-type: none"><li>• Données confidentielles des abonnés</li><li>• IMSI, TMSI, LAI (Location Area Identity) et Ki (Authentication Key)</li></ul>

# Autres risques liés à la sécurité des réseaux

- Network Spoofing → Interception des communications



→ Difficilement réalisable sur les réseaux 3G du fait de la vérification de l'intégrité des clés de chiffrement

# Autres risques liés à la sécurité des réseaux

- Indisponibilité du réseau:
  - Due à la demande croissante des flux de données (selon Cisco: le trafic de données doublera chaque année jusqu'en 2014, soit un trafic multiplié par 39 entre 2009 et 2014) !
  - Exemple: ATT aux USA en 2007 avec l'introduction de l'iPhone

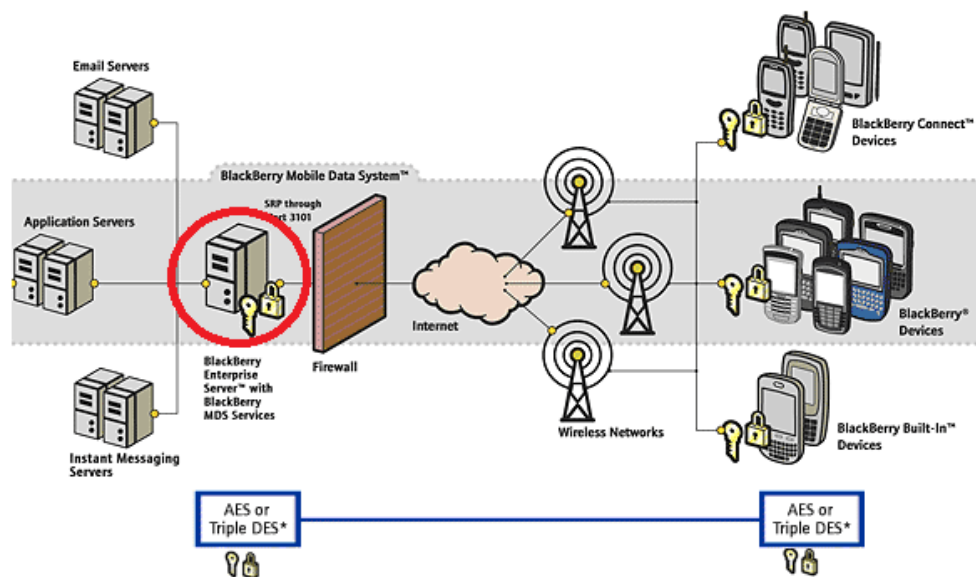
De nouvelles solutions (QoS=Quality of Service, 3GPP Fast Dormancy) sont d'ores et déjà implémentées afin de palier à ce problème.

Les nouveaux protocoles (4G / LTE) intègrent également de tels mécanismes.

## Cas particulier: les Blackberry



**Août 2010:** Emirats Arabes Unis, Inde, Indonésie et l'Algérie réclament à RIM un meilleur contrôle des données transitant par les Blackberry



Flux de données chiffrés des terminaux jusqu'aux serveurs RIM  
➔ opérateurs ne peuvent rien contrôler

- mal accepté dans de nombreux pays, notamment ceux pratiquant la censure Internet
- serveurs hébergés aux USA et Canada...

# Quelques précédents... et les nouvelles mesures de sécurité

- **1993:** localisation de Pablo Escobar par écoute et triangulation GSM
- **Autres cas courants :**
  - Indisponibilité des réseaux par surcharge (Nouvel An)
  - Vol ou perte de terminaux
  - Vol de données par Bluetooth
- **Nouvelles mesures:**
  - Blocage des cartes SIM par le réseau
  - Blocage/désactivation/verrouillage des terminaux par le réseau
  - Localisation des terminaux

## Conclusion

- La sécurité des réseaux mobiles est de très haut niveau, et est prise très au sérieux par tous les acteurs de l'écosystème « *réseaux mobiles* » :
  - les opérateurs
  - les constructeurs (Alcatel, Matra, Ericsson, Nortel, Cisco, Siemens)
  - Les Etats (aspects normatifs)
  - Les institutions de paiement.

- Nécessité d'instaurer la confiance auprès des usagers.

- Il est important de ne pas oublier qu'il s'agit de sécurité des flux de données.

Comme le montre le contre-exemple récent de Sony avec l'attaque finalement assez simple de son réseau PlayStation Network, la sécurité des données doit être intégralement prise en considération, **du terminal jusqu'au serveur (client vers fournisseur).**

# MERCI

**Frédéric Crestin**

AESMA

16, rue Béranger PARIS 3<sup>e</sup>

+33 1 71 60 93 12

[www.aesma-group.com](http://www.aesma-group.com)

[info@aesma-group.com](mailto:info@aesma-group.com)

# Signature électronique et dématérialisation

**Anne Murgier**

Directrice du commerce

**Keynectis**

## KEYNECTIS : Tiers de Confiance, Editeur, Opérateur

### Leader Européen de la sécurité des échanges numériques

#### Notre mission :

*« Protéger les identités,  
les données et les échanges  
au cœur d'un monde connecté »*



#### Notre métier :

- Editeur logiciel, licence et SaaS
- Autorité de Certification
- PSCE / PSCO



**25 millions de cartes e-ID distribuées**  
**10 millions de Certificats actifs**  
**15 pays équipés**

**2 millions e-Contrats signés par an**  
**450 millions de transactions OCSP par an**  
**220 AC en SaaS - 2 Datacenters**

## Un acteur de confiance, audité et reconnu



Une offre logicielle d'un très haut niveau de sécurité



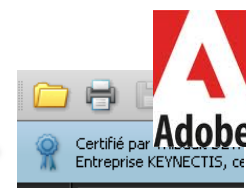
Une offre SaaS / PSCE conforme aux référentiels français et internationaux les plus stricts



Certification Authorities



Des identités numériques reconnues dans les principaux outils bureautiques



Une Autorité de certification reconnue dans 99% des navigateurs



## Authentification + signature : une réponse au besoin du marché

- Constat : les clients veulent utiliser le canal web pour
  - Augmenter leurs ventes
  - Offrir de nouveaux services à leurs clients
  - Fidéliser une nouvelle clientèle
- Ce besoin implique la mise en œuvre de moyens pour :
  - Garantir l'identité des clients internautes
  - Protéger les échanges avec le client
  - Permettre au client de finaliser en ligne



## La signature électronique ... ... une innovation technique en toute sécurité

- Le principe : remplacer la signature manuscrite par une signature numérique ayant la même valeur légale
- Les enjeux :
  - Un gain de temps
  - Des économies financières
  - Une nouvelle étape vers le « zéro papier »
  - Une meilleure sécurité des échanges



## K.Websign® : la solution de signature en ligne

- Permet la signature électronique d'un document par un organisme et un internaute (contrat, commande, déclaration de capacité etc.).
  - Sans contrainte technique sur le poste utilisateur
  - A l'image du paiement électronique sur internet
- Assure les fonctions de gestion de la preuve
  - Dépôt du document original
  - Traçabilité des événements de signature (horodatage)
  - Archivage et restitution d'un fichier de preuve chez un tiers Archiveur



## K.Websign® : pour les acteurs du e-Commerce

- ✓ Souscription
- ✓ Contractualisation
- ✓ Gestion de la Preuve et du Consentement
- ✓ Simplification du Parcours Client
- ✓ Mobilité et Liberté
- ✓ Dématérialisation



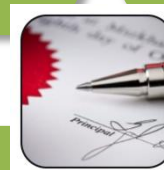
### Banques

- ✓ Ouverture de comptes
- ✓ Prêt à la consommation
- ✓ Consentement aux CGV



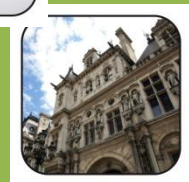
### Médias & Telcos

- ✓ Souscription d'abonnement
- ✓ Signature d'avenants



### Services

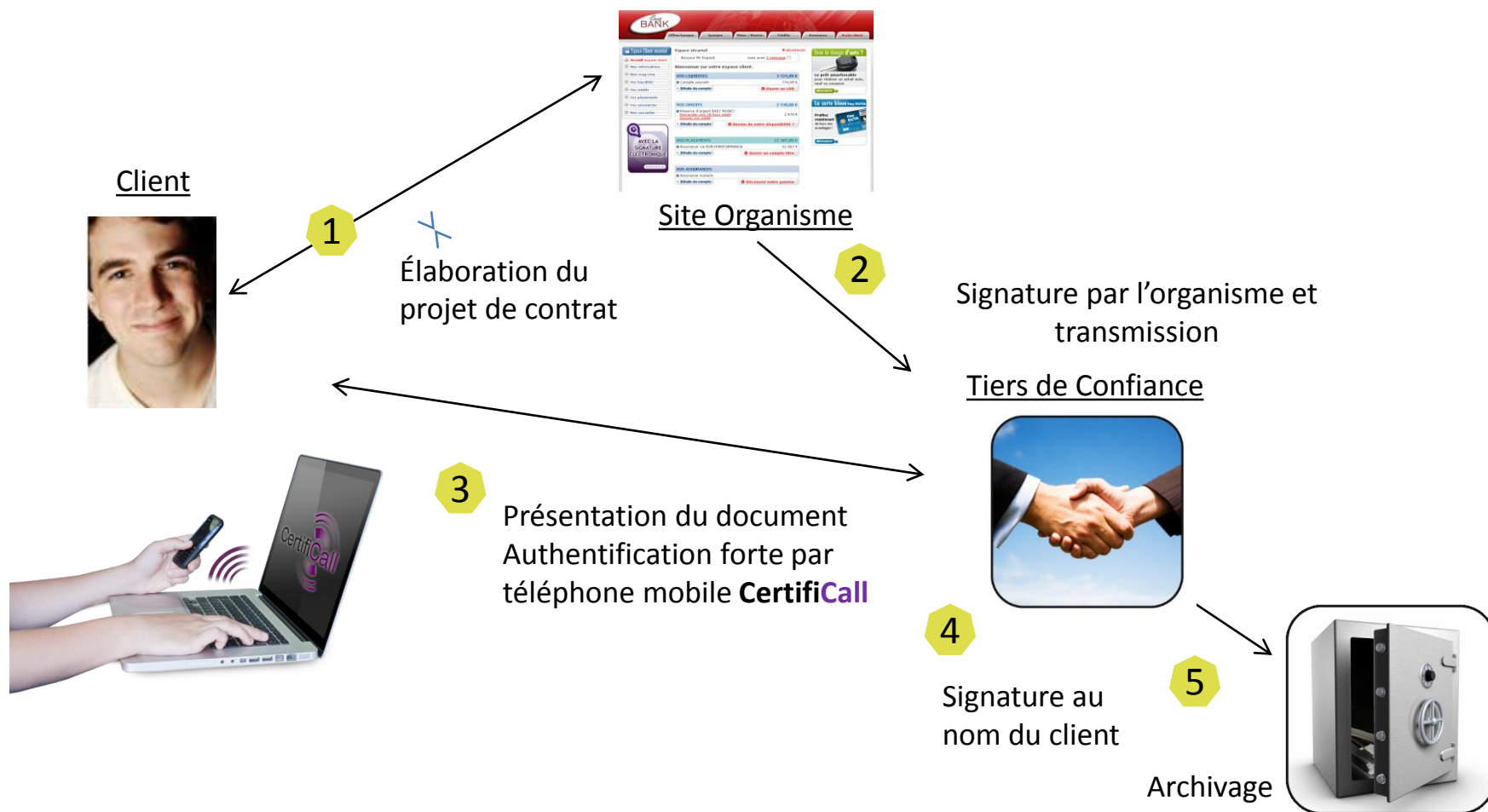
- ✓ Signature des contrats de distribution
- ✓ Dématérialisation des cahiers produits
- ✓ Signatures des commerciaux itinérants



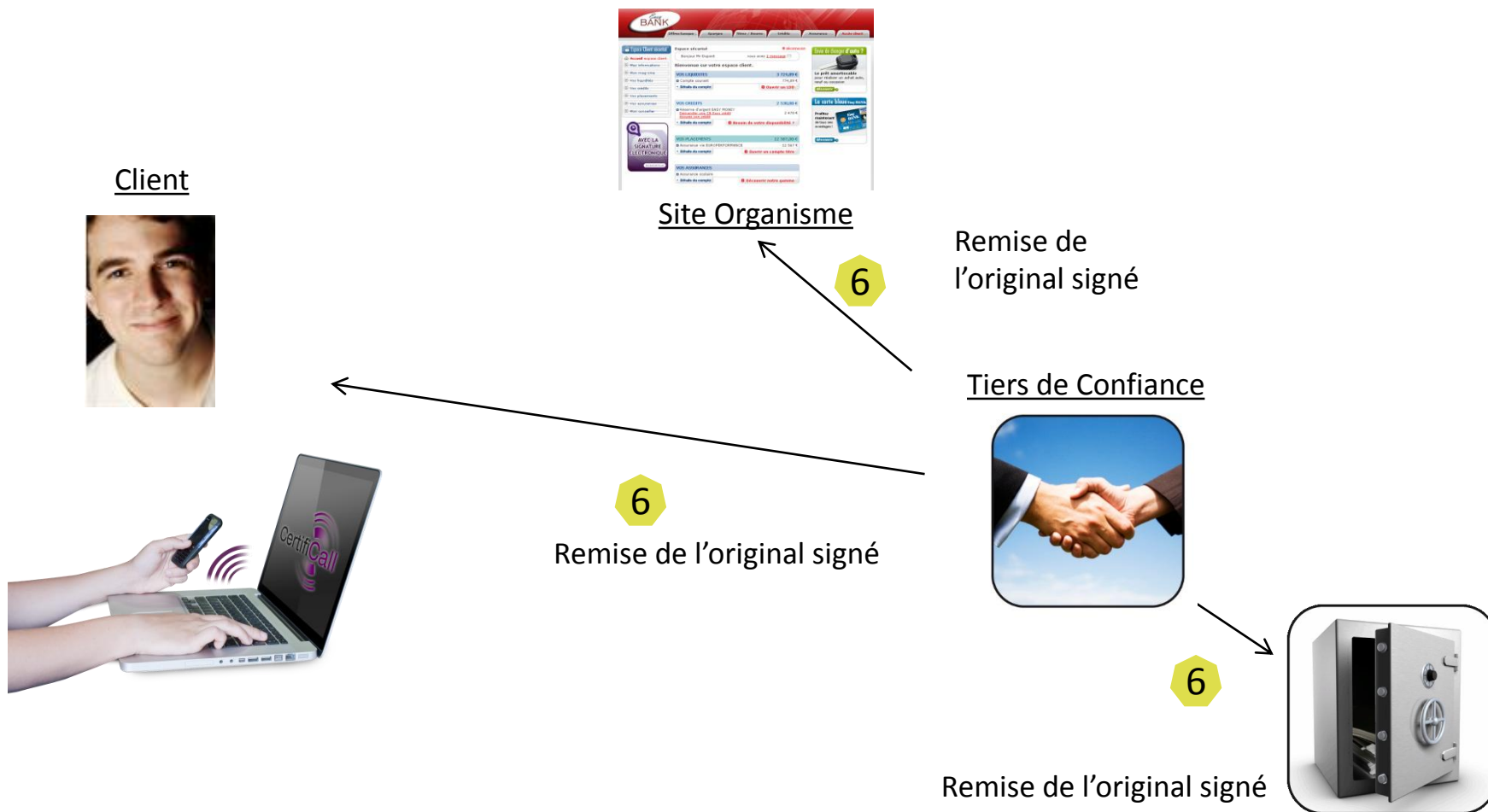
### Assurances

- ✓ Souscription de polices
- ✓ Présentation des notices
- ✓ Approbation des conditions

## K.Websign® : comment ça marche ?



## K.Websign® : comment ça marche ?



## Bénéfices pour l'utilisateur : un processus de conclusion simplifié, immédiat et gratuit

**1** Simple

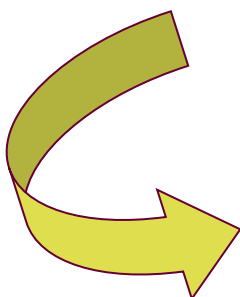
**Une souscription en 2 clics !**

**2** Immédiat

**Une activation du service immédiate**

**3** Gratuit

**Pas de frais postaux**



### Applications

- Souscription en ligne
- Télé-Déclaration
- Signatures de contrat (workflow)
- Preuve AR
- Avenants de contrat ...

## Bénéfices pour l'offreur : vendre mieux et à moindre coûts

**1** Vendre mieux ...

- Conclure de façon simple et immédiate
- Accélérer le cycle de vente
- Augmenter les taux de transformation

**2** ... à moindre coûts

- Améliorer la collecte des conventions
- Supprimer les frais de dossiers papiers

**3** Fidéliser

- Renvoyer une image innovante
- Proposer de nouvelles offres
- Etre en contact « temps réel »

# Ils nous font confiance ...



# Merci

**Anne MURGIER**

anne.murgier@keynectis.com

11-13 rue René Jacques - 92131 Issy-les-Moulineaux Cedex France

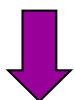
+33 1 55 64 22 34 - [www.keynectis.com](http://www.keynectis.com)

# Enjeux de l'authentification forte pour les citoyens dans l'usage des services publics en ligne

Hervé Le Bars  
DGME

## INNOVATION

- **organisation centrée sur l'utilisateur**
  - Un département par cible (part, pro, colloc, asso)
  - Une mission méthode
- **objectif : le marketing de l'Administration**
  - Ecoute active usagers pour connaître les priorités
  - Analyse des attentes des usagers
  - Identification des leviers d'amélioration
  - Propositions pour un meilleur service au meilleur coût

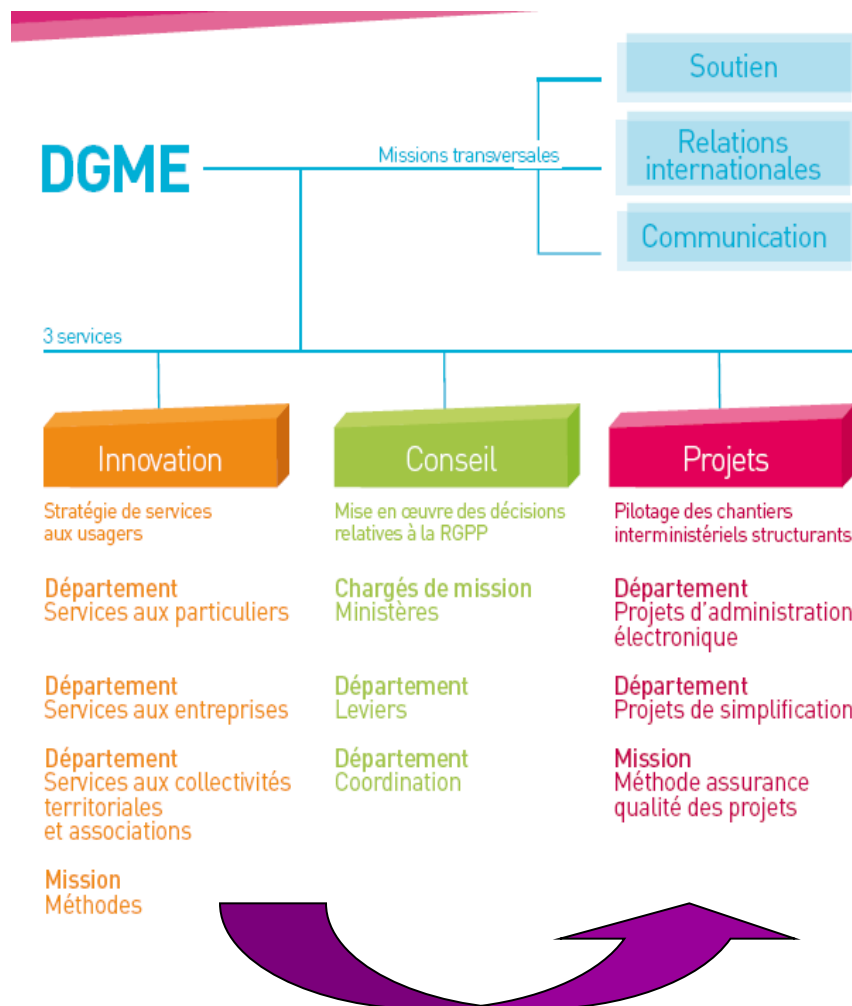


**Mandat (visa DGME)**



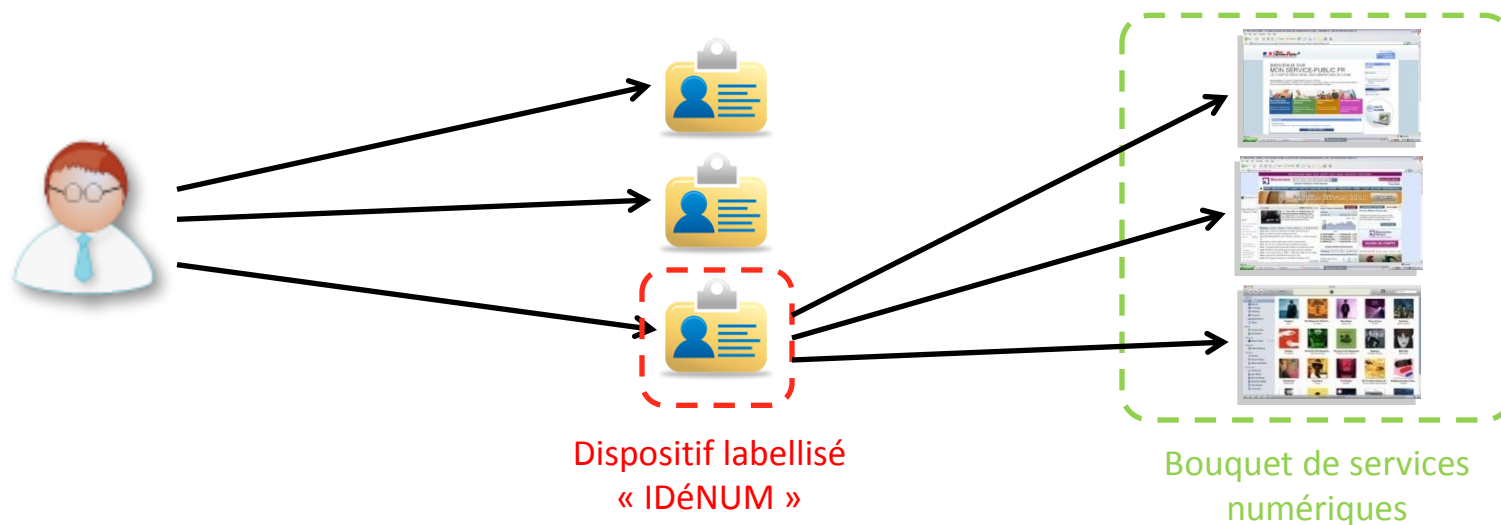
## PROJETS

- **organisation en mode projet**
  - Un département Simplification (Lean)
  - Un département Administration Electronique
  - Une mission Méthode Assurance Qualité
- **objectif DPAE : le « delivery » au label CQFD**
  - Développement rapide
  - Industrialisation de la production



Un individu **possède plusieurs identités** numériques, ...

... une identité permet d'**accéder à un bouquet de services en ligne**.



Un dispositif matérialise **une seule identité** numérique de l'usager.

Un individu pourrait avoir **plusieurs dispositifs**, chacun représentant une identité.

Un moyen d'authentification simple et à la portée de tous  
supérieur au login / password et moins contraignant que des certificats.

The screenshot displays the 'Portail Service Public' website. At the top, it features the French Republic logo and the text 'Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE'. Below this is a navigation bar with 'Accueil' and 'Portail Service Public'. The main content area is divided into several sections:

- Login:** A section titled 'Connexion' with a prompt 'Veuillez saisir votre login et mot de passe.' It includes input fields for 'Login' and 'Mot de passe', checkboxes for 'Authentification avec double code' and 'Téléphone perdu ou volé', and a 'Connexion' button.
- Nouveau compte:** A section titled 'Inscription' with the text 'Créez votre compte dès maintenant' and a 'M'inscrire' button.
- Infos Election:** A section featuring an image of hands holding a ballot and a list of candidates: Charles Baudelaire, Guy De Maupassant, Jean-Jaques Rousseau, Victor Hugo, and Vote Blanc.
- Currency Converter:** A section with a 'Convert' button, a '1.0' input field, and dropdown menus for 'USD' and 'EUR'. Below it is a table of currencies:
 

Currency	British Pound (GBP)	Chinese Yuan (CNY)	Euro (EUR)	Japanese Yen (JPY)	U.S. Dollar (USD)
- RSS:** A section with a title 'Elections Régionales - LeMonde.fr' and several news items with timestamps and links.
- À la une - Google Actualités:** A section with a title 'Rapport Clotti: Nicolas Sarkozy veut durcir le ton sur l'exécution' and a small image of Nicolas Sarkozy.

## Un moyen de signature de formulaires et de vote électronique.

**mon. Portail Service-Public**  
Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE

Accueil Ma vie citoyenne **Mes démarches** Mes documents Mon compte

Portail Service Public > Mes démarches

**Déclaration de cession**

[Cerfa usager](#)

**Etape 1**

Pour effectuer la déclaration de cession/cession pour destruction d'un véhicule, veuillez télécharger le formulaire n°13754\*01 (format PDF, ouverture dans une nouvelle fenêtre).

Accès formulaire n°13754\*01

**Etape 2**

Une fois celui-ci complété et sauvegardé, vous pouvez le téléverser ici. Vous serez ensuite identifié via le procédé "Certificat".

Formulaire n°13754\*01

**DAACT**

DAACT

Démarrez la saisie du D.A.A.C.T

**mon. Portail Service-Public**  
Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE

Accueil **Ma vie citoyenne** Mes démarches

Portail Service Public > Ma vie citoyenne

**Vote**

[Vote ouvert](#)

☐ Charles Baudelaire

☐ Guy De Maupassant

☐ Jean-Jaques Rousseau

☐ Victor Hugo

☐ Vote Blanc

Choisissez un candidat (ou vote blanc) et cliquez sur "Voter"

# Merci

**Hervé LE BARS**

[herve.le-bars@finances.gouv.fr](mailto:herve.le-bars@finances.gouv.fr)

64-70 allée de Bercy – 75572 PARIS cedex 12

[mon.service-public.fr](http://mon.service-public.fr)

## Echanges & Questions

Le téléphone mobile  
est une clé de sécurité incontournable.

# Merci

Le téléphone mobile  
est une clé de sécurité incontournable.

Informations complémentaires  
[contact@certificall.net](mailto:contact@certificall.net) [www.certificall.net](http://www.certificall.net)