

L'authentification par téléphones mobiles et smartphones





Les enjeux du e-Commerce mondial

- Dès 2006, la barre des 100 millions d'acheteurs européens en ligne devrait être dépassée. Avec un montant d'achats de 1000 € en moyenne sur l'année, il en résulte un marché du commerce électronique qui va dépasser la barre symbolique des 100 milliards €.
 - Selon Forrester, qui prévoit une forte croissance pour les 5 années à venir, le commerce électronique en Europe devrait atteindre en 2011 : 263 milliards € et 174 millions d'acheteurs en ligne.
 - Plus de 2 milliards de téléphones mobiles
 - Plus d'1 milliard de PC raccordés à l'Internet haut-débit
- Désormais, plus d'1 internaute sur 2
effectue des achats en ligne.**
- Des internautes quasiment tous équipés de téléphones mobiles



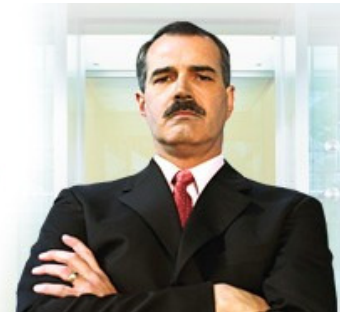
Les enjeux du e-commerce mondial

- Nous savons que le commerce électronique « B to C » est promis à un bel avenir.
- Mais un point essentiel, le point crucial du commerce électronique n'est toujours pas résolu...
- En effet, l'essor de ce commerce bute sur un problème majeur :
 - la validité des transactions.
- Cette validité des transactions passe par :
 - l'authentification du client.
- De même, la confiance dans cette transaction nécessite des garanties tant en livraison qu'en paiement.



L'authentification : clé de voûte de la sécurité

Identify
yourself



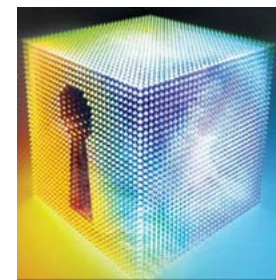
Les enjeux du e-commerce mondial

C'est aussi une meilleure sécurité, notamment au niveau du paiement en ligne, qui renforce la confiance des utilisateurs et augmente le marché du commerce numérique :

- Confidentialité des ordres et des informations de paiement
- Intégrité de toutes les données transmises
- **Authentification** du porteur de carte
- **Authentification** du commerçant
- Protection de tous les intervenants impliqués dans la transaction de commerce numérique
- Interopérabilité entre les fournisseurs de l'infrastructure logicielle et réseau



L'authentification : clé de voûte de la sécurité



La sécurité du e-commerce mondial

- La solution proposée à l'heure actuelle pour sécuriser le paiement en ligne repose sur l'usage de son numéro de carte bancaire (en France notamment) et le chiffrement de sa communication au serveur par SSL.
- Mais SSL n'authentifie pas le porteur de la carte !
- Le numéro de CB n'est qu'un semi-secret que l'on peut recopier ou générer :
 - N'importe qui peut utiliser le vôtre !
- Dans le commerce classique, une signature manuscrite ou mieux la frappe de votre code PIN garantit le commerçant que vous êtes bien le porteur de la carte :
 - Pas de signature ni de code PIN sur Internet !
- Le système fonctionne tant que la fraude ne se généralise pas.



+



= **sécurité très relative**

WEB

L'authentification : clé de voûte de la sécurité

La sécurité du e-commerce mondial

- Pendant des années, la plupart des solutions ont essayé de résoudre le problème précédent et prévoyaient un déploiement massif de cartes à puces dans les foyers.
- Ce déploiement a été maintes fois annoncé, mais ne s'est jamais réalisé (échec de Cybercom) !
- Aujourd'hui, les PC et les portables de base vendus au grand public ne comportent toujours pas de lecteur de carte à puce intégré.
- Le système reste vulnérable par certaines attaques d'implémentation sur cartes à puce (timing attack, Differential Power Analysis...)
- Le coût d'un lecteur de carte à puce varie :
 - de 10 € pour un lecteur de base (vulnérable)
 - > à 50 € pour un lecteur vraiment sécurisé
- Cette solution « carte à puce » se heurte à des problèmes que l'on essaie toujours de résoudre par boîtier connectable, téléphone à triple lecteur...
- Sans compter les coûts de déploiement.



La sécurité du e-commerce mondial

- Parmi les solutions viables dans le domaine du paiement en ligne :

La facturation des achats de l'internaute sur sa facture télécom fixe ou mobile.

- L'authentification de l'utilisateur est finalement confiée au soin de l'opérateur télécom :
 - aucun système d'authentification n'est imposé
 - aucune technologie d'authentification n'est imposée
- Il reste le choix du mode d'authentification et de son support physique (authentification à 2 facteurs) !

La sécurité du e-commerce mondial

- Cette solution doit pouvoir fonctionner avec des matériels déjà largement déployés comme les clés USB à mémoire... mais pas seulement.
- Car chacun d'entre nous possède aujourd'hui un lecteur de carte à puce sans le savoir.
- Il n'est pas dans notre ordinateur...
- Mais dans notre téléphone mobile
- Ou notre smartphone...



Les mobiles et les smartphones



Que trouve-t-on dans ces téléphones mobiles ?

- Des puces spécifiques (SIM) qui constituent des environnements semi-scellés.
- Ils peuvent recevoir des programmes JAVA.
- Aujourd'hui, nous avons porté notre technologie XC sur ce support détenu par tous.
- Le téléphone mobile de monsieur tout le monde devient :
 - un terminal de paiement individuel,
 - un support d'authentification forte.
- Il n'est donc plus nécessaire de déployer des lecteurs de cartes à puce coûteux :
 - lecteur sécurisé, donc prix élevé,
 - installation d'un appareil avec les coûts induits, assistance, dépannage...
- Car la quasi-totalité des internautes sont déjà équipés d'un mobile... et savent s'en servir.



Utilisation en entreprise

- Au même titre que le téléphone mobile peut être utilisé pour le paiement en ligne, il peut aussi être utilisé en entreprise pour l'authentification des utilisateurs :
 - ☞ Intranet, Extranet, Internet
- Mais aussi pour la consultation directe d'informations privées sur l'écran de son téléphone.



Quelques champs d'application



Site marchand



Entreprise

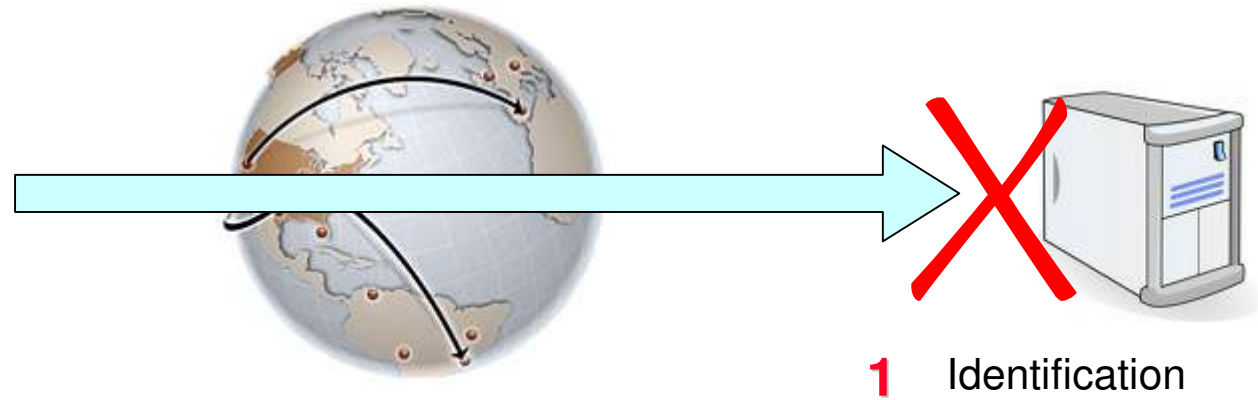


Administration



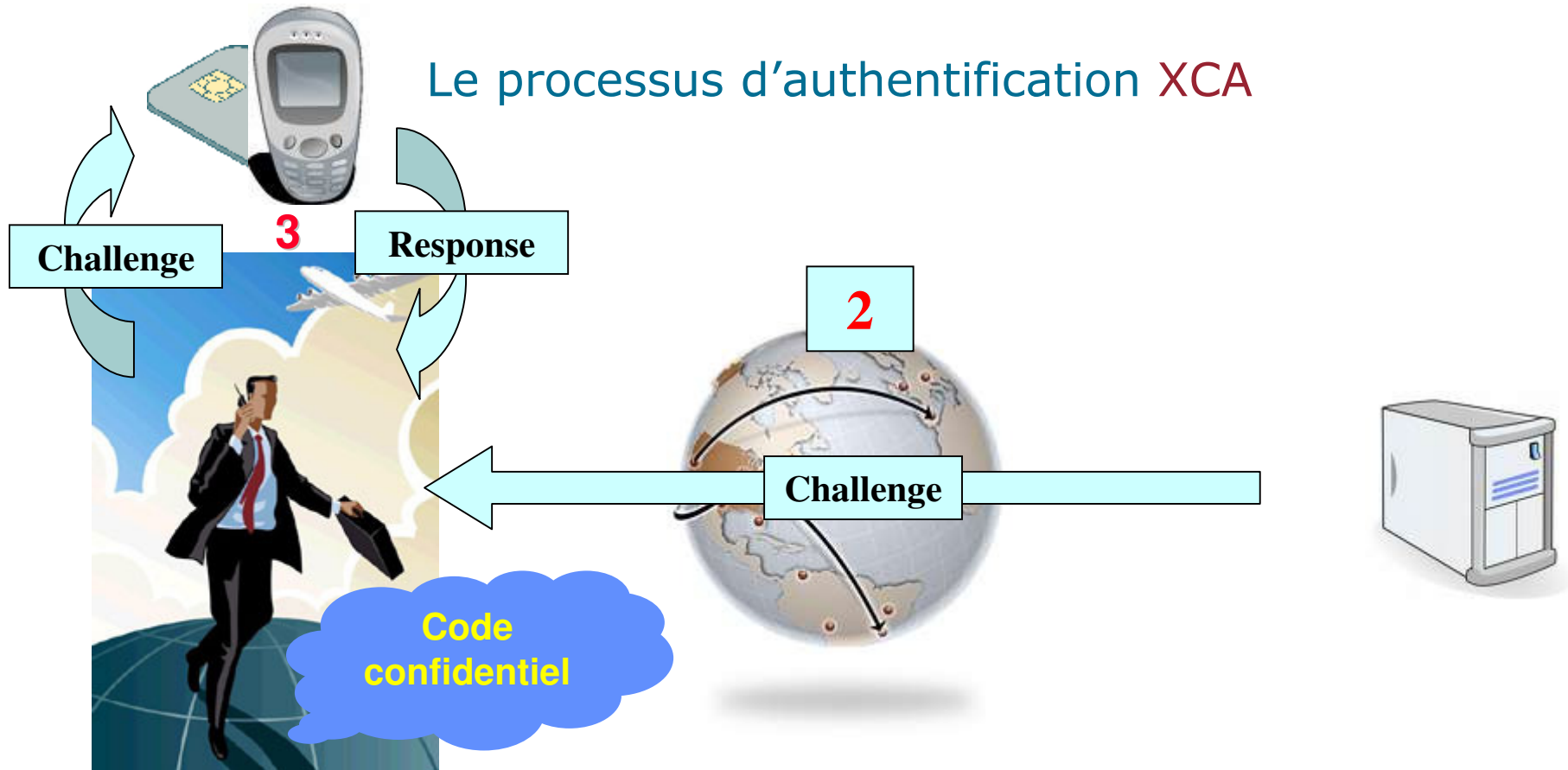
Banque

Le processus d'authentification



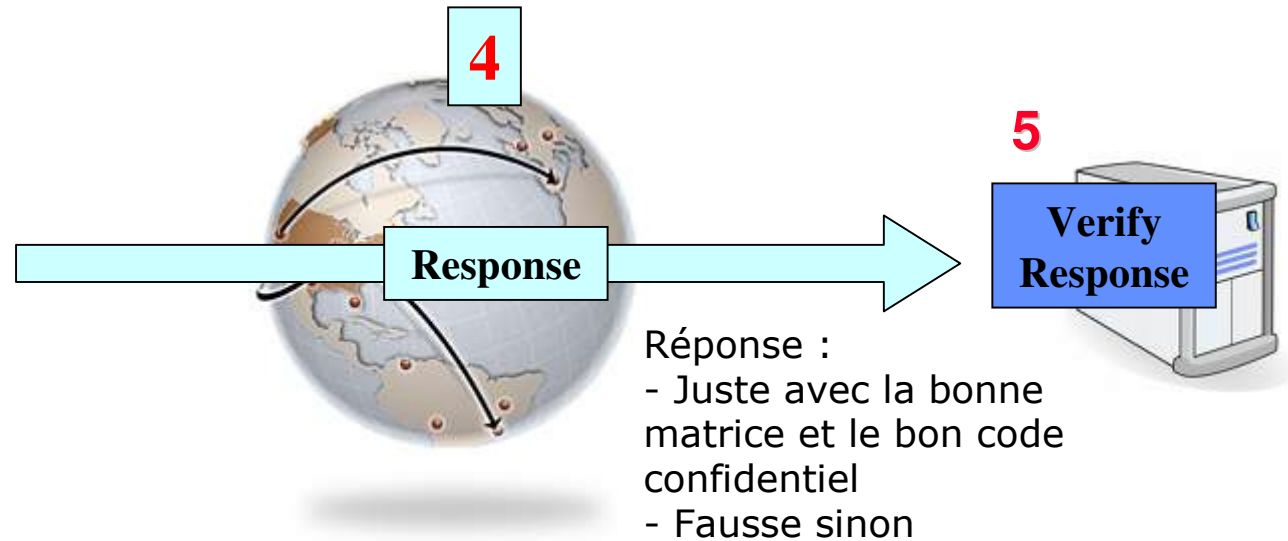
Une simple authentification par identifiant + mot de passe statique (même haché ou chiffré) ne suffit plus. Il faut que ce mot de passe change à chaque transaction pour ne pas pouvoir être rejoué.

Le processus d'authentification XCA



Le meilleur protocole pour obtenir un mot de passe à usage unique (OTP) est le protocole défi-réponse. Il est très sûr et évite tous les problèmes de synchronisation.

Le processus d'authentification XCA



Si le téléphone portable est perdu, volé ou emprunté, personne ne pourra jamais retrouver le code confidentiel de l'utilisateur !

Le processus d'authentification XCA



Pas d'usurpation possible d'identité avec XC

Un achat en ligne par téléphonie mobile



L'authentification : clé de voûte de la sécurité

© NTX research, 2004-2009

L'inscription

1. Le client souscrit au service « paiement par téléphone » auprès de l'opérateur télécom.
2. Il donne à l'opérateur l'autorisation de prélever son compte bancaire du montant de ses achats en ligne **validés à l'aide de son mobile**.
3. Le client télécharge le module d'authentification **XCA** sur son **téléphone mobile** ou son smartphone (midlet java).
4. Le client personnalise son module (matrice spécifique) en activant son compte avec le code reçu par courriel.
5. Enfin, le client choisit et paramètre son propre code confidentiel **inviolable** car non stocké dans le téléphone ni envoyé au serveur.



Un achat en ligne



**Acheteur
Internaute**

L'acheteur choisit articles/services et :
- donne son n° de téléphone portable
- donne l'adresse de livraison
(physique ou numérique)

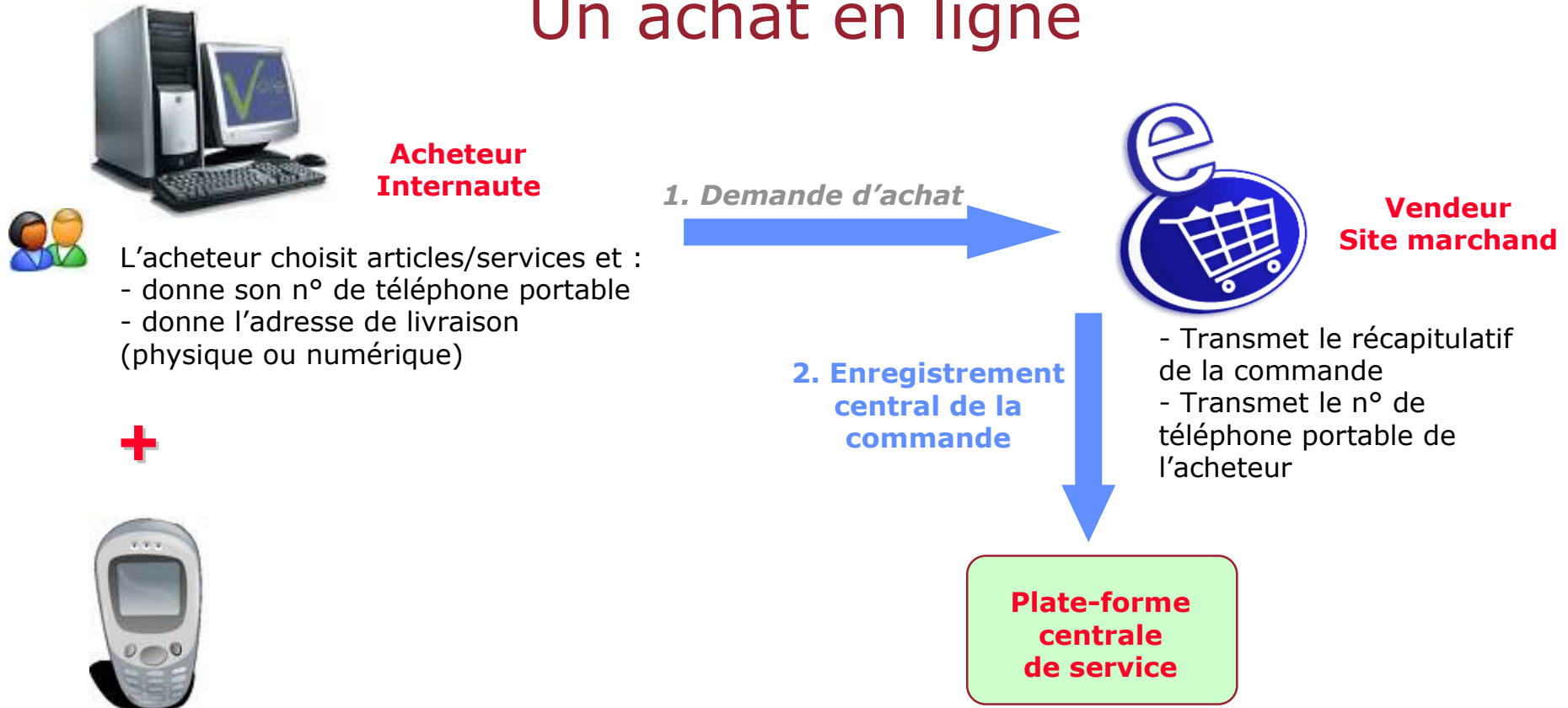
1. Demande d'achat



**Vendeur
Site marchand**



Un achat en ligne



Un achat en ligne



Acheteur Internaute

L'acheteur choisit articles/services et :

- donne son n° de téléphone portable
- donne l'adresse de livraison (physique ou numérique)

Vendeur Site marchand

- Transmet le récapitulatif de la commande
- Transmet le n° de téléphone portable de l'acheteur

3. Authentification de l'acheteur

Identifiant (n° de téléphone)

Défi

Réponse

Plate-forme centrale de service

a) Vérifie l'identité, le n° de téléphone et l'adhésion au service.
b) Authentifie l'utilisateur avec **XC**

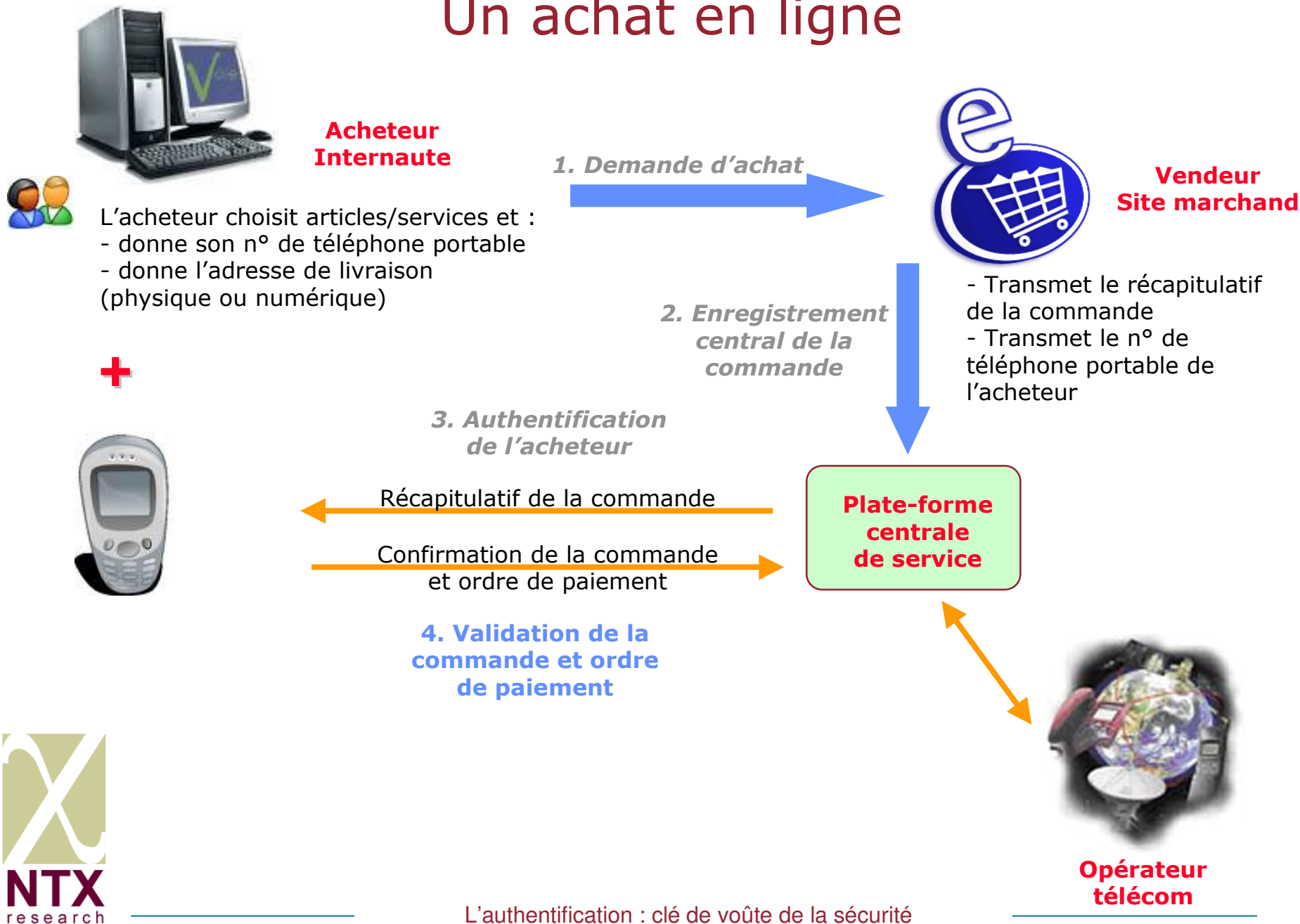
L'acheteur s'authentifie auprès de la plate-forme centrale en mode défi-réponse avec la saisie de son code confidentiel

(Transferts chiffrés)

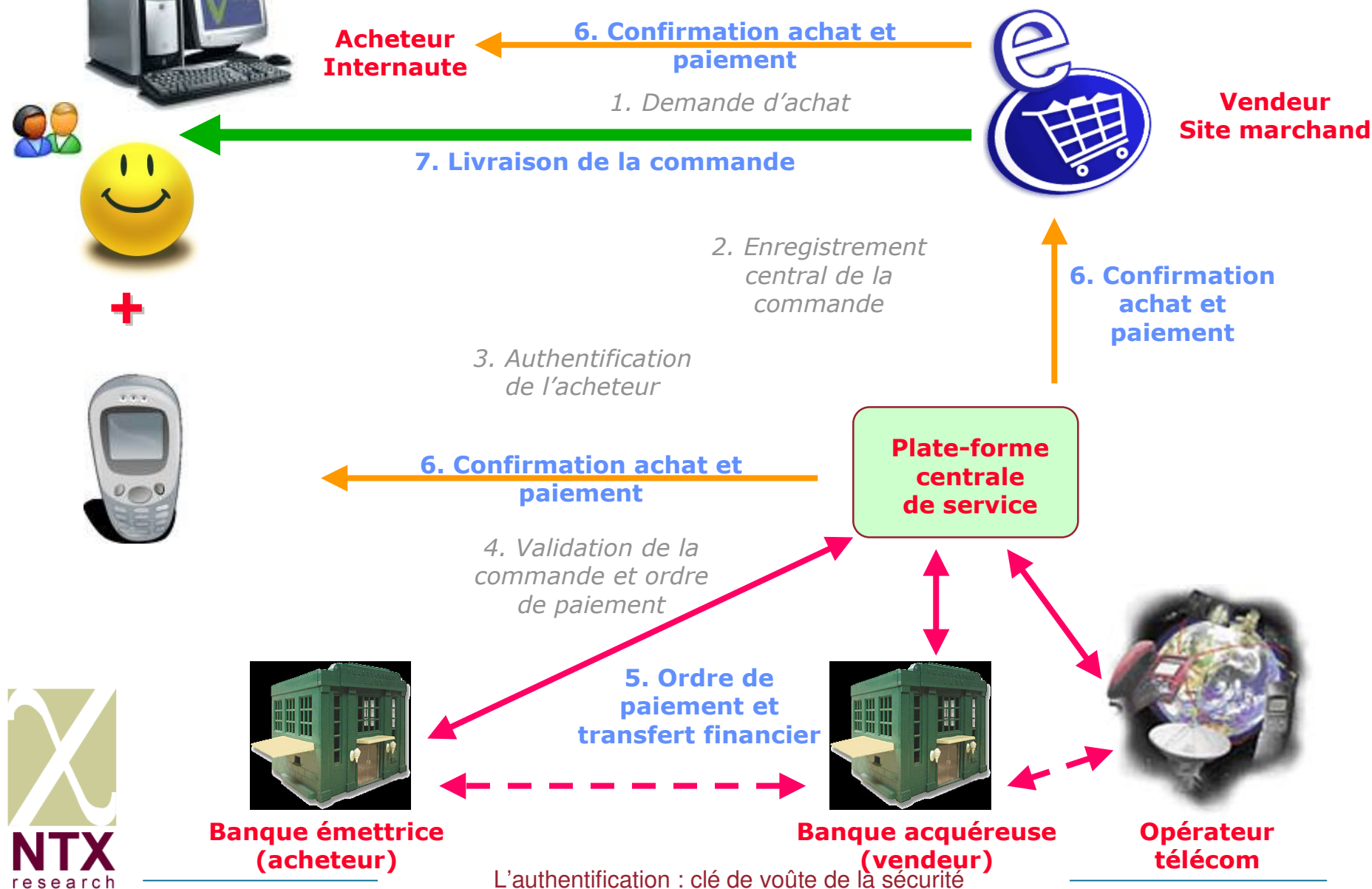
L'authentification : clé de voûte de la sécurité

Opérateur télécom

Un achat en ligne



Un achat en ligne



L'authentification : clé de voûte de la sécurité

Un achat en ligne

- Un double canal pour plus de sécurité
 - Internet xDSL pour le PC.
 - Internet GPRS ou 3G pour le téléphone portable.
- Notre **technologie XCA** est aujourd'hui la seule adaptée à un environnement semi-scellé.
- Peu importe le terminal web utilisé (PC, PDA, mobile...)
- Plus d'utilisation du numéro de carte bancaire pendant la transaction.
- A titre de rappel, la fraude au paiement sur Internet augmente tous les ans de plus de 10%.

Un code confidentiel :

- choisi par l'utilisateur
- mémorisable
- modifiable à volonté
- inviolable

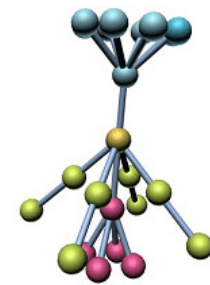


Structure matérielle

- **En terme de structure matérielle, les seuls équipements importants se trouvent sur la plate-forme centrale de service :**
 - **Bases de données**
 - **Serveur de gestion des commandes (validation) : Services Web**
 - **Serveur d'authentification XCA de NTX Research**
 - **Liens sécurisés avec les opérateurs et le système bancaire**
- **Chez les sites marchands, un seul service de redirection (web service).**
- **Chez le client, aucune installation à l'exception du téléchargement et de l'activation d'une midlet java sur son mobile ou smartphone.**
- **Pas de double/triple lecteur de carte à puce.**
- **L'utilisation de la carte SIM rendra indépendant vis à vis du téléphone portable employé (nouvelle génération).**
- **Coût minime.**
- **Déploiement instantané.**
- **Sécurité élevée.**



L'authentification : clé de voûte de la sécurité



Sécurité élevée

- La fraude, l'escroquerie nécessitent la mise en place de solutions complexes :
 - Ecoute de la transaction d'achat xDSL
 - Ecoute de la transaction de validation
 - Décrypter la transaction d'achat chiffrée par SSL
 - Décrypter la transaction de validation chiffrée par Blowfish (ou AES)
 - Compromettre le protocole défi-réponse
 - Retrouver le code confidentiel du client stocké nulle part
- La conjugaison de ces différents éléments rend bien évidemment impossible l'escroquerie classique par utilisation du numéro de carte bancaire.
- En effet, celui-ci n'est plus utilisé dans la transaction décrite.



Conclusion (1)

- Les solutions "propriétaires" ne concernent qu'un nombre limité d'acteurs (acheteurs, vendeurs et institutions financières) et imposent une limitation considérable de la portée et donc de la valeur du service.
- Les solutions classiques "universelles" de type SET (Secure Electronic Transaction) ou C-SET (Chip-SET) impliquent la création de véritables "usines à gaz" à l'échelle de la planète et empêchent la mise en place rapide du système.
- Les solutions "d'avant-garde" qui visent à la création d'un véritable nouveau modèle économique et financier fondé sur la création d'une véritable « monnaie digitale » sont bloquées par le système actuel dont la refonte globale n'est pas envisageable, même à moyen terme.



Conclusion (2)

- A contrario, la solution proposée atteint les objectifs suivants :
 - Universalité de la portée du service : chaque consommateur accède directement à l'offre complète du magasin planétaire, chaque commerçant a la possibilité de vendre au plus grand nombre
 - Simplicité de mise en place, de mise en œuvre et de déploiement à grande échelle
 - Adaptabilité au système économique, financier, législatif, technologique, sociologique et culturel existant



Conclusion (3)



L'innovation conceptuelle consiste à généraliser l'utilisation des téléphones "portables" des personnes physiques comme terminal de paiement universel pour les transactions du commerce numérique :

- **Aujourd'hui, ce sont les commerçants qui proposent l'usage aux consommateurs des terminaux de paiement électroniques loués aux institutions financières telles que le Groupement Cartes bancaires.**
- **Demain, chaque consommateur possèdera son propre terminal de paiement dont il aura la libre et entière disposition.**



L'innovation technologique est conduite suivant trois axes principaux :

- **La nouvelle définition des rôles des différents acteurs dans les transactions de paiement du commerce électronique et notamment des opérateurs télécom.**
- **La création d'un protocole original de stockage, de traitement et de flux d'informations économiques et financières entre ces différents acteurs.**
- **L'utilisation d'une technique cryptographique inédite de sécurisation et de protection des serveurs de paiement, des terminaux de paiement et des échanges numériques au sein du nouveau système, ainsi qu'entre ce système et son environnement**

Le socle de la confiance dans le e-Commerce...

Confiance

Authentification
forte de l'utilisateur

Intégrité de la transaction



Non-répudiation de la transaction





Contacts

Pascal Thoniel, CEO-CTO

thoniel@ntx-research.com

Francis Melemedjian, VP sales

melemedjian@ntx-research.com

Marie-Maxence Angleys, VP marketing & communication

angleys@ntx-research.com

*

NTX Research SA

111 avenue Victor Hugo

75116 Paris (France)

+33 1 47 66 39 85

<http://www.ntx-research.com>



L'authentification : clé de voûte de la sécurité

© NTX research, 2004-2009