



Sécuriser le e-Commerce avec la technologie XCA



« Une sécurité qui inspire la confiance »

© NTX Research, 2007-2009



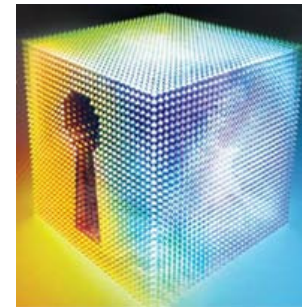
Les enjeux du e-Commerce mondial

- Dès 2006, la barre des 100 millions d'acheteurs européens en ligne a été dépassée. Avec un montant moyen d'achats de 1000 € par an, il en résulte un marché du commerce électronique qui franchit la barre symbolique des 100 milliards €.
- Forrester prévoit une forte croissance pour les 5 années à venir : en 2011 le commerce électronique en Europe devrait atteindre 174 millions d'acheteurs en ligne et 263 milliards € de CA.
- 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 et de smartphones.



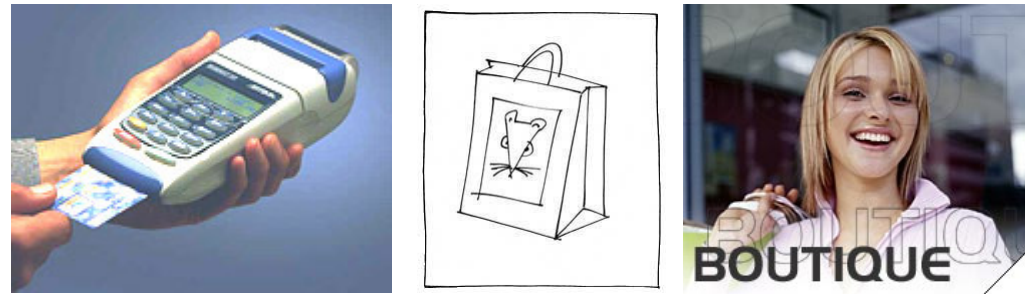
Instaurer la confiance dans le e-Commerce mondial

- Accompagner et promouvoir le e-Commerce c'est aussi sécuriser ses modes de paiement.
- Aujourd'hui la Carte Bancaire représente plus des 2 tiers des modes de paiement utilisés... et sa part continue de progresser.
- Ce paiement doit être :
 - Sûr
 - Facile à mettre en œuvre
 - Multi-canal (web, mobile...)
 - Avoir un faible coût

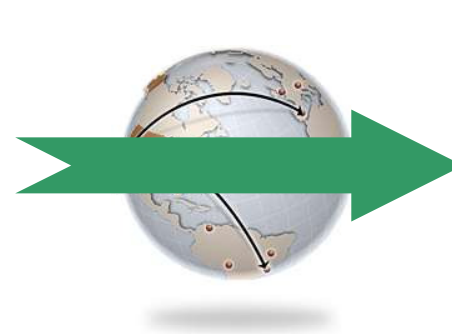


Les 2 formes du paiement sécurisé

- Dans le monde **physique**, la vente de proximité dans une boutique se conclut par un « paiement de proximité »

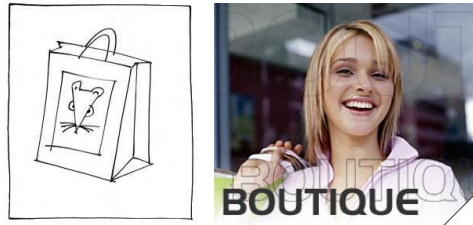


- Dans le monde **numérique**, la vente à distance sur un site Internet se conclut par un « paiement à distance »



« Une sécurité qui inspire la confiance »

Le paiement de proximité



- Le paiement de proximité va évoluer vers plus de facilité pour le client/acheteur et pour le commerçant/vendeur :
 - Evolution des TPE vers le « sans contact »
 - Utilisation des téléphones mobiles dotés d'une puce NFC et d'un module logiciel EMV
- Horizon 2010 :
 - Les expérimentations ont déjà débutées (Strasbourg, Caen...)
 - les mobiles commencent à être équipés en 200
 - En 2010 1/3 des téléphones seront opérationne



Le paiement à distance



- La solution proposée à l'heure actuelle pour sécuriser le paiement à distance repose sur la communication de son numéro de Carte Bancaire et son envoi au serveur, chiffré 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 !**
- Ce système fonctionne tant que la fraude ne se généralise pas.

Le paiement à distance



WEB

Ce système doit évoluer !

C'est le rôle des banques de proposer et de mettre à disposition des outils de paiement adaptés aux nouveaux modèles de distribution.

La sécurité du paiement à distance

- Pendant des années, la plupart des propositions ont essayé de résoudre le problème précédent en prévoyant 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 et lecteurs locaux.
- Le coût d'un lecteur de carte à puce vraiment sécurisé reste élevé, sans compter les coûts de déploiement.
- Cette solution « carte à puce » se heurte à des problèmes que l'on essaye toujours de résoudre sans succès par boîtier connectable, téléphone à triple lecteur, etc.



« Une sécurité qui inspire la confiance »



La nouvelle sécurité du paiement en ligne

- Enfin, il semble qu'une initiative commune récente (2002 aux USA puis 2005 en France) soit vraiment porteuse d'avenir dans le domaine du paiement en ligne :

3-D Secure

- Une alliance qui regroupe enfin toute la communauté des Cartes Bancaires : VISA + MasterCard + JCB + Amex...
- **3-D Secure** est une architecture internationale de paiement sur Internet.
- La sécurité des données stockées/traitées/échangées est assurée par l'initiative PCI « Payment Card Industry » du côté des commerçants, des hébergeurs web, des tiers de paiement et des plate-forme de paiement.
- Mais qu'en est-il de la sécurité du côté du client/acheteur porteur de la Carte Bancaire et de sa banque ?



« Une sécurité qui inspire la confiance »



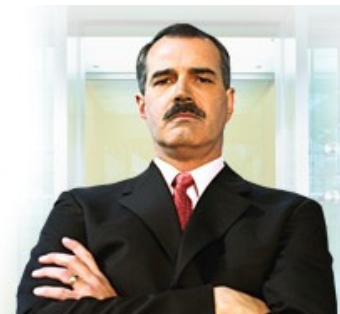
3-D Secure

- Avec 3-D Secure, l'authentification du consommateur est finalement confiée à la banque du client/acheteur, porteur de la CB :
 - aucun système d'authentification n'est imposé
 - aucune technologie d'authentification n'est imposée

Quelle solution
d'authentification forte
sera donc en mesure
de compléter idéalement
l'architecture 3-D Secure ?



Identify
yourself



« Une sécurité qui inspire la confiance »

L'authentification pour 3-D Secure

- L'authentification par « identifiant + mot de passe statique » est définitivement condamnée.
- Elle a déjà été bannie aux USA par l'administration américaine.
- Cette solution nouvelle doit être adaptable sur plusieurs supports physiques :
 - Il sera difficile d'imposer le même support d'authentification à tous
- Cette solution nouvelle ne doit pas dépendre spécifiquement d'une réalisation hardware :
 - Le coût serait prohibitif
 - Le temps de déploiement serait trop long
- Cette solution nouvelle doit permettre l'ajustement du niveau de sécurité – et donc des contraintes - aux enjeux et à la maturité des utilisateurs.



L'authentification pour 3-D Secure

- Cette solution d'authentification ne doit pas dépendre spécifiquement d'une réalisation hardware :

elle doit être logicielle.

- Cette solution doit être adaptable sur plusieurs supports physiques et fonctionner avec des matériels de faible coût ou bien déjà largement déployés :

les disques dur des portables,

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 mobile !



Les mobiles et les smartphones



Que trouve-t-on dans ces téléphones mobiles ?

- Une mémoire et une puce amovible spécifique (SIM) qui constitue un environnement semi-scellé.
- Ils peuvent recevoir des programmes JAVA.
- Notre **technologie XC** est présente depuis longtemps sur ce support détenu par tous.
- Le mobile de tout un chacun 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.
- Car la quasi-totalité des internautes sont déjà équipés de mobiles, l'ont constamment avec eux... et savent s'en servir.



« Une sécurité qui inspire la confiance »

Les 3 modes modernes de la vente à distance

1. Le mode « web-web » :

- Achat sur le Web (via un PC)
- Authentification XC par le Web (applet Java + clé USB dans le PC)



2. Le mode « web-mobile » :

- Achat sur le Web (via un PC)
- Authentification XC par le mobile (midlet Java dans le mobile)



3. Le mode « mobile-mobile » :

- Achat sur le mobile (via un PDA, mobile)
- Authentification XC par le mobile (midlet Java dans le mobile)



Les avantages de la technologie XC (#1)

- La solution d'authentification XC fonctionne dans les 3 modes de vente à distance :
web-web, web-mobile et mobile-mobile
- XC est compatible avec tous les systèmes d'exploitation et tous les navigateurs du marché (Java).
- Pas de matériel supplémentaire à installer sur les PCs, PDA et mobiles : 100 % logiciel.
- Pas de logiciel à installer sur les PCs en mode web-web (applet Java).
- XC est compatible avec tous les authentifieurs physiques.
- Le niveau de sécurité est ajustable suivant les enjeux et la maturité des consommateurs (moyen, fort, très fort).
- Sécurité renforcée contre l'écoute de ligne (pseudo masque jetable).
- Sécurité renforcée contre l'emprunt, la perte et le vol de l'authentifieur (code **inviolable**).



Les avantages de la technologie XC (#2)

- Le client/acheteur conserve sa démarche habituelle acquise lors d'un achat de proximité :
 - Saisie d'un code confidentiel facilement mémorisable.
- Le client/acheteur peut choisir son code.
- Ce code n'est pas contraint ni en taille, ni en caractères.
- Le client/acheteur peut changer son code à tout moment, « off-line » :
 - Sans le communiquer à qui que ce soit
 - Sans le stocker nulle part
- Le client/acheteur est maître de la personnalisation de sa sécurité ce qui lui procure un sentiment de confiance.
- Le client/acheteur peut bénéficier d'une option de code d'alerte sous contrainte, totalement indétectable, lorsque les enjeux sont importants.



Les avantages de la technologie XC (#3)

- La solution de sécurité XC est entièrement paramétrable et ajustable :
 - Sur le plan de la sécurité (cryptographie, stéganographie)
 - Sur le plan de son interface : mode off-line possible sur un téléphone mobile, fonctionne aussi bien en GPRS/3G qu'en mode SMS
- XC est une solution technologique 100 % française.
- XC est une solution dont les banques peuvent s'approprier la maîtrise.
- XC est une solution de sécurité mobile apportée par les banques aux opérateurs télécom.

XC est en définitive
la meilleure solution d'authentification
pour 3-D Secure !



« Une sécurité qui inspire la confiance »

Conclusion

- La solution combinée 3-D Secure / authentication XCA 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
 - Adapté au système économique, financier, législatif, technologique, sociologique et culturel existant



« Une sécurité qui inspire la confiance »

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

Confiance

**Authentification
forte du
consommateur**

**Plate-forme de paiement sécurisée
3-D Secure**



« Une sécurité qui inspire la confiance »



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>



« Une sécurité qui inspire la confiance »

© NTX Research, 2007-2009

Annexe n°1

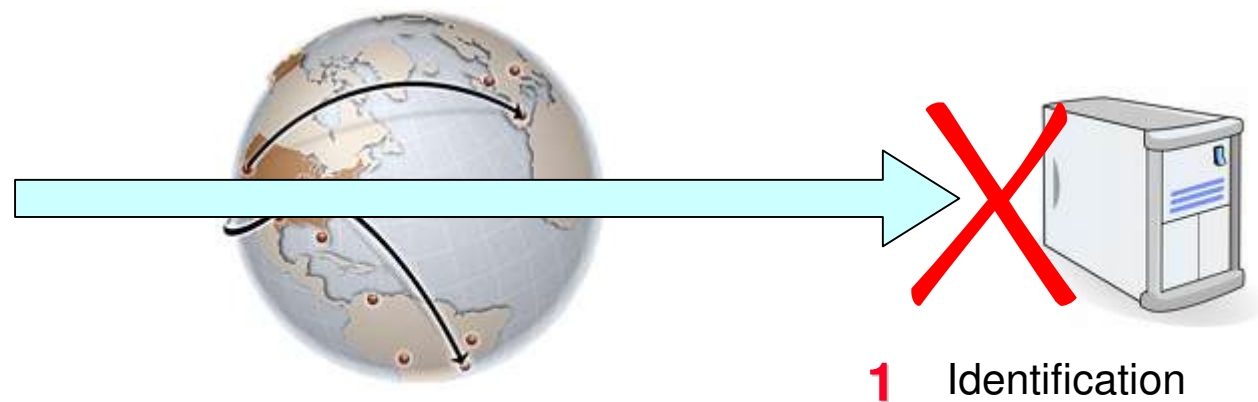
Le processus d'authentification XCA



« Une sécurité qui inspire la confiance »

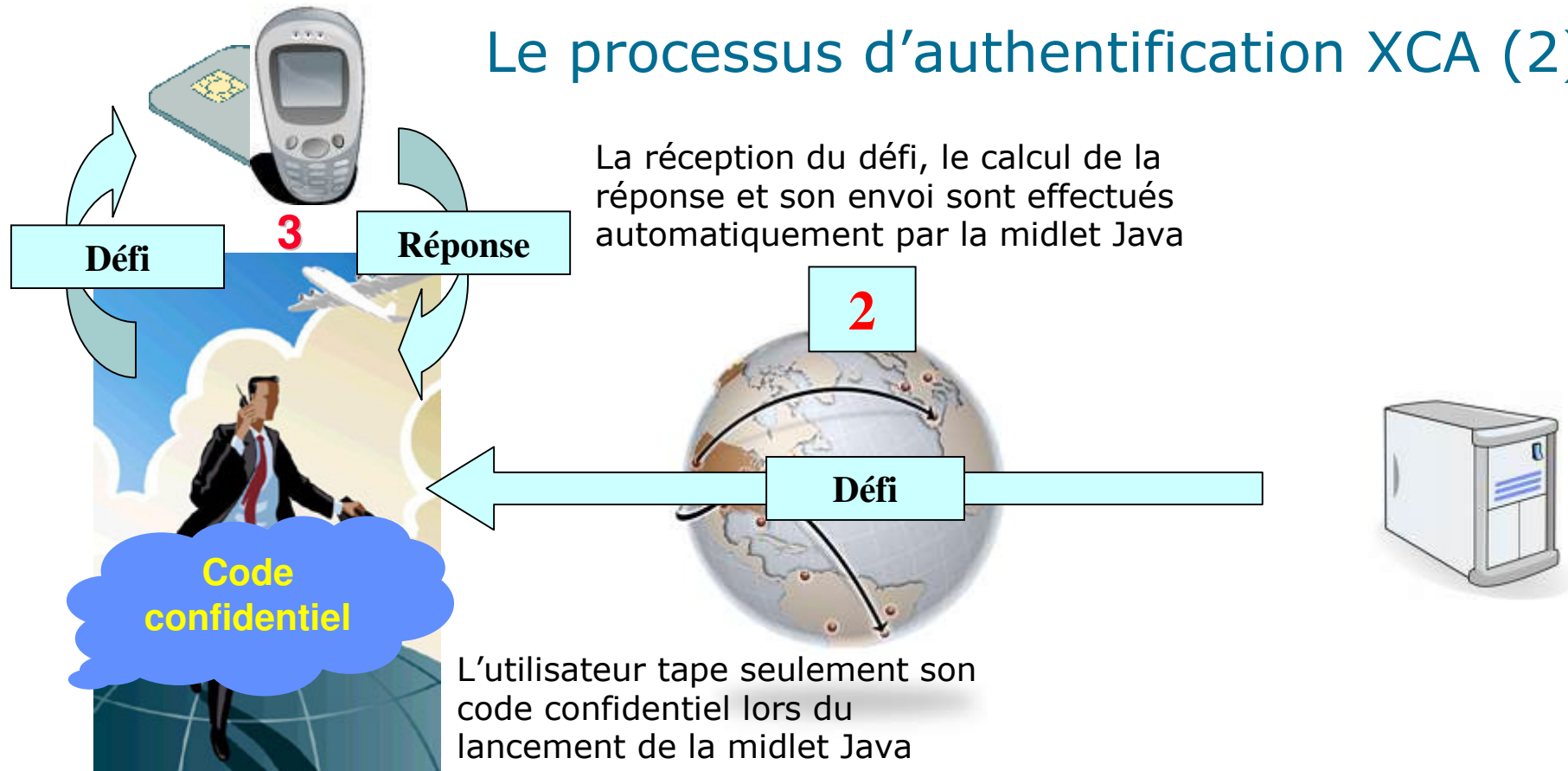
© NTX Research, 2007-2009

Le processus d'authentification (1)



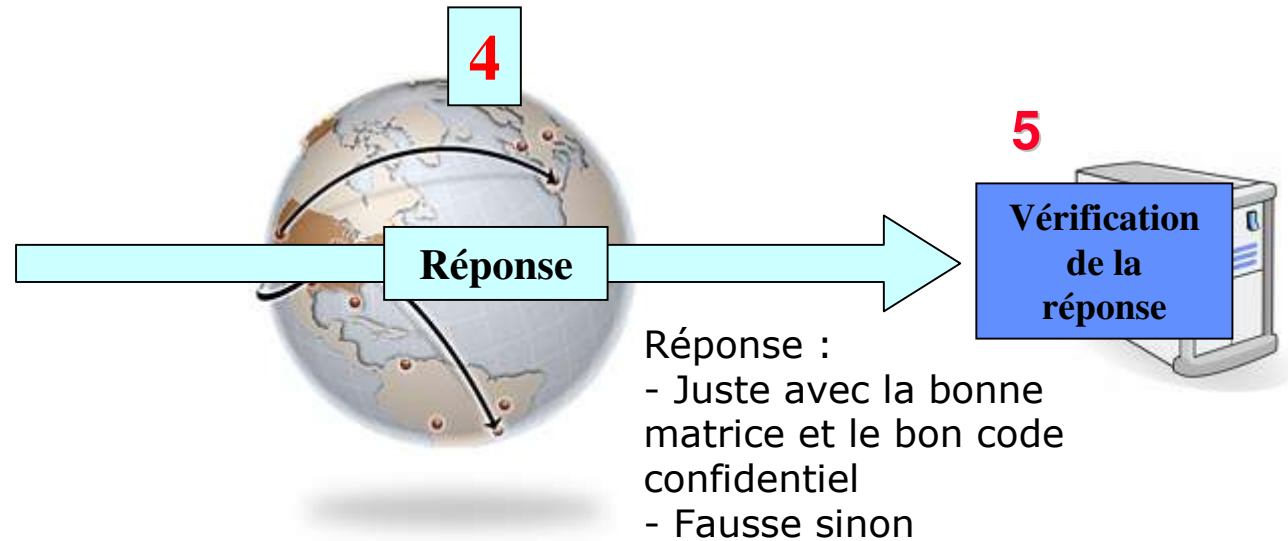
Une simple authentification par identifiant + mot de passe statique (même haché ou chiffré) ne suffit plus. Il faut que ce mot de passe change à chaque transaction pour ne pas pouvoir être rejoué.

Le processus d'authentification XCA (2)



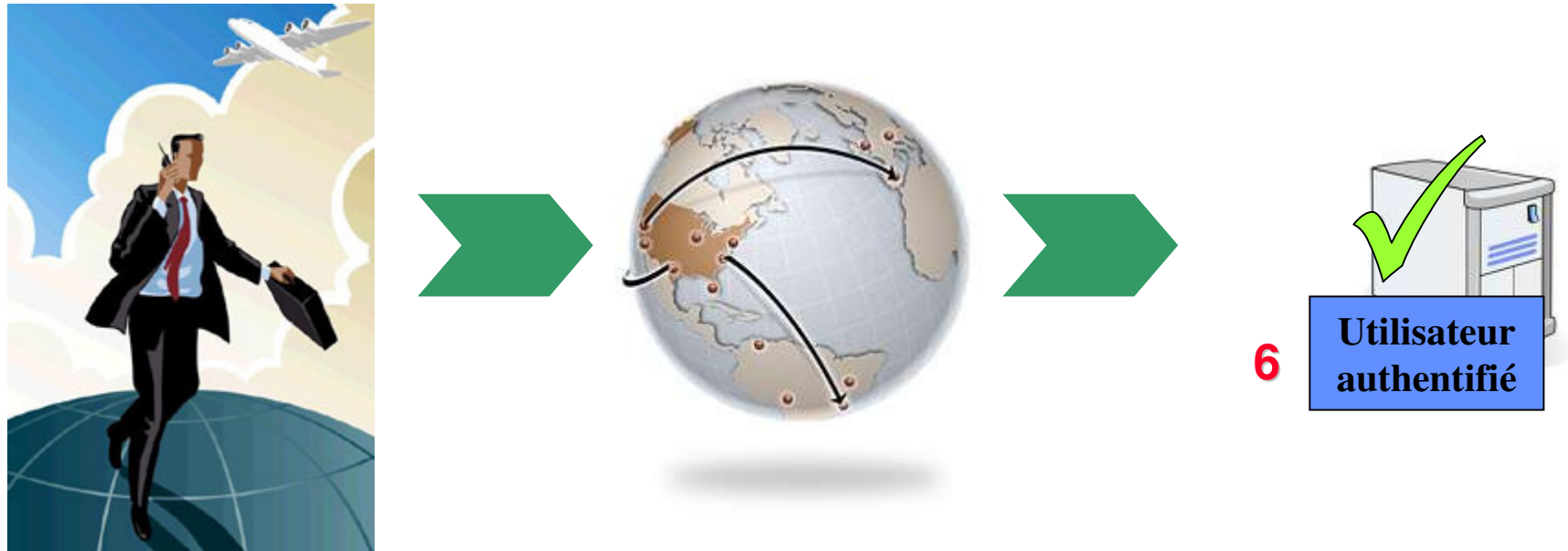
Le meilleur protocole pour obtenir un mot de passe à usage unique (OTP) est le protocole **défi-réponse**. Il est très sûr et évite tous les problèmes de synchronisation.

Le processus d'authentification XCA (3)



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

Le processus d'authentification XCA (4)



Pas d'usurpation possible d'identité avec XC :
utilisateur authentifié
= ordre de paiement validé

Annexe n°2

Initialisation du mobile avec la technologie XCA



« Une sécurité qui inspire la confiance »

© NTX Research, 2007-2009

Initialisation du mobile pour l'authentification XCA

