harmonie

GS DAYS 2015

Touch ID, OAuth, Authentification mobile,

Quelle confiance vis-à-vis de ces nouveaux mécanismes ?

…Dans un contexte de révolution digitale




www.harmonie-technologie.com
+331 73 75 08 47 – info.ssi@harmonie-technologie.com

CABINET DE CONSEIL EN SECURITE DU SI

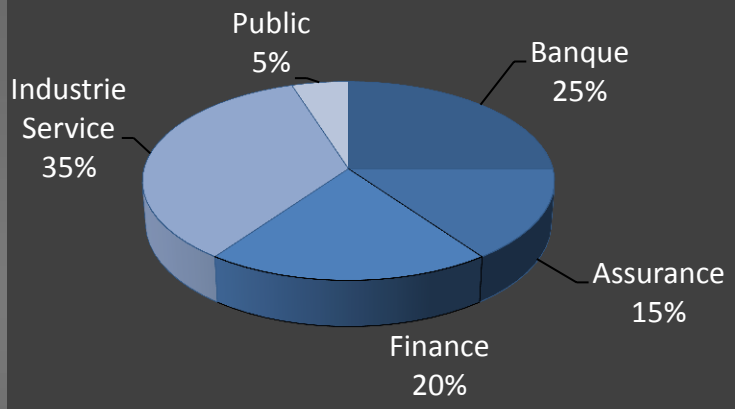
harmonie

2005-2016

Double compétence fonctionnelle et technique

AUDIT	CONSEIL	INTÉGRATION	FORMATION

Partenaire sécurité des grands comptes



Répartition de nos activités 2014 par secteur d'activité

Top 10 de nos clients

BPCE / NATIXIS
CREDIT AGRICOLE
COVEA
SOCIETE GENERALE
MALAKOFF MÉDÉRIC
CHOREGIE
THALES / ALCATEL
TOTAL
KILOUTOU
CARREFOUR

CHIFFRE CLES

Croissance organique soutenue depuis 2005 entre 20 et 30% par an

2014
65 collaborateurs et CA de 6,5 M€

Objectif 2015
80 collaborateurs et CA de 8 M€

Projection 2016
100 collaborateurs CA de 10M€

EVENEMENTS

4 DOMAINES D'EXPERTISES

harmonie

GOUVERNANCE, RISQUES & CONFORMITE

ORGANISER ET PILOTER LA SSI

Organisation et management de la sécurité Roadmap et schéma directeur SSI ; Analyse de risques ; Continuité d'activité ; Politique de sécurité et tableaux de bord SSI ; Sensibilisation; Certification ISO, PCI-DSS, HDS, etc.

GESTION DES IDENTITES & DES ACCES

MAÎTRISER LES HABILITATIONS ET ACCÈS AU SI

Gestion des habilitations ; Role management ; Audit et revue d'habilitations ; Gestion des comptes à privilèges ; Authentification, SSO, fédération d'identité

SECURITE DES APPLICATIONS & DONNEES

PROTÉGER SON PATRIMOINE INFORMATIONNEL

Intégration de la sécurité dans les projets ; Classification des actifs ; Protection des données sensibles : DLP, DRM ; Sécurité des espaces partagés, collaboratifs ; PKI, signature et chiffrement

CYBER-SECURITE

AUDITER ET SURVEILLER LA SÉCURITÉ DU SI

Audits des architectures et des développements ; Tests d'intrusion ; Patch management ; Log management / SIEM

UNE APPROCHE TRANSVERSE DE LA SSI AU SERVICE DES INNOVATIONS D'ENTREPRISE

- Mobilité et télétravail
- Digitalisation de la relation clients
- Cloud
- Objets connectés
- Etc.

AGENDA

Touch ID, OAuth, Authentification mobile,

Quelle confiance vis-à-vis de ces nouveaux mécanismes ?

→ CONTEXTE : UNE REVOLUTION EN MARCHE

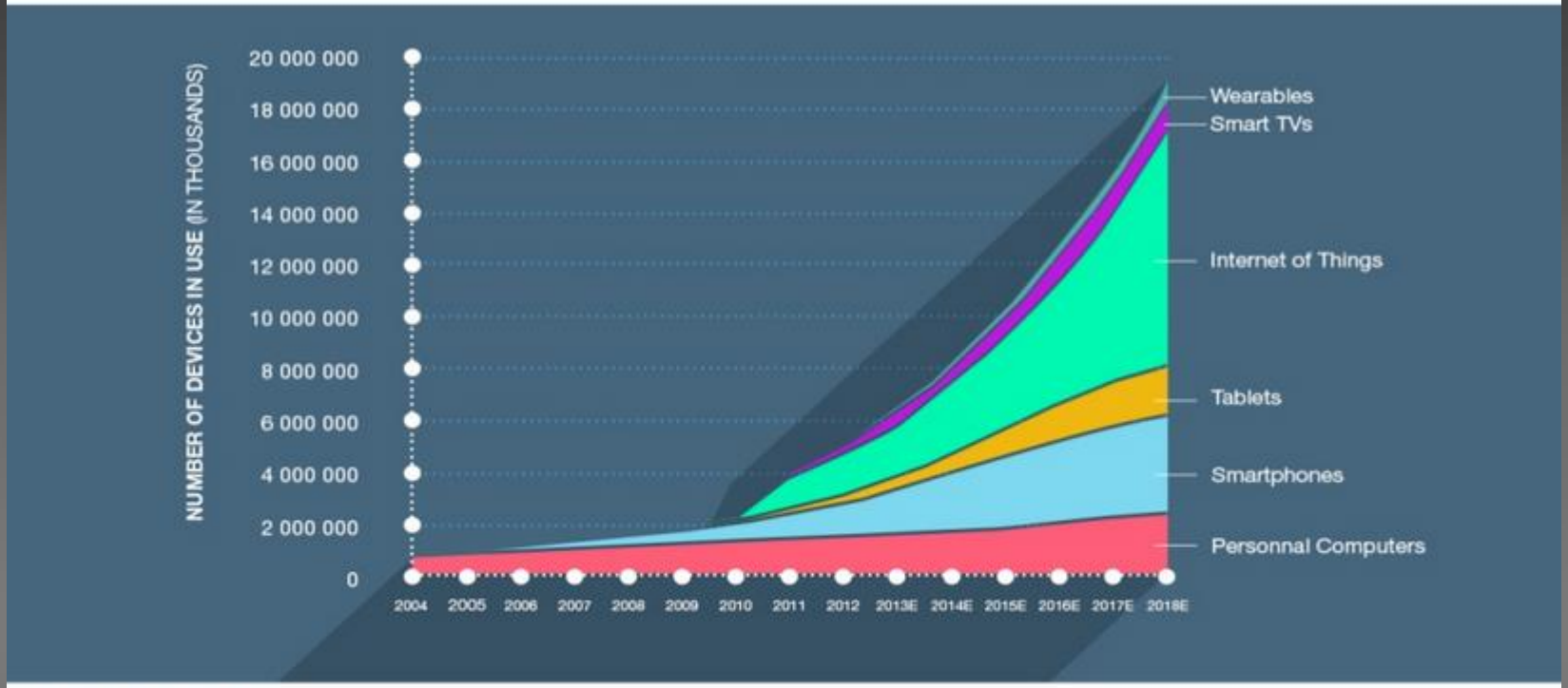
→ ANALYSE : IMPLEMENTATION D'AUTHENTIFICATIONS

→ VERS UNE STRATEGIE DE MISE EN OEUVRE

UNE DIVERSIFICATION DES DEVICES

Multiplication des objets connectés

VERS LE MOBILE EVERYWHERE & EVERYTHING



Source : BI Intelligence 2013

Repenser sa communication, les produits, la distribution

MOBILE MARKETING ASSOCIATION

RAPPEL DES MENACES

FAIRE FACE À L'EVOLUTION DES ATTAQUES SPECIFIQUES AU MOBILE

« PHISHING » D'APPLICATION MOBILE

UN TERMINAL FACILEMENT « VOLABLE », AVEC UN NIVEAU DE SÉCURITÉ « SOUVENT » DIMINUÉ

CONNEXION AU TRAVERS DE RÉSEAUX NON-SÉCURISÉS

QUELLES ATTENTES EN MATIERE DE SECURITE ?

Simplifier l'usage — **Sécurité « Réelle » et ressentie**

62%	des utilisateurs considèrent la sécurité web comme très importante *Etude opinionway pour kaspersky (juillet 2014)*	***accrocher***
67%	des utilisateurs considèrent leur identité numérique comme très importante *Même étude*	
19%	de la perte du CA est liée à une perte de clients *http://www.theguardian.com/media-network/media-network-blog/2014/apr/17/protect-business-data-loss-cyber-infographic*	***Ne pas perdre !***
72%	des entreprises qui subissent une attaque majeure arrêtent leur activité dans 24 mois qui suivent *Même étude*	

QUELLES ATTENTES EN MATIERE DE SECURITE ?

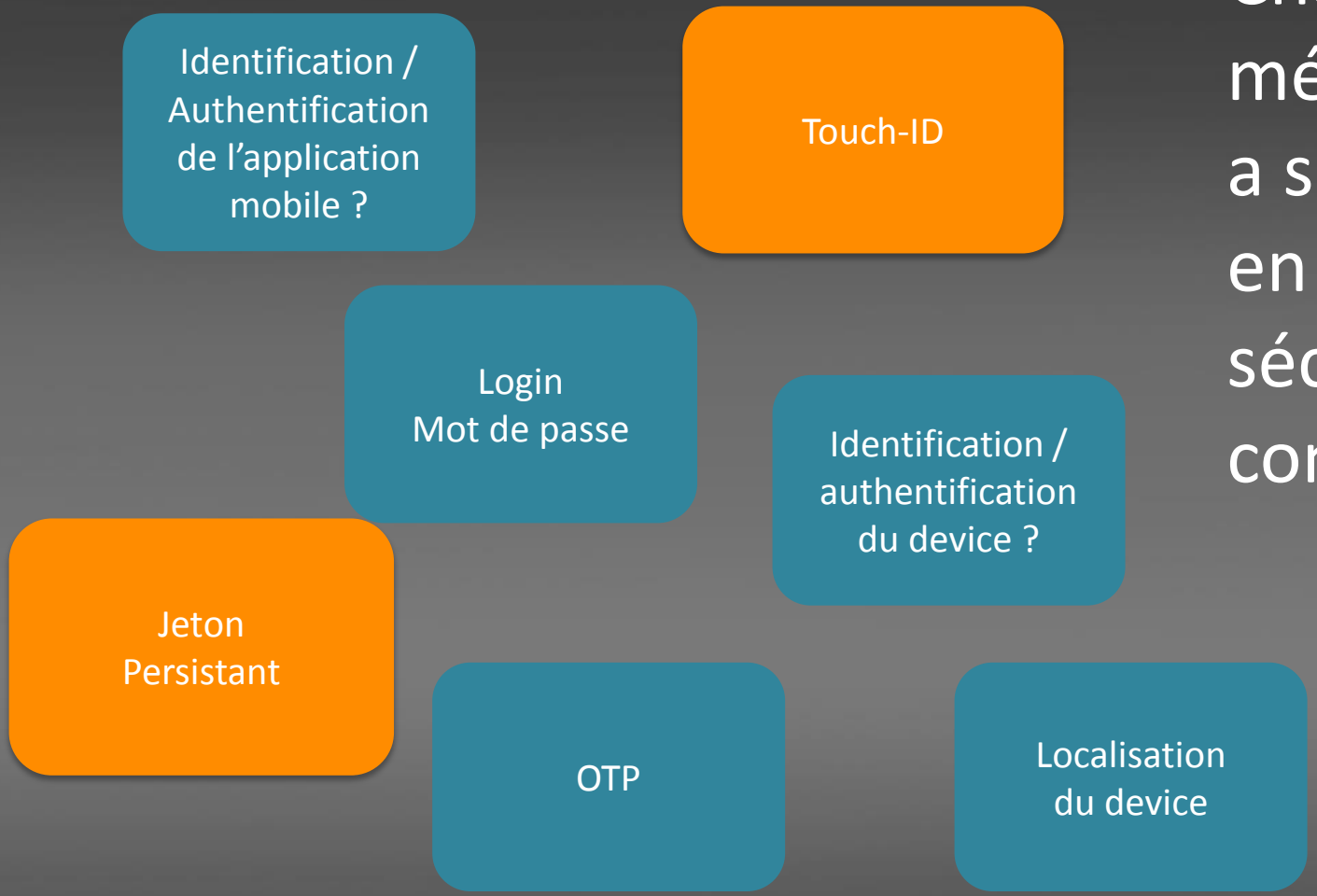
Simplifier l'usage

Sécurité « Réelle » et ressentie

L'AUTHENTIFICATION
au cœur des problématiques
de sécurité sur mobile

Vers une authentification simplifiée

Quelle confiance vis-à-vis
des mécanismes actuels ?



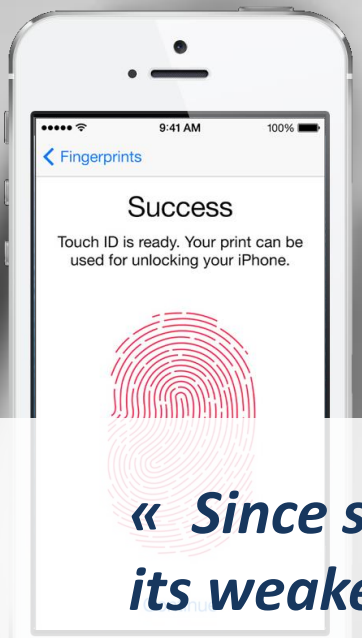
Chaque mécanisme a sa limite soit en matière de sécurité ou de confort

TOUCH ID : « Secure or not » ?!

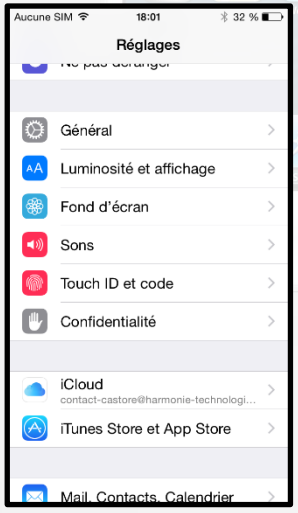
TOUCH ID : « Secure or not » ?!

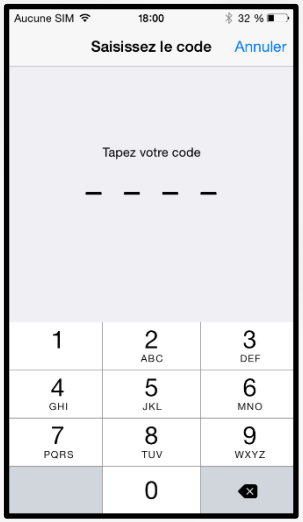
TOUCH ID : « Secure or not » ?!

Lancement d'une application



Accès à l'application





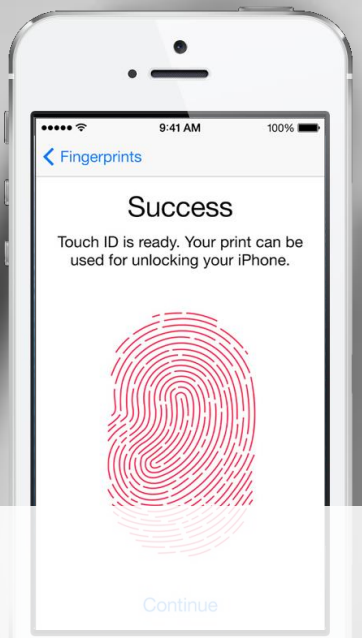
« Since security is only as secure as its weakest point, you can choose to increase the security of a 4-digit passcode by using a complex alphanumeric passcode »

APPLE

Ajout d'une nouvelle empreinte sur téléphone

TOUCH ID : « Secure or not » ?!

Lancement d'une application



Accès à l'application

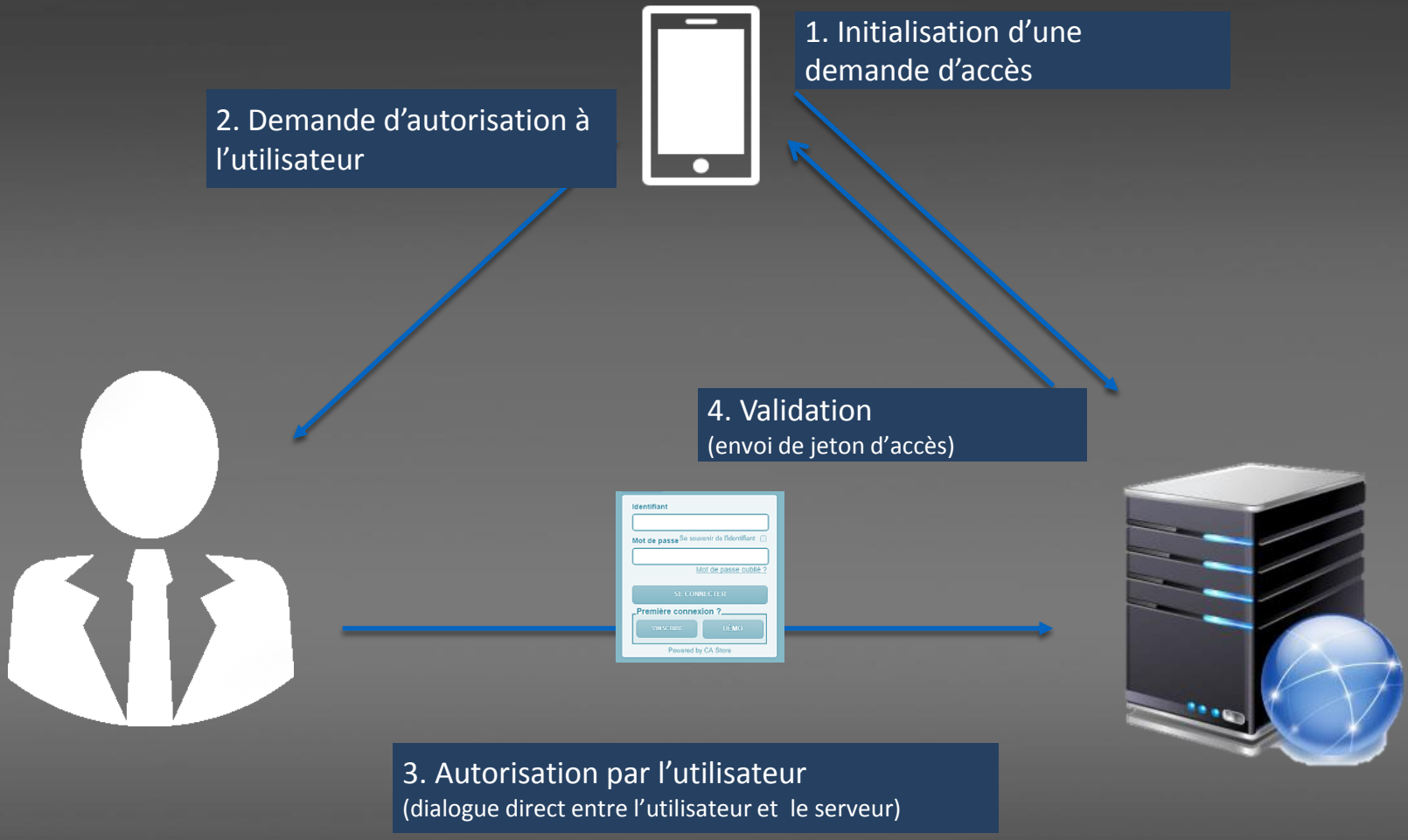
Cependant…

Protection efficace face au regard indiscret

Accès sécurisé au keychain sans trop alourdir l'expérience utilisateur

JETON PERSISTANT

L'exemple par OAuth



JETON PERSISTANT

L'exemple par OAuth

Plusieurs versions du standard Oauth …

→ Signatures des requêtes sortantes
→ Durée de vie des jetons émis potentiellement illimitée

DEPRECATED

→ Jetons en transit à chaque requête
→ Durée de vie limitée, avec mécanismes de renouvellement
→ Divers profils pour divers usages (mobile, web etc.)

✓ **Un standard « riche », permettant de nombreux usages** (Fédération, confort utilisateur sur mobile, etc.) …

⚠ **Plusieurs points clés de sécurité à traiter pour une implémentation efficace :**

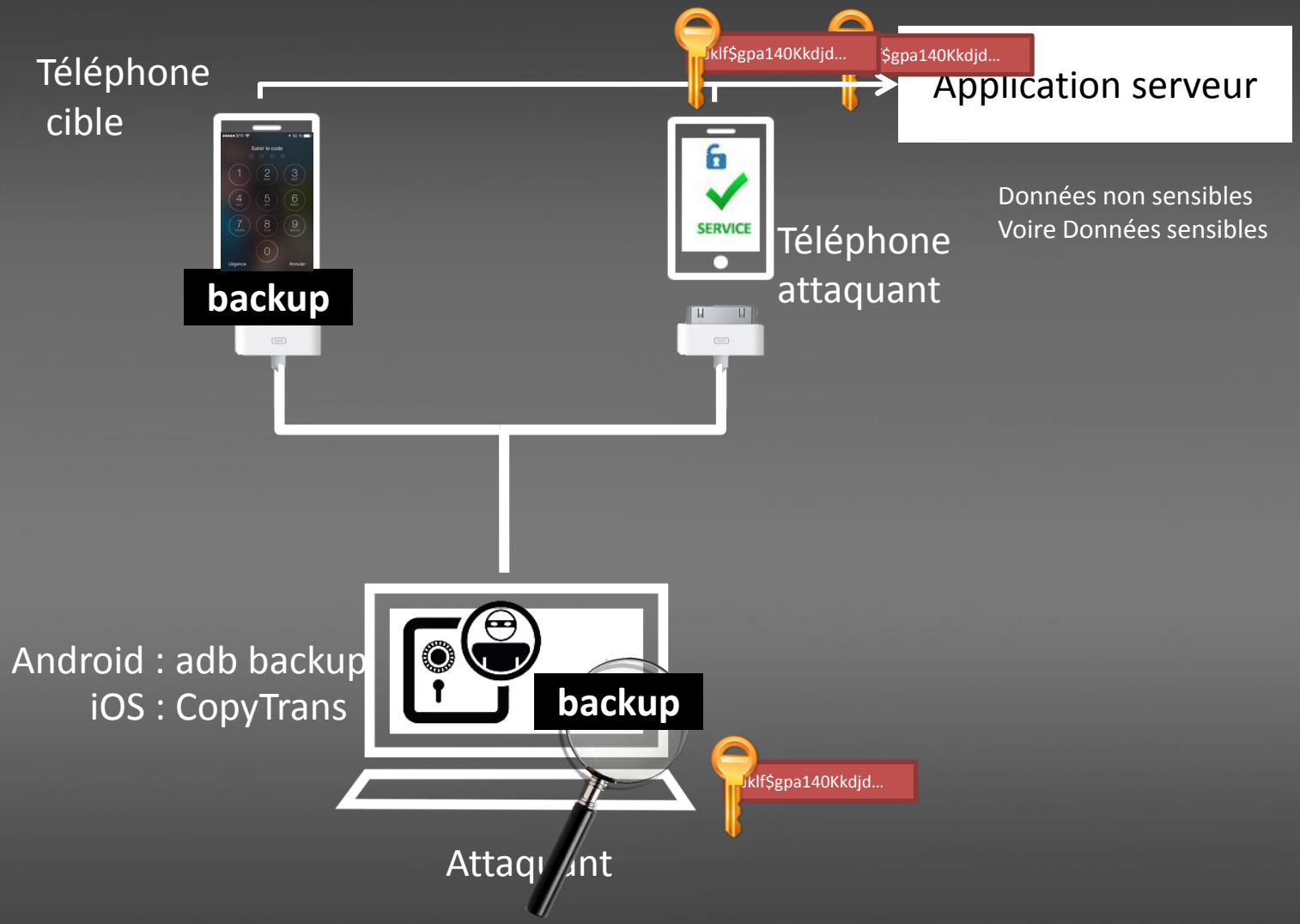
Fonctionnels :

- Quelle durée de vie du jeton fonction des usages attendus ?
- Quelle maîtrise de la diffusion des jetons après émission ?
- Quel est le périmètre des données accessibles ?
- …

Techniques :

- Quel profil ? OAuth correspond à l'usage souhaité ?
- Les jetons sont-ils conservés côté serveur ? Avec quelle protection ?
- Attention au stockage des jetons dans les logs des proxys
- …

ATTAQUE SUR UN MOBILE CIBLÉ



REVUE DES FAIBLESSES LES PLUS COURANTES

1 / Une sécurité souvent « illusoirement » renforcée par le Touch-ID

2 / Des jetons stockés dans la mémoire de l'application, dont l'usage n'est pas lié au téléphone

3 / Vérification des certificats SSL ignorés par les applications

4 / Informations sensibles accessibles après authentification persistante, et pourtant inutilisées

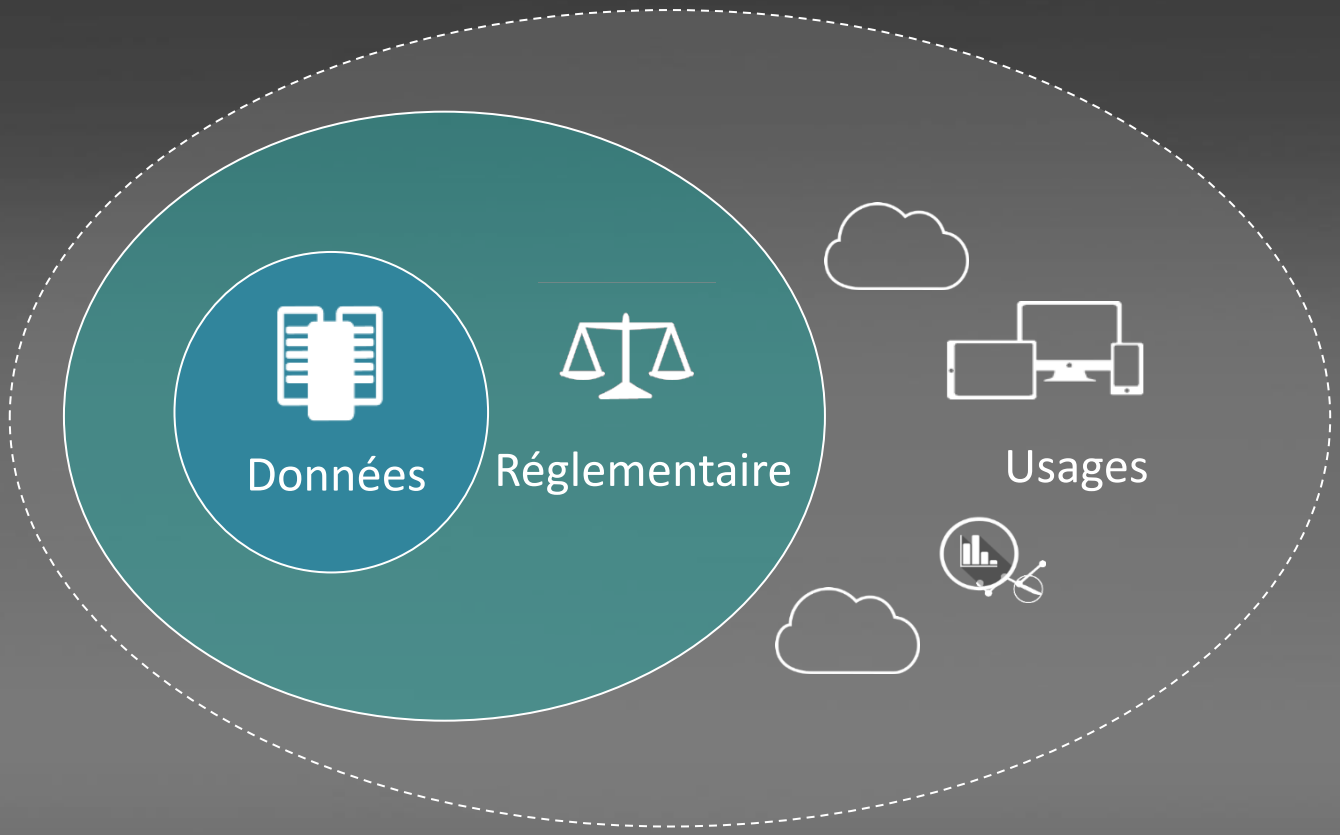
5 / Déconnexion inefficace (l'application se limite à supprimer le jeton en mémoire)

Vers une mise en œuvre …

La criticité des données
au cœur de la réflexion

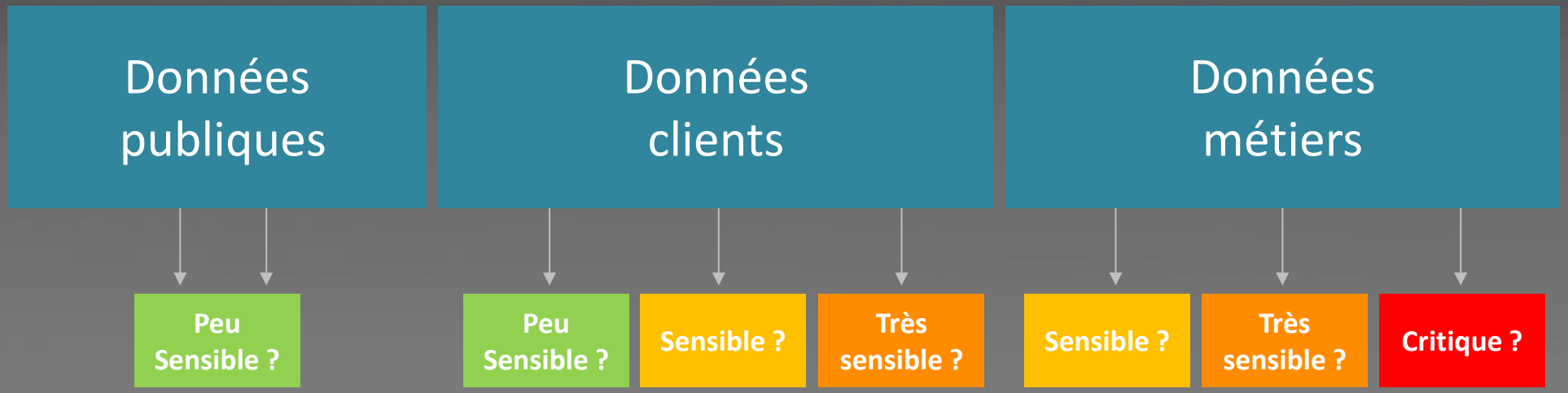
USAGES & DONNEES

Les usages évoluent beaucoup et rapidement, mais les données (et les contraintes associées) évoluent peu



Les cycles de mise en production des usages étant rapides,
il est nécessaire que ***le cadre d'accès à la donnée porte au maximum la sécurité***

IMPORTANCE DE LA CLASSIFICATION DES DONNEES

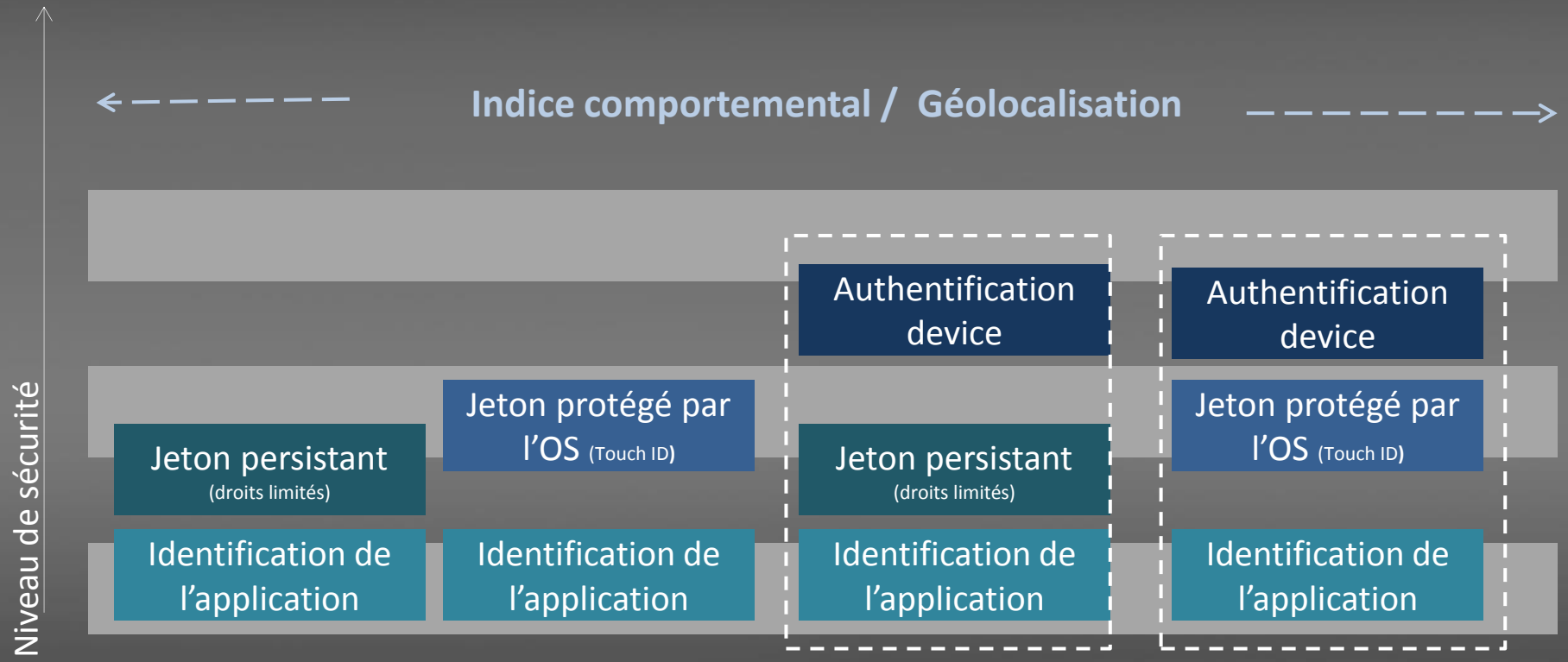


A chaque niveau doit être associé des mesures de sécurité adéquates

CONSÉQUENCE SUR L'AUTHENTIFICATION

EXEMPLE DE COMBINAISONS POUR MOBILE AVEC UNE APPROCHE « ERGONOMIQUE »

BASÉ SUR JETON PERSISTANT, PROTÉGÉ OU NON PAR L'OS



Questions ?

Merci de votre attention

Harmonie Technologie
Spécialiste de la sécurité du système d'information
Gouvernance - Conseil - Audit - Intégration - Formation

Nous contacter
www.harmonie-technologie.com
+331 73 75 08 47 *info.ssi@harmonie-technologie.com*