www.cnrs.fr

BYOD Bring Your Own Device

SARI Grenoble 13/11/2013

François Morris

Plan

- ❑ Définition et positionnement
- ❑ Problématiques juridiques et ressources humaines
- ❑ Economie
- ❑ Risques
- ❑ Des éléments de réponse

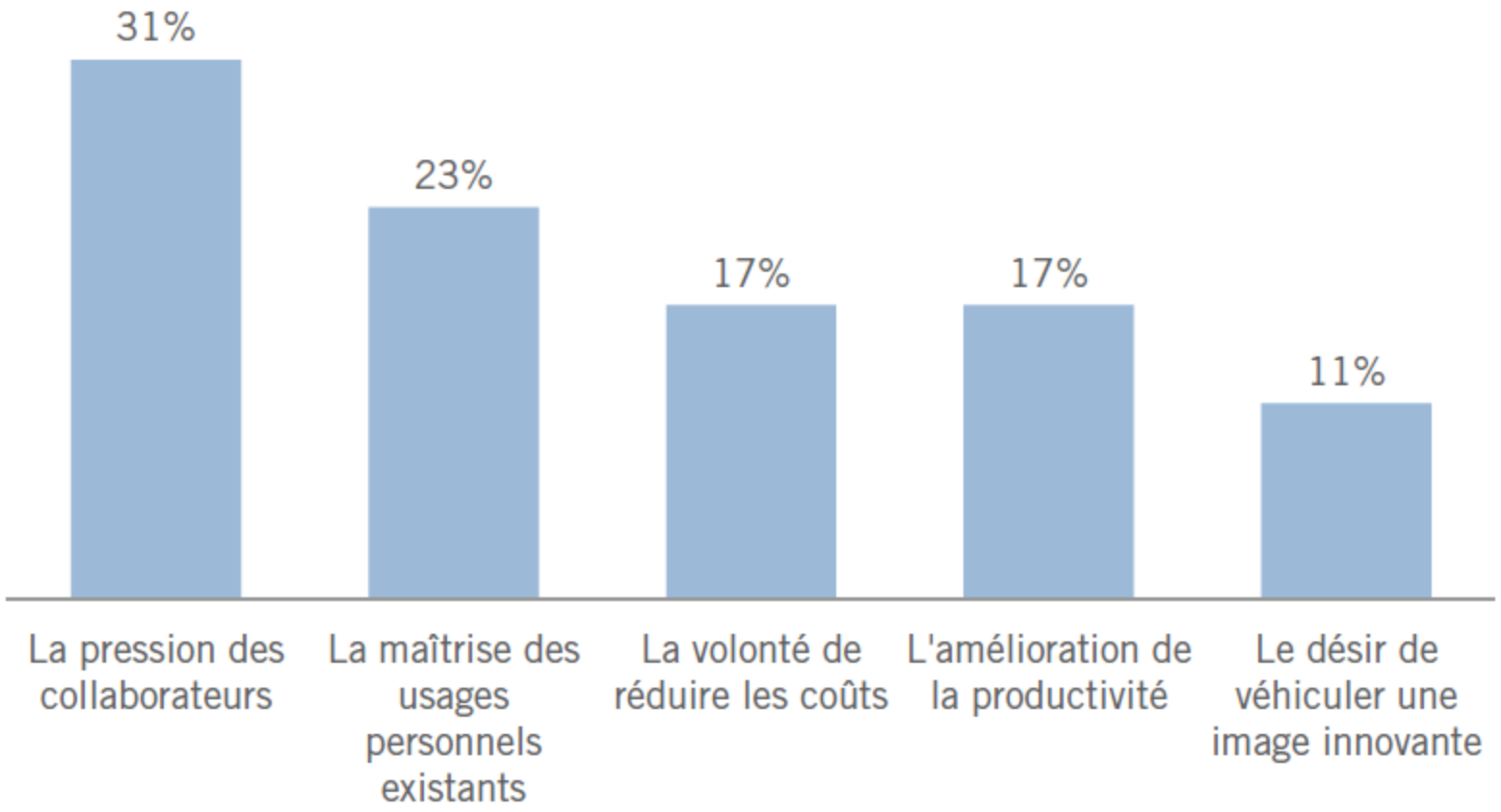
Plan

- ❑ **Définition et positionnement**
- ❑ Problématiques juridiques et ressources humaines
- ❑ Economie
- ❑ Risques
- ❑ Des éléments de réponse

BYOD

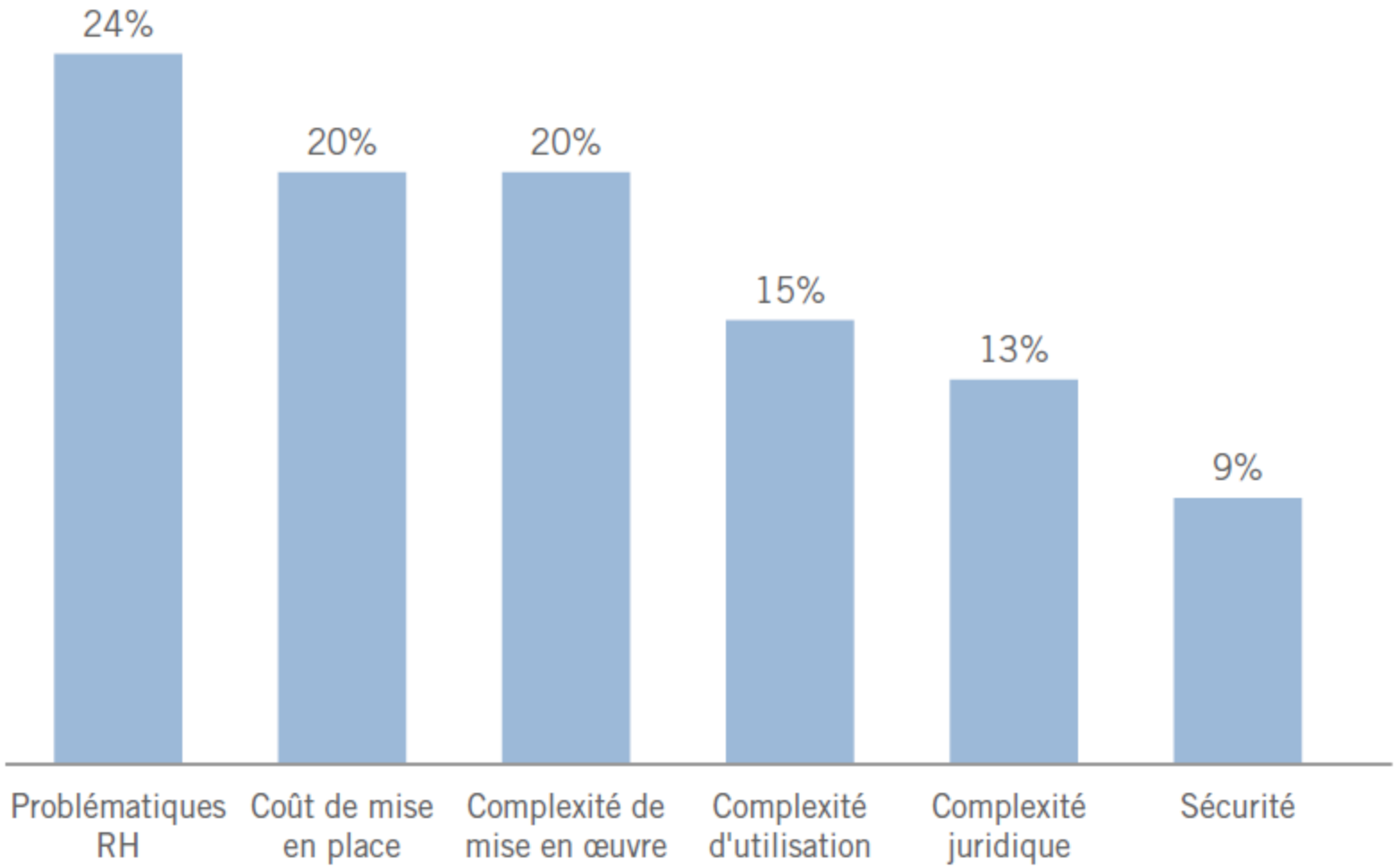
- **Concept à la mode**
  - Tout le monde en parle
  - Des déploiement encore très ciblés
- **N'est pas totalement nouveau**
  - Prolongement du télétravail
- **Manifestation d'une évolution de la société**
  - Génération Y
  - Rapports au travail
  - Fusion vie professionnelle & privée
  - Instantanéité, ubiquité

Quels sont les éléments déclencheurs d'un projet BYOD ?



Etude Solucom novembre 2012

Quels sont les freins à la mise en place d'un projet BYOD ?



Etude Solucom novembre 2012

Définitions et objectifs du BYOD

- **Bring Your Own Device**
- **Favoriser l'achat par le personnel lui-même des terminaux informatiques**
  - PC
  - Smartphones
  - Tablettes
- **Avec ou sans aide financière**
- **Autoriser son utilisation dans le cadre professionnel**
- **Doit permettre à l'organisation d'économiser de l'argent dans la mesure où elle ne gère plus les terminaux**

Situation au CNRS

- **Continuum entre matériel professionnel et privé**
  - CNRS
  - Partenaire dans une unité mixte
  - Société avec laquelle a été passé un contrat de recherche
  - Université du chercheur étranger qui est en visite pour trois mois
  - Employeur d'un prestataire
  - Autre laboratoire dans le cas de l'étudiant qui fait un doctorat dépendant de deux laboratoires (éventuellement dans des pays différents)
  - Utilisateur lui-même
- **BYOD = tout ce qui n'est pas CNRS**
- **Extension de la réflexion à des domaines dont la problématique est connexe**
  - Mobilité
  - Télétravail

Attitude vis-à-vis du BYOD

- **Problématiques compliquées et risques élevés**
  - Juridique
  - Ressources humaines
  - Techniques
  - Sécurité
- **Interdiction du BYOD**
  - Position de l'ANSSI : « ***La sécurité c'est aussi avoir le courage de dire non*** »
  - Position la plus confortable pour le RSSI
  - Irréaliste et non productif au sein du CNRS
    - Sauf situations particulières (certains utilisateurs, unités, zones très sensibles)
- **Encadrement pour limiter les risques**

Plan

- ❑ Définition et positionnement
- ❑ **Problématiques juridiques et ressources humaines**
- ❑ Economie
- ❑ Risques
- ❑ Des éléments de réponse

Points d'attention

❑ Juridique et ressources humaines

- ➢ Soumis aux services concernés
- ➢ Attente de réponse
- ➢ Intégration dans les futures versions de la charte et de la PSSI

❑ Sécurité des systèmes d'informations

- ➢ Technique
- ➢ Organisationnel

Licences logicielles

- **Les contrats actuels permettent-ils une installation dans le cadre du BYOD ?**
- **Logiciels ayant des licences différentes suivant les usages**
  - Privé
  - Professionnel

Qui a le droit d'intervenir ?

- **Quelles tierces personnes ont le droit d'intervenir sur ces matériels et dans quel contexte ?**
- **Concept de « vie privée résiduelle »**
  - Bien fixé par la CNIL, la jurisprudence
  - N'est plus opérant pour un matériel personnel
  - « sphère professionnelle » dans un monde privé
    - A encadrer juridiquement
- **En cas d'incident**
  - Séquestre, copie du disque possible ?
  - Analyse forense possible ?
- **Audits, tests d'intrusion**
  - Est-ce réellement envisageable sur un matériel privé ?

Quelles frontières entre utilisation professionnelle et personnelle ?

- **Utilisation par des tiers**
  - Conjoint
  - Enfants
  - Collègues
- **Plages horaires pour l'utilisation professionnelle**

Propriété et protection des données

- Qu'en est-il de la propriété intellectuelle des données de l'organisme sur un matériel privé ?
- Le CNRS peut-il édicter des règles de sécurité concernant les données traitées par ce matériel et comment gère-t-on le conflit éventuel entre ces règles et celles que l'utilisateur souhaite appliquer sur son matériel ?
- Conflits de règles lorsqu'il ne s'agit pas de matériel personnel mais de matériel appartenant à un autre organisme.
- On ne peut interdire à l'utilisateur d'être administrateur de son poste car c'est justement lui qui contrôle son propre matériel.
- Récupération des données par le CNRS et la famille en cas de départ ou de décès de l'employé ?

Propriété et protection des données

- Que se passe-t-il si à la suite d'une perte ou d'un vol l'organisme efface à distance l'ensemble des données d'un terminal y compris celles qui sont personnelles et que le terminal est retrouvé ?
- Jusqu'où l'organisme peut-il aller : traces, récupération des données, etc.
- Qui fournit les outils de sécurité comme l'antivirus ? Qui les paye ? Choix par l'utilisateur ou imposé ?
- A qui appartiennent les informations créées, collectées, envoyées depuis le terminal de l'employé

Responsabilité vis-à-vis du matériel

- Que se passe-t-il en cas de perte, de vol du matériel ?
- Que se passe-t-il en cas de dommages à l'organisme causés par un bien personnel (diffusion d'un virus, déclenchement d'un incendie, etc.) ?
- Que se passe-t-il en cas de dommages à un bien personnel causé par l'organisme ou un de ses employés (par exemple effacement intempestif des données personnelles, destruction par incendie, etc.) ?
- Passages de frontières et utilisation dans certains pays, quelles règles ?

Quelle prise en charge par le CNRS ?

- **Prise en charge des coûts : abonnement téléphonique, matériel, applications achetées dans les « e-store »**
  - Qui paye, qui rembourse ?
  - Incidences fiscales, charges sociales
- **Assurance : qui assure et pour couvrir quoi ?**
- **Qui assure la maintenance ?**
- **Réparation, remplacement en cas de panne, perte, vol ?**

Des situations à prévoir

- **Saisie dans le cadre d'une enquête judiciaire concernant :**
  - l'employeur
  - l'employé
- **Responsabilité de l'employé en cas de fuite d'informations confidentielles de l'organisation à la suite d'un vol ou perte**

Compatibilité avec la législation et règlementation

- **L'employeur doit fournir l'outil de travail**
  - L'ouvrier ne vient pas avec sa pelle
- **Loi informatique et libertés**
  - Mélanges des données professionnelles et privées
  - Obligation de transparence vis-à-vis des données à caractère personnel
  - Rôle du CIL
- **Equité, non discrimination**

Plan

- ❑ Définition et positionnement
- ❑ Problématiques juridiques et ressources humaines
- ❑ **Economie**
- ❑ Risques
- ❑ Des éléments de réponse

Le BYOD gain financier ?

- **Bien évaluer les gains, coûts directs et indirects tant financiers qu'humains du BYOD**
  - L'organisme ne paye plus le matériel
  - Remboursement, prime versée pour l'achat
  - L'utilisateur a le choix de son matériel, il est donc satisfait
  - Infrastructure matérielle et logicielle pour accueillir le BYOD : gestion de parc, vérification de la conformité, sauvegardes, MDM, etc.
  - Sensibilisation, formation
  - Temps passé par l'utilisateur à administrer sa machine (il peut être plus cher et moins efficace qu'un administrateur professionnel)
- **Globalement illusoire**
  - Sauf contexte extrêmement favorable
  - Coût de possession >> coût du matériel
  - Coût estimé 70 à 100€ par an dans une étude de Solucom

Plan

- ❑ Définition et positionnement
- ❑ Problématiques juridiques et ressources humaines
- ❑ Economie
- ❑ **Risques**
- ❑ Des éléments de réponse

Problématique et risques à couvrir

- **La problématique liée au BYOD est d'abord du ressort**
  - DAJ (risque juridique)
  - DRH (acceptation et encadrement des usages)
  - Direction (validation des risques résiduels et des moyens à mettre en œuvre pour traiter les risques)
- **Principal risque SSI est la divulgation d'informations confidentielles**
  - Bien évaluer les menaces, les moyens des attaquants en fonction de la nature des informations.
    - Une agence gouvernementale ne s'intéressera probablement pas à la rémunération du personnel
    - Par contre celle-ci peut être très attractive pour des activistes qui vont la diffuser largement pour défendre leur cause
  - Le BYOD est souvent associé au cloud.
- **Risques pesant sur le SI lui-même**
  - Matériel BYOD comme vecteur d'attaque

Prise en compte des risques

- Les principes généraux de la PSSI devraient s'appliquer certes avec des adaptations pour éviter que le BYOD ne mette à mal tout le dispositif de protection du patrimoine informationnel.
- Ne pas vouloir tout faire, tout de suite pour tout le monde. Prévoir un séquencement dans l'approche.
- Prévoir le cas où le matériel n'est pas personnel mais est professionnel appartenant à un autre organisme.
- Faire une appréciation des risques en fonction de la nature des informations traitées par les différents utilisateurs. Ce n'est pas forcément la même politique pour tous.
- L'offre de sécurité pour le BYOD est loin d'être mature. Les produits sont très récents, de nouveaux acteurs se lancent (fournisseur d'antivirus, opérateurs téléphoniques, etc.).
- Un outil, une solution technique de sécurisation doit être simple d'utilisation et la plus transparente possible sinon il y aura rejet ou contournement.

Prise en compte des risques

- La sécurisation de la mobilité doit s'inscrire dans une démarche de sécurisation classique
- La sensibilisation est un élément clé mais est coûteuse.
- La téléphonie est gérée par les services généraux et n'est donc pas considérée au départ comme faisant partie du SI.
- Penser que les utilisateurs n'auront pas besoin de support sous prétexte qu'il s'agit d'un matériel personnel est illusoire. De plus il reste l'accès au SI de l'organisme qui peut requérir une assistance.
- Changement d'échelle pour certains processus. On est au contact direct de l'ensemble des utilisateurs et non plus uniquement d'intermédiaires et de spécialistes (ASR, CSSI, etc.).

Plan

- ❑ Définition et positionnement
- ❑ Problématiques juridiques et ressources humaines
- ❑ Economie
- ❑ Risques
- ❑ **Des éléments de réponse**

Non maîtrise du terminal

- **Quelle confiance peut-on avoir ?**
  - Par définition l'organisme n'a aucun contrôle sur un terminal privé
  - Du point de vue de la sécurité doit être considéré comme potentiellement hostile
- **Que peut-on faire ?**
  - Ne rien stocker → déport d'affichage
  - Contrôle d'accès et de conformité pour les connexions au SI → NAC
  - Diffuser des politiques (mots de passe, chiffrement, etc.) → MDM
  - Utiliser une application ou espace dédiée à l'organisme → silo, conteneur
  - Responsabiliser les utilisateurs
  - Limites évidentes
- **Refus**
  - ANSSI
  - Areva

MDM

- **Mobile Device Management**
  - Issu de la gestion de parc
  - Intégration de la sécurité
- **Multiplicité des fournisseurs**
  - Gestion de téléphones
  - Acteurs dans la sécurité (antivirus)
  - Opérateurs
  - Nouveaux entrants

MDM

- **Marché non mature**
  - Pérennité des solutions ?
- **Plus adapté à la gestion d'un parc de terminaux d'entreprise qu'au BYOD**
  - Limites à ce que l'on peut faire sur un terminal non maîtrisé (installation d'un agent)
- **Utilisation fréquente du protocole ActiveSync**
  - Serveurs Exchange
  - La plupart des terminaux (iOS, Android, etc.)
- **Non exempts de failles**

Effacement à distance

- **En cas de perte ou de vol**
- **Envoie un ordre d'effacement à partir**
  - MDM
  - Un service dans le cloud, souvent accompagné de localisation, voire de contrôle (caméra, micro, haut-parleur) de l'appareil
  - Serveur Exchange, serveur Apple
- **Problématique**
  - Délais de réaction
  - Inefficace vis-à-vis d'un voleur un peu déterminé
    - Retire SIM
    - Ne se connecte à aucun réseau Wifi
  - Risques d'effacement intempestif
    - Erreur dans la demande
    - Détournement du mécanisme par un pirate

Canal sécurisé

- **Interception facile**
  - Canal radio (GSM, 3G)
  - Wifi vraiment trivial (ex. borne pirate)
- **Systématiquement chiffrer et authentifier les échanges**
  - SSL/TLS/HTTPS avec validation des certificats

Interdiction jailbreak

- **Jailbreak incompatible avec la sécurité**
  - Casse tous les mécanismes de protection
  - Introduit des vulnérabilités supplémentaires
    - iOS serveur SSH → accès root (mot de passe « alpine »)
  - Facilite l'analyse forense
- **Règle pas facile à imposer**
  - Repose sur le comportement des utilisateurs
  - Détection et rapport dans un outil (MDM)
    - Pas toujours évident
    - Outils pour cacher la situation
      - Demander à un menteur s'il ment
- **Exceptions**
  - Tests sur du matériel dédié
  - Jamais sur un matériel utilisé normalement

Silos

❑ Silos, conteneurs, cloisonnement, isolation

- ➢ Application
  - Encapsule les données et outils de l'entreprise dans une application
  - Environnement non maîtrisé et potentiellement hostile
  - Solutions disponibles sur le marché
- ➢ OS
  - Nécessite un OS modifié
  - L'employeur n'est pas maître de l'OS
  - Knox de Samsung
- ➢ Processeur ARM/TrustZone
  - Une piste pour le futur ?

Trusted Execution Environments

- **Benjamin Morin, ANSSI séminaire Aristote 07/02/2013**
- **Technologie matérielle ARM/TrustZone**
- **Séparation de l'environnement d'exécution en deux domaines**
  - Un domaine dit « non sécurisé » (l'OS de l'utilisateur) et un domaine « sécurisé »
  - Protection en intégrité et en confidentialité des applications qui s'exécutent dans le domaine sécurisé contre le domaine non sécurisé
  - Y compris en cas de compromission du noyau du domaine non sécurisé
- **Cas d'applications types**
  - Applications de paiement, DRM, etc.
  - Cas d'application du BYOD pour des applications professionnelles ?
    - TIMA (Samsung Knox), vérifications intégrité OS

Trusted Execution Environments

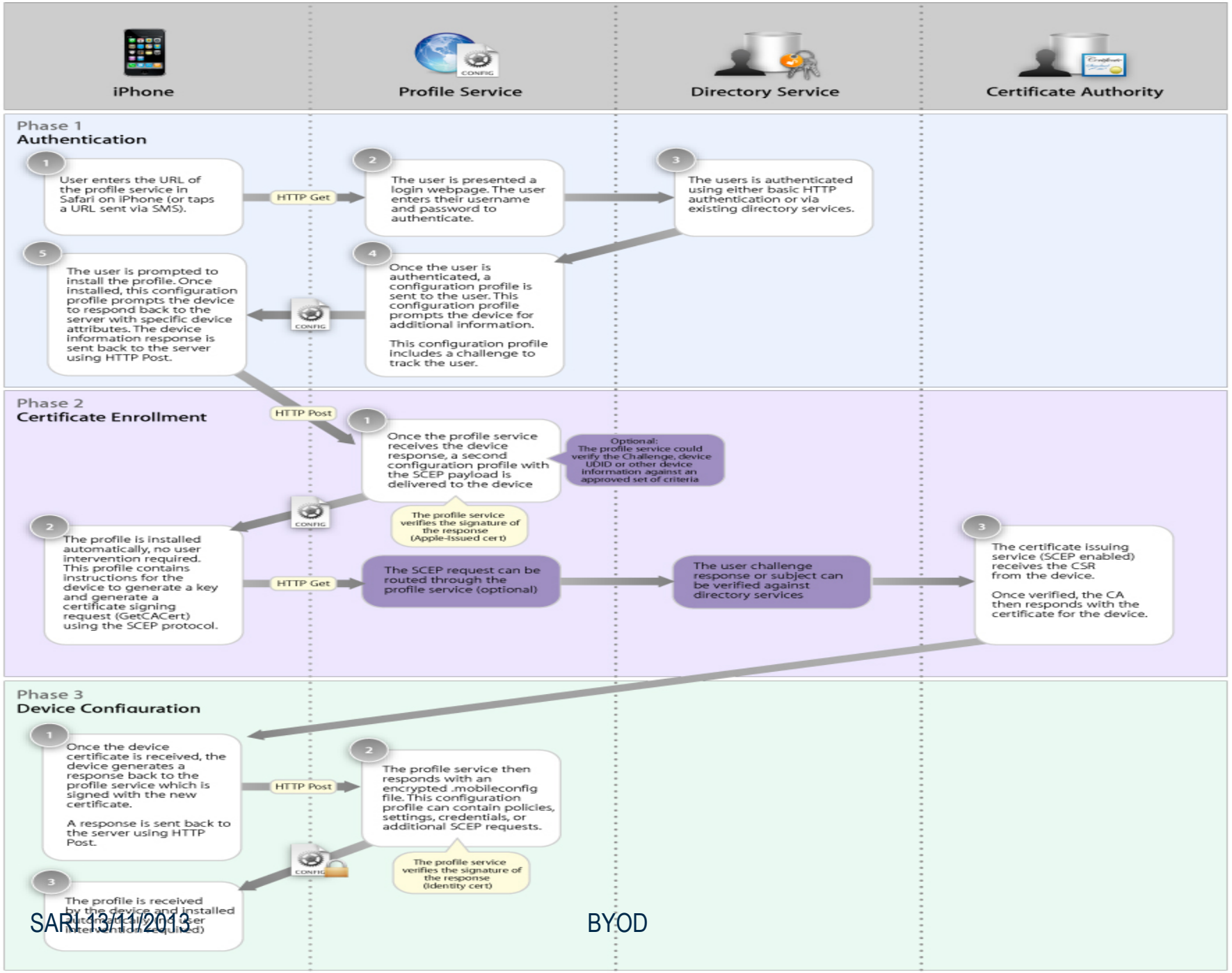
- **Des interrogations subsistent sur ce type de technologie**
  - Technologie encore fermée
  - Quid de la personnalisation de l'environnement sécurisé ?
  - Quid des garanties d'isolation au sein de l'environnement sécurisé ?
  - Qui contrôle l'environnement d'exécution sécurisé ?
- **Pas encore de réalisation aujourd'hui pour le BYOD**

Mobile outil de sécurisation

- **Terminal mobile devient outil de sécurisation**
  - Envoi de mot de passe par SMS
  - SMS de confirmation
- **Deux canaux distincts ?**
  - Vrai avec téléphones ancienne génération
  - Pas nécessairement si on utilise un smartphone
    - SMS 3D-Secure sur le même terminal qui a servi à la commande
    - Il existe déjà des codes malfaisants exploitant cette vulnérabilité

Simple Certificate Enrollment Protocol

- SCEP est au stade d'internal draft au sein de l'IETF, promu par CISCO
- Sert à automatiser le déploiement de certificat X509
- Apple l'utilise pour permettre d'installer des certificats « over the air » et configurer des matériels
- Vulnérabilité relevé par le CERT US
  - SCEP does not strongly authenticate certificate requests (27/06/2012)
- Désormais déconseillé par le draft au profit de
  - Certificate Management Protocol (CMP) [RFC4210]
  - Certificate Management over CMS (CMC) [RFC5272]


iPhone
Profile Service
Directory Service
Certificate Authority
Phase 1
Authentication
1
User enters the URL of the profile service in Safari on iPhone (or taps a URL sent via SMS).
HTTP Get
2
The user is presented a login webpage. The user enters their username and password to authenticate.
3
The users is authenticated using either basic HTTP authentication or via existing directory services.
4
Once the user is authenticated, a configuration profile is sent to the user. This configuration profile prompts the device for additional information.
This configuration profile includes a challenge to track the user.
CONFIG
5
The user is prompted to install the profile. Once installed, this configuration profile prompts the device to respond back to the server with specific device attributes. The device information response is sent back to the server using HTTP Post.
HTTP Post
Phase 2
Certificate Enrollment
1
Once the profile service receives the device response, a second configuration profile with the SCEP payload is delivered to the device
Optional:
The profile service could verify the Challenge, device UDID or other device information against an approved set of criteria
CONFIG
The profile service verifies the signature of the response (Apple-Issued cert)
2
The profile is installed automatically, no user intervention required. This profile contains instructions for the device to generate a key and generate a certificate signing request (GetCACert) using the SCEP protocol.
HTTP Get
The SCEP request can be routed through the profile service (optional)
The user challenge response or subject can be verified against directory services
3
The certificate issuing service (SCEP enabled) receives the CSR from the device.
Once verified, the CA then responds with the certificate for the device.
Phase 3
Device Configuration
1
Once the device certificate is received, the device generates a response back to the profile service which is signed with the new certificate.
A response is sent back to the server using HTTP Post.
HTTP Post
2
The profile service then responds with an encrypted .mobileconfig file. This configuration profile can contain policies, settings, credentials, or additional SCEP requests.
CONFIG
The profile service verifies the signature of the response (Identity cert)
3
The profile is received by the device and installed (User intervention required)

Cloud

- **Nomadisme et BYOD vont souvent de pair avec l'utilisation de services dans le *cloud***
- **Problématiques du cloud à traiter**
  - C'est un autre et vaste sujet
- **Aucune garantie pour un cloud public**
  - Patriot Act
  - Cloud privé
  - Chiffrement
- **Projet de cloud du CNRS**
  - Stockage, synchronisation
  - Etudes en cours
  - Owncloud ?

Références de recommandations

- **Déborde du cadre du BYOD *stricto sensu* pour englober la mobilité**
- **Publications sur le site SSI du CNRS**
  - Règles élémentaires de sécurité - Objets nomades communicants
  - Voyager avec son ordinateur portable
- **ANSSI**
  - Partir en mission
  - Passeport du voyageur
- **CDSE (Club des directeurs de sécurité des entreprises)**
  - Passeport