



# Bring Your Own Device & Mobile Security

**Grégory Ogonowski & Bert Vanhalst**  
**Sectie Onderzoek**

**December 2012**

# Sommaire

---

- Introduction
- Stratégies
- Solutions BYOD
- Authentification forte
- Recommandations
- Conclusion



X

# Sommaire

---

- Introduction
- Stratégies
- Solutions BYOD
- Authentification forte
- Recommandations
- Conclusion



# Introduction

---

- BYOD = Bring Your Own Device
- Buzzword
- Technologie  $\neq$  BYOD = Tendence
- A l'initiative des employés et non de l'employeur
  
- Pas nouveau
  - Utilisation de carnets de notes personnels
  - Utilisation de clés USB personnelles



**Intro – Stratégies – Solutions – Auth forte – Recommandations - Conclusion**

# Introduction :

## BYOD, pourquoi maintenant ?

---

- Notebooks populaires, mais...
- Netbooks bien plus portables
- Démocratisation des tablettes et smartphones
- De plus en plus présent/visible
- Parcs informatiques de plus en plus hétérogènes (laptop, tablettes, smartphones, appareils professionnels, appareils privés)



# Introduction : Rôle du Cloud

---

- Impact d'Internet : BYOA (A = Application)
  - Présent bien avant BYOD
  - Introduit grâce au/à cause du Cloud
  - Dispersion des données
  - Problèmes de sécurité



# Introduction : Rôle du Cloud



**Ce site est  
intéressant**



**On a parlé  
de ça en  
réunion**



**Je m'intéresse  
à ce produit**



**Je travaille  
sur ceci**



**Il y avait  
du monde  
à cette  
conférence**



**Mon chef  
veut que je  
fasse cela**



**Cette #technologie  
est géniale**



**Il n'y a pas  
grand monde  
ici**



**Je relirai  
ce document  
ce soir**



# Introduction : BYOA → BYOD

---

- L'appareil personnel ne fait que changer le point d'accès au Cloud
- Protéger les données > Protéger l'appareil
  - Un appareil sécurisé n'empêchera pas l'utilisateur de diffuser des données dans le Cloud



# Introduction : BYOD, les causes

- Raisons potentielles du BYOD
  - Matériel professionnel non satisfaisant
  - Portables lourds
  - Machines lentes
  - Permissions restreintes
  - Logiciels peu appréciés
  - 1 seule machine pour usage privé et professionnel
  - Volonté de rébellion/liberté ?
- Raisons acceptables ?



# Introduction :

## BYOD pour quels usages ?

---

- Consultation mails/calendrier
- Surfer sur le web (y compris pour usage personnel)
- Prendre des notes en réunion
- Utiliser divers utilitaires (to do list, mindmap, ...)
- Accéder aux ressources de l'entreprise (intranet)
- Editer des documents



# Introduction : BYOA, BYOD, BYON

---

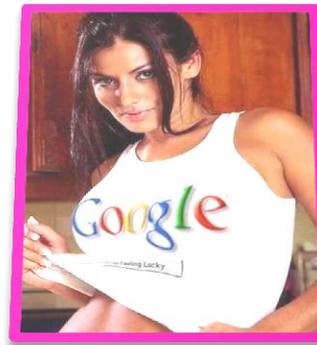
- BYOD pour quel usage ?
  - Contourner des restrictions en entreprise (ex : blocage de Facebook)
- BYOA + BYOD + BYON (Network : internet mobile)
  - Difficile à empêcher en pratique



# Introduction :

## BYOD, perceptions différentes

- BYOD et outils dans le Cloud
- Vu par l'employeur
  - Hétérogénéité du parc
  - Problèmes de sécurité
  - Fuites de données
  - Augmentation des coûts
- Vu par l'employé
  - Augmentation de la productivité
  - Flexibilité
  - Cool ;-)
  - Diminution des coûts



# Introduction :

## BOYD : les aspects juridiques

---

- Obligation de l'employeur de fournir le matériel nécessaire pour le travail
- Possibilité d'interdire l'usage de certains équipements/logiciels dans le cadre professionnel
- L'employé peut consulter sa messagerie en dehors des heures de travail sur son propre appareil, mais on ne peut l'y contraindre



# Introduction :

## BYOD, une tendance particulière

---

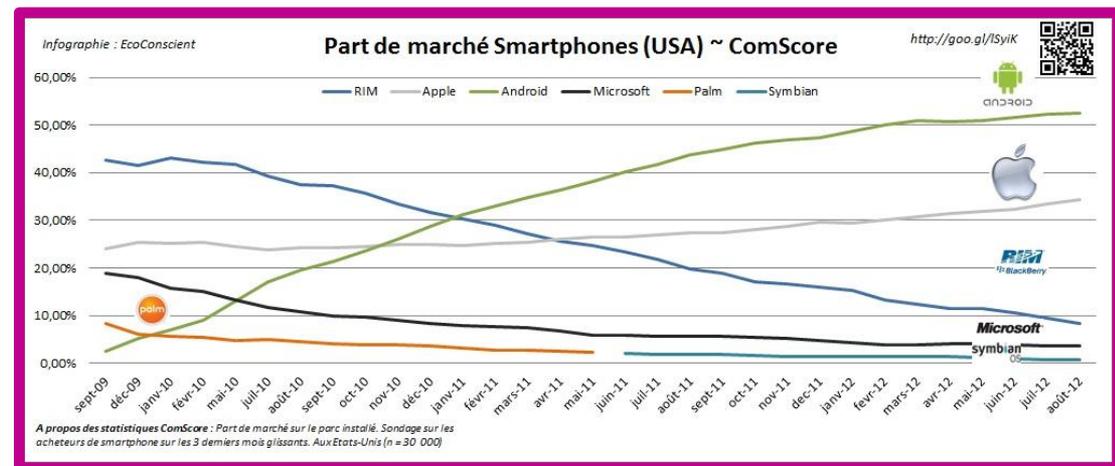
- BYOD : initiative de l'employé
  - Utilisateur pas toujours conscient des dangers
  - Besoin de gérer appareils professionnels et privés de manière cohérente
- ➔ Nécessité de définir une stratégie



# Introduction :

## BYOD : des choix s'imposent

- Sujet très vaste
- Demandes diversifiées
- Impossible de répondre à tout
- Impossible de tout traiter durant la présentation
- Systèmes retenus :
  - Windows / OS X
  - iOS / Android



# Sommaire

---

- Introduction
- Stratégies
- Solutions BYOD
- Authentification forte
- Recommandations
- Conclusion



# Strategieën voor BYOD

---



## Verbieden

Enkel corporate devices  
Organisatie heeft volledige  
controle

## Beperkt toelaten

Enkel e-mail  
Beperkte support  
Internet-only wifi

## Omarmen

Bedrijfstoepassingen  
Beveiligde toegang tot  
intern netwerk



# Verbieden

---

- Enkel corporate devices toegelaten
- Niet ondersteunen versus verbieden?
- Risico dat security policy omzeild wordt... omdat er een behoefte is



# Gedeeltelijk toelaten

---

- Toelaten voor e-mail / kalender
- Tegemoetkomen aan vraag n°1
- Wifi guest access, gescheiden van het interne bedrijfsnetwerk
- Minimale ondersteuning



# Volledig omarmen

---

- Toelaten voor "alle" bedrijfstoepassingen
- Hoe zijn de gegevens beveiligd op de toestellen?
- Quid veiligheid interne netwerk?



# Strategieën voor BYOD

---

De meeste organisaties  
bevinden zich hier...



Verbieden

Beperkt toelaten

Omarmen



# Sommaire

---

- Introduction
- Stratégies
- Solutions BYOD
- Authentification forte
- Recommandations
- Conclusion

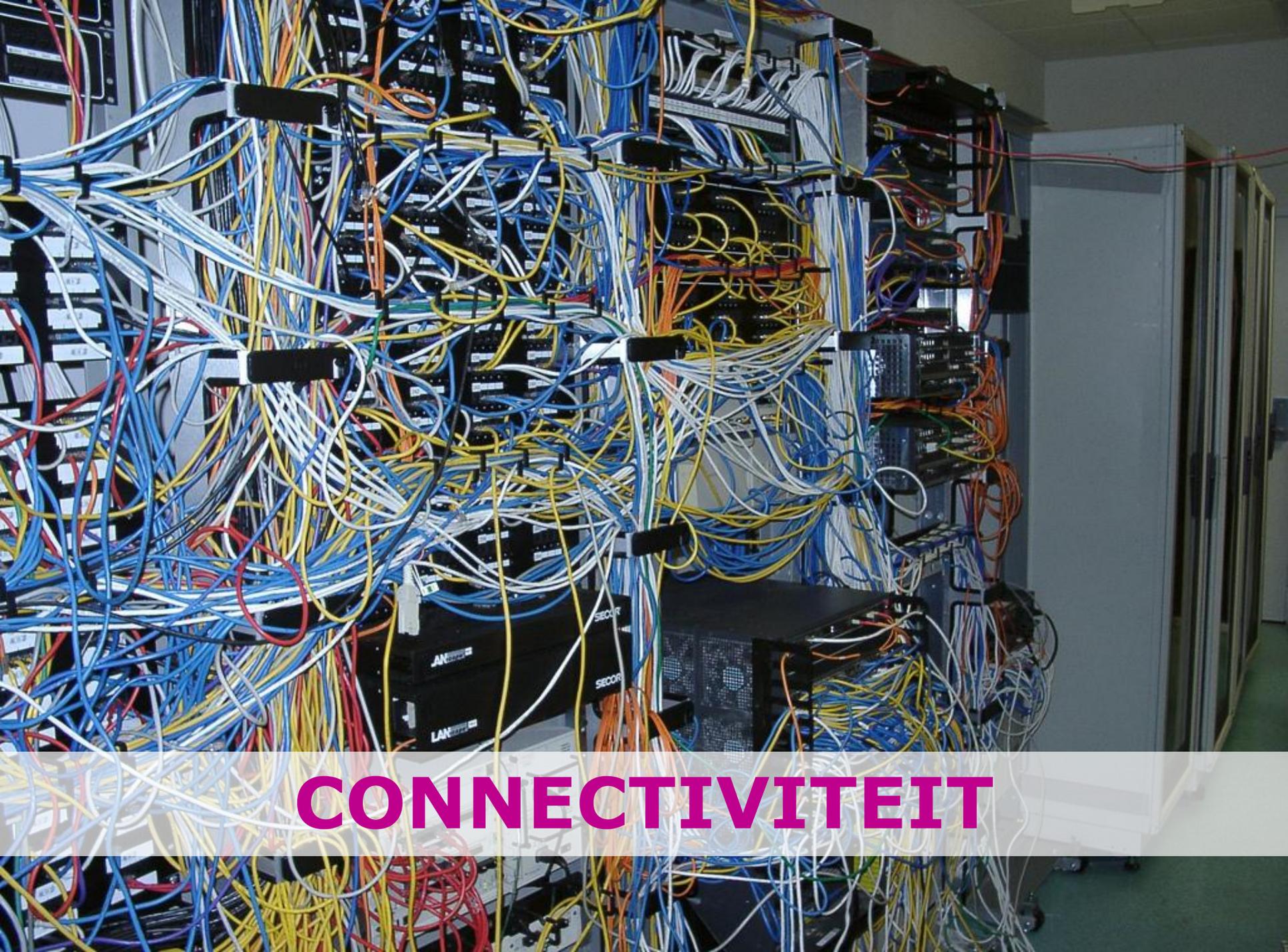


# Solutions

---

Type de solution	Fournisseurs
Réseau intelligent	Cisco
Mobile Device Management	Airwatch, MobileIron, Zenprise
Isolation	Enterploid, Thales
Virtualisation	Citrix, VMware





**CONNECTIVITEIT**

# Connectiviteit: "intelligente netwerken"

**Context-aware security:** policies gebaseerd op

Wie

Wat

Waar

Wanneer

Hoe



werknemer



guest

websites

social media

storage



wifi



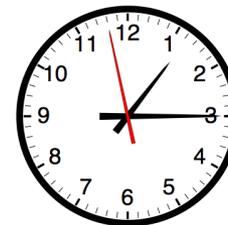
trusted wifi



mobile 3g/4g



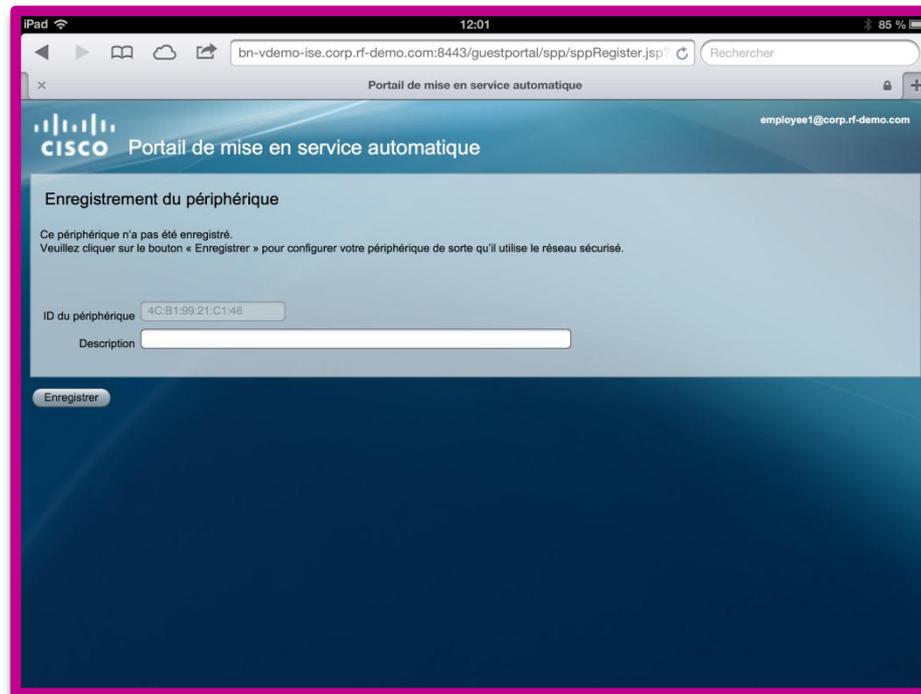
Lokaal netwerk



Intro – Stratégies – Solutions – Auth forte – Recommandations - Conclusion  
Réseau intelligent - MDM – Isolation – Virtualisation

# Demo Cisco ISE

- Introduction d'un nouvel appareil dans le réseau



1

**Intro – Stratégies – Solutions – Auth forte – Recommandations - Conclusion  
Réseau intelligent - MDM – Isolation – Virtualisation**

# Cisco ISE: logboek van authenticaties

## Live Authentications

Add or Remove Columns Refresh

Refresh Every 3 seconds Show

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
Oct 29,12 12:01:41.805 PM	✓		Employee1	4C:B1:99:21:C1:46		WLC1		PermitAccess	RegisteredDevices	NotApplicable	Authentication ...
Oct 29,12 12:01:40.354 PM	✓					WLC1					Dynamic Author...
Oct 29,12 12:00:07.611 PM	✓		Employee1	4C:B1:99:21:C1:46		WLC1		Provisioning	Profiled:Apple-Device	Pending	Authentication ...
Oct 29,12 11:58:30.362 AM	✓		Employee1	4C:B1:99:21:C1:46		WLC1		Provisioning	Profiled:Apple-Device	Pending	Authentication ...
Oct 29,12 11:57:08.135 AM	✓		Employee1	4C:B1:99:21:C1:46		WLC1		Provisioning	Profiled:Apple-Device	Pending	Authentication ...



# Cisco: Authorization policies

**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

▶ Exceptions (0)

**Standard**

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_802.1X	then Blackhole_Wireless_Access
✓	WirelessIPPhone	if <b>IP-Phone</b> AND Wireless_802.1X	then PermitAccess
⊖	AccessPoint-Flex	if <b>FlexAP OR JanzenGroup</b>	then FlexAP
⊖	No Guest access for Employees	if <b>RegisteredDevices</b> AND Network Access:EapAuthentication NOT_EQUALS EAP-TLS	then DenyAccess
✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones
✓	BYOD_Registration	if <b>(Android OR Apple-iPad OR Apple-iPhone OR Apple-Device)</b> AND AD1:ExternalGroups EQUALS corp.rf-demo.com/Users/Domain Users	then Provisioning
✓	BYOD_Registered	if <b>RegisteredDevices</b> AND Network Access:EapAuthentication EQUALS EAP-TLS	then PermitAccess
⊖	Android Redirect	if <b>RegisteredDevices</b>	then Google_Play_redirect
✓	Guest	if <b>Guest OR ActivatedGuest</b>	then Guest-VLAN
✓	Default	if no matches, then CWA	

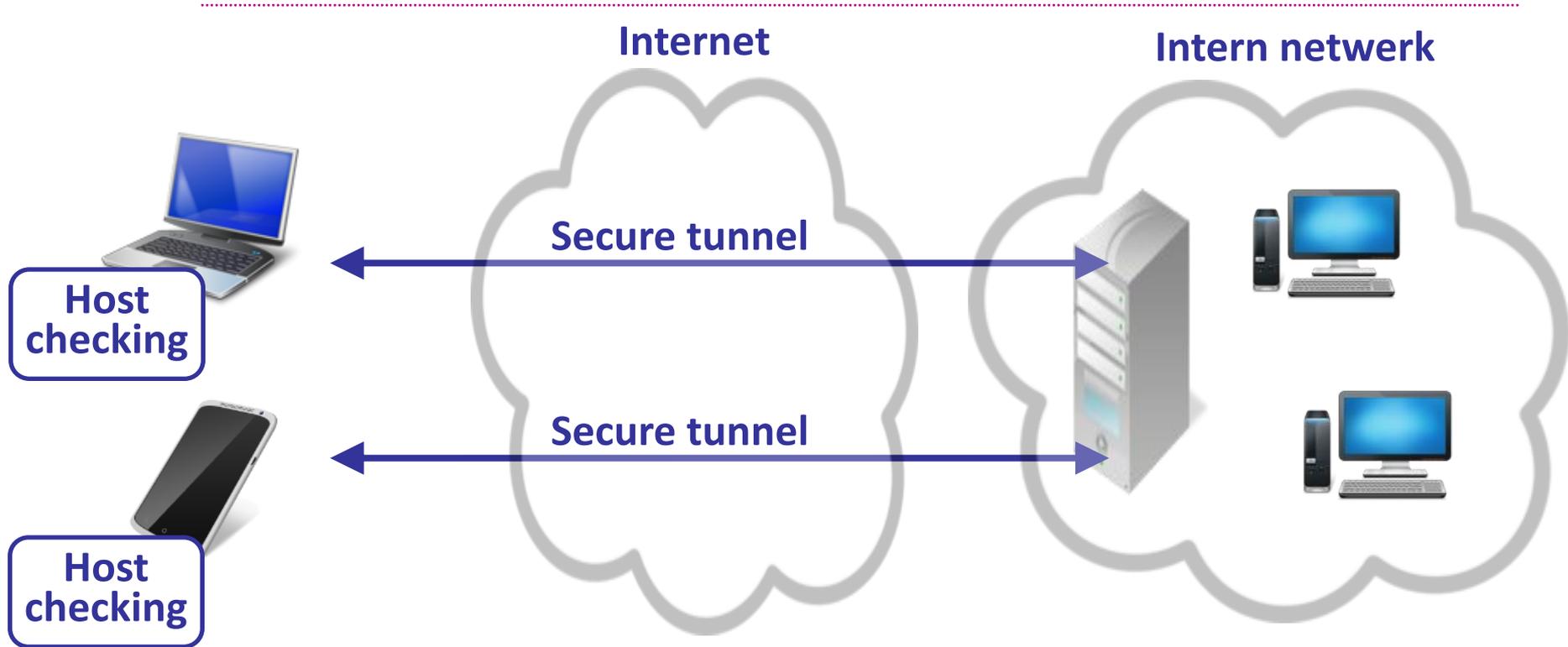
# Conclusie "intelligente netwerken"

---

- Intelligente netwerken: evolutie, trend
- Vereist aanpassingen aan de infrastructuur
- Voordeel van centraal beheer



# Mobile VPN



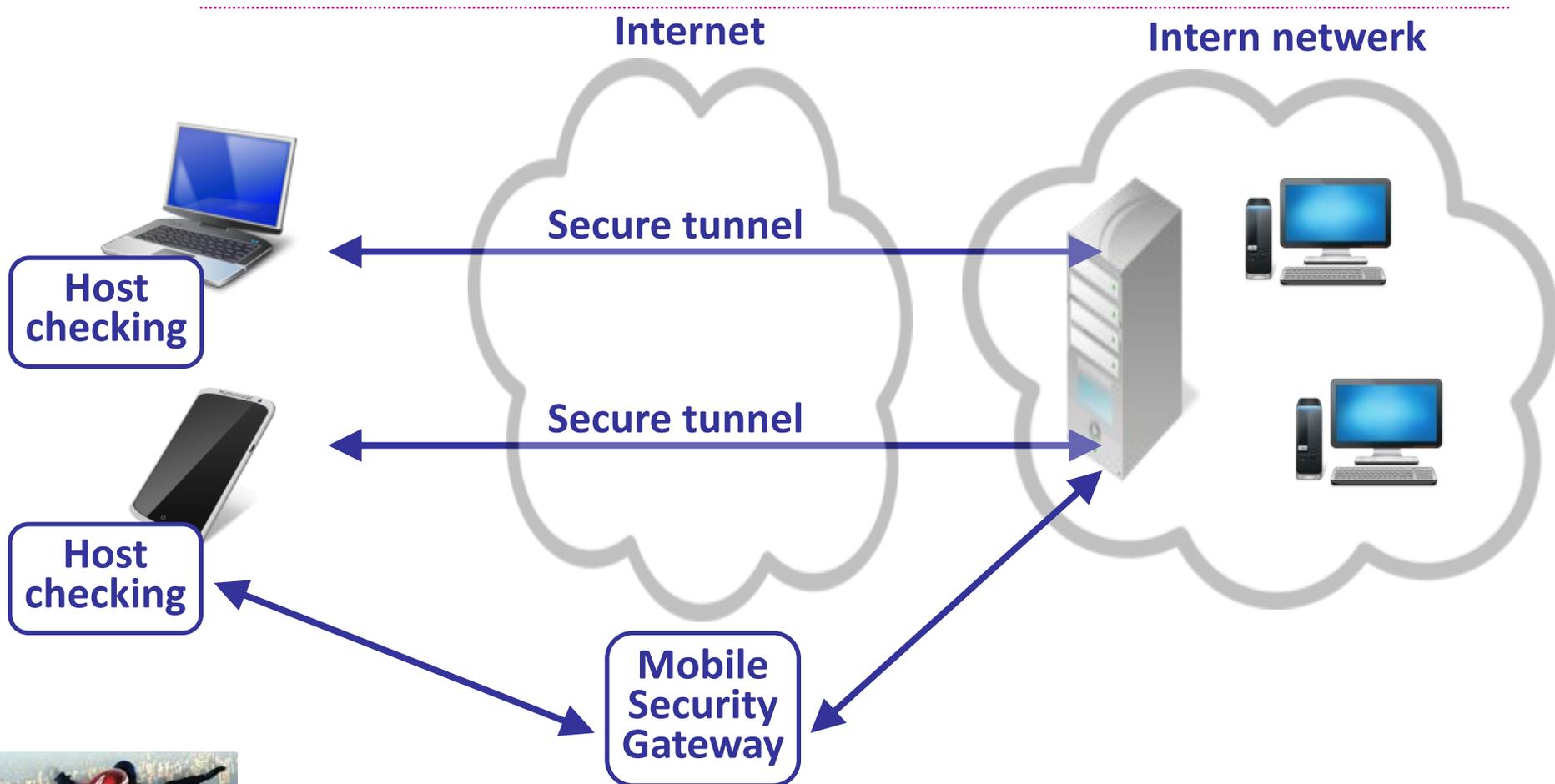
# Mobile VPN

---

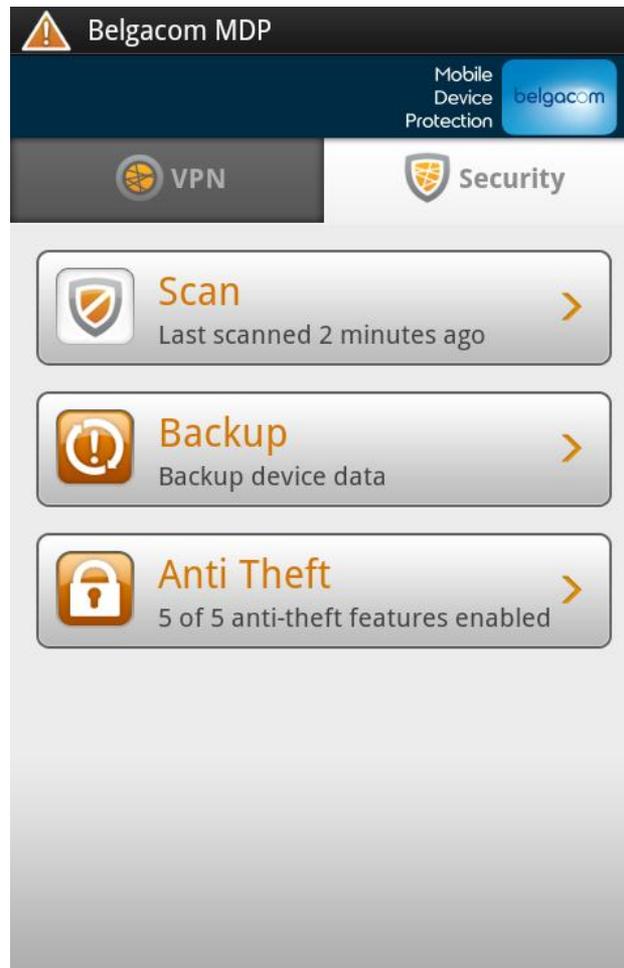
- Beveiligde verbinding tussen toestel en bedrijfsnetwerk
- Basisidee: zelfde policy op alle toestellen
  - Huidige policy voor laptops ook toepassen voor tablets en smartphones
- Authenticatie: certificaat + token of eID
- Host-checking: zelfde mogelijkheden op mobiele devices?
- Testen Juniper Junos Pulse client + Mobile Security Gateway



# Mobile VPN



# Mobile VPN





**MOBILE DEVICE MANAGEMENT**

# Mobile Device Management

---

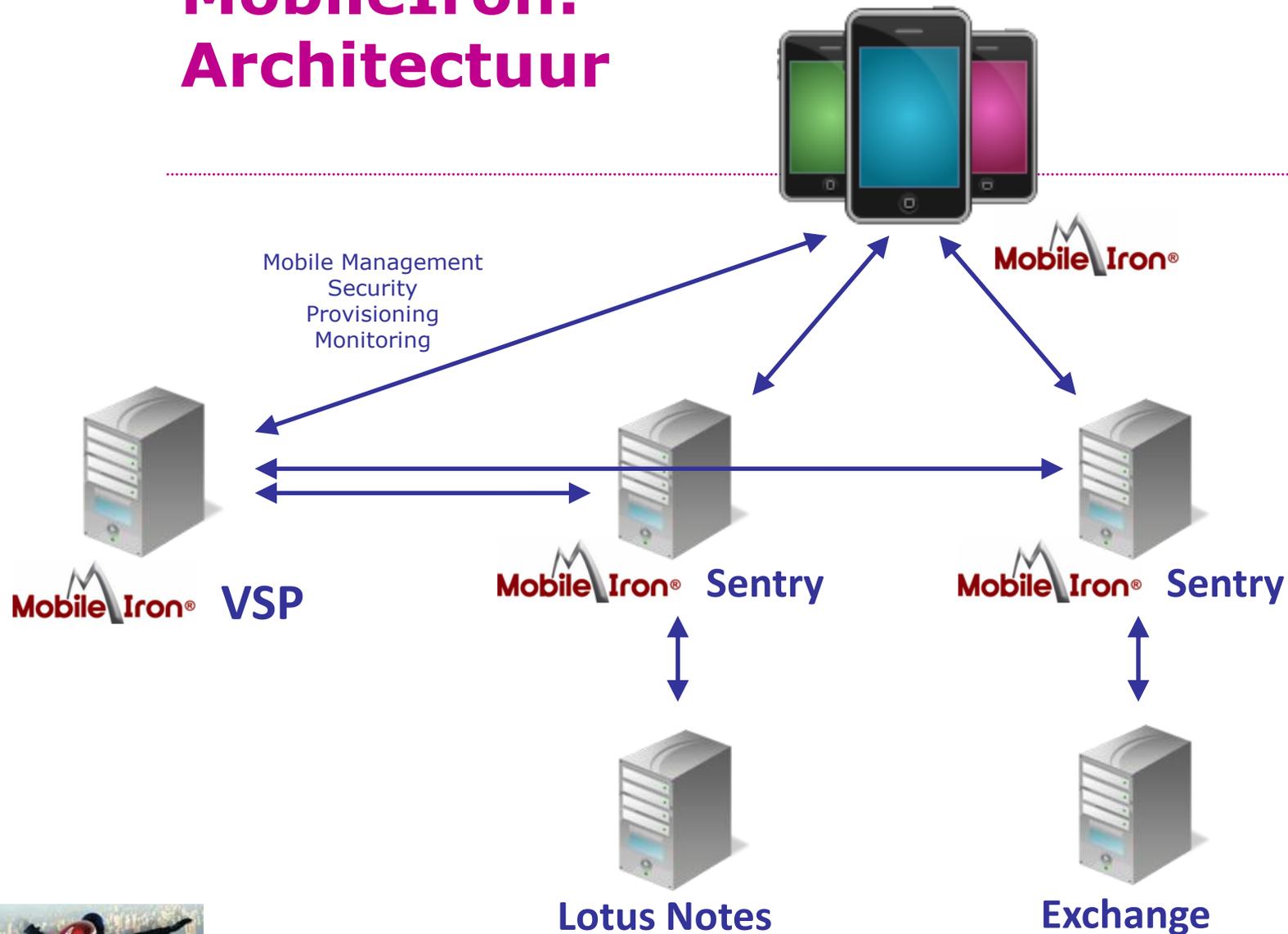
- Evaluatie van MDM oplossingen



- POC uitgevoerd met MobileIron
  - Corporate devices



# MobileIron: Architectuur



# Functionaliteiten

- Inventaris
- Security policies
- Monitoring
- Provisioning
- App control
- Lock & wipe

User	Number	Phone	OS	Country	Status	Last Connected	E/C	Registered	Opera...
Clarissa...	141560...	iPhone 3GS	iOS 4.0	United States	Active	4 h 15 m	C	2010-08-06 12:48:11...	AT&T
Eric Mid...	140820...	iPhone 3GS	iOS 4.0	United States	Active	6 d 7 h	C	2010-08-02 10:36:25...	AT&T
Greg Ge...	+16508...	iPhone 4	iOS 4.0	United States	Active	5 d 1 h	C	2010-08-03 5:58:43 PM	AT&T
JC Counts	PDA	Compromised Device OS Unlocked	iOS 4.0	United States	Wiped	6 d 5 h	E	2010-08-02 1:43:21 PM	AT&T
Jesse Li...	+12026...	iPhone 4	iOS 4.0	United States	Active	2 d 4 h	C	2010-08-04 5:45:17 PM	AT&T
Kimberly...	408221...	Not Available	iOS	United States	Pending		E	2010-08-02 2:23:02 PM	AT&T
Lance M...	+12316...	iPhone 4	iOS 4.0	United States	Active	1 h 56 m	C	2010-08-08 4:32:19 PM	AT&T
Lance M...	123140...	LGE-GW820 by...	WinMo	United States	Active	2 h 50 m	E	2010-08-08 4:39:21 PM	AT&T
Nick Rago	165041...	iPhone 3GS	iOS 4.0	United States	Active	2 h 20 m	C	2010-08-02 12:31:17...	AT&T
Randy P...	167851...	iPhone 3GS	iOS 4.0	United States	Active	5 h 27 m	C	2010-08-02 11:34:20...	AT&T
Robert...	408204...	9630 by Resear...	Blac...	United States	Active	1 m 0 s	E	2010-08-03 2:17:14 PM	Verizon
Samir G...	+16509...	iPhone 4	iOS 4.0	United States	Active	6 d 5 h	C	2010-08-02 1:53:29 PM	AT&T
Sean Gi...	PDA	iPod touch, ...	iOS		Active	6 d 1 h	C	2010-08-01 10:19:42...	PDA
Sean Gi...	+16504...	iPhone 4	iOS 4.0	United States	Active	Not MDM checke...	C	2010-08-02 9:26:32 AM	AT&T
Sean Gi...	301706...	iPhone 3GS	iOS 4.0	United States	Active	2 d 1 h	C	2010-08-06 5:58:08 PM	AT&T



# Functionaliteiten

Inventaris

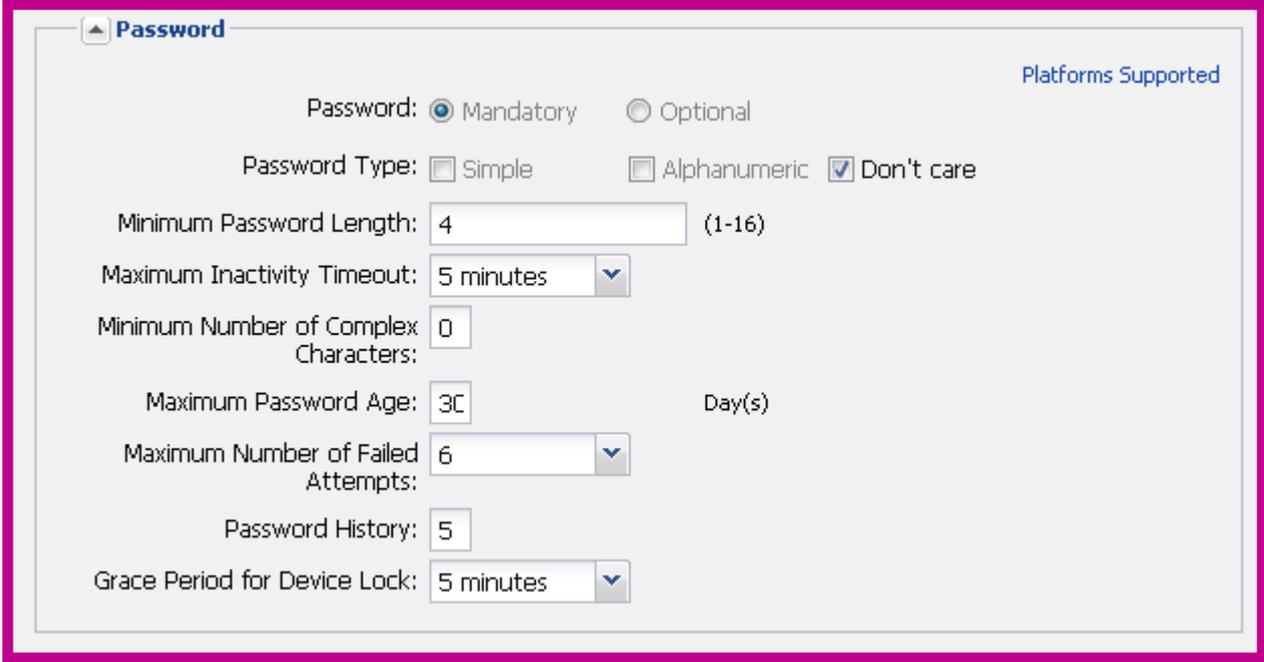
Security policies

Monitoring

Provisioning

App control

Lock & wipe



**Password** Platforms Supported

Password:  Mandatory  Optional

Password Type:  Simple  Alphanumeric  Don't care

Minimum Password Length:  (1-16)

Maximum Inactivity Timeout:

Minimum Number of Complex Characters:

Maximum Password Age:  Day(s)

Maximum Number of Failed Attempts:

Password History:

Grace Period for Device Lock:



# Functionaliteiten

Inventaris

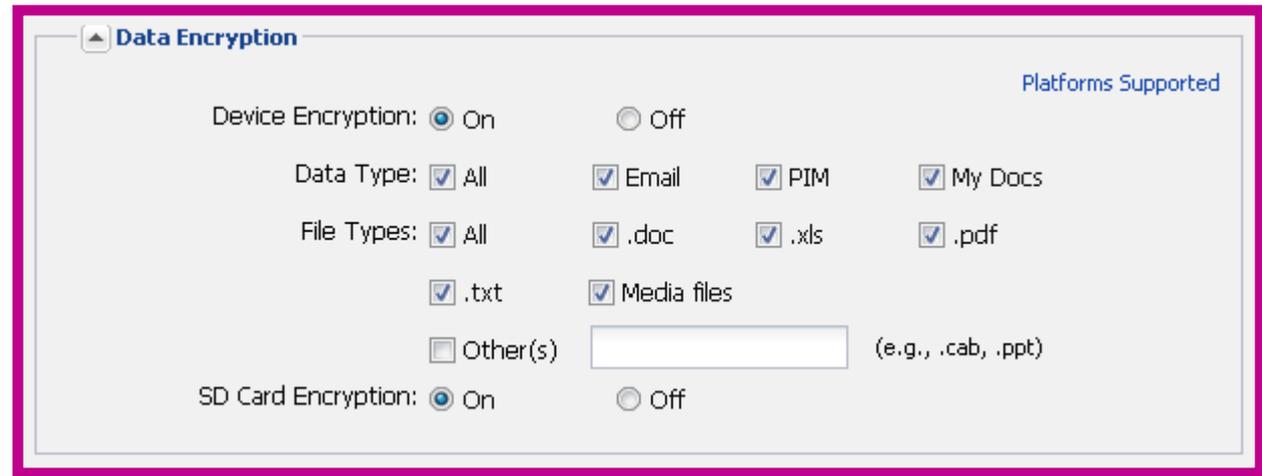
Security policies

Monitoring

Provisioning

App control

Lock & wipe



**Data Encryption** Platforms Supported

Device Encryption:  On  Off

Data Type:  All  Email  PIM  My Docs

File Types:  All  .doc  .xls  .pdf

.txt  Media files

Other(s)  (e.g., .cab, .ppt)

SD Card Encryption:  On  Off



# Functionaliteiten

Inventaris

Security policies

Monitoring

Provisioning

App control

Lock & wipe

**For iOS devices**

- Block ActiveSync and Send Alert when iOS version is less than 3.0
- Block ActiveSync and Send Alert when Data Protection is disabled
- Block ActiveSync and Send Alert when a compromised iOS device is detected
- Block ActiveSync and Send Alert for the following disallowed devices
  - Allowed**  
Original iPhone  
iPhone 3G  
iPhone 3GS  
iPod touch, 1st gen
  - Disallowed**
- Block ActiveSync and Send Alert when device MDM is deactivated (iOS 5.0 or higher)

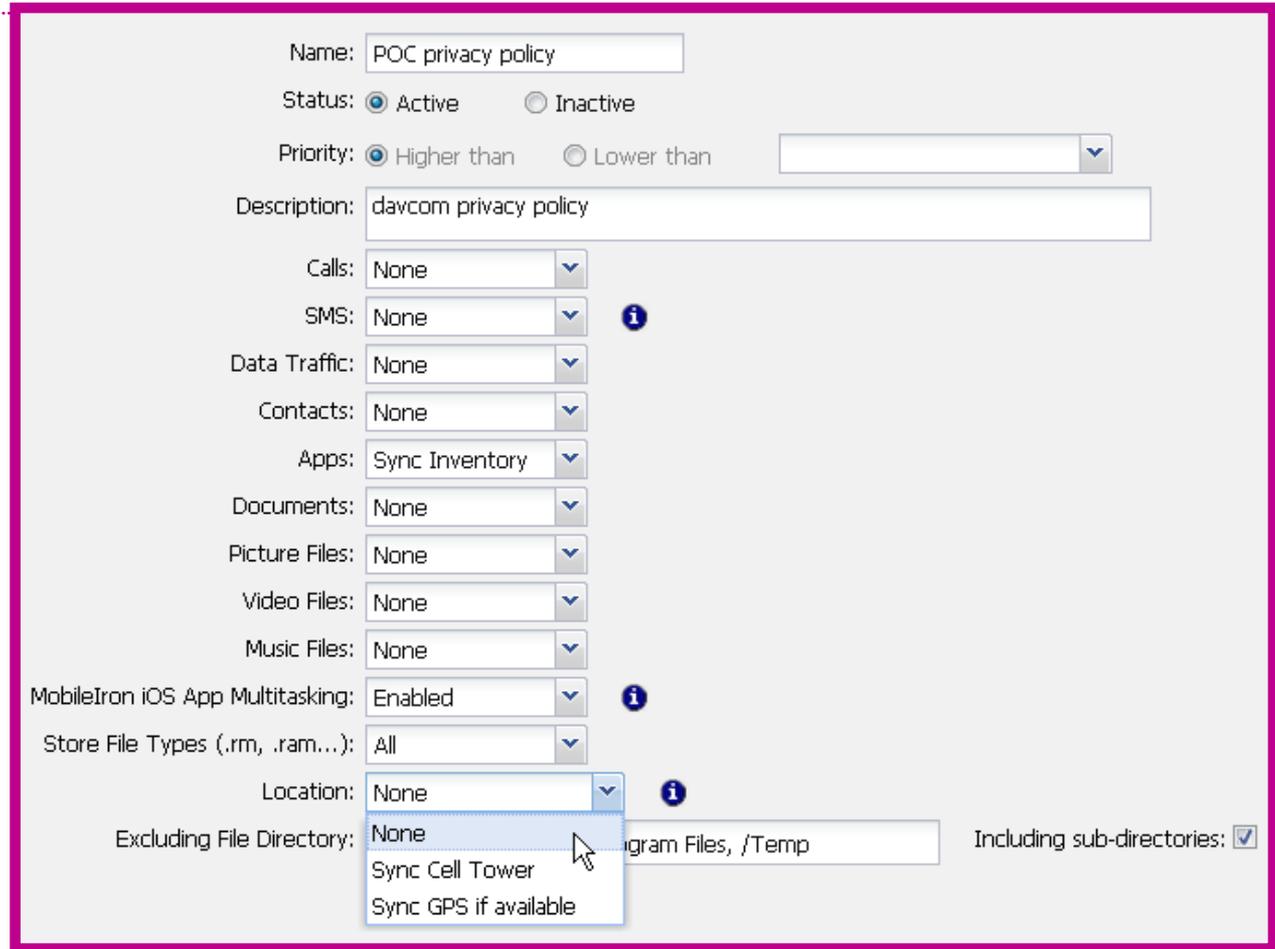
**For Android devices**

- Block ActiveSync and Send Alert when Android version is less than 2.2
- Block ActiveSync and Send Alert when a compromised Android device is detected
- Block ActiveSync and Send Alert when Data Encryption is disabled
- Block ActiveSync and Send Alert when device administrator is deactivated



# Functionaliteiten

- Inventaris
- Security policies**
- Monitoring
- Provisioning
- App control
- Lock & wipe



Name: POC privacy policy

Status:  Active  Inactive

Priority:  Higher than  Lower than

Description: davcom privacy policy

Calls: None

SMS: None

Data Traffic: None

Contacts: None

Apps: Sync Inventory

Documents: None

Picture Files: None

Video Files: None

Music Files: None

MobileIron iOS App Multitasking: Enabled

Store File Types (.rm, .ram...): All

Location: None

Excluding File Directory: None

Including sub-directories:



# Functionaliteiten

Inventaris

Security policies

Monitoring

Provisioning

App control

Lock & wipe

MobileIron Smartphones | System

Smartphones & Users | Mobile Activity Intelligence | Security & Policies | Apps & Files | Troubleshooting

Dashboard | All Smartphones | ActiveSync Smartphones | BES Smartphones | Retired Smartphones | Manage Labels | User Management

All Smartphones(1.1.2-3.0.1-57)

Lock | Wipe | More Actions | Labels: All-Smartphones | Search by User | Advanced Search | Reg

User	Number	Phone	OS	Country	Status	Last Connected	E/C	Registered	Opera...
Clarissa...	141560...	iPhone 3GS	iOS 4.0	United States	Active	4 h 15 m	C	2010-08-06 12:48:11...	AT&T
Eric Mid...	140820...	iPhone 3GS	iOS 4.0	United States	Active	6 d 7 h	C	2010-08-02 10:36:25...	AT&T
Greg Ge...	+16508...	iPhone 4	iOS 4.0	United States	Active	5 d 1 h	C	2010-08-03 5:58:43 PM	AT&T
JC Counts	PDA	Compromised Device OS Unlocked	iOS 4.0	United States	Wiped	6 d 5 h	E	2010-08-02 1:43:21 PM	AT&T
Jesse Li...	+12026...	iPhone 4	iOS 4.0	United States	Active	2 d 4 h	C	2010-08-04 5:45:17 PM	AT&T
Kimberly...	408221...	Not Available	iOS	United States	Pending		E	2010-08-02 2:23:02 PM	AT&T
Lance M...	+12316...	iPhone 4	iOS 4.0	United States	Active	1 h 56 m	C	2010-08-08 4:32:19 PM	AT&T
Lance M...	123140...	LGE-GW820 by...	WinMo	United States	Active	2 h 50 m	E	2010-08-08 4:39:21 PM	AT&T
Nick Rago	165041...	iPhone 3GS	iOS 4.0	United States	Active	2 h 20 m	C	2010-08-02 12:31:17...	AT&T
Randy P...	167851...	iPhone 3GS	iOS 4.0	United States	Active	5 h 27 m	C	2010-08-02 11:34:20...	AT&T
Robert...	408204...	9630 by Resear...	Blac...	United States	Active	1 m 0 s	E	2010-08-03 2:17:14 PM	Verizon
Samir G...	+16509...	iPhone 4	iOS 4.0	United States	Active	6 d 5 h	C	2010-08-02 1:53:29 PM	AT&T
Sean Gi...	PDA	iPod touch, ...	iOS		Active	6 d 1 h	C	2010-08-01 10:19:42...	PDA
Sean Gi...	+16504...	iPhone 4	iOS 4.0	United States	Active	Not MDM checke...	C	2010-08-02 9:26:32 AM	AT&T
Sean Gi...	301706...	iPhone 3GS	iOS 4.0	United States	Active	2 d 1 h	C	2010-08-06 5:58:08 PM	AT&T



# Functionaliteiten

Inventaris

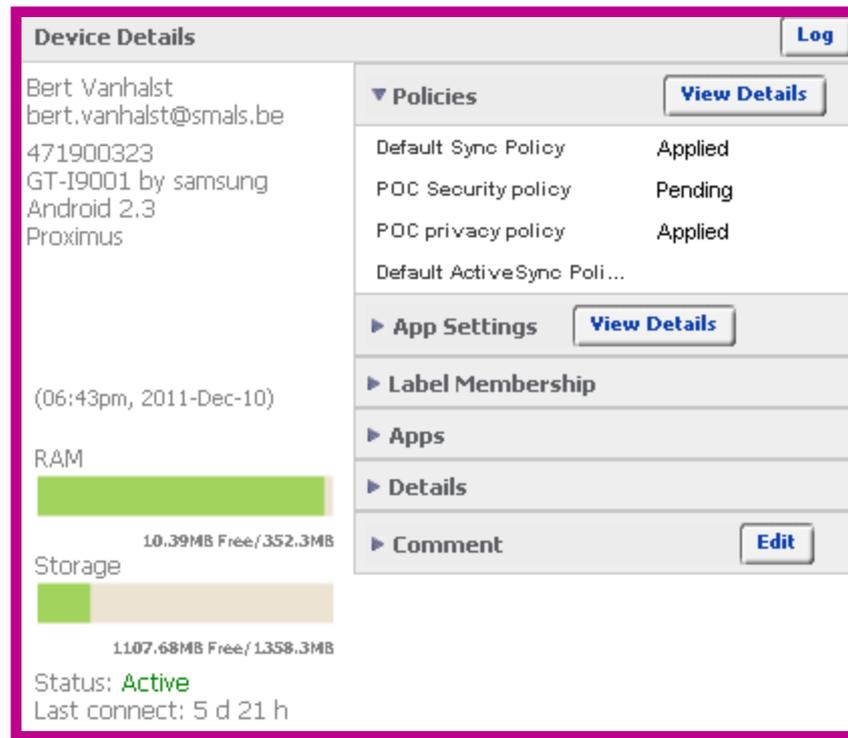
Security policies

Monitoring

Provisioning

App control

Lock & wipe

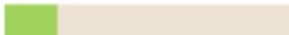


**Device Details** [Log](#)

Bert Vanhalst  
bert.vanhalst@smals.be  
471900323  
GT-I9001 by samsung  
Android 2.3  
Proximus

(06:43pm, 2011-Dec-10)

RAM  
  
10.39MB Free / 352.3MB

Storage  
  
1107.68MB Free / 1358.3MB

Status: **Active**  
Last connect: 5 d 21 h

**▼ Policies** [View Details](#)

Default Sync Policy	Applied
POC Security policy	Pending
POC privacy policy	Applied
Default ActiveSync Poli...	

**▶ App Settings** [View Details](#)

**▶ Label Membership**

**▶ Apps**

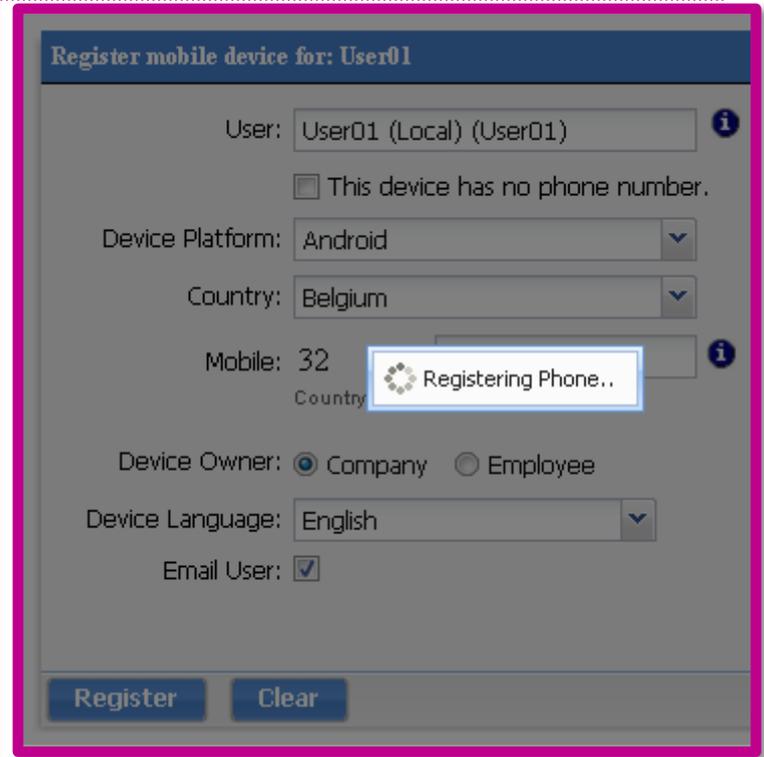
**▶ Details**

**▶ Comment** [Edit](#)



# Functionaliteiten

- Inventaris
- Security policies
- Monitoring
- Provisioning**
- App control
- Lock & wipe



# Functionaliteiten

Inventaris

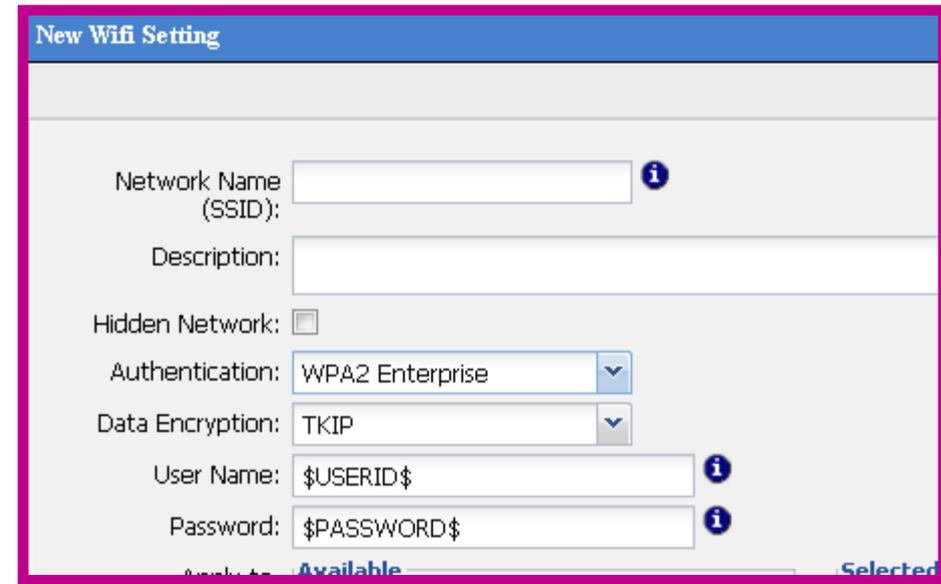
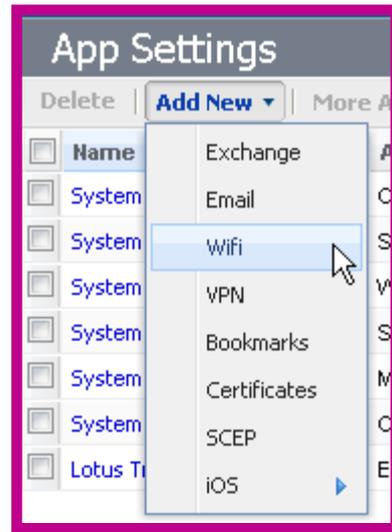
Security policies

Monitoring

Provisioning

App control

Lock & wipe



# Functionaliteiten

Inventaris

Security policies

Monitoring

Provisioning

App control

Lock & wipe

All Smartphones

Lock | Wipe | More Actions ▾ | Labels: All-Smartphones ▾ | Search by Us

<input type="checkbox"/>	User ▲	Number	Phone	OS	Country
<input checked="" type="checkbox"/>	User01	470803381	 Nexus S by samsung	Android 2.3	Belgium
<input type="checkbox"/>	User01	+32470188821		<b>App Control Security Policy Violated</b> Violating app(s) should be added or removed	

Device Details Log

User01  
bert.vanhalst@smals.be  
470803381  
Nexus S by samsung  
Android 2.3  
Proximus



(01:22pm, 2011-Sep-21)

▼ Policies View Details

Default Security Policy	Pending
Default Privacy Policy	Applied
Default Sync Policy	Applied

► App Settings

► Label Membership

▼ Apps

3G Watchdog 0.30.1
 Beyond Tetris 1.1.2
Lotus Installer 8.5.2.3 201105311501
Maps 5.10.0
Market 2.3.6



# Functionaliteiten

Inventaris

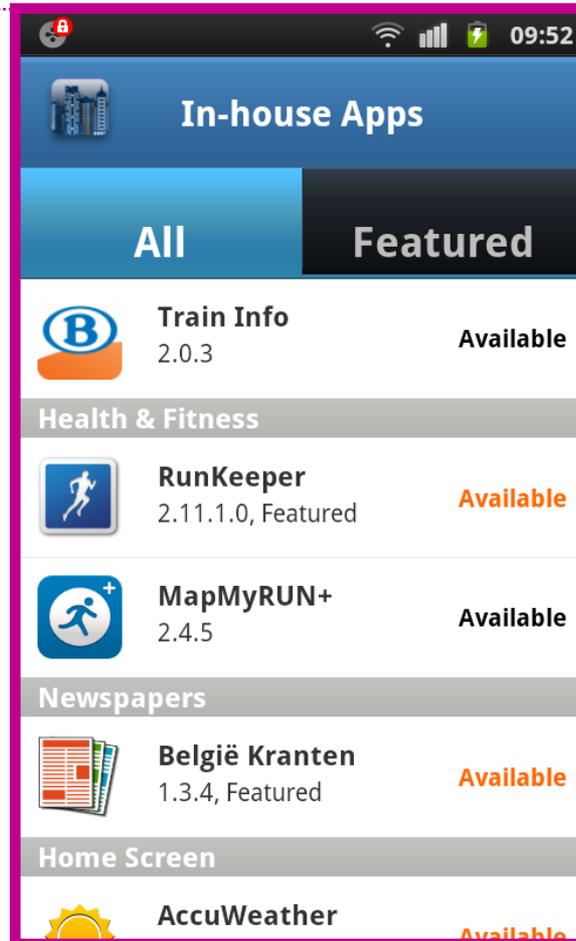
Security policies

Monitoring

Provisioning

App control

Lock & wipe



# Functionaliteiten

- Inventaris
- Security policies
- Monitoring
- Provisioning
- App control
- Lock & wipe



All Smartphones

Lock | Wipe | More Actions ▾ | Labels: All-Smartphones | Search by Us

<input type="checkbox"/>	User ▲	Number	Phone	OS	Country
<input checked="" type="checkbox"/>	User01	470803381	Nexus S by samsung	Android 2.3	Belgium
<input type="checkbox"/>	User01	+32470188821		<b>App Control Security Policy Violated</b> Violating app(s) should be added or removed	



# Security policy

## Voorzie minimaal het volgende:

---

- Verplicht paswoord
  - Timeout period
  - Password retry limit
- Data encryptie
- Platformen:
  - Android 4.0 of hoger
  - iOS 5.0 of hoger
- Geen rooted/jailbroken devices
- Blokkeer toegang tot bedrijfsnetwerk voor non-compliant devices



# MDM bruikbaar in een BYOD context?

---

- Beveiliging op niveau van het **toestel**
  - ... en secure email
- Opletten met **privacy**
  - Geen strikte scheiding van de omgevingen
  - Remote wipe, lokalisatie, monitoring
- Tendens naar application en data security
  - MobileIron AppConnect / AppTunnel





**Isolation**

# Isolation : principes

- Principe
  - Créer un environnement professionnel cloisonné
  - L'employeur ne contrôle que l'environnement professionnel
  - L'employé est responsable de la partie privée

Environnement privé

Environnement  
professionnel

Environnement privé

Environnement  
professionnel



# Isolation : fonctionnalités

---

- Fonctionnalités essentielles (dans l'environnement professionnel):
  - Cloisonnement par rapport à l'environnement hôte
  - Chiffrement des données
  - Installation d'applications
  - Remote Wipe



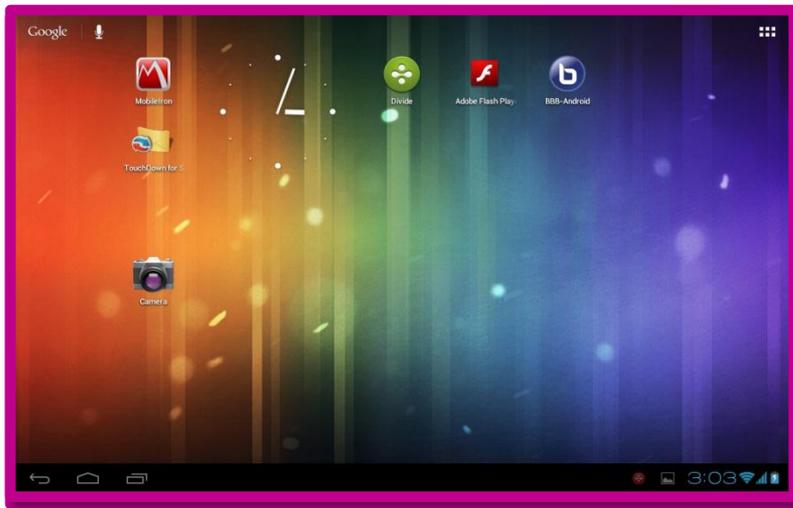
# Isolation : solutions

- Principales solutions :
  - Divide (Enterproid)
  - Teopad (Thales)
    - Demo



# Isolation : Divide

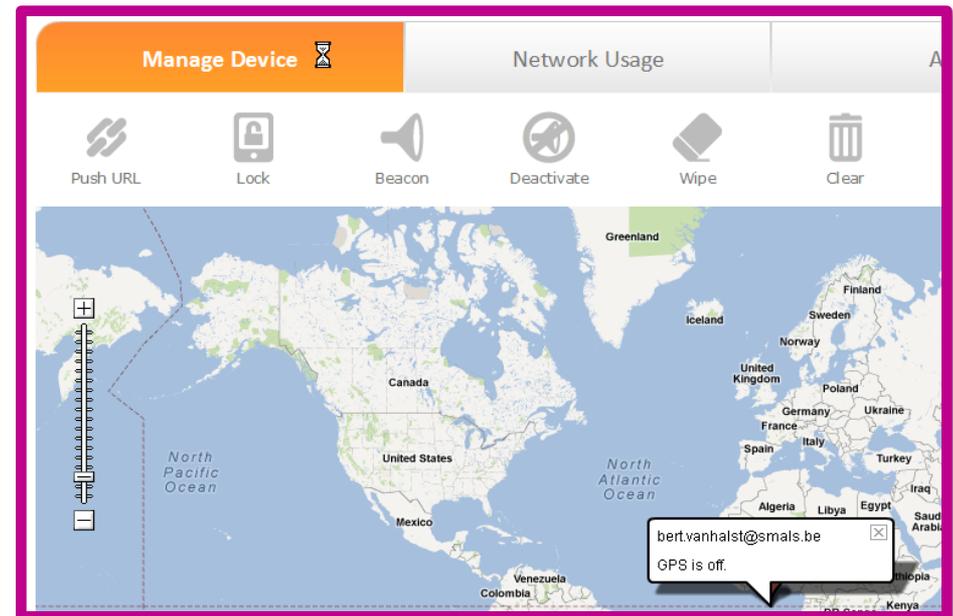
- Orienté respect de la vie privée : l'utilisateur reste maître de son appareil
- Bureau privé / Bureau professionnel



# Isolation : Divide

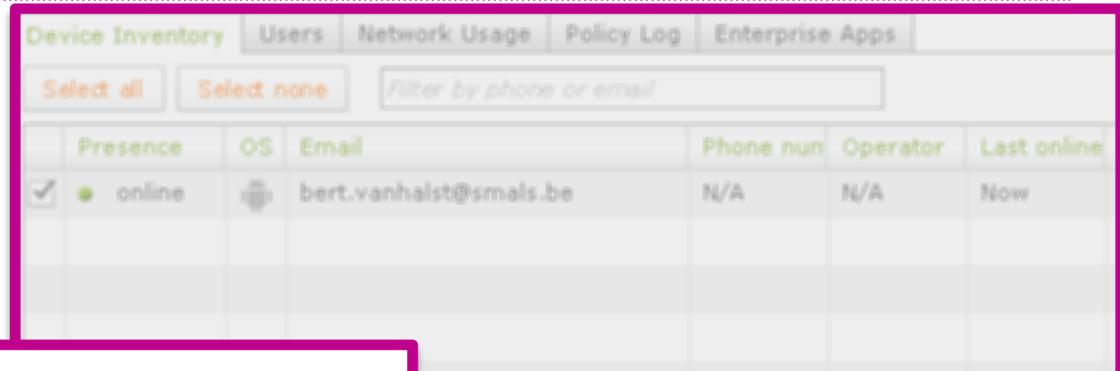
- Interface admin pour l'utilisateur et pour l'employeur
- L'utilisateur peut ne pas révéler certaines informations (position, consommation de données personnelles)

Detail	Apps	Policy Settings	Settings
Internet state			CONNECTED
Internet type			WIFI
is_device_admin			true
last_status_update			1346156802
Latitude			0
locale			en_GB
Location fixed time			-
Location privacy			Only show in My Divide
Location provider			
Longitude			0
Mail sync time (ActiveSync)			-
Maximum battery level			100
Microphone mute			Off
Model number			GT-I9001
Music active			Off
Music volume			7/15
Network provider			



# Isolation : Divide

- Suppression des données professionnelles



Presence	OS	Email	Phone num	Operator	Last online
<input checked="" type="checkbox"/>	online	bert.vanhaalst@smals.be	N/A	N/A	Now



https://manager.divide.com

Domain Policies Administer device

Device Inventory

Select all

Presence

online

Screenlock

Configure

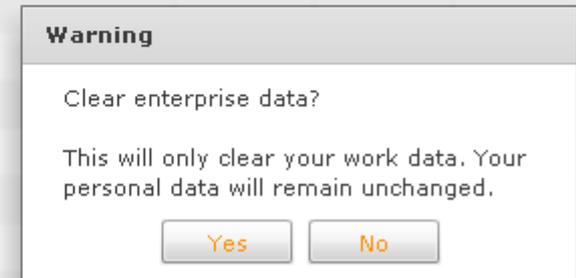
Locate

Status

Remote Wipe

EMDF

Corporate data only



**Warning**

Clear enterprise data?

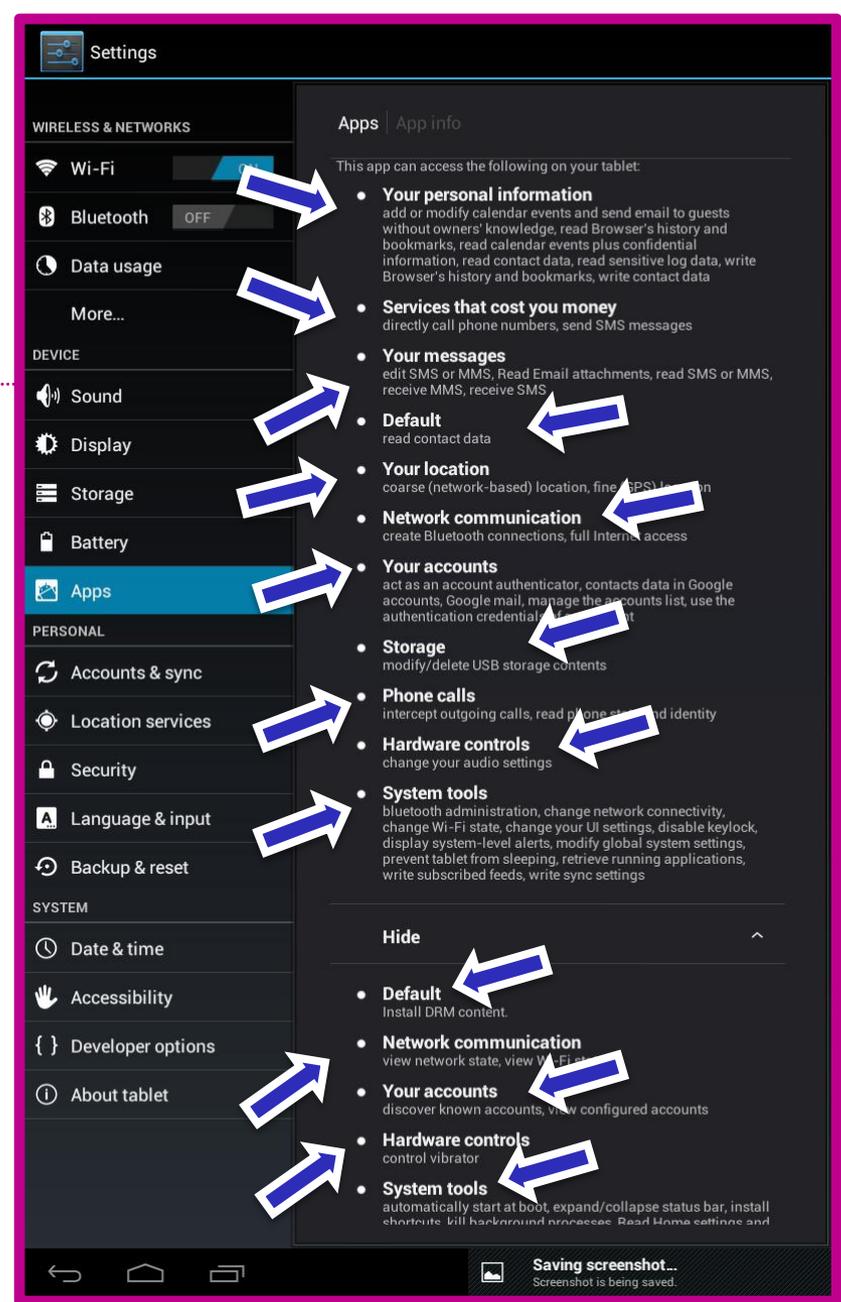
This will only clear your work data. Your personal data will remain unchanged.

Yes No



# Isolation : Divide

- Des besoins d'accès au système normaux...
- mais qui inquiètent les utilisateurs...
- à tort (?)
- Nécessite de désactiver une option de sécurité d'Android



# Isolation : avantages/inconvénients

---

- Avantages
  - Respect de la vie privée
  - Politique de sécurité de l'entreprise n'interfère pas avec l'environnement privé
  - Contrôle des applications utilisées pour la manipulation des données professionnelles
- Inconvénients
  - Solutions pas toujours mûres
  - Expérience variable en fonction de l'OS
  - Pas adapté pour les PC (virtualisation = piste ? )



# PAUSE

---



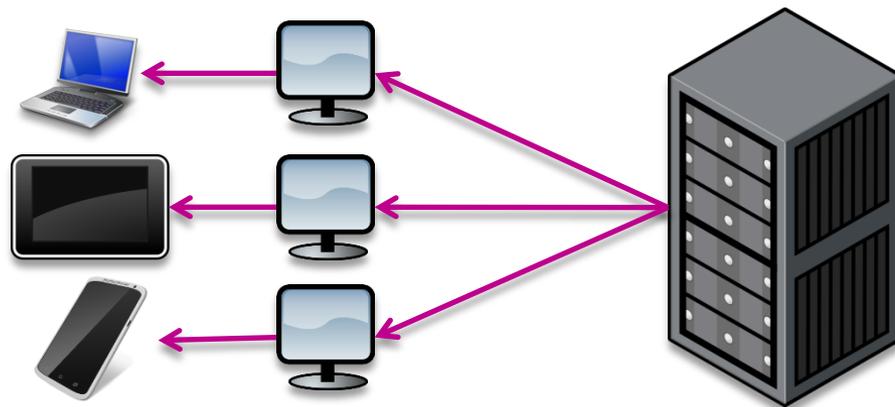
Table with multiple columns and rows of data, likely representing a dataset or log. The text is rotated 90 degrees counter-clockwise.

# Virtualisation (client léger)

# Virtualisation : principe

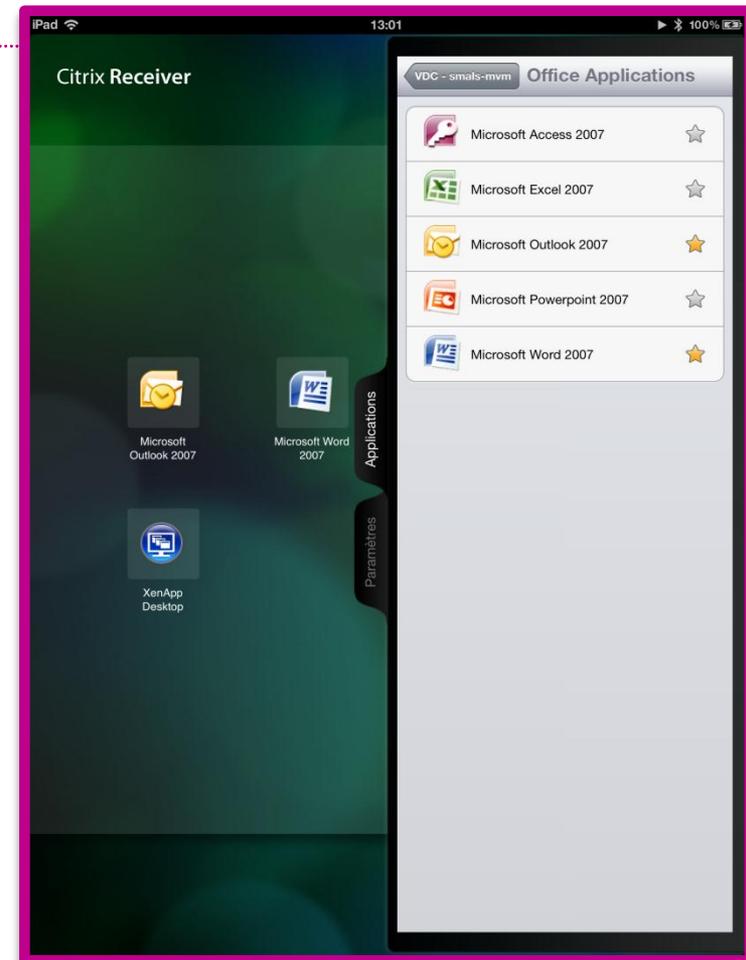
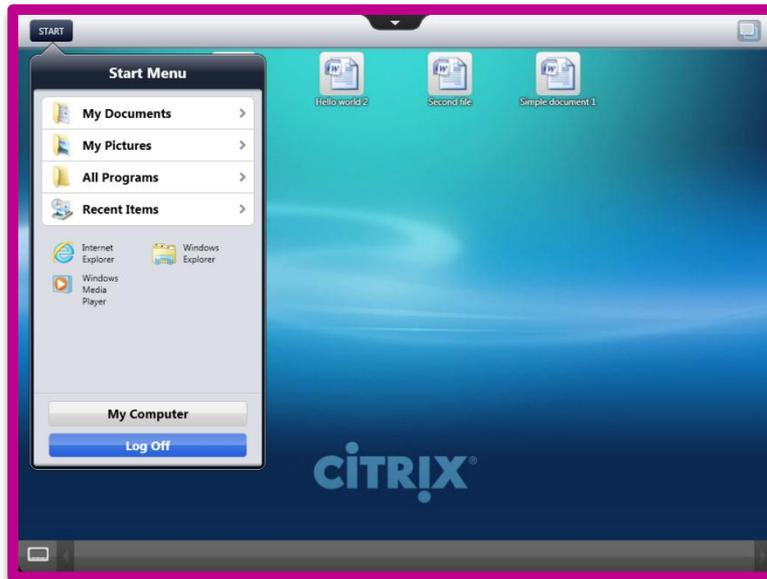
---

- Virtualisation = brique pour mise en place infrastructure client léger
- Client léger
  - Environnement géré par l'entreprise
  - Affichage déporté vers l'appareil de l'employé
  - Protocole de communication optimisé



# Virtualisation : Xenapp (Citrix)

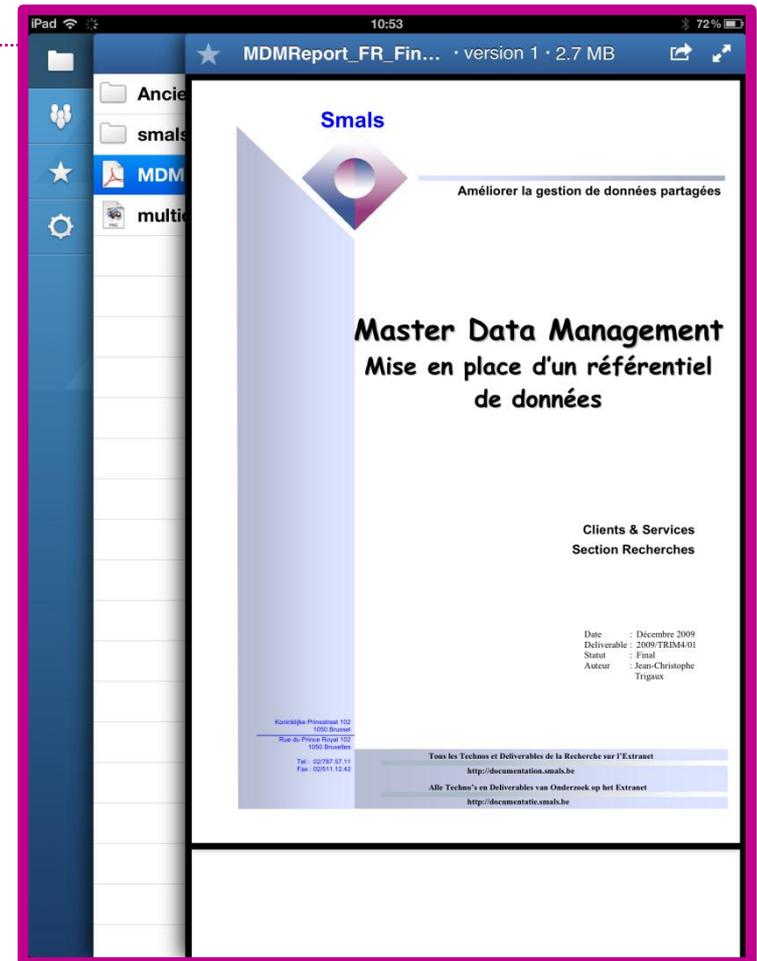
- Xenapp (Citrix)
  - Catalogue d'applications
  - Catalogue de machines virtuelles
  - Bureau spécifique (pour interfaces tactiles)



Intro – Stratégies – **Solutions** – Auth forte – Recommandations - Conclusion  
Réseau intelligent - MDM – Isolation – **Virtualisation**

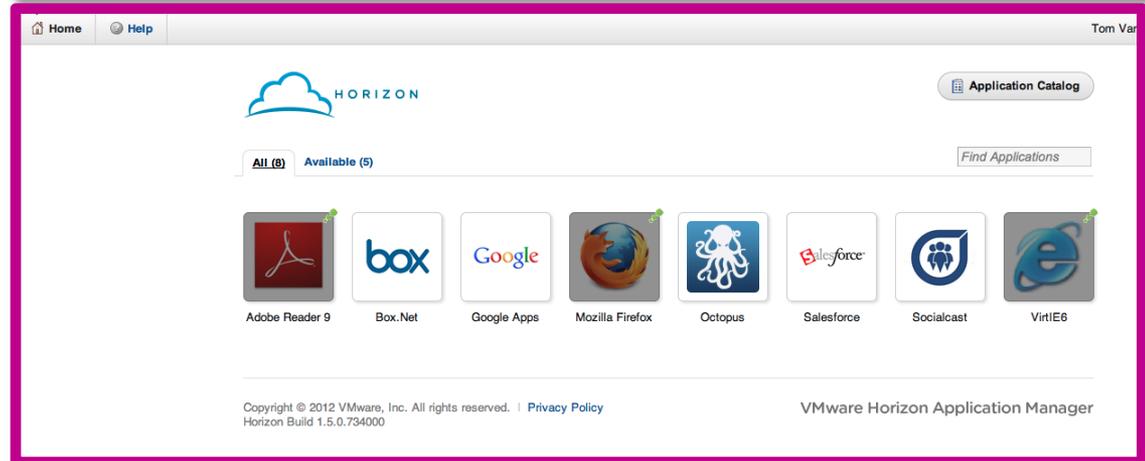
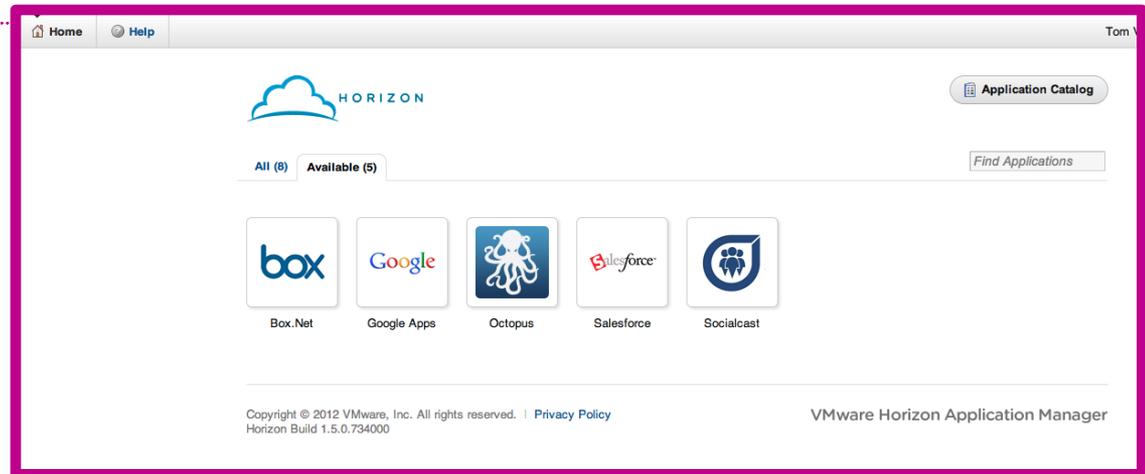
# Virtualisation : Horizon (VMware)

- VMware Horizon data
  - Sorte de Dropbox pour l'entreprise



# Virtualisation : Horizon VMware

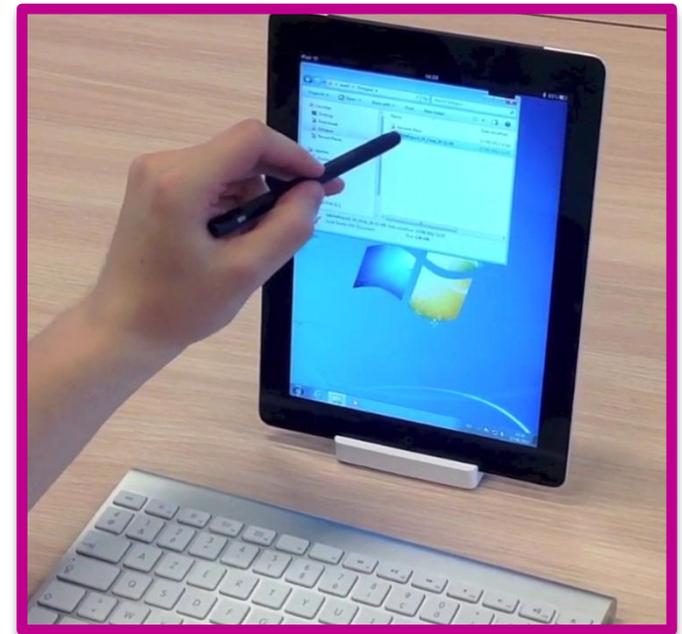
- VMware Horizon Application Manager
  - Catalogue applicatif



# Virtualisation : fonctionnalités et démos

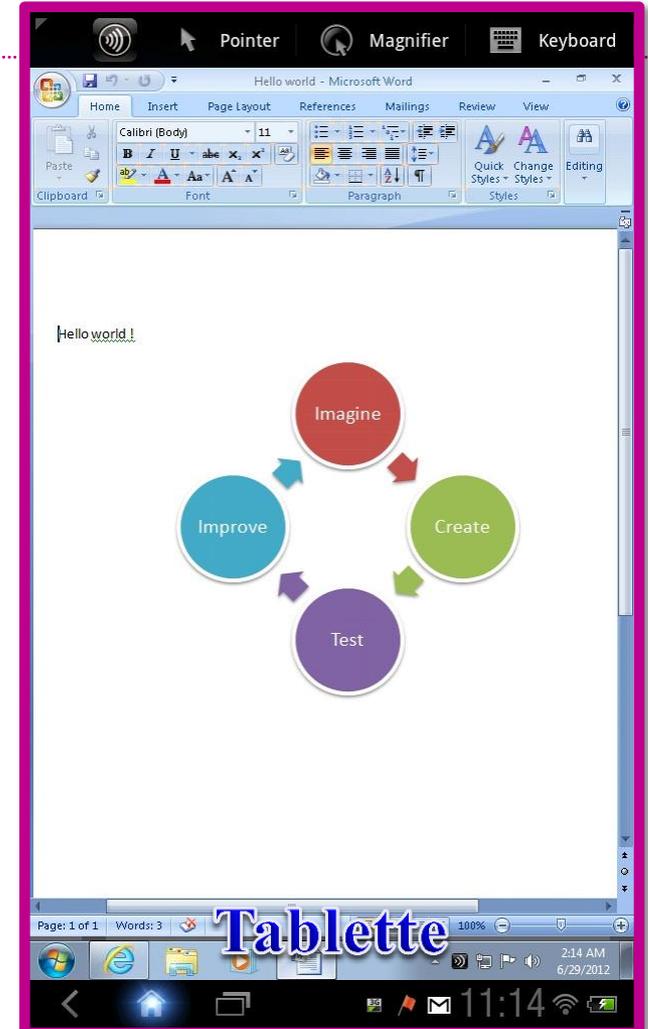
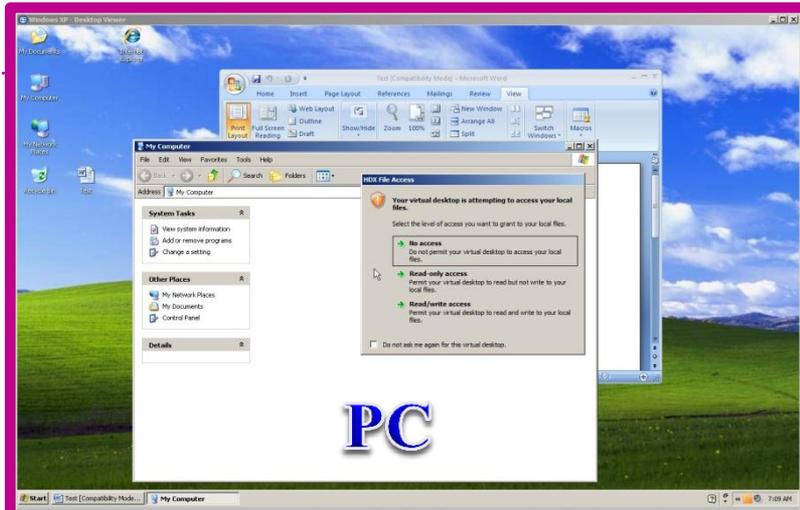
---

- Support de l'USB (pour PC)
- Indépendance par rapport au type d'appareil
- Session sauvée sur une machine distante



4

# Virtualisation : usability



# Virtualisation : avantages/inconvénients

---

- Avantages
  - Indépendant du client
  - Environnement contrôlé par l'entreprise
  - Maintenance aisée (car l'environnement est le même pour tous)
  - S'adapte bien au flexdesk / télétravail
- Inconvénients
  - Pas adapté aux smartphones
  - Windows XP et 7 non adaptés au tactile
  - Clavier physique plus que recommandé
  - Coûteux



# Sommaire

---

- Introduction
- Stratégies
- Solutions BYOD
- Authentification forte
- Recommandations
- Conclusion





**STERKE AUTHENTICATIE**

# Sterke authenticatie

- Twee factoren  
iets wat je bezit + iets wat je weet

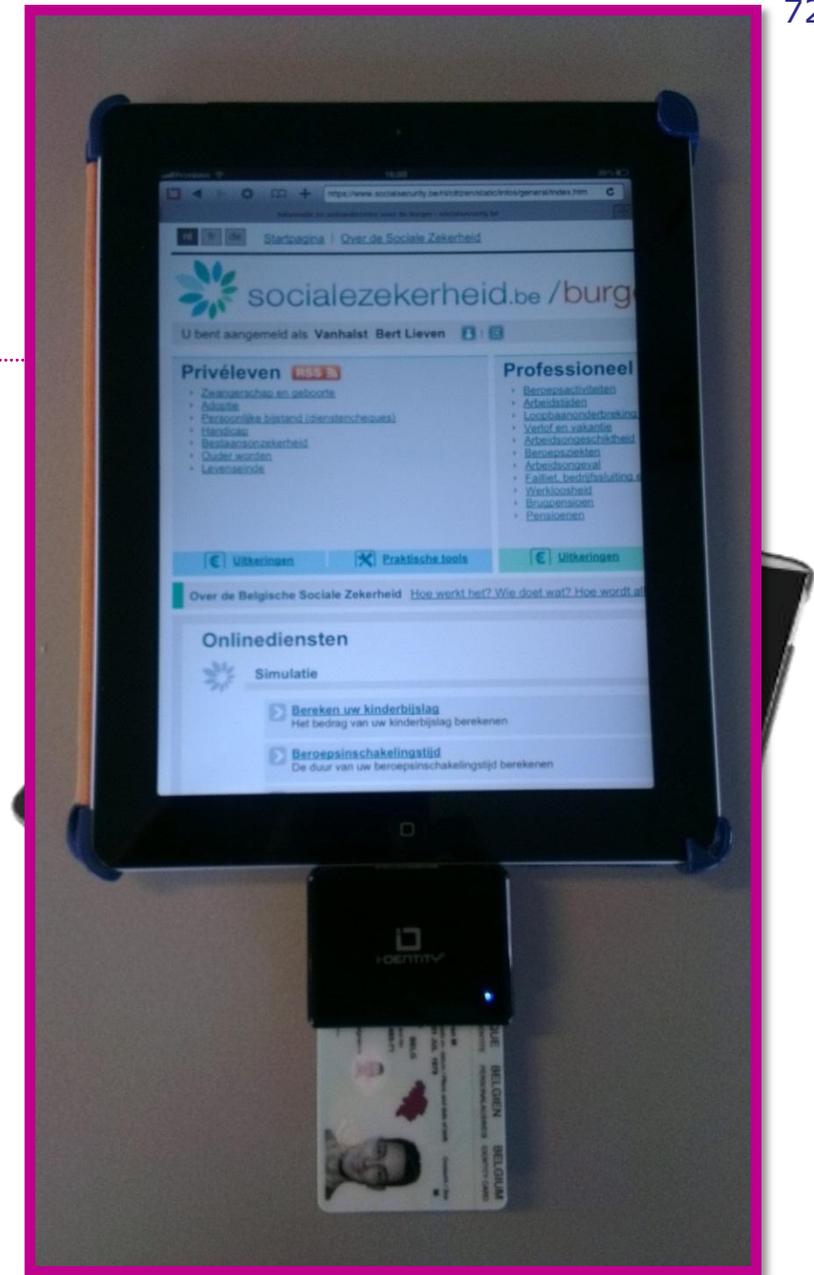


- eID niet compatibel met tablets en smartphones
- Zijn er gelijkwaardige alternatieven?



# eID kaartlezers

- Sterke authenticatie met eID
- Specifieke browser nodig
- Specifieke cover voor iPad & iPhone
  - Covers voor Android = grote uitdaging
- Library voor integratie in eigen apps
- i-Dentity



# Hardware OTP tokens

---

- OTP = One Time Password
- In combinatie met paswoord
- Veilige oplossing
- Onafhankelijk van platform
- RSA SecurID



# OTP met PIN

---

- PIN ingeven om een OTP te verkrijgen
- Iets minder gebruiksvriendelijk ten opzichte van token (ingeven PIN)



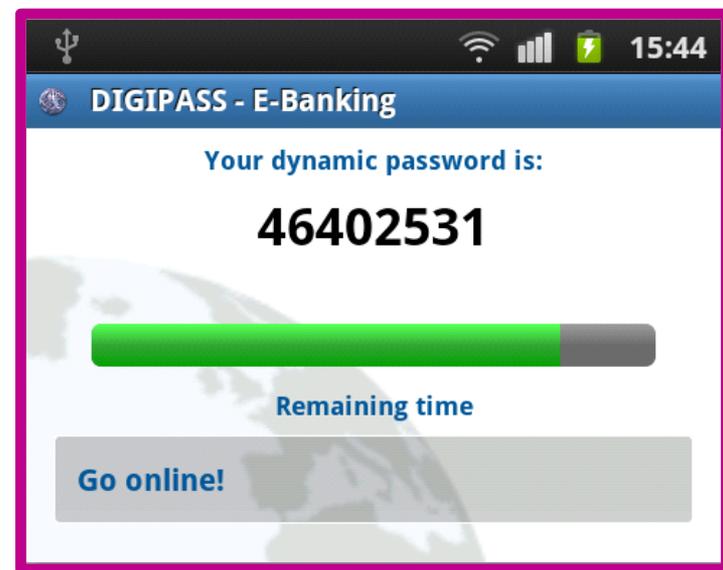
# OTP gebaseerd op eID

- Gekend proces (cf homebanking)
- Niet compatibel met Digipass van banken
- Iets minder gebruiksvriendelijk: eID en Digipass bijhebben
- Vasco Digipass 810 for eID



## Software OTP tokens

- OTP wordt gegenereerd op het toestel zelf, door een app
- Geen fysieke token bijhebben
- OTP overtypen minder gebruiksvriendelijk
- Verminderde veiligheid: token en endpoint zijn zelfde toestel, bij diefstal valt men terug op paswoord
- Digipass for Mobile



## SMS tokens

- Na authenticatie via userid/pw wordt een sms verstuurd met een OTP; OTP vervolledigt de authenticatie
- Verminderde veiligheid als token en endpoint hetzelfde toestel zijn, bij verlies/diefstal van het toestel valt men terug op paswoord



# Geprinte OTP tokens

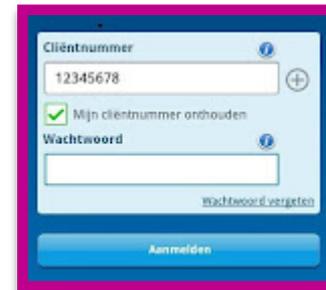
- Burgertoken, ambtenarentoken
- Lage kost
- Minder veilig: beperkte lijst van tokens, OTP niet time-based



# Koppeling met toestel

---

- Voorafgaande koppeling van toestel met identiteit (rijksregisternummer)
- Gebruiker meldt zich aan met userid en paswoord; app checkt daarnaast ook device ID (IMEI)
- Cf mobile banking
- Enkel voor native apps
- Minder veilig  
→ toegang/functionaliteit beperken

A screenshot of a mobile application login screen. It features a light blue background with white text and input fields. At the top, there is a label 'Clientnummer' with a blue information icon. Below it is a text input field containing the number '12345678' and a blue plus icon. Underneath is a checkbox with a green checkmark and the text 'Mijn clientnummer onthouden'. Below that is a label 'Wachtwoord' with a blue information icon, followed by a password input field. At the bottom right of the form, there is a small link that says 'Wachtwoord vergeeten'. At the very bottom, there is a blue button with the text 'Aanmelden'.

## En verder...

- Smartcard met toetsen en scherm
  - Vb: MasterCard Display Card
- Tendens naar contactloos (NFC)
  - Vb: MasterCard PayPass
- NFC tokens
  - Vb: Yubico YubiKey Neo
- NFC-toestel nodig



# Conclusie sterke authenticatie

---

- Usability versus security
  - Een moeilijke oefening...
  - Risico dat gebruikers oplossing niet aanvaarden
- Keuze afhankelijk van:
  - Veiligheidsniveau
  - Doelgroep: open of gesloten
  - Kost



# Aanbeveling

---

- Aantal nodige handelingen beperken
- Bij voorkeur geen authentication device
- Verlies van device asap melden zodat toegang kan geblokkeerd worden op de server



# Sommaire

---

- Introduction
- Stratégies
- Solutions BYOD
- Authentification forte
- **Recommandations**
- Conclusion



# Recommandations : Comment empêcher le BYOD

---

- Pas de bonne/mauvaise stratégie
- Interdire  $\neq$  Ne rien faire  $\approx$  tolérer
  - Définir une politique par écrit
  - Définir les actions interdites ( ex : stockage de fichiers dans le Cloud, transfert d'email, prise de notes, ...)
  - Interdire  $\neq$  Empêcher
  - Empêcher = mettre en place mécanismes type EDLP (entre-autres)
  - Empêcher le BYOD est très difficile en pratique



# Recommandations : Comment l'encadrer

---

- BYOD = initiative des employés  
→ Commencer par comprendre leurs besoins
- Comprendre les besoins = comprendre ce qui ne plaît pas dans le matériel et les logiciels fournis
- Faut-il proposer d'autres équipements/logiciels ?
- Déterminer si les demandes des utilisateurs sont réalistes
- Trouver le bon **compromis** demande/offre



# Recommandations : Commencer par une policy

---

- Définir une policy :
  - Profils utilisateurs pour qui le BYOD sera autorisé
  - Types d'appareils supportés (dépendra grandement de la solution choisie)
  - Lister les utilisations autorisées
  - Proposer des pistes pour ces utilisations
  - Favoriser le self-service et la création d'une communauté (au travers d'un outil tel que Yammer)



# Recommandations : Quels types d'outils choisir ?

---

- Pour un accès limité : le webmail est-il possible ?
  - Si pas, envisager MDM ou Isolation
- Pour un accès plus large, identifier les types d'appareils (Laptop, tablettes, smartphones)

Stratégie	Type de solution
Interdit	EDLP
Accès limité	Isolation, MDM
Accès large	Isolation, MDM, Virtualisation



# Recommandations : Récapitulatif des solutions

Type de solution	Fournisseurs
<p>Réseau intelligent</p> 	Cisco
<p>Mobile Device Management</p> 	Airwatch, MobileIron, Zenprise
<p>Isolation</p> 	Enterproid, Thales
<p>Virtualisation</p> 	Citrix, VMware



# Recommandations : Tester la policy

---

- Trouver un bon **compromis** sécurité/usability pour éviter un rejet
- Tester la mise en œuvre de la policy au moyen d'un POC
- Le POC doit durer plusieurs mois
- Tenir compte de l'avis des utilisateurs
- Regarder comment ils vont contourner les restrictions mises en place



# Sommaire

---

- Introduction
- Stratégies
- Solutions BYOD
- Authentification forte
- Recommandations
- Conclusion



# Conclusion

---

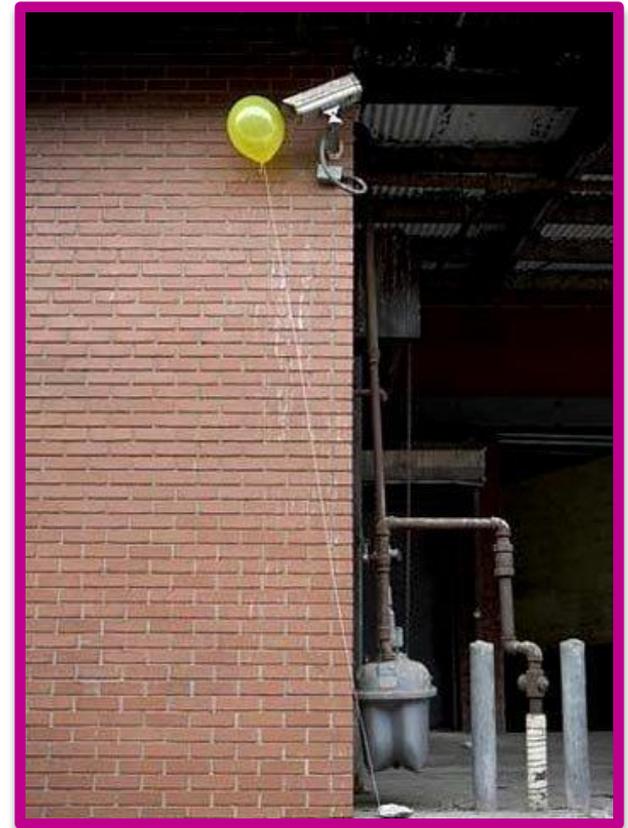
- BYOD = tendance inévitable  
→ Nécessité de définir une stratégie
- Pas nouveau (+ rôle du Cloud)
- Applications plus problématiques que les appareils (point de vue de la sécurité)
- Impossible de satisfaire toutes les demandes → trouver un **compromis** acceptable
- L'accès aux applications sécurisées ne doit pas être trop lourd



# Conclusion

---

- Plan d'approche :
  - Définir une stratégie et une policy puis choisir un outil
  - Une politique trop contraignante sera contournée
  - Tester la stratégie et la politique au moyen d'un POC



# Conclusion

---

- Pas encore de solution qui convienne pour tous les appareils
- Appareils privés/professionnels gérés différemment
- Si BYOD autorisé, réaliser un POC et...
- ... éduquer les utilisateurs
- Ne dispense pas de prévoir du matériel pour l'employé
- Faire preuve d'originalité ?



# Conclusion

---

- BYOD peut être envisagé sans détériorer la sécurité :
  - Le vrai danger : l'utilisateur et une utilisation irréfléchie des outils dans le Cloud
  - Une politique trop stricte incitera les utilisateurs à commettre des imprudences
- Moyennant une bonne approche, tout le monde peut y gagner :
  - Employé satisfait
  - Sécurité non détériorée



# Questions ???

---



gregory.ogonowski@smals.be



bert.vanhalst@smals.be

