

Gevoelige Overheidsdata en de Cloud



Kristof Verslype

Smals Research

www.smalsresearch.be

3 april 2014

De Cloud - Intro



Cloud Services Brokerage



Buitenlandse Overheden



Case: File Sync & Share



Afronding

A full-page background image featuring a vibrant sunset or sunrise. The sun is a bright, glowing orb in the upper center, casting a brilliant orange and yellow light across the sky. Below the sun, a thick, undulating layer of white and grey clouds stretches across the horizon, resembling a sea of clouds. To the left, the dark, silhouetted ridge of a mountain slopes down towards the bottom left corner. The overall atmosphere is serene and majestic.

De Cloud - Intro

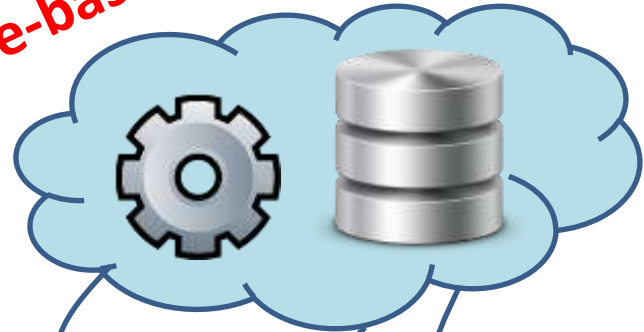
Product-based



One heavy client

Shift

Service-based



Many mobile thin clients

Enkele voorbeelden

Een virtuele server aanmaken
om een product te testen



Een office-pakket toegankelijk
vanaf elke computer met
internet



Het ontwikkelen van
een web-toepassing



Delen van gegevens
tussen mijn PC, tablet
en smartphone en
delen met collega's

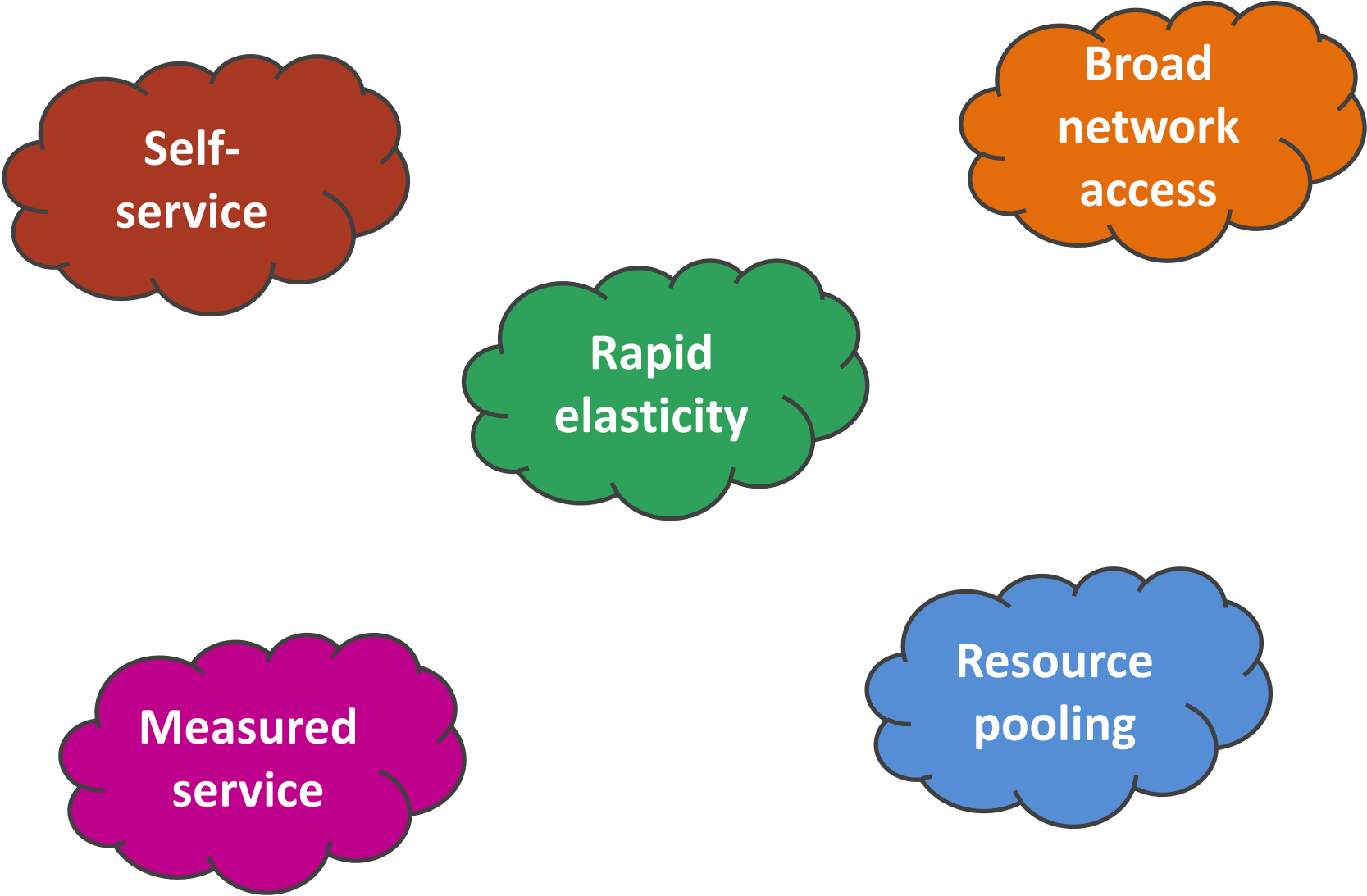


Dropbox

Een e-Mailomgeving waar het
personeel overal toegang tot heeft



Eigenschaften



**Self-
service**

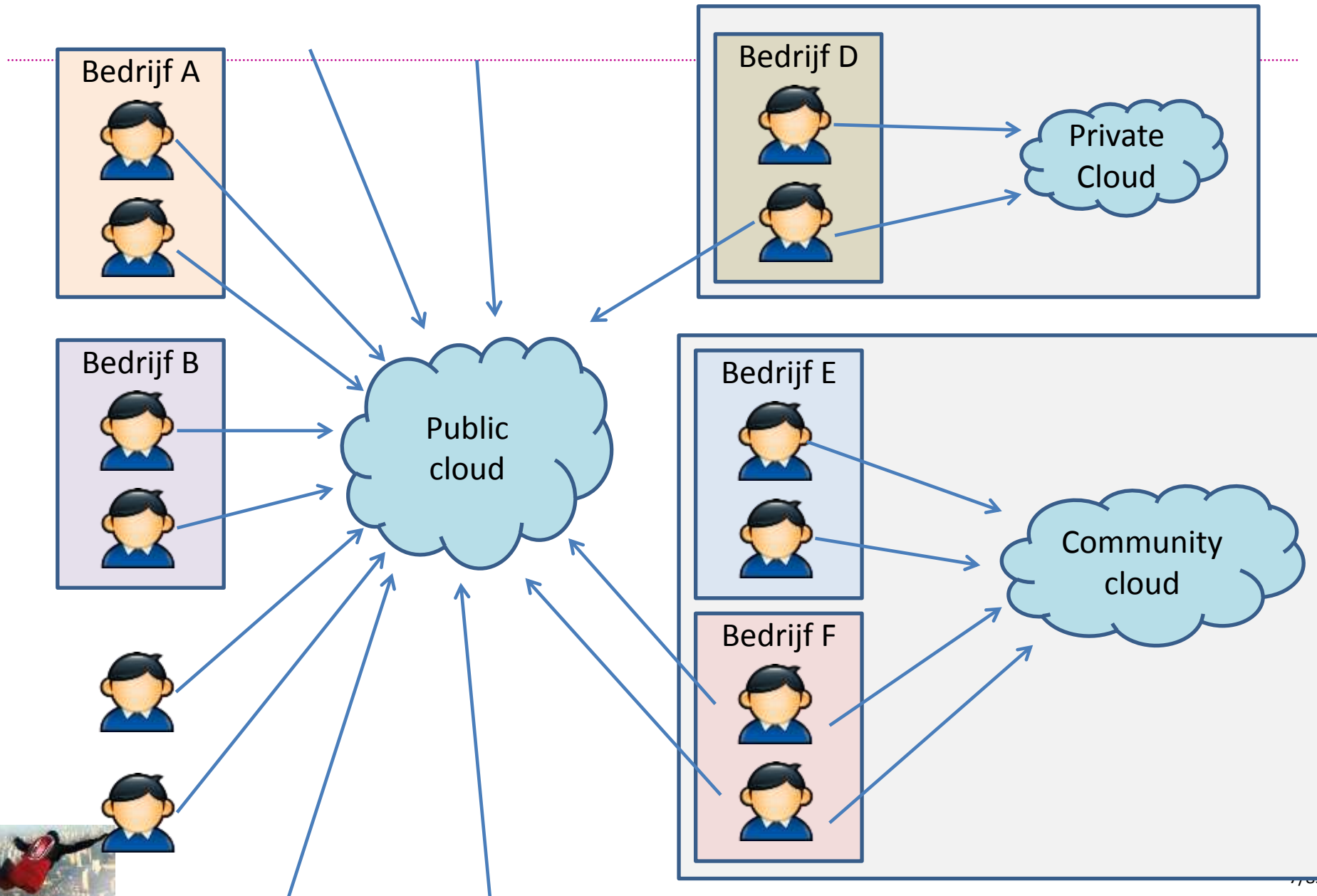
**Broad
network
access**

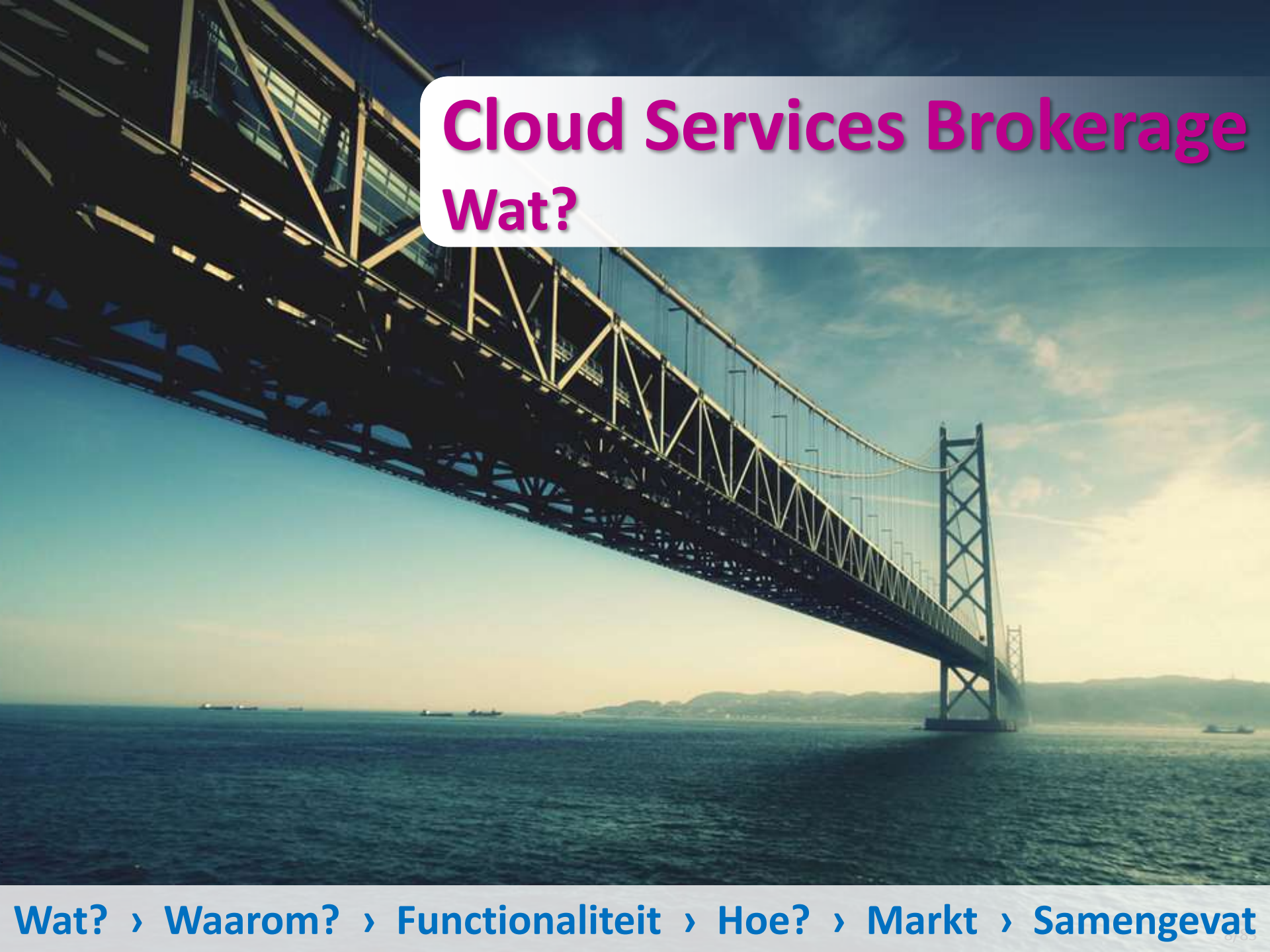
**Rapid
elasticity**

**Measured
service**

**Resource
pooling**

Public VS Private VS Community





Cloud Services Brokerage Wat?

Wat? › Waarom? › Functionaliteit › Hoe? › Markt › Samengevat

Wat?

Een Cloud Service Broker levert meerwaarde als schakel tussen aanbieders en eindgebruikers van cloud diensten.

In public, community of private cloud

Intern of extern



Werking en beschikbaarheid cloud diensten vallen buiten controle cloud service broker

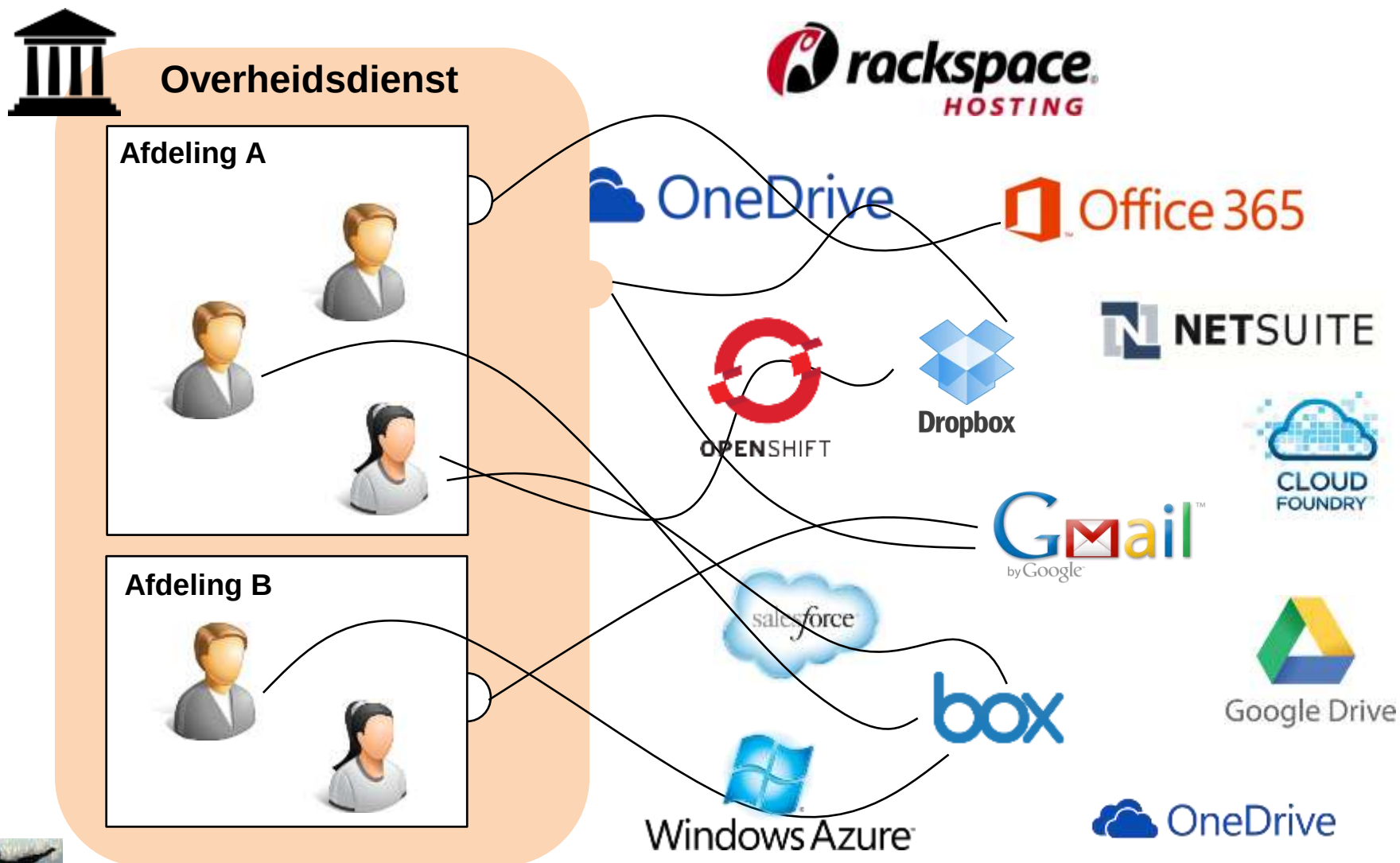


Cloud Services Brokerage Waarom?



Wat? › Waarom? › Functionaliteit › Hoe? › Markt › Samengevat

Spaghetti-architectuur



Spaghetti-architectuur

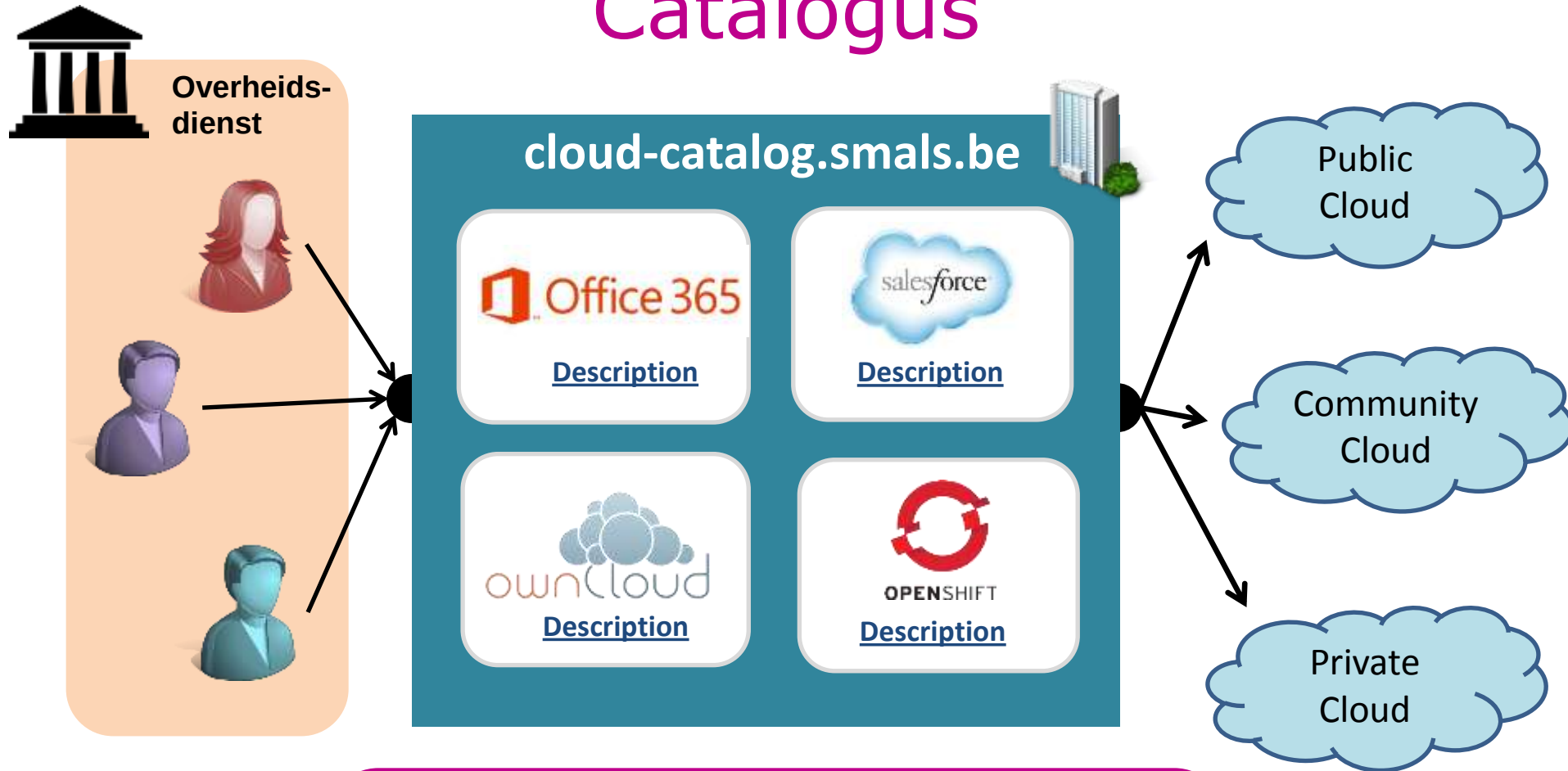


Cloud Services Brokerage Functionaliteit



Wat? › Waarom? › Functionaliteit › Hoe? › Markt › Samengevat

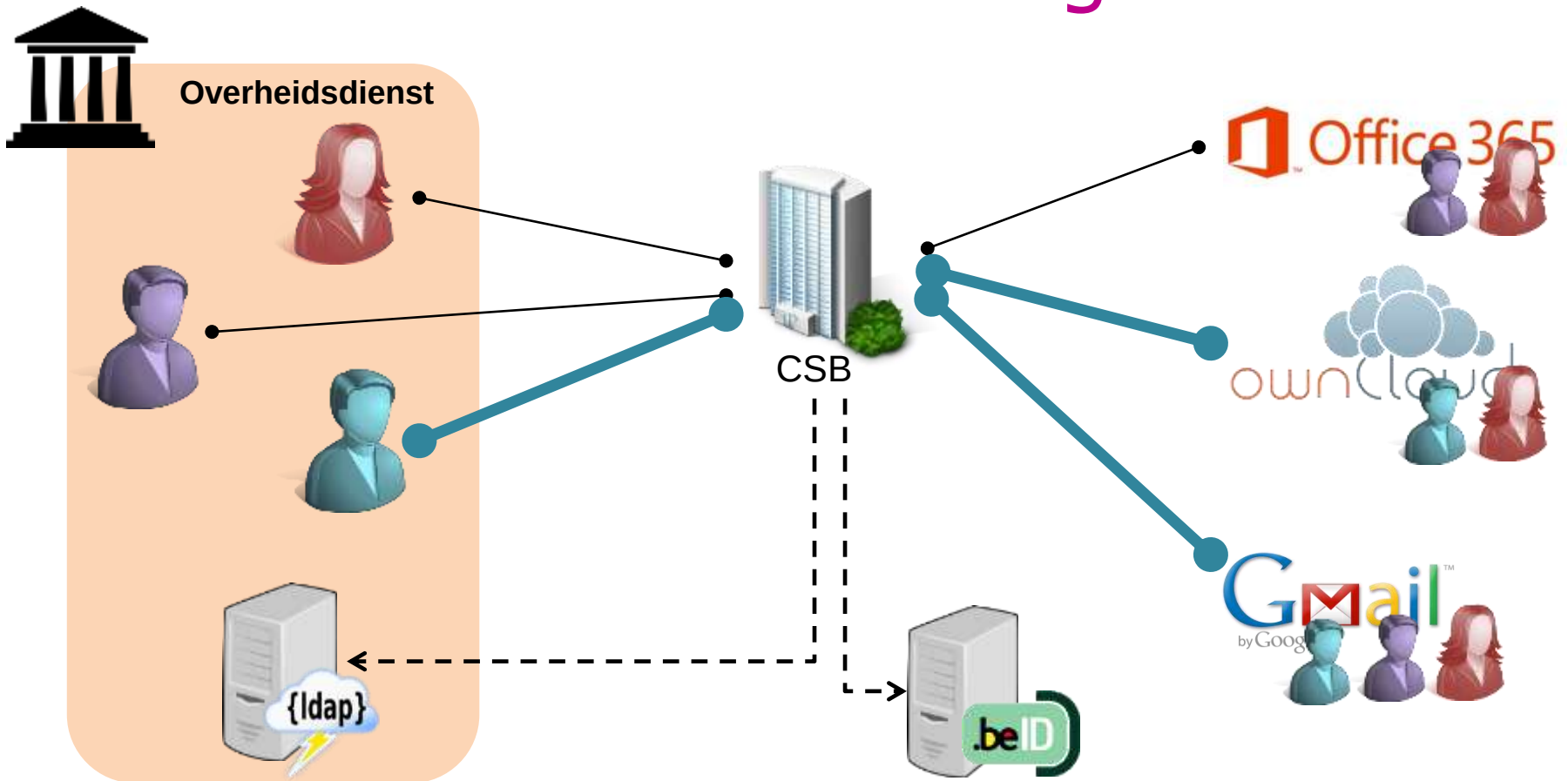
Catalogus



- Aanbod gevalideerde cloud-diensten
- Gebruiksvriendelijk
 - Ondersteuning
 - Gepersonaliseerde catalogi
 - Abstractie achterliggende clouds

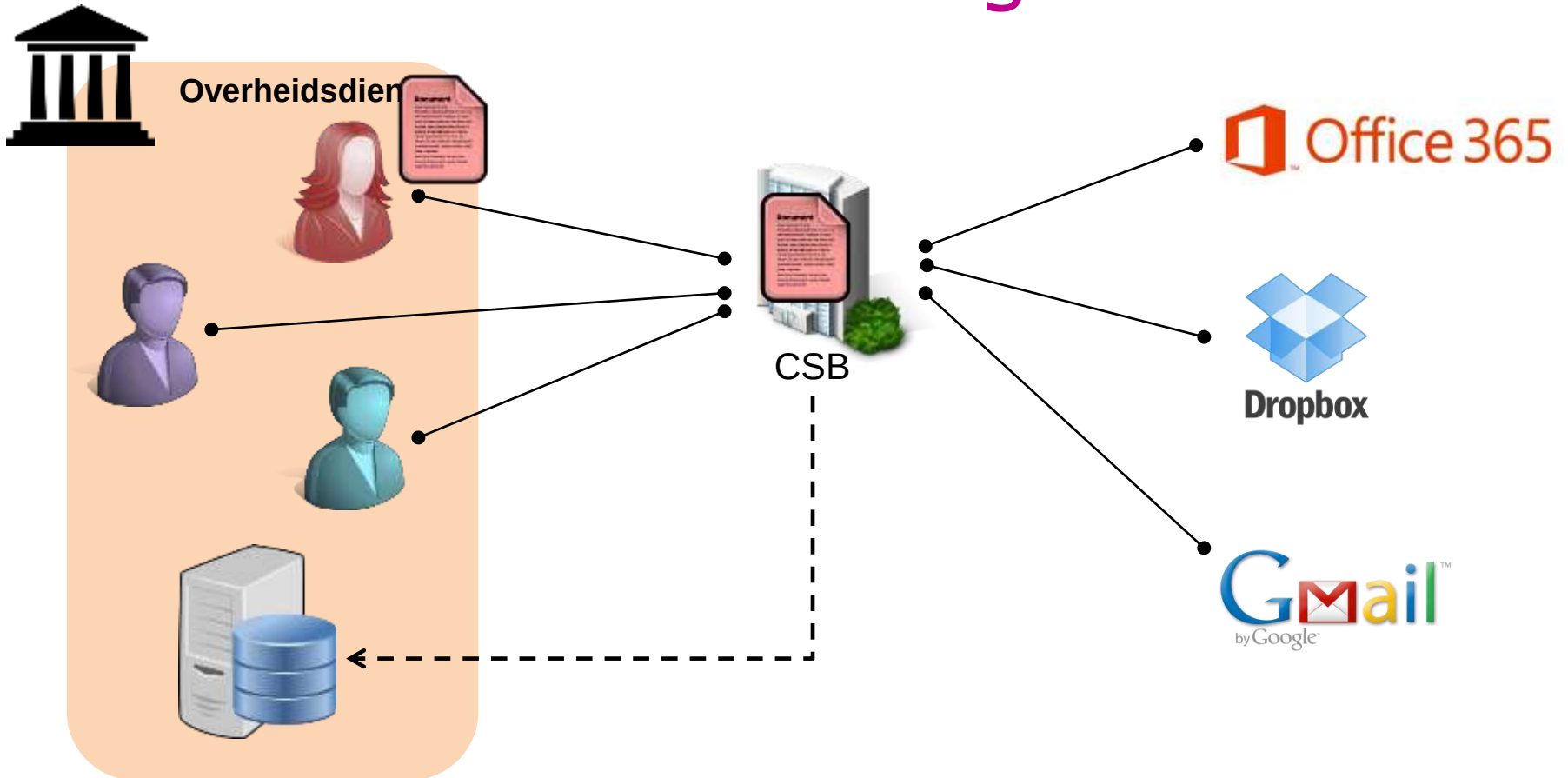
=> Vermijdt wildgroei, stimuleert compliance

User & Access Management



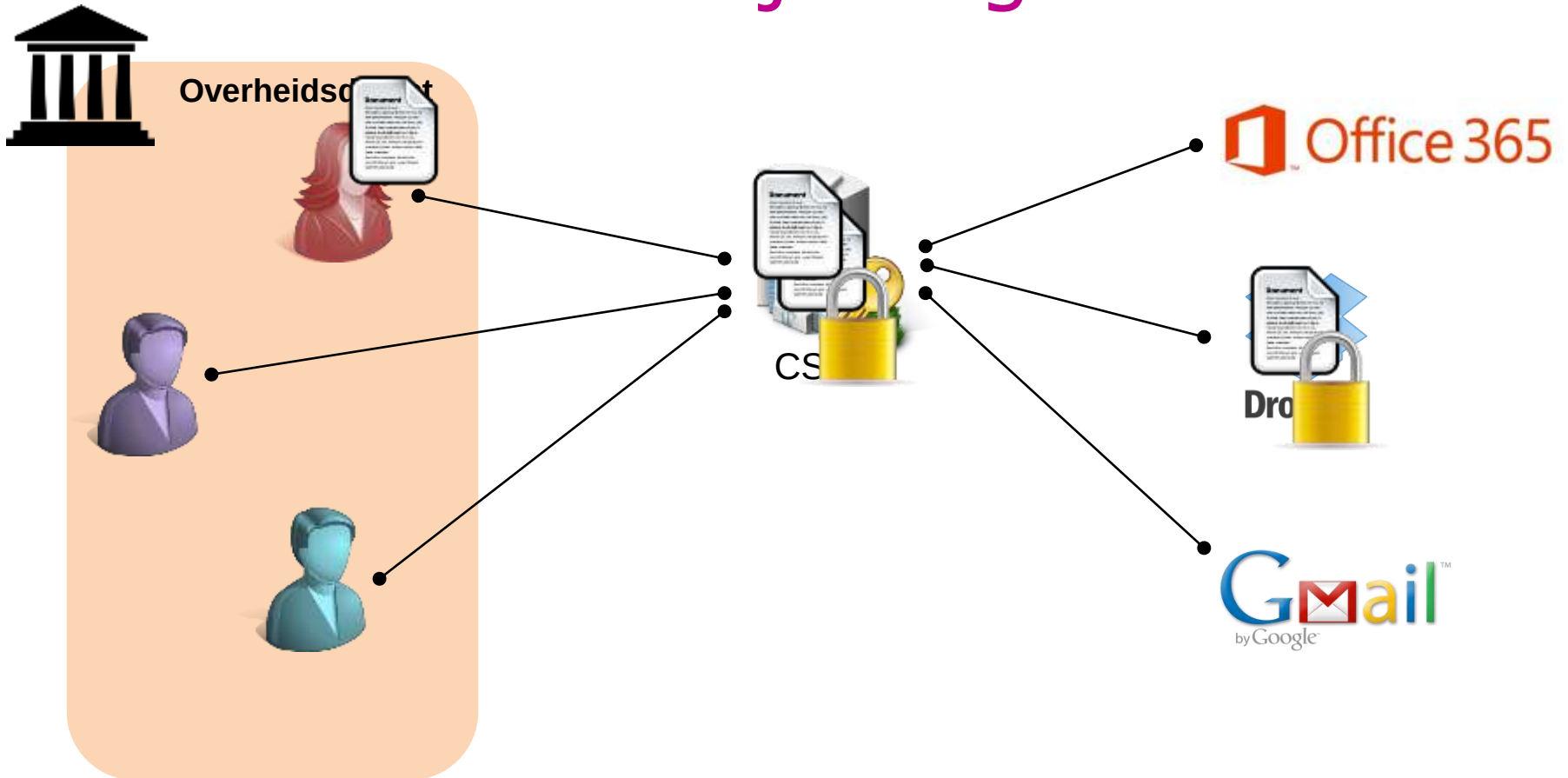
- (De)provisioning
 - Single sign-on
 - Integration LDAP, eID, SAML,
 - Policy enforcement
- => **Verbetering UAM**

Archivering



- Eigen beleid rond archivering
 - Vb. Clouddienst levert geen langetermijngaranties
 - Vb. Wat bij faillissement dienst?
- => Beschikbaarheid data langetermijn**

Vercijfering

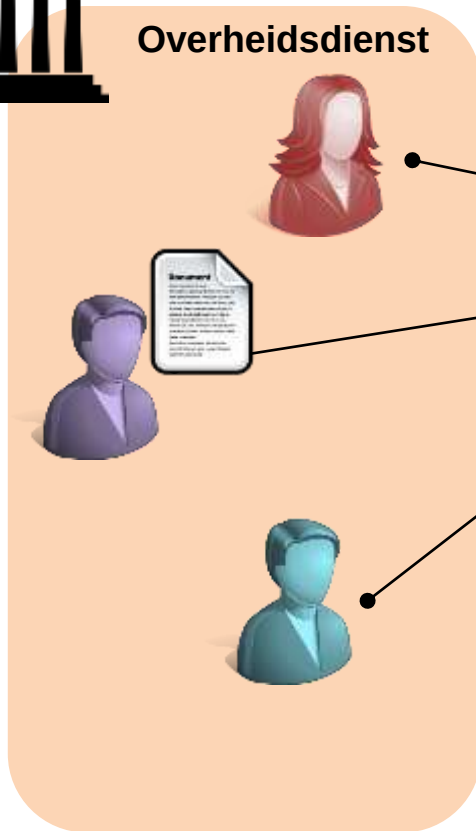


- Gevoelige gegevens worden gecijferd vooraleer naar publieke cloud
 - Bestandsopslag & uitwisseling, e-Mail,
- => Verhogen confidentialiteit**

Monitoring / Reporting



Overheidsdienst



Office 365

Dropbox

Gmail
by Google

- Cloud-gebruikers
- Data in transit (DLP)
- Cloud-diensten (SLA's)
- ⇒ **Verhogen inzicht/overzicht gebruik data**
- ⇒ **Eventueel ingrijpen indien nodig**
- ⇒ **Nuttig bij veiligheidsincident**

Technisch / Intelligence

Kennis v/d markt

Configuratie cloud-diensten

Integratie

- Cloud – Cloud
- Cloud – Legacy

Helpdesk

Vermijden vendor lock-in

- Vb. Door aanbieden uniforme API

Financieël / Contractueel

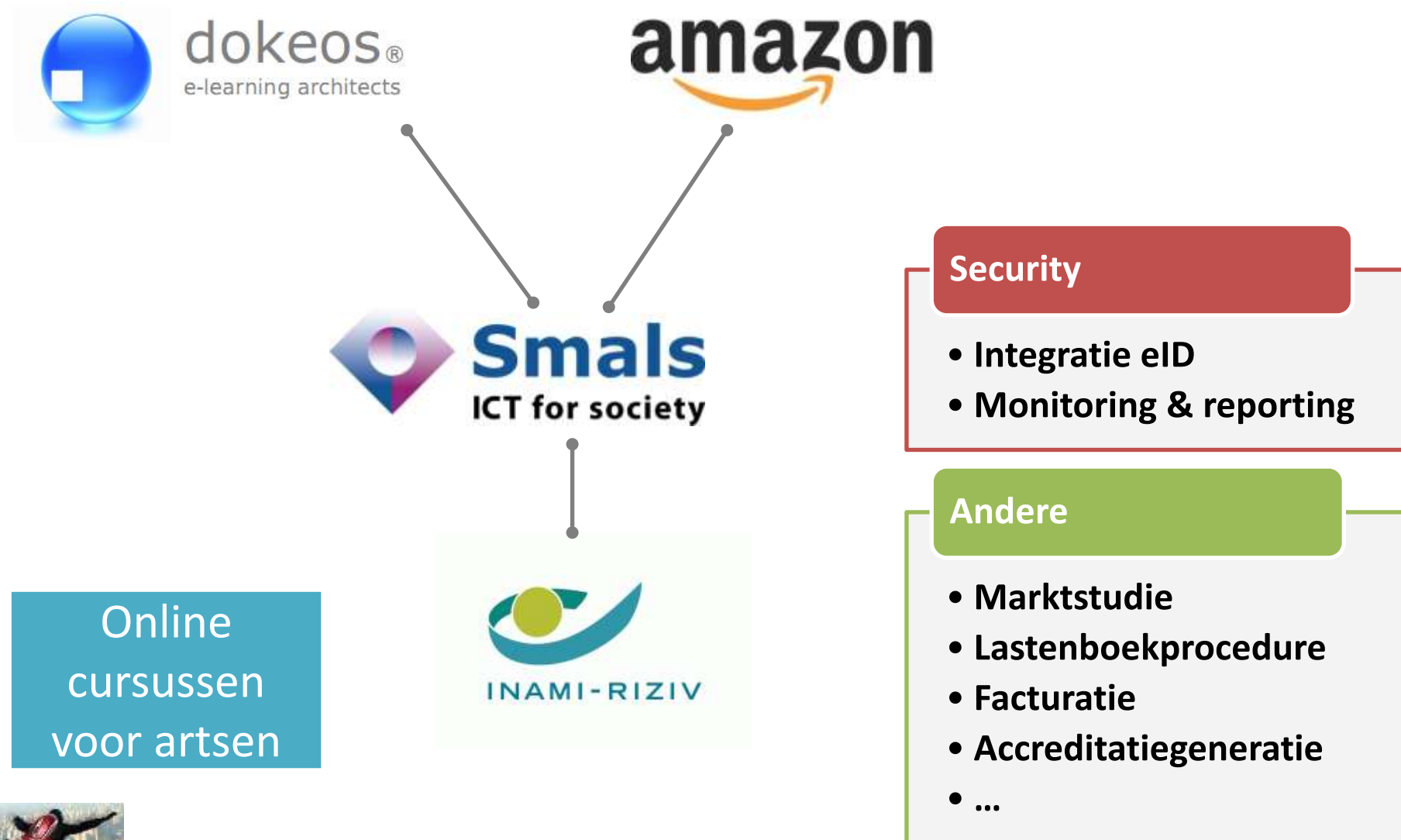
Financieël

- Eén factuur voor alle cloud-diensten
- Chargeback
- Gebruik kredietkaart
- Indekken tegen wisselkoersen

Contractueel

- Raamcontracten (volumekorting)
- SLA's gerespecteerd?
- Juridische vertegenwoordiging

Smals als embryonale CSB



Cloud Services Brokerage Hoe?

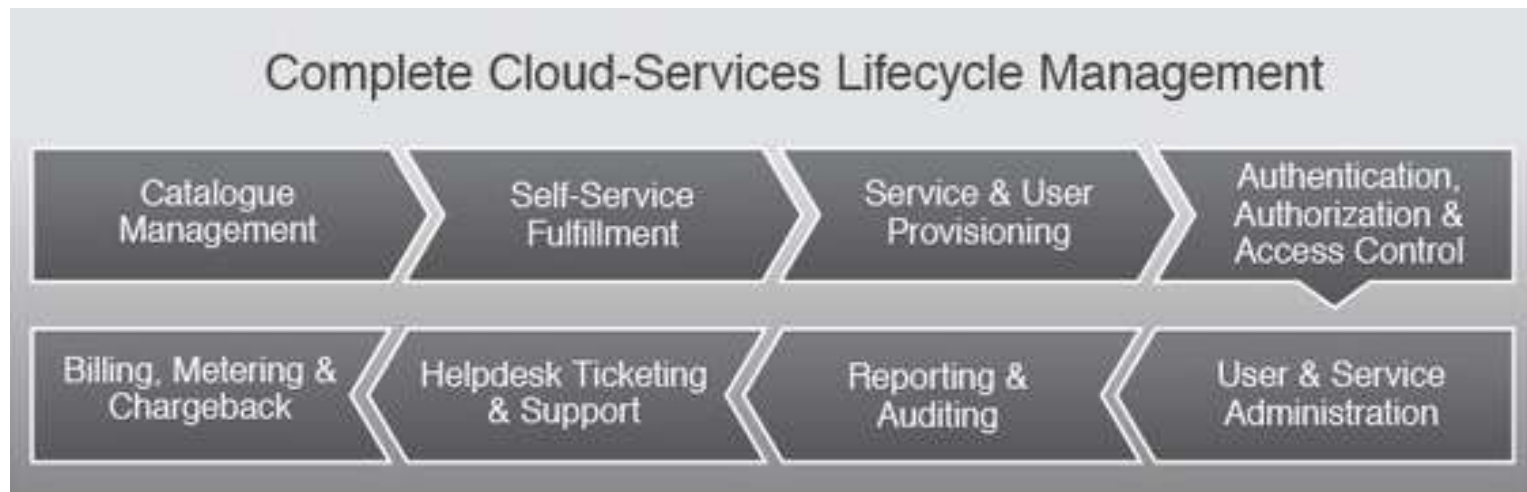


Wat? › Waarom? › Functionaliteit › Hoe? › Markt › Samengevat

CSB Enablers

Een CSB enabler levert technologie en ondersteuning om een CSB op te zetten

Een bekende speler:



<http://www.jamcracker.com/>



Two cases



=> 2 x telco

Cloud Services Brokerage Markt



Wat? › Waarom? › Functionaliteit › Hoe? › Markt › Samengevat

Een markt in expansie

“Omzet 100 miljard voor CSB + CSB Enablers jaarlijks tegen eind 2014”

Gartner
 December 2012

	2013 (in miljard \$)	2018 (in miljard \$)	Jaarlijkse groei
Cloud brokers	1,57	10,5	46,2%
Cloud broker enablers	0,225	2,03	55,3%

Bron: Market & Markets, Maart 2013

“Tegen 2015 zal minstens 20% van alle cloud-diensten via CSBs afgenomen worden.”

Gartner
 Oktober 2013



CSB Enablers - Cool Vendors



Cloud Services Brokerage Samengevat



Wat? › Waarom? › Functionaliteit › Hoe? › Markt › Samengevat

Samengevat...

Personeel neemt initiatief, zonder nodige overleg

CSB positieve impact op security

Onvolwassen markt met sterke groei

Term CSB niet altijd even scherp afgebakend

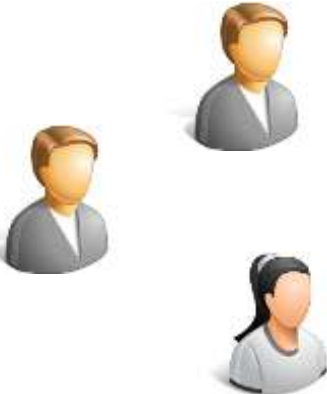
Traditionele service providers (vb. telco's) nemen de rol van CSB op

Spaghetti-architectuur

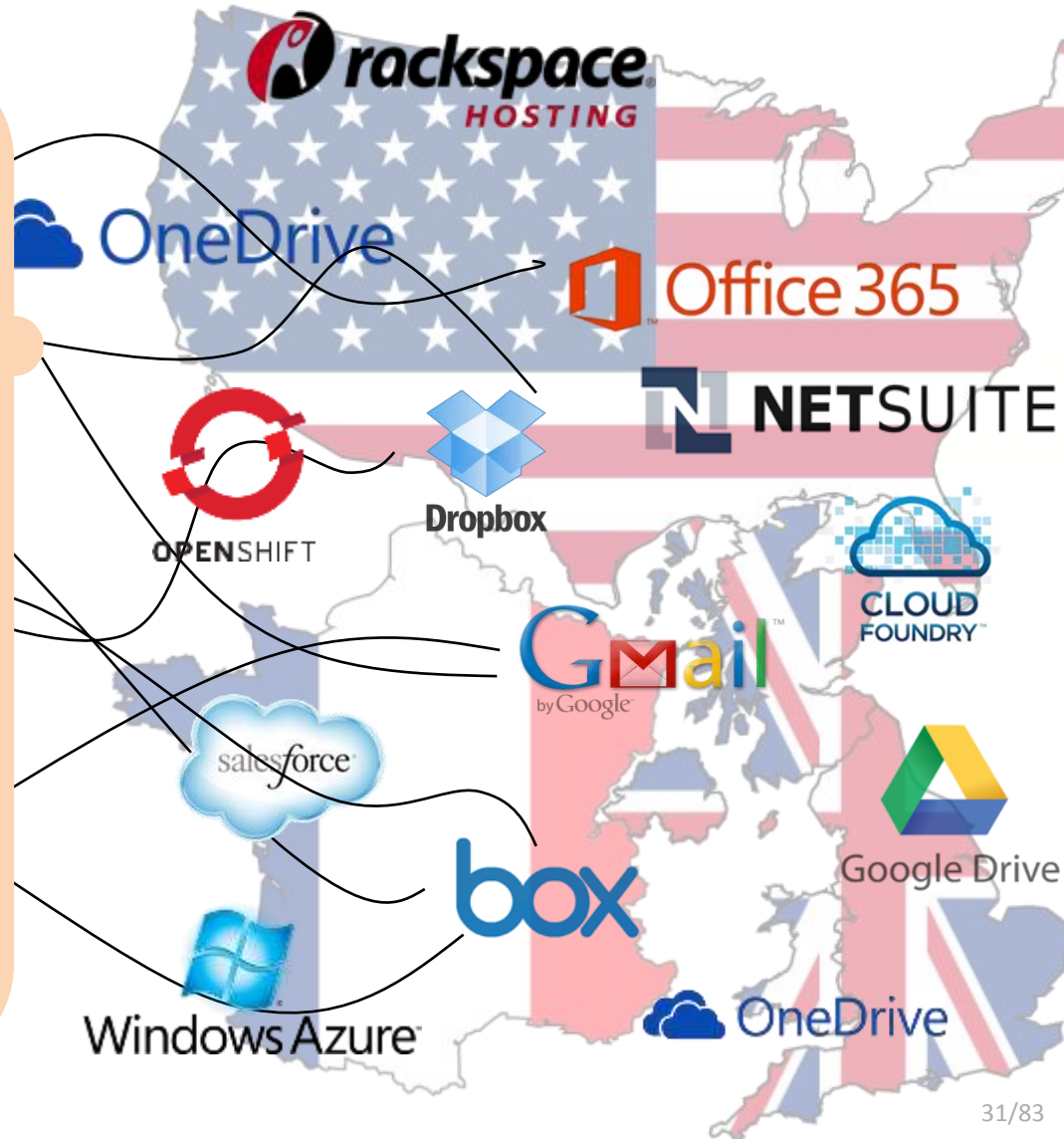


Overheidsdienst

Afdeling A

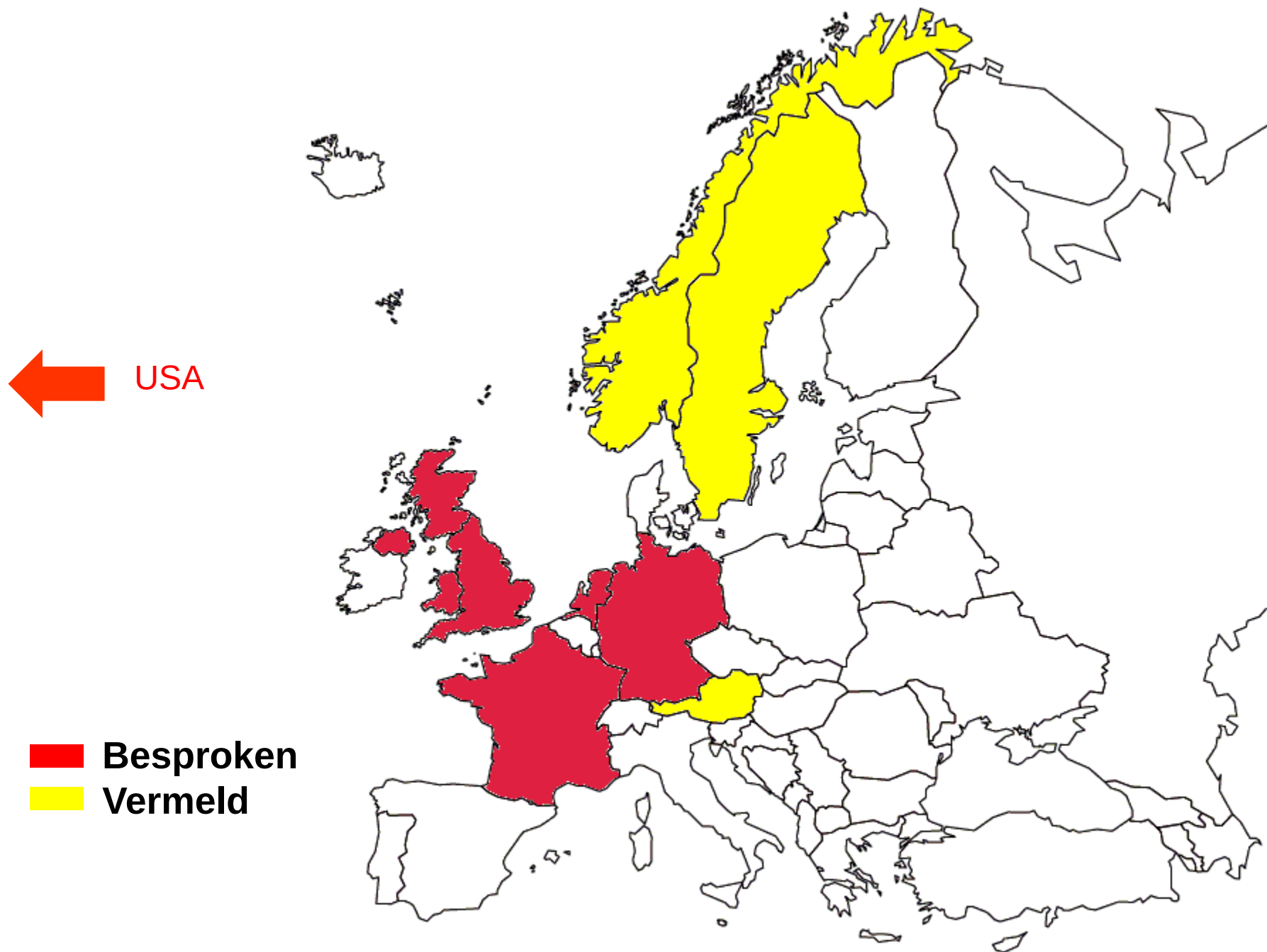


Afdeling B



Overheden Buitenland





A large, ornate glass chess set is displayed on a checkered board. The pieces are made of clear, reflective glass and include a king, queen, rook, knight, bishop, and various pawns. The background is a vibrant sunset or sunrise sky with orange, yellow, and blue hues. The chessboard is white and blue checkered.

Overheden Buitenland Nederland

April 2011

*"Het kabinet kiest er daarom voor om een gesloten Rijkscloud in eigen beheer in te richten als een voorziening die **generieke diensten** levert binnen de Rijksdienst. Deze voorziening wordt ingericht **binnen een eigen beveiligd netwerk en wordt beheerd door een eigen, rijksbrede organisatie.**"*

Brief aan de Kamer op 20 april 2011

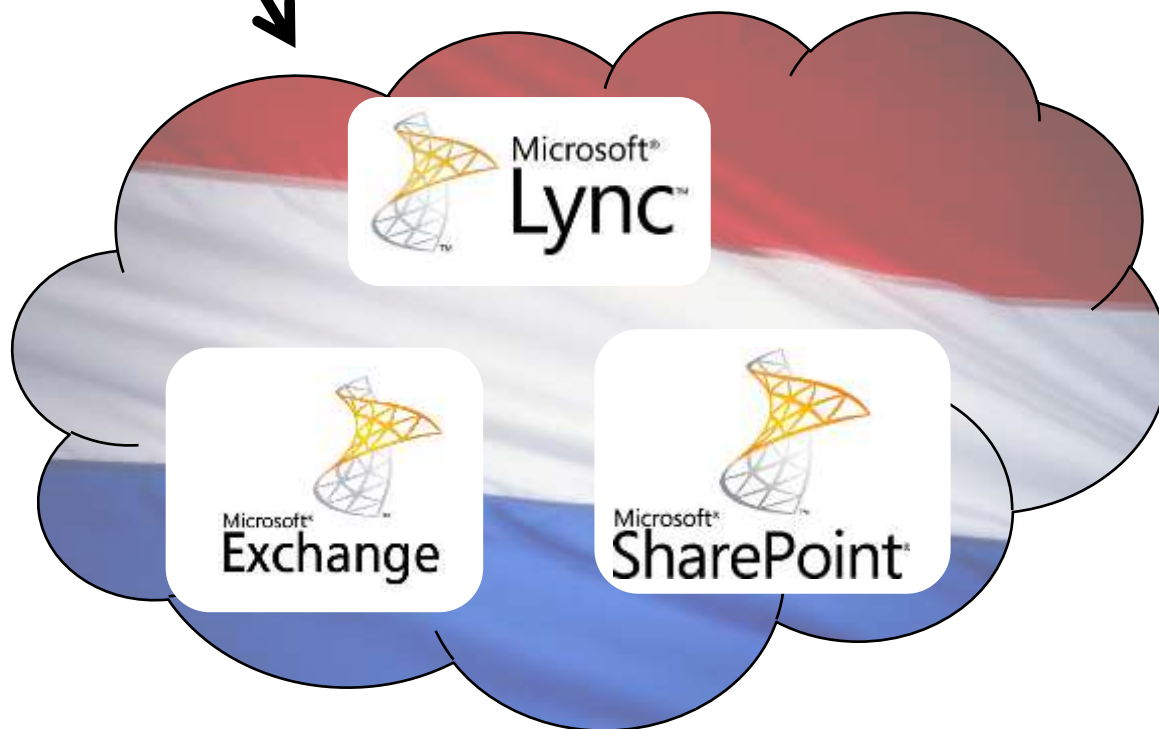
...



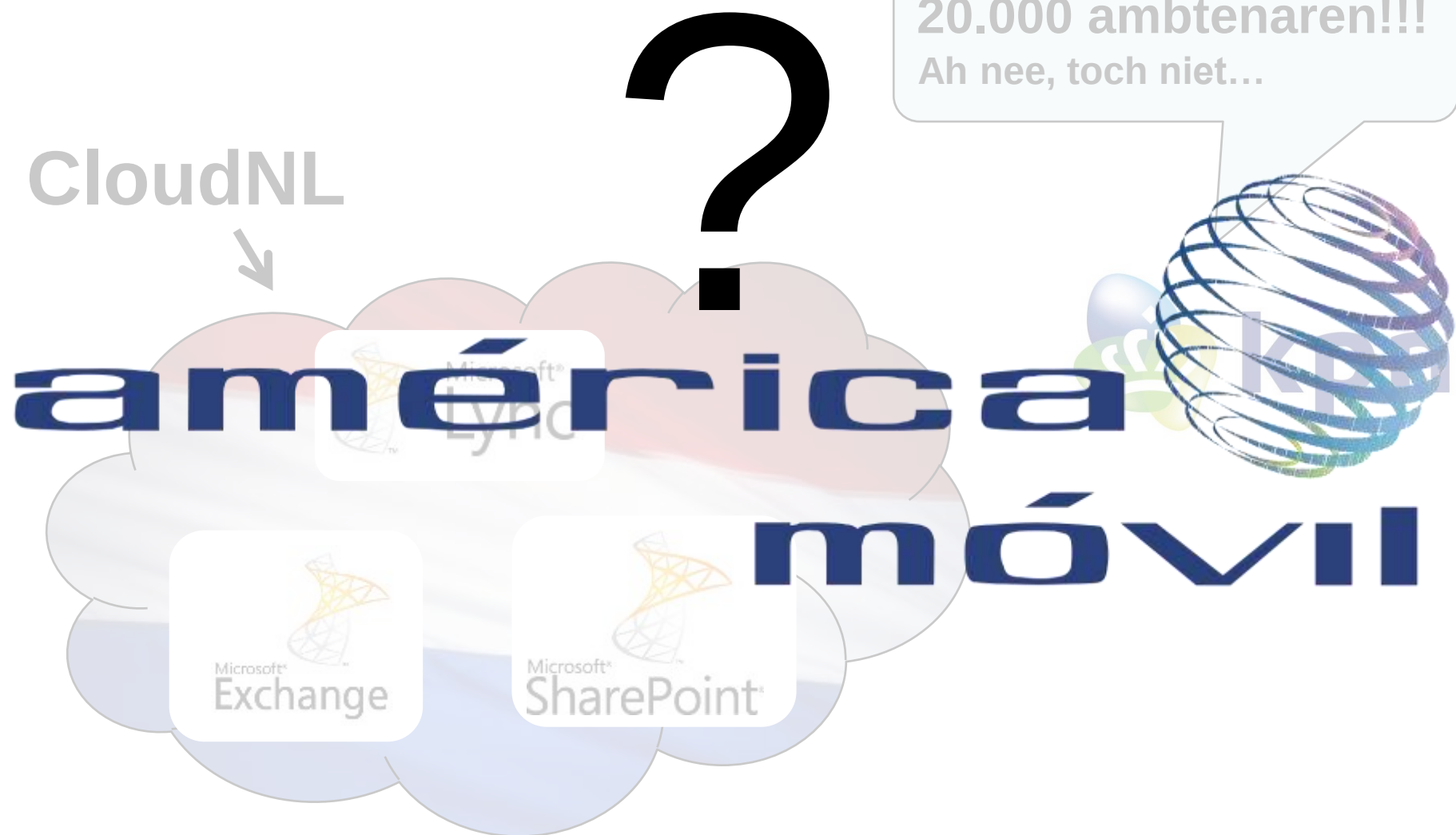
September 2012

20.000 ambtenaren!!!
Ah nee, toch niet...

CloudNL



September 2012



Juni 2013

**Datacenter in eigen
beheer, zoals AIVD,
is verstandiger!**



€



- Rijkswaterstaat
- Dienst Justitiële Inrichtingen,
- Inspectie SZW Opsporing,
- Dienst Terugkeer en Vertrek,
- Rijksinstituut voor Volksgezondheid en Milieu,
- Koninklijk NL Meteorologisch Instituut
- Planbureau voor de Leefomgeving,
- College ter Beoordeling van Geneesmiddelen,
- Centraal planbureau
- Sociaal en Cultureel Planbureau.



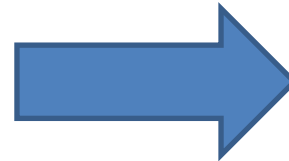
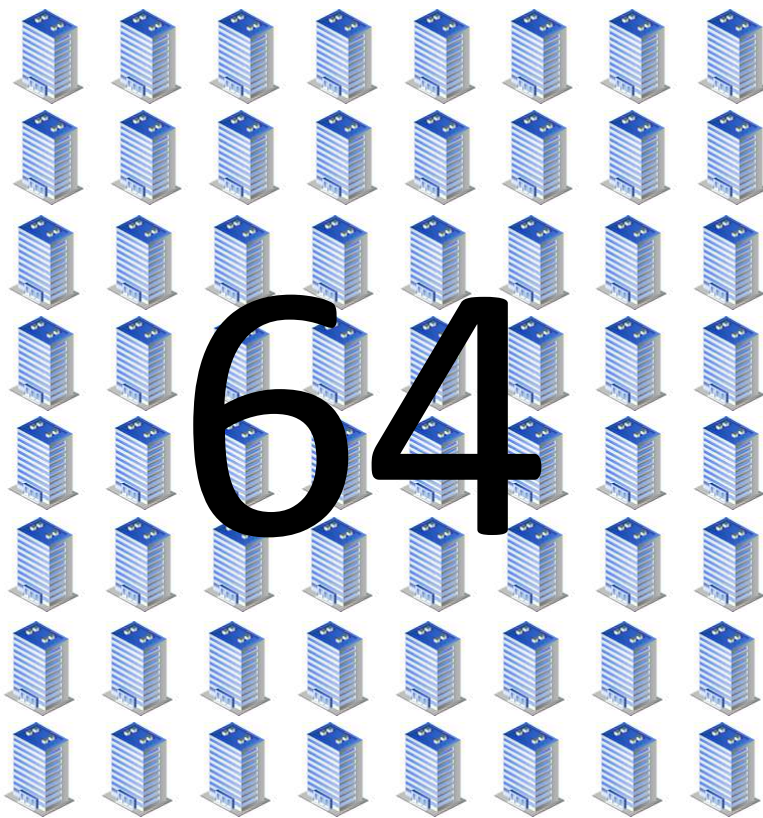
Alle informatie over grote projecten, maar bijvoorbeeld ook de camera's en de bediening van de matrixborden boven de snelweg gebeurt via dit datacentrum. Je moet qua hoeveelheid niet meer aan gigabyte denken, we hebben het hier eerder over 70 terabyte.



Maarten Hillenaar

hoofd van de afdeling ICT bij de overheid

Consolidatie Data Centers



Eigen beheer

+



Extern





Nederland: Conclusies

Ambitieuze plannen teruggeschroefd

Datacenters in eigen land

Consolidatie

Kritiek wegens niet alles in eigen beheer

Cloud in kinderschoenen

Cloud 1st strategie

Wat bij overname nationale spelers?

Overheden Buitenland Frankrijk



Frankrijk, 2012

Vorming 2 consortia



Door



<https://www.numergy.com/>



Door



<https://www.cloudwatt.com/>



Frankrijk

Data centers in Frankrijk

- Numergy: Tier 3+
- CloudWatt: Tier 4

PPS (per consortium)

- Franse bedrijven: $2/3 = € 150.000.000$
- Staat: $1/3 = € 75.000.000$

Doelgroep

- Overheidsinstellingen
- Bedrijven

Aanbod (wordt uitgebreid)

- Cloudwatt: Cloudwatt-box - File Sync & Share
- Numergy: gevirtualiseerde omgevingen
- Zie volgende slides...



1 utilisateur
50 GO de stockage

29 €

ht / an
au lieu de 42 € HT*



COMMANDER

10 utilisateurs
100 GO de stockage

299 €

ht / an
au lieu de 520 € HT*



COMMANDER

Configurez votre stockage



1,2m²

de surface d'archivage ⓘ



250

vidéos ⓘ

sélection du niveau de stockage

Octets

50 Go

100 Go

200 Go

500 Go

Prix HT/an

0 €

100 €

200 €

500 €



Sélectionner le stockage souhaité :

1 000 Go - 1000 € HT par an

Sélectionner le nombre d'utilisateurs souhaité :

100 Utilisateurs - 4200 € HT par an

Total HT : 5200.00 €

Tva (19.6%) 1019.20 €

Total TTC 6219.20 €

ANNULER

COMMANDER



[Offre Cloud Numergy](#)[Tarifs et achat](#)[Partenaires](#)[Découvrez Numergy](#)[Contactez un expert](#)[Essayez gratuitement](#)**OFFRE DÉCOUV**

Offre découverte : 2 mois gratuits pour tester votre Cloud sur-mesure

Profitez dès maintenant de tous les avantages offerts par Numergy Self-Services.

[Essayez gratuitement](#)[Essayez gratuitement](#)[Machine virtuelle](#)[Rejoignez-nous !](#)

Le Cloud computing Numergy

L'offre Cloud (IaaS) de Numergy définit de nouveaux standards en termes de performance, sécurité et qualité de service. Découvrez Numergy.

Numergy, producteur d'énergie numérique



Calculez le coût de votre cloud

De combien de VM avez-vous besoin ?



1

5

10

15

20

> 25

[Configurez votre offre](#)

Le Cloud Numergy

Comment ça marche ? →





Frankrijk: Conclusies

2 x PPS met Franse bedrijven

Datacenters in Frankrijk

Staat investeert vrij veel geld (150m €)

Aanbod gevirtualiseerde server-omgevingen & FSS

Soevereine cloud staat vrij ver

Partnerships binnen EU (vb. Numergy met Belgacom)

A large, detailed chess set is arranged on a checkered board. The pieces are made of a dark, reflective material, possibly polished wood or metal, and are highly detailed. The background is a vibrant sunset or sunrise sky with warm orange and yellow hues. The chess pieces are arranged in a way that suggests a game in progress, with some pieces moved from their starting positions. The lighting is dramatic, highlighting the textures and shapes of the pieces.

Overheden Buitenland Duitsland

Duitsland, 2011

2 initiatieven



**Veilige, Duitse
Bundesccloud nodig voor
regeringsinstellingen**

12/2011



Hans-Peter Friedrich, toenmalig
minister Binnenlandse Zaken (CSU)



Officieel voorgesteld op Cebit 2011

“Cloud made in Germany”

- Datacenters in Duitsland
- Uitbating & beheer: Duitse bedrijven

Transparantie

- Open standaarden, formaten, interface
- Volledige stack open source

Ontdubbeling over datacenters

- Bestaande infrastructuur



<http://www.deutsche-wolke.de/>

OSB Open Source
Business
ALLIANCE



Aanbod (via resellers)



« wordt uitgebreid »



Gestart in 2011

- *“Ontwikkelen en testen van innovatieve, veilige en rechtsconforme cloudcomputing-oplossingen”*

100 miljoen €

- 50% gov, 50% privé
- Overwegend Duitse bedrijven

Doelgroep

- KMO's
- Gezondheidszorg
- Publieke sector





Activiteit

Aanbod (in ontwikkeling)

- KMO's (9)
- Gezondheidszorg (3)



TRESOR

- Publieke sector (2)



Pilootproject voor certificering clouddiensten

Juridisch luik





Duitsland: Conclusies

Uitbouw nationale cloud

Aanbod in ontwikkeling

Investering overheid (50m €)

Focus op SaaS. Mindere mate IaaS

Overheden Buitenland UK



G-Cloud

Catalogus geaccrediteerde clouddiensten

Volledige publieke sector

Kansen nationale spelers

Aanbod

- 800 aanbieders
- 7,000 diensten

Business via G-Cloud

- £92,7m tot 28/01/14 (sinds begin 2012)
- 70% KMO's
- Meeste contracten consultancy

<http://gcloud.civilservice.gov.uk/>





Specialist Cloud Services



Accredited services



Buyer's guide



Who's bought what?



Accessibility

SaaS



Alerts

SaaS



Antispam

SaaS



Asset Management

SaaS



CMS

SaaS



Compute

IaaS



Agile

SaaS



Analytics

SaaS



Application Deployment

PaaS



CDN

IaaS



Components

PaaS

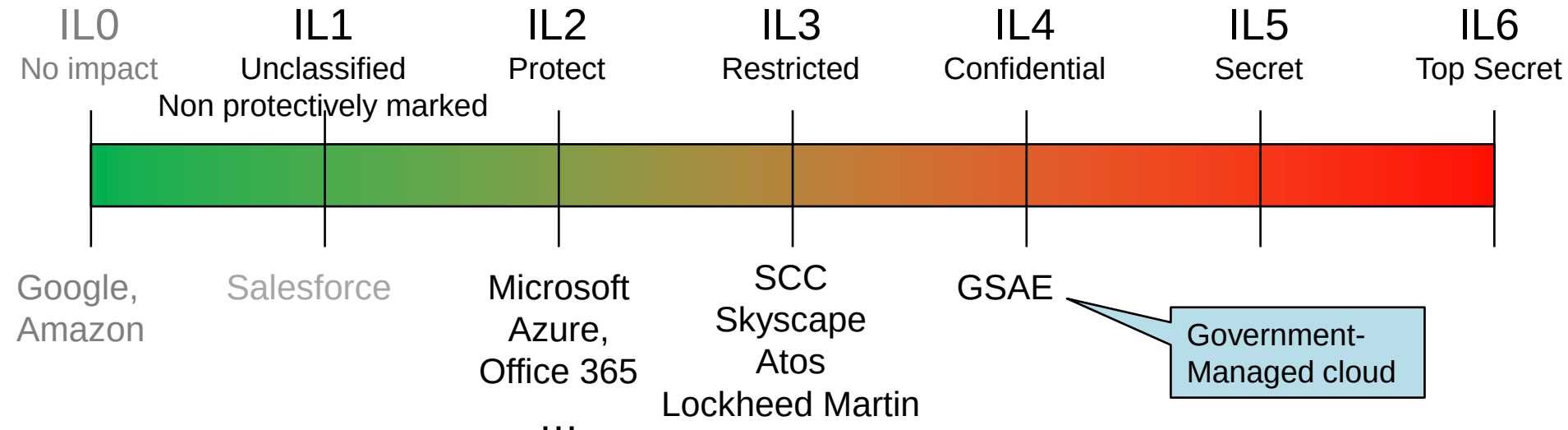


CRM

SaaS

G-Cloud

Accreditations



Amerikaanse bedrijven reageren

- Oracle wil IL3 en bouwt datacenter in UK
- Salesforce gelijkaardig



G-Cloud

- Business Impact Level (« BIL » of « IL »)

BIL 3.3.4
Availability
Integrity
Confidentiality

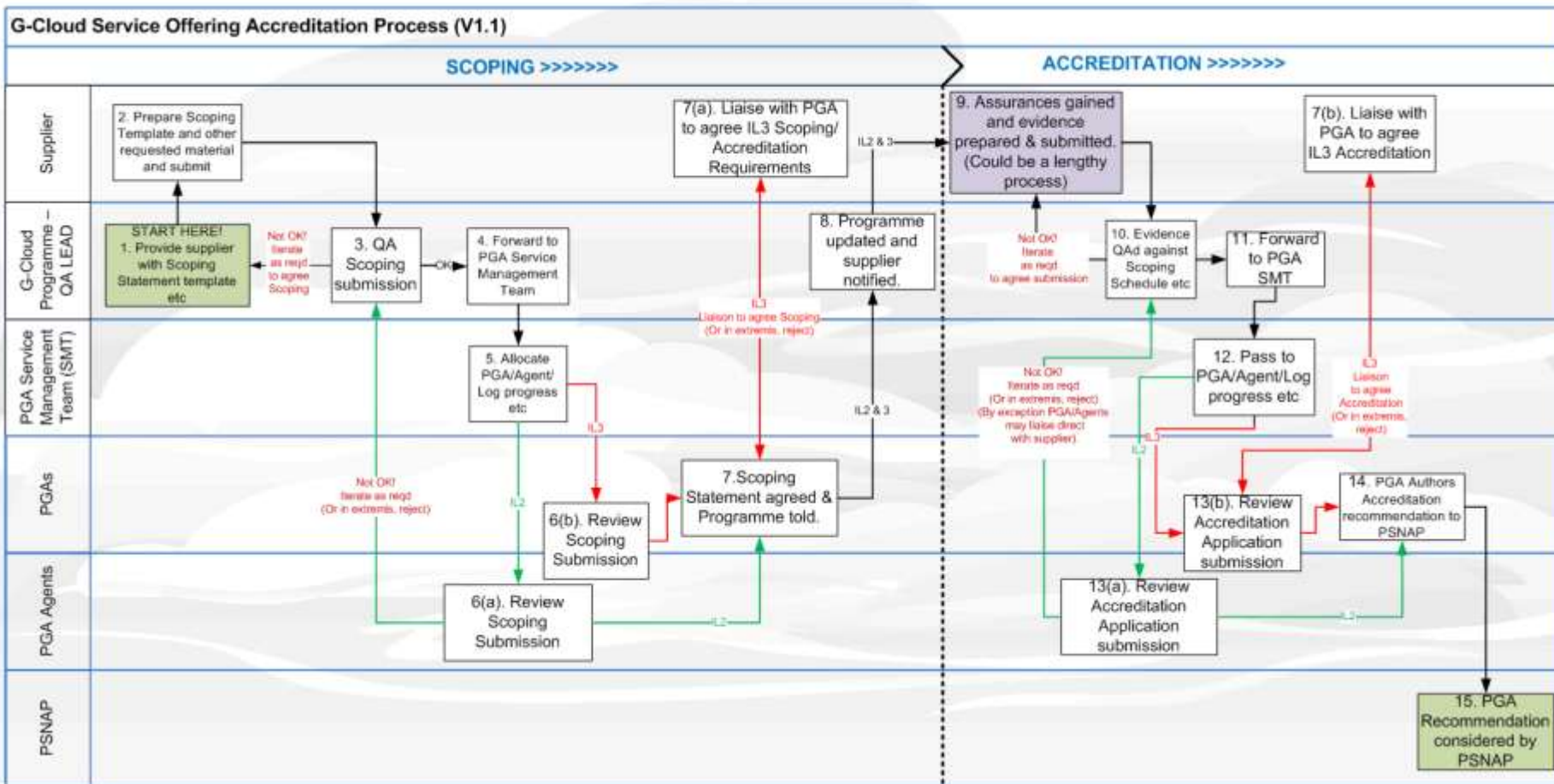


BIL 3



Pan Government Accreditation

⇒ Do it once



KEY

Green Lines are IL2 specific
 Red Lines are IL3 specific
 Black Lines are IL2 & 3
 Blue Lines are Function Separators

ABBREVIATIONS

IL - Impact Level
 PGA - Pan Government Accreditor
 PSNAP - Public Services Network Accreditation Panel
 QA - Quality Assurance
 SMT - Service Management Team

MISC NOTES:

- Boxes 6(b)/13(b). Straddle Functions
 - Assumes potential for dual resourcing.
- Boxes 7/7(a)
 - For IL2, direct liaison with supplier is by exception.
- Box 9. Evidence to comprise:
 - Certified Statement of Applicability (SoA)
 - Certification Report
 - Certificate
 - Risk Management Accreditation Document (RMAD)
 - Residual Risk Statement

G-Cloud

- Accreditation



*“11x/22x makes extensive use of suitably scoped **ISO/IEC 27001** certification “*

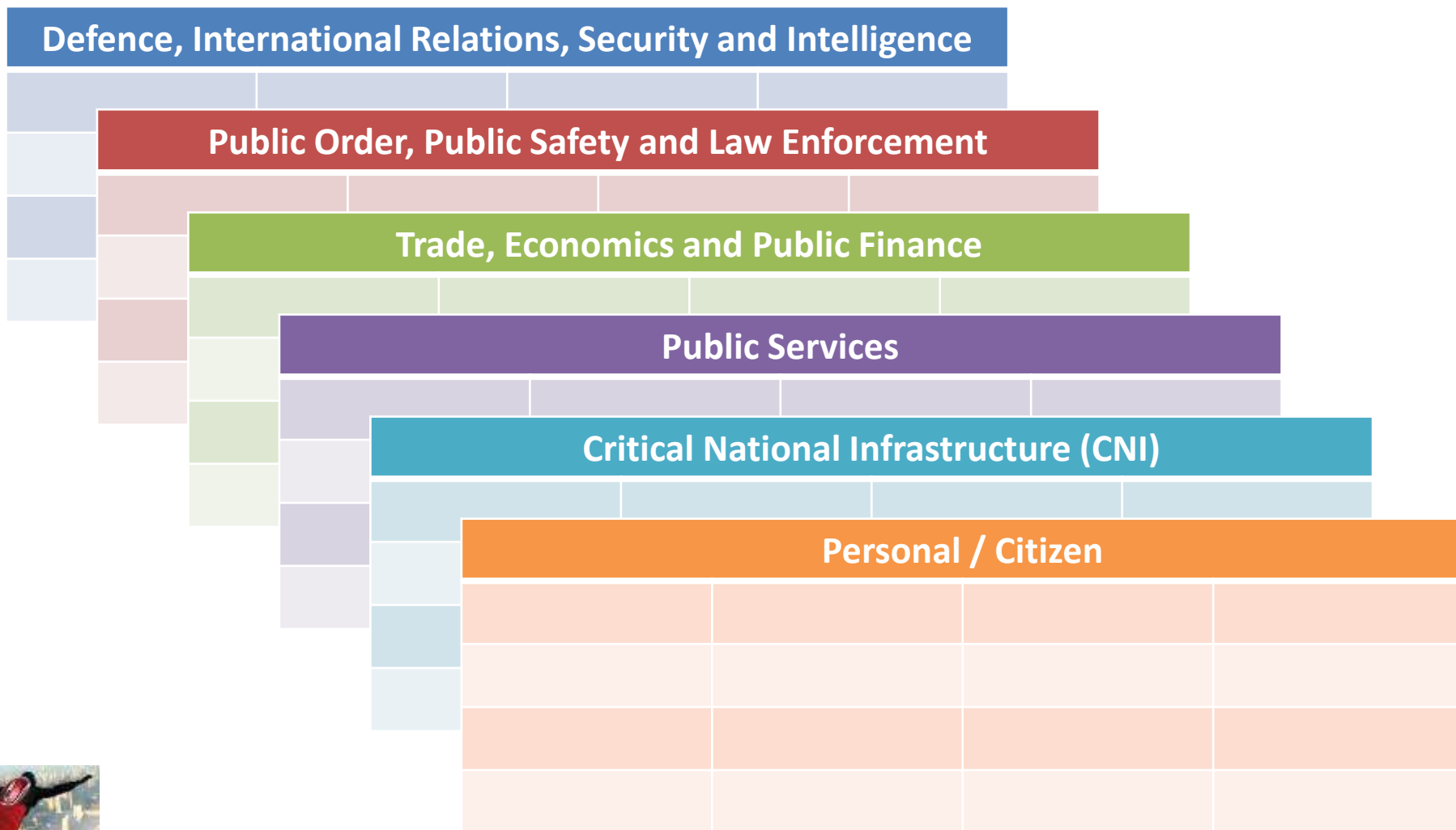
*“**BIL 33x** services will be delivered through **PSN Direct Network Service Providers (DNSPs)** and **will not be offshored** outside the UK. “*

*“Usage of cloud services at **BIL4** and above for Confidentiality should be implemented through **private cloud** services“*



G-Cloud

Bepalen gevoeligheid gegevens a.d.h.v. zes tabellen



G-Cloud

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4
				Minor injuries to a group of individuals or serious injury to an individual	
Impact on the Privacy of the Citizen	BIL 2		BIL 3		BIL 4
	Loss of control of many citizens' personal data beyond those authorised by each citizen.		Loss of control of a citizen's sensitive data beyond those authorised by the citizen. A compromise to the identity or financial status of an individual citizen.		Loss of control of many citizens' sensitive or financially significant personal data beyond those authorised by each citizen. A compromise to the identity or financial status of many citizens. Increased vulnerability to criminal attack.
Impact on the Privacy of the Citizen	None	personal data beyond those authorised by the citizen.	citizens' personal data beyond those authorised by each citizen.	beyond those authorised by the citizen. A compromise to the identity or financial status of an individual citizen.	authorised by each citizen. A compromise to the identity or financial status of many citizens. Increased vulnerability to criminal attack.
Impact on the Identity of the Citizen.	None	Illicit access using one individual's identity on behalf of another would cause inconvenience to the victim.	Illicit access using one individual's identity on behalf of another would allow the entry of incorrect information, thereby causing distress, or access to payments intended for that person or could further a subsequent impersonation attack on that individual.	Illicit access using several individual's identities would allow the entry of incorrect information, thereby causing distress, or access to payments intended for those people or could further subsequent impersonation attacks on several individuals.	Illicit access using many (thousands of) individual's identities would allow the entry of incorrect information, thereby causing distress, or access to payments intended for those people or could further subsequent impersonation attacks on many individuals.



Conclusies

Catalogus cloud-diensten op G-Cloud

Verfijnd classificatiemodel voor diensten en data

Protect data blijft in UK, Confidential data gov-managed

Pan-government accreditatie

Omzet vooral via consultancy

Cloud first strategy

Overheden Buitenland USA





Verenigde Staten

Cloud 1st strategy

Cloud Store stopgezet (~G-cloud)

Federal Data Center Consolidation Initiative (FDCCI)

- 3000 -> 1800 in 2015(-40%)
- D.m.v. cloud principes
- Ook nieuwe datacenters (vb. Utah Data Center)



Verenigde Staten

Gebruik commerciële diensten



Wel extra maatregelen

- Extra security
- FISMA accreditatie, ITAR, FedRAMP
- Logisch en fysiek gescheiden omgeving

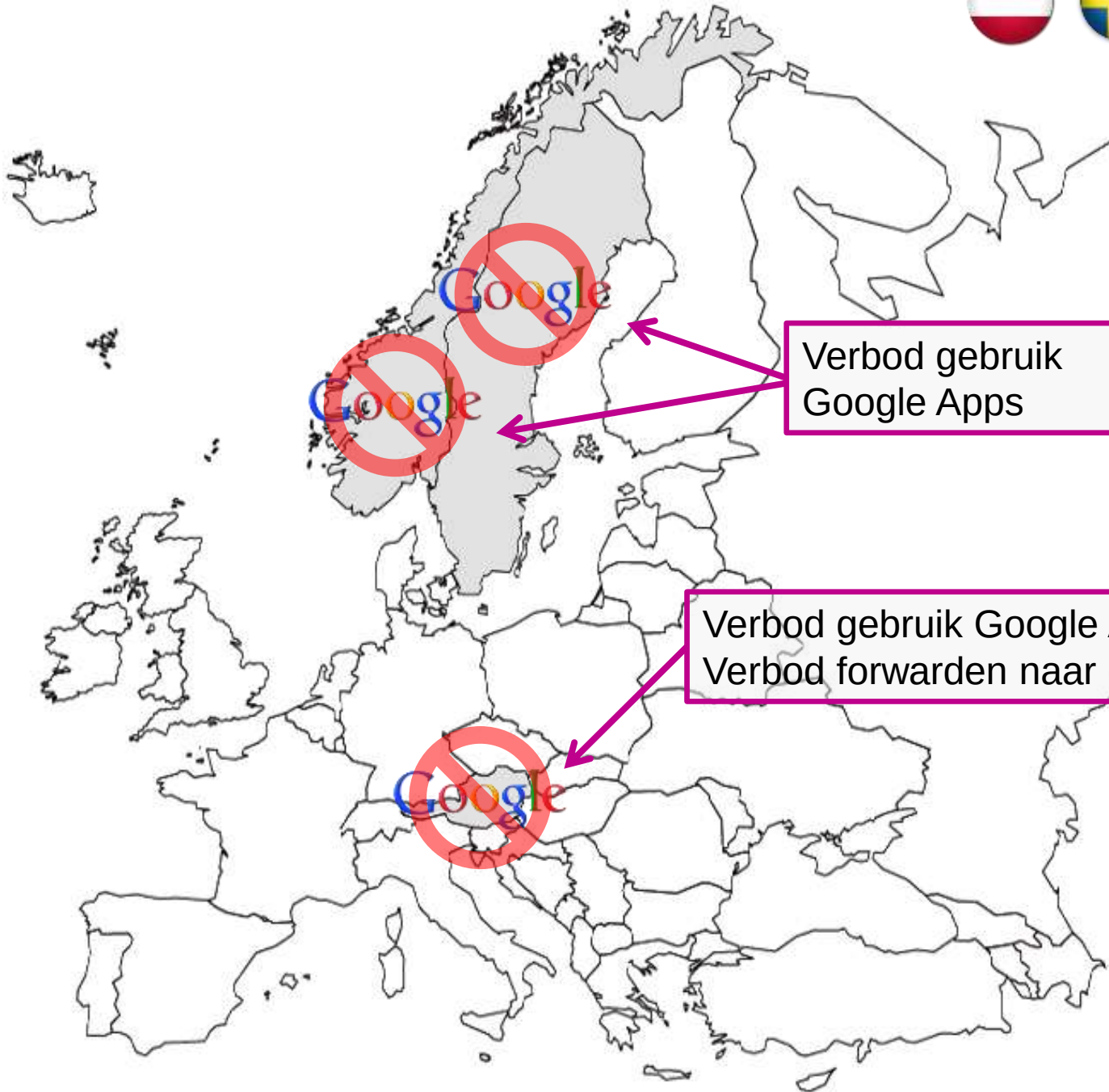
Nationale spelers ~ wereldspelers



Overheden Buitenland

Andere





Verbod gebruik
Google Apps

Verbod gebruik Google Apps
Verbod forwarden naar gMail

Overheden Buitenland Conclusies



Conclusies



**Confidential data
stays inside
the country**



**Soevereine clouds
in opbouw**

De soevereine cloud...



Toekomst



Europe



World economy

*« Vertrouwen is goed,
controle is beter »*

**Wat gebeurt echt met gegevens in de cloud?
Vb. Onthullingen Snowden**



facebook

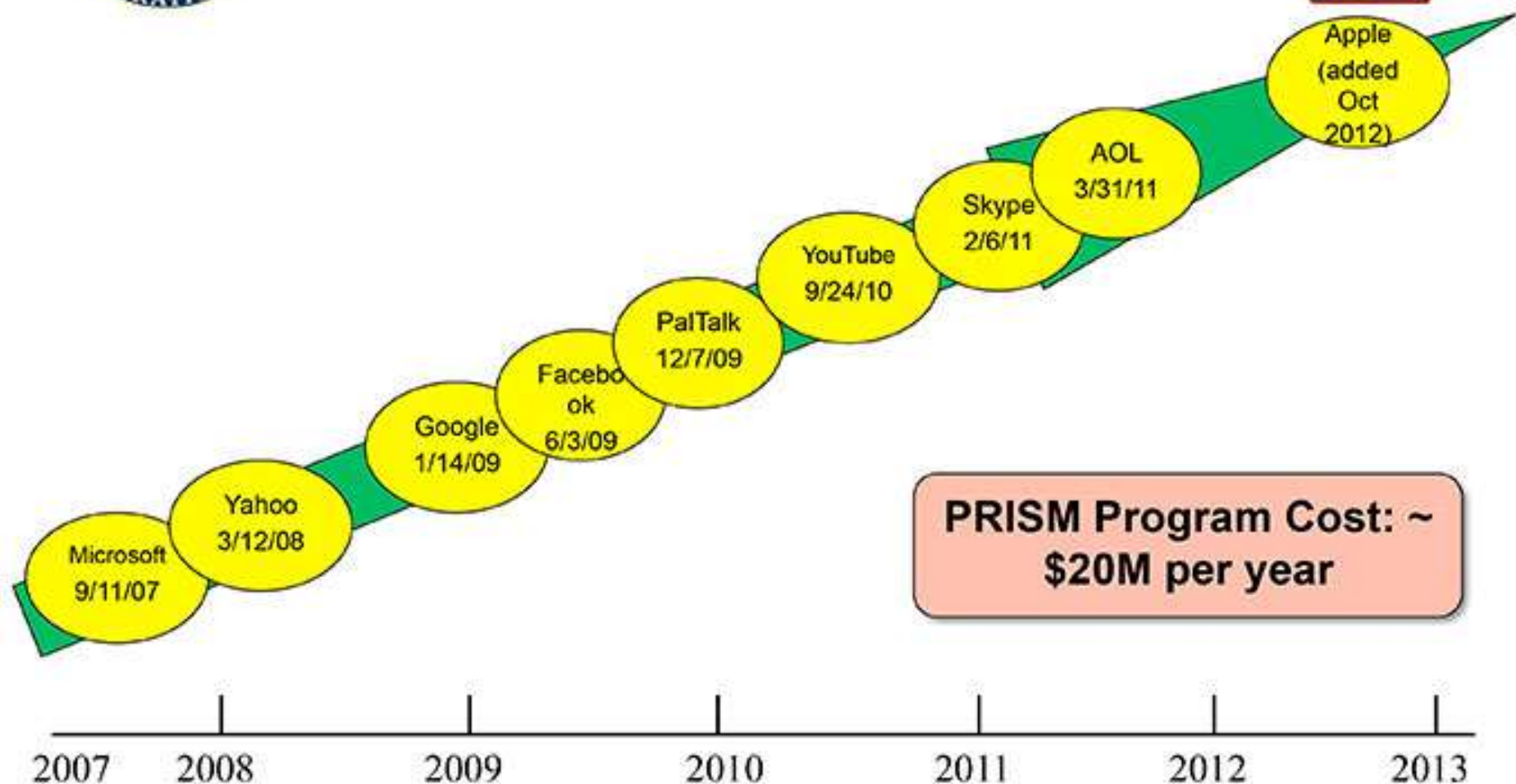


Hotmail

YAHOO!



(TS//SI//NF) Dates When PRISM Collection
Began For Each Provider



**PRISM Program Cost: ~
\$20M per year**

Ook andere landen bouwen inlichtingendiensten verder uit

*« BNC (Bundesnachrichtendienst)
wil 100 miljoen € investeren om
het Internet af te luisteren »*

Der Spiegel, 06/2013

**Natuurlijk moeten onze
inlichtingendiensten op
internet aanwezig zijn**

06/2013



Hans-Peter Friedrich, toenmalig
minister Binnenlandse Zaken (CSU)

Afhankelijkheid andere landen



Wat bij buitenlandse overname
eigen nationale spelers?

Nationale belangen VS. vrijemarktprincipes

Tegelijkertijd besparingsdruk

**Grotere landen meer schaalvoordelen bij
soevereine cloud**

En België

Verspreide initiatieven

- VDAB, VAPH
- Cloud policy SZ
- Synergieën SZ -> Community cloud

Nationale initiatieven?

- Fedict stootte op financiële obstakels

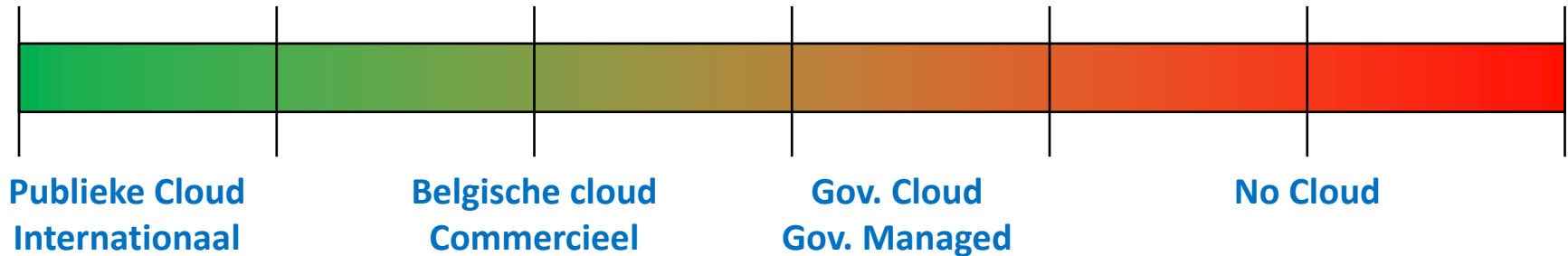
>> België loopt achter! <<



Mogelijke rol Smals

**Publieke
gegevens**

**Top Secret
gegevens**



Smals als CSB

Catalogus, UAM, monitoring,
advies, ...

Synergieën?

**Smals als
cloud aanbieder**

Vb. File sync & Share,
Virtuele servers

**Smals infrastructuur
(mits certificering)**

Suggesties?



« Was mich nicht umbringt, macht mich stärker »

Friedrich Nietzsche, Duits filosoof



Eindelijk...

File Sync & Share



De Cloud - Intro



Cloud Services Brokerage



Buitenlandse Overheden



Case: File Sync & Share

- Wat?
- Public Cloud
- Private Cloud
- Apps
- End-Point Security
- Nieuwe Dienst



Afronding

File Sync & Share Wat?



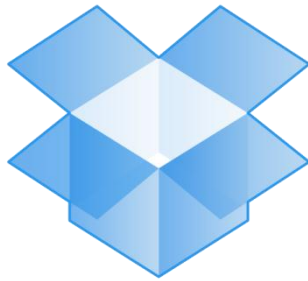
Zoals...

amazon cloud drive

 **OneDrive**



Google Drive

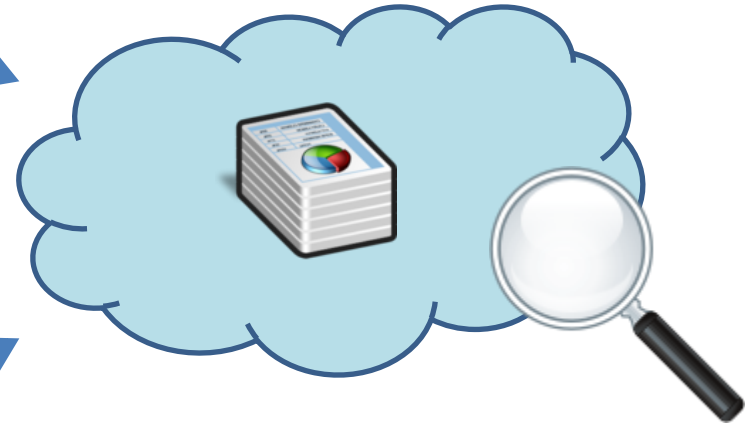


Dropbox

box

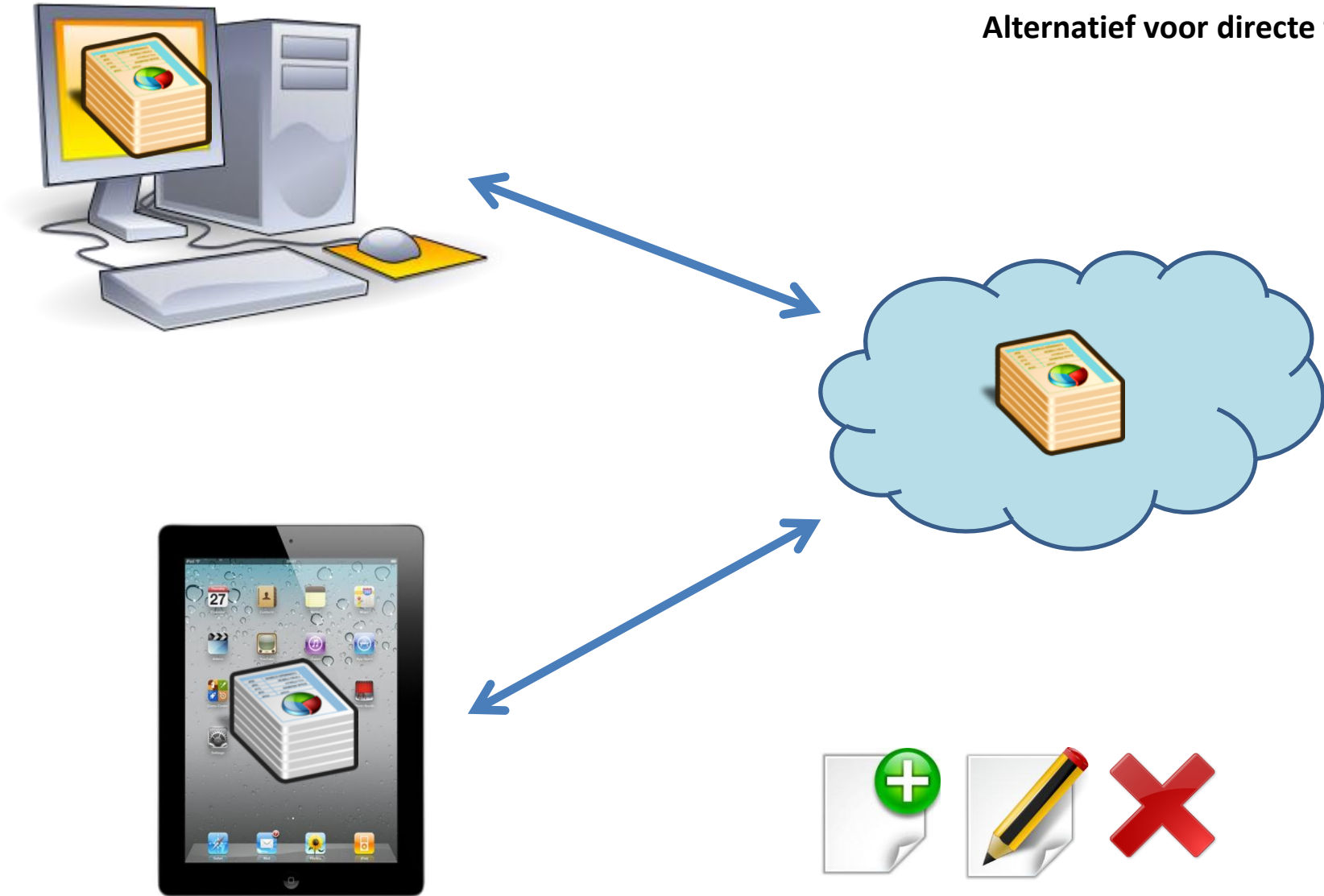
**voor bedrijven/overheden
= Enterprise File Sharing**

Direct Access (from everywhere)



Synchronisatie

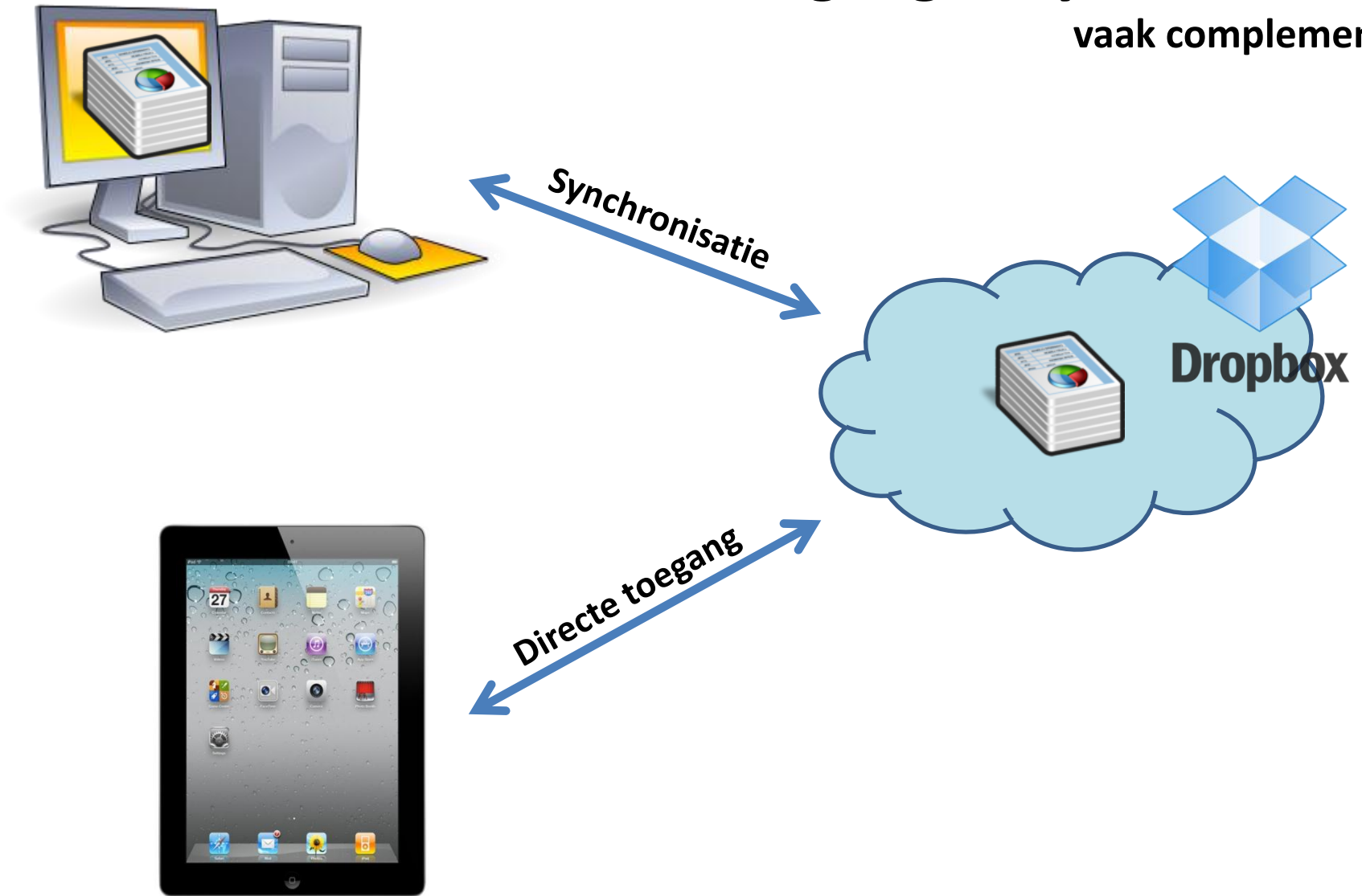
Alternatief voor directe toegang



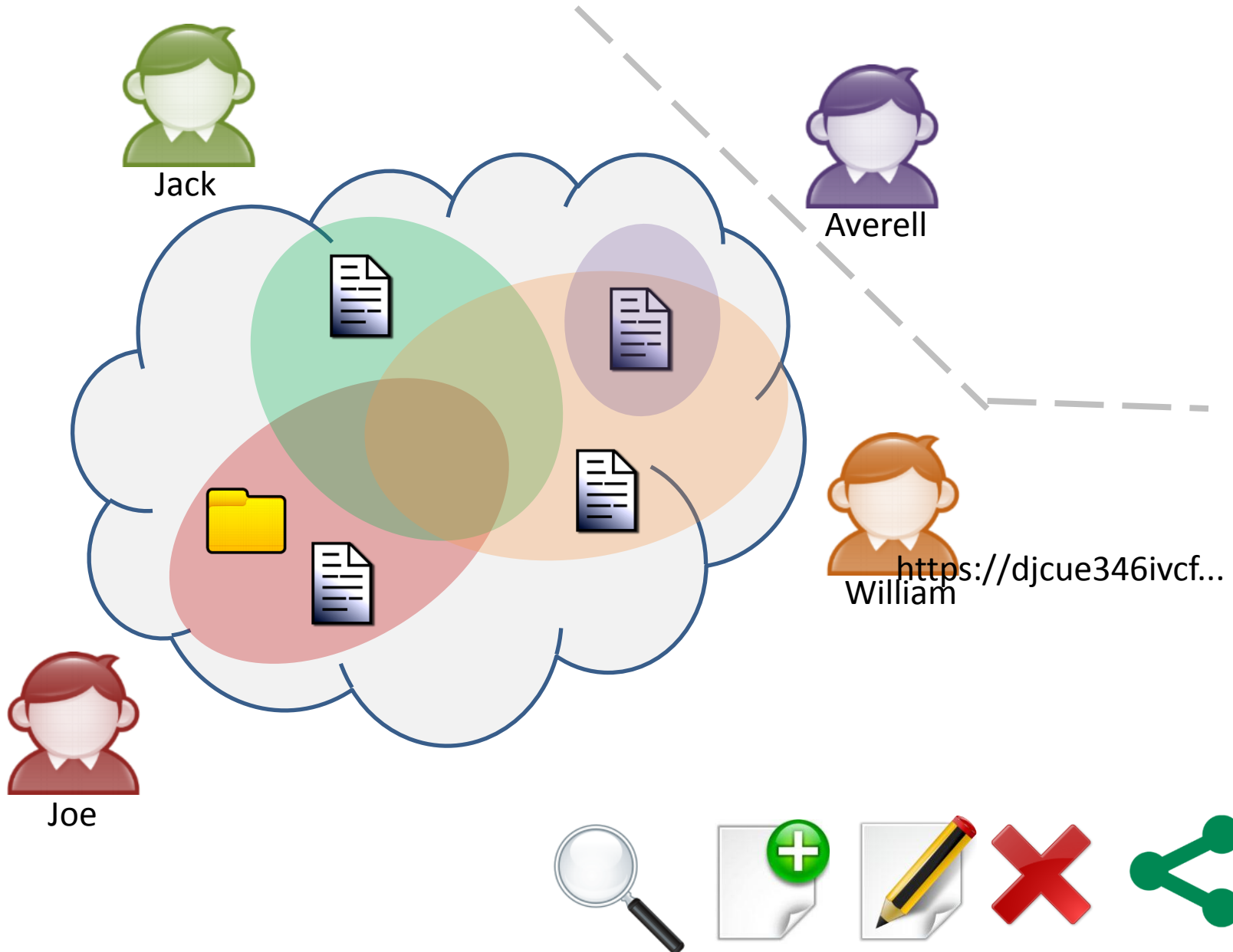
Extra synchronisatiestap neemt tijd
Daarna wel sneller toegang tot gegevens

Directe toegang & Synchronisatie

vaak complementair



Delen



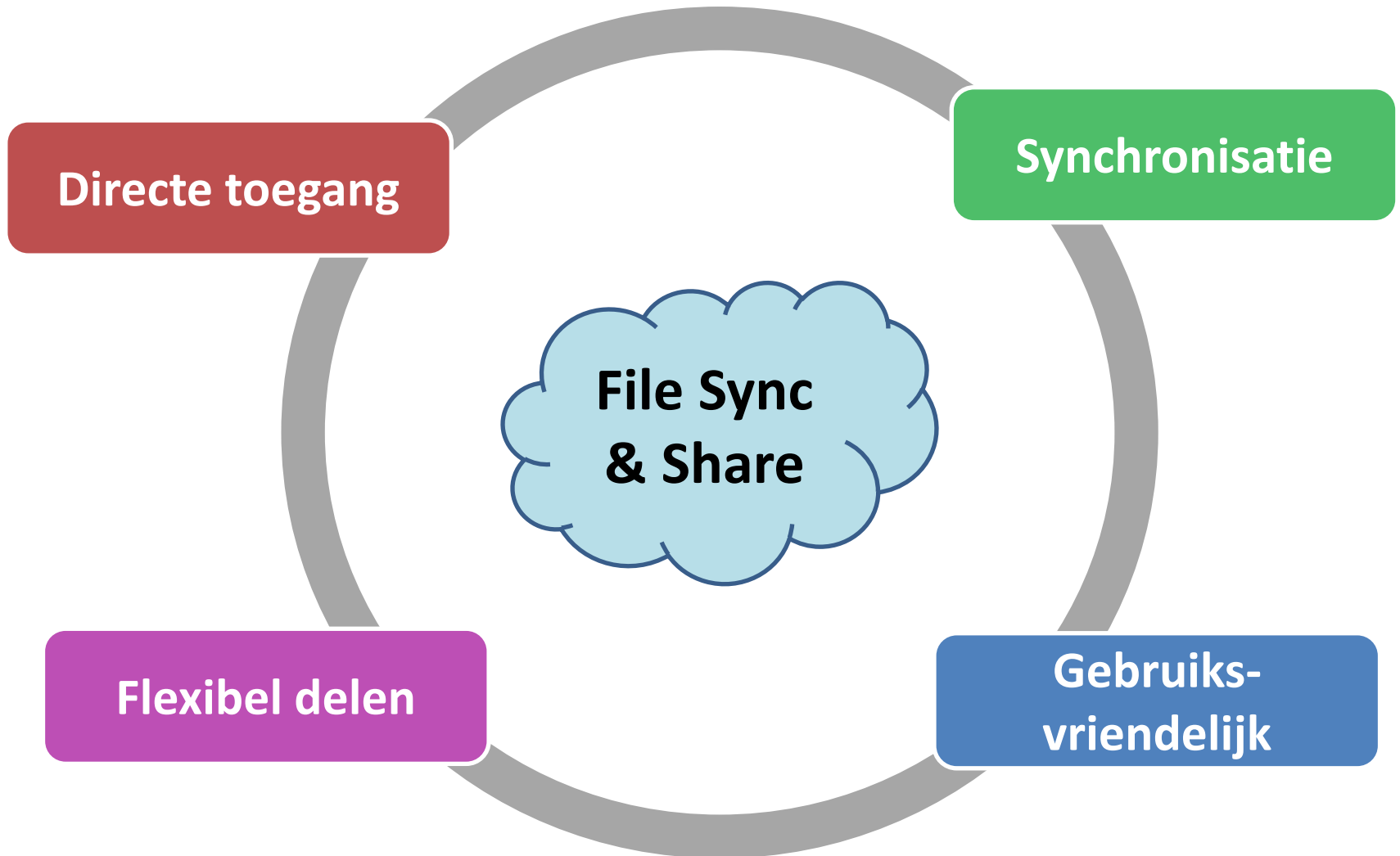
Gebruiksvriendelijk



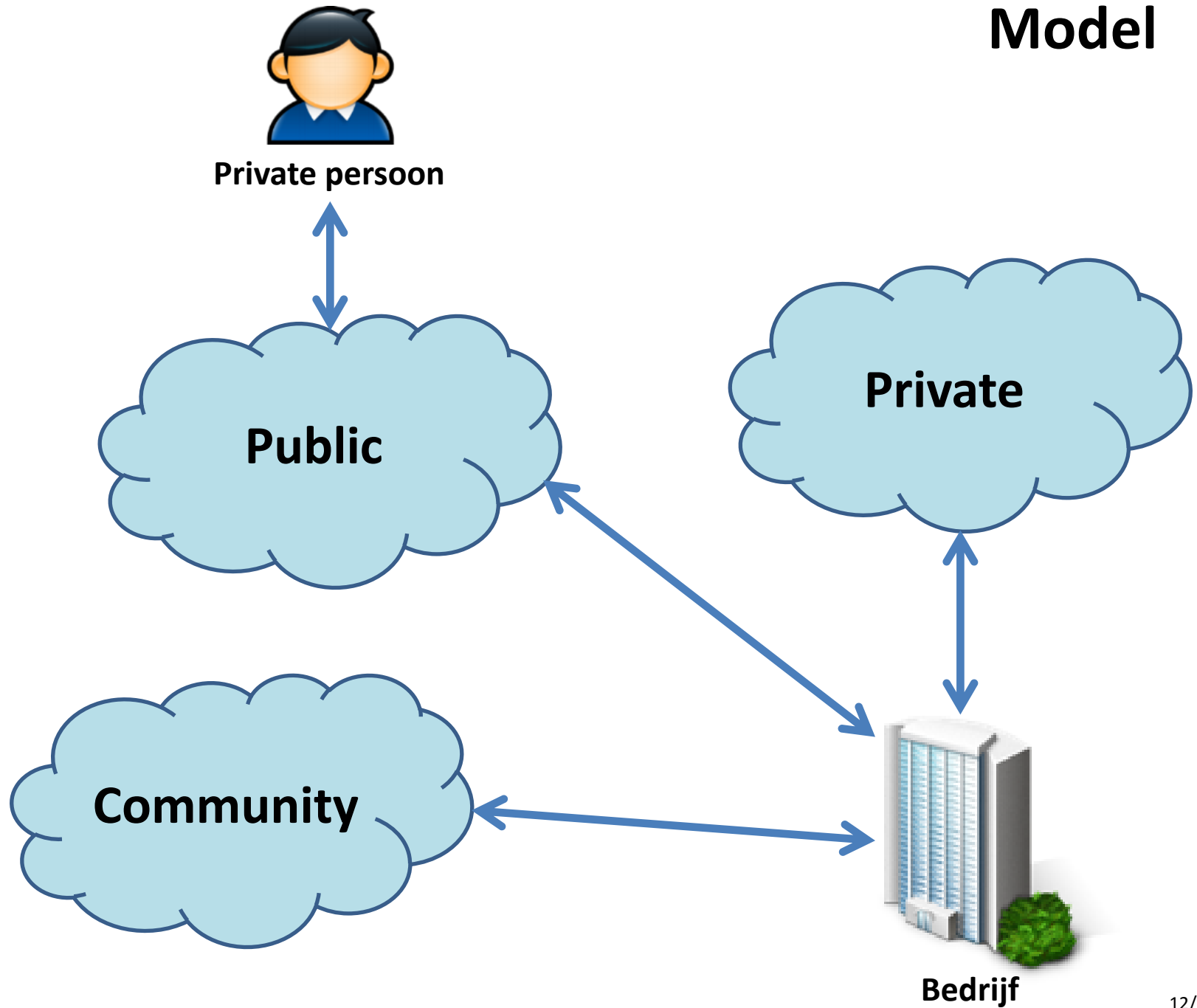
Te vermijden....



Samengevat



Model

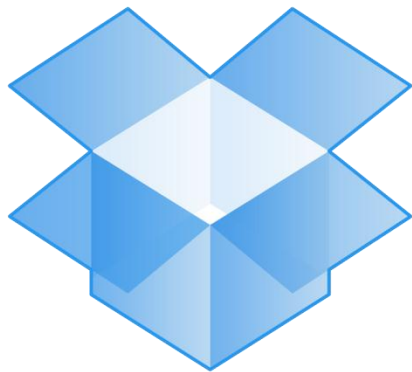


File Sync & Share Public Cloud





Google Drive



Dropbox



huddle™



Gevaren



Data exfiltration

- Wat indien medewerker weg (vb. naar concurrentie)
- Gehackte account (vb. door zwak paswoord)



Import malware

- Vb. Hacker plaatst bestand via Dropbox account op PC¹

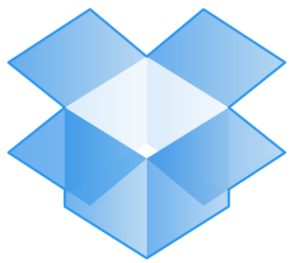


Geen controle

- Wie gebruikt welk FSS voor welke gegevens
- In hoeveel clouds staat onze gevoelige data?
- Data gelekt? Incident? -> Pers



(1) <http://www.infosecurity-magazine.com/view/33422/attackers-using-dropbox-and-wordpress-to-target-disguise-and-distribute/>

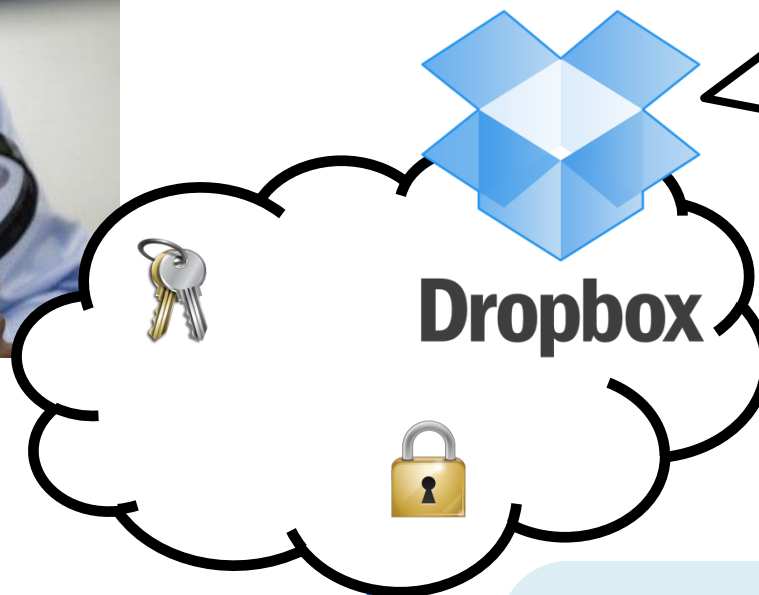


Dropbox

« Ook voor enterprise use! »

	Dropbox	Dropbox Pro	Dropbox for Business
Price	Free	\$9.99 / user / month	\$15 / user / month Minimum 5 users
Storage	2 GB	100 GB	As much as needed

Beperkingen...



"Secure Sockets Layer (SSL) & AES-256 bit encryption. Privacy policy and procedures"



SSL



- Dropbox? NSA? GCHQ? Anderen?
=> **Confidentialiteit?**
- Afhankelijk andere landen
=> **Beschikbaarheid?**

►► **Niet voor gevoelige data** ◄◄

Veelal gelijkaardig voor concurrenten in publieke cloud.

Op te lossen?



boxcryptor

≠



**BoxCryptor
Classic**

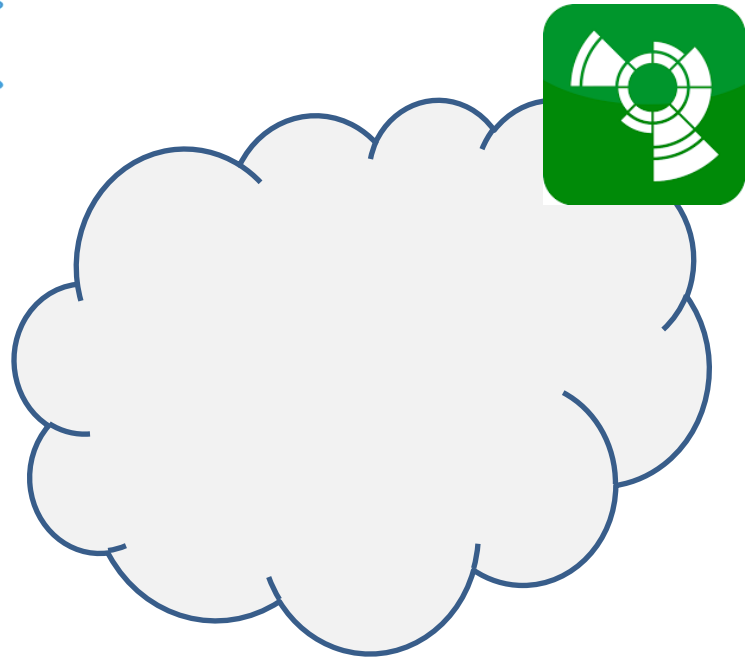
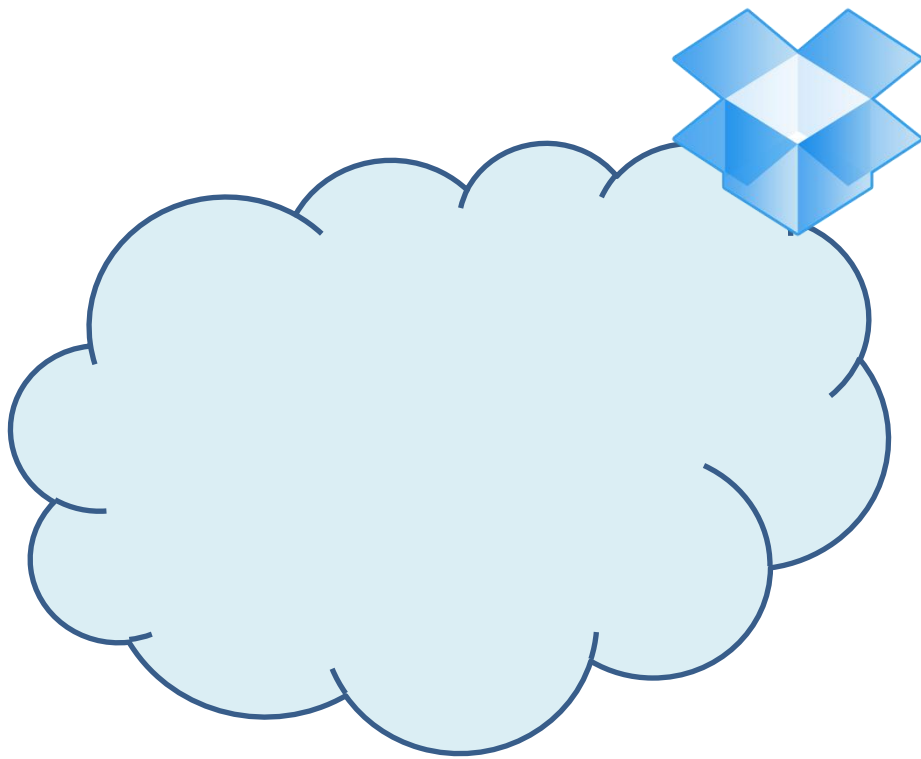


SafeMonk



BitTorrent® Sync

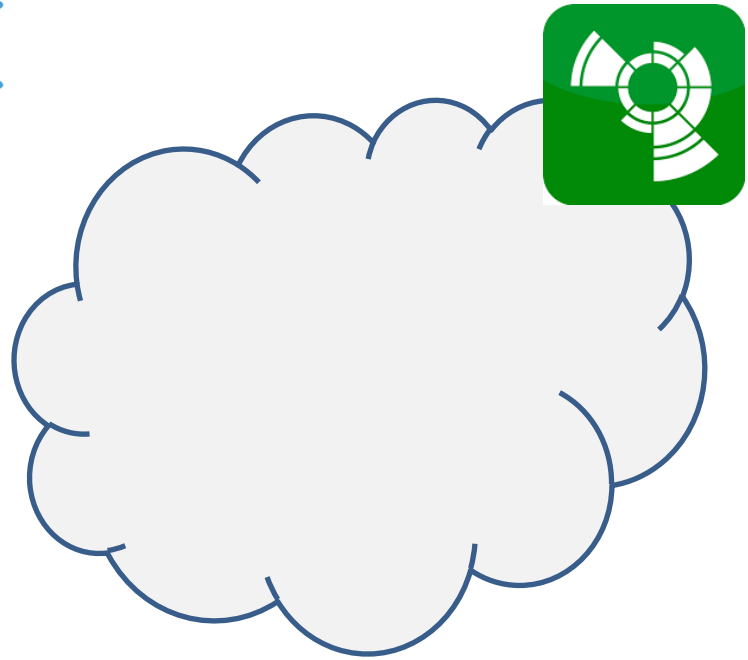
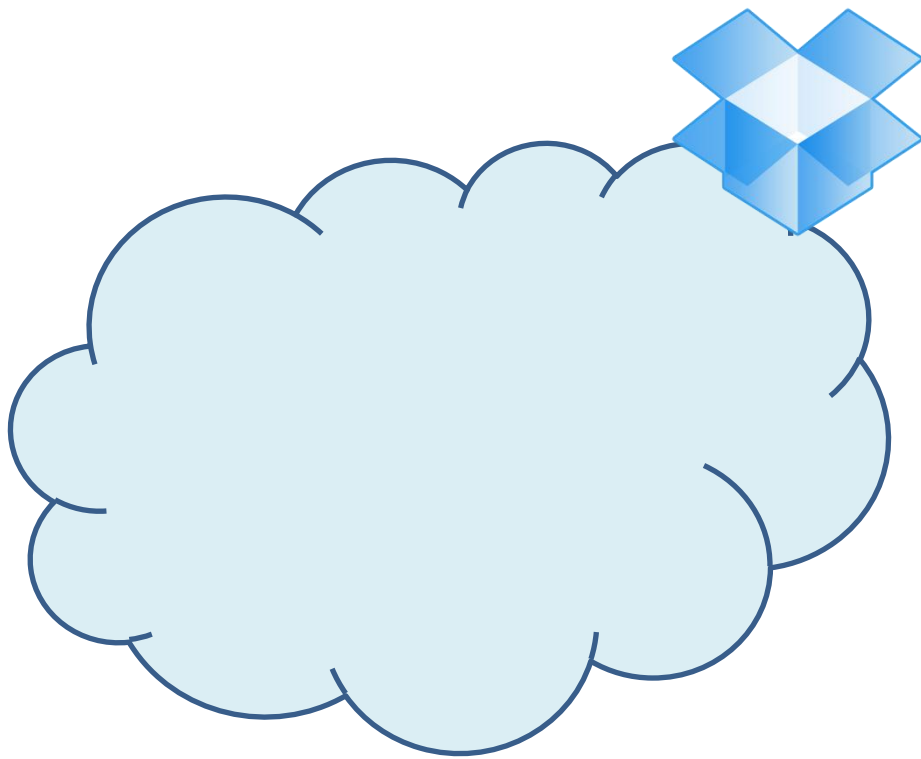




Bob



Johan



Initialisatie

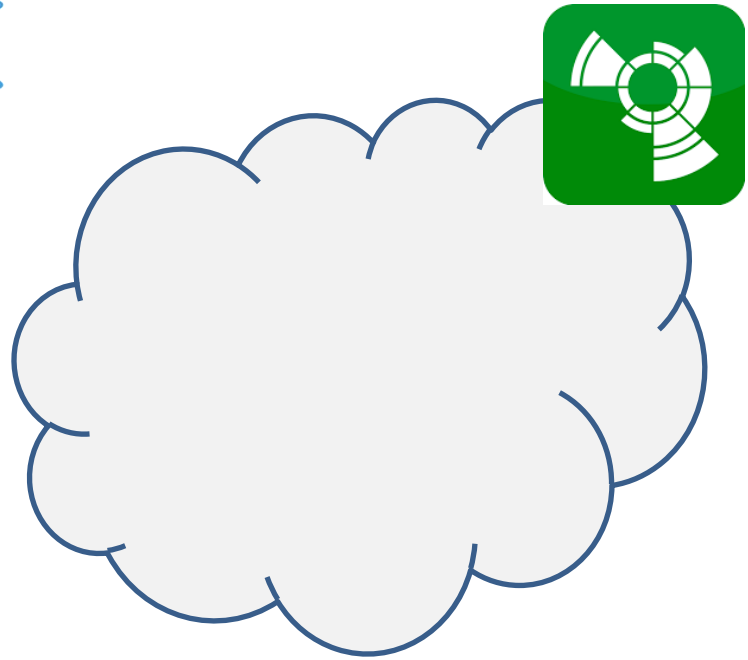
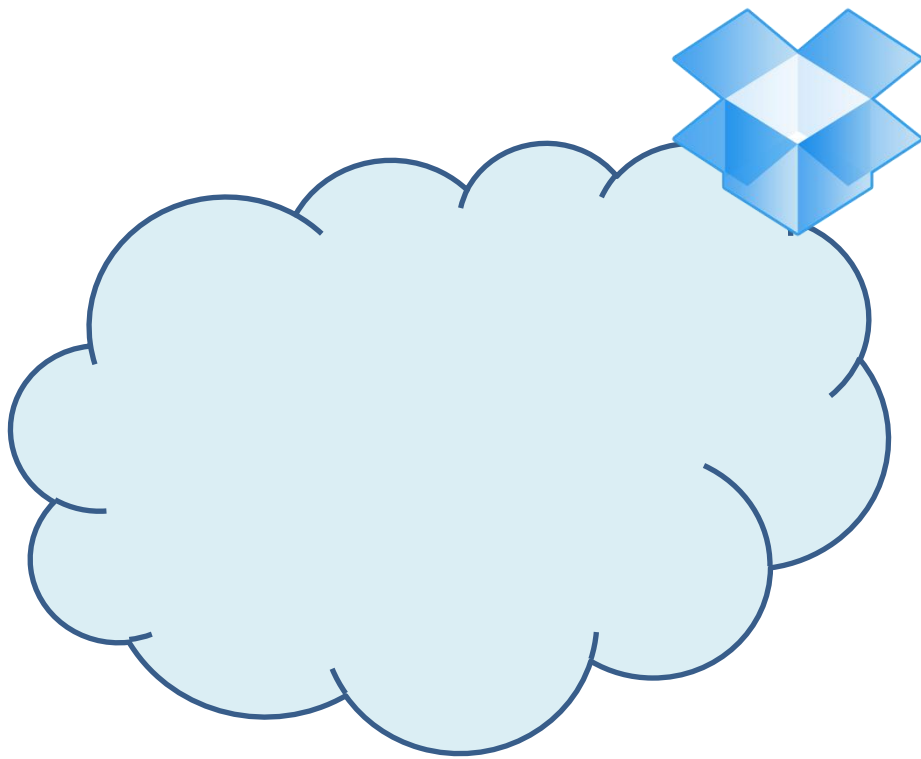
Sleutels lokaal gegenereerd in BoxCryptor client



Bob



Johan



Initialisatie

Sleutels lokaal gegenereerd in BoxCryptor client

Private sleutel password protected

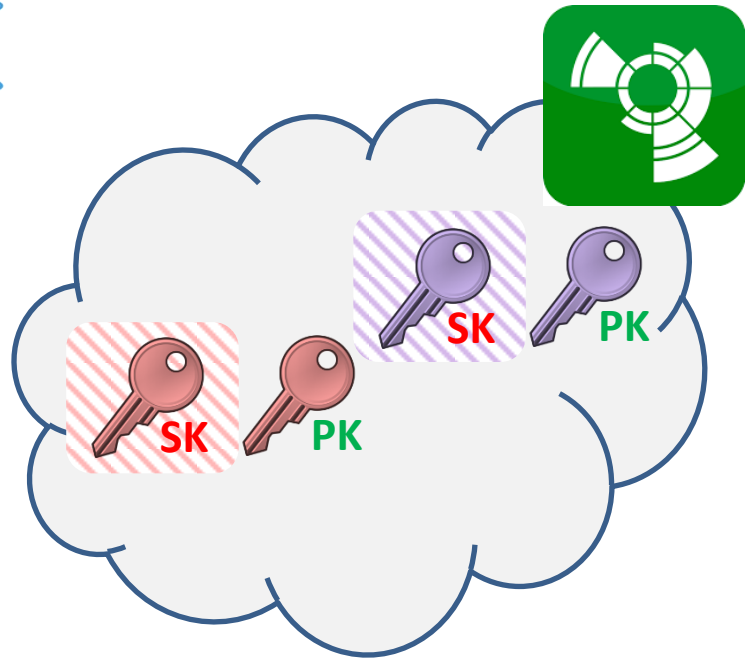
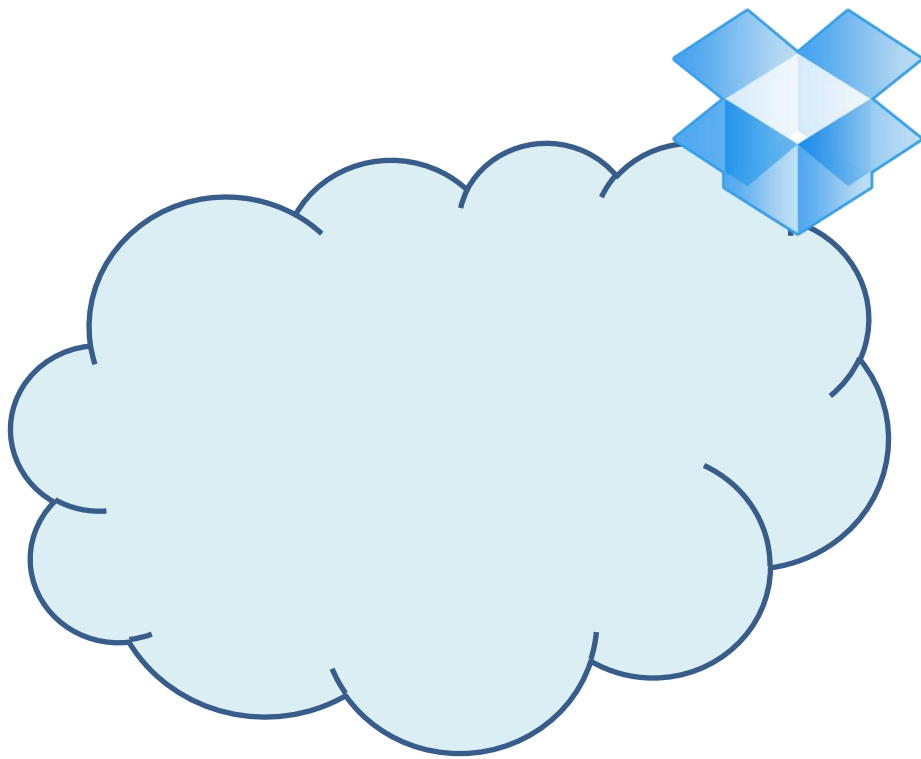
Beschermd sleutelpaar naar BoxCryptor cloud



Bob



Johan



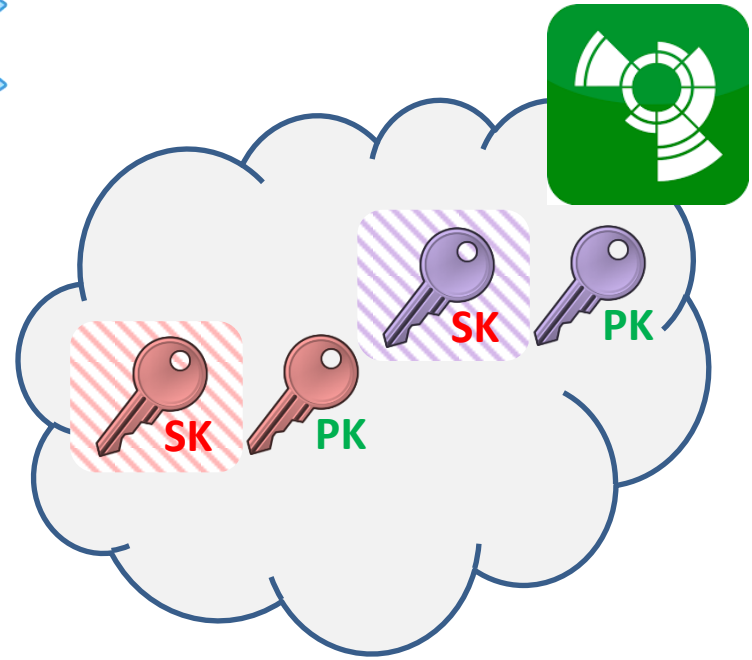
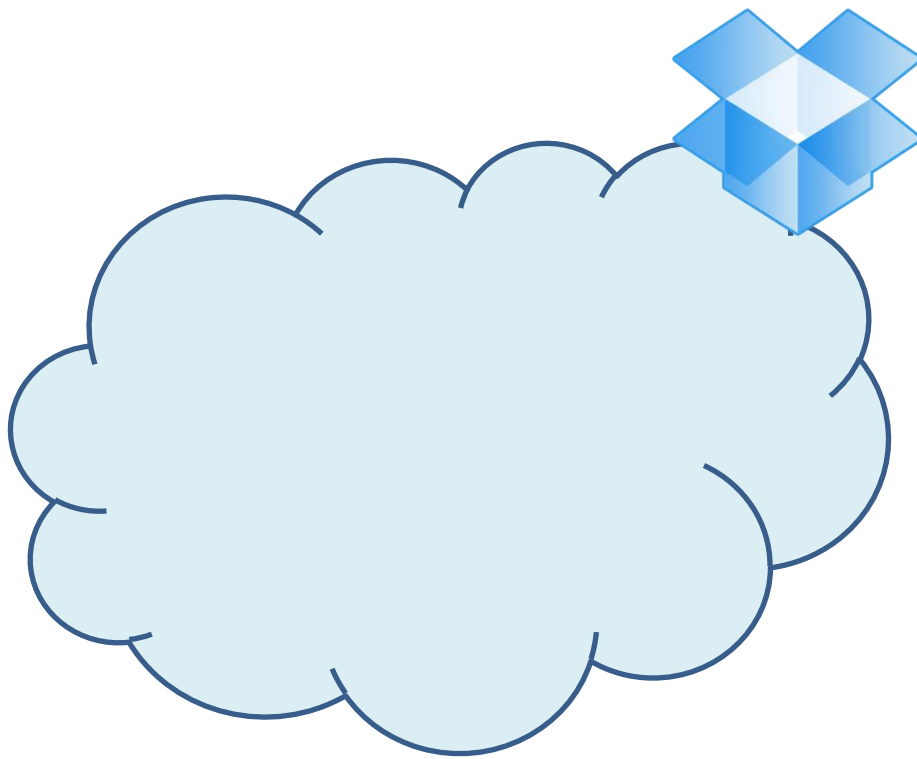
Uploaden bestand



Bob



Johan

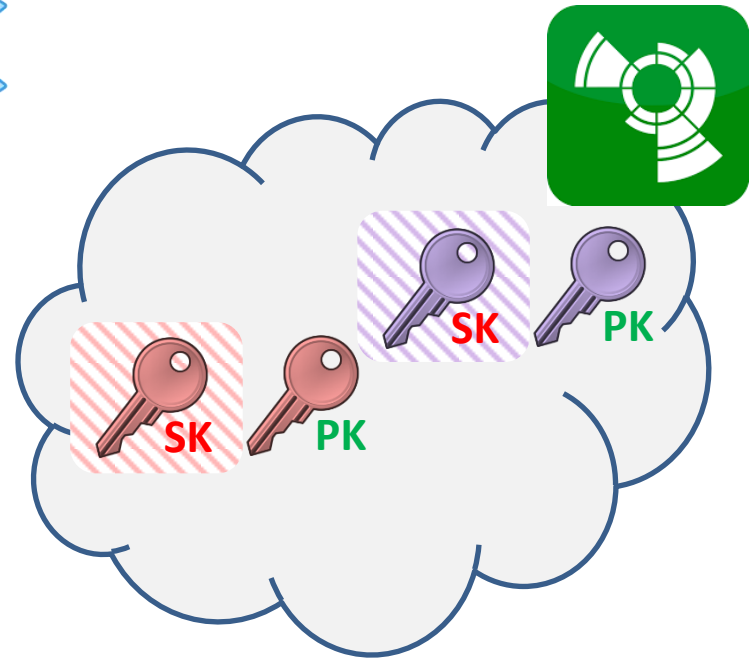
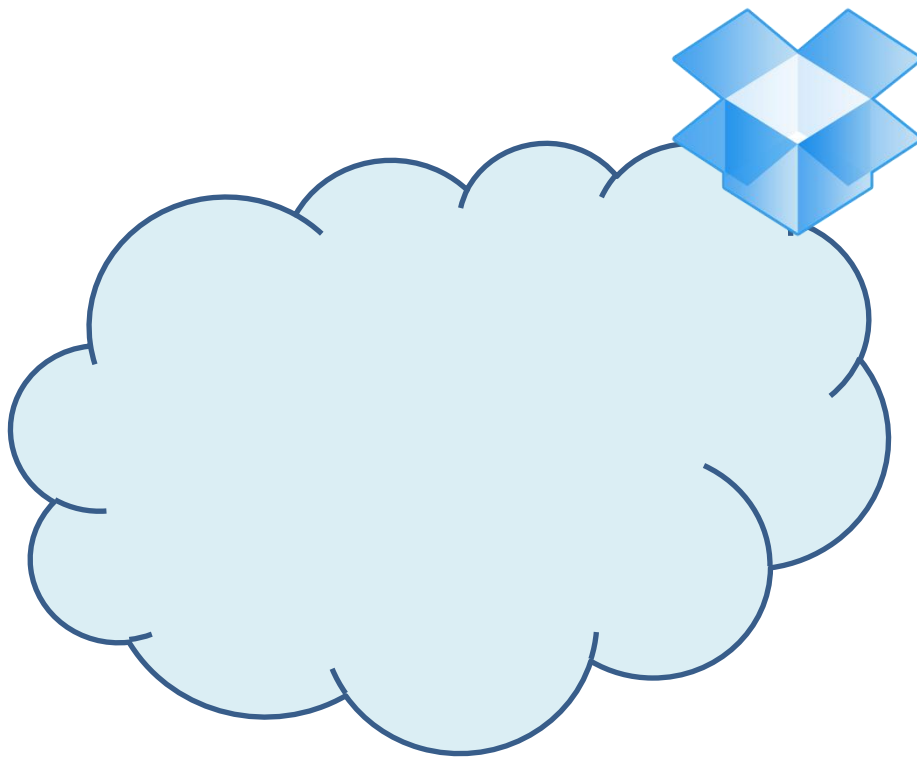


Bob

Uploaden bestand
Per file unieke AES sleutel gegenereerd



Johan



Uploaden bestand

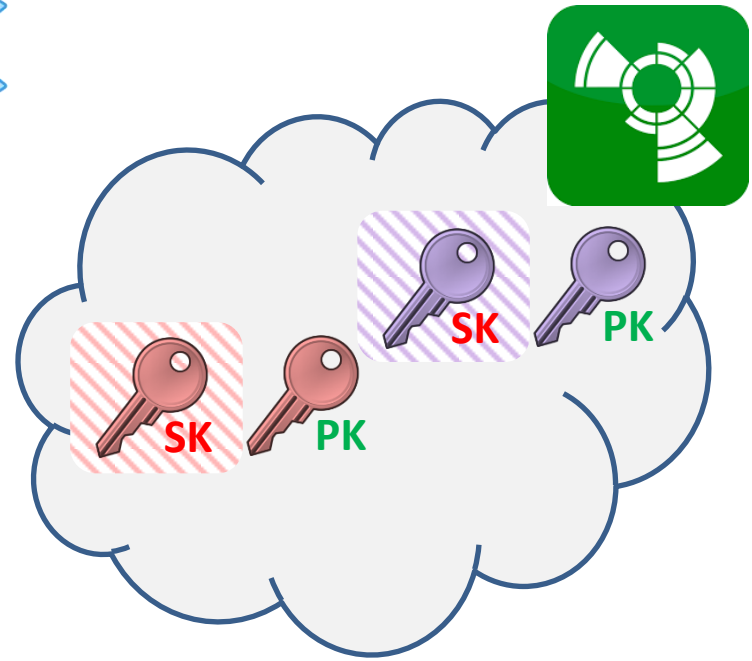
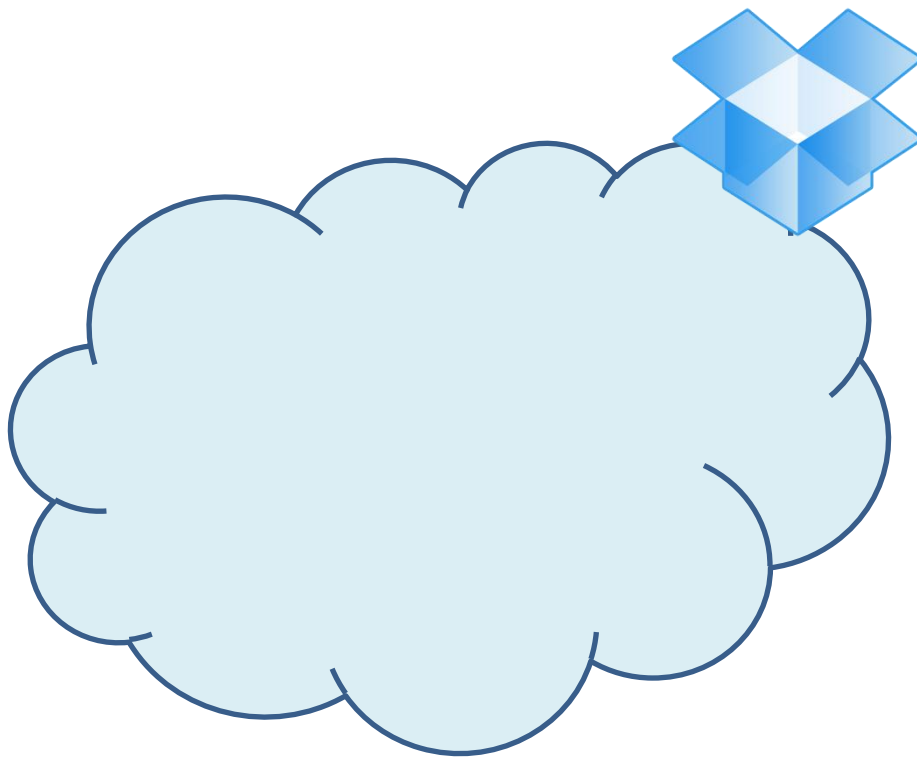
Per file unieke AES sleutel gegenereerd
AES sleutel vercijferd met publieke sleutel user



Bob



Johan



Uploaden bestand

Per file unieke AES sleutel gegenereerd
AES sleutel gecijferd met publieke sleutel user

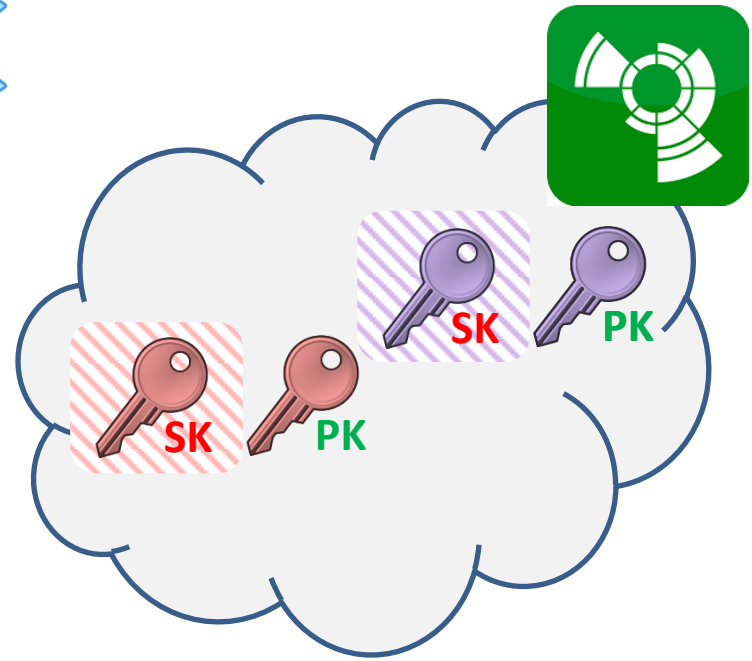
Vercijferde document + gecijferde sleutel naar Dropbox cloud



Bob



Johan



Delen

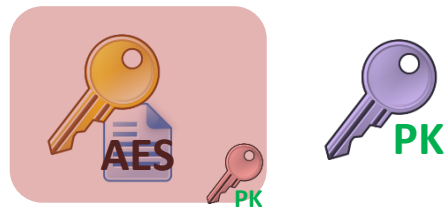
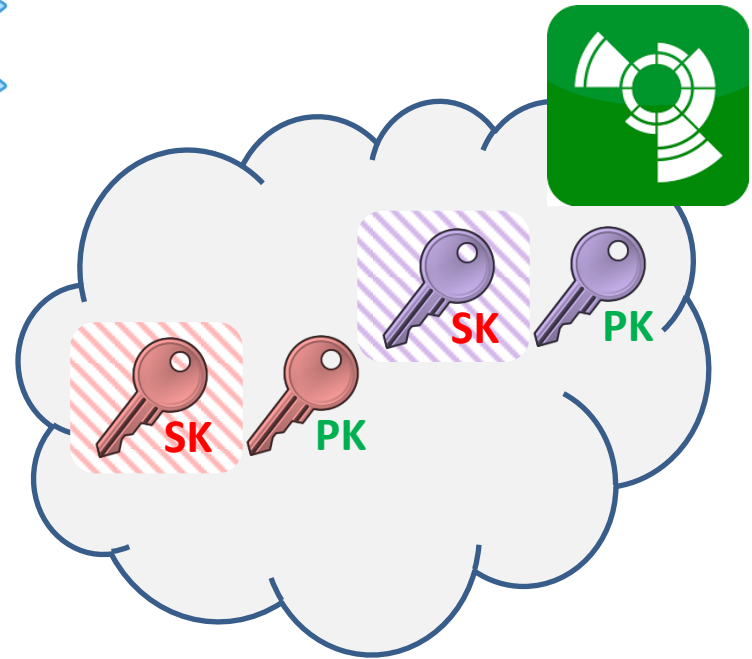
File-key + publieke sleutel Johan gedownload door Bob



Bob



Johan



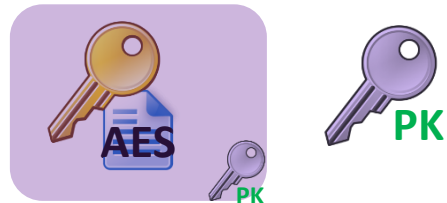
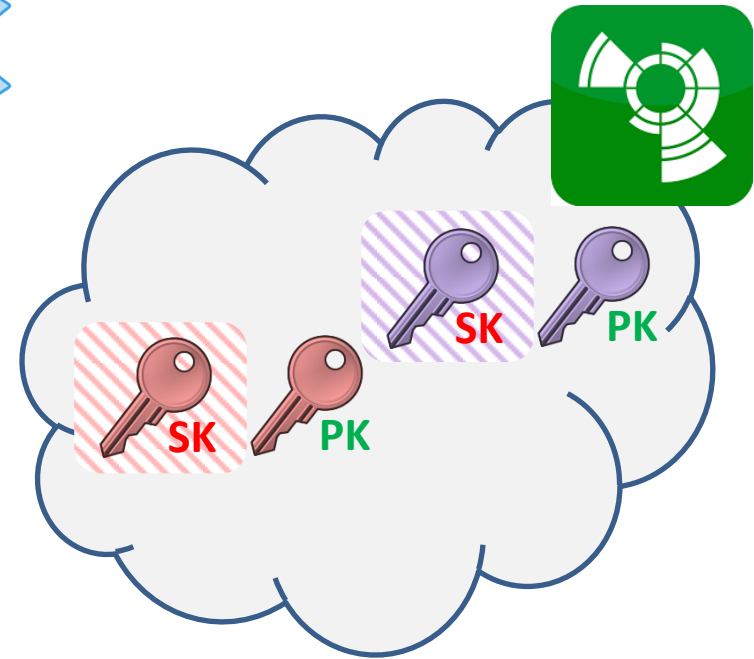
Bob



Johan

Delen

File-key + publieke sleutel Johan gedownload door Bob
Bob decrypteert file-key



Bob



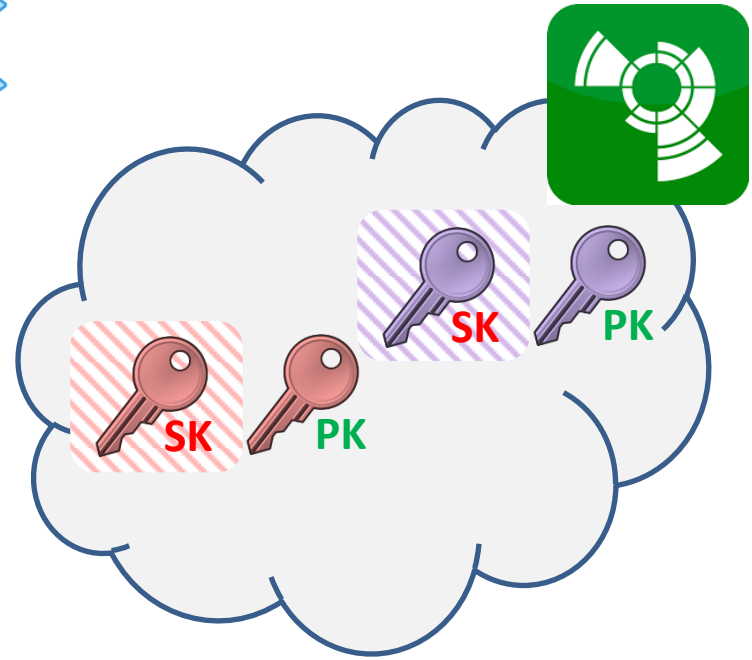
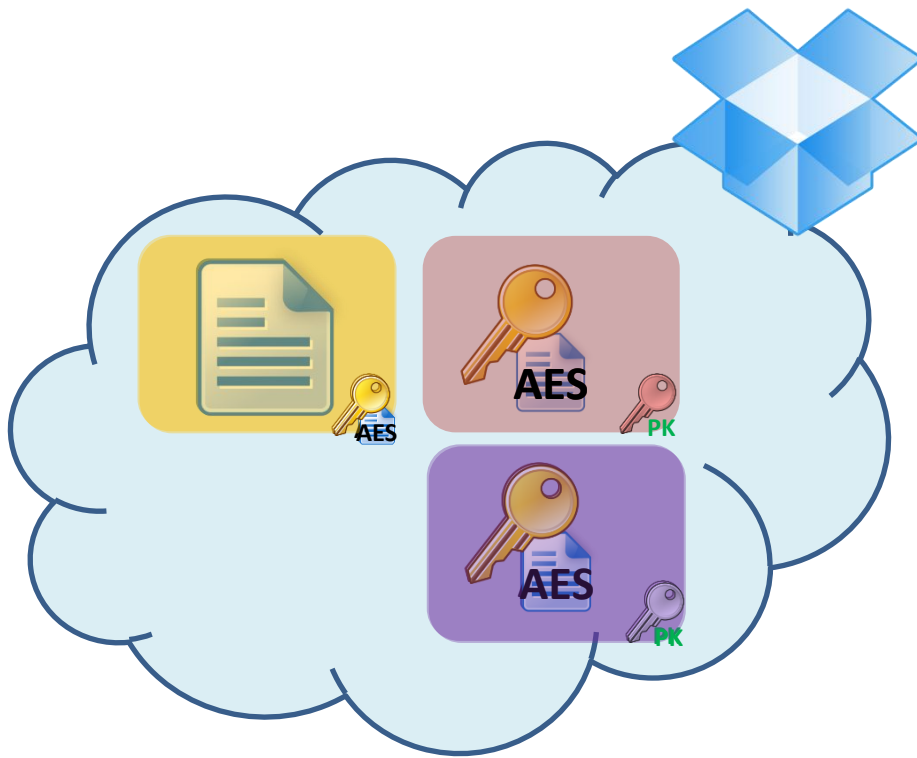
Johan

Delen

File-key + publieke sleutel Johan gedownload door Bob

Bob decrypteert file-key

Bob encrypteert file key met publieke sleutel Johan



Toegang gegevens

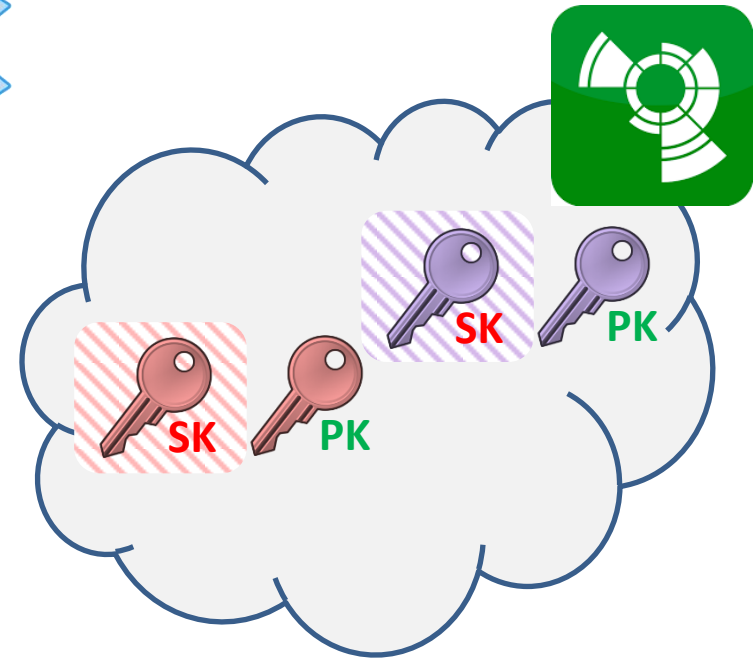
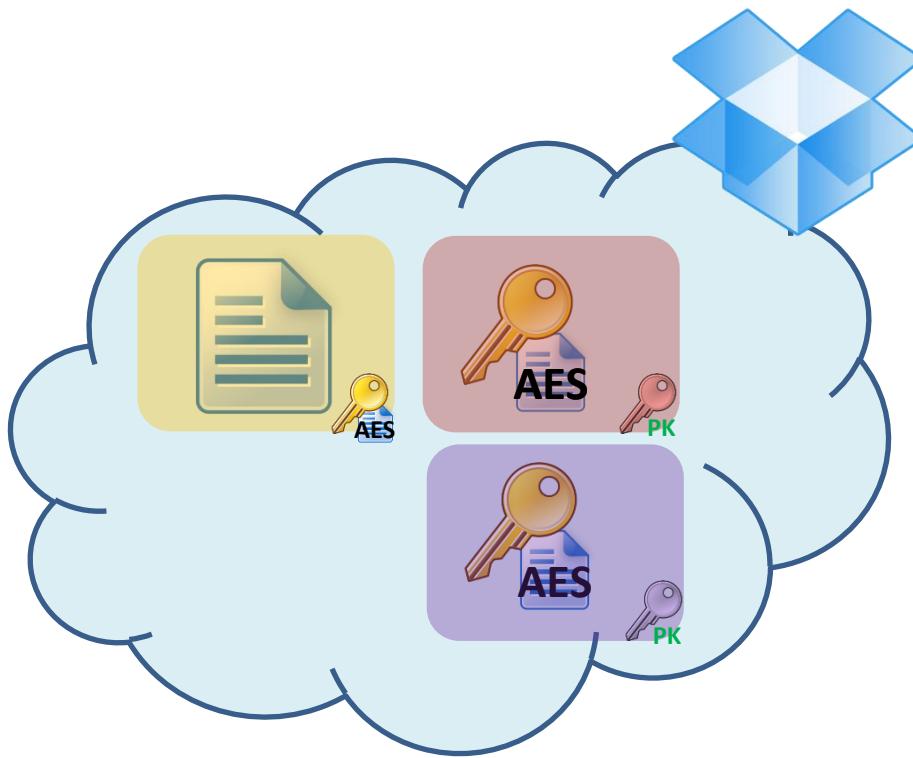
Johan downloadt doc + geëncrypteerde file key



Bob



Johan



Toegang gegevens

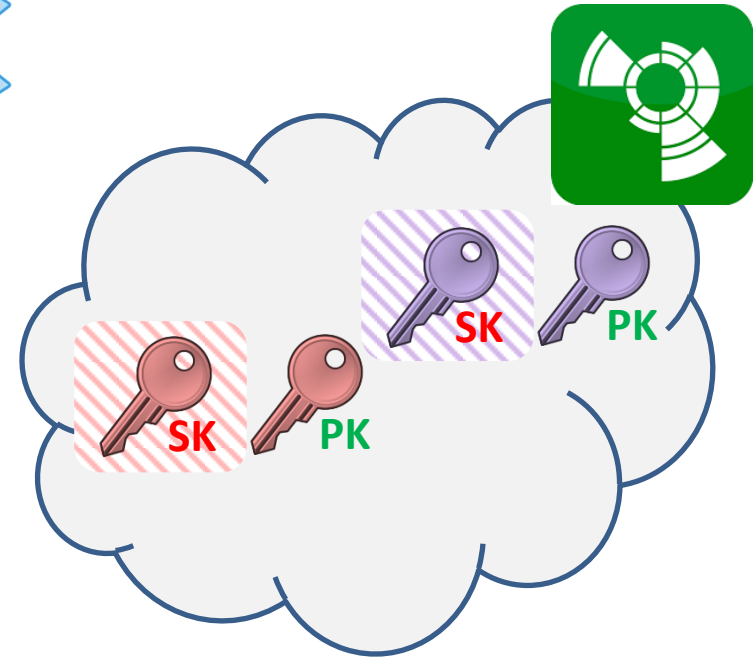
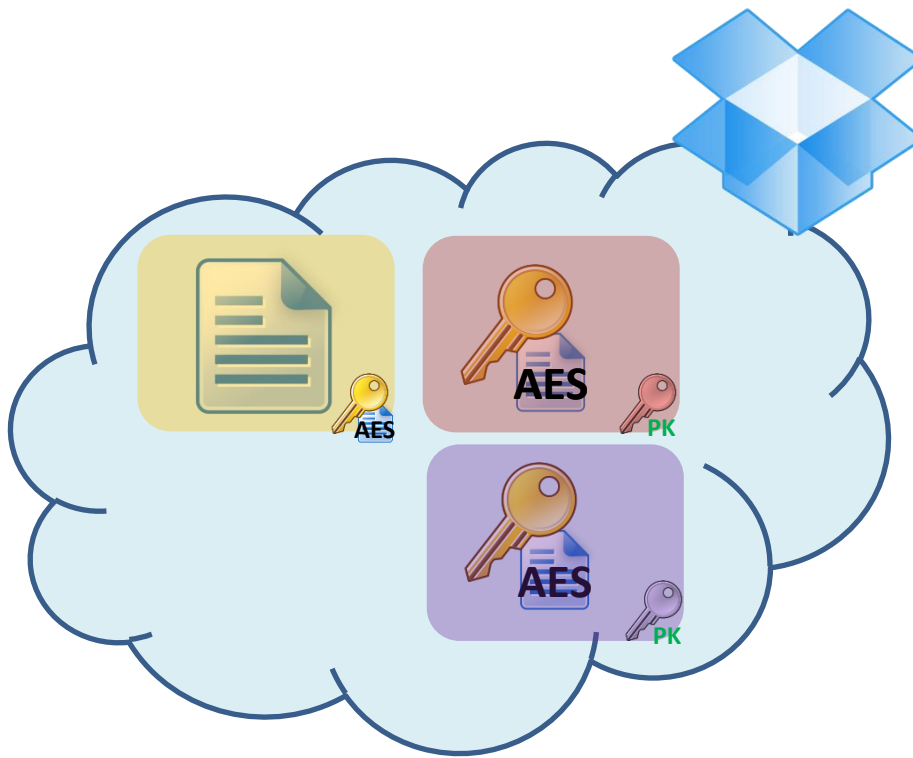
Johan downloadt doc + geëncrypteerde file key
Johan decrypteert file key met zijn private sleutel



Bob

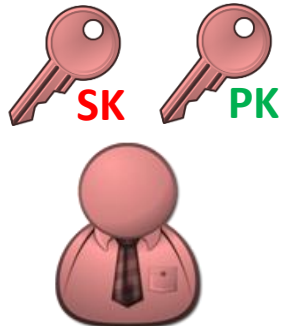


Johan



Toegang gegevens

- Johan downloadt doc + geëncrypteerde file key
- Johan decrypteert file key met zijn private sleutel
- Johan decrypteert doc met file-key



Bob



Johan

Conclusies

Functionaliteit & gebruiksvriendelijkheid

- Delen blijft mogelijk
- Enkel toegang met BoxCryptor client
- Dropbox webclient onbruikbaar
- 2 accounts nodig (Dropbox & BoxCryptor)

Security

- Dropbox geen toegang tot gegevens
- Afhankelijkheid buitenland blijft
- Indien overal zelfde paswoord -> BoxCryptor toegang tot data?
- Beperkte enterprise-functionaliteit (volgende slide)

FUNCTIONS

My Account

Groups

Devices

Policies

Users

Help

Add policy

Policy	Disable remember password
Description	Disable remember password
	Disallow creation of groups
	Disallow filename encryption
	Disallow to join groups
	Login ip restriction
	Master key
	Maximum number of devices
	Maximum number of root folders
	Minimum password length
Value	Require filename encryption

Download

Windows

Mac

Android

iPhone / iPad

Chrome

We willen integratie met eigen UAM
i.p.v. beperkt user & policy mgt voor
elke cloud-dienst afzonderlijk



*Interessant concept,
maar minder geschikt in onze context*



SafeMonk



boxcryptor

Client-side encryptie + opslag bij bestaande FSS dienst



TeamDrive
Sync your data fast & secure



Client side encryptie + Eigen opslag



syncplicity

Uitgebreid enterprise management
Geen client side encryptie
Eigen opslag mogelijk

*Enkele bedenkingen
bij public cloud FSS oplossingen*

FSS oplossingen vaak
initieel **consumer**-oriented



Trachten nu **enterprise**
functionaliteit toe te voegen
(incl. security)



SafeMonk



boxcryptor

Er zijn oplossingen
met extra security

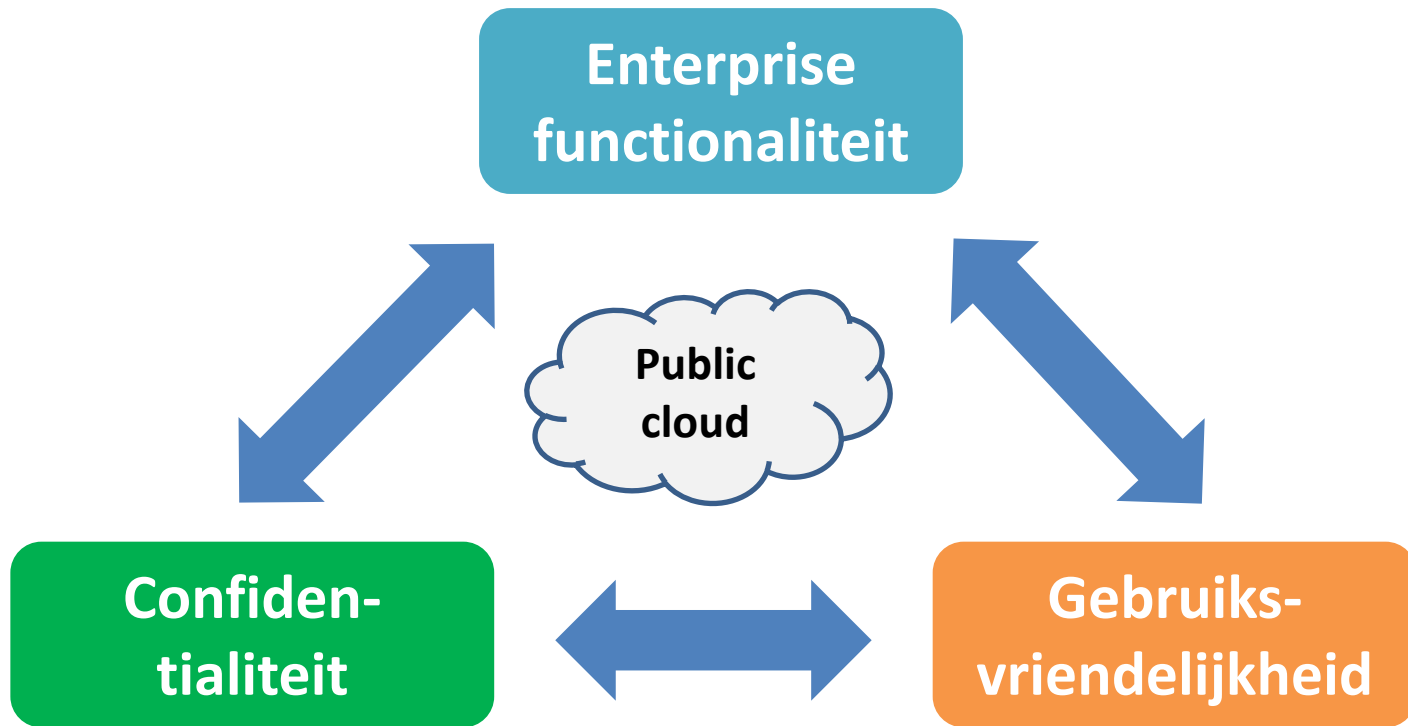


syncplicity



Desondanks...

Spanningsveld



De drie elementen samen in de public cloud
lijkt momenteel moeilijk

Hoe op te lossen?



File Sync & Share Private Cloud



Scenario: Delen Documenten

- ~ OneDrive / DropBox / ...
- Gehost door Smals
- Delen docs meetings
- Tablet
- Off-line toegang
- Gebruiksvriendelijk



Een CEO



Cobaye



Proefkonijn





Server
bij Smals



Tablet CEO



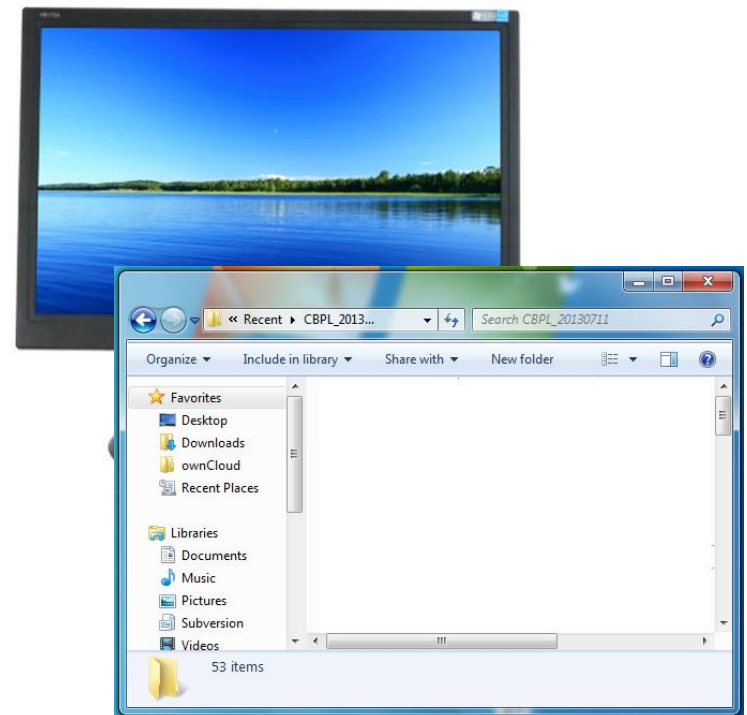
Computer
Secretariaat CEO



Server
bij Smals



Tablet CEO

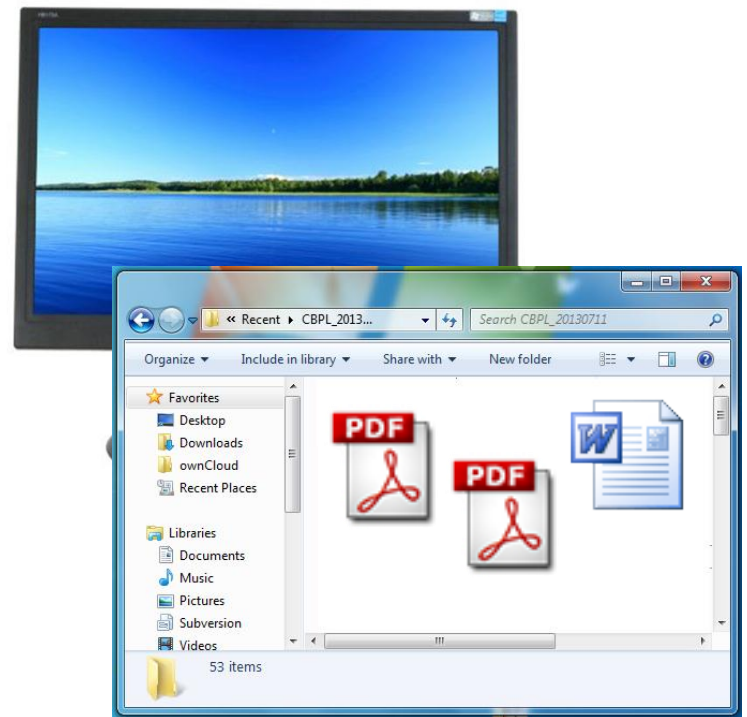




Server
bij Smals



Tablet CEO



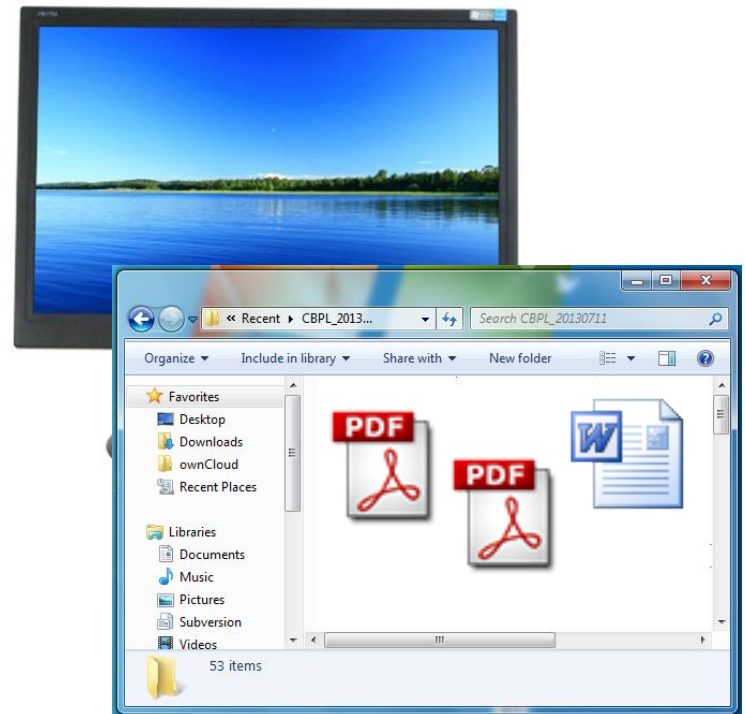


Server
bij Smals

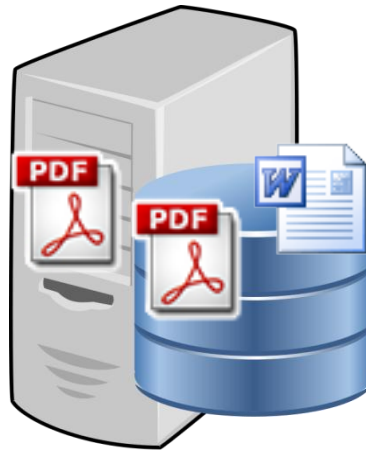
Synchronisatie
Bestanden worden
automatisch gekopieerd
naar server bij Smals



Tablet CEO



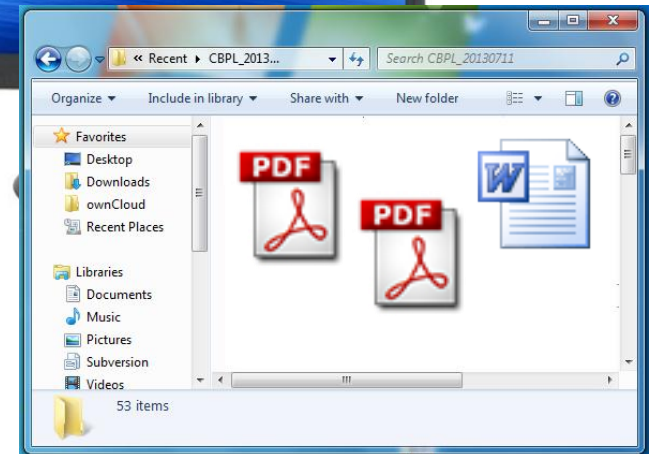
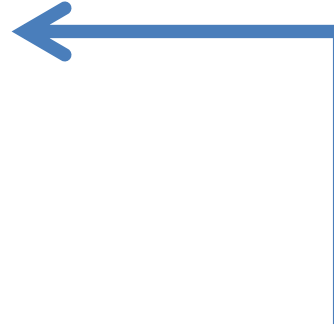
CEO synchro-
niseert zijn tablet met
de server bij Smals

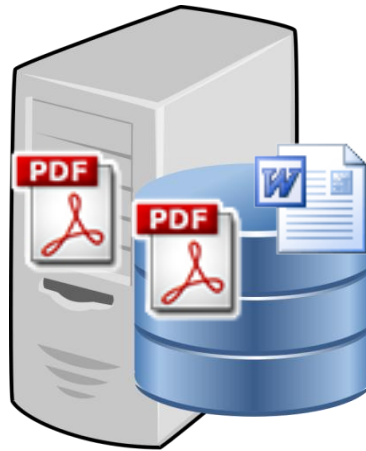


Server
bij Smals



Tablet CEO



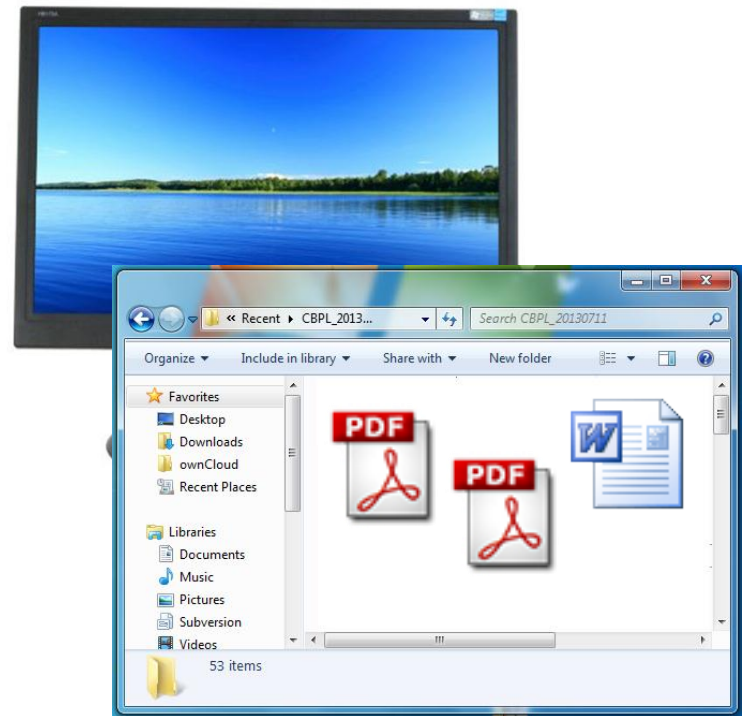


Server
bij Smals



Tablet CEO

CEO heeft **offline**
toegang tot de
bestanden op zijn
tablet





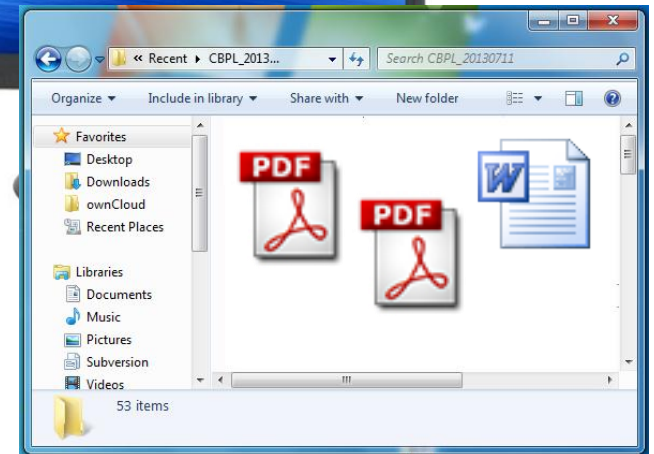
Server
bij Smals



Tablet CEO

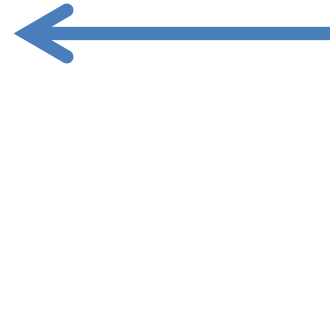


Secretariaat
verwijdert
documenten





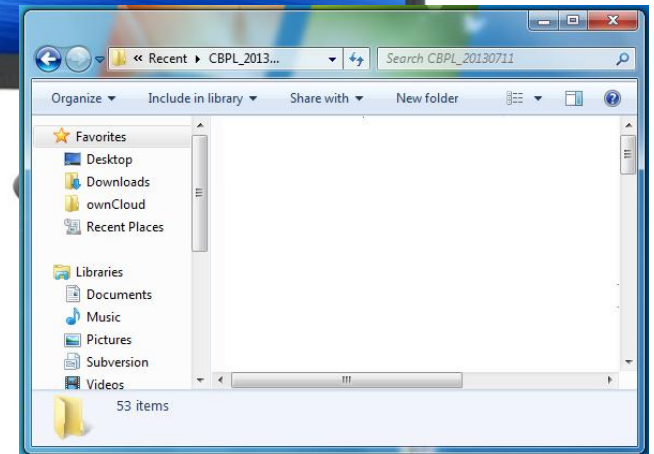
Server
bij Smals



Synchronisatie
Bestanden worden
automatisch verwijderd
op server bij Smals

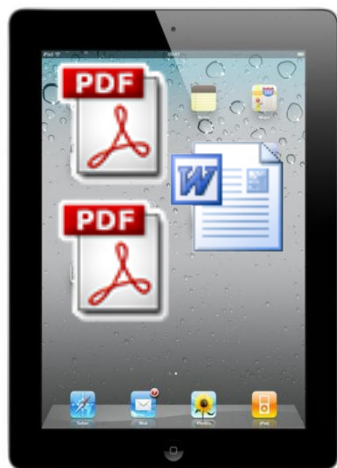


Tablet CEO



Synchronisatie

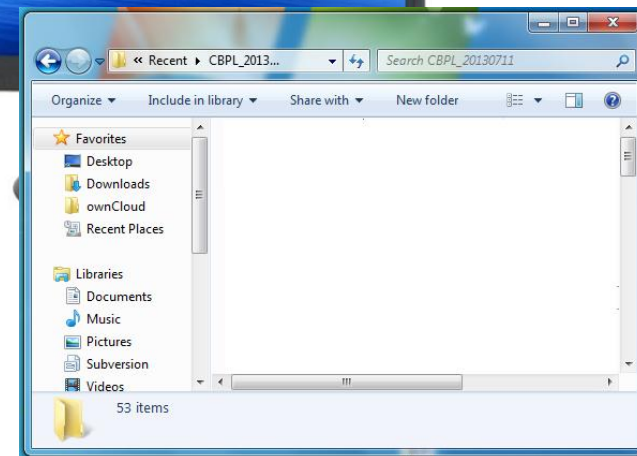
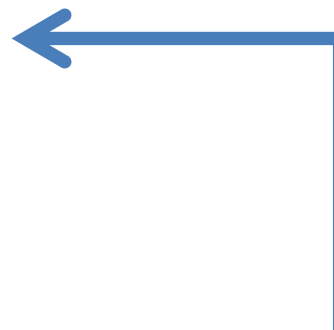
Bestanden
worden
verwijderd op
tablet CEO



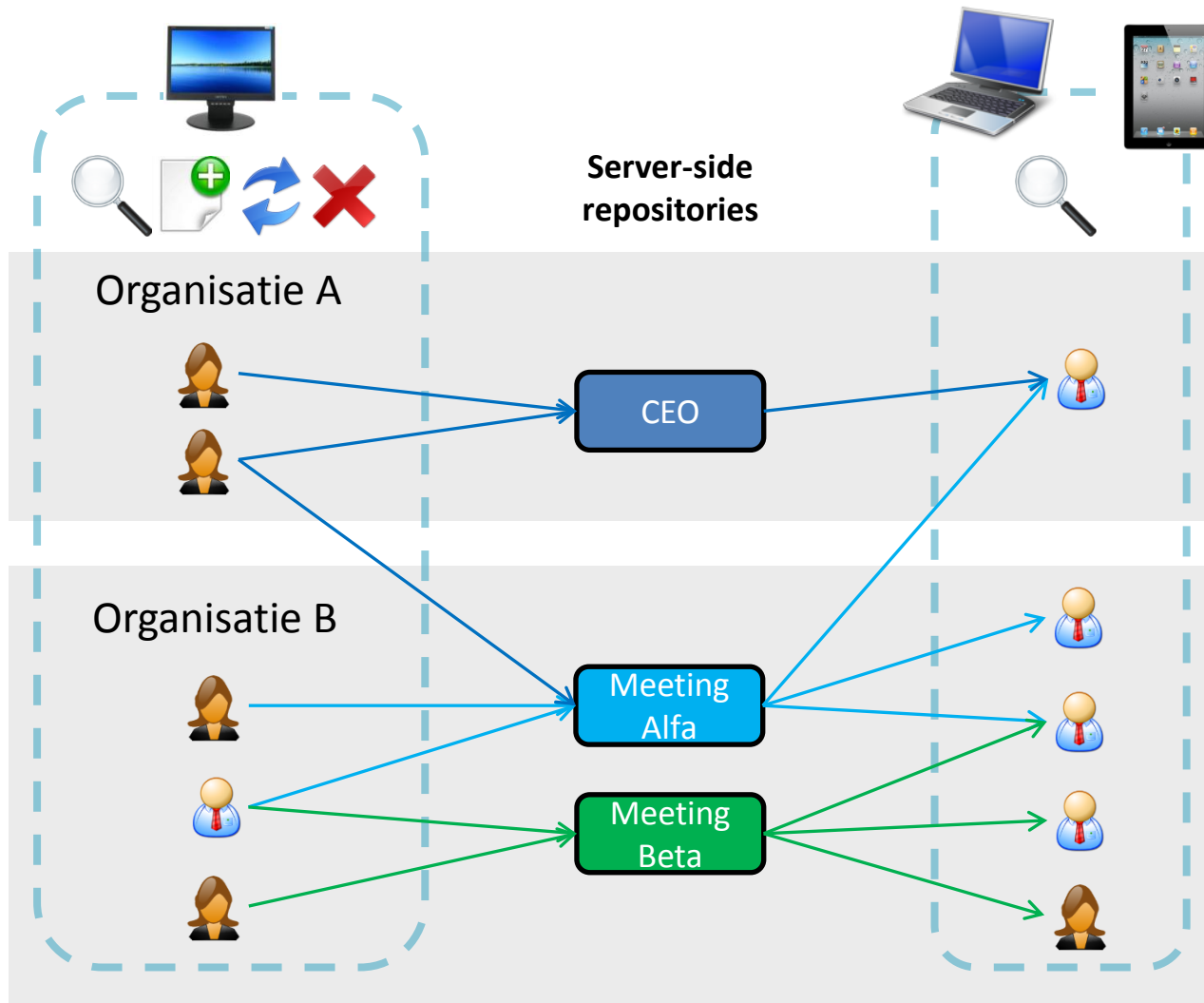
Tablet CEO



Server
bij Smals



Gegeneraliseerd Scenario



FSS Scenario's

Beheren & delen documenten meetings

Foto's en verslagen op verplaatsing (vb. werven) direct delen met team voor analyse

Alternatief voor uitwisselen van zware docs via e-Mail

Directeur synchroniseert zijn verschillende toestellen

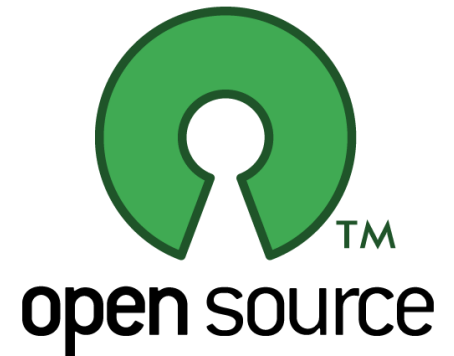
Met welk product te realiseren?



We testten...



Heeft goede referenties





The origins of the **cernbox** project

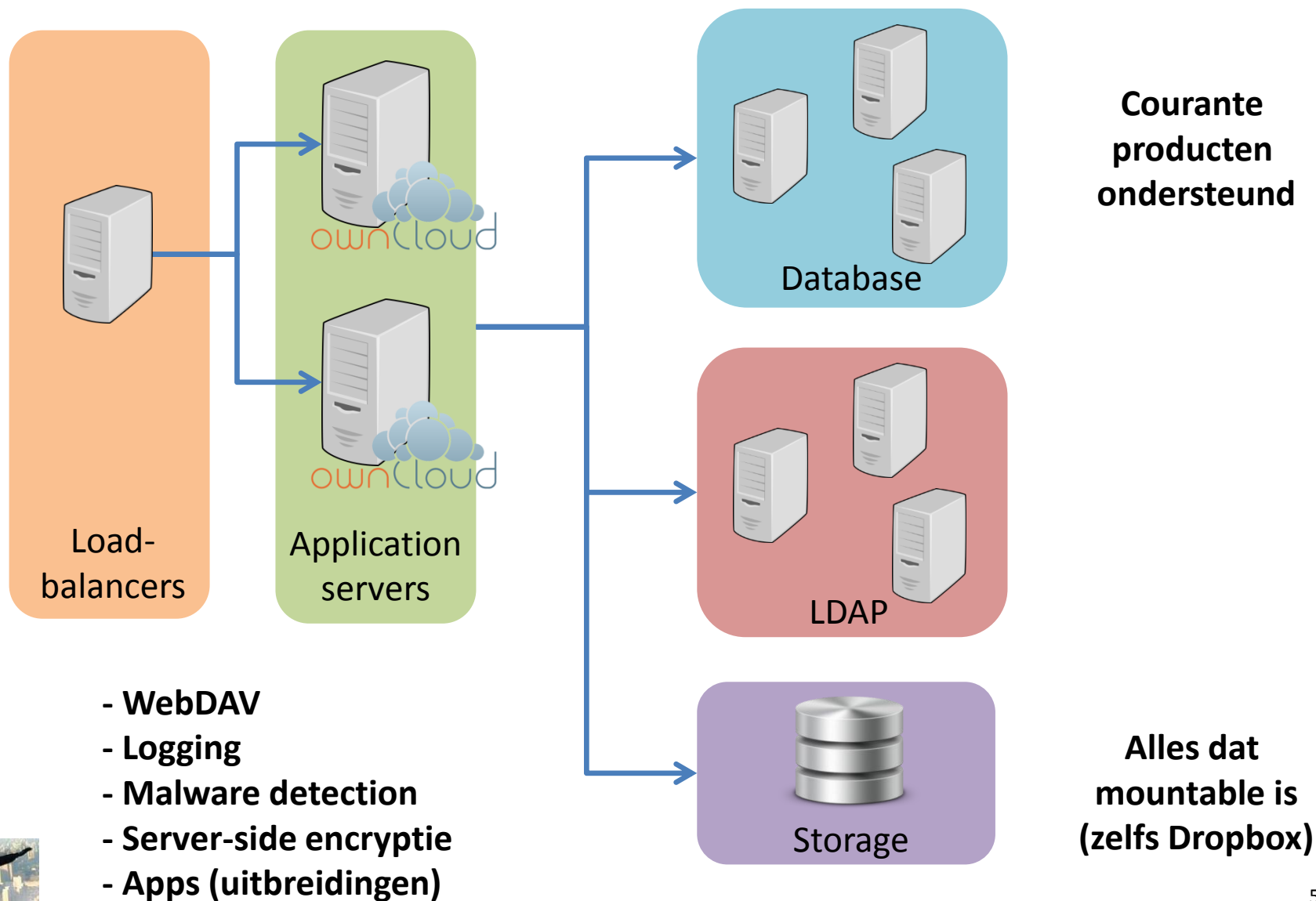
- We need a competitive alternative to Dropbox for CERN users
 - Reasons
 - SLAs: availability, confidentiality
 - integration into IT infrastructure
 - archival & backup policies
 - The scale of the problem is unknown but we have some indications
 - 4500 distinct IPs in DNS from cern.ch to *.dropbox.com (daily...)
 - We also want to adapt to user expectations
 - We manage large-scale online-storage systems
 - ...and we can leverage on them



EOS (RAW)	CEPH (RAW)	Other services
~62 PB	~3.5 PB	~30 PB

Bulk of disk storage operated by IT/DSS

Architectuur



APPS

All

Multimedia

PIM

Productivity

Games

Tools

other

Search

FORUM

global

apps Disabled

user support

Priority

roundcube 1.1.16

How to enable the other
folders

artwork

developer

xism support

Still available?

Speedbar for owncloud

more

Latest

Alphabetical

Highest rated

Most downloaded

**roundcube 1.3.1**

ownCloud Productivity

275 Comments 52 Fans 2 Questions

 Score 87 %
Downloads: 15868

More

**Storage Charts v2.2**

ownCloud Tool

73 Comments 18 Fans 2 Questions

 Score 64 %
Downloads: 14657

More

**Shorty 0.3.30**

ownCloud Productivity

105 Comments 18 Fans 6 Questions

 Score 84 %
Downloads: 12217

More

**Files move 0.6.0**

ownCloud Tool

89 Comments 30 Fans 4 Questions

 Score 81 %
Downloads: 12029

More

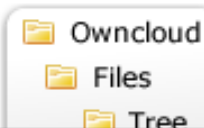
**Video Streamer**

ownCloud Multimedia

44 Comments 9 Fans 2 Questions

 Score 56 %
Downloads: 10787

More

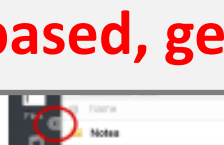
**Files Tree 0.7.0**

ownCloud Tool

120 Comments 30 Fans 1 Question

 Score 84 %
Downloads: 10513

More

**Notes (Y) 0.2.6**

ownCloud Tool

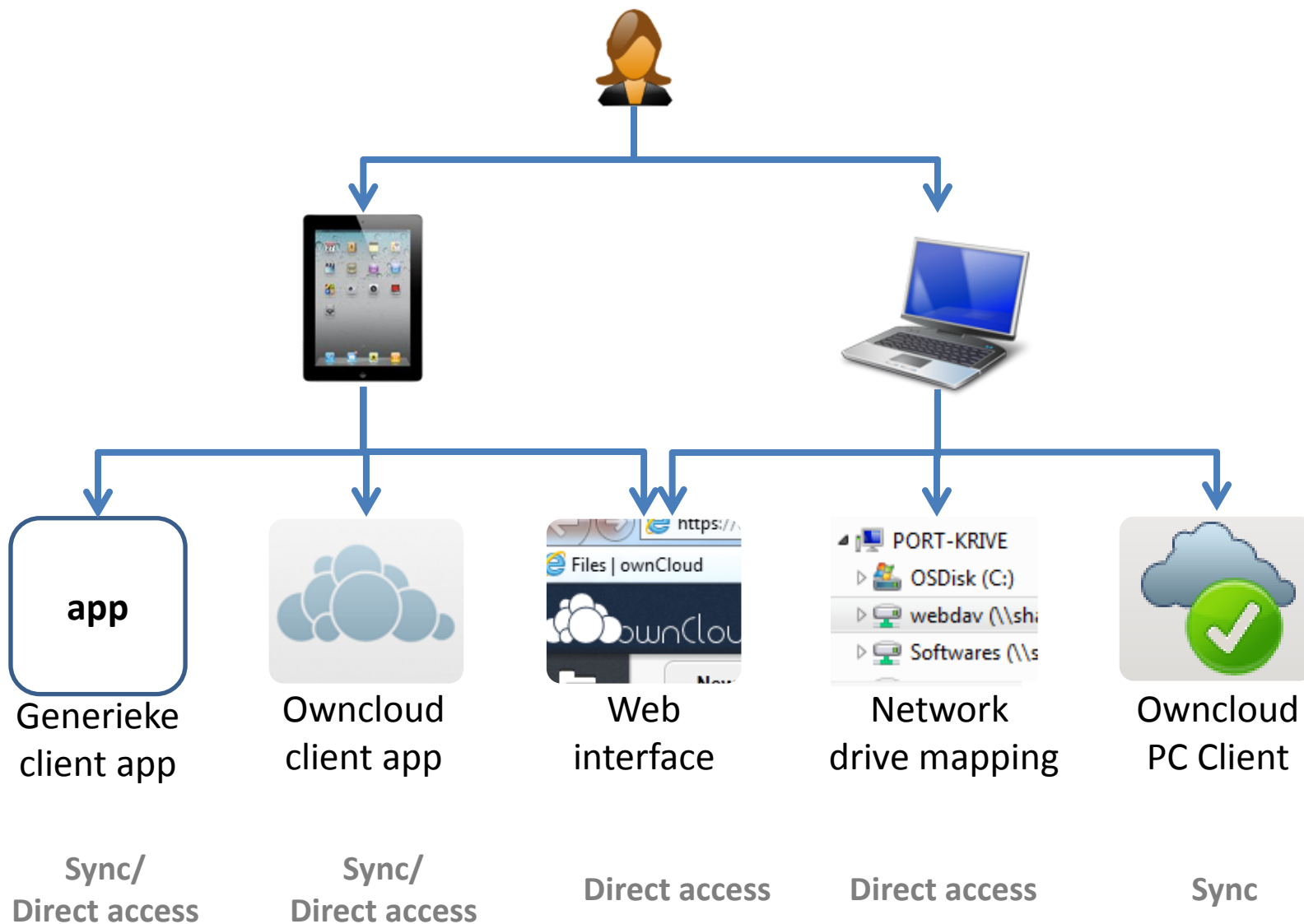
31 Comments 11 Fans 2 Questions

 Score 75 %
Downloads: 8848

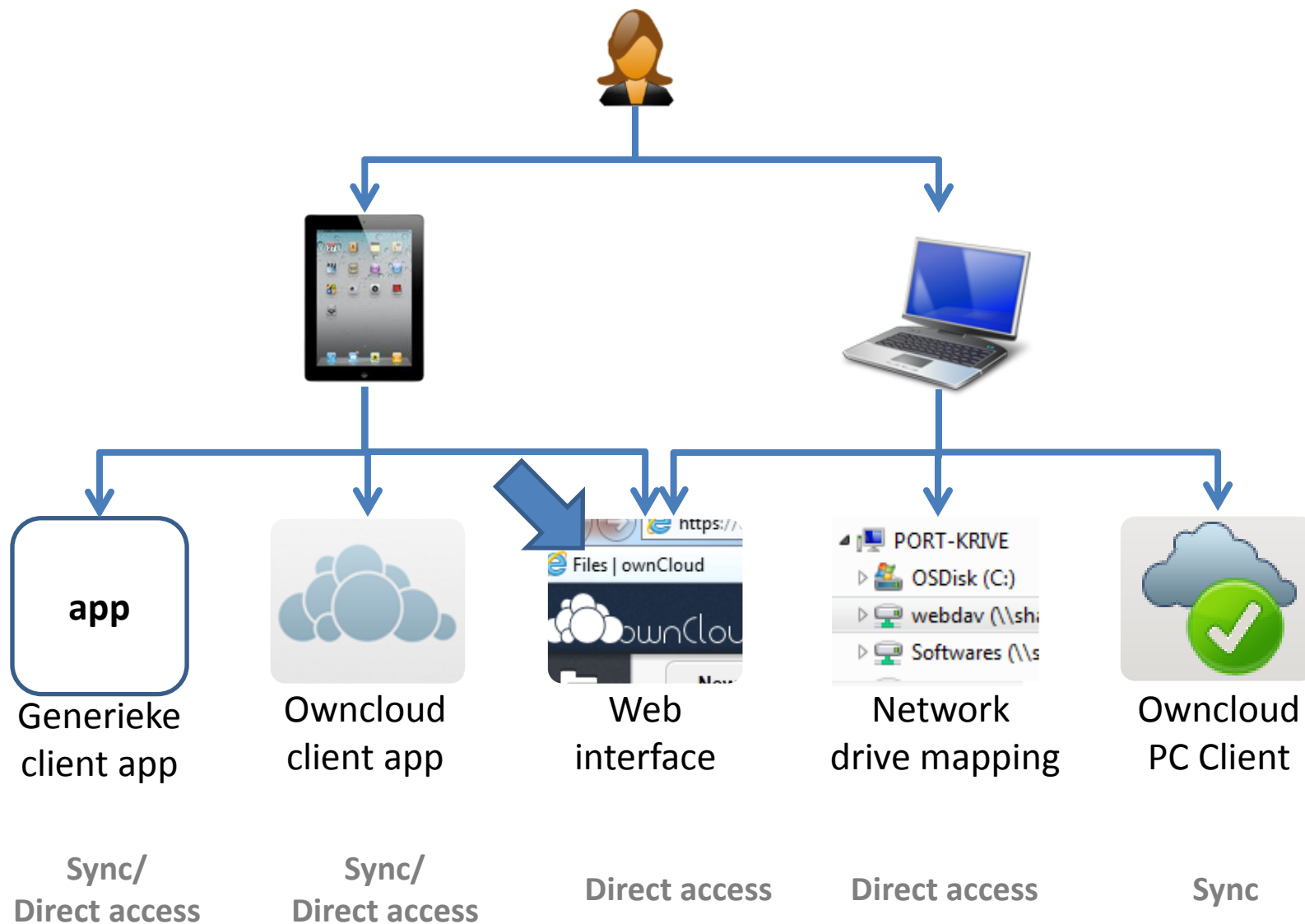
More

**Thomas Manager v1.0****Community-based, geen SLA's!**

De gebruiker



De gebruiker



Files - ownCloud

test.gov4u.be/index.php/apps/files

ownCloud 6.0.2 is available. Get more information on how to update.

 ownCloud



 krive



New

Deleted files

Files

Activity

Documents

Pictures

Apps

	Name		Size	Modified
	Confidentieel	 Shared	112.9 kB	25 days ago
	Documenten		6 MB	4 days ago
	Foto's		91.4 MB	12 days ago
	Shared		662.7 kB	yesterday
	kakkerlak.jpg		385.2 kB	last month
	MI_WP_DocsW		181.2 kB	25 days ago
	presentaties.zip		6.5 kB	25 days ago

Alles dat aan mij gedeeld is

Files - ownCloud

test.gov4u.be/index.php/apps/files

ownCloud 6.0.2 is available. Get more information on how to update.

krive

Files

Activity

Documents

Pictures

Apps

New

Name

Confidentieel

Shared 112.9 kB 25 days ago

Share with user or group ...

kova ☒ notify by email ☒ can edit ☐ create ☒ update ☒ delete ☒ share

☐ Share link

☒ Set expiration date

30-04-2014

MI_WP_DocsWork_0.pdf

presentaties.zip

6 MB 4 days ago

91.4 MB 12 days ago

662.7 kB yesterday

385.2 kB last month

181.2 kB 25 days ago

6.5 kB 25 days ago

Kova zal mijn map /Confidentieel zien in zijn /Shared/Confidentieel



Files



Activity



Documents



Pictures



Apps

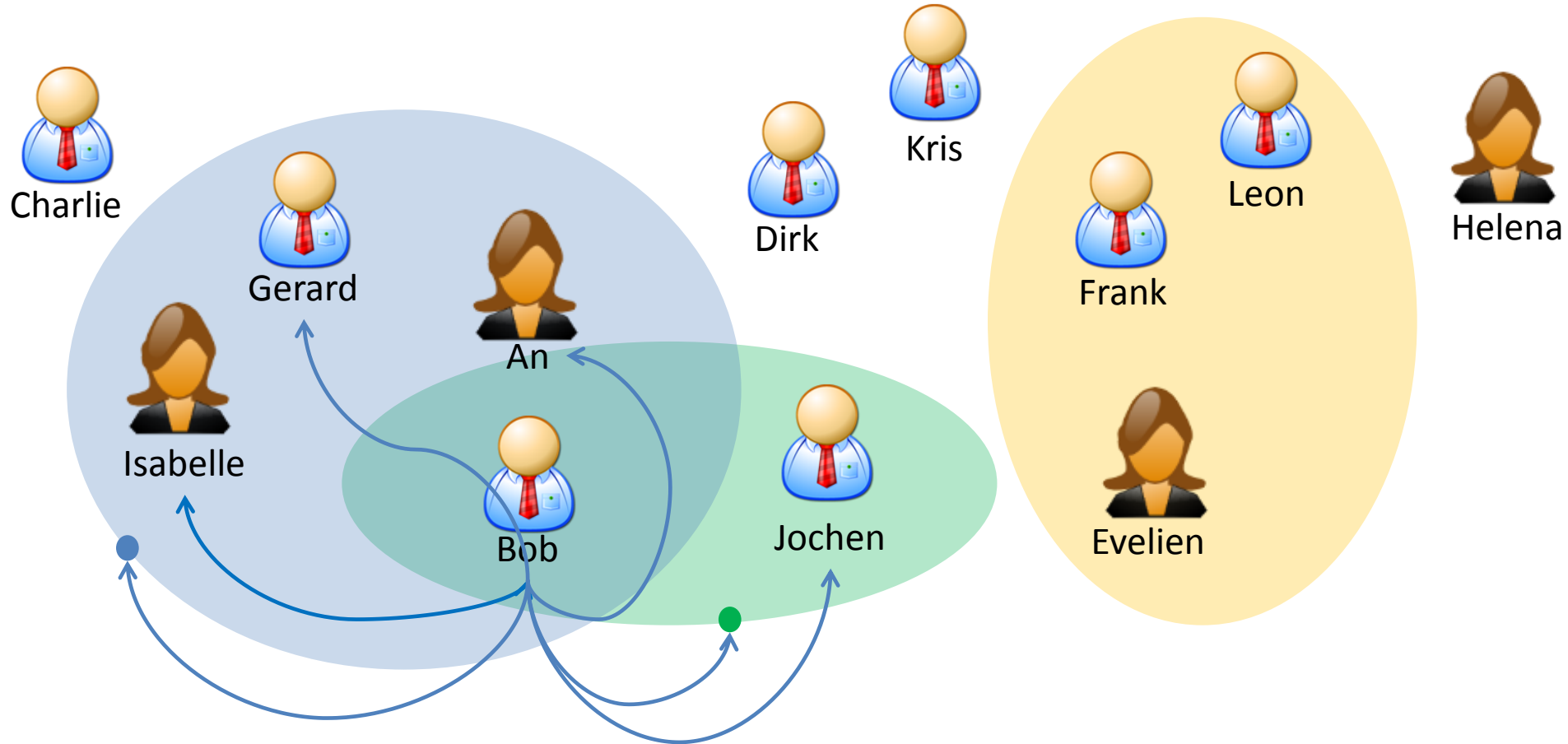
Sharing

☒ Enable Share API*Allow apps to use the Share API*☒ Allow links*Allow users to share items to the public with links*☒ Allow public uploads*Allow users to enable others to upload into their publicly shared folders*☒ Allow resharing*Allow users to share items shared with them again*

- ☒ Allow users to share with anyone
- ☐ Allow users to only share with users in their groups

☒ Allow mail notification*Allow user to send mail notification for shared files*

« Only share in your groups »



→ « Kan delen met »



Files



Calendar



Contacts



Pictures

New



Deleted files

 Name	Size	Modified
 demo	0	11 days ago
 Documenten	0.2	11 days ago
 MobileIron	13.6	11 days ago
 Recent	0	11 days ago
 Shared	16.4	14 days ago
 transit	0	11 days ago
 Infosessie cloud - deel 1.pptx	24.8	7 days ago
 Infosessie cloud  Rename  Move  Download  Versions  Share	18.4	1 minute ago

All versions...



Files



Calendar



Contacts



Pictures

New



Deleted files

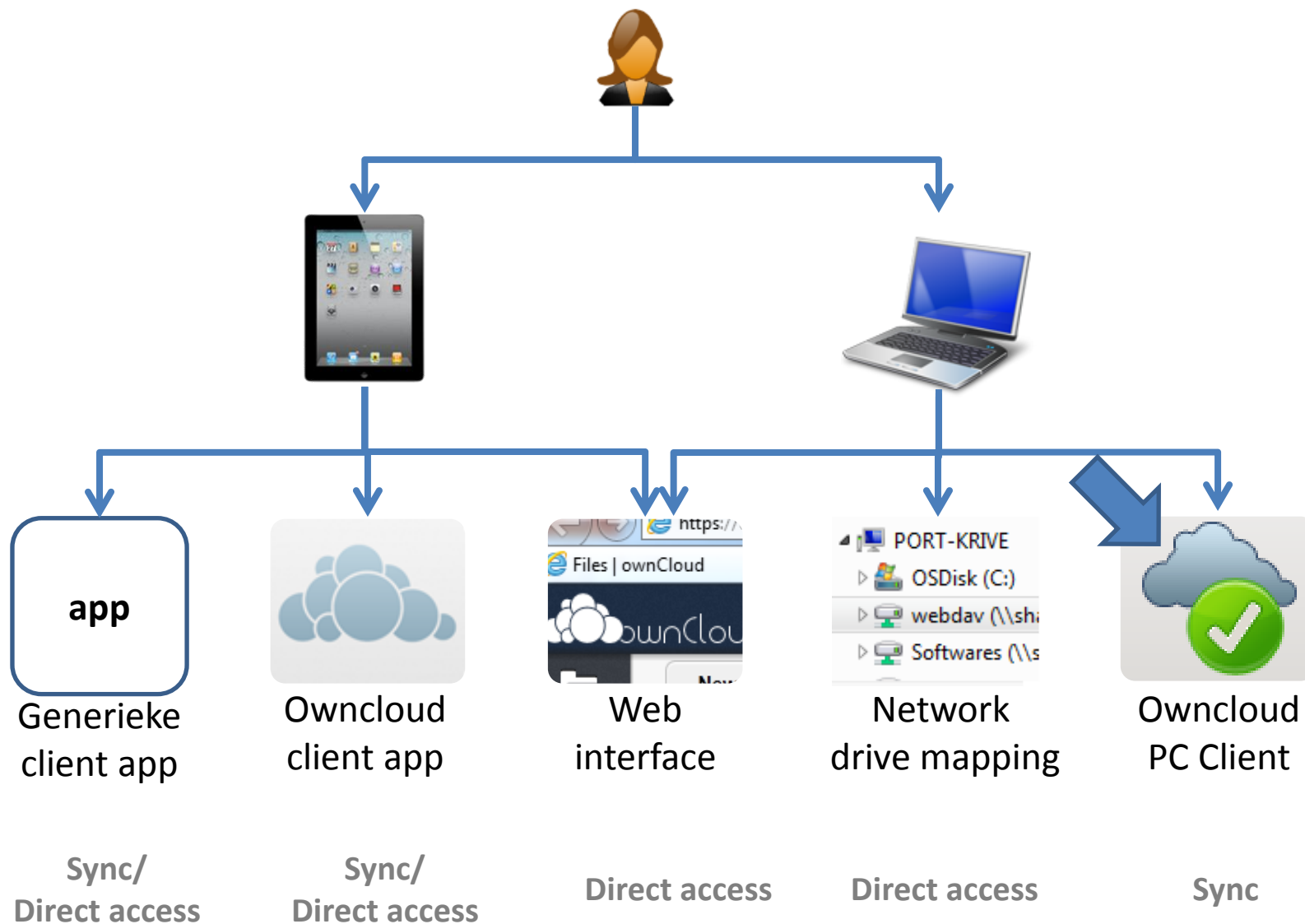
 Name	Size	Modified
 demo	0	11 days ago
 Documenten	0.2	11 days ago
 MobileIron	13.6	11 days ago
 Recent	0	11 days ago
 Shared	16.4	14 days ago
 transit	0	11 days ago
 Infosessie cloud - deel 1.pptx	24.8	7 days ago
 Infosessie cloud   Move  Download  Versions  Share	18.5	seconds ago

January 17, 2014 13:23

January 17, 2014 13:18

January 17, 2014 13:13

De gebruiker



ownCloud

Account

Activity

General

Network

Account to Synchronize

Connected to <https://share.qov4u.be> as *krive*.

Mijn Documenten
Remote path: Documenten
C:\Users\krive\oc-docs

Shared
Remote path: Shared
C:\Users\krive\oc-shared

15 MB of 69 MB, file 12 of 52

Currently downloading fotosfeest/WP_20140131_001.jpg (2 MB of 2 MB)

Add Folder...

Pause

Remove

Storage Usage

111 MB of 558 MB (20%) in use.

Note: Some folders, including network mounted or shared folders, might have different limits.

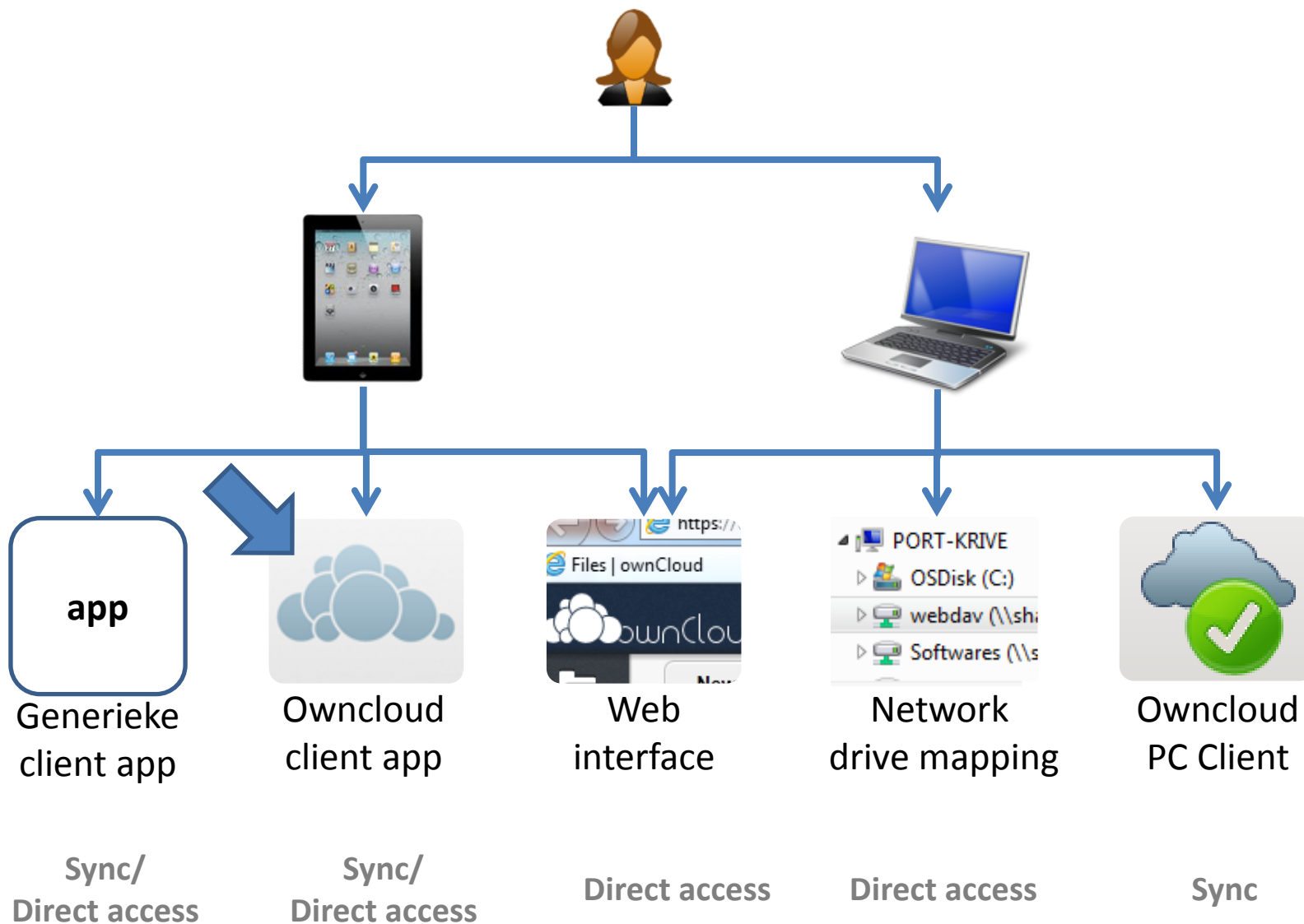
Account Maintenance

Edit Ignored Files

Modify Account

Close

De gebruiker





- Confidentieel
- Documenten
- Foto's
- Infosessie cloud - deel 1.pdf
- kakkerlak.jpg
- MI_WP_DocsWork_0.pdf
- presentaties.zip
- Shared



DOCTRINE

*Cloud computing et protection des données à caractère personnel : mise en ménage possible ?*¹

Jean-Marc Van Gyseghem^{2,3}

Le cloud computing soulève bon nombre de questions qui, si elles ne sont pas nouvelles, exacerbent certaines problématiques déjà existantes. Le cloud computing impose donc des réflexions qui constituent un challenge pour les juristes.

La présente contribution s'attache plus particulièrement à des aspects propres au domaine de la protection des données à caractère personnel. À défaut de pouvoir les aborder tous, nous avons limité notre propos aux questions de détermination des responsables de traitement et sous-traitants ainsi qu'aux principes d'information, de confidentialité et de sécurité.

L'angle pris est celui par rapport à une P.M.E. ou à un indépendant utilisant le cloud computing dans le cadre de ses activités professionnelles/commerciales.



Cloud computing is not a new concept from the point of view of technology but raises several issues which were already existing. It builds a new challenge for the lawyers.

This paper explores issues related to data protection. Unfortunately, we cannot go through all of them and we have to select them. Therefore, we'll give an approach to the determination of data controller and data processor as well as the concepts of information, confidentiality and security.

We tackle these issues thru the prism of SME and self-employed person using the cloud computing in its commercial or professional activities

Gebruiksvriendelijkheid



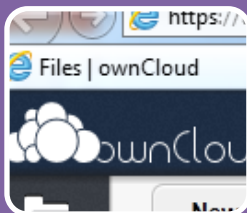
Server

- Eenvoudige basisinstallatie
- Flexibel
- Apps (uitbreidingen) niet steeds matuur



PC client

- Wizard
- Flexibler & complexer dan Dropbox



Web interface

- Spartaans
- Bevat wel alle functionaliteit
- Gebruik recente browser



App (iOS, Android)

- Minimale functionaliteit
- Intuïtief



Ervaringen

Matuur

- Evolueert snel

Sommige functionaliteit enkel in web client

- Uitgebreide functionaliteit om te delen
- Prullenmand
- Vorige versies

Technisch

- Standaard MySQL tot 2500 actieve gebruikers
- VPN & Reverse proxies ok





Demo



Demo - Scenario

0.  +  Rechten op map « Raad van Bestuur »
Geen rechten op map « Directiecomité »
1.  geeft rechten aan  + 
2.  voegt documenten toe aan map « Directiecomité »
3.  consulteert documenten
4.  verwijdert documenten
5.  ziet documenten niet meer



Admin

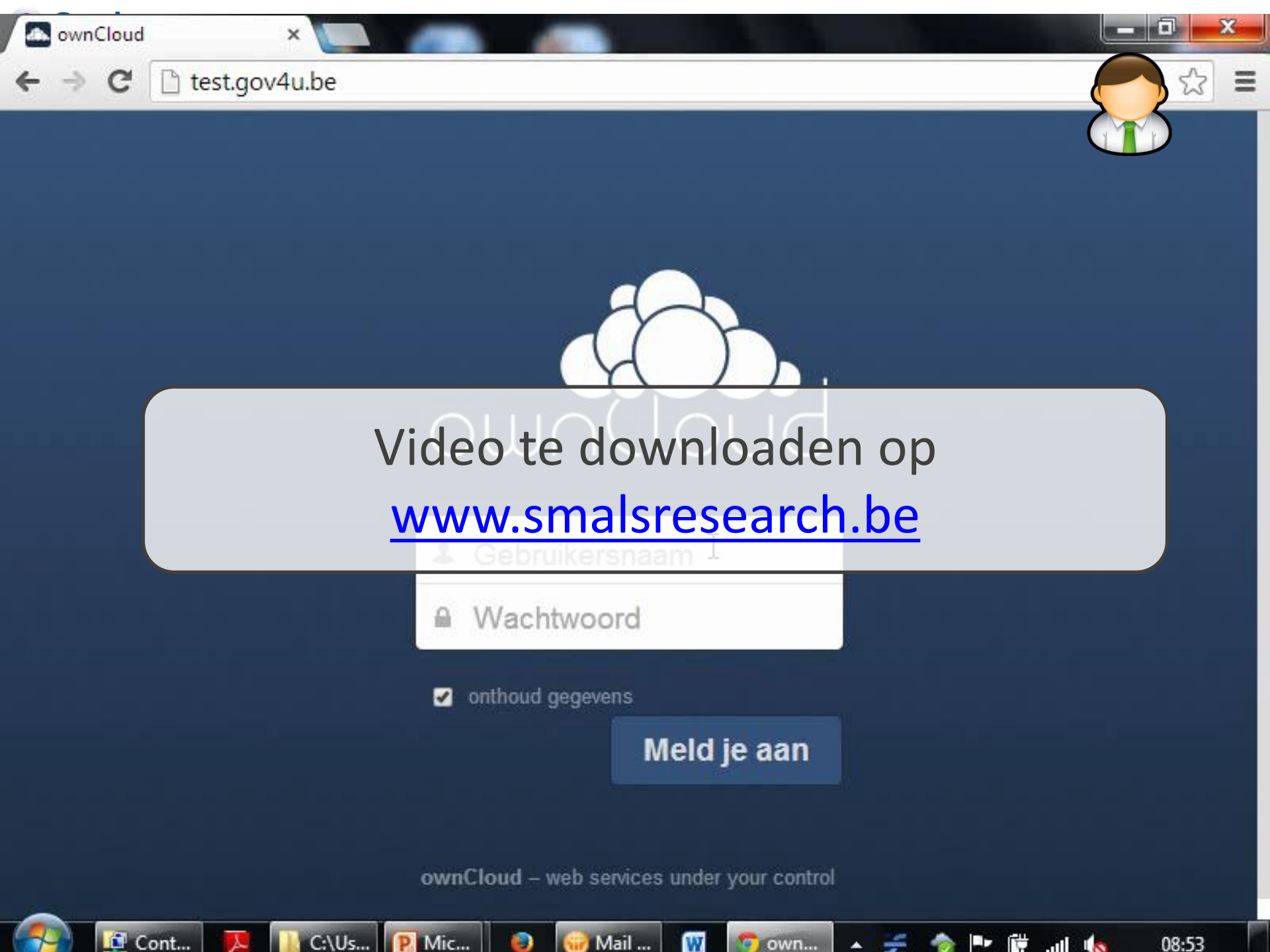


CEO



Secr.





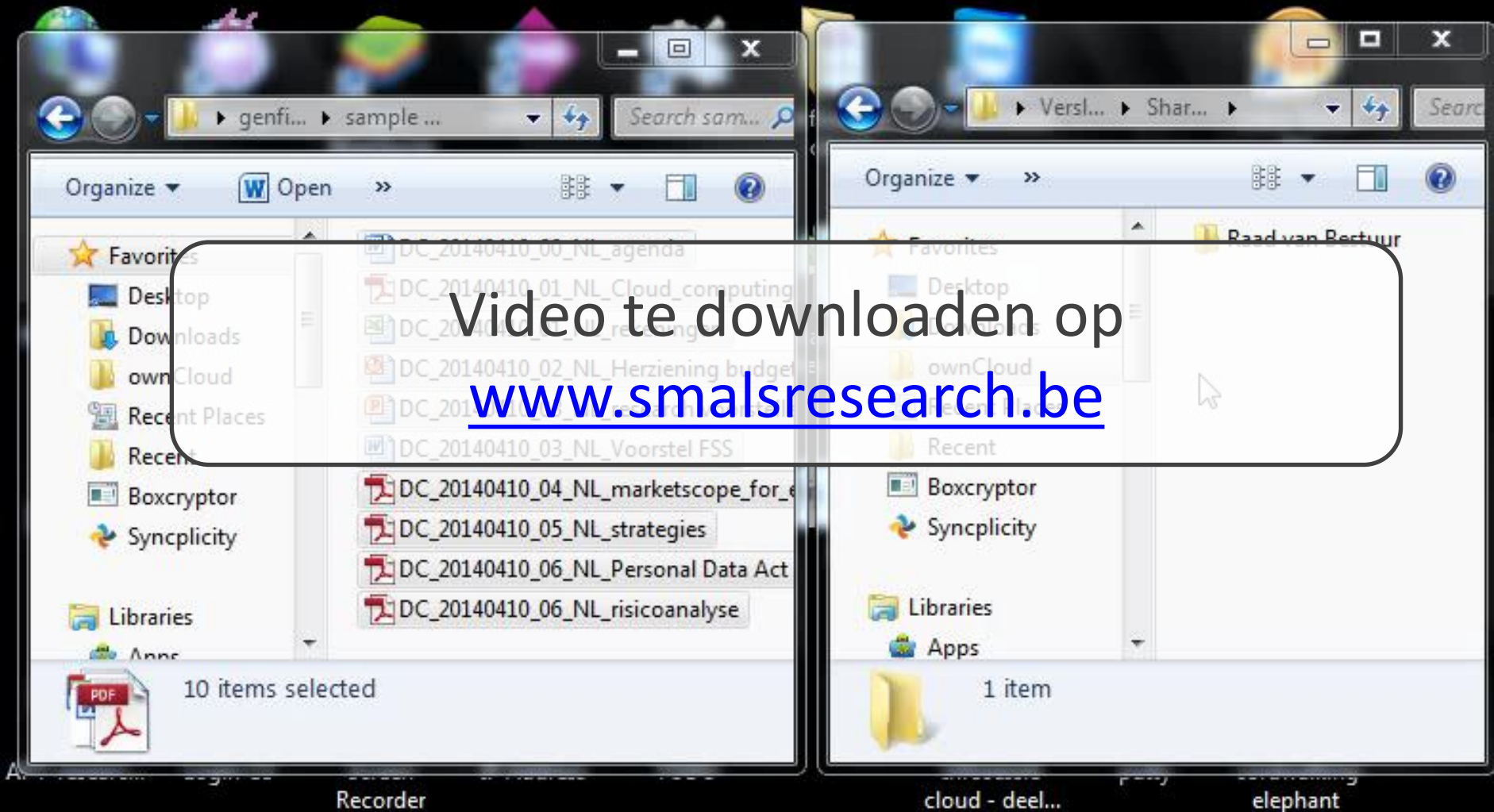
Video te downloaden op
www.smalsresearch.be

Gebruikersnaam

Wachtwoord

☒ onthoud gegevens

Meld je aan





ALL PLAYED APPS



Adobe Reader



App Sync



Appstore



Facebook



FolderSync



Help



Instellingen



Hulp



Instellingen



Twitter

Video te downloaden op
www.smalsresearch.be

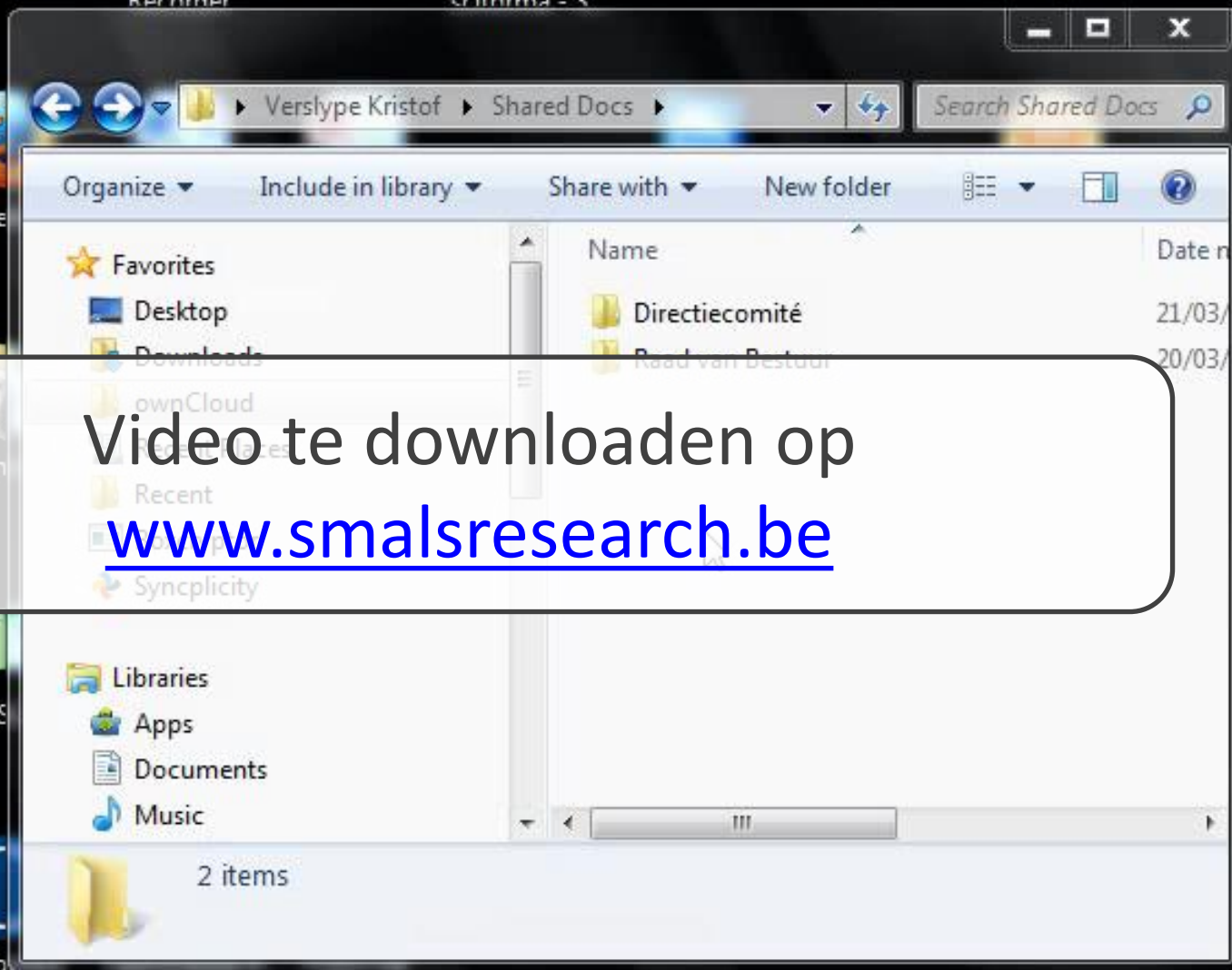
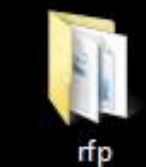
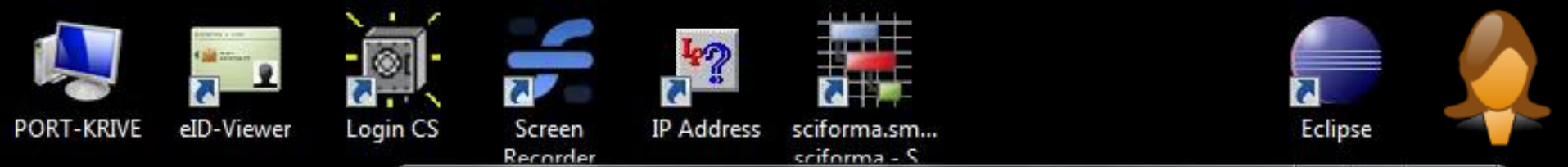


ownCloud

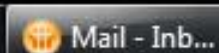


10:00





Video te downloaden op
www.smalsresearch.be





ALL PLAYED APPS



Adobe Reader



App Sync



Appstore



Facebook



FolderSync



Help



Instellingen

Video te downloaden op
www.smalsresearch.be



WhatsApp



Twitter



ownCloud



09:47



Conclusie

Degelijke private cloud FSS oplossingen

- Ook open source
- Uitgebreid getest
- Evaluatie positief

Vergelijking

- Veiliger dan huidige wildgroei
- Misschien niet even veilig als wereldspelers
- Evenmin dezelfde schaal/specialisatie -> kost
- Toegang door buitenlands overheden moeilijker



File Sync & Share Apps



Wat? › Public cloud › Private Cloud › Apps › End-Point › Nieuwe Dienst 6

We bekijken...

- 1) **Client apps** voor toegang bestanden op server
- 2) **Viewers apps** om documenten te bekijken



Client app gebruikt standaard
geïntegreerde viewer



Client app gebruikt
viewer apps

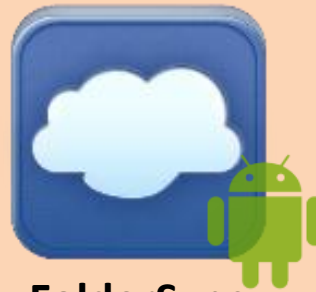


Client apps

Client Apps

We bekeken reeds

Generische client



FolderSync



GoodReader

Owncloud client



Owncloud

Nu volgt kort

My Documents



 **Downloads** (0)
(no backing up to iTunes or iCloud)

 **Shared** (4)
aujourd'hui 10:30



Browse the Web



Enter URL

Downloads

Show All

Clear All

Remote Sync

 **Shared** (68,7 MB)
WebDAV: Goovbox krive
aujourd'hui 10:31



Connect to Servers

Add

Edit

Known Servers:



Goovbox krive



Servers Found via WiFi:

reload list of local servers



My Documents

-  **Downloads** (0)
(no backing up to iTunes or iCloud)
-  **Shared** (4)
aujourd'hui 10:30

Goovbox krive

Close

Folders:

-  **demo**
6 janv. 2014 16:37
-  **Documenten**
17 mars 2014 08:22
-  **MobileIron**
17 janv. 2014 16:09
-  **Recent**
6 janv. 2014 08:51
-  **Shared**
11 févr. 2014 17:35
-  **transit**
hier 10:08

Files:

-  **20130730_Cloud_computing_NL_tcm325-...**
20 août 2013 11:58 2,7 MB
-  **Current usage owncloud.pptx**
hier 10:06 178 KB
-  **Infosessie cloud - deel 1.pptx**
10 janv. 2014 16:53 24,7 MB

Deselect All -05-13-14 Sync -56- PNC Download



Browse the Web



Enter URL

Downloads

Show All

Clear All

Remote Sync

 **Shared** (68,7 MB)
WebDAV: Goovbox krive
aujourd'hui 10:32



Connect to Servers

Add

Edit

Known Servers:



Goovbox krive



Servers Found via WiFi:

reload list of local servers



My Documents

 **Downloads** (0)
(no backing up to iTunes or iCloud)

 **Documenten** (1)
aujourd'hui 10:32

 **Shared** (4)
aujourd'hui 10:30



Browse the Web



Enter URL

Downloads

Show All

Clear All

Remote Sync

 **Documenten** (10 MB)

WebDAV: Goovbox krive
aujourd'hui 10:32



Connect to Servers

Add

Edit

Known Servers:



Goovbox krive



Servers Found via WiFi:

reload list of local servers



My Documents

 **Downloads** (0)
(no backing up to iTunes or iCloud)

 **Documenten** (0)
aujourd'hui 10:32

 **Shared** (4)
aujourd'hui 10:30



syncing Documenten

464 KB done 9,6 MB to go
downloading file: ehealth_cloud_strat.pptx

Cancel



Browse the Web



Enter URL

Downloads

Show All

Clear All

Remote Sync

 **Documenten** (10 MB)

WebDAV: Goovbox krive
aujourd'hui 10:32



Connect to Servers

Add

Edit

Known Servers:



Goovbox krive



Servers Found via WiFi:

reload list of local servers



Client Apps Vergeleken

		OS	Sync	Direct access	Cache	Share	Convi vialité	Flexi bilité	File name length	Viewers	€
Dropbox 2.3			No	Yes	Yes	link	+++	-		Extern	Free
Owncloud 1.5			Selected files	Yes	Yes	No	+++	-	-	Extern	0,79
Owncloud 3.1.1			No	Yes	Yes	link	+++	-	-	Intern / (extern)	0 79
FolderSync 2.5			Yes	No	nvt	No	+	++	+++	extern	2,29
GoodReader 3.19			Yes	Downlo ad only	nvt	No	++	+++	++	Intern / (extern)	4,49
Documents 4.4			Yes	Yes	nvt	No	++	+	+++	Intern	Free
Docs@Work 5.8			Downloa ded files	Yes	No	No	+++	-	-	Intern	10€ /UY



Clients: Custom - Generiek

			Generic client
Config.	+++	++	+
Accounts (gelijktijdig)	 Dropbox	   	    
Delen (met link)		   	



Kies in functie van je voorkeuren & vereisten

- **Directe toegang Vs. synchronisatie**
- **Meerdere accounts Vs. 1 account**

Viewer apps

Enkele Viewer Apps



Microsoft Office



AstralPad



Kingsoft Office



GoodReader



Documents



Smart Office 2



ANDROID



ThinkFree



Kingsoft Office



OfficeSuite



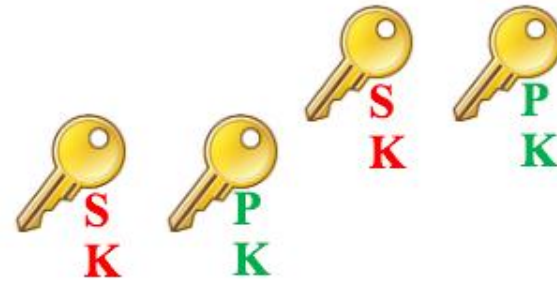
Windows 8



Microsoft Office



Kingsoft Office



Uploaden bestand
Per file unieke AES
sleutel



Bo



Johan

Aandachtspunten

Weergavekwaliteit

Annotatie PDFs

Weergavesnelheid

Editeren Documenten

Vb.



- Quasi perfecte weergave
- Documenten laden traag
- Editeren enkel indien een Office 365 abo

>> Gebruik bij voorkeur PDF <<



Conclusie

*Diverse
Client apps & viewer apps
mogelijk*



Fijn, maar daarmee is onze tablet nog niet veilig...

File Sync & Share End-Point Security



Wat? › Public cloud › Private Cloud › Apps › End-Point › Nieuwe Dienst

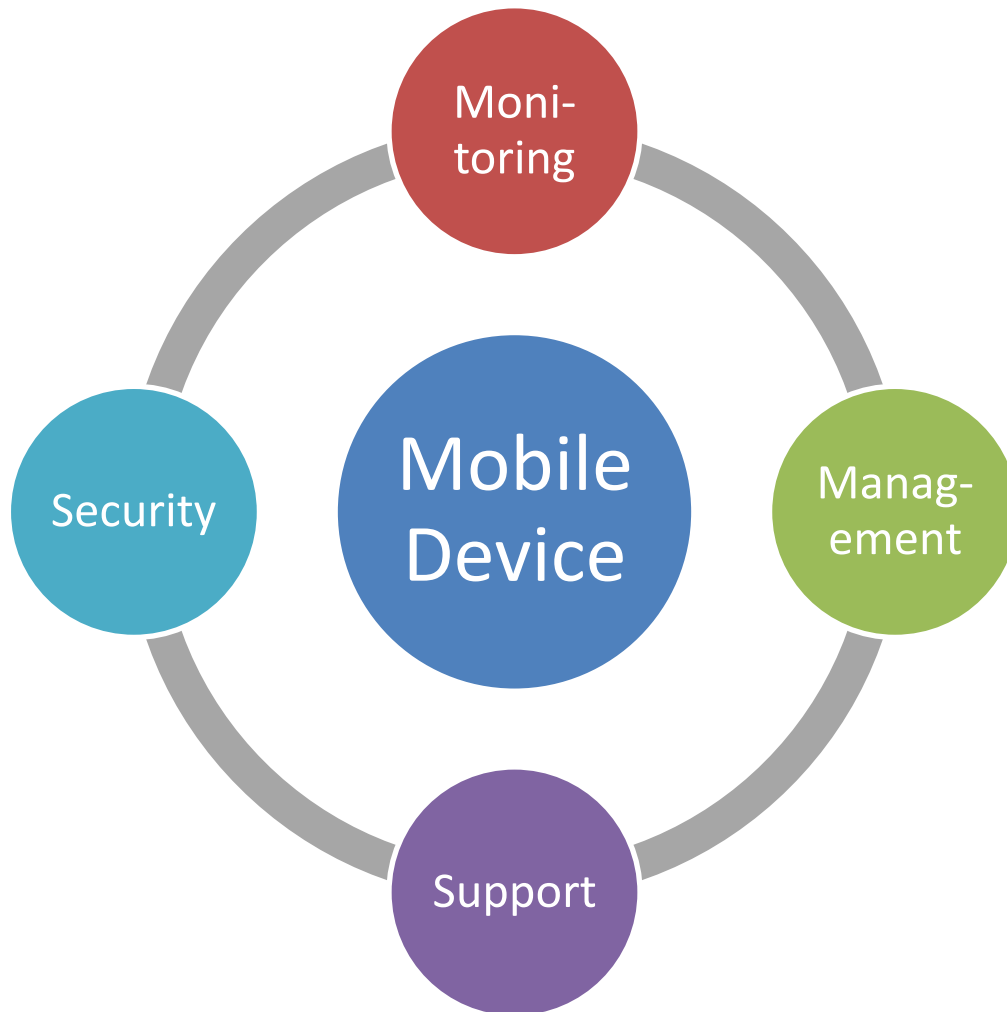
Probleemstelling



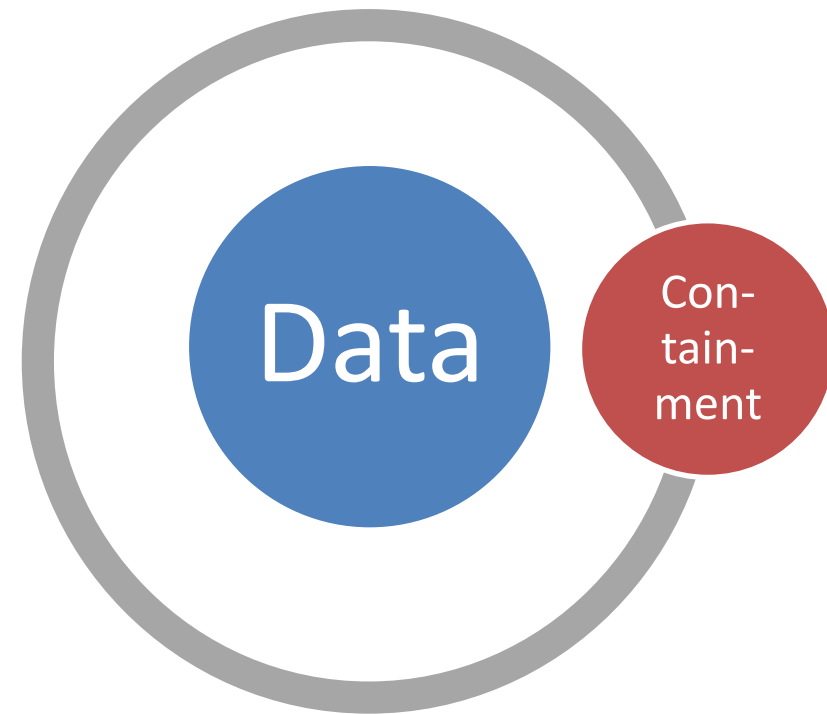
Toegenomen risico compromitteren gevoelige data
Gebrek aan controle door bedrijf problematisch



Mobile Device Management (MDM)



Containerization



Mobile Device Management (MDM)



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...		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

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

All Smartphones					
Lock Wipe More Actions ▾		Labels: All-Smartphones ▾		Search by Us	
☐	User ▴	Number	Phone	OS	Country
☒	User01	470803381	 Nexus S by samsung	Android 2.3	Belgium
☐	User01	+32470188821	 if	App Control Security Policy Violated 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

▼ 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

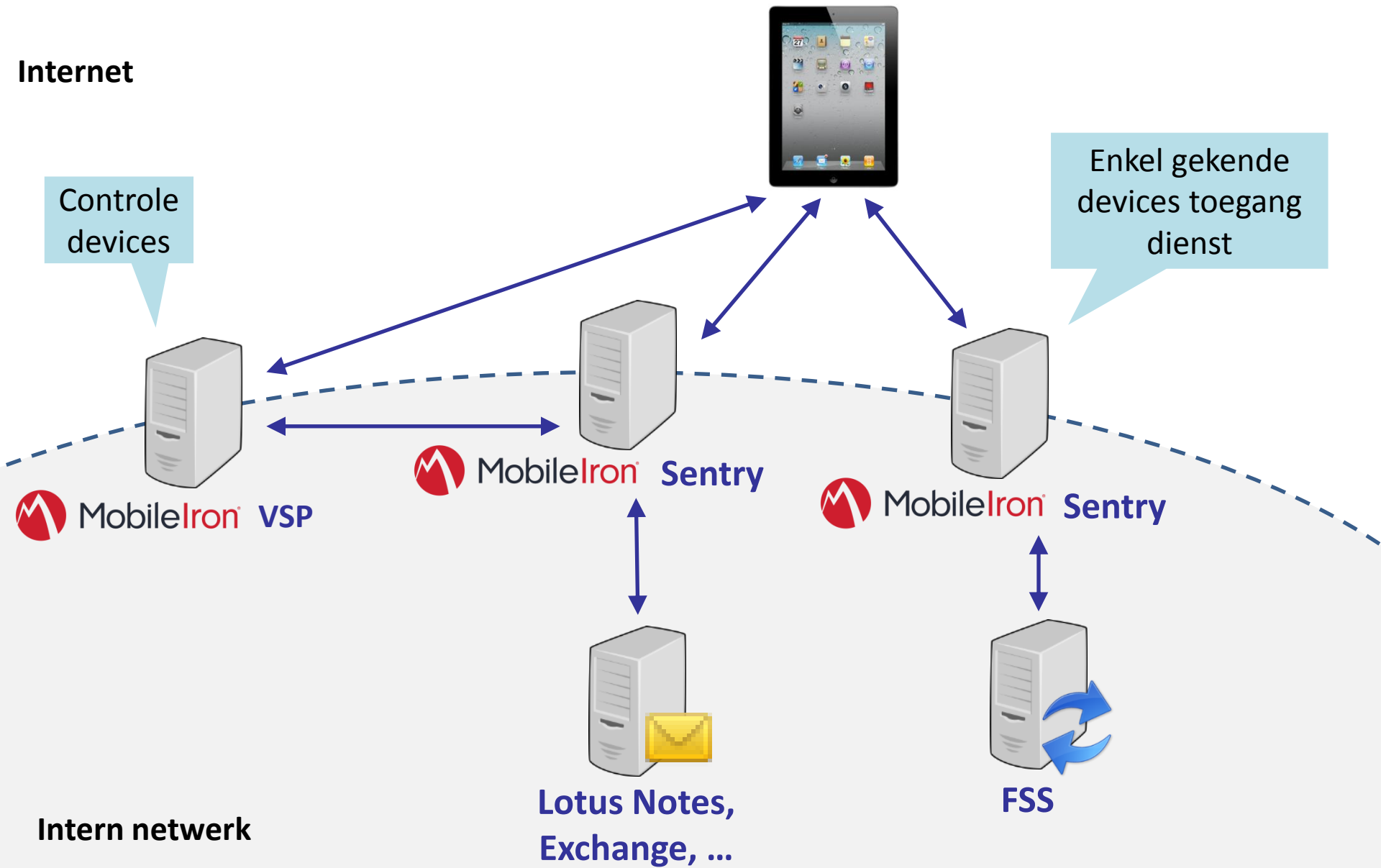
Maps 5.10.0

Market 2.3.6



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

Architectuur



Containerization

Gegevens verlaten afgeschermdde omgeving op mobiel toestel niet

- Niet: openen met andere apps
- Niet: uploaden naar cloud dienst
- Niet: versturen per mail
- Geen knippen-plakken
- ...



MobileIron Containerization uitbreidingen

Docs@Work

Web@Work

Apps@Work





20130730_Clou...325-228881.pdf

2.7 MB, modified 20 août 2013 11:58



Current usage owncloud.pptx

178 KB, modified hier 10:06



DC_20140410_...puting_final.pdf

362 KB, modified aujourd'hui 11:36



demo

1 item



Documenten

4 items



Infosessie cloud - deel 1.pptx

24.8 MB, modified 10 janv. 2014 16:53



MobileIron

3 items



Photo-05-03-14-10-56-56-0.PNG

54 KB, modified 5 mars 2014 11:15



Photo-05-03-14-10-59-28-0.PNG

272 KB, modified 5 mars 2014 10:59



Photo-11-03-14-10-30-52-0.PNG

283 KB, modified 11 mars 2014 10:30



Photo-11-03-14-10-37-00-0.PNG

284 KB, modified 11 mars 2014 10:37



Photo-11-03-14-13-12-55-0.PNG

545 KB, modified 11 mars 2014 13:12



Photo-11-03-14-14-20-55-0.PNG

343 KB, modified 11 mars 2014 14:20



Home



Local Files



File Shares



Settings

DOCTRINE

Cloud computing et protection des données à caractère personnel : mise en ménage possible ? ¹

Jean-Marc Van Gyseghem^{2,3}

Le cloud computing soulève bon nombre de questions qui, si elles ne sont pas nouvelles, exacerbent certaines problématiques déjà existantes. Le cloud computing impose donc des réflexions qui constituent un challenge pour les juristes.

La présente contribution s'attache plus particulièrement à des aspects propres au domaine de la protection des données à caractère personnel. À défaut de pouvoir les aborder tous, nous avons limité notre propos aux questions de détermination des responsables de traitement et sous-traitants ainsi qu'aux principes d'information, de confidentialité et de sécurité.

L'angle pris est celui par rapport à une P.M.E. ou à un indépendant utilisant le cloud computing dans le cadre de ses activités professionnelles/commerciales.



Cloud computing is not a new concept from the point of view of technology but raises several issues which were already existing. It builds a new challenge for the lawyers.

This paper explores issues related to data protection. Unfortunately, we cannot go through all of them and we have to select them. Therefore, we'll give an approach to the determination of data controller and data processor as well as the concepts of information, confidentiality and security.

We tackle these issues thru the prism of SME and self-employed person using the cloud computing in



File Sync & Share + Containerization

Document-oriented

Integreert met Outlook, Sharepoint, ...

Monitor document access

- Next slide

WatchDox Cloud of WatchDox Virtual Appliance

<http://www2.watchdox.com/>



 Workspaces > 2012 Q2 Board Meeting

☐ Sort  Upload  New folder  Download  Send  Delete  More

☐		Agenda for Board Meeting Q2 2012.docx	06 Nov 2013 12:34 tim@watchdox.com 18.3KB ★	
☐		Board of Directors Presentation_Q2_2012(tim@watchdox.com reco...	07 Nov 2013 09:18 tim@watchdox.com 81.3KB ★	
☒		Board of Directors Presentation_Q2_2012.pptx	07 Nov 2013 09:12 tim@watchdox.com 80.3KB ★	 
☐		Company Overview Q2 2012.pdf	01 Aug 2012 21:48 tim@watchdox.com 673.8KB ★	 
☐		Financial Report for Company Q2 2012.docx	01 Aug 2012 21:48 tim@watchdox.com 30.8KB ★	
☐		Profit_and_Loss_Q2_2012.xls	01 Aug 2012 21:48 tim@watchdox.com 63.0KB ★	 
☐		watchdox.pdf	01 Nov 2012 13:09 tim@watchdox.com 303.9KB ★	

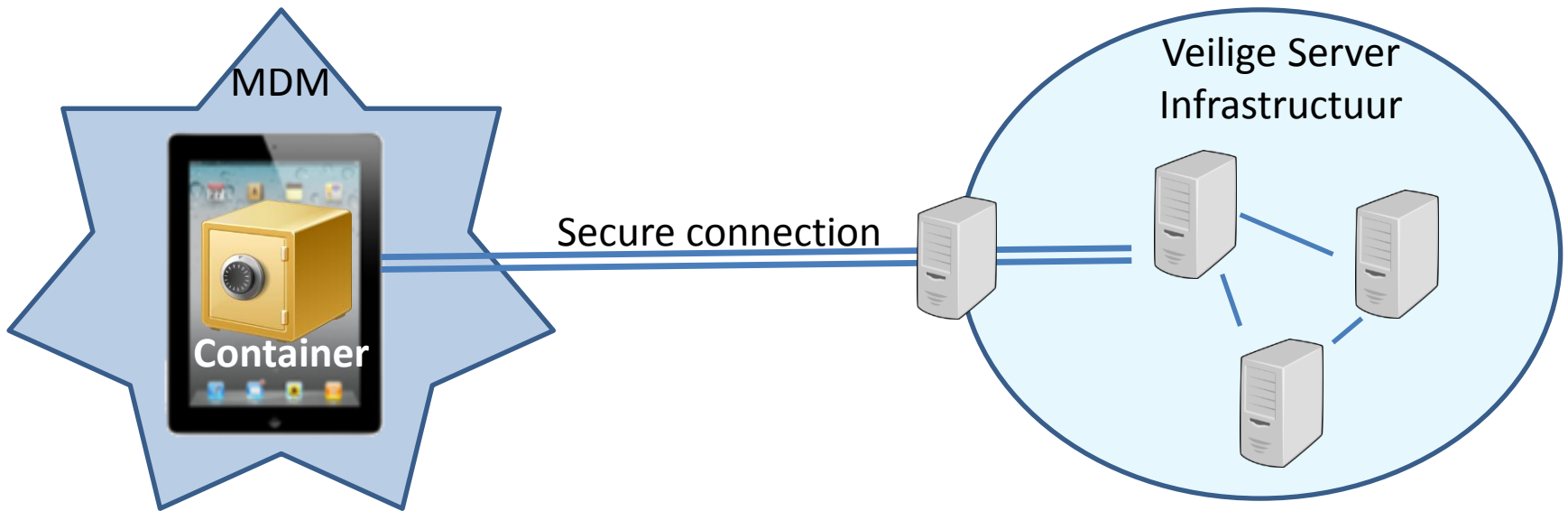
« We gebruiken AES-256 »

≠

« Alles is in elke situatie veilig »

⇒ Volledig ecosysteem nodig!

Een ecosysteem



(Alternatieve oplossing laat alle internetverkeer via bedrijfsgateway passeren)

File Sync & Share

Nieuwe Dienst



Wat? › Public cloud › Private Cloud › Apps › End-Point › Nieuwe Dienst

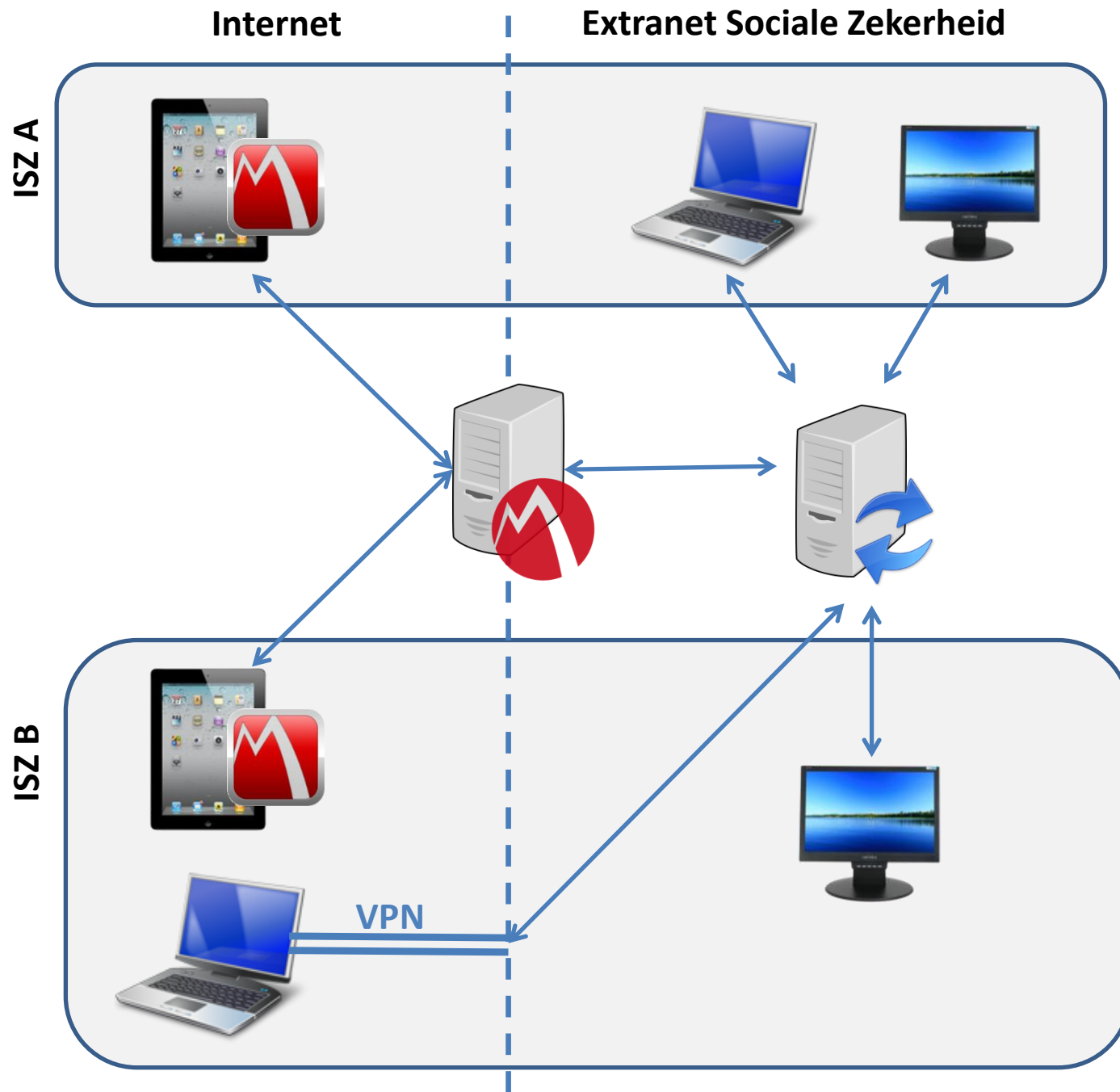
Security Toestellen SZ

	Werkstation (=PC of Draagbare PC)	Werkstation + VPN	Privé mobiel toestel (=Tablet/smartphone)
Netwerk	Extranet	Extranet	Internet
Beheer	ISZ	ISZ	?
Authenticatie	1) Bios pwd 2) Windows pwd (+policy)	1) Bios pwd 2) Windows pwd (+policy) 3) eID (met PIN)	?
P(verlies)	Laag	Medium	Hoog

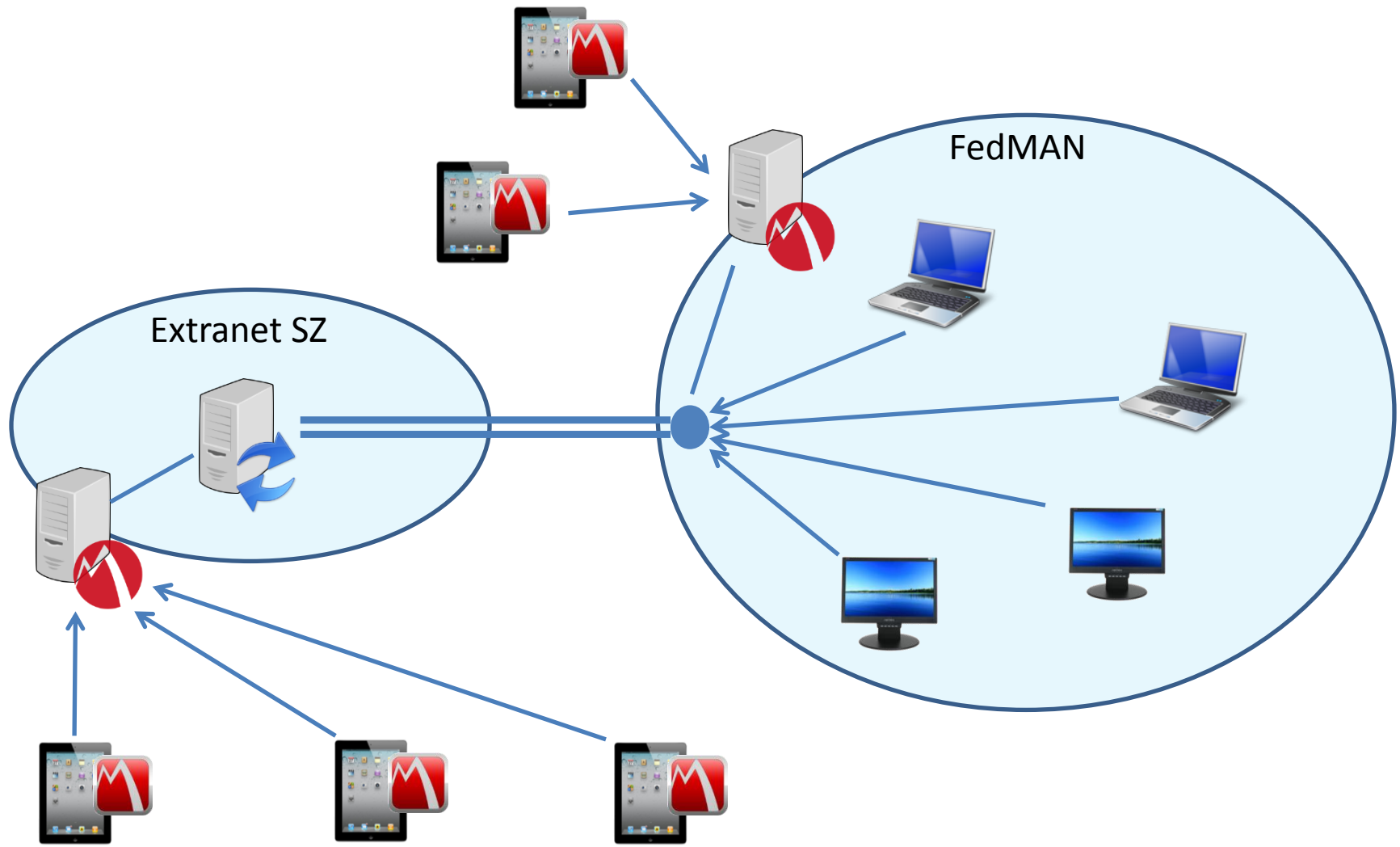
Sterkere security nodig voor mobile devices

Policy Mobiele Toestellen SZ

	Voorbeeld	Mobiel toestel zonder gecentraliseerd beheer	Mobiel toestel met gecentraliseerd beheer	Mobiel toestel met gescheiden omgevingen (Isolatie / VDI)
Publieke gegevens	Site KSZ			
Interne bedrijfsgegevens	Interne strategie, agenda, contacten, mail	Te bepalen		
Vertrouwelijke bedrijfsgegevens	Boekhoudplan, DRP		Te bepalen	
Persoonsgegevens	Persoonlijk dossier HR		Te bepalen	
Sociale persoonsgegevens	gegevens RR			
Medische gegevens	Medische gegevens			

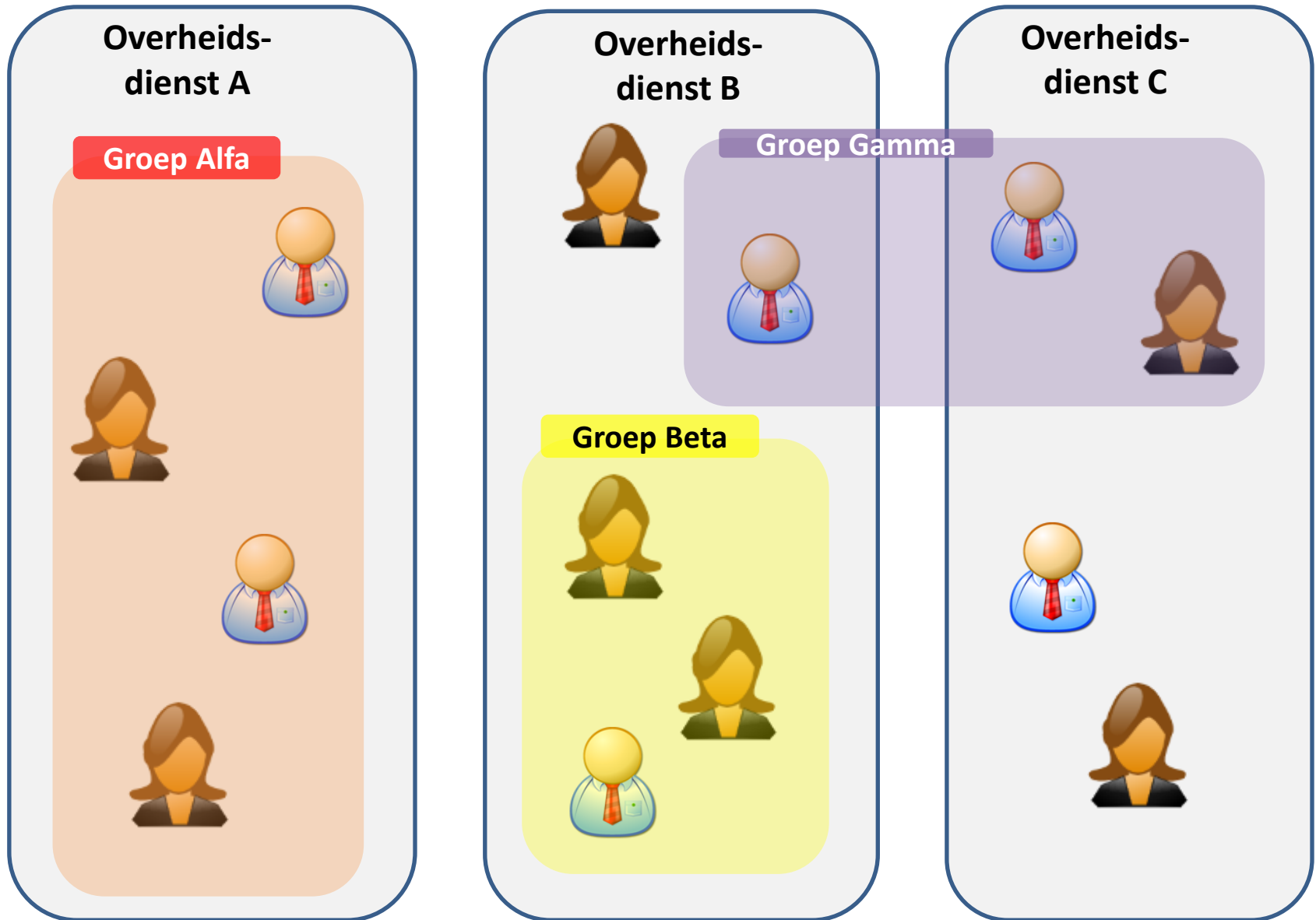


Beyond Social Security



=> Volwaardige dienst voor alle federale overheidsdiensten

Delen binnnen en tussen instellingen



Conclusie

In progress. Smals werkt aan uitbouw veilige FSS dienst om *vertrouwelijke gegevens* te delen binnen en tussen overheidsinstellingen

Next step. Containerization binnen SZ voor verwerking *persoonsgebonden gegevens* op tablet

Vraag. Kan de FSS dienst aangeboden worden buiten extranet SZ en FedMAN?



Afronding



Conclusies

CSB kan security verhogen bij gebruik cloud diensten

Buitenlandse overheden houden gevoelige data intern

FSS: public cloud Vs. private cloud

Ecosysteem (infr, connectie, end-point, data)

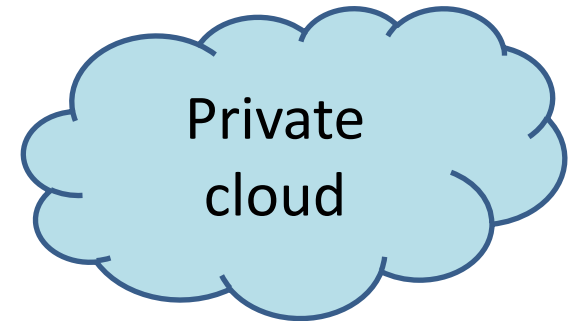
Smals werkt aan FSS dienst



Herwin de controle!



Cloud-anarchie



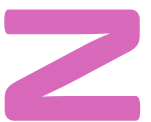
CSB

De public cloud...

Is niet transparant

Verandert constant ongevraagd

Kan oplossen & verdwijnen



Een eigen cloud is...

Minder veilig dan de groten?

Geïnfiltreerd door overheden?

Duurder? Goedkoper?

V
R
A
G
E
N

Meer samenwerking → Meer schaalvoordelen!

Cryptografie evolueert



En sommige data moet erg lang beschermd blijven...

- ⇒ **Vandaag OK $\neq$ morgen OK (rekenkracht, veronderstellingen)**
- ⇒ **Door jou verwijderd $\neq$ effectief verwijderd**
- ⇒ **Applicatie heeft vaak de data in clear-text nodig**

Sociale Zekerheid
Veiligheidspolicy's voor o.a.

Mobiele toestellen
Cloud computing services

=> Must read! <=

Risicoanalyse

Wat is de aard en gevoeligheid van de gegevens?

Is afhankelijkheid van het buitenland tolereerbaar

Wat is de impact bij compromitteren van de data

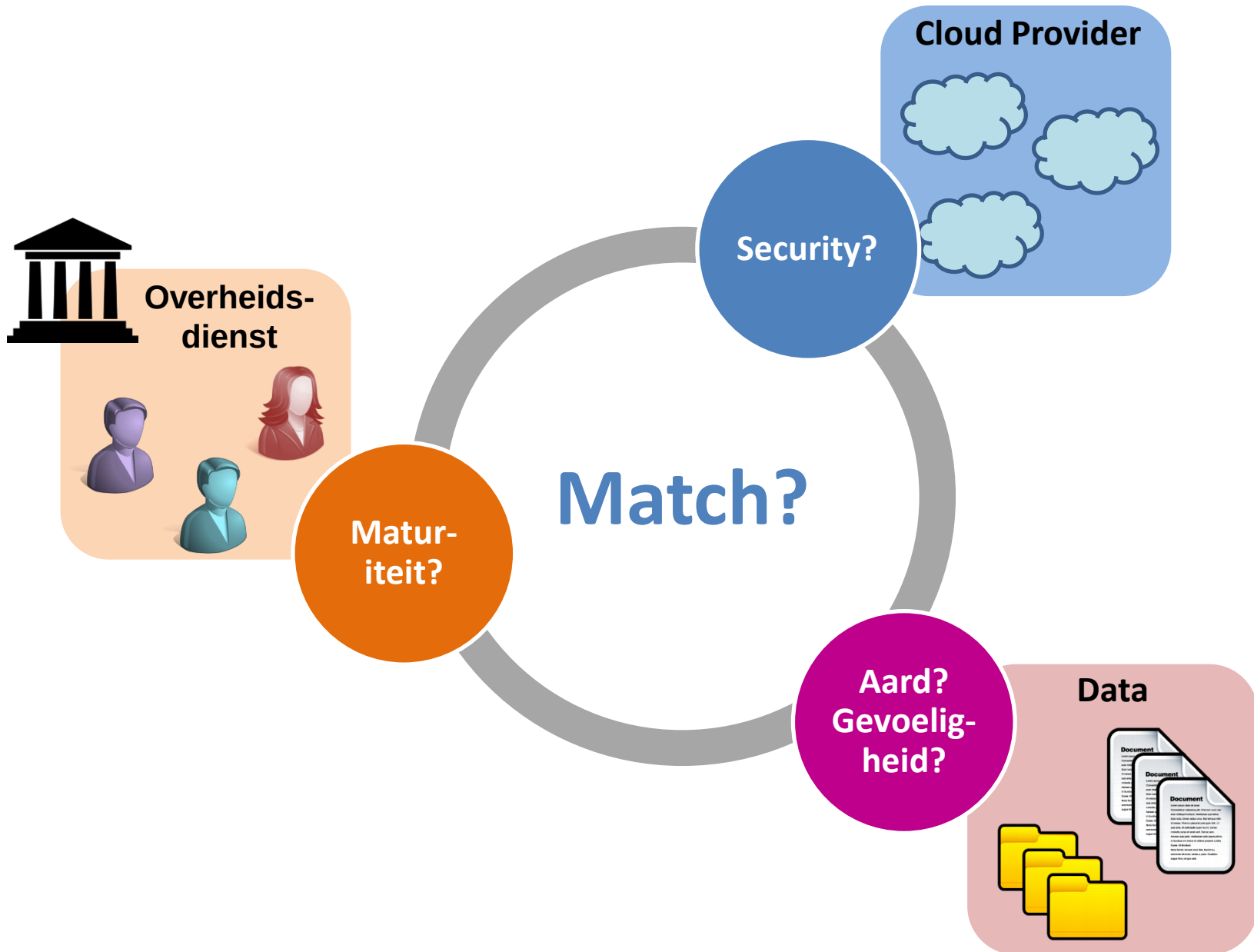
Tot wanneer blijft de data gevoelig?

Volstaan juridische garanties

Welke zijn de contractuele voorwaarden?

....

Next steps...



Artikels

- De Stille machtsgreep van de Cloud
- Hoe het Britse Ministerie van Defensie omgaat met persoonsgegevens
- Hoe de G-Cloud (VK) omgaat met Gevoelige Gegevens

Rapporten

- Cloud Strategieën bij Buitenlandse Overheden

Quick Reviews

- FolderSync
- GoodReader

In voorbereiding

- Open Source Review: ownCloud 6
- Infosessie Cloud Security
- Studie SaaS-Enablement (infosessie?)



Externe referenties

- NIST Special Publication 800-145. The NIST Definition of Cloud Computing. NIST, 2011
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Cloud Computing Guidance. ISACA.
<http://www.isaca.org/cloud>
- European Union Agency for Network and Information Security. ENISA,
<http://www.enisa.europa.eu/>
- Cloud Security Alliance.
<https://cloudsecurityalliance.org/>



App. A: Gebruikerspolicy voor mobiele toestellen SZ

Categorie	Beschrijving
Publieke gegevens	Als publieke gegevens worden alle gegevens beschouwd die openbaar zijn, algemene bekendheid hebben of vrij van vertrouwelijke inhoud zijn. Alle overige categorieën zijn bijgevolg “Niet-publieke gegevens”. De gevoeligheidsklasse van publieke gegevens is “unclassified”. Voorbeeld: voor het algemene publiek toegankelijke website.
Interne Bedrijfsgegevens	Interne bedrijfsgegevens zijn alle gegevens waarvan het gebruik beperkt moet worden intern in het bedrijf. Deze gegevens zijn niet bestemd voor publieke bekendmaking zonder voorafgaande goedkeuring door de directie. De gevoeligheidsklasse van deze gegevens is “sensitive unclassified”. Voorbeeld: Interne telefoonlijst.
Vertrouwelijke Bedrijfsgegevens	Vertrouwelijke bedrijfsgegevens zijn alle gegevens die te maken hebben met de werking van de instelling – het overheidsbedrijf - en die binnen de context van de instelling - en mogelijk ook specifieke partners - een vertrouwelijk karakter hebben. Deze gegevens zijn niet bestemd voor mededeling zonder voorafgaande goedkeuring door de directie. De gevoeligheidsklasse van deze gegevens is “classified”. Voorbeelden: Verslag van het directiecomité; boordtabellen.
Persoonsgegevens	Gegevens die betrekking hebben op een natuurlijke persoon die is of kan worden geïdentificeerd. Alle persoonsgegevens hebben een vertrouwelijk karakter en zijn gebonden aan de richtlijnen uit de privacywet. De gevoeligheidsklasse van deze gegevens is “classified”.
Sociale persoonsgegevens	“Sociale gegevens van persoonlijke aard” zijn alle persoonsgegevens die nodig zijn voor de toepassing van de sociale zekerheid met betrekking tot een natuurlijke persoon. Sociale gegevens die geen persoonsgegevens zijn dienen minstens als vertrouwelijke bedrijfsgegevens te worden behandeld. De gevoeligheidsklasse van deze gegevens is “classified”.
Medische persoonsgegevens	“Sociale gegevens van persoonlijke aard die de gezondheid betreffen” zijn alle sociale persoonsgegevens waaruit informatie kan afgeleid worden over de vroegere, huidige of toekomstige gezondheidstoestand, uitgezonderd louter administratieve of boekhoudkundige gegevens over geneeskundige behandelingen of verzorgingen. De behandeling, uitwisseling en bewaring van deze gegevens moet gebeuren onder toezicht en verantwoordelijkheid van een geneesheer. De gevoeligheidsklasse van deze gegevens is “secret”.
Privé gegevens	Deze speciale categorie betreft privé gegevens die door werknemers opgeslagen kunnen worden op het bedrijfsnetwerk, doch geen enkele binding hebben met zijn professionele activiteiten. Persoonlijke gegevens worden behandeld volgens de regels van de privacywet en het interne reglement van de instelling. Voorbeeld: brief voor privé doeleinden.

[1] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

[2] Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.2, 6°

[3] Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.2, 7°

[4] Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.26, §1



App. B: Gevoelige gegevens op draagbare computers

- « *De bewaring van gevoelige gegevens op de portable PC dient vermeden te worden en gevoelige gegevens moeten zo snel als mogelijk opgeslagen worden in het netwerk.* »
- « *Hieronder enkele voorbeelden van verboden activiteiten (niet volledige lijst):*
 - ...
 - *op eender welke manier, ongeauthoriseerd, vertrouwelijke persoons- of bedrijfsgegevens verspreiden,*
 - *de vertrouwelijkheid en integriteit van de gegevens schenden of hun beschikbaarheid belemmeren;*
 - ... »

Veiligheidsbeleid Draagbare PC V2.20 2009 ISMS



App. C: Gevoelige gegevens via e-Mail en Internet

- *« Alle gegevens van persoonlijke of medische aard die elektronisch moeten worden doorgestuurd, mogen enkel worden overgemaakt via de informatiesystemen die door de bevoegde sectorale comités werden bepaald en goedgekeurd. »*
- *« Bij de elektronische uitwisseling van vertrouwelijke gegevens dienen de gepaste maatregelen te worden getroffen teneinde de vertrouwelijkheid en de integriteit van de overgemaakte gegevens te waarborgen, met inachtneming van de van kracht zijnde wetten en reglementeringen (Kruispuntbank van de Sociale Zekerheid, Rijksregister van de natuurlijke personen, bescherming van persoonsgegevens, ...). »*
- *« E-mail mag standaard niet worden beschouwd als een veilig elektronisch uitwisselingskanaal aan de hand waarvan de vertrouwelijkheid en de integriteit van de gegevens in het bericht kunnen worden gewaarborgd. »*



App. D: Extranet SZ

« De socialezekerheidsinstellingen dienen de minimale veiligheidsnormen na te leven voor hun toegang tot het internet. De instellingen van het primaire netwerk dienen meer bepaald het extranet van de KSZ te gebruiken voor hun internetverbindingen (Minimale normen, §10.3), aangezien het extranet over aangepaste beschermingsmaatregelen beschikt. »

Algemene policy inzake het gebruik van het internet
V0.30, ISMS, 2010

Alle relevante security policies zijn te vinden op
https://www.ksz-bcss.fgov.be/nl/bcss/page/content/websites/belgium/security/security_04/security_04_02.html

