Smals
ICT for society

Gevoelige Overheidsdata en de Cloud

Kristof Verslype
Smals Research
www.smalsresearch.be

3 april 2014

AGENDA

De Cloud - Intro

⬇

Cloud Services Brokerage

⬇

Buitenlandse Overheden

⬇

⬇

Case: File Sync & Share

⬇

Afronding

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

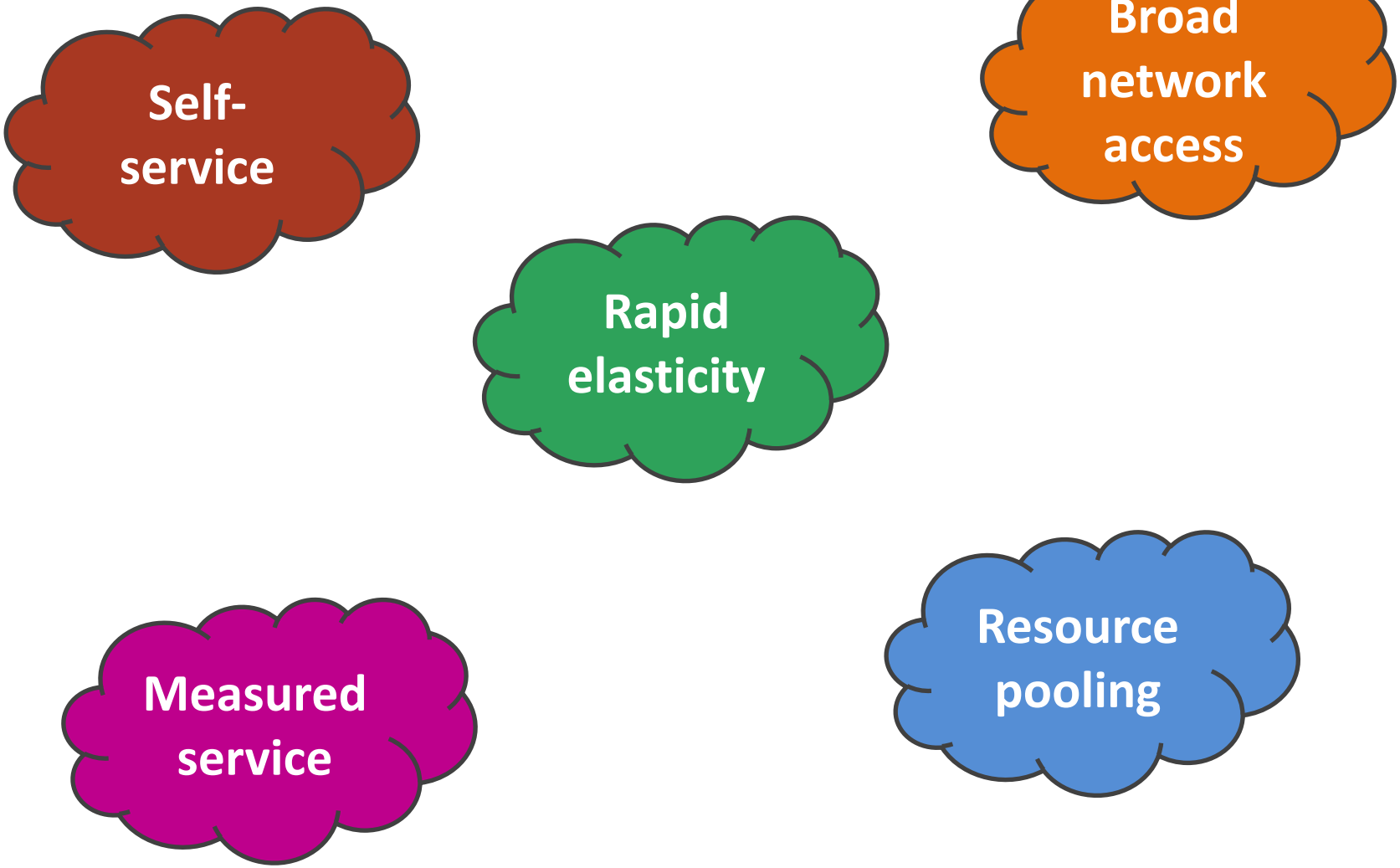
Het ontwikkelen van een web-toepassing

Een office-pakket toegankelijk vanaf elke computer met internet

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

Een e-Mailomgeving waar het personeel overal toegang tot heeft

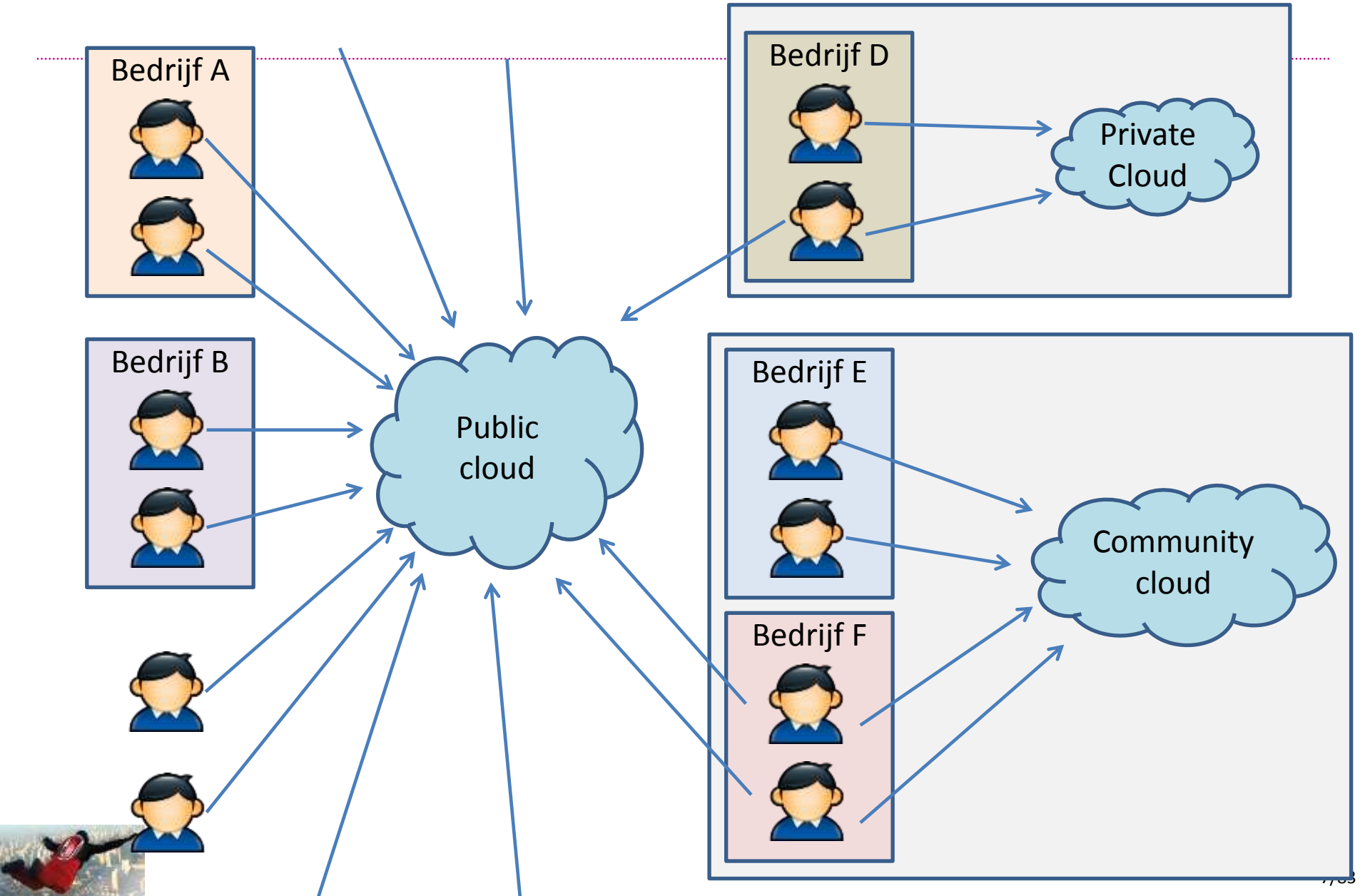
Eigenschappen



Bron: NIST Special Publication 800-145. The NIST Definition of Cloud Computing

Smals
ICT for society

Public VS Private VS Community

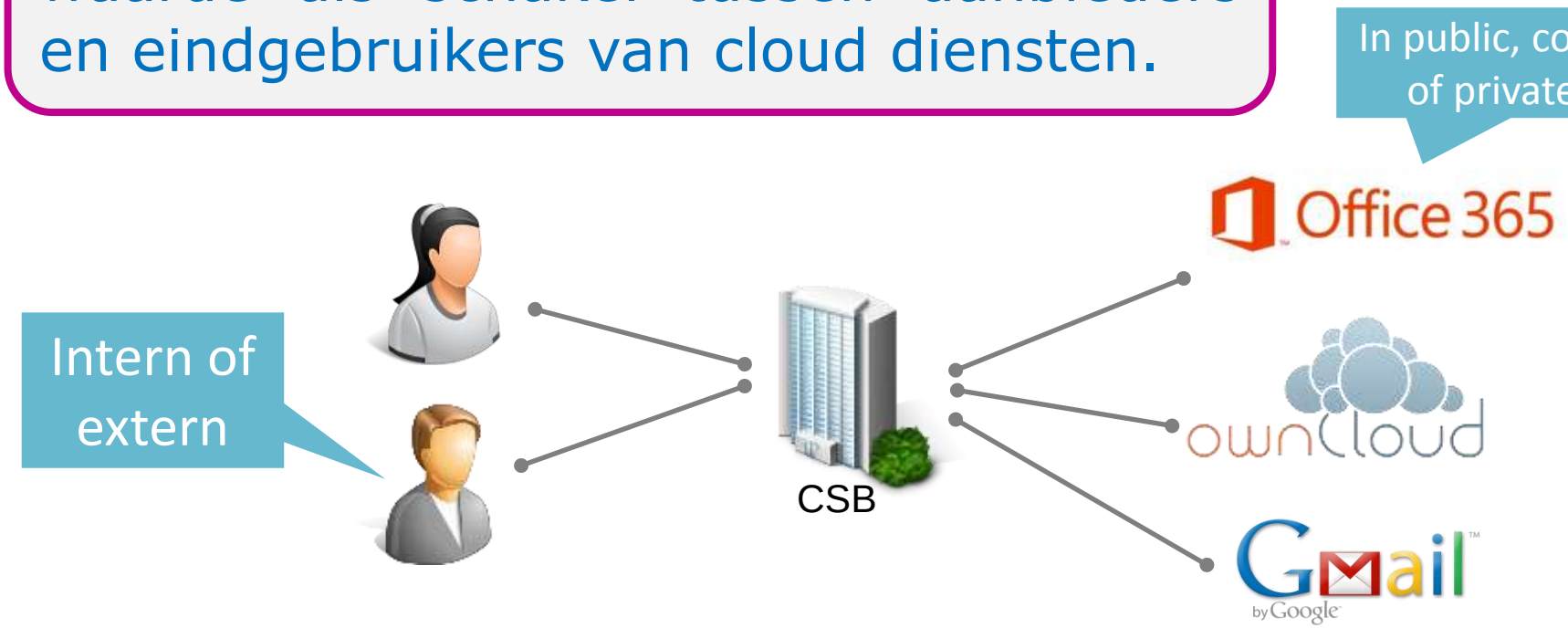


Cloud Services Brokerage

Wat?

Wat?

Een Cloud Service Broker levert meer-waarde als schakel tussen aanbieders en eindgebruikers van cloud diensten.

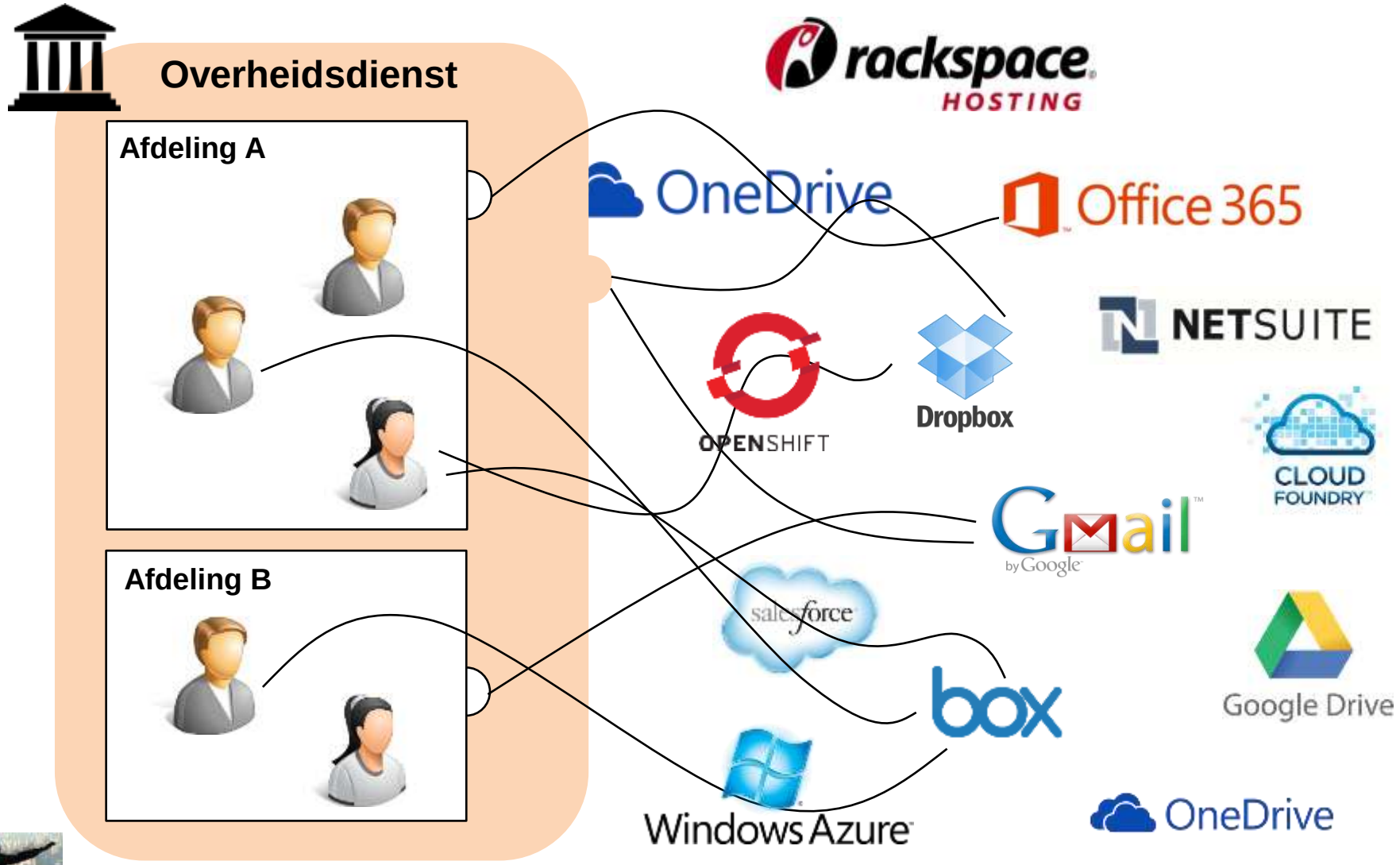


Werking en beschikbaarheid cloud diensten vallen buiten controle cloud service broker

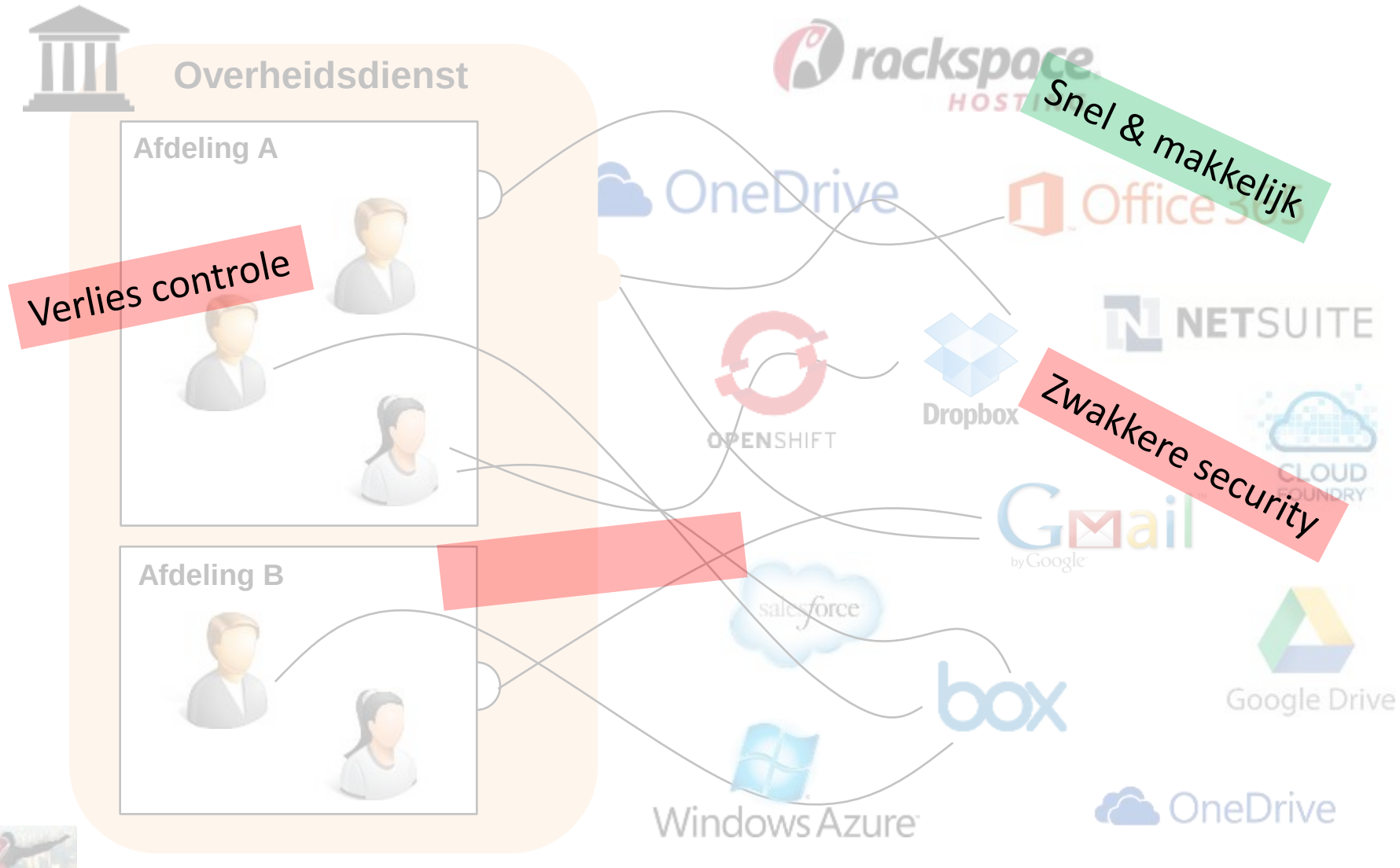
Cloud Services Brokerage

Waarom?

Spaghetti-architectuur

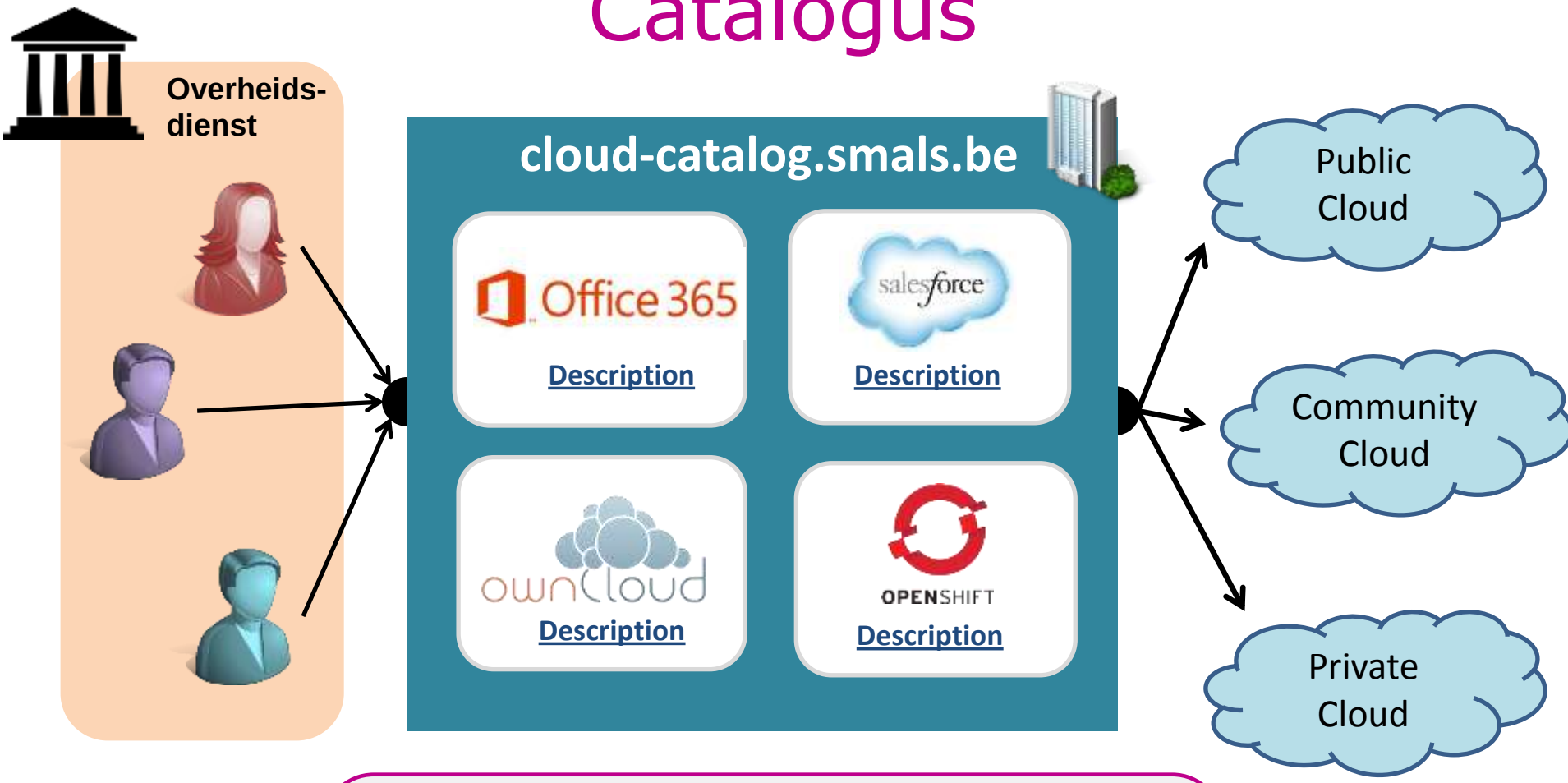


Spaghetti-architectuur



Cloud Services Brokerage
Functionaliteit

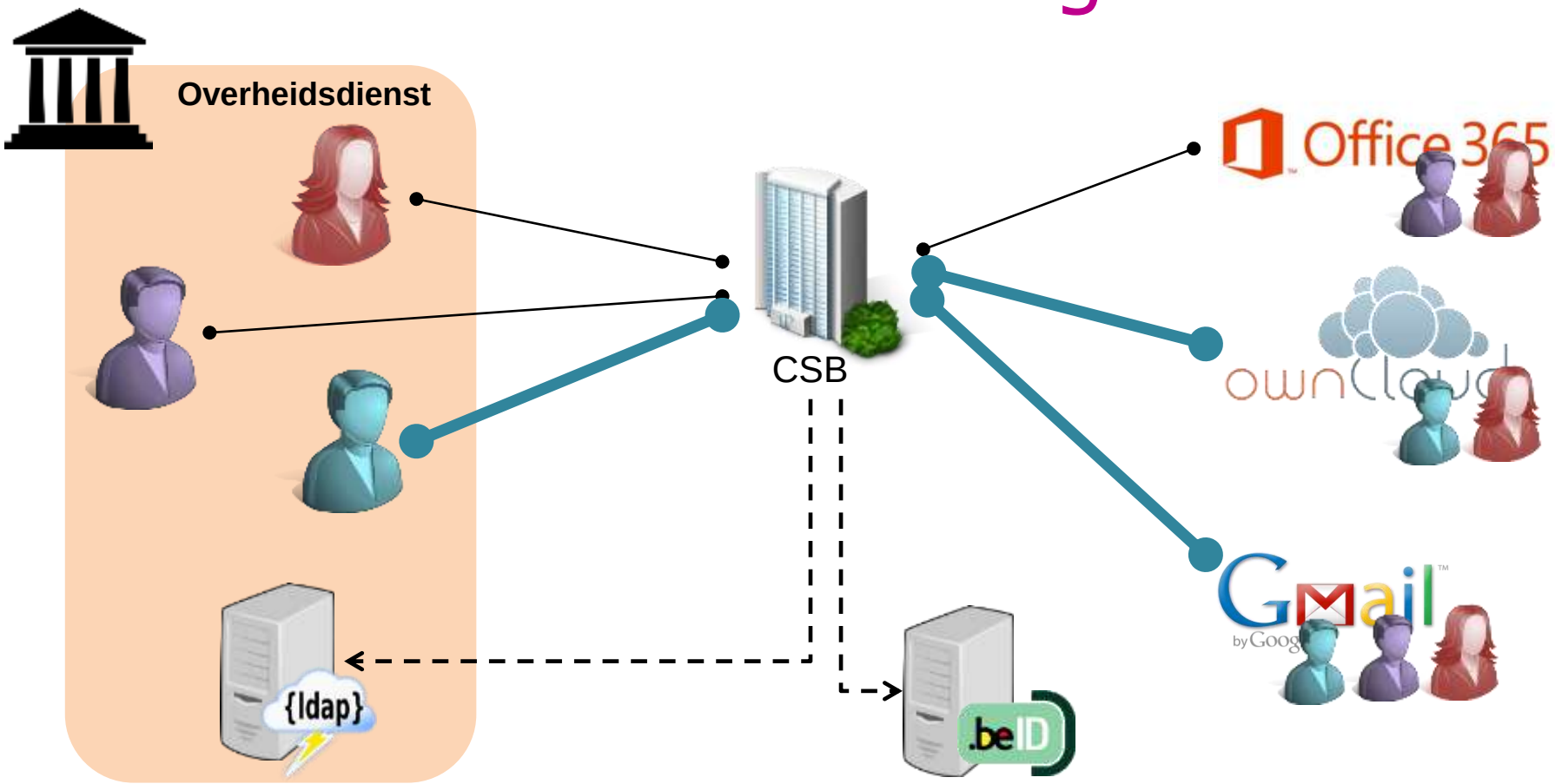
Catalogus



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

=> Vermijdt wildgroei, stimuleert compliancy

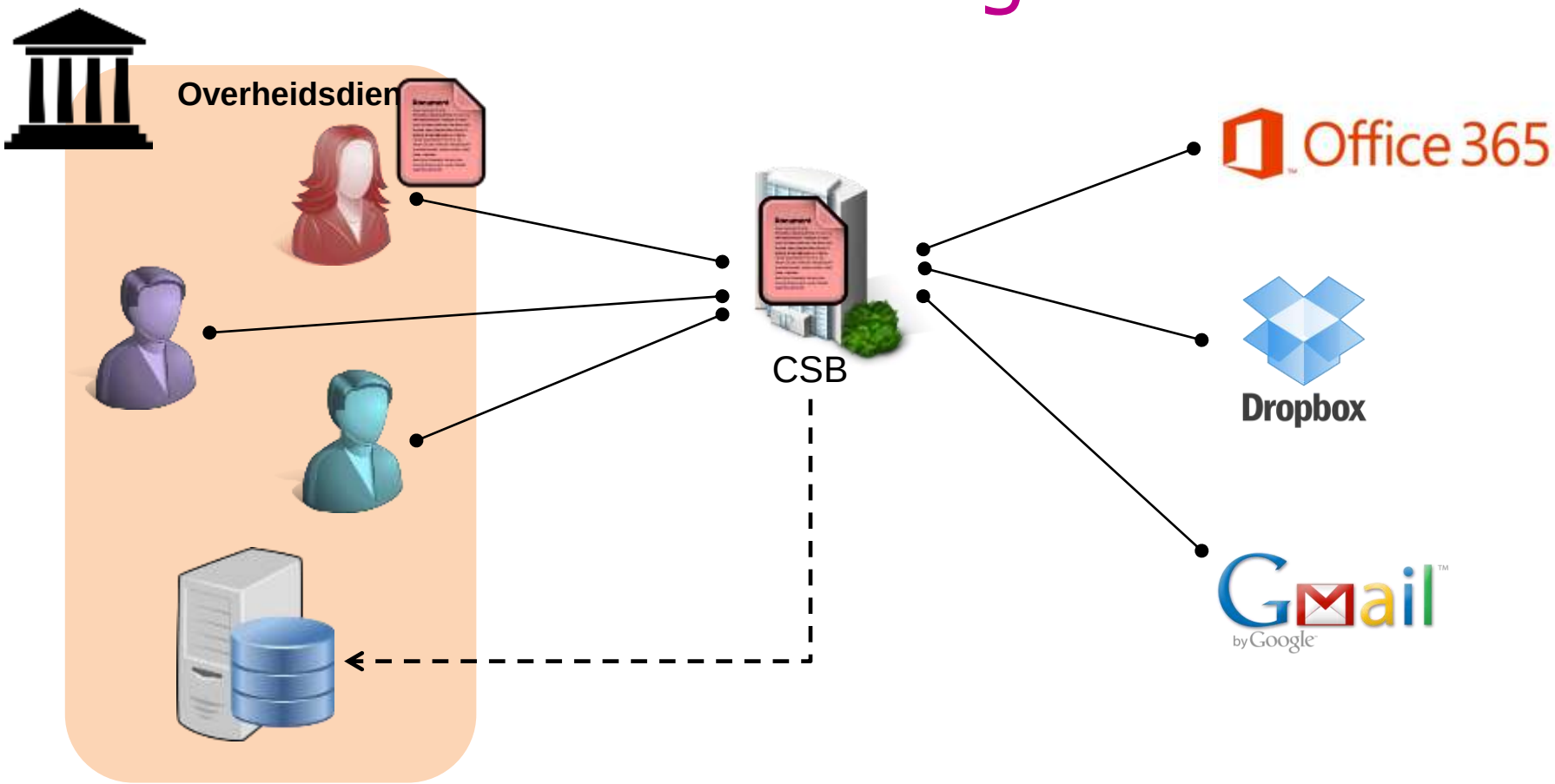
User & Access Management



- (De)provisioning
- Single sign-on
- Integration LDAP, eID, SAML, ….
- Policy enforcement

=> Verbetering UAM

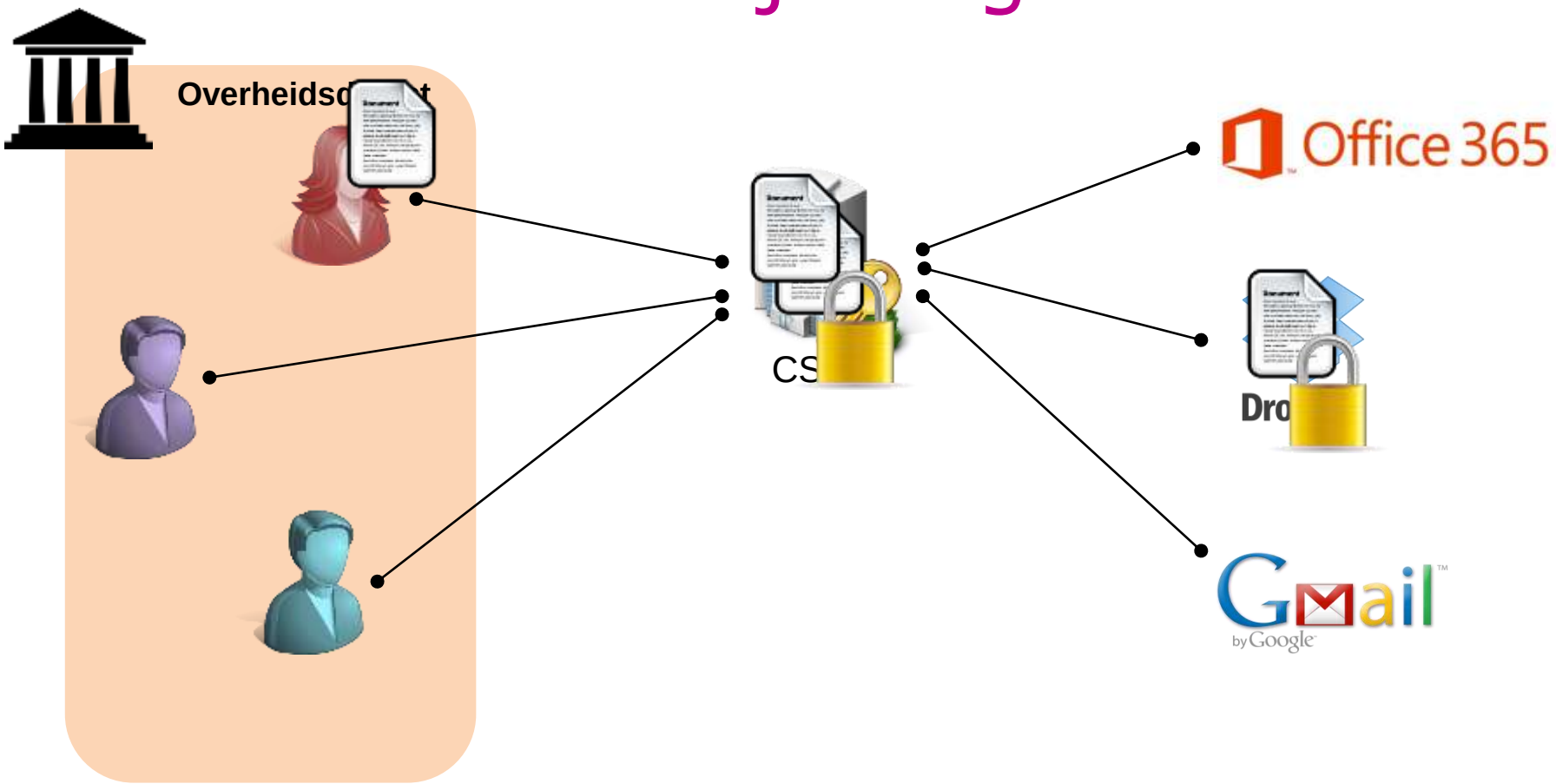
Archivering



- Eigen beleid rond archivering
  - Vb. Clouddienst levert geen langetermijngaranties
  - Vb. Wat bij faillissement dienst?

=> Beschikbaarheid data langetermijn

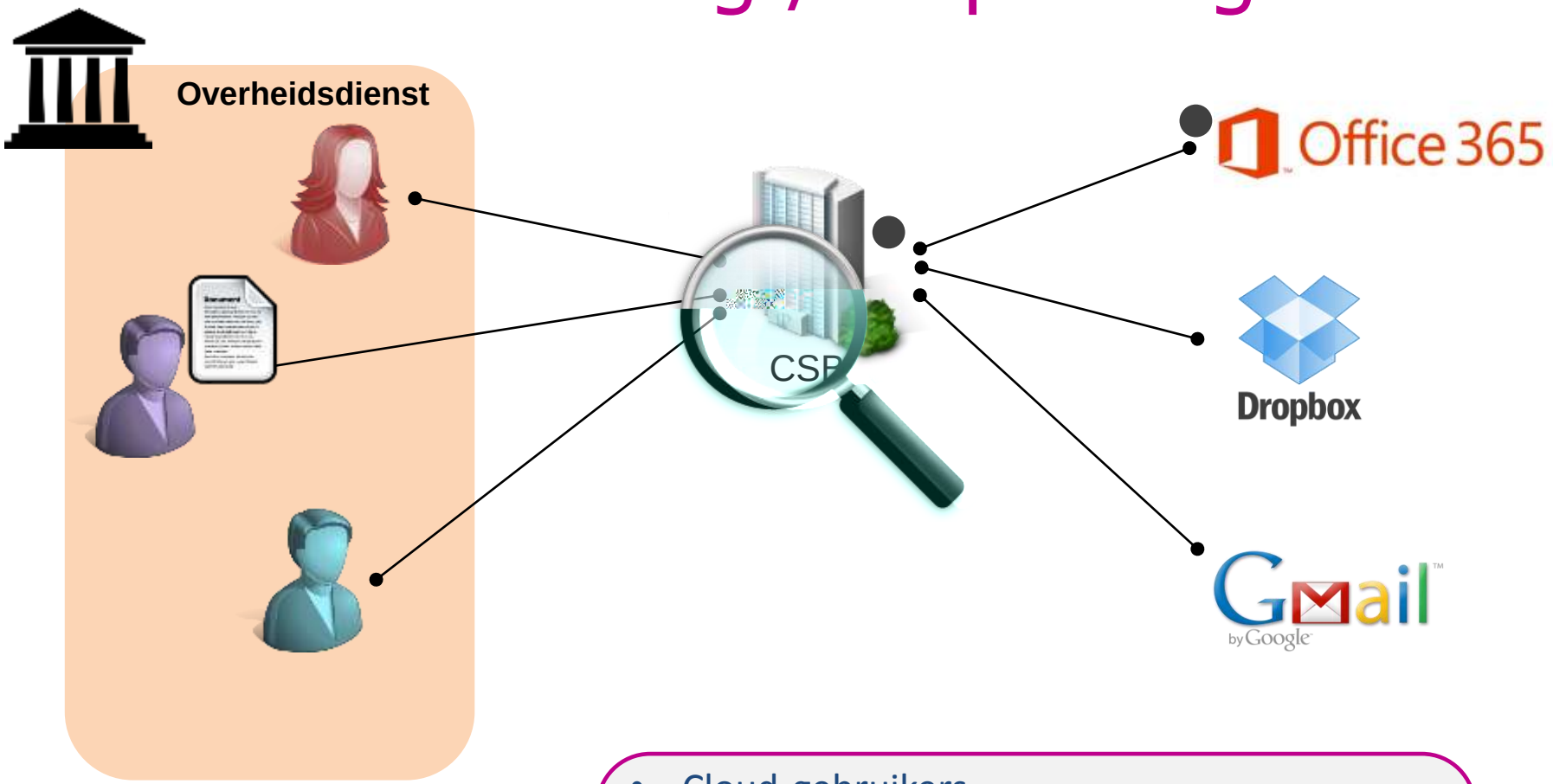
Vercijfering



- Gevoelige gegevens worden vercijferd vooraleer naar publieke cloud
- Bestandsopslag & uitwisseling, e-Mail, ….

=> Verhogen confidentialiteit

Monitoring / Reporting



- 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

dokeos®
e-learning architects

amazon

Smals
ICT for society

INAMI-RIZIV

Online cursussen voor artsen

Security

- Integratie eID
- Monitoring & reporting

Andere

- Marktstudie
- Lastenboekprocedure
- Facturatie
- Accreditatiegeneratie
- …

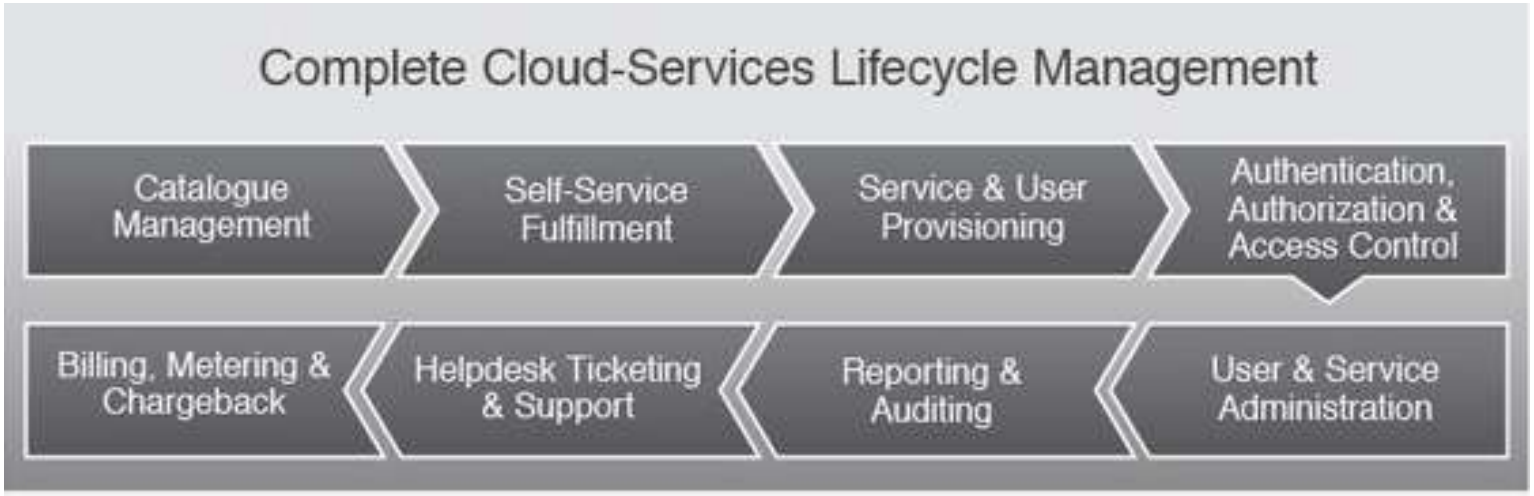
Cloud Services Brokerage

Hoe?

CSB Enablers

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

Een bekende speler: jamcracker™



http://www.jamcracker.com/

Twee cases

=> 2 x telco

Cloud Services Brokerage
Markt

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

Enkele cloud brokers…

	Catalog	SSO	Advies	Contract Beheer	Financieel	Migratie	Integratie	Config	Monitoring	Cloud services
Telenet CloudOffice	X	X								MS Exchange + anti-virus/-spam, kalender, Nomadesk Teamserver
Belgacom BeCloud	X	X								MS Exchange, Sharepoint, Lync, Office
CloudBrokerz.nl			X	X	X	X				No restrictions given
CloudSherpas	X	X	X			X	X	X	X	Focus op Google & Salesforce
Vordel	X	X					X	X	X	No restrictions given
Apperio			X			X	X			Focus op Google, Salesforce & Amazon
Dell				X			X		X	SalesForce
CSC			X							No restrictions given
Accenture			X							No restrictions given

CSB Enablers - Cool Vendors

CLOUDREACH
Make It Happen

FULLARMOR.
The Leaders in Enterprise Policy Management

proximitum
stress free it

Gravitant

LuxCloud
Enabling SaaS Business

Cloud Services Brokerage
Samengevat

Samengevat...

Personeel neemt initiatief, zonder nodige overleg

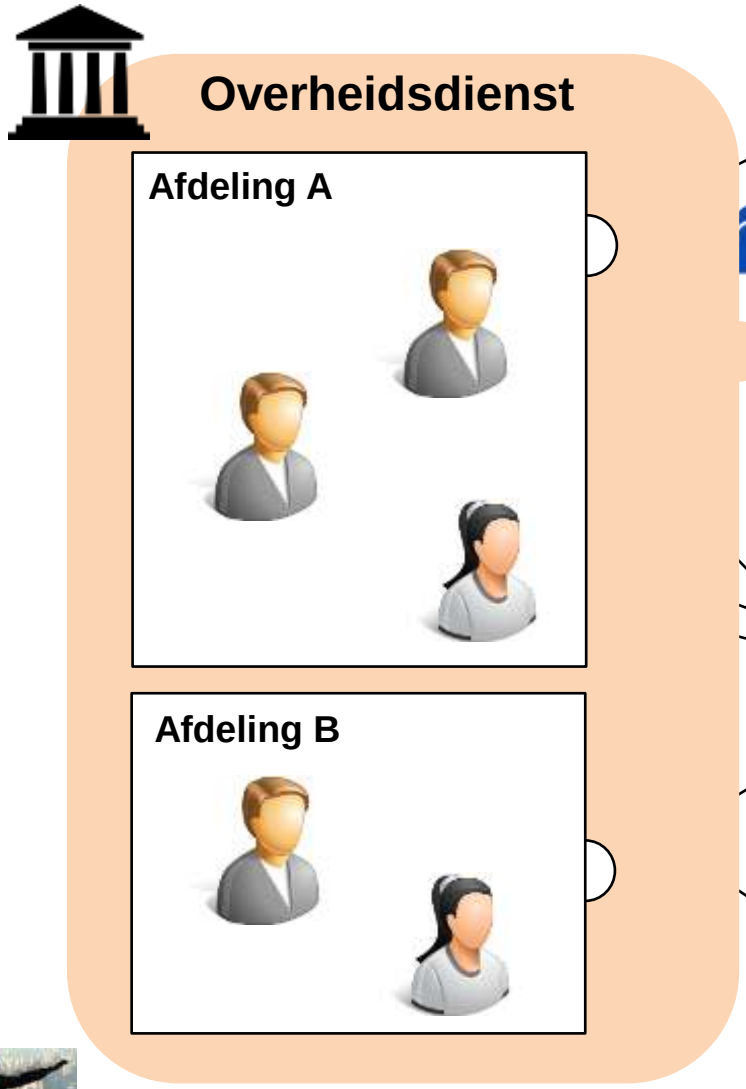
CSB positieve impact op security

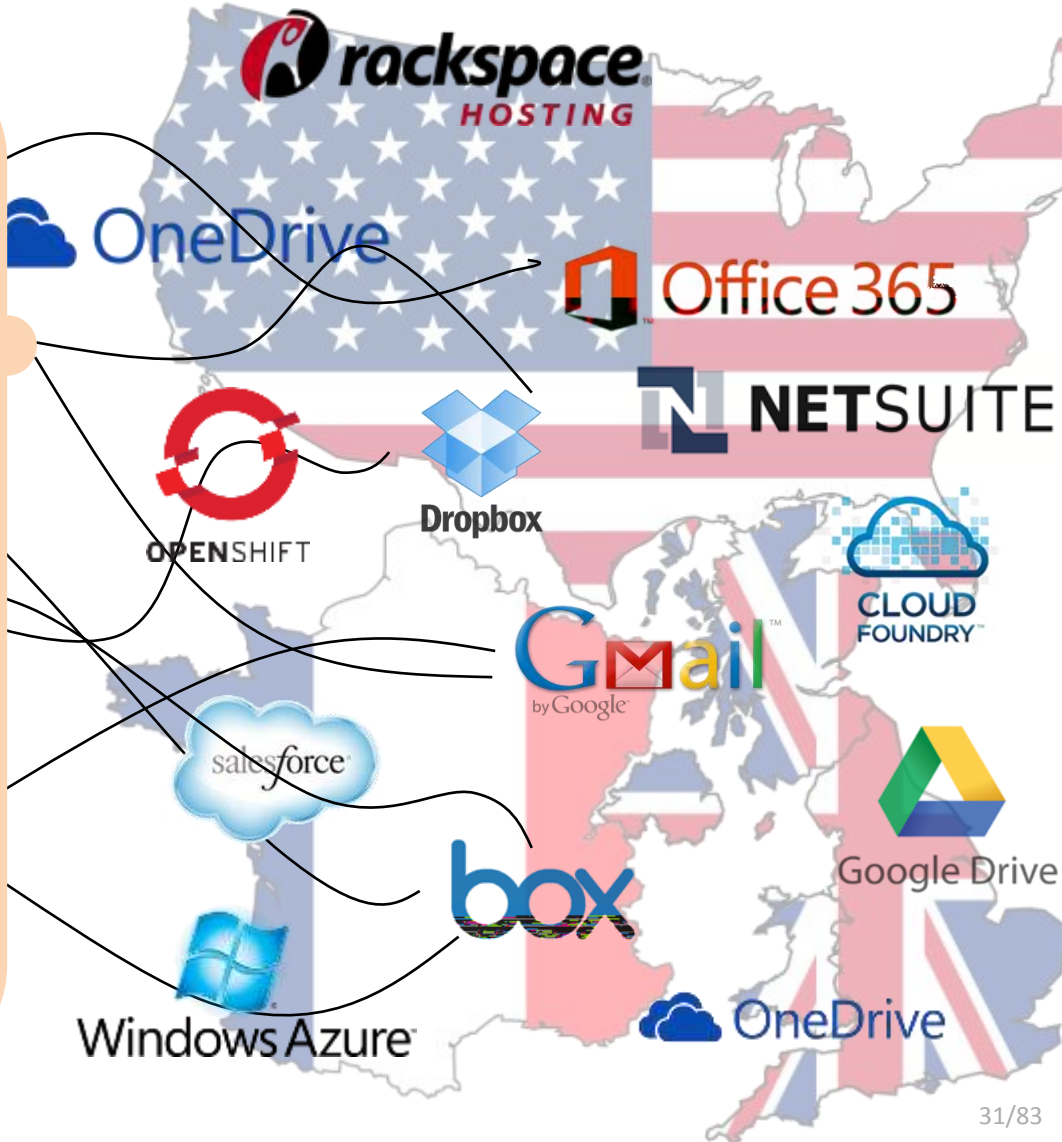
Onvolwassen markt met sterke groei

Term CSB niet altijd even scherp afgebakend

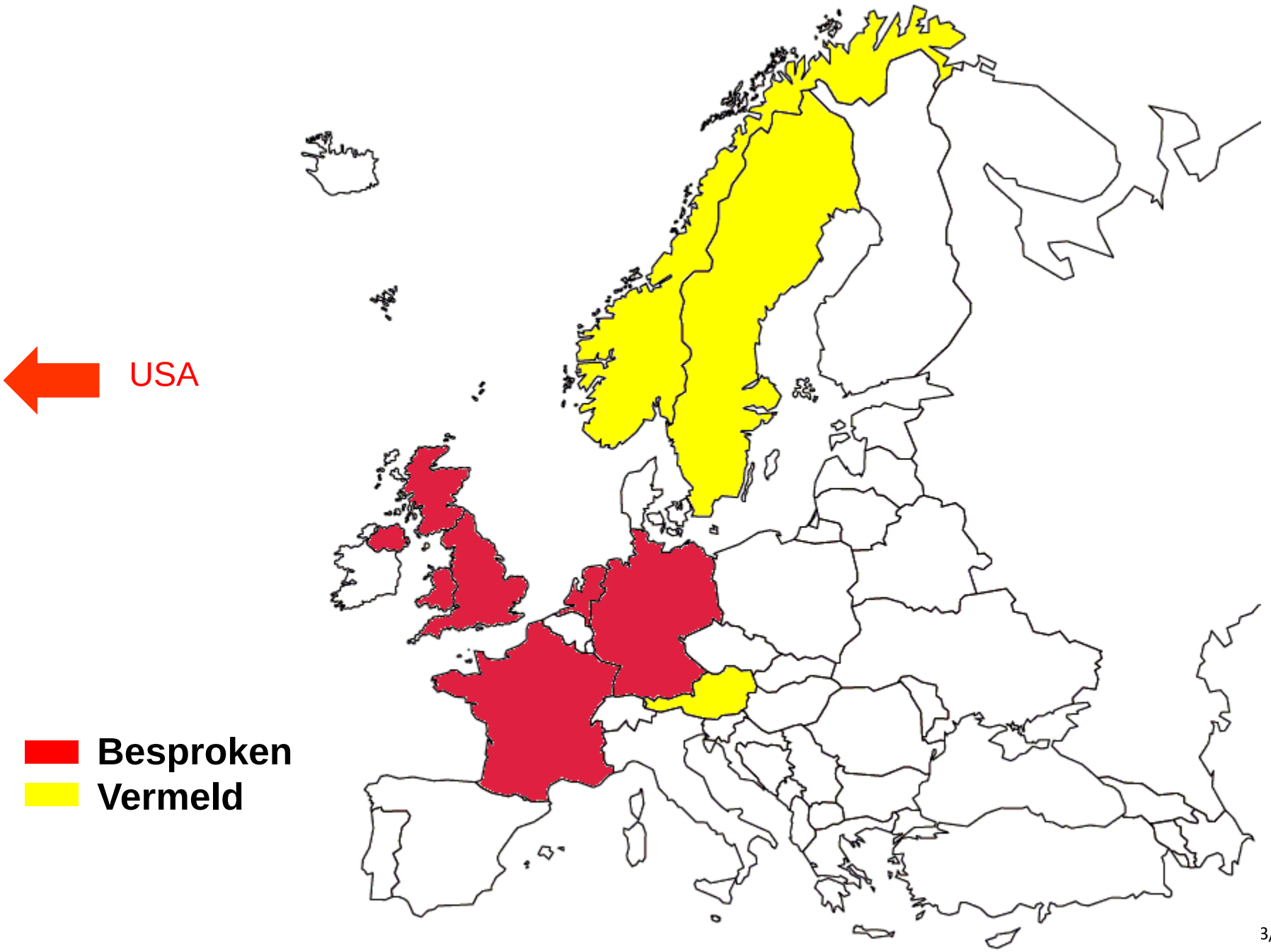
Traditionele service providers (vb. telco's) nemen de rol van CSB op

Spaghetti-architectuur





Overheden Buitenland


USA
Besproken
Vermeld

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**."*

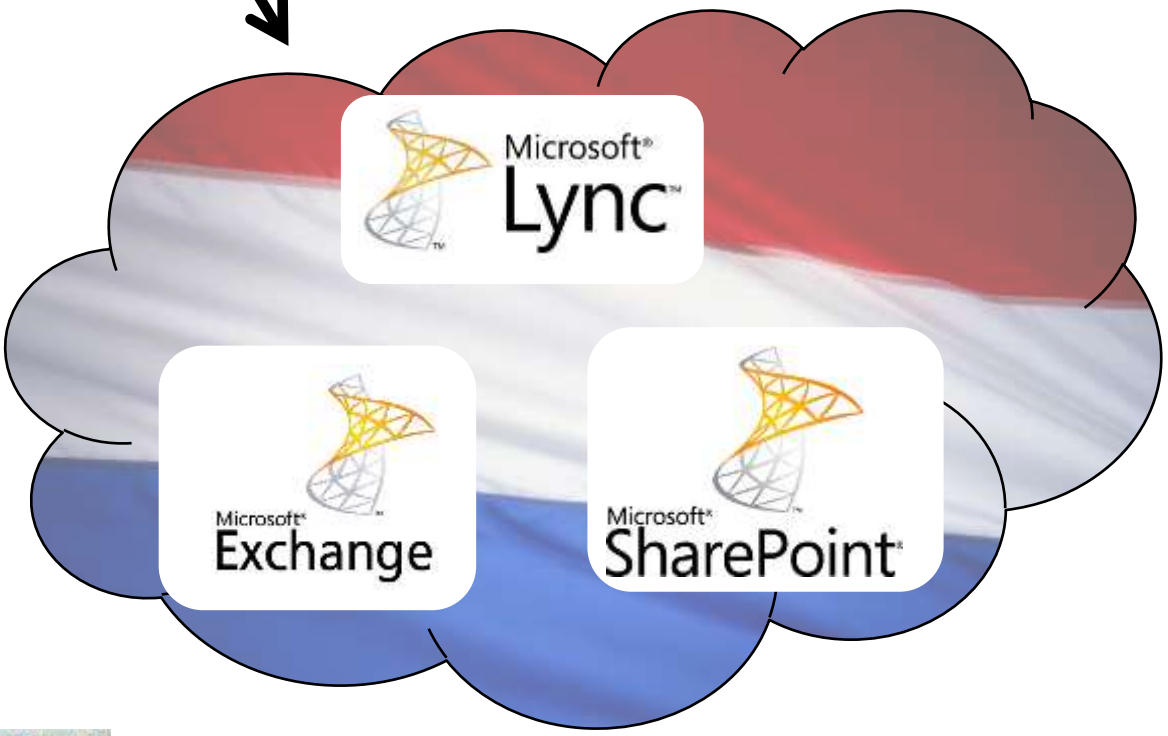
Brief aan de Kamer op 20 april 2011

...

September 2012

20.000 ambtenaren!!!
Ah nee, toch niet…

CloudNL



kpn

20.000 ambtenaren!!!
Ah nee, toch

kpn

Juni 2013

Datacenter in eigen beheer, zoals AIVD, is verstandiger!

EQUINIX

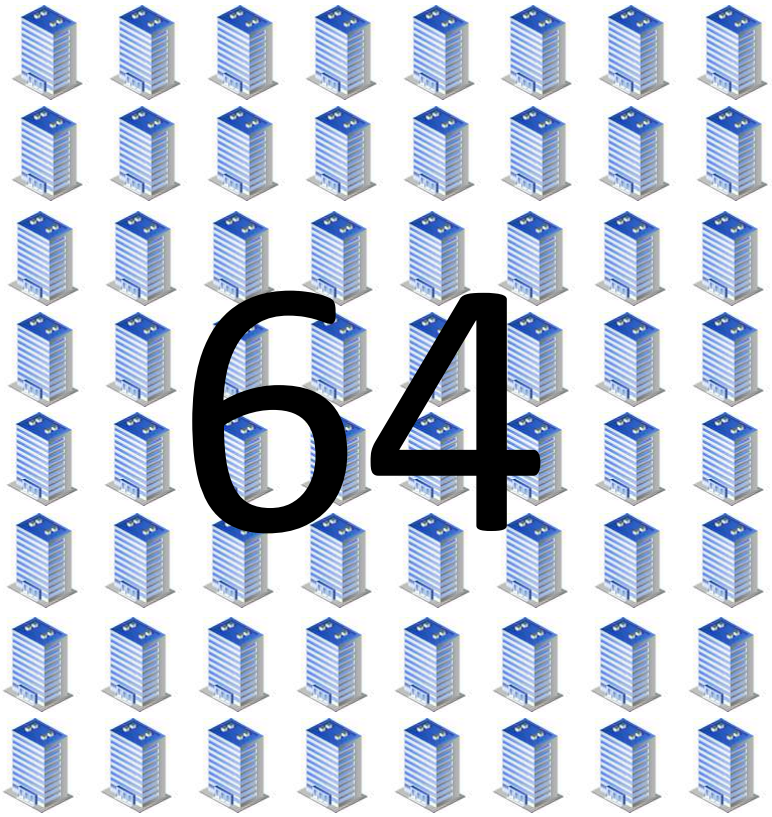
- Rijkswaterstaat
- Dienst Justitiële Inrichtingen,
- Inspectie SZW Opsporing,
- Dienst Terugkeer en Vertrek,
- Rijksinstituut voor Volksgezondheid en Milieu,
- Koninklijk NL Meteorologisch Instituut
- Planbureau voor de Leefomgeving,
- College ter Beoordeling van Geneesmiddelen,
- Centraal planbureau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

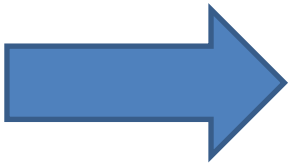
VU VRIJE UNIVERSITEIT AMSTERDAM

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

NUMERGY

PRODUCTEUR D'ENERGIE NUME

IQUE

Door

SFR

BULL

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

https://www.numergy.com/

Cloudwatt

Door

orange

THALES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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…

Support Connexion MON PANIER 357,60

Cloudwatt

Le Cloud et vous | Qui sommes nous ? | Cloudwatt box | Stockage et sauvegarde | Instances et Serveurs | Questions et réponses

Accueil

1 utilisateur
50 GO de stockage

PROMO

29 €
ht / an
*au lieu de 42 € HT**

COMMANDER

10 utilisateurs
100 GO de stockage

299 €
ht / an
*au lieu de 520 € HT**

PROMO

COMMANDER

Configurez votre stockage

1,2m²
de surface d'archivage

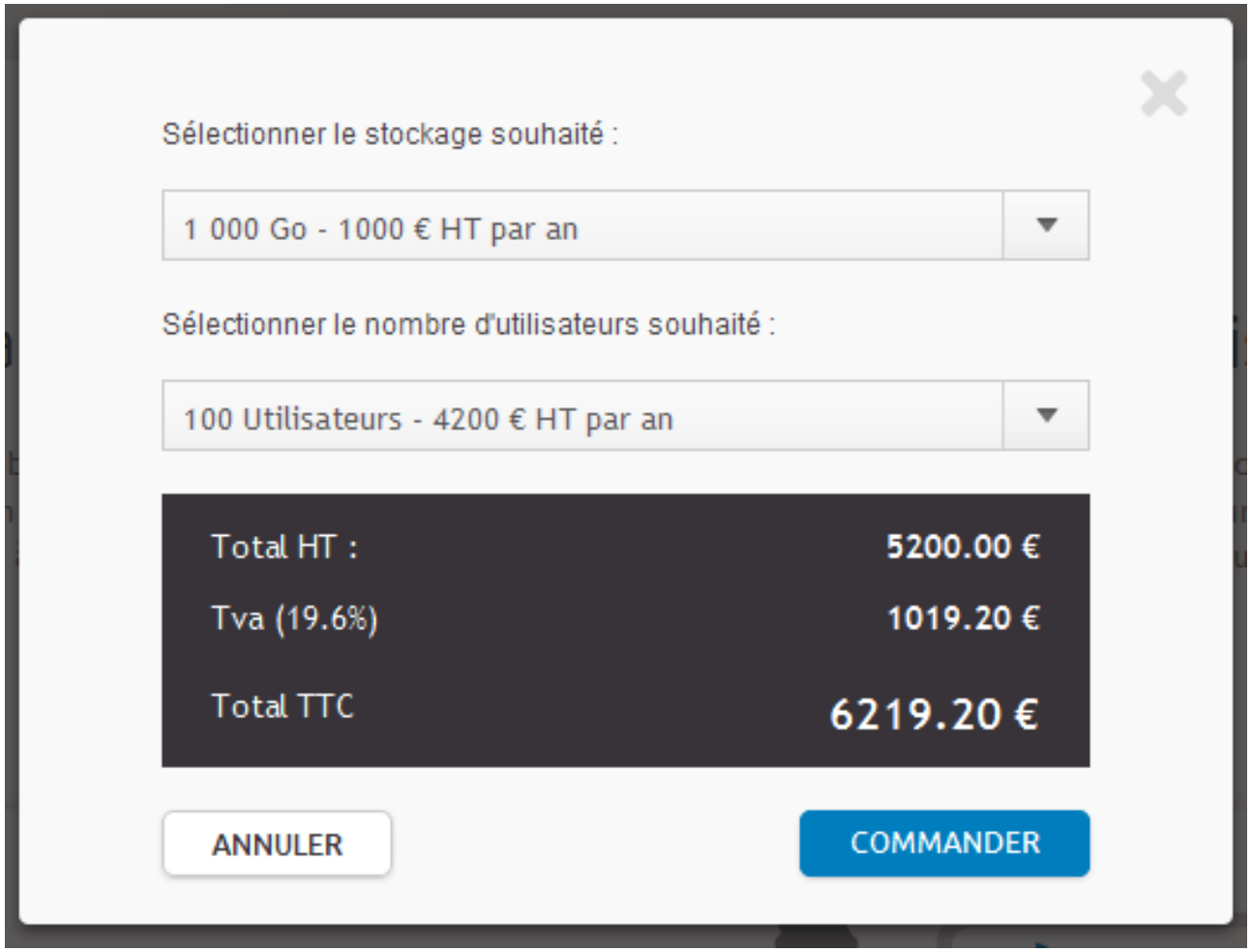
250
vidéos

sélection du niveau de stockage

Octets	Prix HT/an
50 Go	0 €
100 Go	100 €
200 Go	200 €
500 Go	500 €

Smals
ICT for society

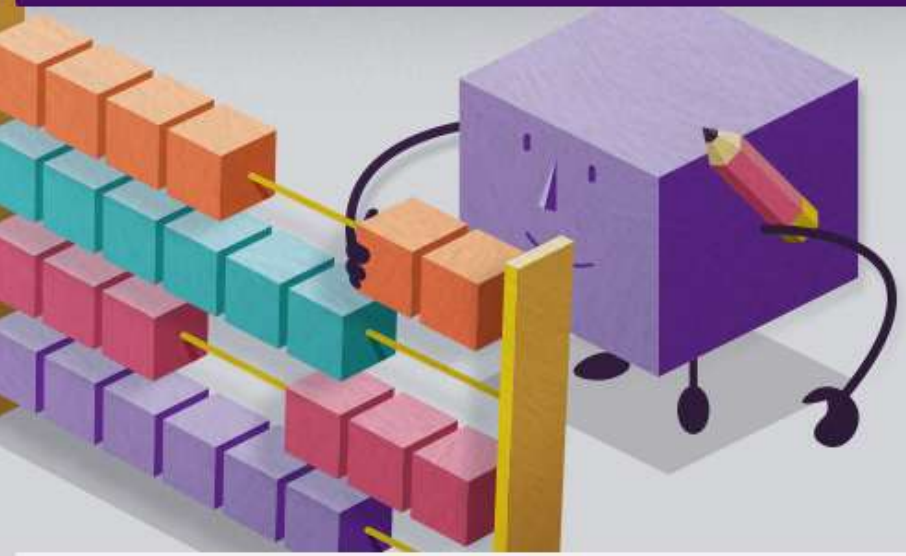
Cloudwatt



NUMERGY
PRODUCTEUR D'ÉNERGIE NUMÉRIQUE

Support Développeurs Espace client

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.

Calculez le coût de votre cloud

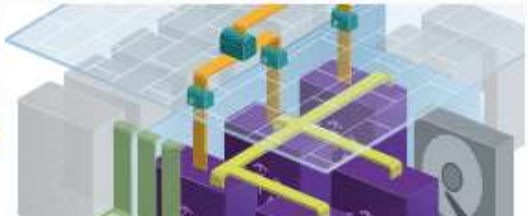
De combien de VM avez-vous besoin ? 1

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)

Overheden Buitenland

Duitsland

Duitsland, 2011

2 initiatieven

DEUTSCHE WOLKE

Trusted Cloud

Veilige, Duitse Bundescloud 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/

DEUTSCHE WOLKE

Aanbod (via resellers)

redhat

GRAUDATA

agorum®
DMS – einfach für jeden!

ownCloud

Zarafa

openSUSE

HELIUM

blue spice
for MediaWiki

projectile

« wordt uitgebreid »

Project

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

www.trusted-cloud.de

Trusted Cloud

Activiteit

Aanbod (in ontwikkeling)

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

cloud4health

GeneCloud

TRESOR

- Publieke sector (2)

goBerlin

CLOUDCYCLE
Sicherheit. Standards. Services.

Pilootproject voor certifiëring 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

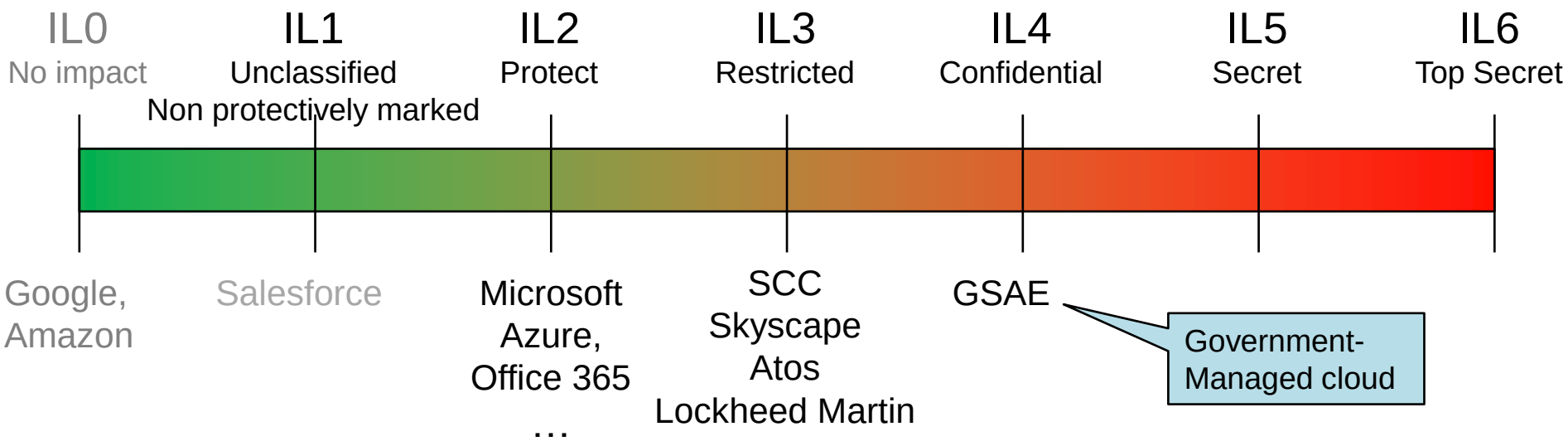
Accredited services

Buyer's guide

Who's bought what?

G-Cloud

Accreditaties



Amerikaanse bedrijven reageren

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

G-Cloud

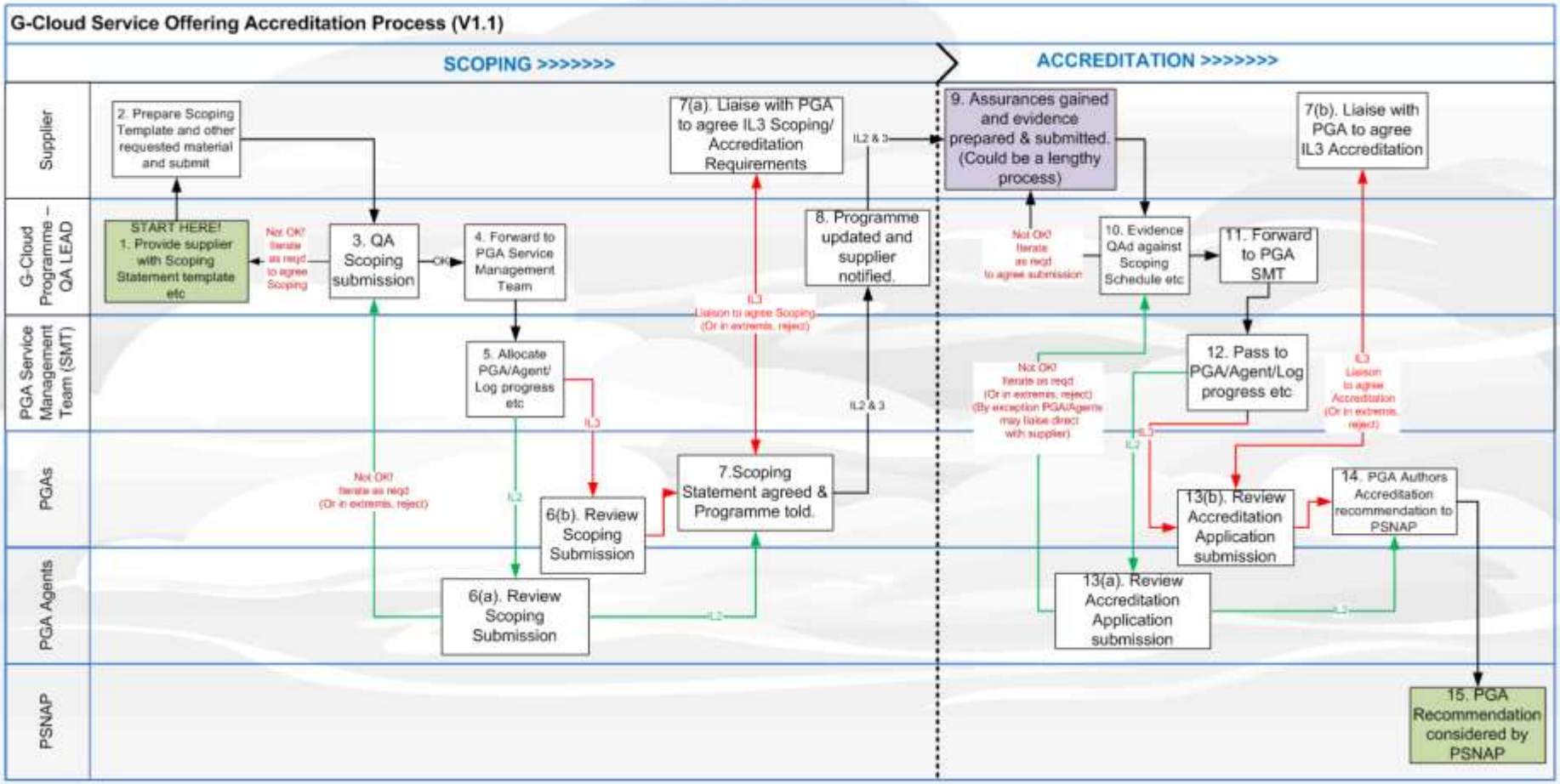
- Business Impact Level (« BIL » of « IL »)

BIL 3.3.4 → BIL 3

Availability
Integrity
Confidentiality

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

- Accreditatie

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

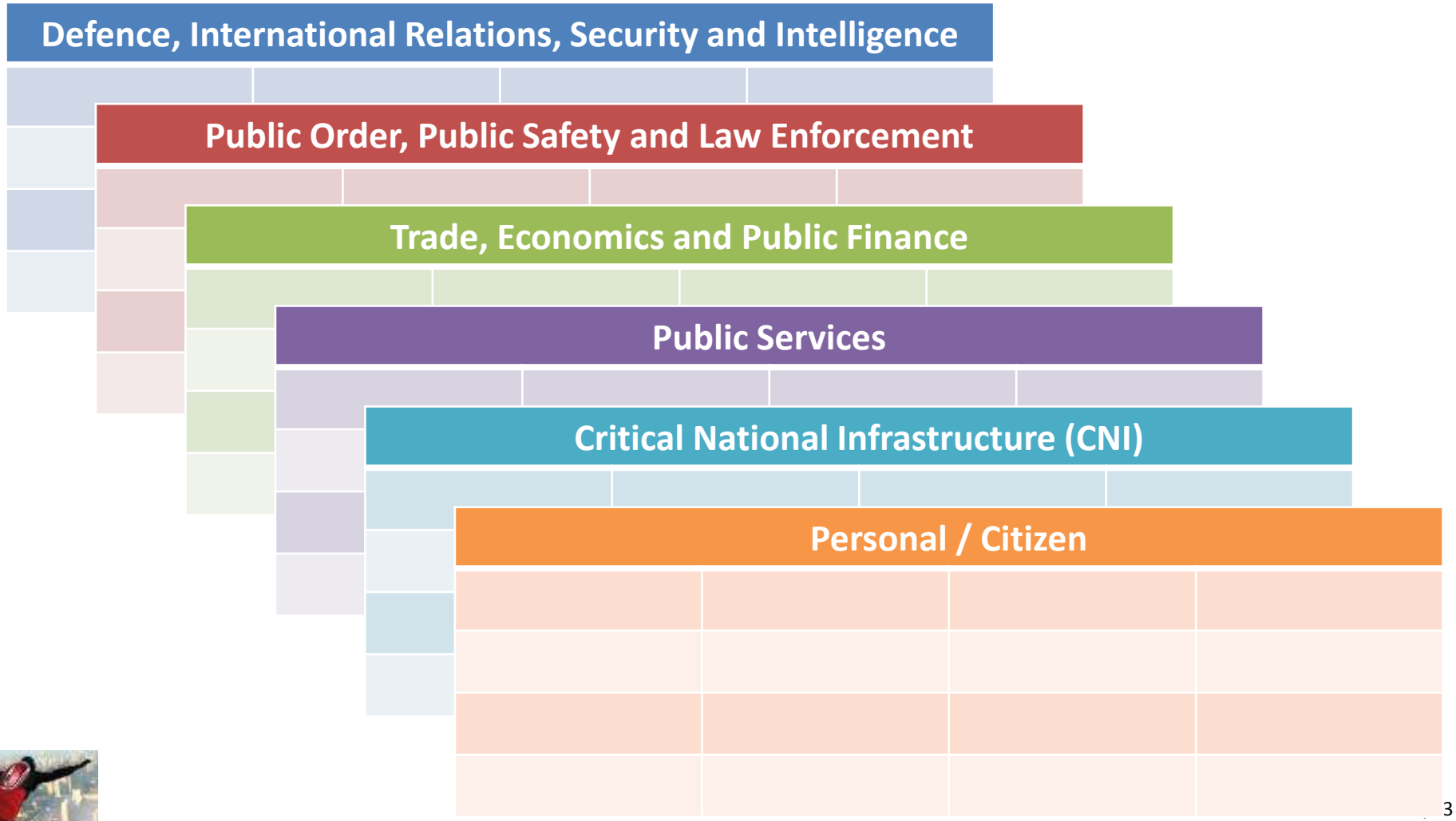
*"**BIL 33x** services will be delivered through **PSN Direct Network Service** Providers (DNSPs) and **will not be offshored** outside the UK. "*

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

Smals
ICT for society

G-Cloud

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



Smals
ICT for society

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	None	personal data beyond those authorised by the citizen.	citizens' personal data beyond those authorised by each citizen.	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.

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.

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

amazon web services™

Google Apps Government Edition

Office 365

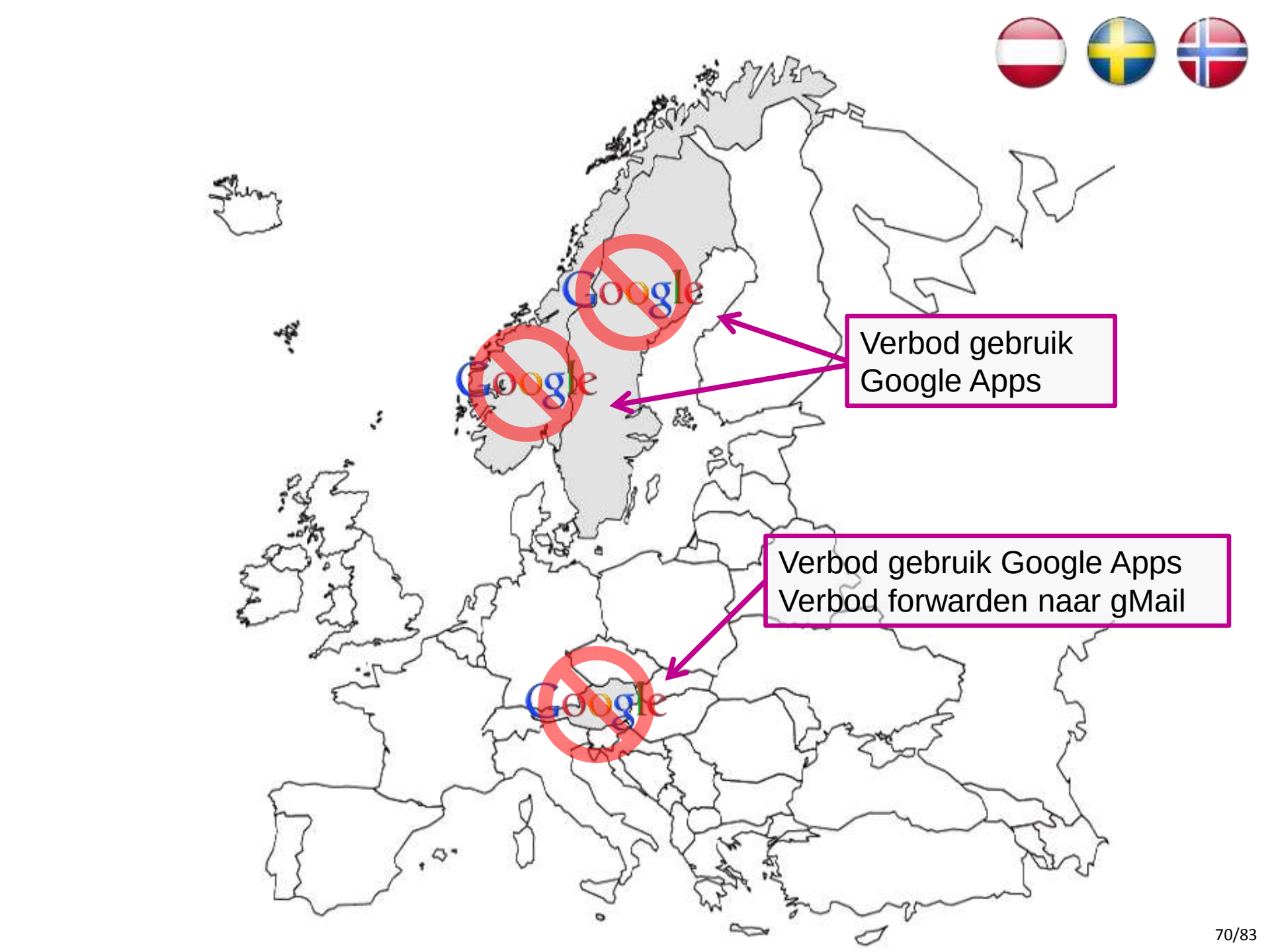
Wel extra maatregelen

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

Nationale spelers ~ wereldspelers

Overheden Buitenland

Andere


Google
Google
Google
Verbod gebruik
Google Apps
Verbod gebruik Google Apps
Verbod forwarden naar gMail

Overheden Buitenland
Conclusies

Conclusies

Strategy

Confidential data stays inside the country

Soevereine clouds in opbouw

De soevereine cloud…

Toekomst

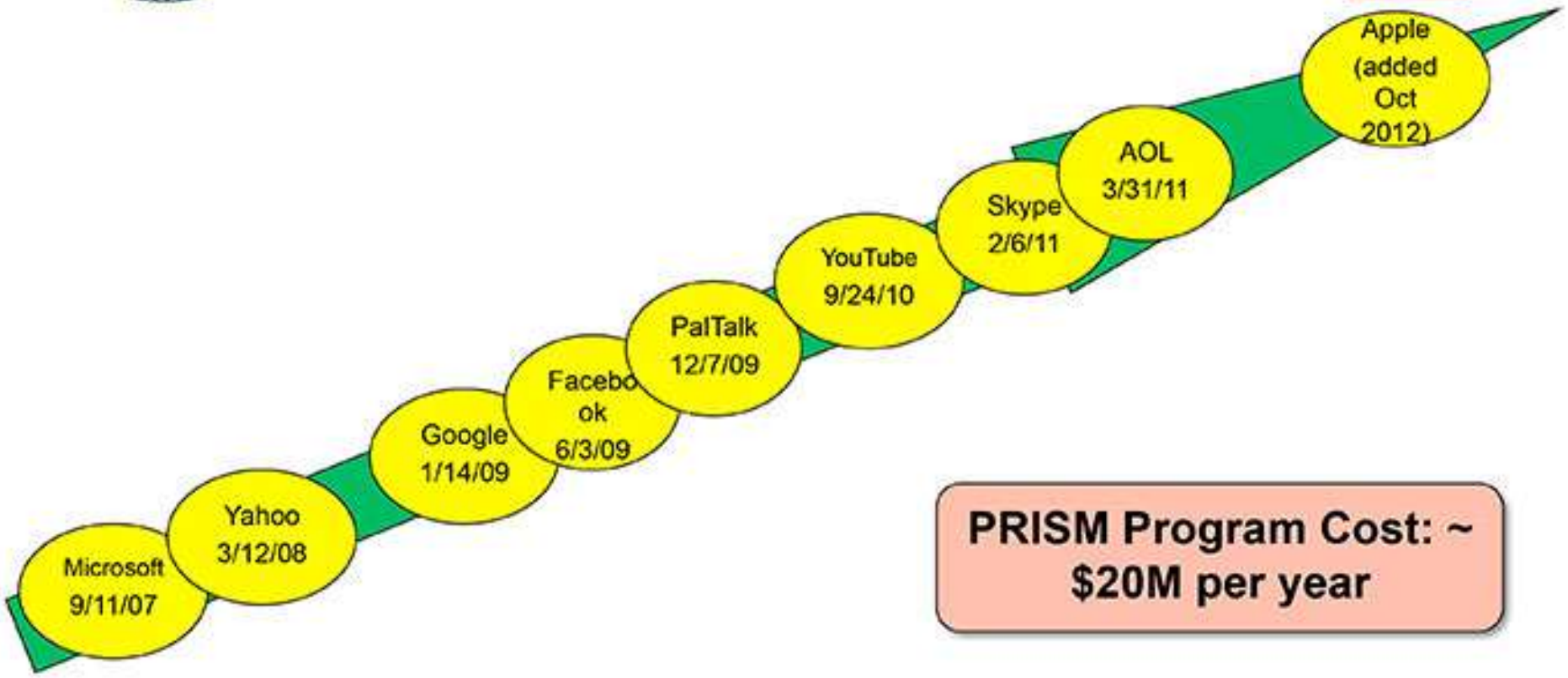
Europe

World economy

« Vertrouwen is goed, controle is beter »

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

(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)

http://www.spiegel.de/politik/deutschland/internet-ueberwachung-bnd-will-100-millionen-investieren-a-905938.html

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?

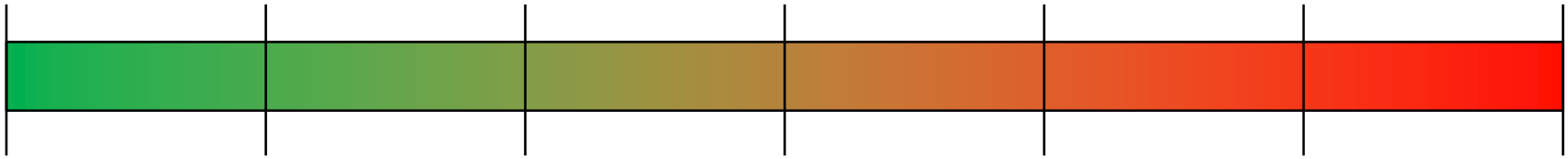
- Fedict stootte op financiële obstakels

>> België loopt achter! <<

Mogelijke rol Smals

Publieke gegevens

Top Secret gegevens



Publieke Cloud Internationaal

Belgische cloud Commercieel

Gov. Cloud Gov. Managed

No Cloud

Smals als CSB
Catalogus, UAM, monitoring, advies, …

Synergieën?

Smals als cloud aanbieder
Vb. File sync & Share, Virtuele servers

Smals infrastructuur
(mits certifiëring)

Suggesties?

« Was mich nicht umbringt, macht mich stärker »

Friedrich Nietzsche, Duits filosoof

Eindelijk…

File Sync & Share

AGENDA

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

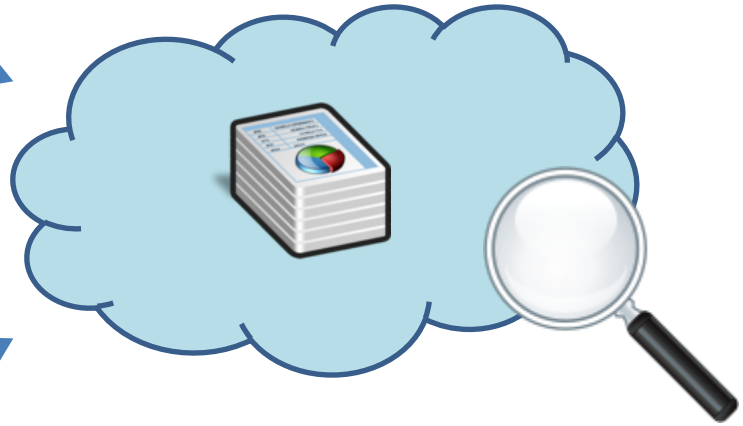
OneDrive

Dropbox

box

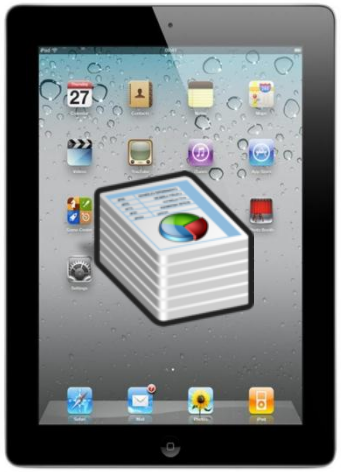
voor bedrijven/overheden
= Enterprise File Sharing

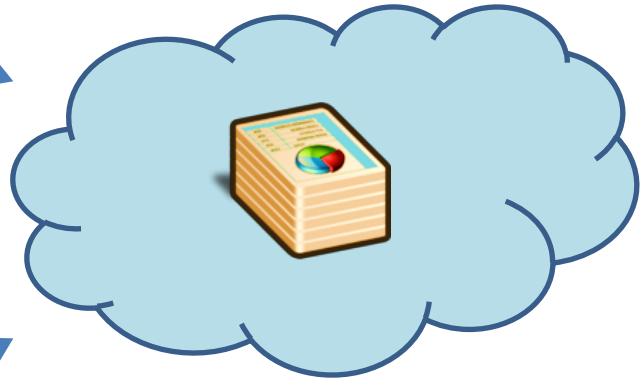
Direct Access
(from everywhere)



Synchronisatie

Alternatief voor directe toegang





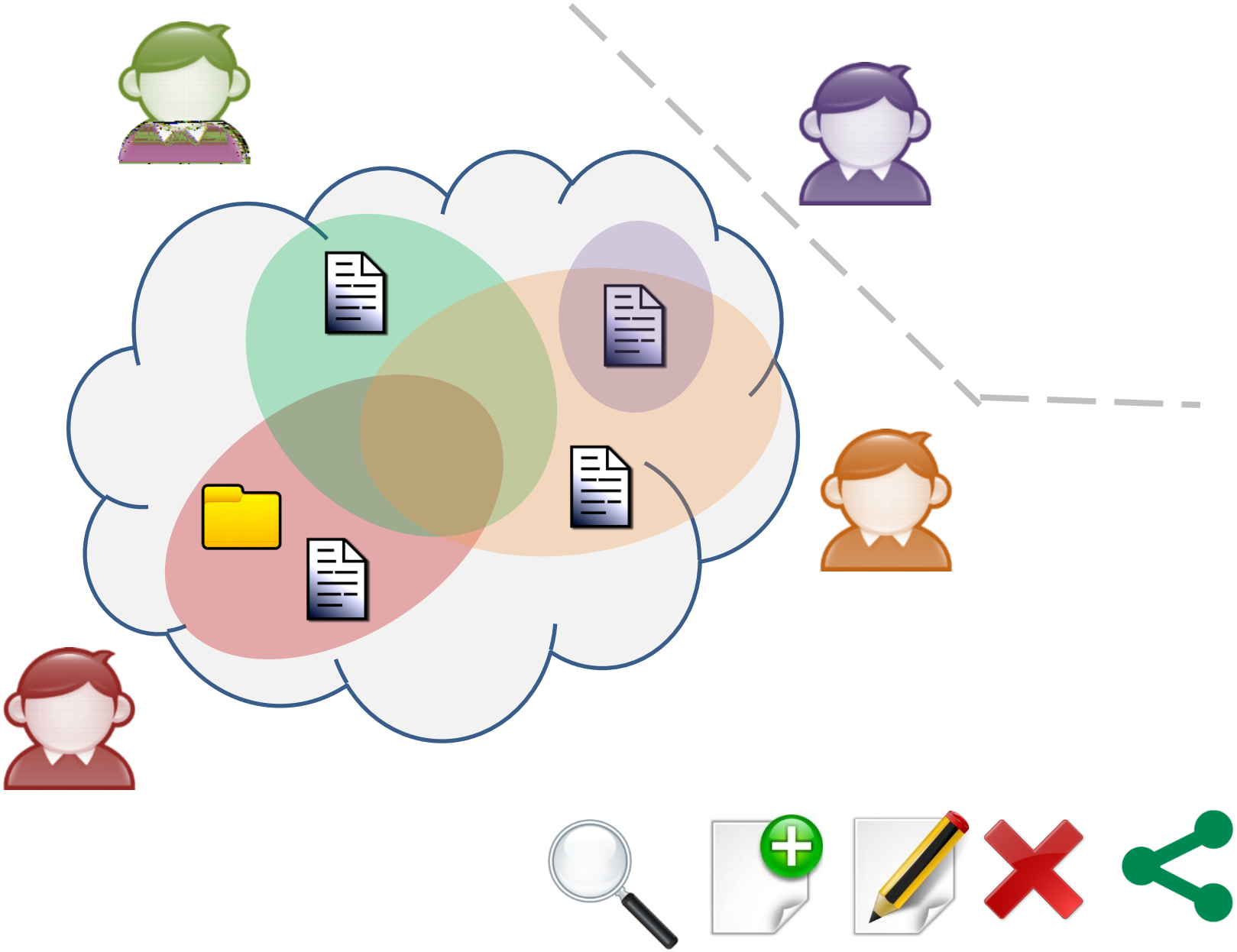
Directe toegang & Synchronisatie

vaak complementair

Synchronisatie

Directe toegang

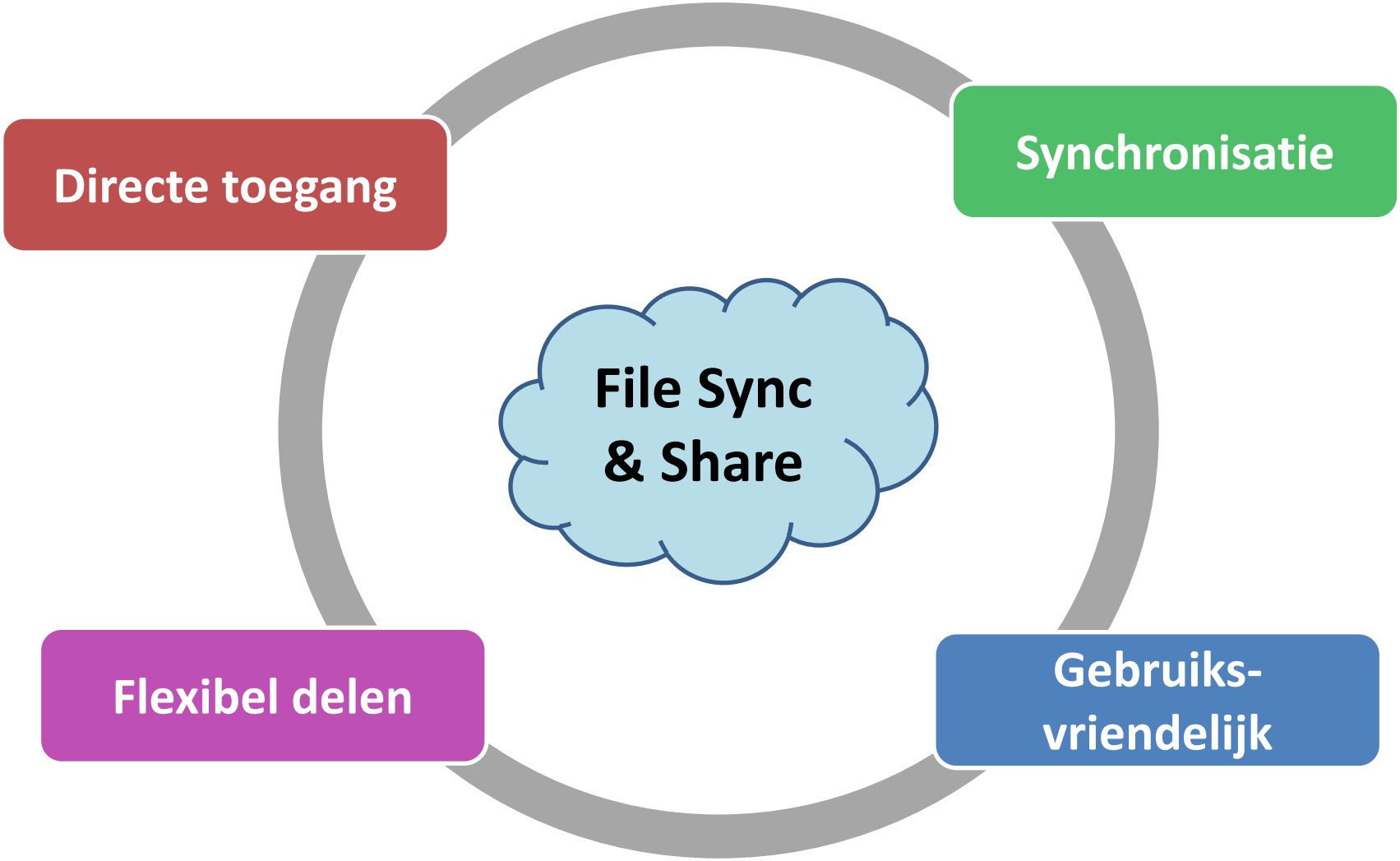
Delen



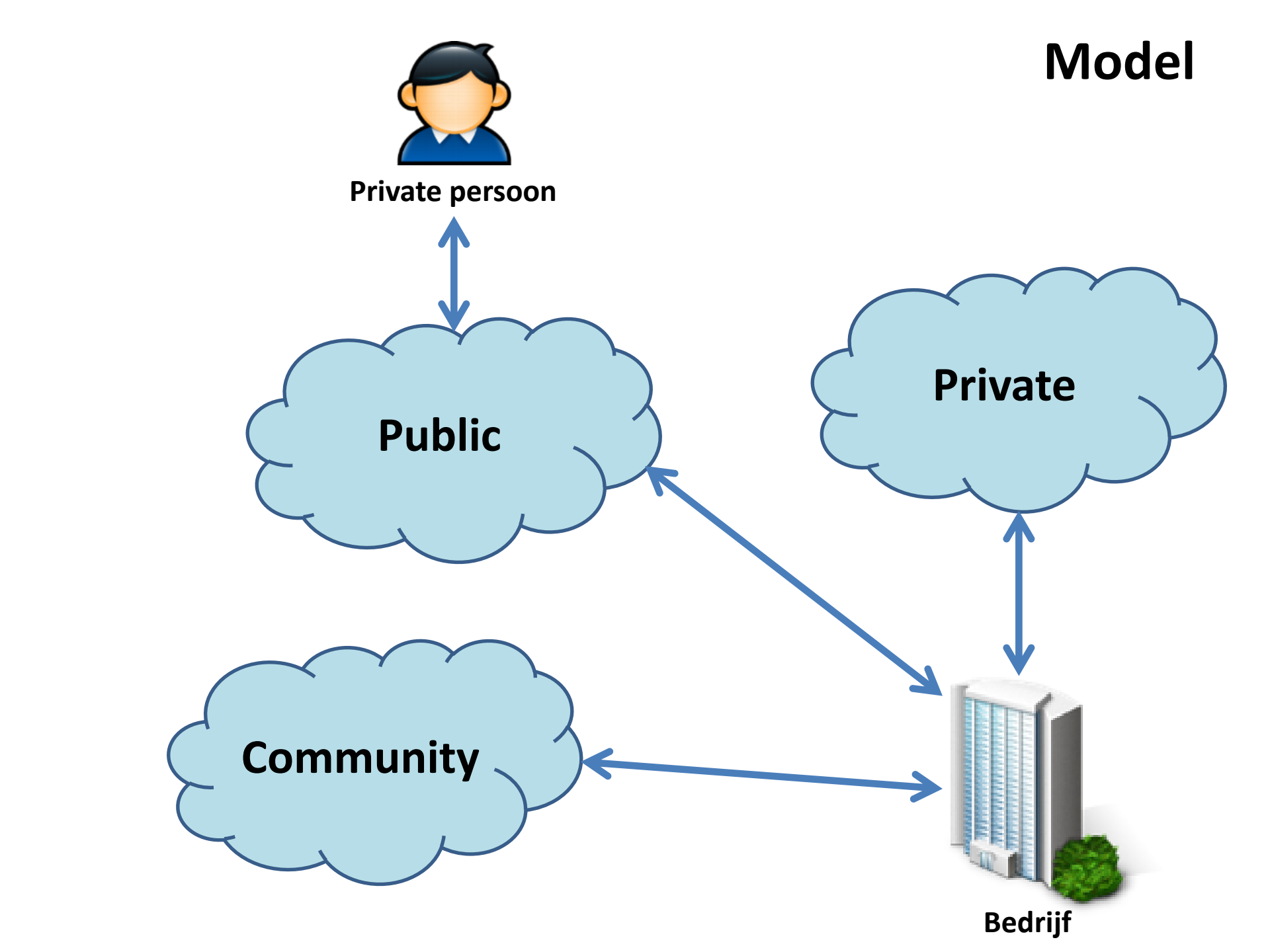
Gebruiksvriendelijk

Te vermijden….

Samengevat


Directe toegang
Synchronisatie
File Sync
& Share
Flexibel delen
Gebruiks-
vriendelijk

Model



File Sync & Share

Public Cloud

ShareFile
by CITRIX

amazon cloud drive

OneDrive

egnyte
HybridCloud

cubby
beta

Google Drive

Dropbox

box

syncplicity

huddle™

Smals
ICT for society

Gevaren

Data exfiltration

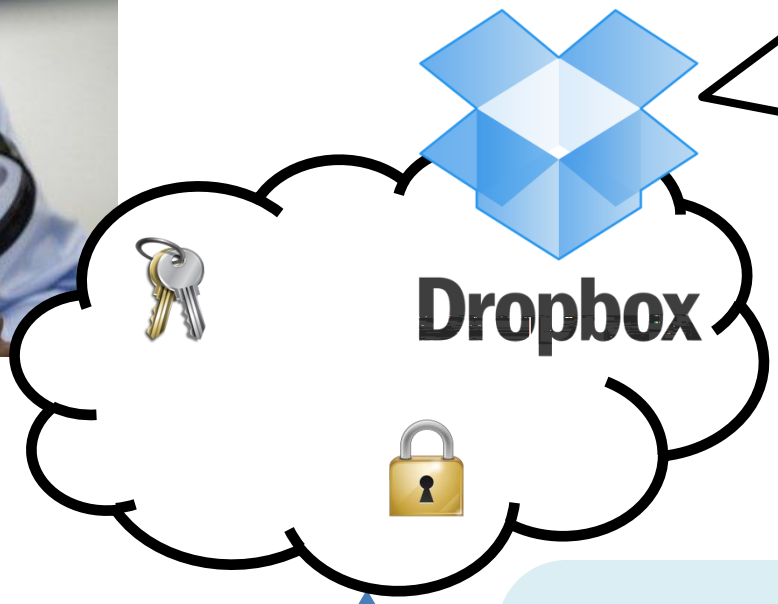
Import malware

Geen controle

« 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…



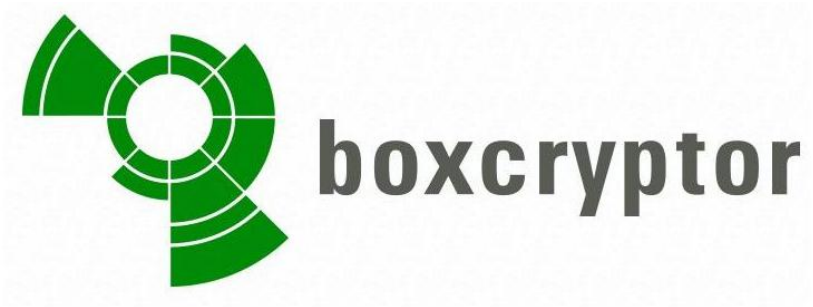
"Secure Sockets Layer (SSL) & AES-256 bit encryption. Privacy policy and procedures"

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

►► Niet voor gevoelige data ◄◄

Veelal gelijkaardig voor concurrenten in publieke cloud.

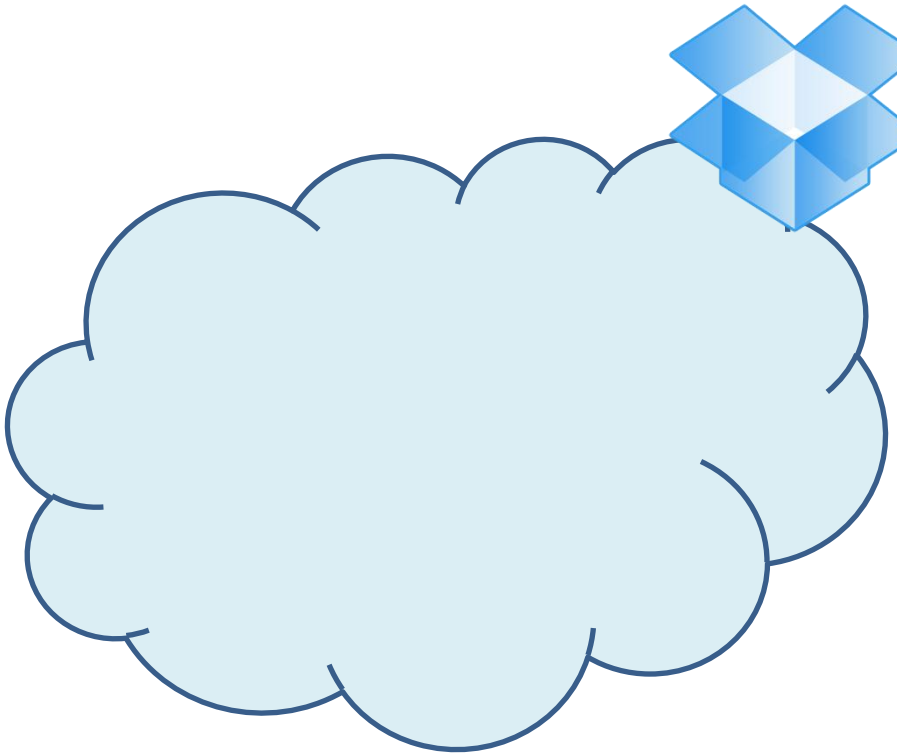
Op te lossen?

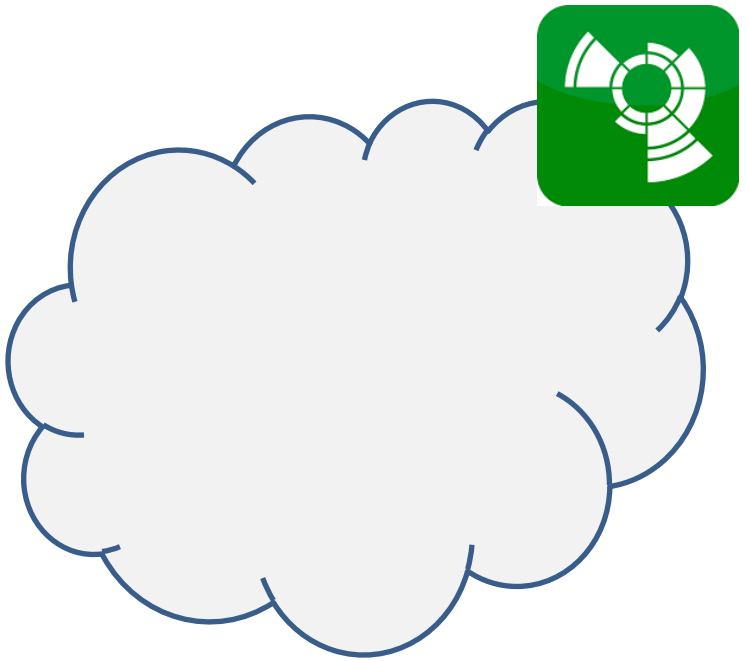


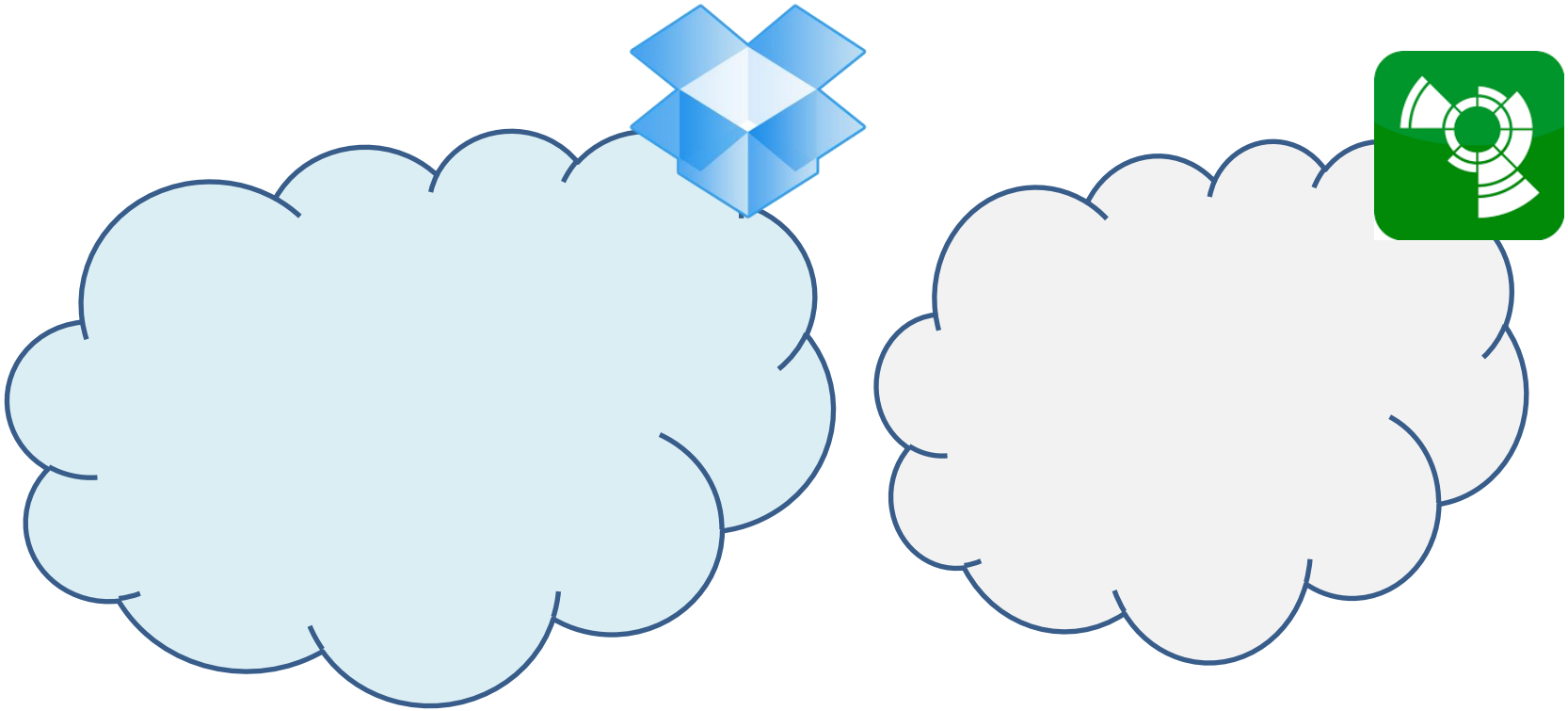
BoxCryptor
Classic

SafeMonk

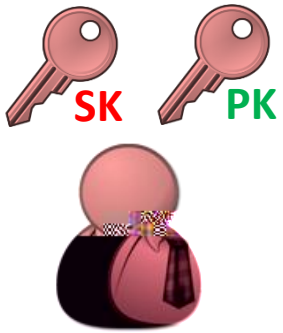
...

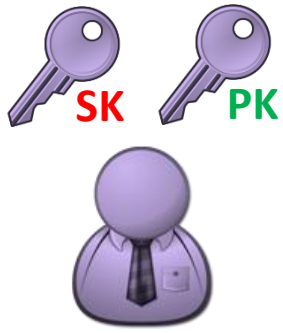


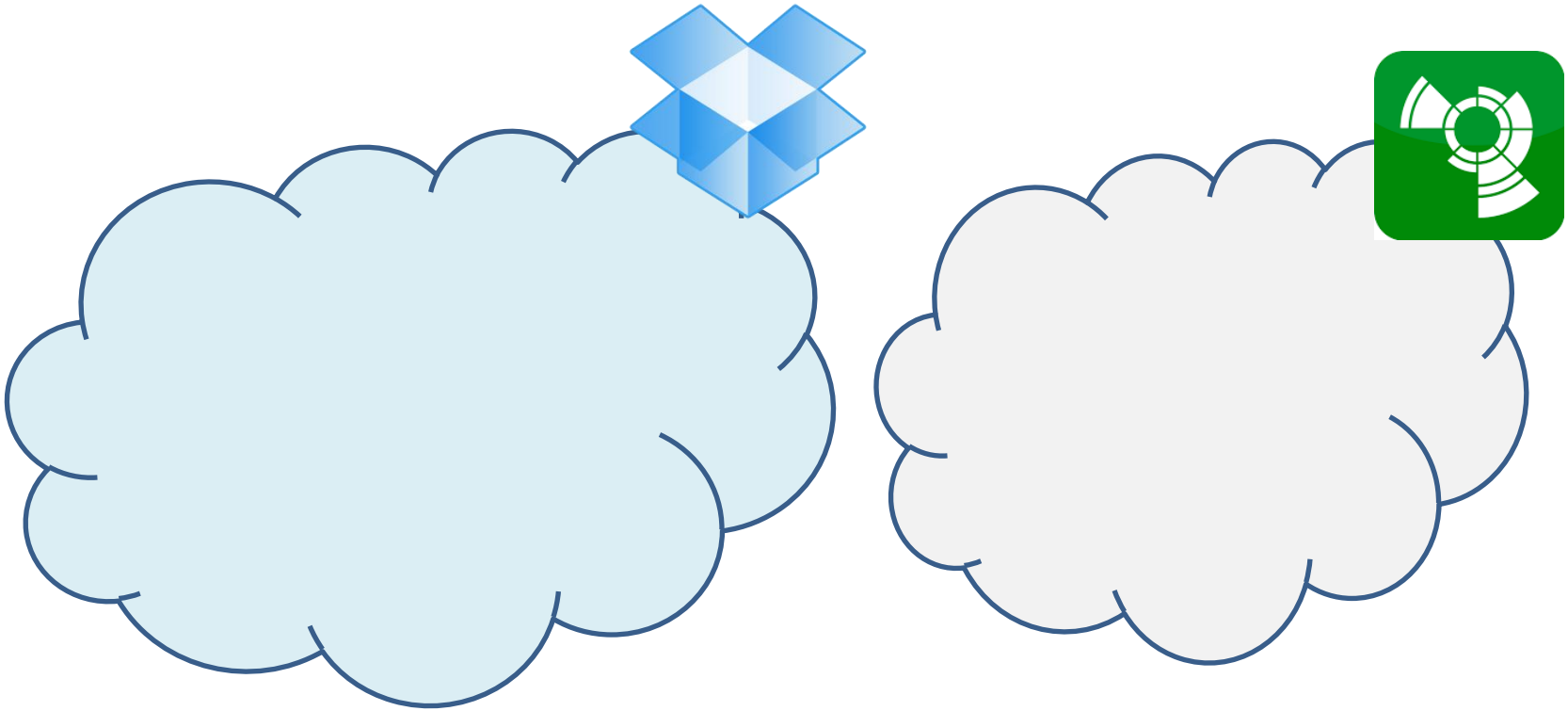




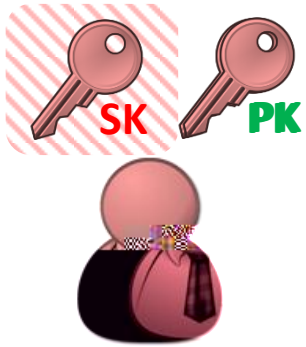
Initialisatie

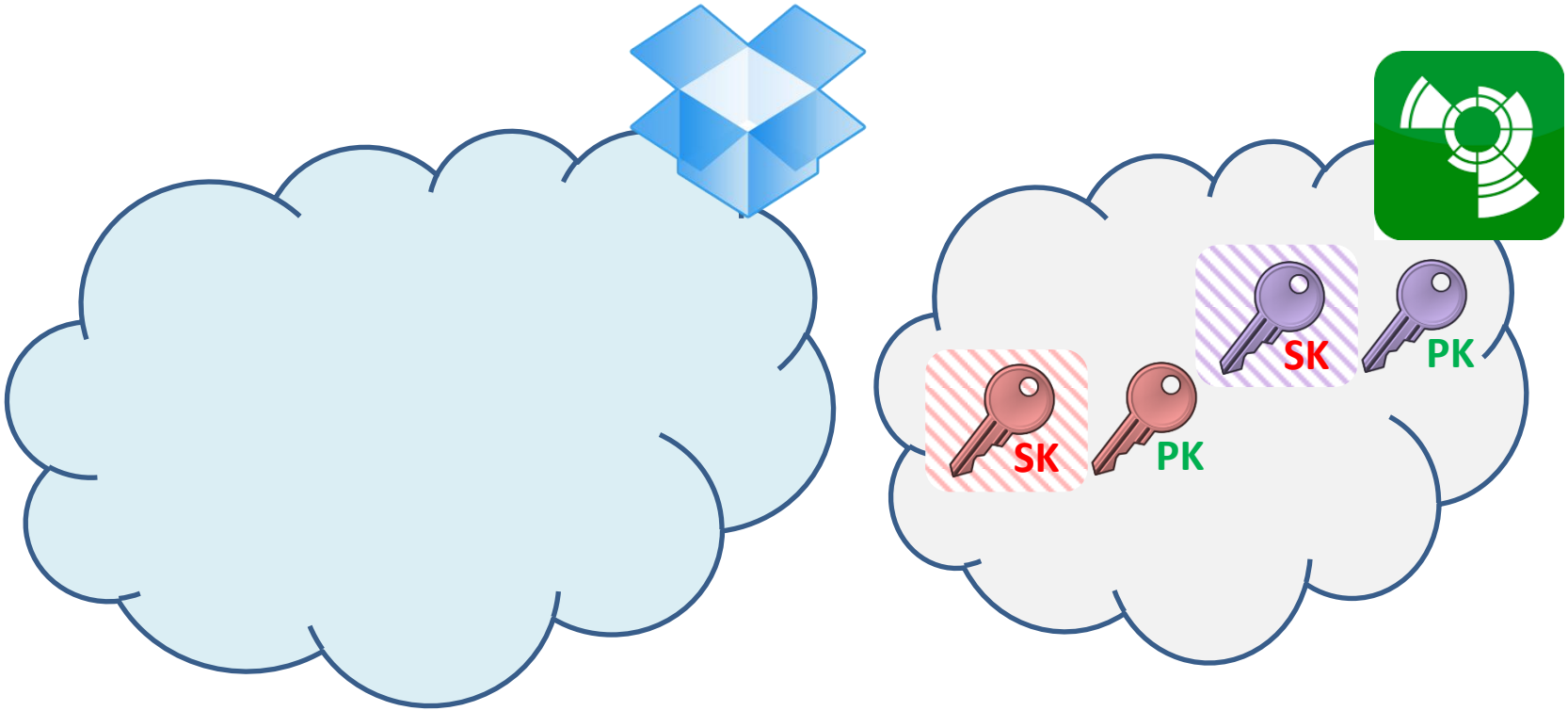




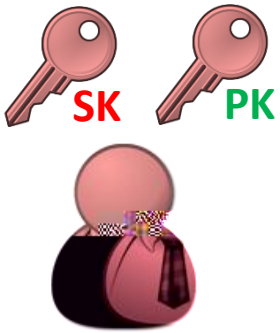


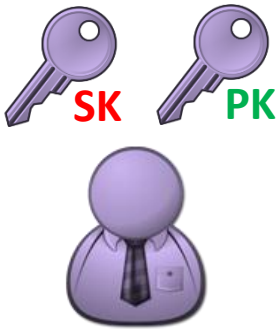
Initialisatie

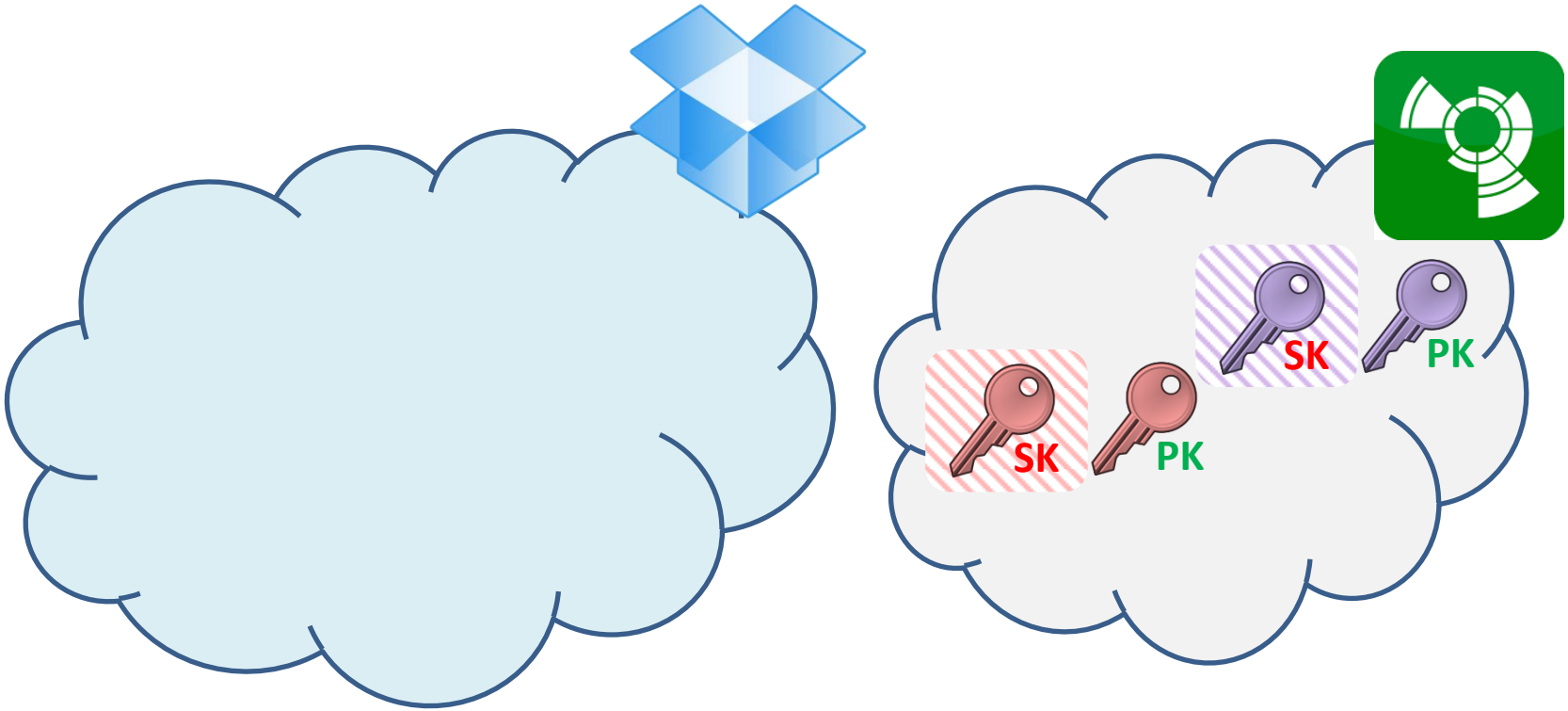




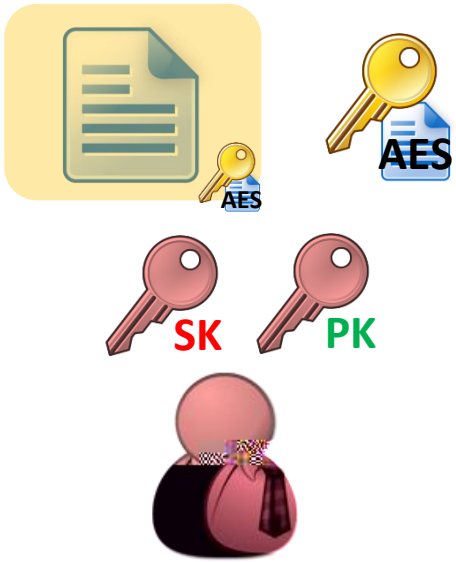
Uploaden bestand







Uploaden bestand



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	
Interne Bedrijfsgegevens	
Vertrouwelijke Bedrijfsgegevens	
Persoonsgegevens	
Sociale persoonsgegevens	
Medische persoonsgegevens	
Privé gegevens	

[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 vie 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 per soonsgegevens, ...). »*

- *« 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. »*

Algemene policy inzake het gebruik van e-mail, IMS, 2010, v0.30

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