Smals
ICT for society

Strong Mobile Authentication

Bert Vanhalst
Smals Research
www.smalsresearch.be

Maart 2015

Smals
ICT for society

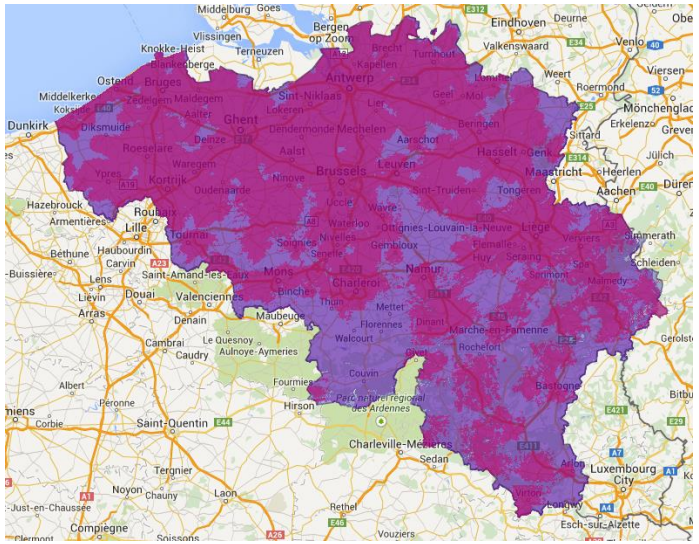
Agenda

1. Inleiding
2. CSAM
3. PAUZE  
4. Concept
5. Marktevoluties
6. Conclusies

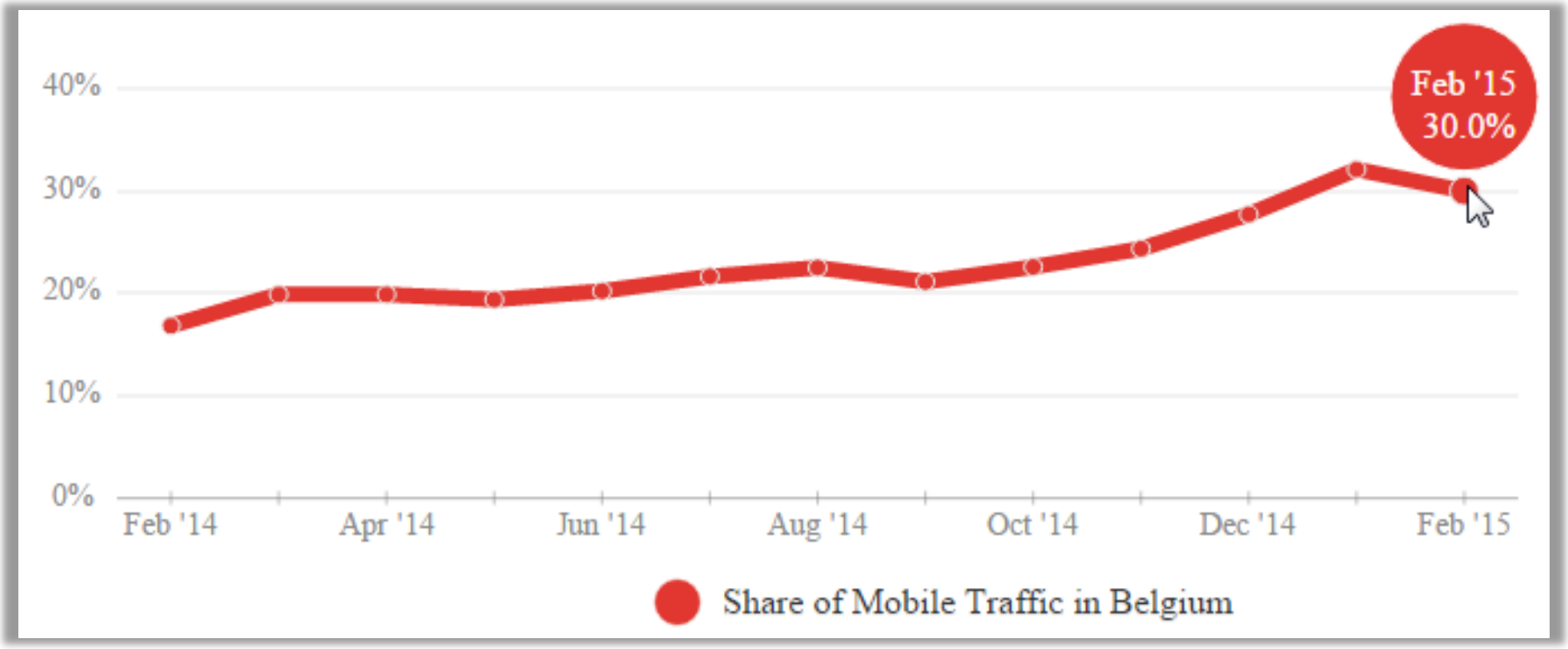
Inleiding

Waarom mobile

- Goedkoper
- Gebruiksvriendelijker
- Sneller (4g)
- Overal beschikbaar
- Apps apps apps



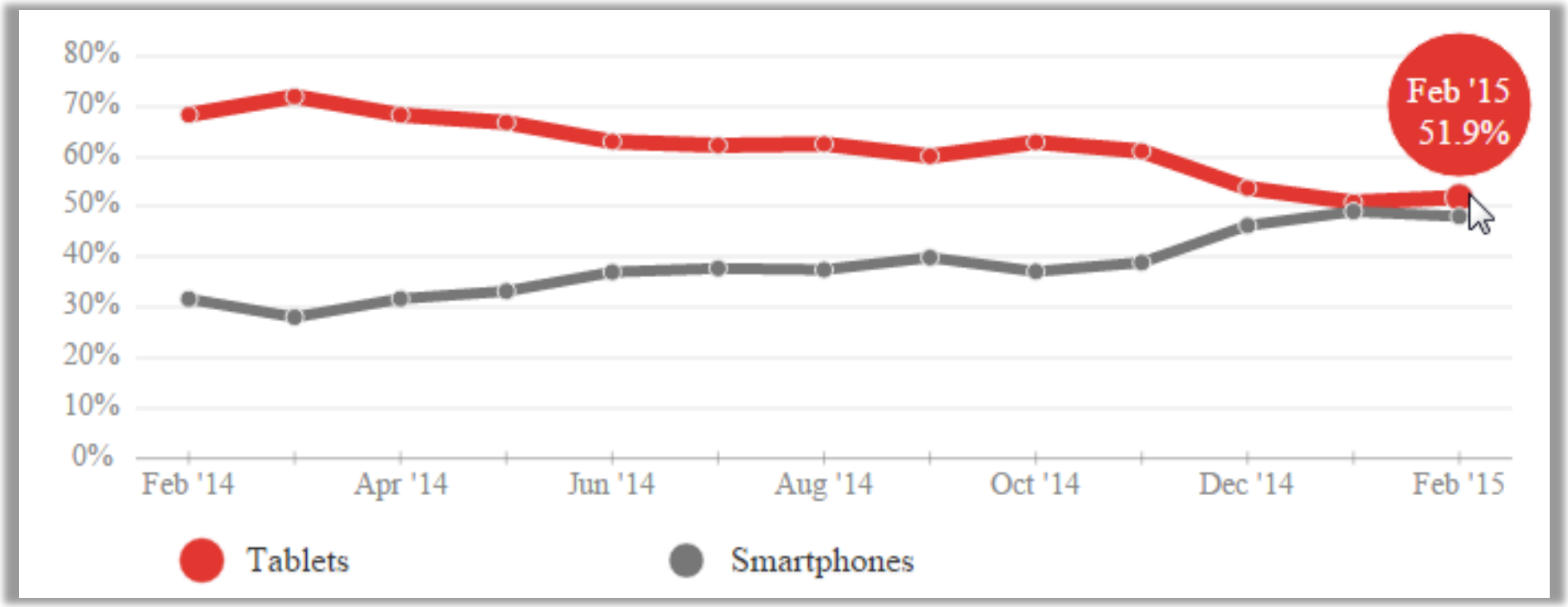
Mobiel dataverkeer



Bron: www.howwebrowse.be

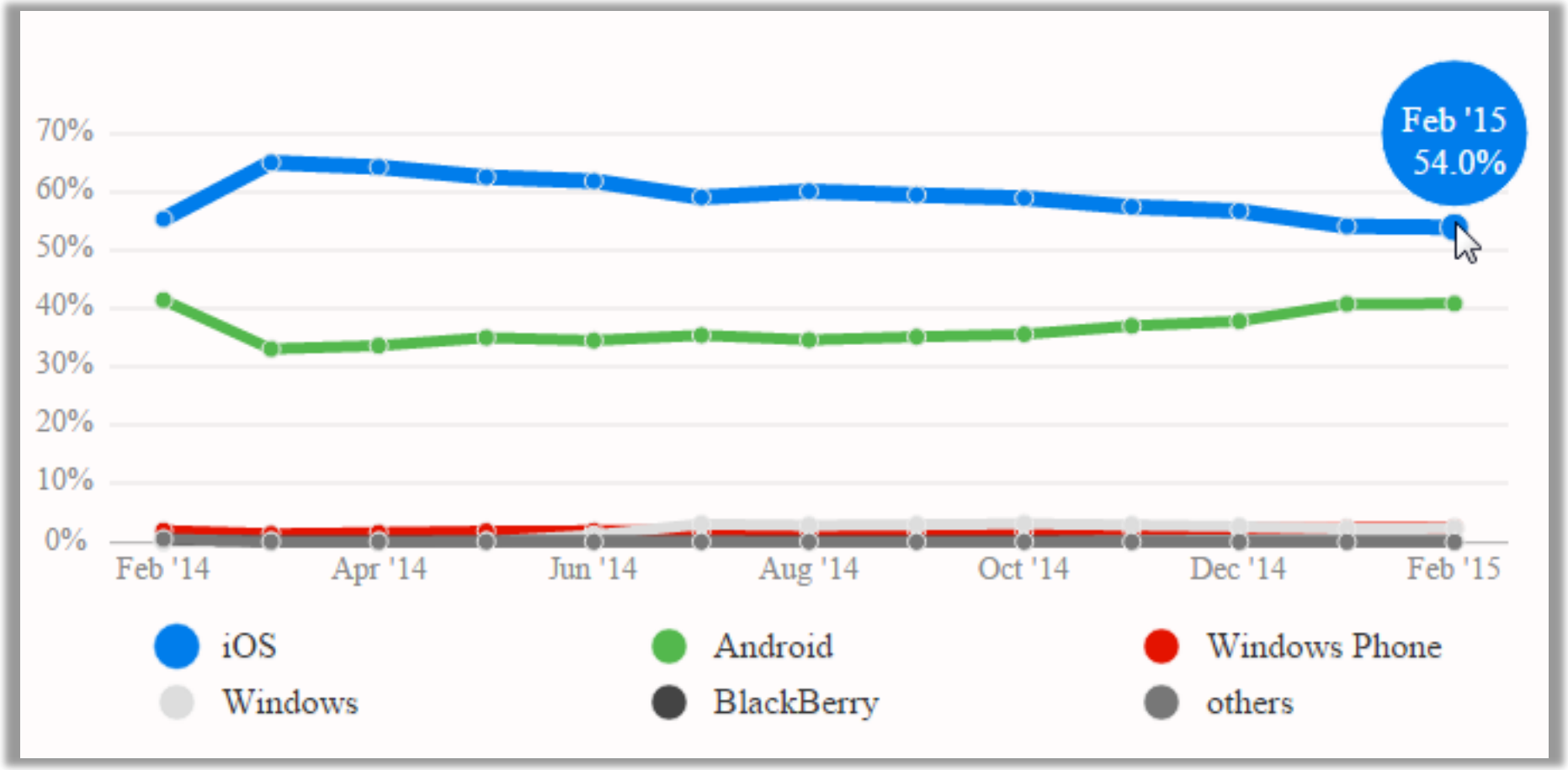
Smals
ICT for society

Tablets versus smartphones



Bron: www.howwebrowse.be

Marktaandeel OS'en



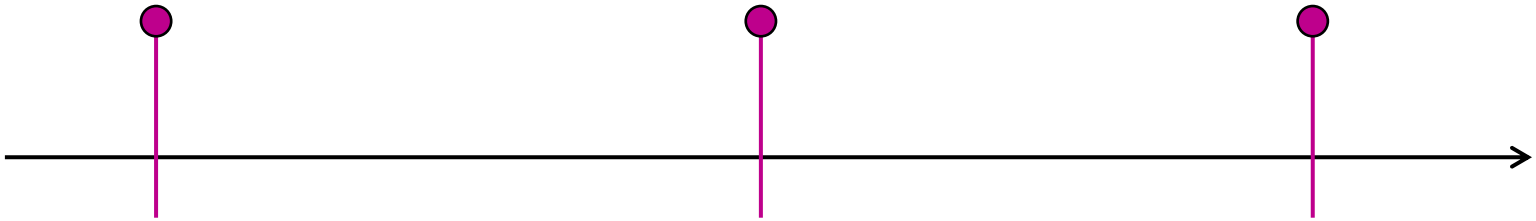
Bron: www.howwebrowse.be

Mobiel wint aan belang

Email, surfen

Mobile banking
en tal van
andere apps

Boom verwacht in
mhealth apps
(telemonitoring, …)



Gisteren

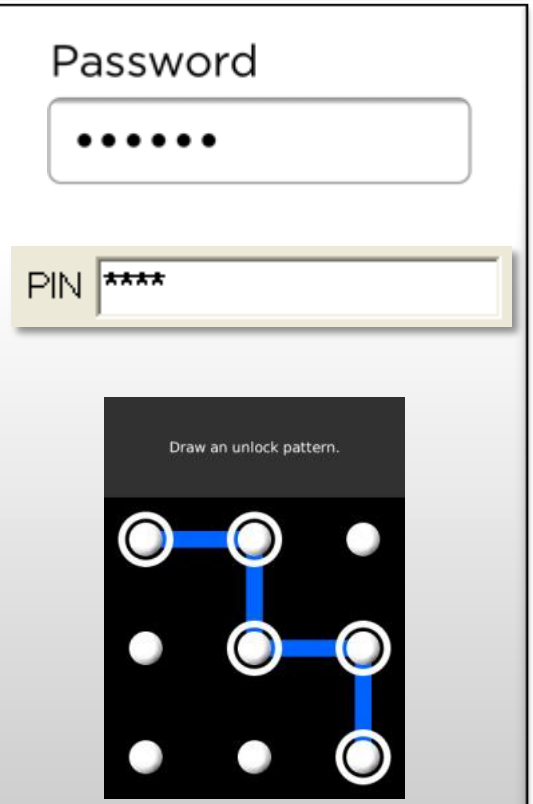
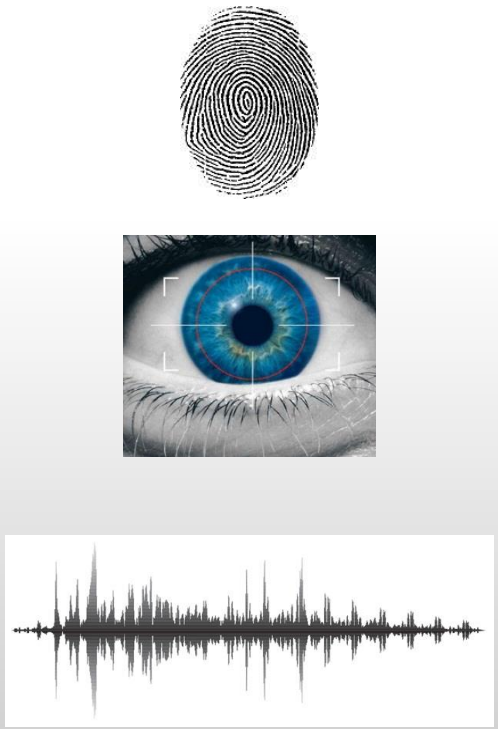
Vandaag

Morgen

Bron: http://www.tijd.be/dossier/nieuwetijden/De_Block_maakt_geneeskunde_op_afstand_mogelijk.9610533-7973.art

Smals
ICT for society

Authenticatie-factoren

Kennis Iets wat je weet	**Bezit** Iets wat je hebt	**Biometrie** Iets wat je bent
		

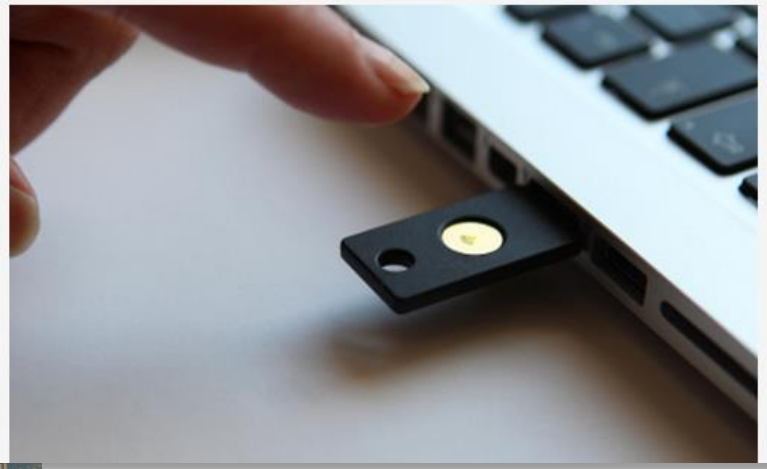
Yubikey – demo

https://demo.yubico.com/start/otp/neo

yubico

Try Out Your YubiKey NEO

YubiKey



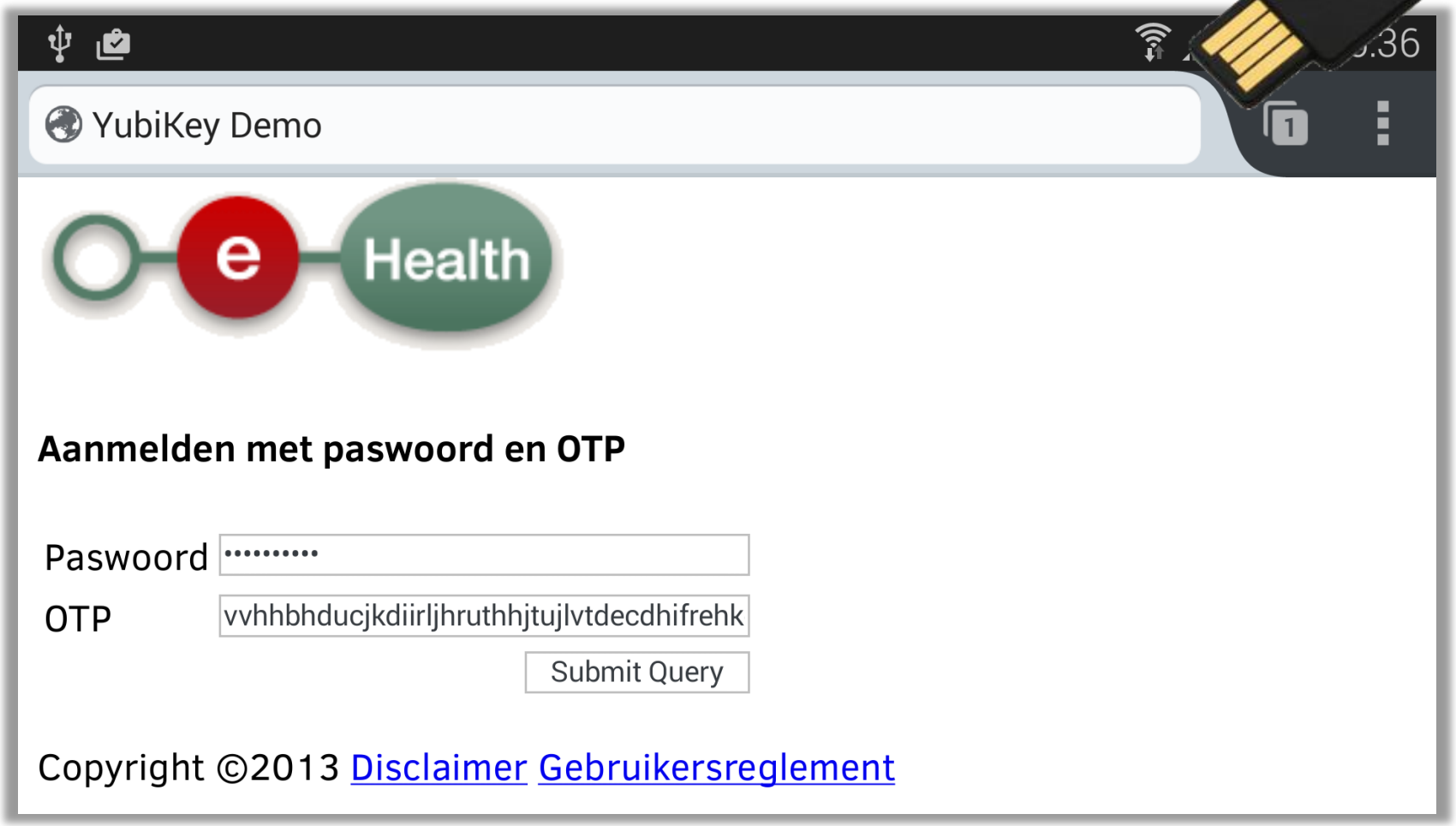
Demo YubiKey for single-factor authentication

1. **Insert your YubiKey into a USB port**
2. **Click in the YubiKey field, and touch the YubiKey button**

Mac users

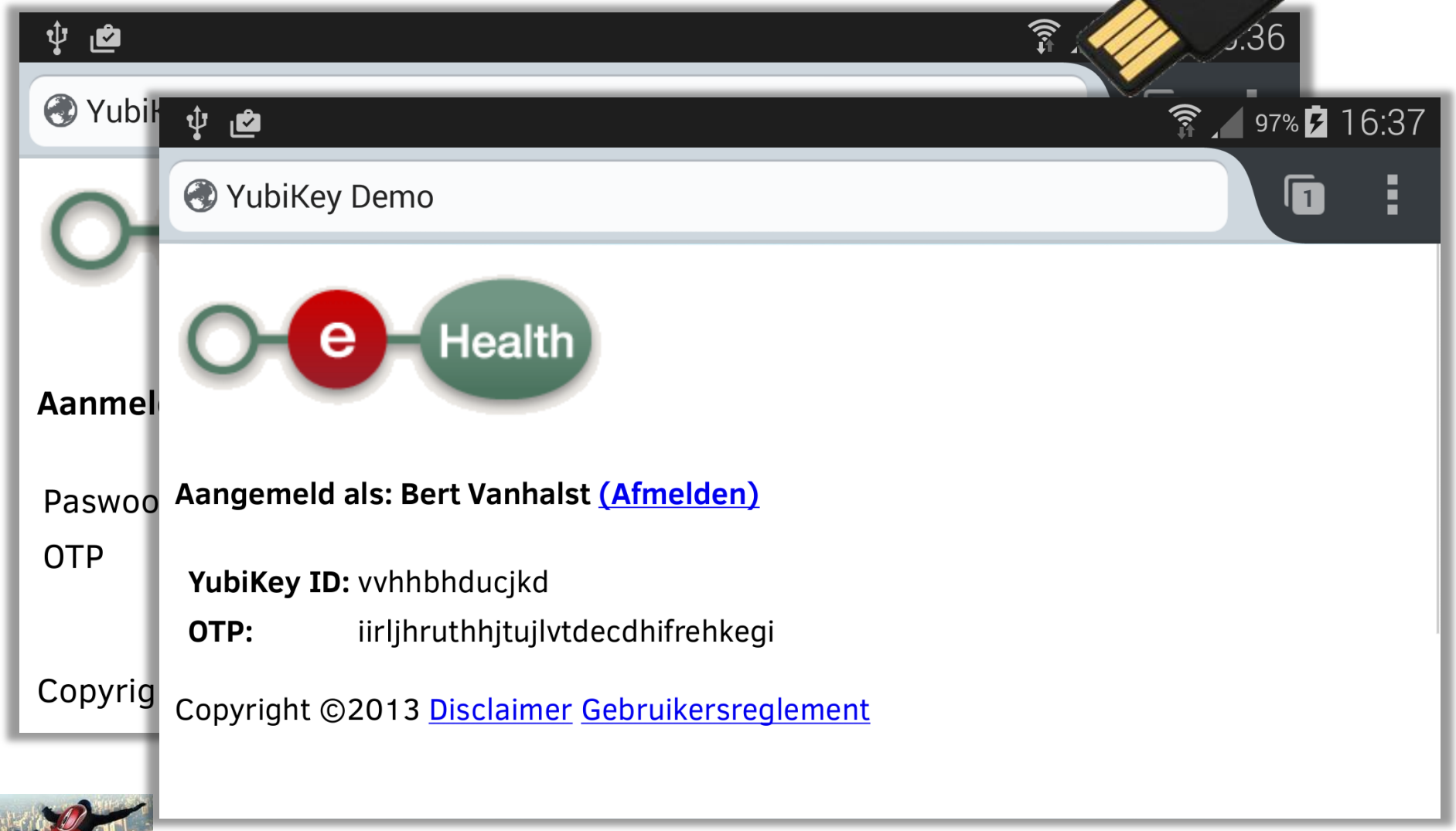
YubiKey NEO product page
YubiKey applications and use cases

Yubikey – demo



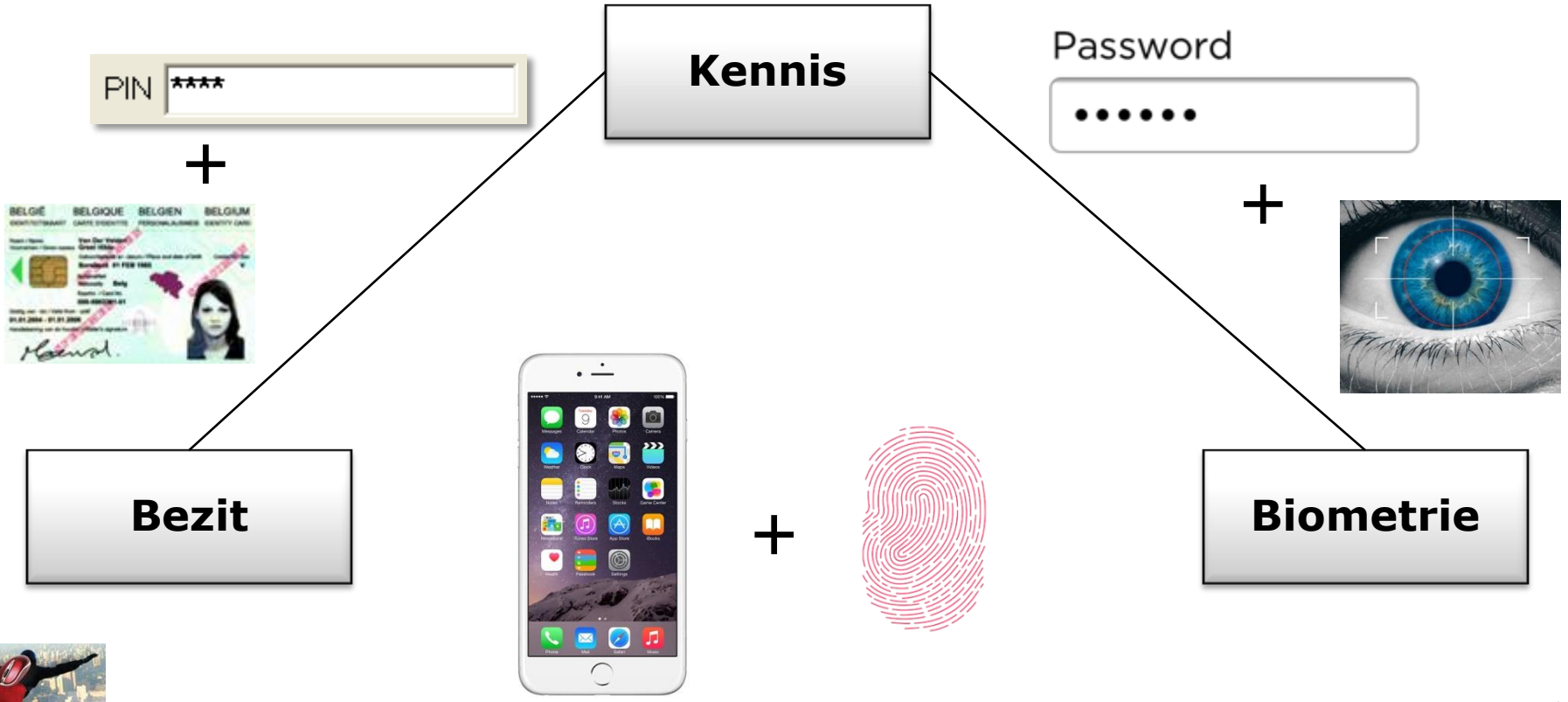
Smals
ICT for society

Yubikey – demo



Sterke authenticatie

Sterke authenticatie = combinatie van minstens 2 factoren



Authenticatie policy

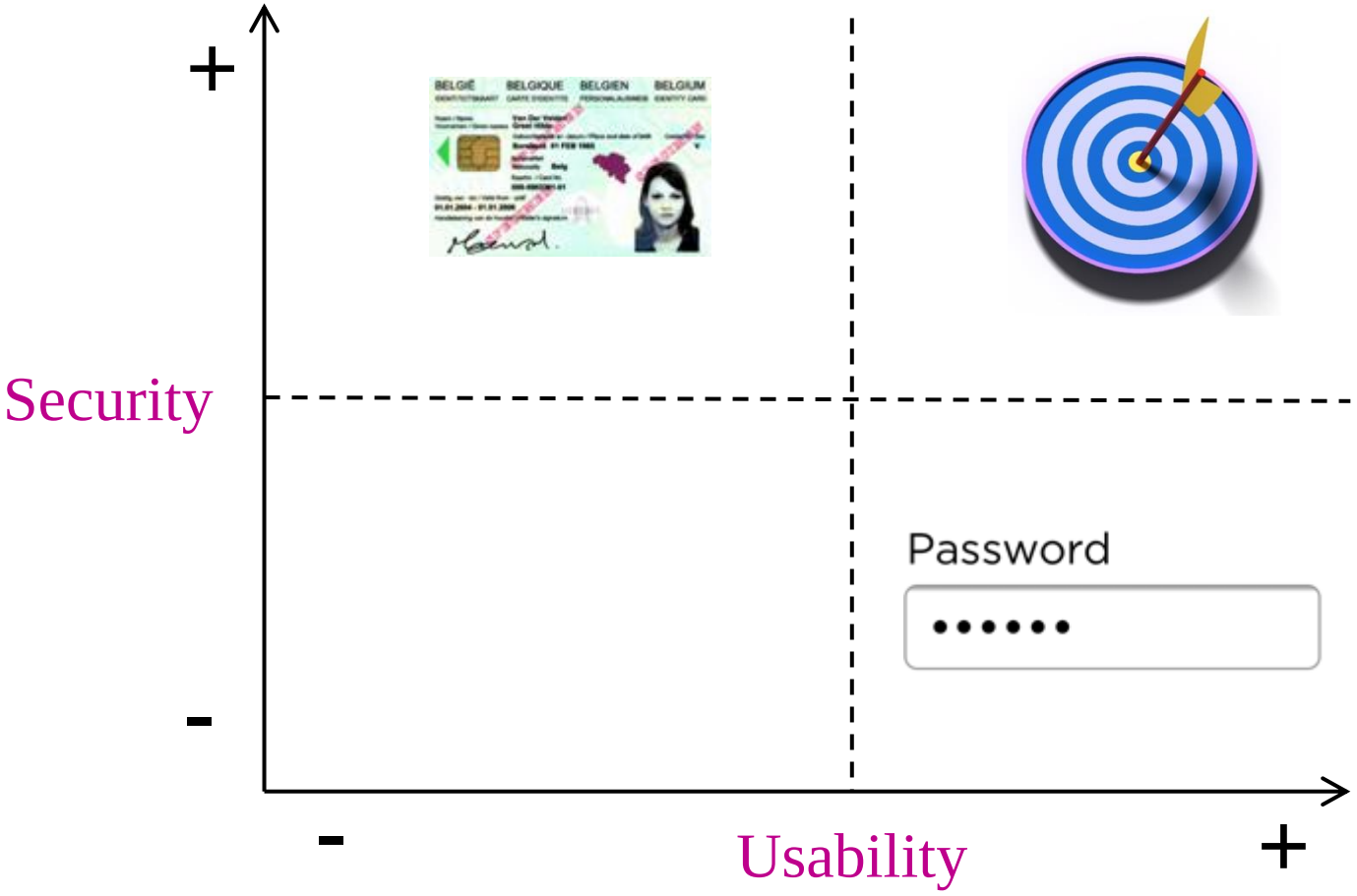
- Vandaag: per toepassing wordt beslist welke authenticatiemiddelen toegelaten worden
- In de toekomst: mapping tussen categorie van de verwerkte gegevens en het authenticatieniveau?

eID + PIN = geprefereerd authenticatiemiddel

Probleemstelling

- Huidige authenticatiemiddelen onvoldoende aangepast aan mobiele context
- eID slechts beperkt compatibel met mobiele toestellen
- Afweging veiligheidsniveau vs. gebruiksgemak
  - Ofwel inboeten op gebruiksgemak (bvb. eID met externe kaartlezer)
  - Ofwel inboeten op veiligheidsniveau (bvb. wachtwoord)

Security vs usability



Gebruiksvriendelijke én veilige authenticatie op mobiele toestellen?


muni
PRESS BAR
TO OPEN
DOOR

gemeenschappelijk

CSAM is de **toegangspoort** tot de **onlinediensten** van de overheid.

CSAM omvat gemeenschappelijke afspraken, regels en diensten voor **identificatie**, **authenticatie**, **autorisatie** en **toegangsbeheer**.

herkenbaar

Maak u het leven gemakkelijker met CSAM. Elke onlinedienst van de overheid volgt dezelfde authenticatieprocedure. U vindt een vertrouwde en betrouwbare omgeving terug telkens u inlogt, toegangsbeheerders aanstelt enzovoort.

beveiligd

CSAM zorgt ervoor dat iedereen dezelfde regels volgt en gebruik maakt van generieke diensten. Zo garandeert het systeem een hoger en constant **veiligheidsniveau**. Bovendien zijn uw inloggegevens nooit zichtbaar voor de toepassingen.

CSAM

CSAM

- CSAM is een geheel van afspraken om het identiteits- en toegangsbeheer binnen het e-government te organiseren
- CSAM diensten
  - Federal Authentication Service (FAS): identificatie en authenticatie van personen
  - Beheer van Toegangsbeheerders (BTB): structureren van toegangsbeheer binnen een onderneming

https://www.csam.be/

Huidige authenticatiemogelijkheden

Sterk

Aanmelden met eID (Burger)

Om je aan te melden met je eID, **steek je elektronische identiteitskaart, elektronische vreemdelingenkaart of kids-ID in de kaartlezer** en druk op de Verdergaan-knop hieronder. Geef je PIN-code in wanneer daarom gevraagd wordt.

Verdergaan

Stap 2

Aanmelden met eenmalig wachtwoord

SMS

Vul hieronder het eenmalig wachtwoord in dat je ontvangt op je gsm. Om veiligheidsredenen blijft dat eenmalig wachtwoord slechts 5 minuten geldig na ontvangst.

Vul je eenmalig wachtwoord in

Verdergaan

Aanmelden met een commercieel certificaat

Om je aan te melden met een commercieel certificaat, zorg ervoor dat het certificaat is opgeladen in je internet browser en klik op **Verdergaan**.

Verdergaan

Aanmelden met gebruikersnaam en wachtwoord in eigen naam

Vul hieronder je gebruikersnaam en wachtwoord in. **Opgelet**, indien je je gebruikersnaam en/of wachtwoord niet meer kent, dien je met je eID in te loggen op Mijn eGov-profiel om vervolgens een nieuw gebruikersnaam en/of wachtwoord in te stellen.

Gebruikersnaam

Wachtwoord

Verdergaan

Zwak

eID bootstrap

- eID-bootstrap principe: aanvragen van authenticatiemiddel op basis van eID (in connected mode)
- Beheer aanmeldmogelijkheden via de self-management application van Mijn e-Gov Profiel

  www.csam.be/myprofile

CSAM

Mijn eGov-profiel

Mijn online profiel bij de overheid

Bert Vanhalst | Afmelden

Mijn identiteit | Mijn aanmeldmogelijkheden | Mijn roltoekenningen

Mijn aanmeldmogelijkheden

Hier beheer je alle aanmeldmogelijkheden die je toegang kunnen geven tot eGov-applicaties, zoals token, gebruikersnaam en wachtwoord, enz.

Standaard aanmeldmogelijkheden

eID / elektronische vreemdelingenkaart / Kids-ID	Deactiveren via DocStop
Burgertoken	Alleen deactiveren / Oud burgertoken deactiveren en nieuw aanvragen

Geavanceerde aanmeldmogelijkheden

Digitale certificaten (type x.509)	Beheren
Eenmalig wachtwoord via sms	Aanvragen

Ondersteunende aanmeldmogelijkheden

Gebruikersnaam en wachtwoord	Wijzigen / Deactiveren

Legende:

- Aanmeldmogelijkheid in je bezit
- Aanmeldmogelijkheid in aanvraag
- Aanmeldmogelijkheid niet in je bezit

Bruikbaarheid huidige authenticatiemiddelen bij webtoepassingen* op mobiele toestellen?

*Native apps: zie verder

Paswoord

- Zonder meer bruikbaar op mobiele toestellen
- Vb: aanmelden bij Student at Work
- Gebruiksvriendelijk…

  … maar niet zo veilig …

Het probleem met paswoorden

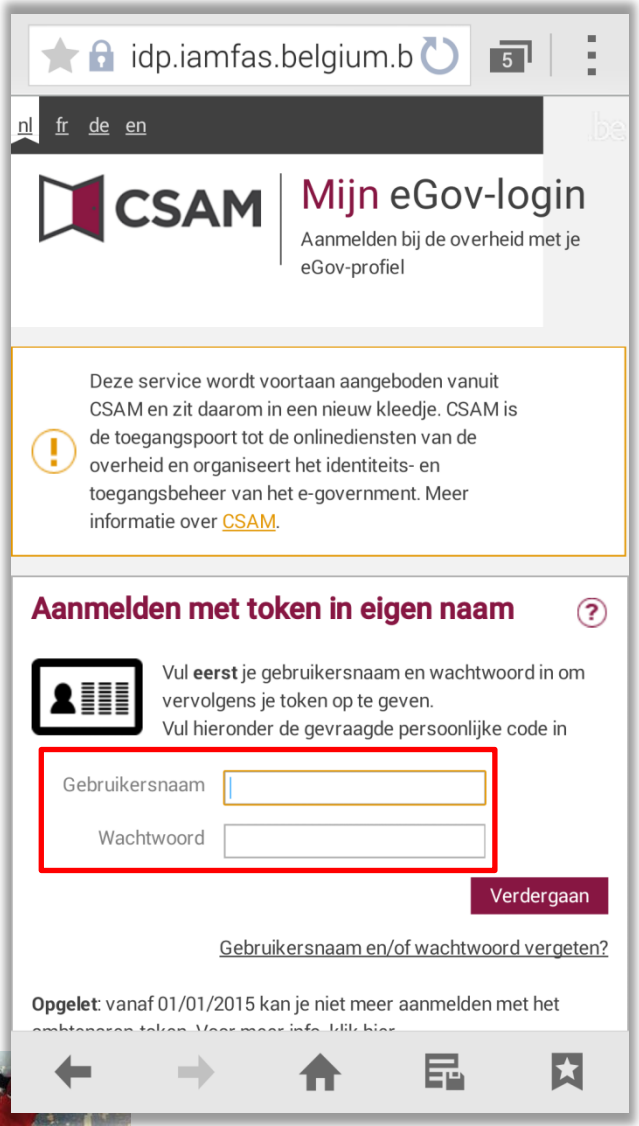
- We kiezen te eenvoudige paswoorden
- We schrijven ze gewoon neer
- We veranderen ze te weinig

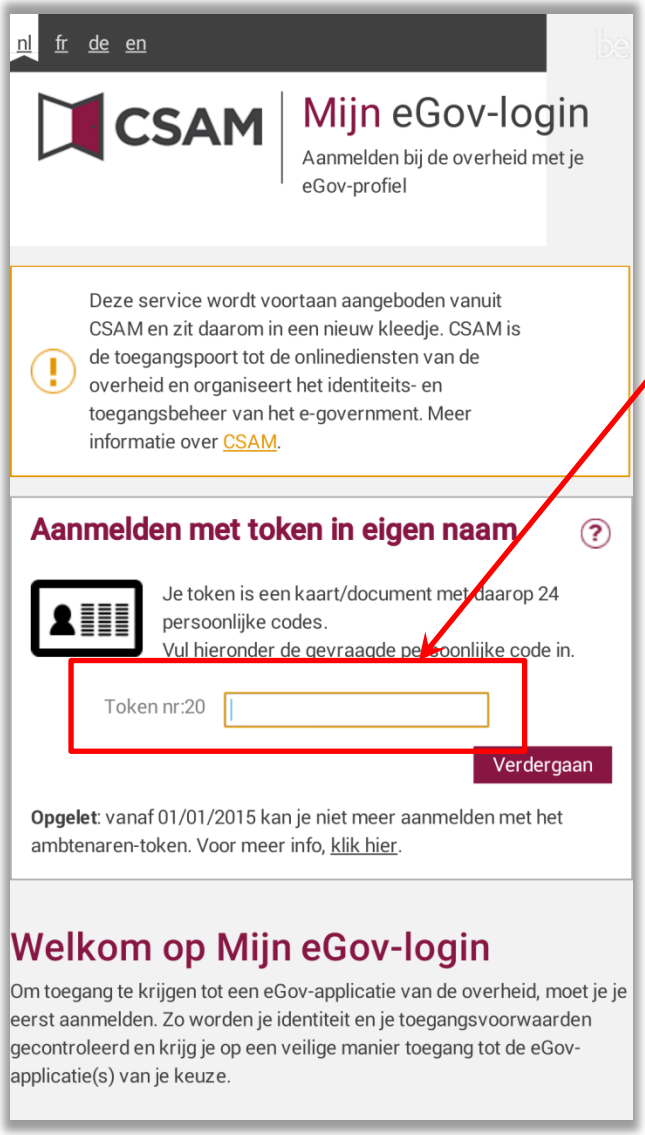
Het probleem met paswoorden

- Paswoorden worden gestolen
  - Shoulder surfing
  - Trojans
  - Phishing
  - Dictionary attacks
  - Key loggers

- Veel paswoorden onthouden is moeilijk, dus hergebruiken we ze voor verschillende diensten
  → grotere impact bij diefstal

Paswoord + token



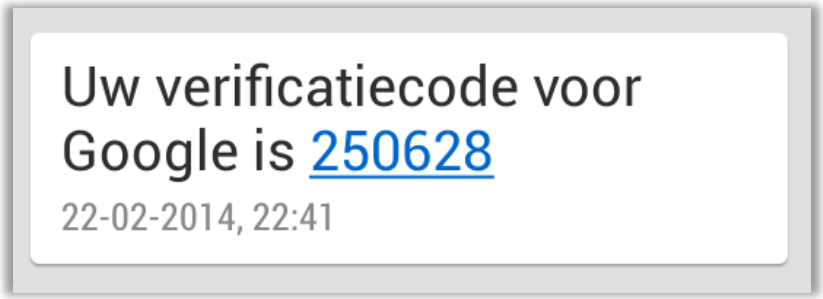


Paswoord + token

- Aanmelden:
  - Geef gebruikersnaam en wachtwoord in
  - Er wordt één van de 24 codes gevraagd
  - Geef de gevraagde code in in het aanmeldscherm
- Perfect bruikbaar op mobiele toestellen
- Iets minder gebruiksvriendelijk dan paswoord

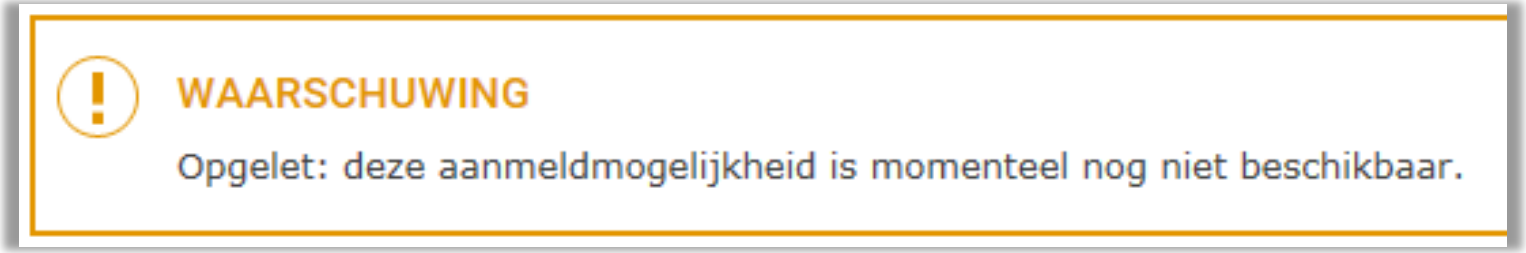
Paswoord + SMS OTP

- OTP = One Time Password
- Registreren van GSM-nummer in eGov profiel
- Aanmelden:
  - Vul gebruikersnaam en wachtwoord in
  - Eénmalige wachtwoord wordt verzonden naar geregistreerd GSM-nummer
  - Vul het éénmalig wachtwoord in in het aanmeldscherm



Paswoord + SMS OTP

- OTP kan je slechts één keer gebruiken en is tijdelijk geldig
- Perfect bruikbaar op mobiele toestellen
- Ietwat onhandig om OTP over te typen
- Kost verbonden aan versturen SMS'en



Paswoord + Digitaal Certificaat

- Vooraf:
  - Koppelen van commercieel certificaat aan eGov profiel
  - Installeren van certificaat op mobiel toestel: private sleutel doorsturen via mail (= onveilig)
- Aanmelden:
  - Ingeven gebruikersnaam en wachtwoord

Unconnected eID

Nog niet beschikbaar

- Mydigipass.com partner account
  - Koppeling tussen Mydigipass en CSAM
- Aanmelden
  - OTP op basis van eID en kaartlezer
  - OTP overtypen in aanmeldscherm
- Digipass 870
  - Verdeeld door Belfius of via online shop Vasco
  - Fungeert ook als connected eID-lezer

Aanmelden met eID (draadloos)

1. Kies in CSAM om aan te melden met Mydigipass partner account
   → doorverwijzing naar mydigipass.com
2. Geef email-adres in en éénmalig wachtwoord (gegeneerd met Digipass + eID + PIN)
3. Doorverwijzing naar toepassing na geslaagde aanmelding

nl fr de en .be

CSAM | My eGov Login

Login using my eGov profile with the government

fedict e-gov

Log in with your eID card as yourself

To log in with your eID **insert your electronic identity card, electronic foreigner card or Kids-ID into** below. Enter your PIN

Please find below authenticate:

Token as you
In order to a
Choose butt

Partner acco
MYDIGIPASS
eGov-applicaties van de overheid. Aanmelden gebeurt met je elektronische identiteitskaart (eID) met behulp van een **draadloze kaartlezer**.

Opgelet: gebruik de laatste versie van de eID software.

Hoe kan je MYDIGIPASS gebruiken?
Meer weten over de erkenning van aanmeldmogelijkheden?

Choose

Welcome to My eGov-login

In order to access an eGov application of the administration, you must first log in. That way, your identity and access conditions will be checked and you will be provided with secure access to eGov-application(s) of

use. If possible please
wn name or the name of

in options, please
in My eGov-profile.

e answer quickly by

Partner account

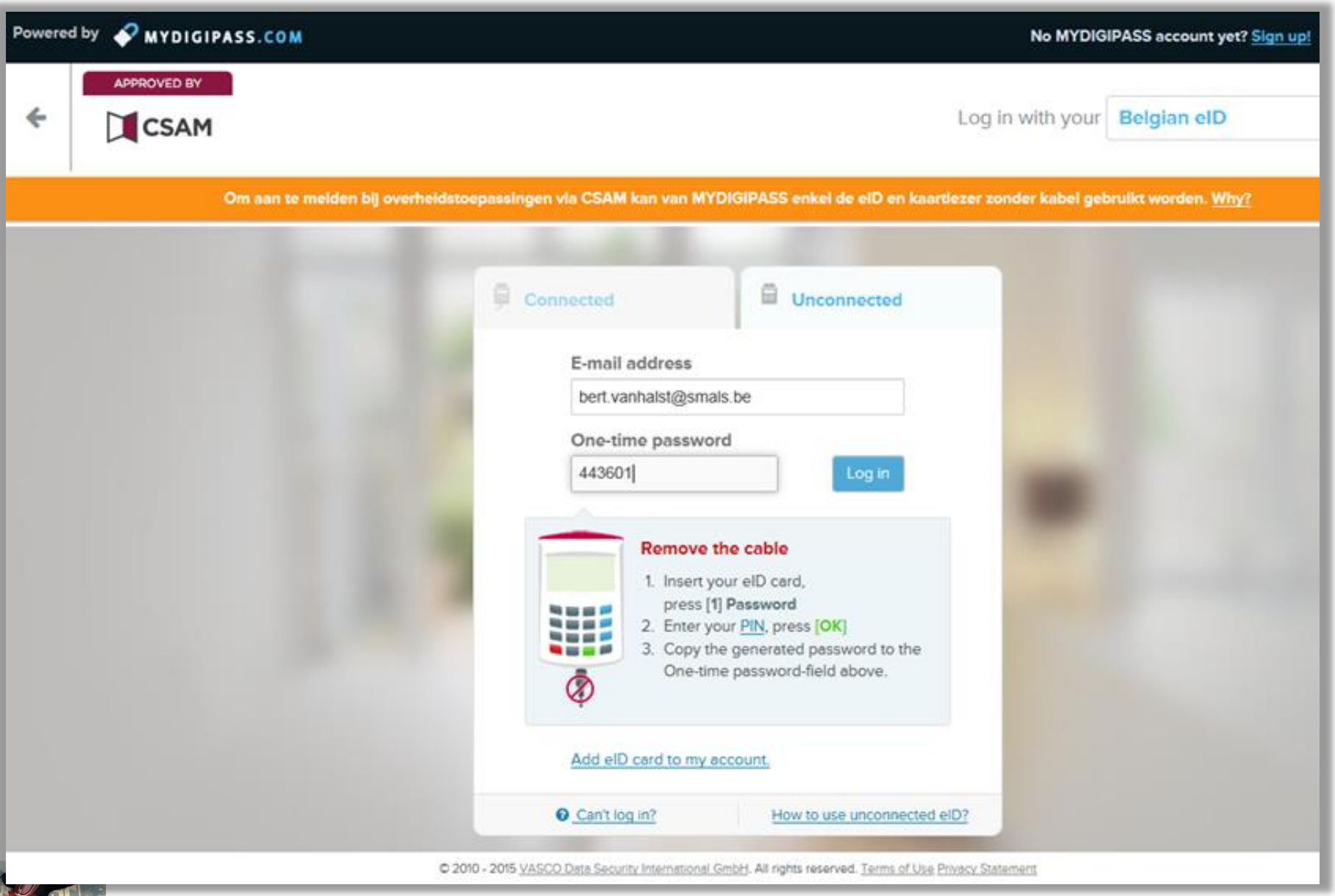
MYDIGIPASS is een erkende aanmeldmogelijkheid voor eGov-applicaties van de overheid. Aanmelden gebeurt met je elektronische identiteitskaart (eID) met behulp van een **draadloze kaartlezer**.

Opgelet: gebruik de laatste versie van de eID software.

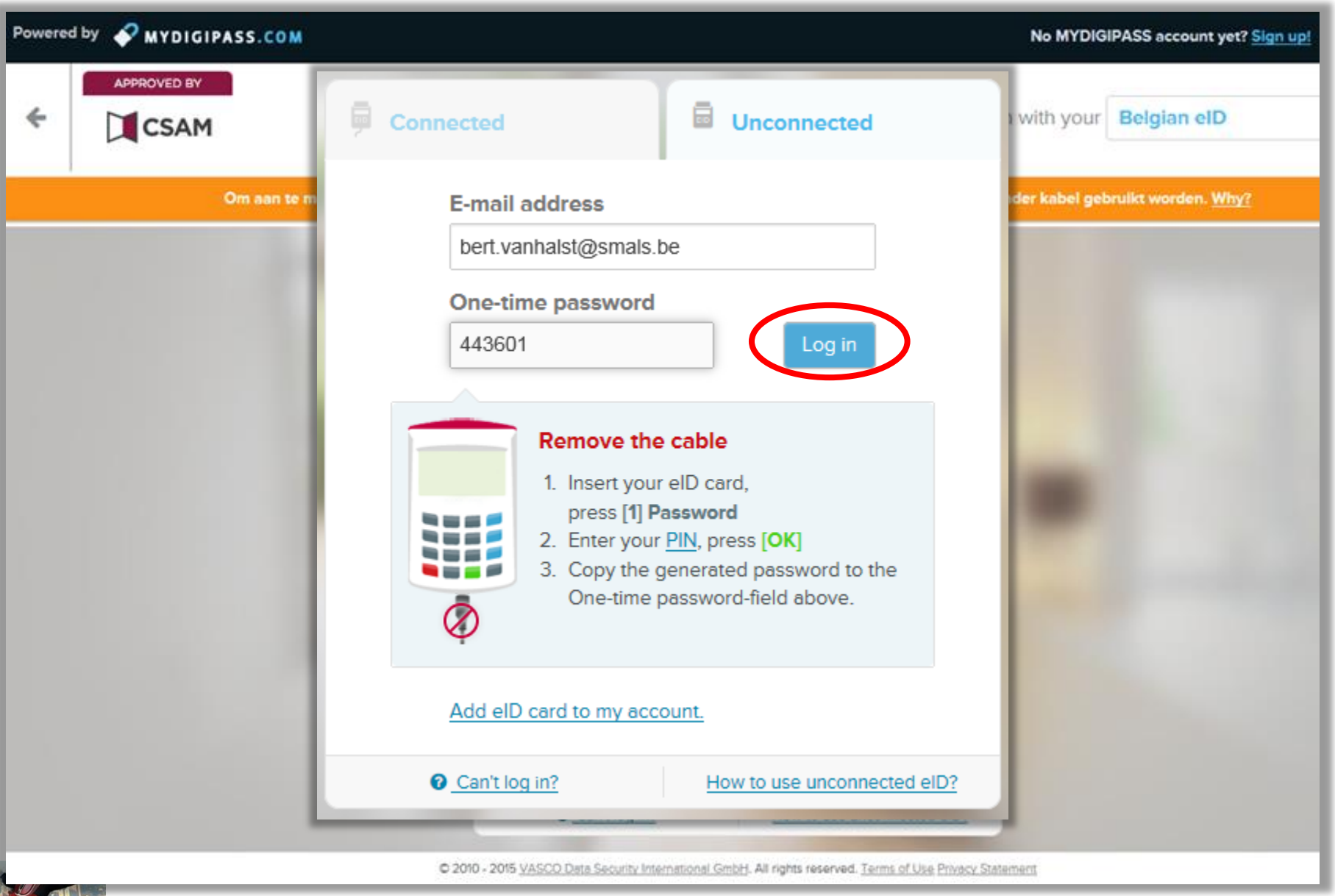
Hoe kan je MYDIGIPASS gebruiken?
Meer weten over de erkenning van aanmeldmogelijkheden?

Choose

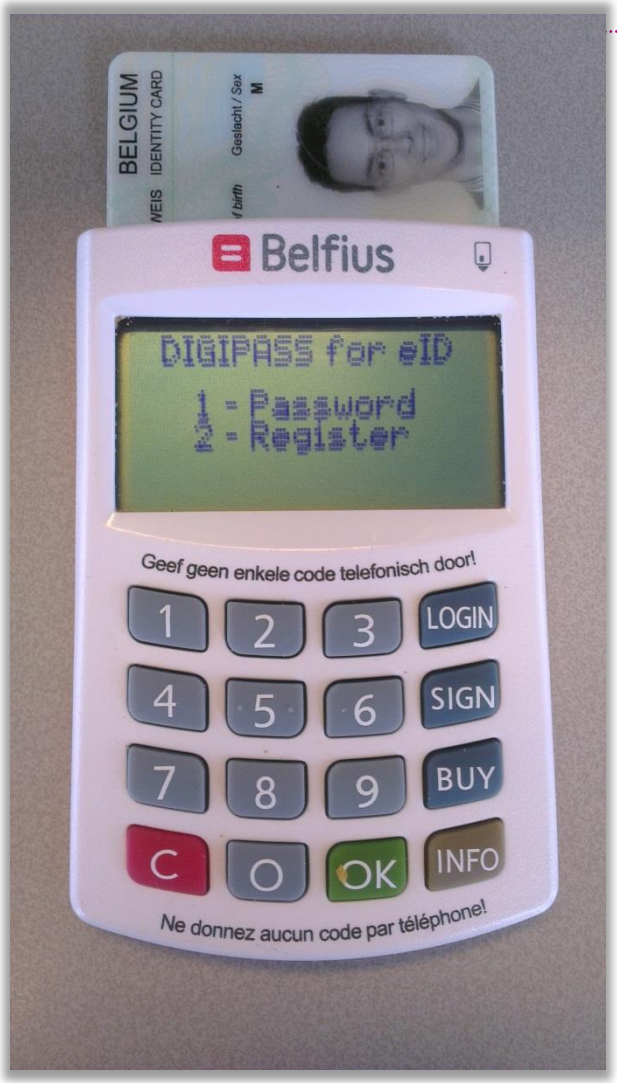
Aanmelden bij MDP.COM

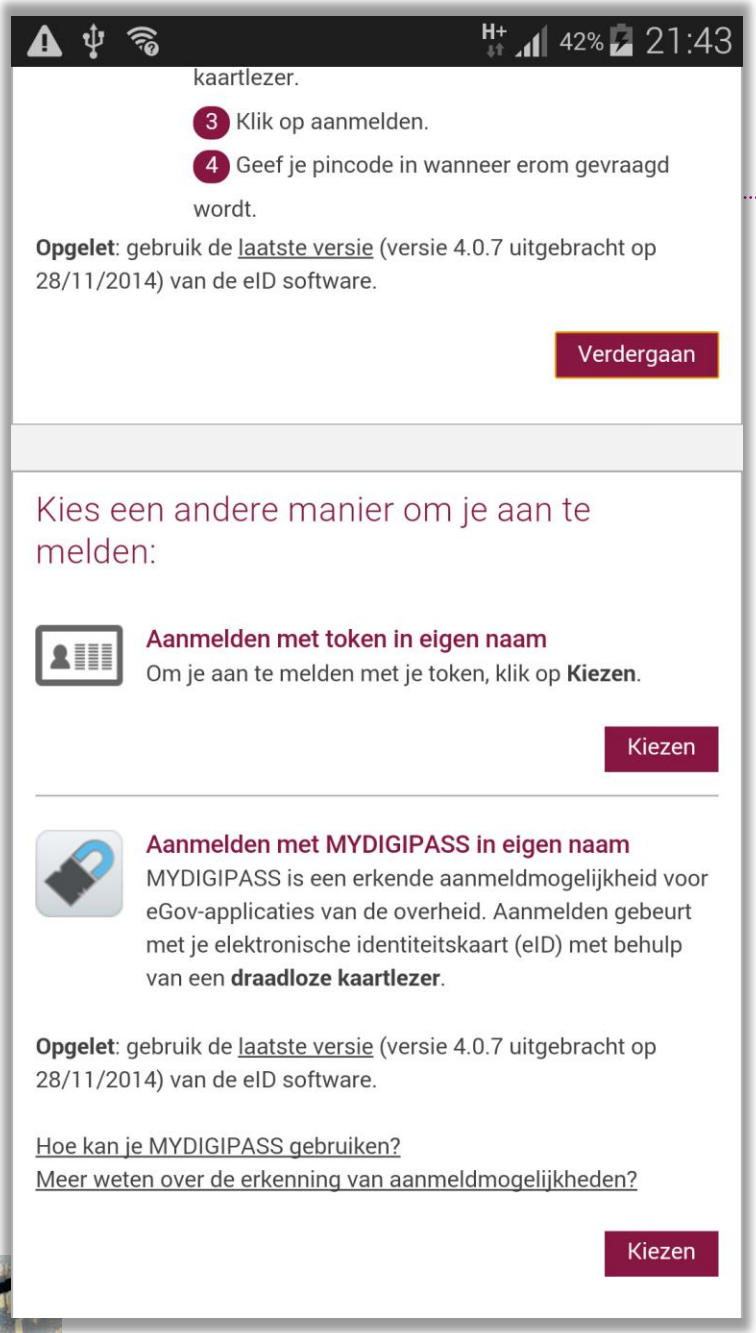


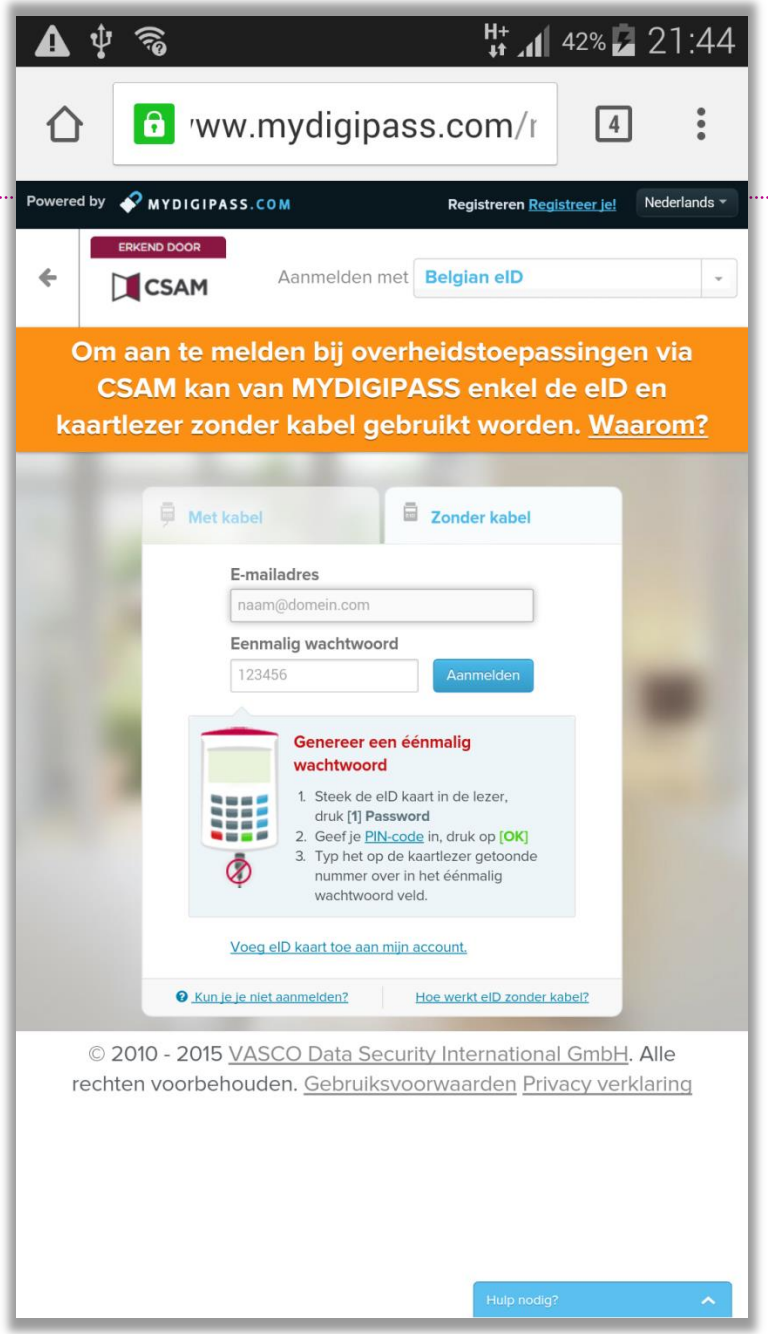
Aanmelden bij MDP.COM



Eénmalig wachtwoord op basis van eID




21:43
kaartlezer.
3 Klik op aanmelden.
4 Geef je pincode in wanneer erom gevraagd wordt.
Opgelet: gebruik de laatste versie (versie 4.0.7 uitgebracht op 28/11/2014) van de eID software.
Verdergaan
Kies een andere manier om je aan te melden:
Aanmelden met token in eigen naam
Om je aan te melden met je token, klik op Kiezen.
Kiezen
Aanmelden met MYDIGIPASS in eigen naam
MYDIGIPASS is een erkende aanmeldmogelijkheid voor eGov-applicaties van de overheid. Aanmelden gebeurt met je elektronische identiteitskaart (eID) met behulp van een draadloze kaartlezer.
Opgelet: gebruik de laatste versie (versie 4.0.7 uitgebracht op 28/11/2014) van de eID software.
Hoe kan je MYDIGIPASS gebruiken?
Meer weten over de erkenning van aanmeldmogelijkheden?
Kiezen


21:44
ww.mydigipass.com/
Powered by MYDIGIPASS.COM
Registreren Registreer je!
Nederlands
ERKEND DOOR
CSAM
Aanmelden met Belgian eID
Om aan te melden bij overheidstoepassingen via CSAM kan van MYDIGIPASS enkel de eID en kaartlezer zonder kabel gebruikt worden. Waarom?
Met kabel
Zonder kabel
E-mailadres
naam@domein.com
Eenmalig wachtwoord
123456
Aanmelden
Genereer een éénmalig wachtwoord
1. Steek de eID kaart in de lezer, druk [1] Password
2. Geef je PIN-code in, druk op [OK]
3. Typ het op de kaartlezer getoonde nummer over in het éénmalig wachtwoord veld.
Voeg eID kaart toe aan mijn account.
Kun je je niet aanmelden?
Hoe werkt eID zonder kabel?
© 2010 - 2015 VASCO Data Security International GmbH. Alle rechten voorbehouden. Gebruiksvoorwaarden Privacy verklaring
Hulp nodig?

Registreren bij Mydigipass.com

1. Kies "registreer je"
2. Hou klaar: eID, kaartlezer en USB-kabel
3. Installeer de Mydigipass card reader plugin
4. Steek de eID in de lezer en geef PIN in
5. Ga akkoord met de voorwaarden van MDP
6. Vul in: email, wachtwoord en gsm-nummer
7. Meld aan in Mijn eGov Profiel om de koppeling met je MDP account te voltooien

nl fr de en .be

CSAM | My eGov Login

Login using my eGov profile with the government

fedict e-gov

Log in with your eID card as yourself

To log in with your eID **insert your electronic identity card, electronic foreigner card or Kids-ID into** below. Enter your PIN

Please find below authenticate:

Token as you
In order to a
Choose butt

Partner acco
MYDIGIPASS
eGov-applicaties van de overheid. Aanmelden gebeurt met je elektronische identiteitskaart (eID) met behulp van een **draadloze kaartlezer**.

Opgelet: gebruik de laatste versie van de eID software.

Hoe kan je MYDIGIPASS gebruiken?
Meer weten over de erkenning van aanmeldmogelijkheden?

Choose

Welcome to My eGov-login

In order to access an eGov application of the administration, you must first log in. That way, your identity and access conditions will be checked and you will be provided with secure access to eGov-application(s) of

use. If possible please
wn name or the name of

in options, please
in My eGov-profile.

e answer quickly by

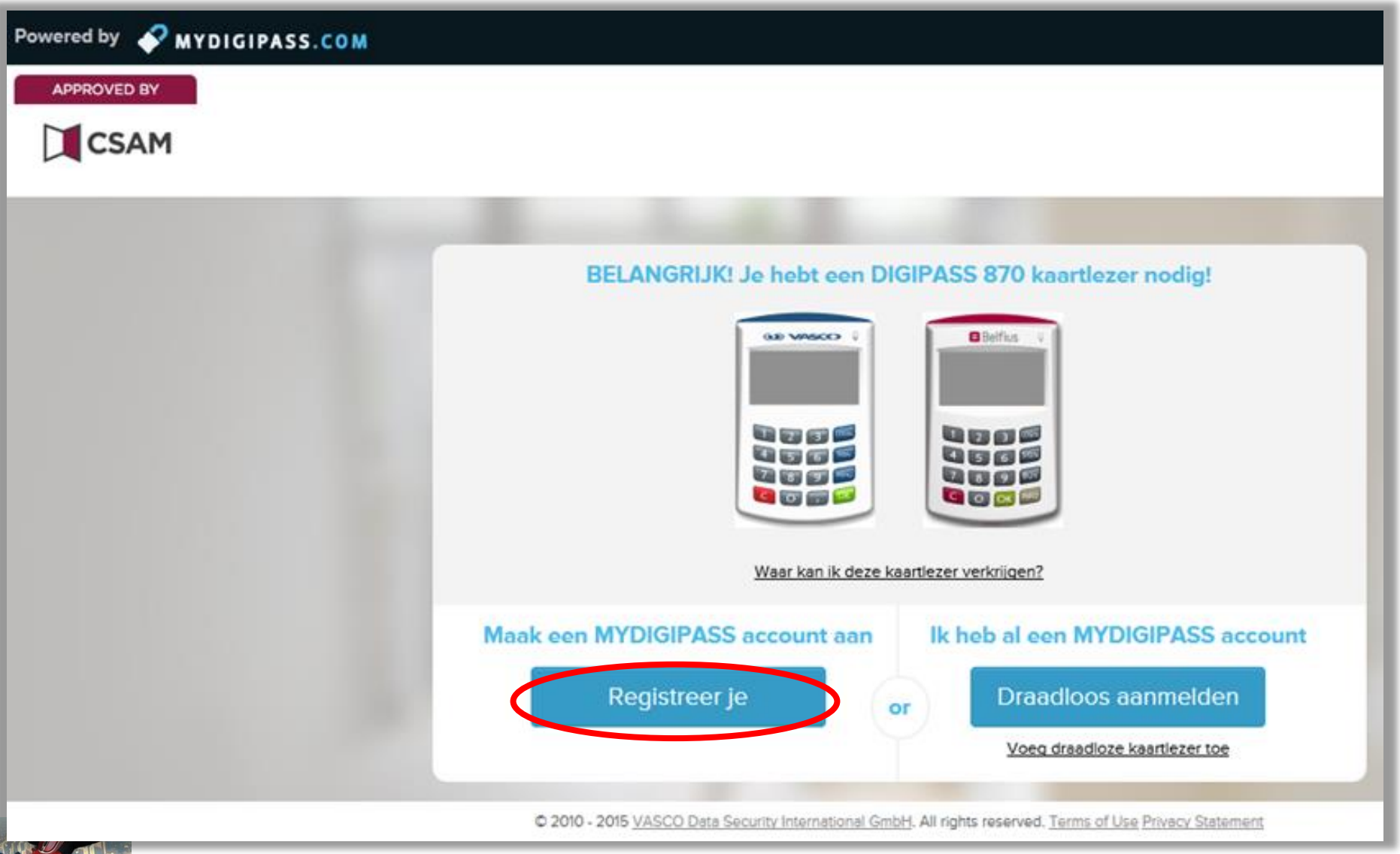
Partner account

MYDIGIPASS is een erkende aanmeldmogelijkheid voor eGov-applicaties van de overheid. Aanmelden gebeurt met je elektronische identiteitskaart (eID) met behulp van een **draadloze kaartlezer**.

Opgelet: gebruik de laatste versie van de eID software.

Hoe kan je MYDIGIPASS gebruiken?
Meer weten over de erkenning van aanmeldmogelijkheden?

Choose


Powered by MYDIGIPASS.COM
APPROVED BY
CSAM
BELANGRIJK! Je hebt een DIGIPASS 870 kaartlezer nodig!
Waar kan ik deze kaartlezer verkrijgen?
Maak een MYDIGIPASS account aan
Registreer je
or
Ik heb al een MYDIGIPASS account
Draadloos aanmelden
Voeg draadloze kaartlezer toe
© 2010 - 2015 VASCO Data Security International GmbH. All rights reserved. Terms of Use Privacy Statement

APPROVED BY

CSAM

EN NL FR IT DE

Log in

Step 1 of 3 - **Prepare** your material

You need to have the following items to register with MYDIGIPASS

1. Your eID card

2. A card reader *

3. A USB cable
(éénmalig bij registratie)

* Compatible card readers:
Latest Belfius card reader or VASCO DIGIPASS 870

Continue

Smals

APPROVED BY

CSAM

EN NL FR IT DE

Aanmelden

Stap 2 van 3 - **Activatie** van jouw toestel.

Verbind je kaartlezer met je computer ✔

Steek je eID kaart in ✔

Geef je eID PIN-code in en druk op OK ✔

- Je eID kaart is geverifieerd
- Deze eID reader, samen met je eID kaart, is nu klaar voor gebruik op MYDIGIPASS.

Verdergaan

Ben je je PIN vergeten?

APPROVED BY CSAM

EN NL FR IT DE

Aanmelden

Stap 2 van 3 - **Activatie** van jouw toestel.

Persoonsgegevens

Naam [redacted]

Geboortedatum [redacted]

Geslacht M

Adres

Straat [redacted]

Postcode [redacted]

Gemeente [redacted]

Overeenkomst i.v.m. gebruik van eID gegevens

"Door te klikken op de knop "Ik ga akkoord en ga door" zullen bepaalde persoonlijke gegevens op uw door de Belgische overheid verstrekte elektronische identiteitskaart ("eID-kaart") naar uw account van MYDIGIPASS bij VASCO Data Security, een private dienstverlener, worden overgedragen en daar opgeslagen. U kunt zien welke gegevens zijn vergaard met de functie "ID-gegevens België weergeven" die op uw profielpagina verschijnt en het privacybeleid van MYDIGIPASS doorlezen. Met uw account bij MYDIGIPASS en telkens met uw toestemming kunt u uw identiteit controleren op MYDIGIPASS, die compatibel is met websites van derden."

Ik ga akkoord en ga door

Ik wil mijn gegevens niet delen

APPROVED BY CSAM

Aanmelden

Stap 3 van 3 - **Registreer** jouw account.

Jouw apparaat is geactiveerd

Account info

Velden met een * zijn verplicht

E-mail *

John@voorbeeld.com

Hoofdwachtwoord *

Hoofdwachtwoord

Herhaal hoofdwachtwoord

BELANGRIJK

Het is zeer belangrijk dat je je hoofdwachtwoord onthoudt. Je zal het nodig hebben bij het beheer van jouw MYDIGIPASS account.

Persoonlijke info

GSM nummer

+32 1234567

Waarom is mijn GSM nummer verplicht?

Door te registreren aanvaardt u automatisch onze Gebruiksvoorwaarden en onze Privacy verklaring

Rond je registratie af

Nu chatten

nl fr de en | Veelgestelde vragen | Gebruikersovereenkomst .be

CSAM

Mijn eGov-profiel

Mijn online profiel bij de overheid

Welkom op mijn eGov-profiel

Je wilt deze MYDIGIPASS account koppelen aan je eGov-profiel. Hieronder zie je hoe die koppeling verloopt.

MYDIGIPASS.COM™

Je bent succesvol aangemeld met je MYDIGIPASS account

Je bevindt je hier

CSAM

Je moet je identiteit nog bevestigen door je aan te melden met je eID

CSAM

Na het aanmelden zal je MYDIGIPASS account gekoppeld zijn met je eGov-profiel

Nu moet je je nog **aanmelden** met je eID om de koppeling van je MYDIGIPASS account met je eGov profiel te voltooien.

Aanmelden

nl fr de en .be

CSAM | Mijn eGov-login

Aanmelden bij de overheid met je eGov-profiel

Aanmelden met eID in eigen naam

1. Sluit je eID kaartlezer aan op je computer.
2. Steek je elektronische identiteitskaart, elektronische vreemdelingenkaart of kids-ID in je kaartlezer.
3. Klik op aanmelden.
4. Geef je pincode in wanneer erom gevraagd wordt.

Opgelet: gebruik de laatste versie (versie 4.0.7 uitgebracht op 28/11/2014) van de eID software.

Verdergaan

Welkom op Mijn eGov-login

Om toegang te krijgen tot een eGov-applicatie van de overheid, moet je je eerst aanmelden. Zo worden je identiteit en je toegangsvoorwaarden gecontroleerd en krijg je op een veilige manier toegang tot de eGov-applicatie(s) van je keuze.

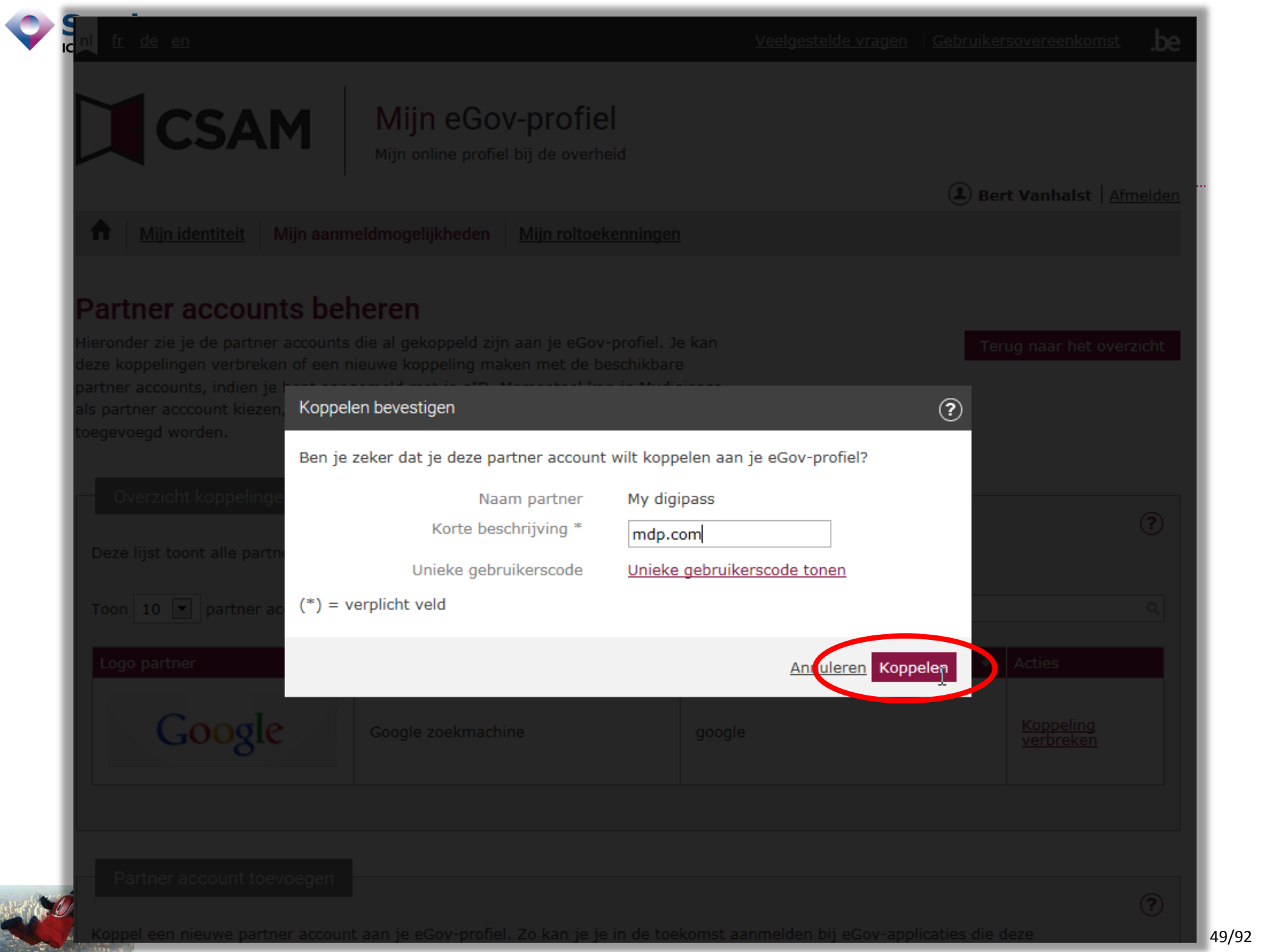
Kies hiernaast met welke aanmeldmogelijkheid je je wilt aanmelden. Kies eventueel ook in welke naam je je wilt aanmelden: in je eigen naam of in naam van een onderneming.

Beschik je niet over (de gevraagde) aanmeldmogelijkheden, beheer je aanmeldmogelijkheden in Mijn eGov-profiel.

Heb je andere vragen, vind snel een antwoord in de Veelgestelde vragen.

Belangrijke informatie:

Opgelet: gebruik de laatste versie (versie 4.0.7 uitgebracht op 28/11/2014) van de eID software.


nl fr de en
Veelgestelde vragen | Gebruikersovereenkomst .be
CSAM
Mijn eGov-profiel
Mijn online profiel bij de overheid
Bert Vanhalst | Afmelden
Mijn identiteit | Mijn aanmeldmogelijkheden | Mijn roltoekenningen
Partner accounts beheren
Hieronder zie je de partner accounts die al gekoppeld zijn aan je eGov-profiel. Je kan deze koppelingen verbreken of een nieuwe koppeling maken met de beschikbare partner accounts, indien je
als partner acccount kiezen,
toegevoegd worden.
Terug naar het overzicht
Koppelen bevestigen
Ben je zeker dat je deze partner account wilt koppelen aan je eGov-profiel?
Naam partner
My digipass
Korte beschrijving *
mdp.com
Unieke gebruikerscode
Unieke gebruikerscode tonen
(*) = verplicht veld
Annuleren
Koppelen
Overzicht koppelinge
Deze lijst toont alle partn
Toon 10 partner ac
Logo partner
Acties
Google
Google zoekmachine
google
Koppeling verbreken
Partner account toevoegen
Koppel een nieuwe partner account aan je eGov-profiel. Zo kan je je in de toekomst aanmelden bij eGov-applicaties die deze

Unconnected eID

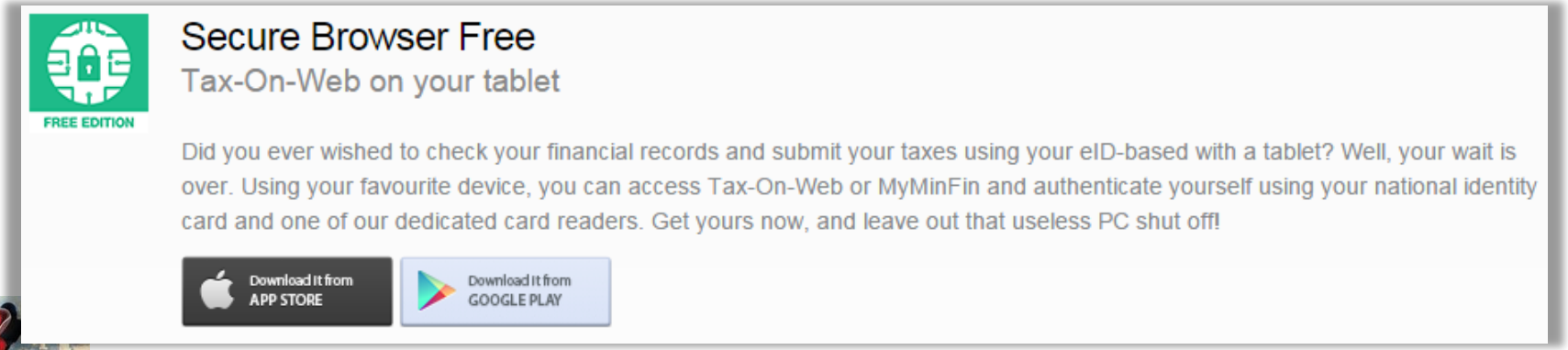
- Bruikbaar op mobiele toestellen
- Gebruiksgemak: niet evident in mobiele context
  - 3 dingen vasthouden
  - OTP overtypen
- Digipass 870 bekomen:
  - Via Belfius
  - Vasco online shop (€24,95)
    http://shop.vasco.com/digipass_870_detail.aspx

Connected eID

- Beperkt compatibel met mobiele toestellen
- Tablets met ingebouwde kaartlezer
  - Beperkt aantal modellen
  - Dell en Fujitsu Windows tablets
  - Voor professioneel gebruik

Connected eID

- Mobiele "add-on" kaartlezers
  - Zetes - Sipiro M
    - eID-BrowZer: enkel iOS
    - http://www.belgeid.be/
  - Freedelity
    - Secure Browser: Android, iOS
    - http://mobile.freedelity.be/



Connected eID

- Zetes Sipiro M
  - Voor iPhone en iPad
  - Kostprijs: €40 à €75
  - Gratis eID-BrowZer app
  - iPad casing
  - Product Review op http://www.smalsresearch.be/

Smals
ICT for society

Samenvatting

	Veiligheids-niveau	Mobiel gebruiksgemak	Gemak registratie	Beschikbaar in CSAM?
Paswoord	★	★★★★	★★★	✓
Burgertoken	★★	★★	★★★	✓
SMS OTP	★★★	★★★	★★★	✗
Commercieel certificaat	★★★	★★★	★	✓
Unconnected eID	★★★★	★★	★★	✗
Connected eID	★★★★★	★	★★	✓

Native apps

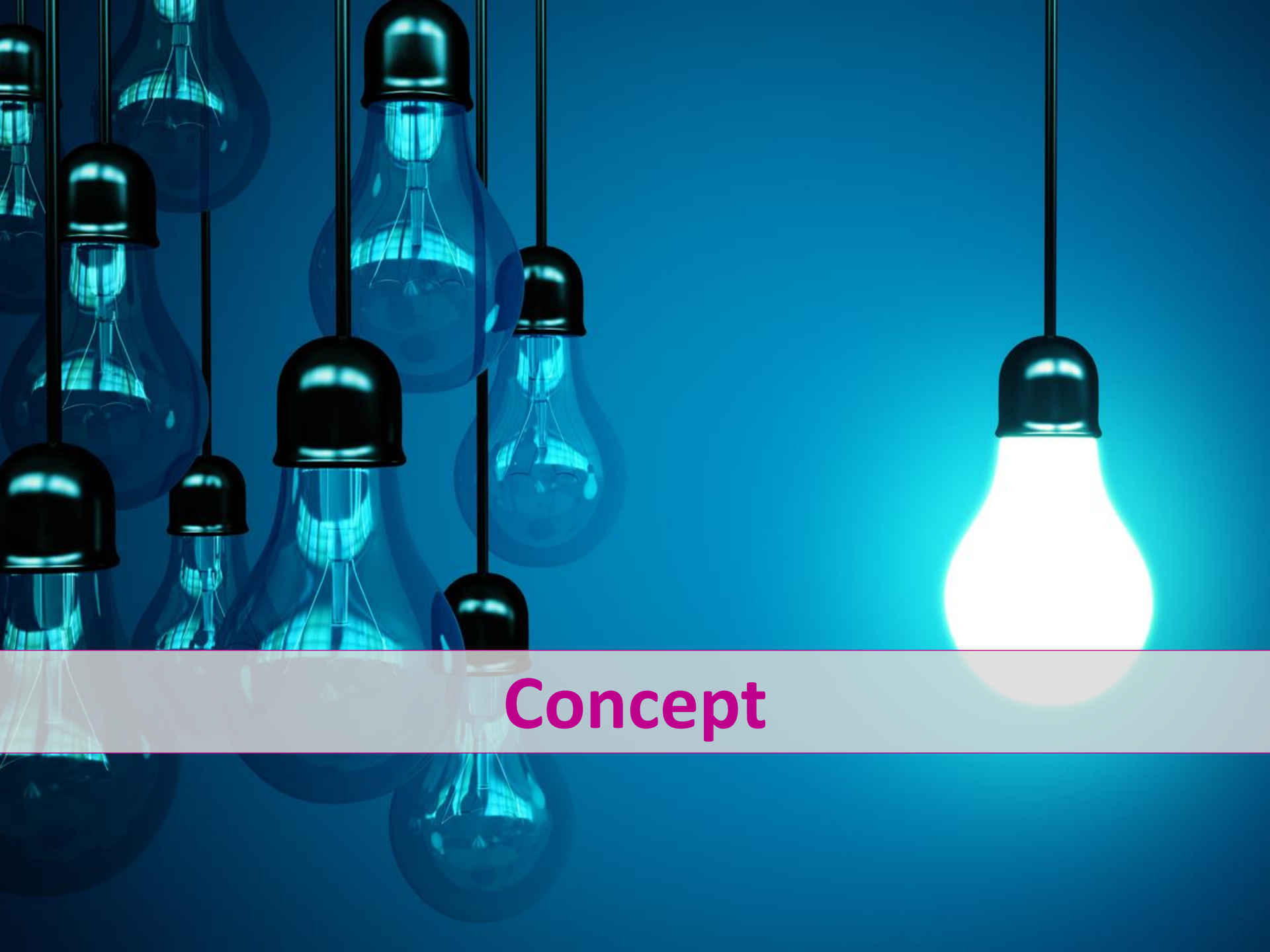
- Authenticatie: communicatie nodig vanuit native app met CSAM
  - OpenID Connect
- Authenticatie kan centraal afgehandeld worden door "authenticator app"
  - Eenvoudigere updates (security + functioneel)


PAUZE

Smals
ICT for society

Agenda

1. Inleiding
2. CSAM
3. PAUZE  
4. Concept
5. Marktevoluties
6. Conclusies



Concept

Concept

- Gedeeltelijke mismatch tussen beschikbare authenticatiemiddelen en mobiele context
- Zoektocht naar gebruiksvriendelijke én sterke mobiele authenticatie
- Samenwerking en overleg met Fedict en dienst Informatieveiligheid Smals
- Concept uitgewerkt
- Prototype

Uitgangspunten

- ✓ Hoog veiligheidsniveau
  Toegang tot vertrouwelijke informatie
- ✓ Maximale gebruiksvriendelijkheid
  Geen kaartlezers, tokens, liefst geen OTP overtypen
- ✓ Multi-platform
  Android, iOS, Windows Phone
- ✓ Compatibiliteit
  Met zowel native apps als webapps
- ✓ In te pluggen in CSAM
  eID bootstrap

Smals
ICT for society

Concept

+

PIN ****

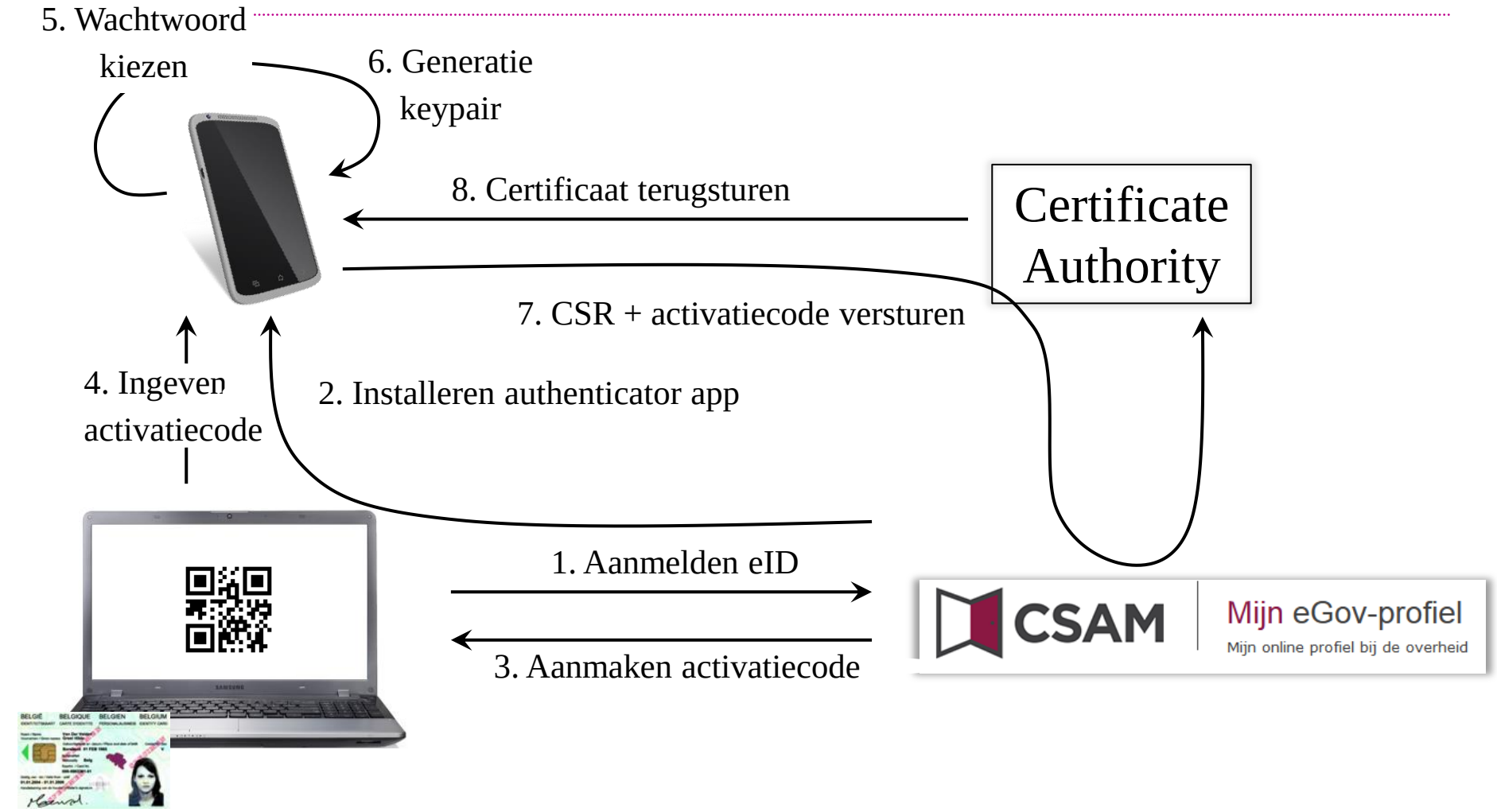
+

Enter a passcode

Vergelijking met mobile banking apps

Mobile banking apps	Concept
Authenticatie zit ingebakken in **één app**	Ondersteuning voor **meerdere apps** → authenticatie centraal afgehandeld door "authenticator app"
Specifieke oplossing voor **native app**	Ondersteuning voor **zowel webapps als native apps**
Risicobeheer: beperkte limiet; enkel overschrijving naar vooraf geregistreerde begunstigden. Maar **compensatie mogelijk** bij geldverlies.	**Geen compensatie mogelijk** bij gegevensdiefstal → hoger veiligheidsniveau nodig (bvb. hardware security) of beperking tot bepaalde categorie van gegevens

Registratie-flow

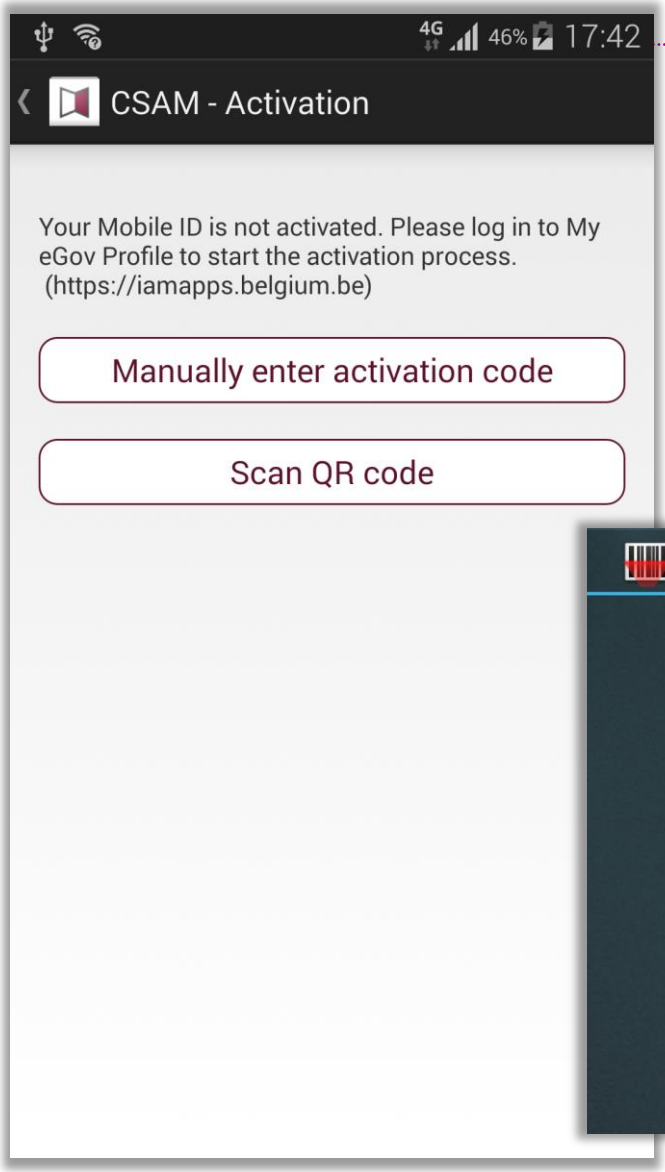


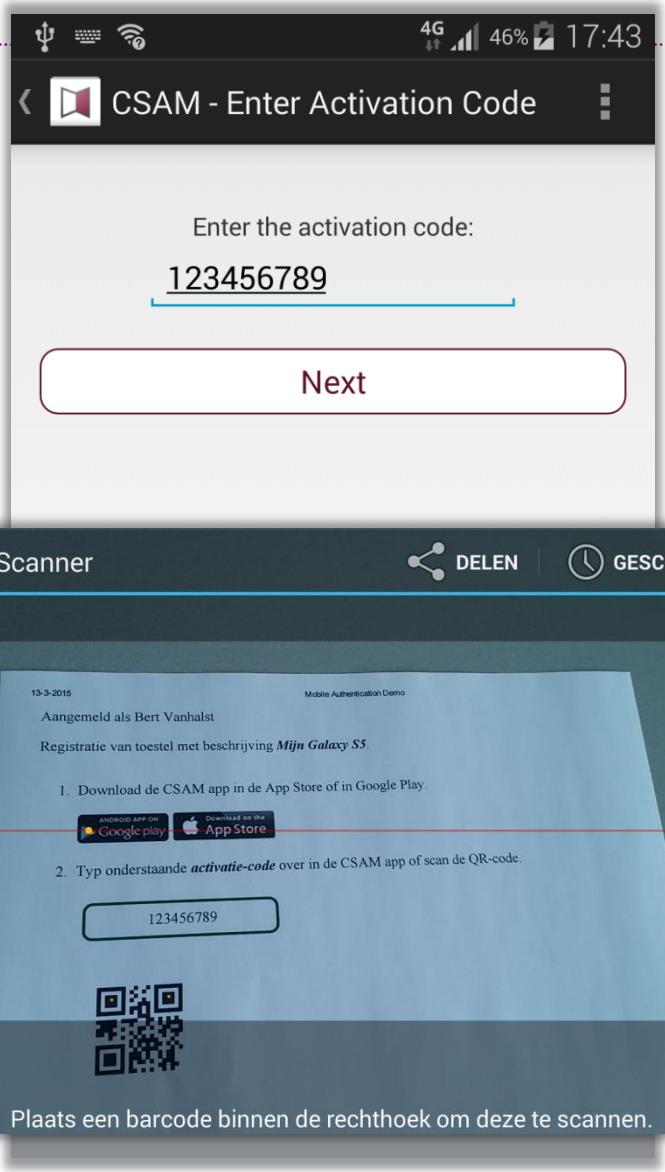
CSR = Certificate Signing Request
CA = Certificate Authority

Registratie-flow

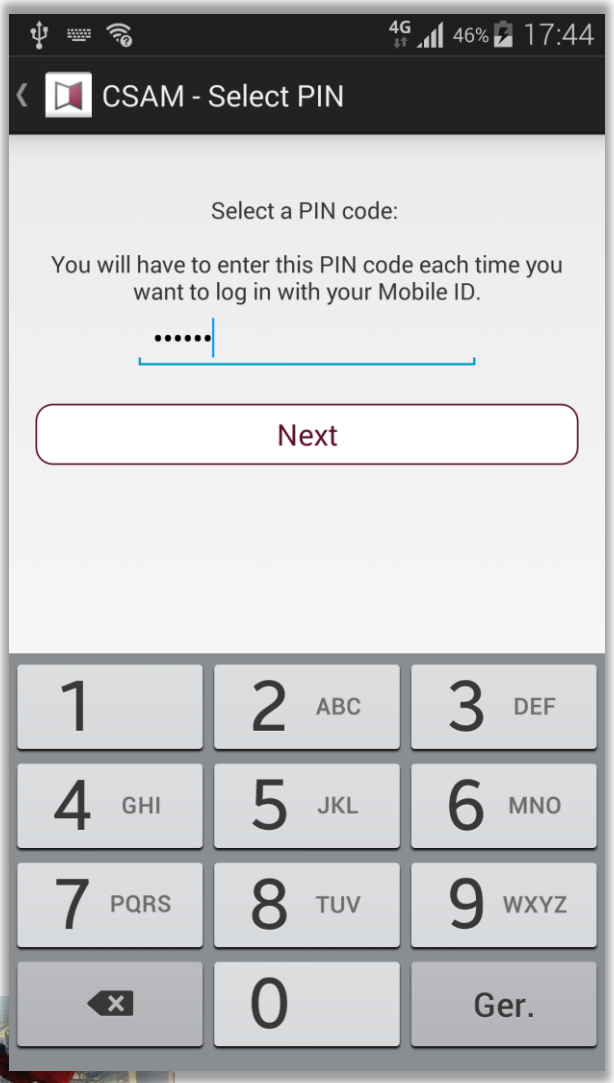
Demo prototype

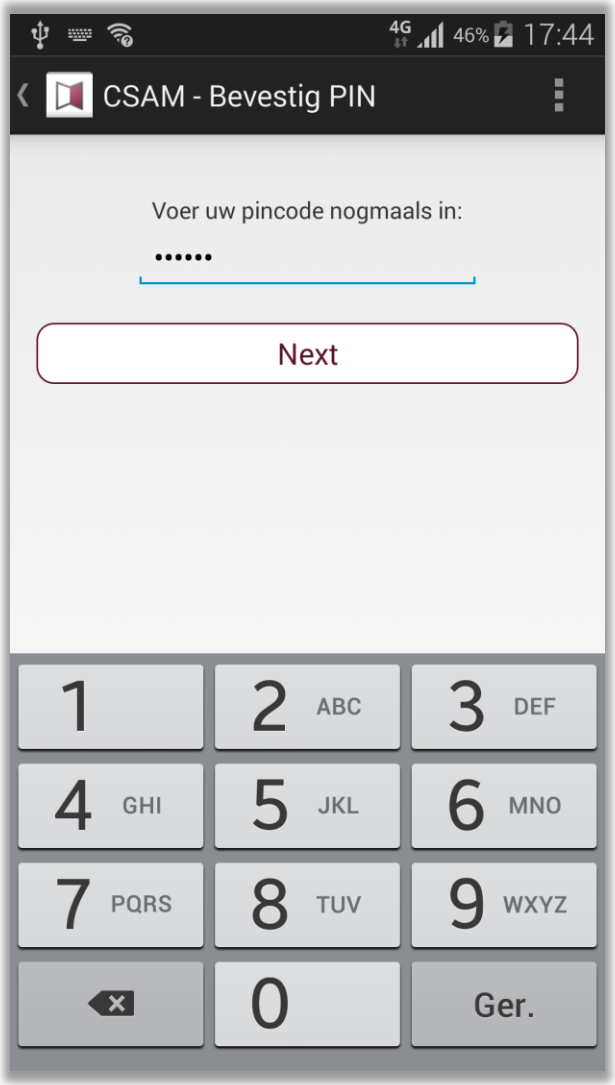
Registratie-flow (prototype)

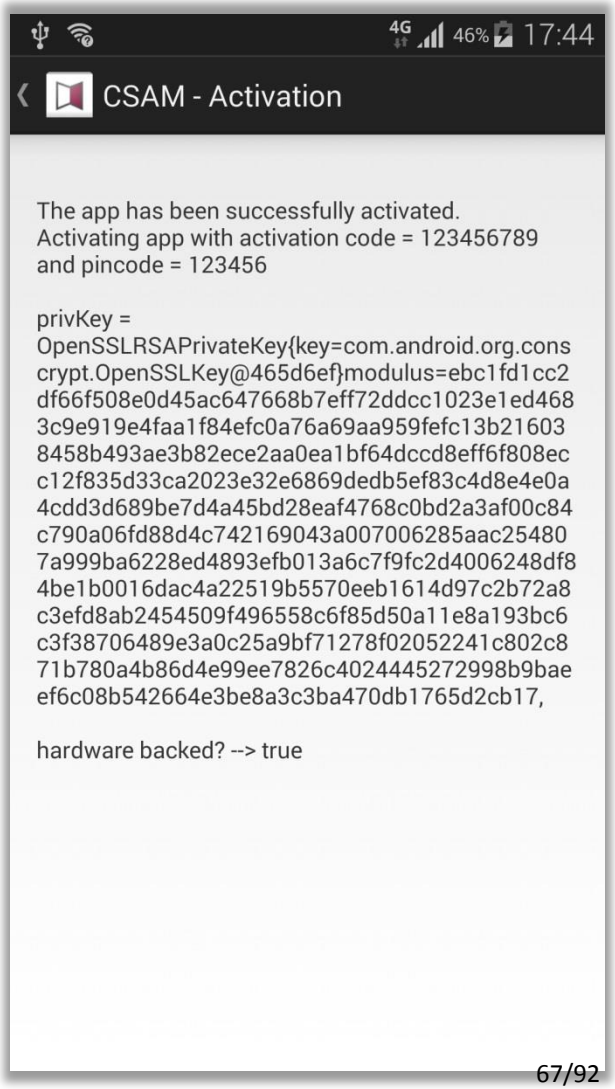




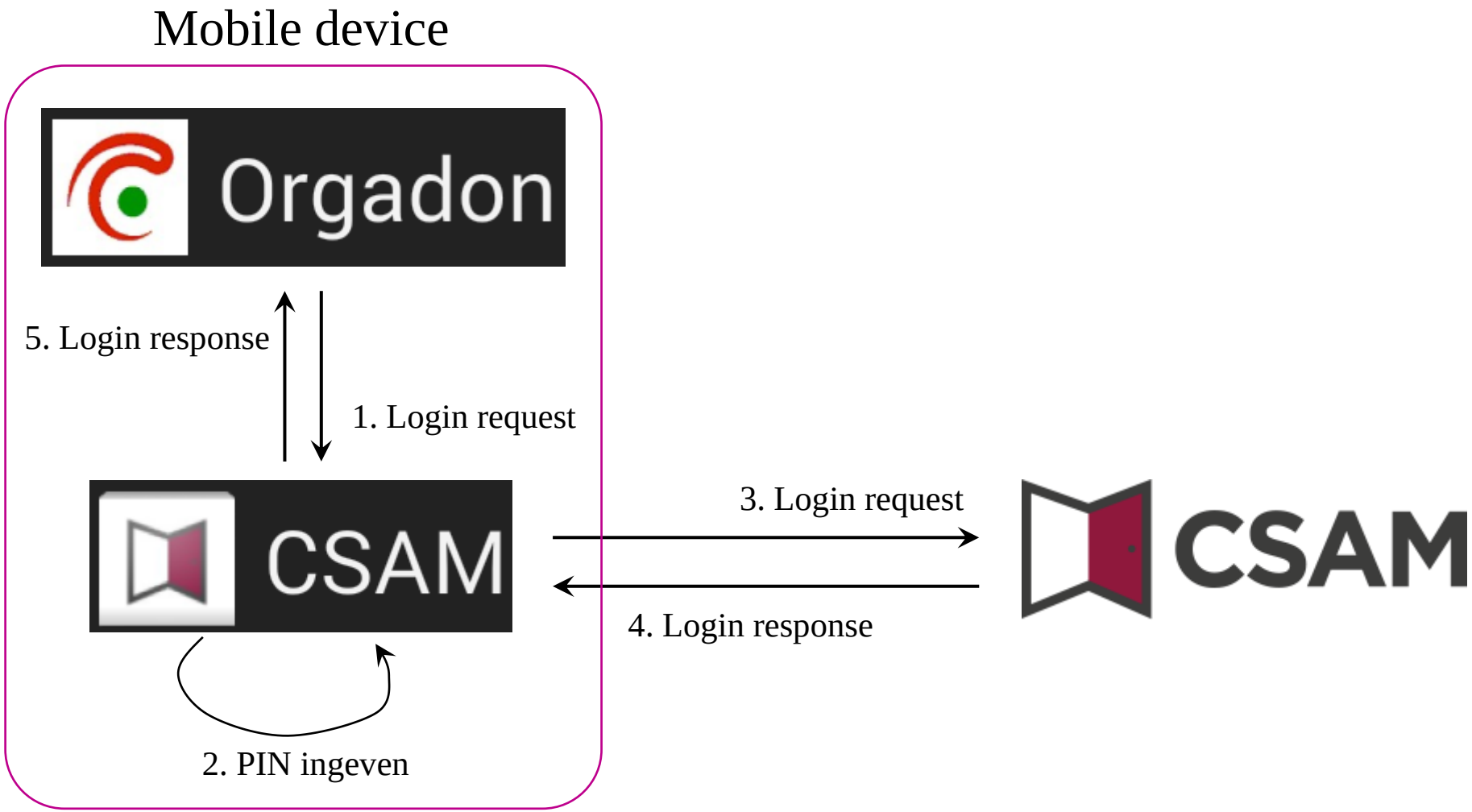
Registratie-flow (prototype)







Authenticatie-flow

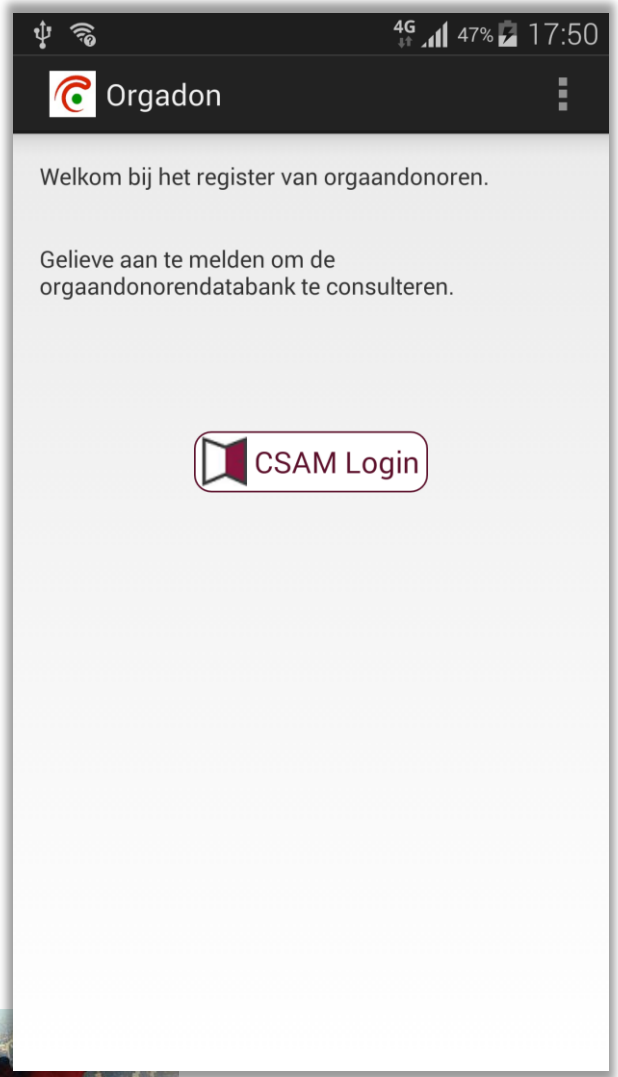


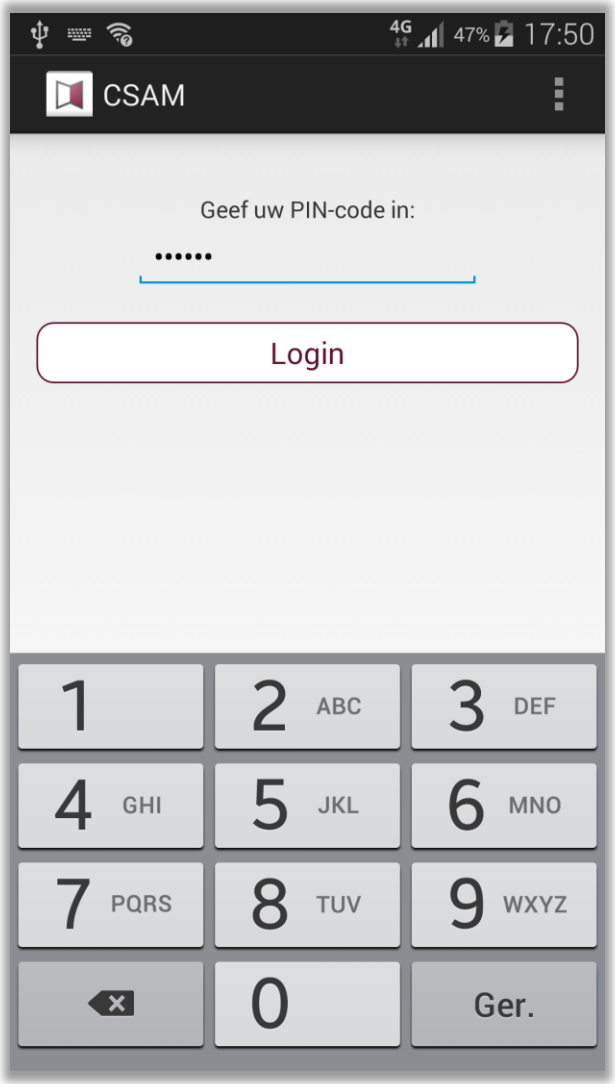
Authenticatie-flow

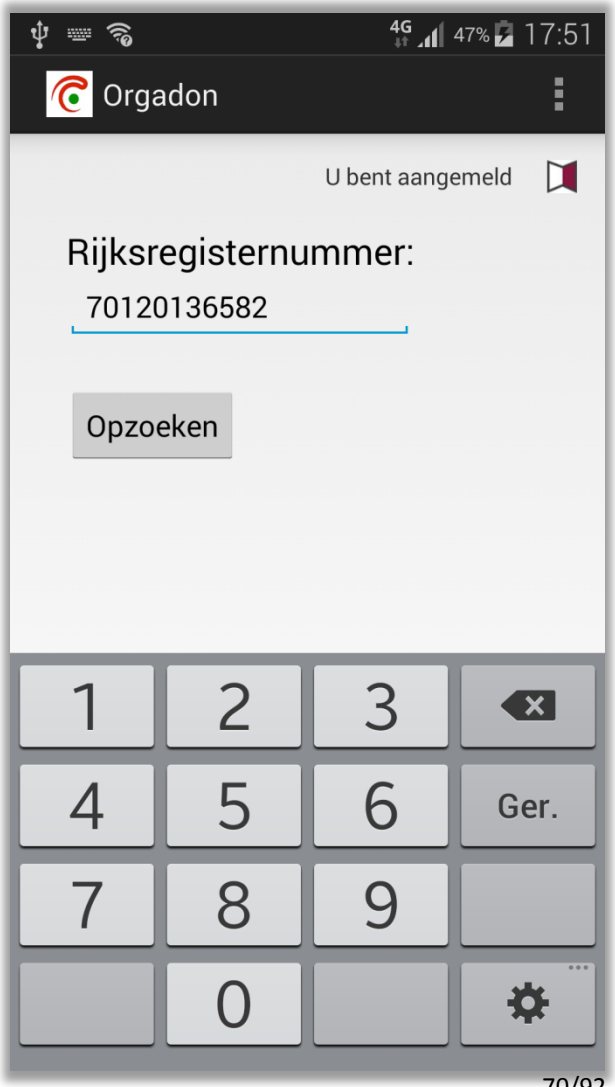
Demo prototype

Smals
ICT for society

Authenticatie-flow (prototype)







Technische opties

Technische opties voor de beveiliging van de sleutelinformatie:

1. Software keystores van mobile OS'en
2. SIM-kaart 
3. Trusted Platform Module (TPM) 
4. Secure SD 
5. Trusted Execution Environment (TEE)

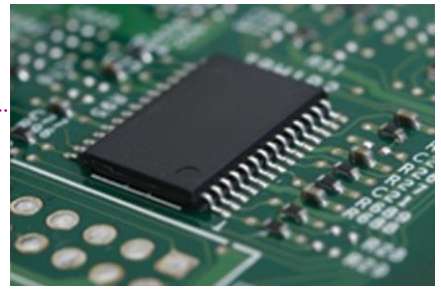
Secure Elements

Technische opties

SIM-kaart

- Portable tussen verschillende toestellen
- Vereist samenwerking met operatoren
- Reeds in gebruik in bepaalde landen (vb. Estland)
- Quid wifi-only toestellen?
- Mobile Connect initiatief (GSMA)
  - MC1: single factor (enkel SIM)
  - MC2: two-factor (SIM + PIN)
  - http://www.gsma.com/personaldata/mobile-connect

Technische opties



Trusted Platform Module (TPM)

- "Ingebouwde smartcard"
- Fysieke tamper resistance
- Vooral beschikbaar in pc's en laptops, beperkt beschikbaar in tablets en smartphones

Technische opties

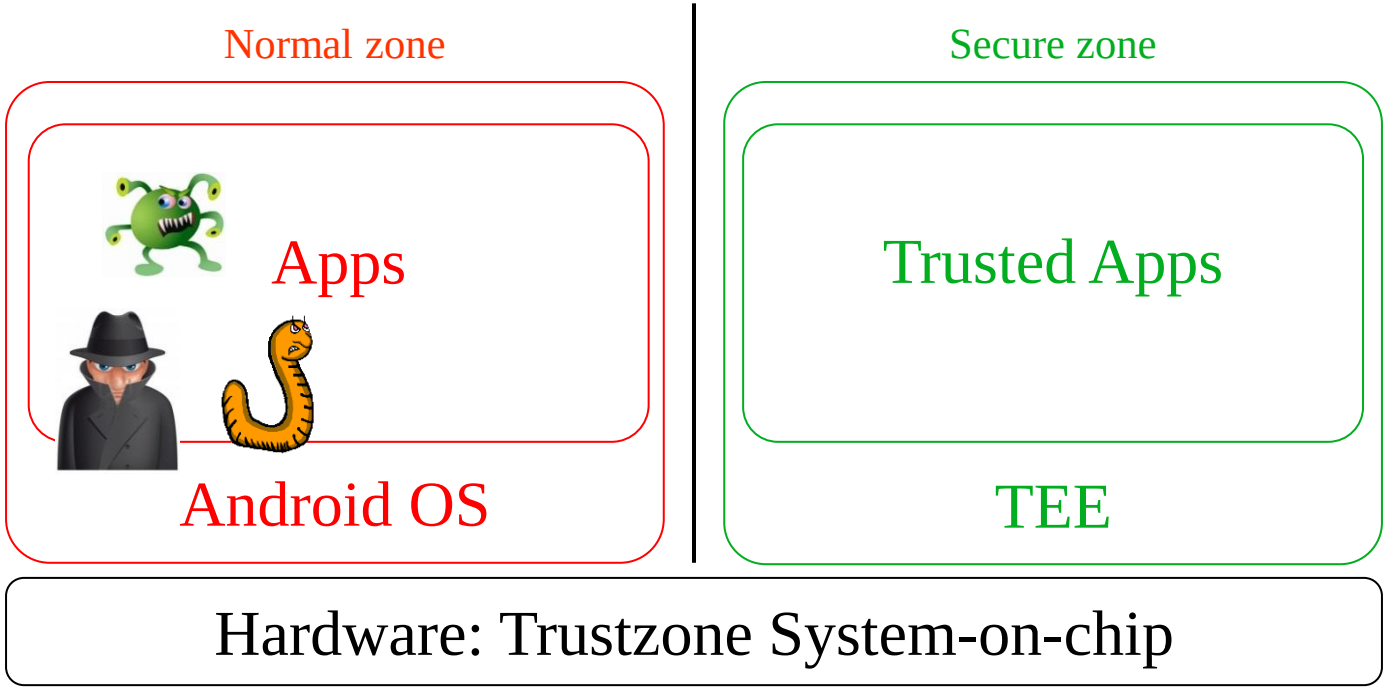
Secure SD

- Portable tussen verschillende toestellen
- Maar niet elk toestel heeft een SD-kaartslot
- Relatief hoge kost

Technische opties

Trusted Execution Environment (TEE)

- Afzonderlijke beveiligde zone op de main processor



Technische opties

Trusted Execution Environment (TEE)

- Veilige opslag van sleutelinformatie
- Beveiligde uitvoering van cryptografische bewerkingen
- Malware resistant
- Trusted User Interface: vermijden dat malware pincodes onderschept of zelf ingeeft

Technisch overzicht

	Rich OS Environment	Trusted Execution Environment (TEE)	Secure Element (SE) (when present)
Functionality	★★★	★★	★
Performance	★★★	★★	★
Memory Size Access	★★★	★★	★
Peripherals Access (display, touchscreen, video decoder/renderer, …)	★★★	★★	N/A
Attack Resistance	★	★★ (designed for SW-based attacks resistance)	★★★ (tamper-resistant)

Bron: Kevin Gillick, GlobalPlatform, RSA Conference 2014
http://www.rsaconference.com/events/us14/agenda/sessions/1018/integrating-any-smartphone-into-your-mobile-id

Prototype op basis van TEE

TRUSTONIC

- Samenwerkingsverband tussen ARM, Gemalto en Giesecke&Devrient
- Product: t-base TEE
- Beschikbaar op recente Android toestellen (Samsung, HTC, Alcatel, ZTE)
- Software Development Kit (SDK)

Trusted Execution Environment (TEE)

- Hardware Unique Key: laat toe om cryptografische sleutels hardware-matig te linken met een toestel.
- Bevindingen met SDK:
  - Beveiligde generatie sleutelpaar geïmplementeerd
  - Beveiligde opslag van sleutelinformatie geïmplementeerd

Status concept

- Concept uitgewerkt
- Prototype uitgevoerd
- Concept gevalideerd door dienst Informatieveiligheid (Smals) en Fedict
- Project "Mobile ID" geïnitieerd bij Fedict
- Aanpak: gebruikmaken van partner-oplossingen mits eID bootstrap

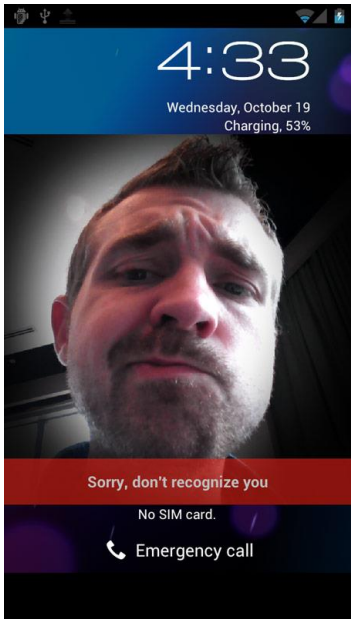
Marktevoluties

Biometrie

- Opkomst vingerafdrukscanners
  - Apple Touch ID
  - Samsung fingerprint scanner
- Toepassingen:
  - Toestel ontgrendelen
  - Betalen
  - Aanmelden

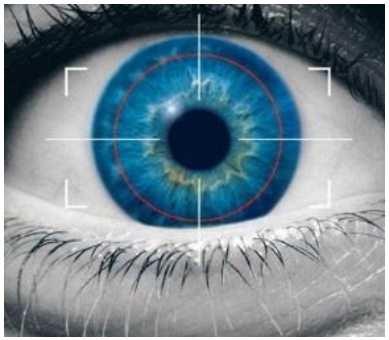
Biometrie

Gezichtsherkenning



Stemherkenning

Irisscan



En binnenkort online bankieren met hartslagmeter?

FIDO Alliance

fido alliance | simpler stronger authentication

- Globaal initiatief Google Microsoft PayPal VASCO THE AUTHENTICATION COMPANY
- Doel: open, op standaarden gebaseerde sterke authenticatie; verminderen van de afhankelijk van paswoorden
- Focus op gebruiksgemak en interoperabiliteit van authenticatiemiddelen
- Indien in overheidscontext: elk authenticatie-middel koppelen aan identiteit door middel van eID bootstrap

Blog: http://www.smalsresearch.be/de-fido-alliance-geen-vertrouwen-meer-in-het-paswoord/

PASSWORDLESS EXPERIENCE (UAF standards)

SECOND FACTOR EXPERIENCE (U2F standards)

Conclusies

Smals
ICT for society

Conclusies

	Veiligheids-niveau	Mobiel gebruiksgemak	Gemak registratie	Beschikbaar in CSAM?
Paswoord	★	★★★★	★★★	✓
Burgertoken	★★	★★	★★★	✓
SMS OTP	★★★	★★★	★★★	✗
Commercieel certificaat	★★★	★★★	★	✓
Unconnected eID	★★★★	★★	★★	✗
Connected eID	★★★★★	★	★★	✓
Toekomst??	★★★★	★★★★★	★★	??

Conclusies

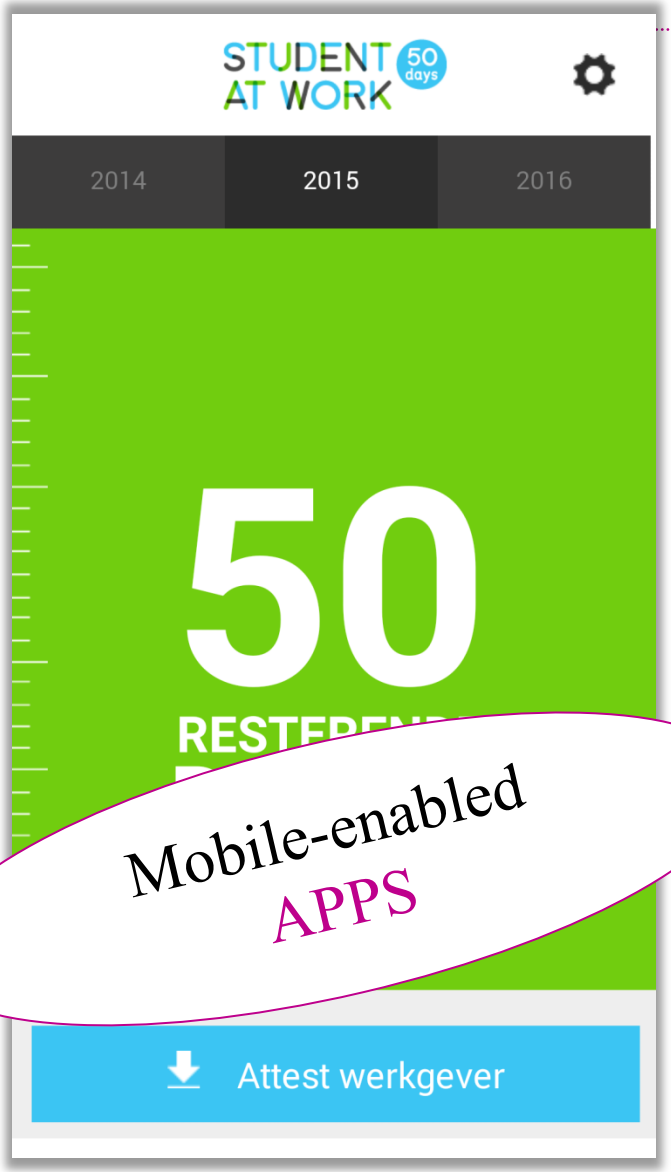
Paswoord
Burgertoken
(SMS OTP)
Comm. certificaat
Connected eID

Nu

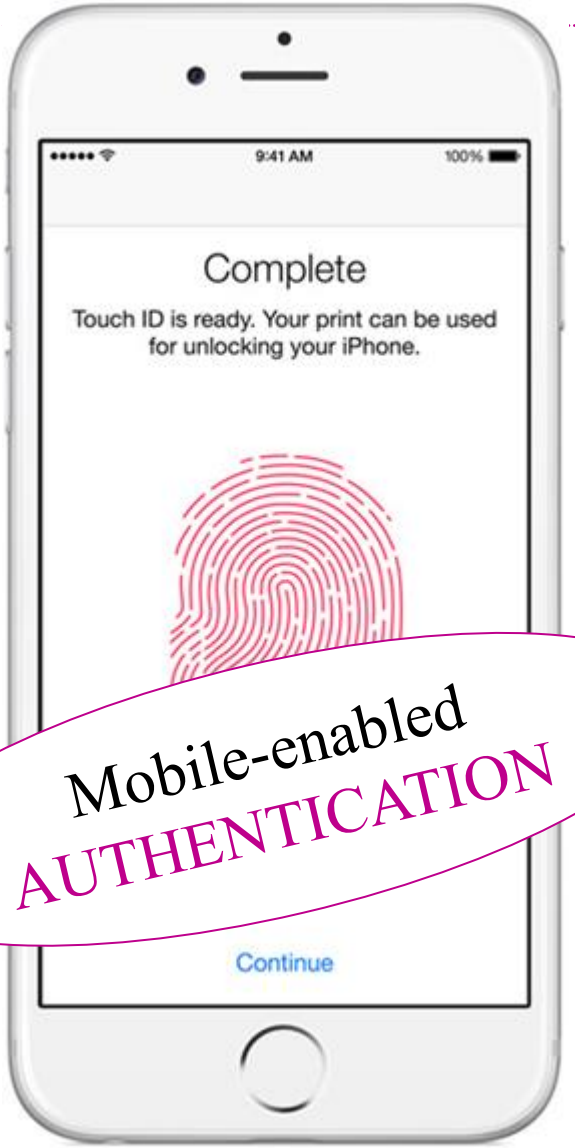
Nabije toekomst

Langere termijn

Conclusies



Mobile-enabled
APPS



Mobile-enabled
AUTHENTICATION

Bert Vanhalst

☎ 02 787 48 02
✉ bert.vanhalst@smals.be

Smals

www.smals.be
@Smals_ICT
www.smalsresearch.be
@SmalsResearch

Lectuur

Product Review Zetes Sipiro M (mobiele kaartlezer)

http://www.smalsresearch.be/publications/document/?docid=132

Blog "De FIDO Alliance: geen vertrouwen meer in het paswoord"

http://www.smalsresearch.be/de-fido-alliance-geen-vertrouwen-meer-in-het-paswoord/

Product Review Yubikey Neo (OTP token)

http://www.smalsresearch.be/publications/document/?docid=3

Links

- CSAM – https://www.csam.be/
- FIDO Alliance – https://fidoalliance.org/
- Freedelity – http://mobile.freedelity.be/
- Howwebrowse – http://howwebrowse.be/
- Mydigipass – https://www.mydigipass.com/
- Trustonic – https://www.trustonic.com/
- Yubikey – https://www.yubico.com/
- Zetes – http://www.belgeid.be/