

# *On-line* registratie en verstrekking van authenticatiemiddelen

[Eric.Verheul@keycontrols.nl](mailto:Eric.Verheul@keycontrols.nl)  
(presentatie op persoonlijke titel)

## Agenda

- Introductie
- Bestaande methoden en gebruik daarvan
- Opzet ontwikkelde methode
- Afsluiting

## Introductie

- Architect binnen Idensys met aandachtsgebied technische informatiebeveiliging en cryptografie. Lid expertgroep normenkaders.
- Idensys publiek-private samenwerking voor elektronische toegang bij overheid en bedrijfsleven.
- Idensys pilots aanloggen met private middelen bij de overheid op **niveau 3** ("STORK").

Mijn Belastingdienst Pilot Inloggen met een ander toegangsmiddel

Inloggen met een ander toegangsmiddel

In deze pilot kunt u kennismaken met een nieuwe manier van inloggen. U kunt in de toekomst veel overheidsinstaties, waaronder de Belastingdienst, inloggen met een toegangsmiddel van IDIN. Hebt u een toegangsmiddel van IDIN? Dan moet u deze wel eerst activeren voordat u inloggen. Kijk voor meer informatie over deze pilot op [www.belastingdienst.nl/pilot](http://www.belastingdienst.nl/pilot)

**Inloggen met Idensys**  
Met Idensys werken overheid en bedrijfsleven samen aan eenvoudiger en veiliger inloggen.

**Kies hoe u wilt inloggen**

U wilt inloggen bij **Belastingdienst**. U heeft hiervoor een inlogmiddel nodig van minimaal niveau 3.

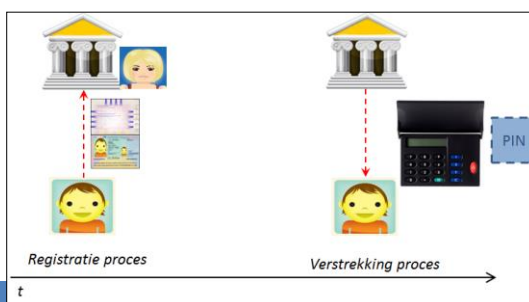
**Alleen geen keuze:**

- CreAim Idensys
- Digidentity
- KPN Idensys
- Secureidentity

16 juni, 2016 Digitaal zakendoen en EID 2016 3

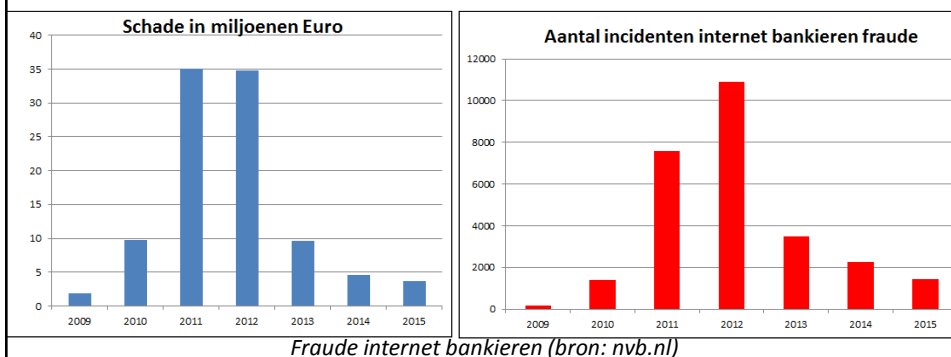
## Vraagstelling

- Conventionele opzet is dat bij klant registratie en/of middel verstrekking sprake is van een **fysieke verschijning**, hetgeen niet bijzonder gebruikersvriendelijk is.
- Vraag: is Registratie en Verstrekking proces **betrouwbaar** mogelijk voor niveau 3 zonder fysieke verschijning, i.e. volledig on-line?
- **Good practice** ontwikkeld vanuit de expertgroep.
- Rekening houden met **Social Engineering** en Man-in-the-Browser (**MITB**) aanvallen is cruciaal.



## Man-in-the-Browser (MITB)

- Veel internet browsers van gebruikers zijn geïnfecteerd met malware. Schatting van TU Delft is **10%**.
- Dergelijke browsers zijn dan onder controle van fraudeurs. Fraudeurs kunnen **namens** de gebruiker dingen **doen** wat zij willen en ook in de browsers gebruikers laten **zien** wat zij willen.
- Eerste massale 'toepassing' rond 2011 Nederlandse banken bij internet bankieren fraude.



## Man-in-the-Browser (MITB)

Aanmelden bij Platform Identity Management Nederland (PIMN) Nieuw? Klik hier om lid te worden

E-mailadres

Wachtwoord

**Aanmelden**

Je wachtwoord vergeten?

...Of meld u aan met een van deze:

YAHOO! LinkedIn Windows Live ID

---

**Nu ook aanloggen via DigiD** Nieuw? Klik hier om lid te worden

DigiD gebruikersnaam

Wachtwoord

**Aanmelden**



Je wachtwoord vergeten?

...Of meld u aan met een van deze:

YAHOO! LinkedIn Windows Live ID

---

Over Platform Identity Management Nederland (PIMN)

  ...en nog 1006 meer

PIMN staat voor beter identity management

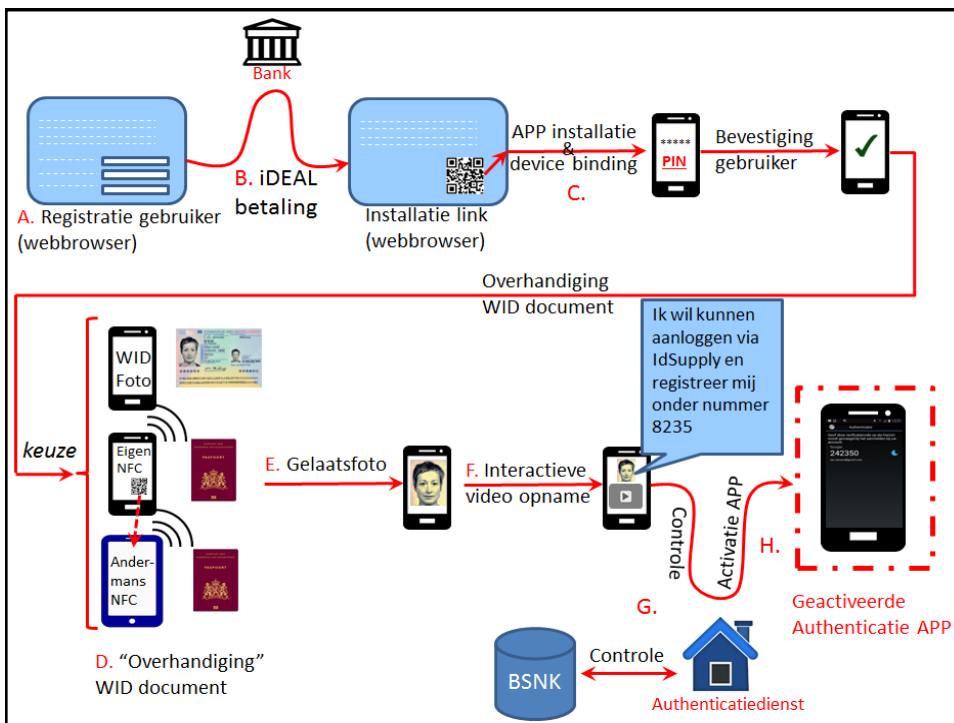
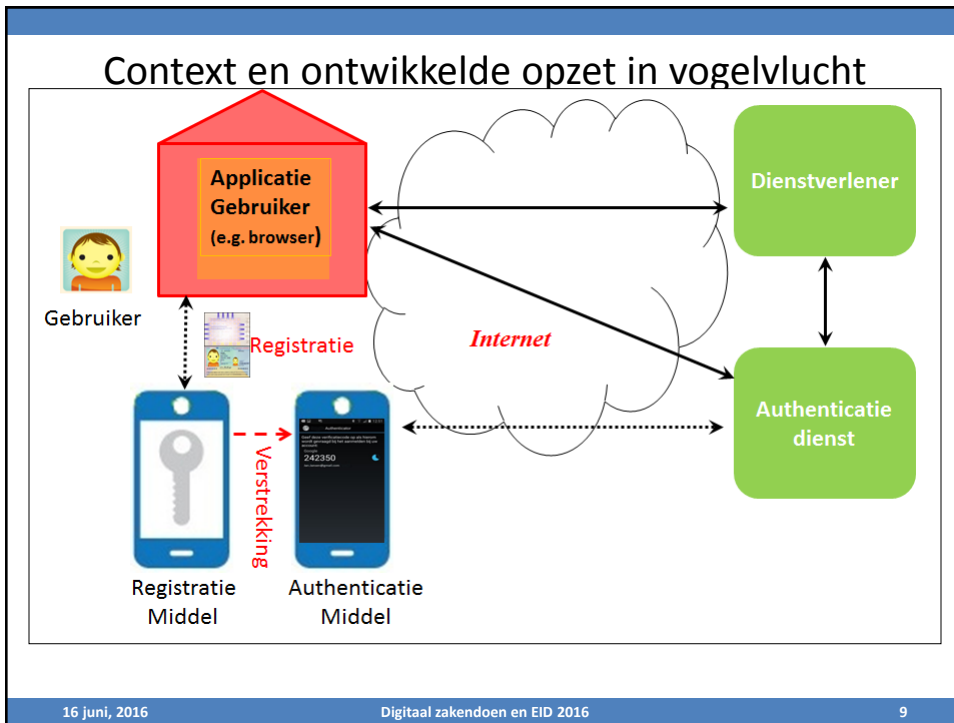
16 juni, 2016

Man-in-the-Browser

## Bestaande methoden en gebruik daarvan

- Nederlandse banken maken gebruik van **afgeleide identificatie** op basis van een financiële overschrijving op naam van de gebruiker.
- BAFIN, de Duitse financiële Toezichthouder (“Duitse AFM”) heeft een **face2face** registratie & verstrekking proces beschreven op basis van een video verbinding.
- Beide hebben voordelen en (beveiligings-)nadelen. Combinatie van beide methoden levert **solide basis** tegen social engineering en MITB:
  - gebruik van iDEAL in plaats van ad-hoc betaling om *attack surface* te beperken
  - op zoveel mogelijk plaatsen **tijdens** het proces waarschuwingen opnemen ook notificatie **na** afronding
  - authenticatie middel is een **APP** die ook bij het registratieproces wordt gebruikt voor binding tussen registratie en verstrekking.

## Opzet ontwikkelde methode

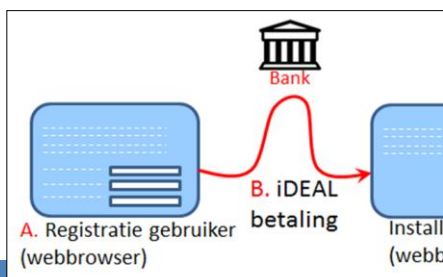


## Stappen

- A. Registratie gebruiker in Webbrowser
- B. iDEAL Transactie
- C. APP installatie device binding
- D. On-line overhandiging WID document via APP
- E. Maken gelaatsfoto via APP
- F. 'Challenge Response Video'
- G. Controle door Authenticatiedienst
- H. Activatie APP als authenticatiemiddel

## Stap B: iDEAL Transactie

- iDEAL biedt de mogelijkheid om bij **start** van betaling en bij **afronding** daarvan de gebruiker te **informer**en/wilsuiting te vragen over registratie.
- iDEAL biedt ook de mogelijkheid om de (afgeronde) registratie op **betaaloverzicht** te vermelden.
- iDEAL levert **digitaal getekend bericht** (F') van bank aan authenticatiedienst met daarin de voorletters en achternaam van de gebruiker.



## Stap B: iDEAL Transactie



### Selecteer betaalrekening (stap 2 van 4)

Selecteer het abonnement en de betaalrekening waarmee u de iDEAL-betaling wilt doen.

**Bedrag** € **0,01**

**Naam begunstigde** NL42 INGB 0454 8927 35 | registratie.authdienst.nl

**Datum** 03-11-2015

**Mededelingen** Let op: identiteit registratie 6UHY

#### Selecteer betaalrekening

Betaalrekeningen	Betaalrekening	€ 1.637,66
	NL38 INGB 0005 7611 36 - J.A.K.Pietersen	

**Selecteren** Annuleren



► Help

## Stap B: iDEAL Transactie



### Bestelling afronden (stap 4 van 4)

De betaling is geslaagd! Klik op 'Bestelling afronden' om uw bestelling af te ronden.

Afdrukken

#### Betalingsbevestiging

**Bedrag** € **0,01**

**Begunstigde** INGB 0454 8927 35 | registratie.authdienst.nl

**Van betaalrekening** NL38 INGB 0003 9134 90 - J.A.K.Pietersen

**Datum** 03-11-2015 13:37

**Transactienummer** 0050-0020-5855-3138

**Mededelingen** Let op: identiteit registratie 6UHY  
BIJ TWIJFEL OF VRAGEN BEL 08001111

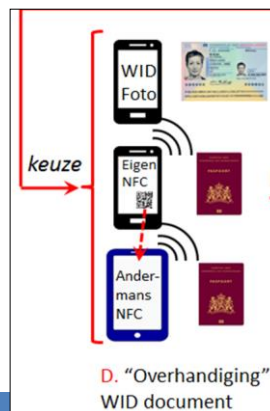
**Bestelling afronden**



► Help

## Stap D: On-line overhandiging WID document via APP

- De *practice* beschrijft een basis variant (foto WID document) en twee geavanceerde varianten.
- Bij de geavanceerde varianten wordt het WID document op afstand elektronisch uitgelezen (NFC). Met standaard WID cryptografie kan worden vastgesteld:
  - **authenticiteit** van het **document** (AA)
  - **authenticiteit** van de **gegevens** (PA)
- WID cryptografie is zo sterk dat zelfs **andermans** NFC enabled smartphone kan worden gebruikt zonder substantiële privacy risico's.

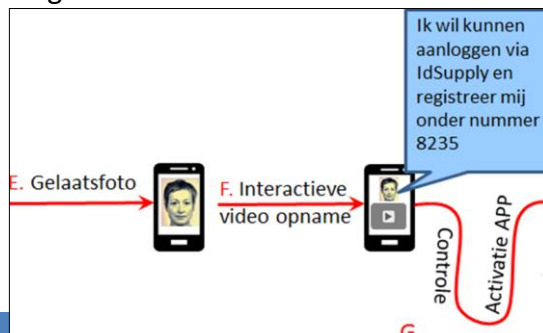


16 juni, 2016

Digitaal zakendoen en EID 2016

## Stap F: 'Challenge Response Video'

- Om zekerheid te krijgen dat gebruiker bewust is van de aanvraag wordt gebruik gemaakt van 'Challenge Response Video'. Dit is een variant van de Duitse BAFIN methode.
- Eigenschappen:
  - Wilsuiting gebruiker
  - Freshness (geen replay)
  - Device binding



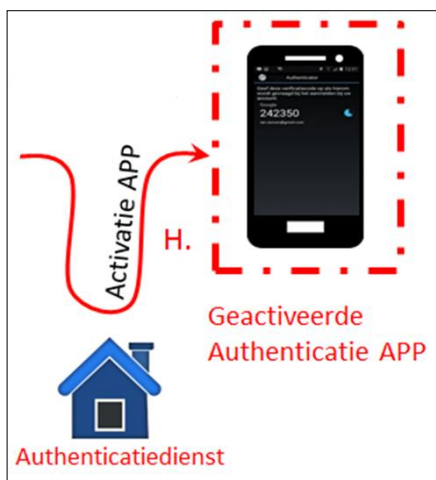
16 juni, 2016

16



## Stap H: Activatie APP als authenticatiemiddel

- Nadat de controles succesvol zijn afgerond wordt 'een knop omgezet' bij de authenticatiedienst en verandert de Registratie APP in een Authenticatie APP. Feitelijk is dit de **verstrekking** van het middel.



## Afsluiting

Resultaat op

<https://afsprakenstelsel.etoegang.nl/> (PDF).