On-line registratie en verstrekking van authenticatiemiddelen

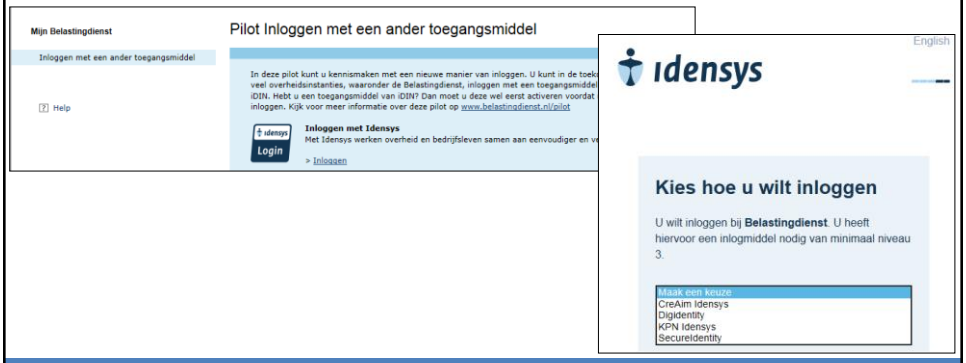
Eric.Verheul@keycontrols.nl
(presentatie op persoonlijke titel)

Agenda

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

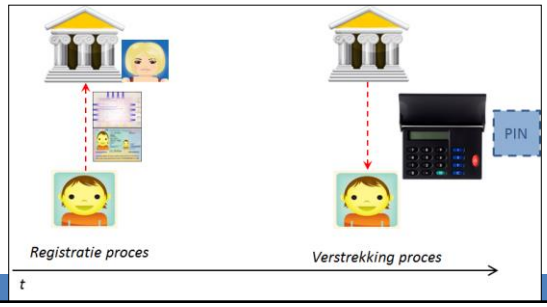
Introductie

- 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”).



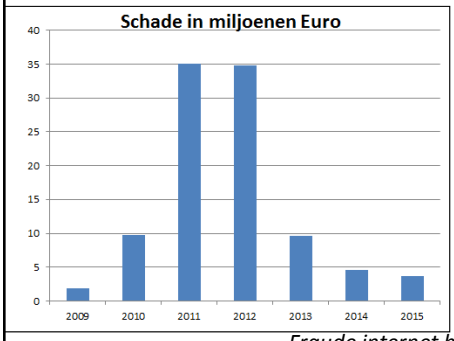
Vraagstelling

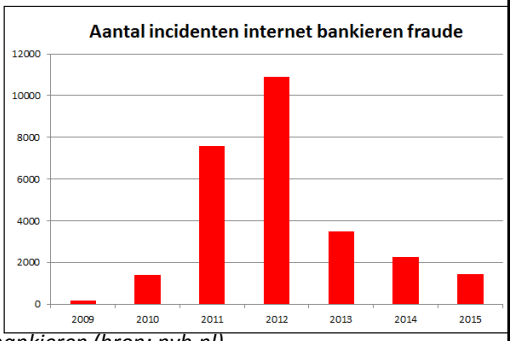
- Conventionele opzet is dat bij klant registratie en/of middel verstrekking sprake is van een fysieke verschijning, hetgeen niet bijzonder gebruikersvriendelijk is.
- Vraag: is Registratie en Verstrekking proces betrouwbaar mogelijk voor niveau 3 zonder fysieke verschijning, i.e. volledig on-line?
- *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)

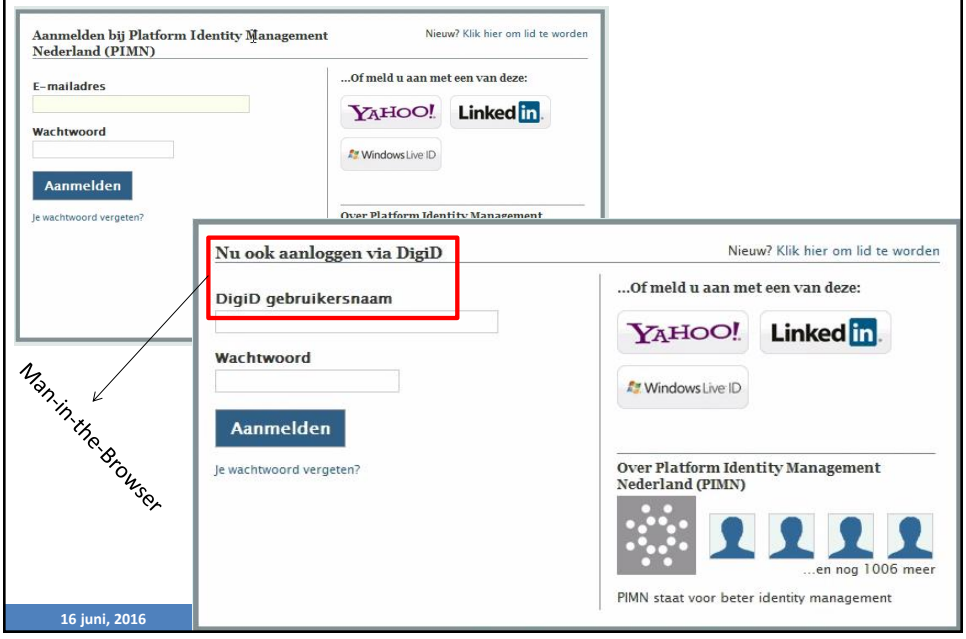
- Veel internet browsers van gebruikers zijn geïnfecteerd met malware. Schatting van TU Delft is 10%.
- Dergelijke browsers zijn dan onder controle van fraudeurs. Fraudeurs kunnen *namens* de gebruiker dingen *doen* wat zij willen en ook in de browsers gebruikers laten *zien* wat zij willen.
- Eerste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





Fraude internet bankieren (bron: nvb.nl)

Man-in-the-Browser (MITB)

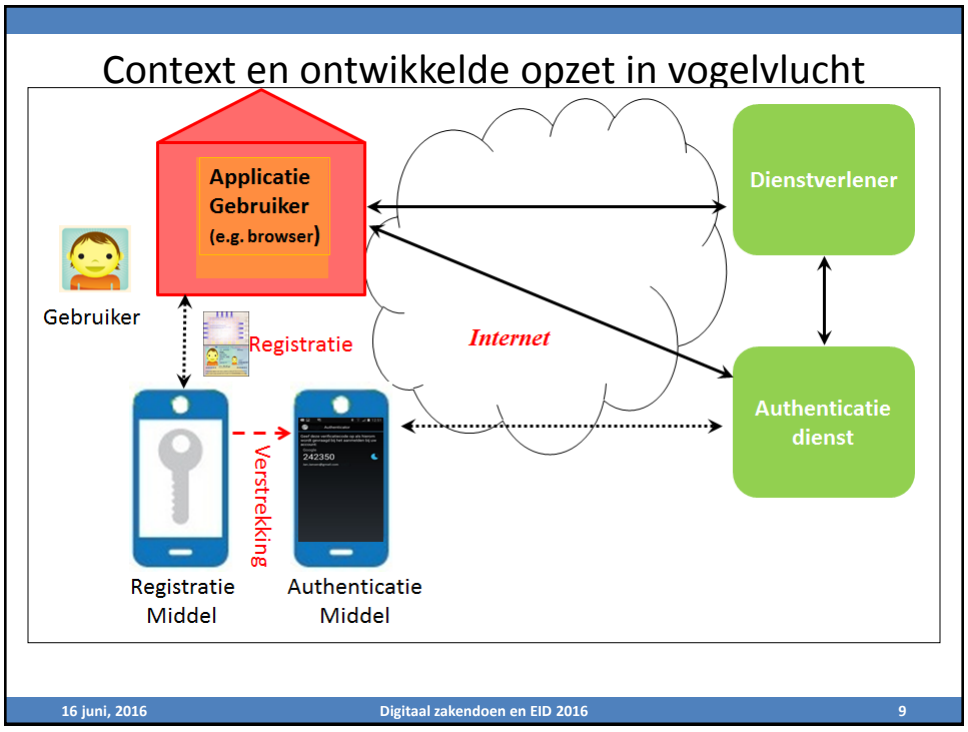


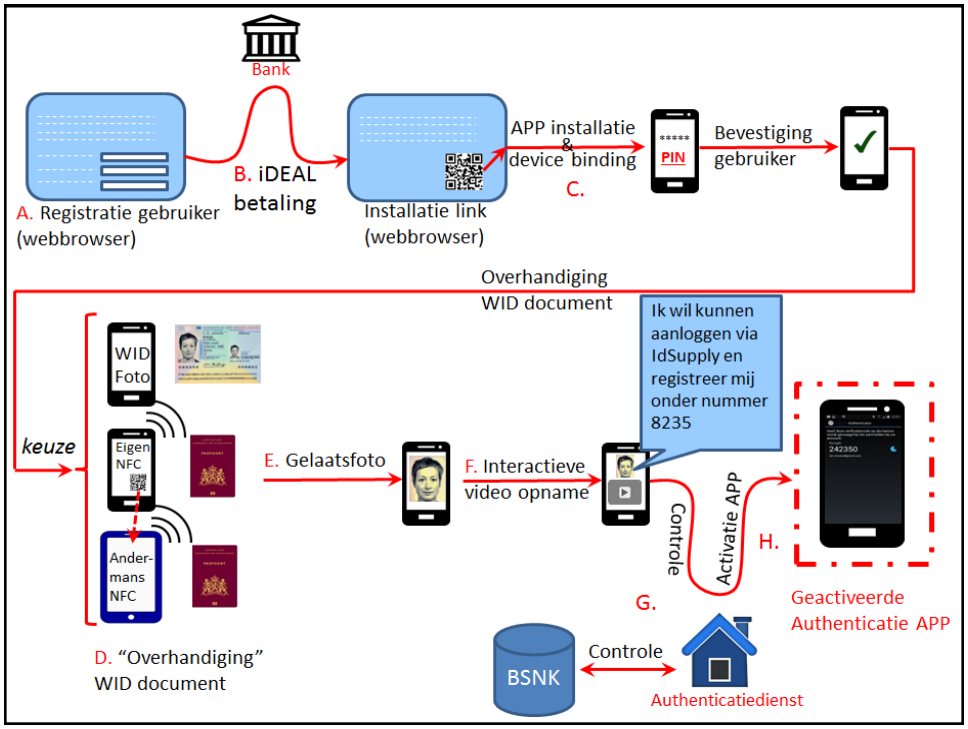
16 juni, 2016

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


Context en ontwikkelde opzet in vogelvlucht
Applicatie
Gebruiker
(e.g. browser)
Dienstverlener
Gebruiker
Registratie
Internet
Authenticatie
dienst
Verstrekking
Registratie
Middel
Authenticatie
Middel
16 juni, 2016
Digitaal zakendoen en EID 2016
9

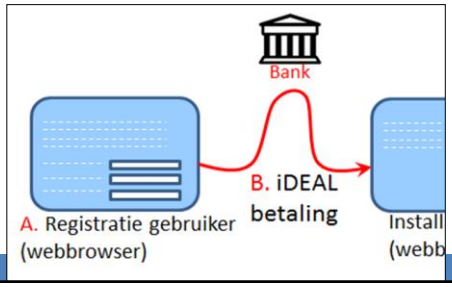

Bank
A. Registratie gebruiker
(webbrowser)
B. iDEAL
betaling
Installatie link
(webbrowser)
APP installatie
&
device binding
C.
PIN
Bevestiging
gebruiker
Overhandiging
WID document
keuze
WID
Foto
Eigen
NFC
Ander-
mans
NFC
D. "Overhandiging"
WID document
E. Gelaatsfoto
F. Interactieve
video opname
Ik wil kunnen
aanloggen via
IdSupply en
registreer mij
onder nummer
8235
Controle
Activatie APP
H.
G.
Geactiveerde
Authenticatie APP
BSNK
Controle
Authenticatiedienst

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

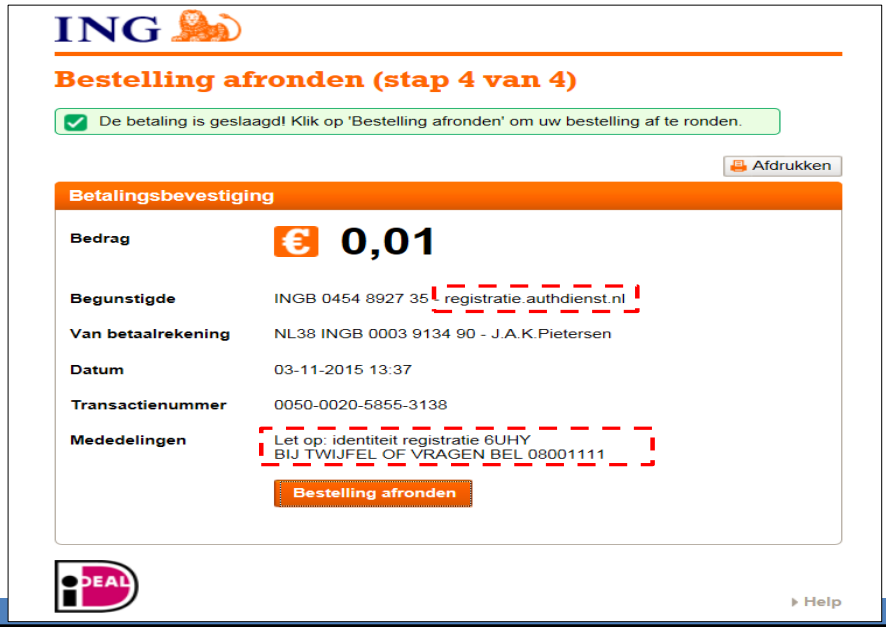
Stap B: iDEAL Transactie

- iDEAL biedt de mogelijkheid om bij start van betaling en bij afronding daarvan de gebruiker te informeren/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.



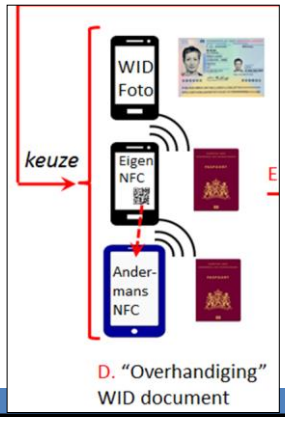
Stap B: iDEAL Transactie

Stap B: iDEAL Transactie



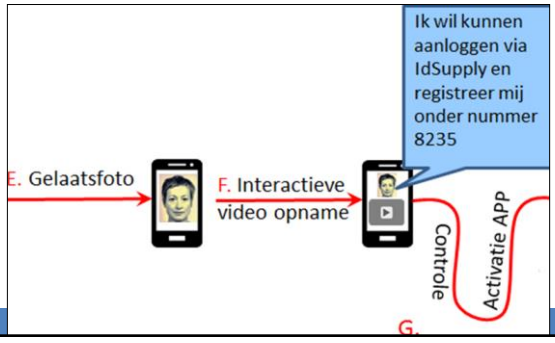
Stap D: On-line overhandiging WID document via APP

- 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.



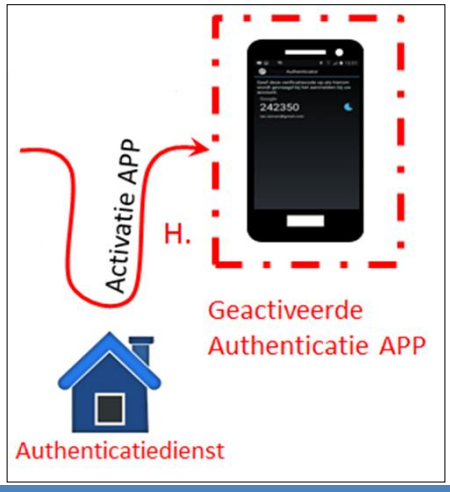
Stap F: 'Challenge Response Video'

- 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



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).