



Inloggen bij de overheid door burgers en bedrijven

Wet Digitale Overheid (WDO)

SIDN Connect 28-11 2019

*Barbera Veltkamp
Ministerie van BZK*





Waar gaat het over?

- › Maatschappij digitaliseert; de overheid en publieke dienstverleners ook
- › Wetgeving digitale overheid is relatief nieuw
- › Regeerakkoord 2013: recht op digitaal 'zaken doen' met ovh. Nodig: 1) AWB en 2) wetgeving toegang tot digitale dienstverlening overheid ('sleutel')
- › Ondertussen: eID-pilots (PPS -> publiekrecht)
- › 'vertaling' eID-stelsel naar wetgeving: WGDI -> WDO
- › Eerste tranche: toegang tot de overheid (publieke dienstverleners)
- › Wetsvoorstel ligt in TK (nr 34 972)



Wat is toegang?



1. Identificatie
Wie ben je?



2. Authenticatie
Hoe bewijs je dat?



kredietwaardig

leeftijd

machtiging

3. Autorisatie
Wat mag je? Waar heb je toegang toe?



Online transacties nu

- › Nu bepalen **organisaties** hoe de gebruiker zich identificeert
- › Geen sprake van **standaardisatie**





Gevolgen van huidige online transactie

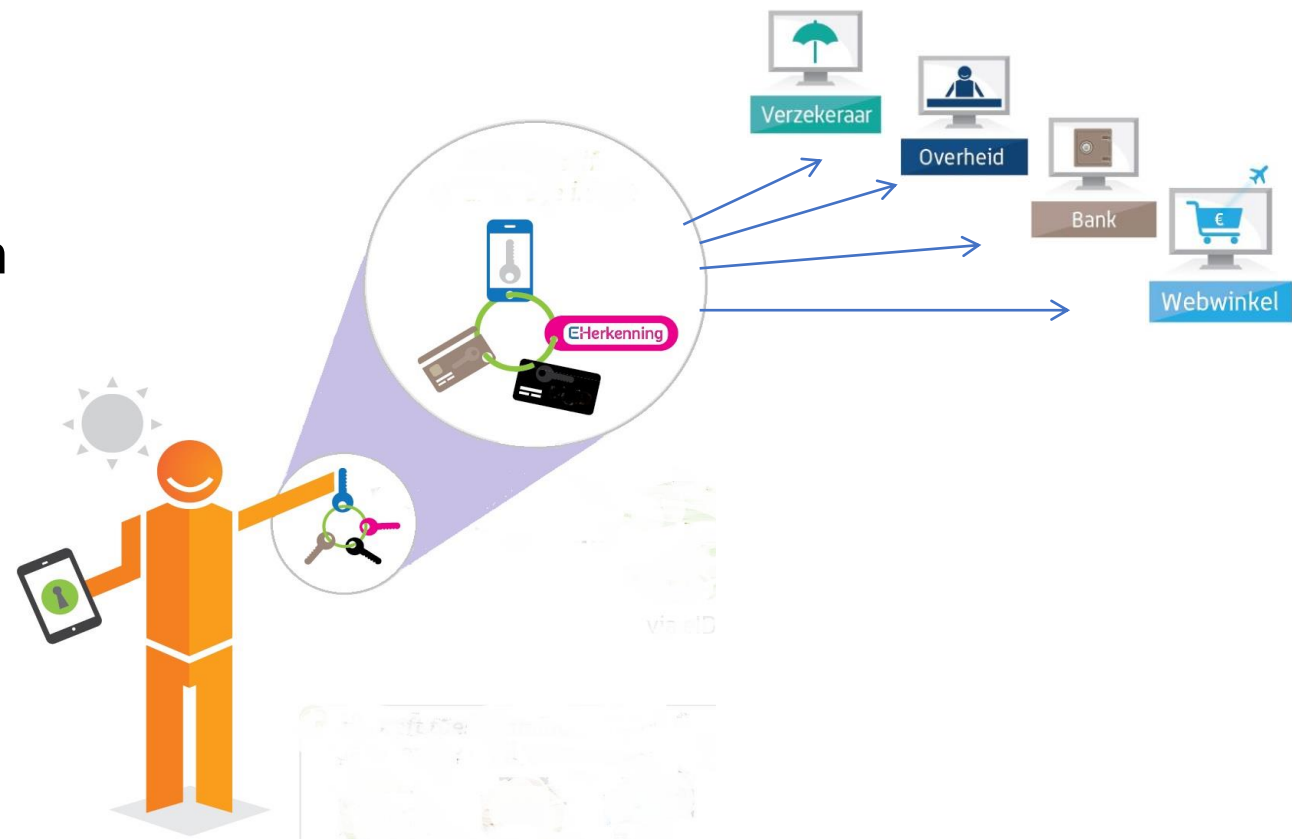
- › Gebruiker moet veel verschillende gebruikersnamen en wachtwoorden gebruiken / onthouden
- › Lastig en risicovol voor zowel gebruiker als voor dienstverlener





Online transacties in de toekomst

- › De **gebruiker** bepaalt hoe hij zich identificeert
- › Eenduidige toegang voor burgers en bedrijven





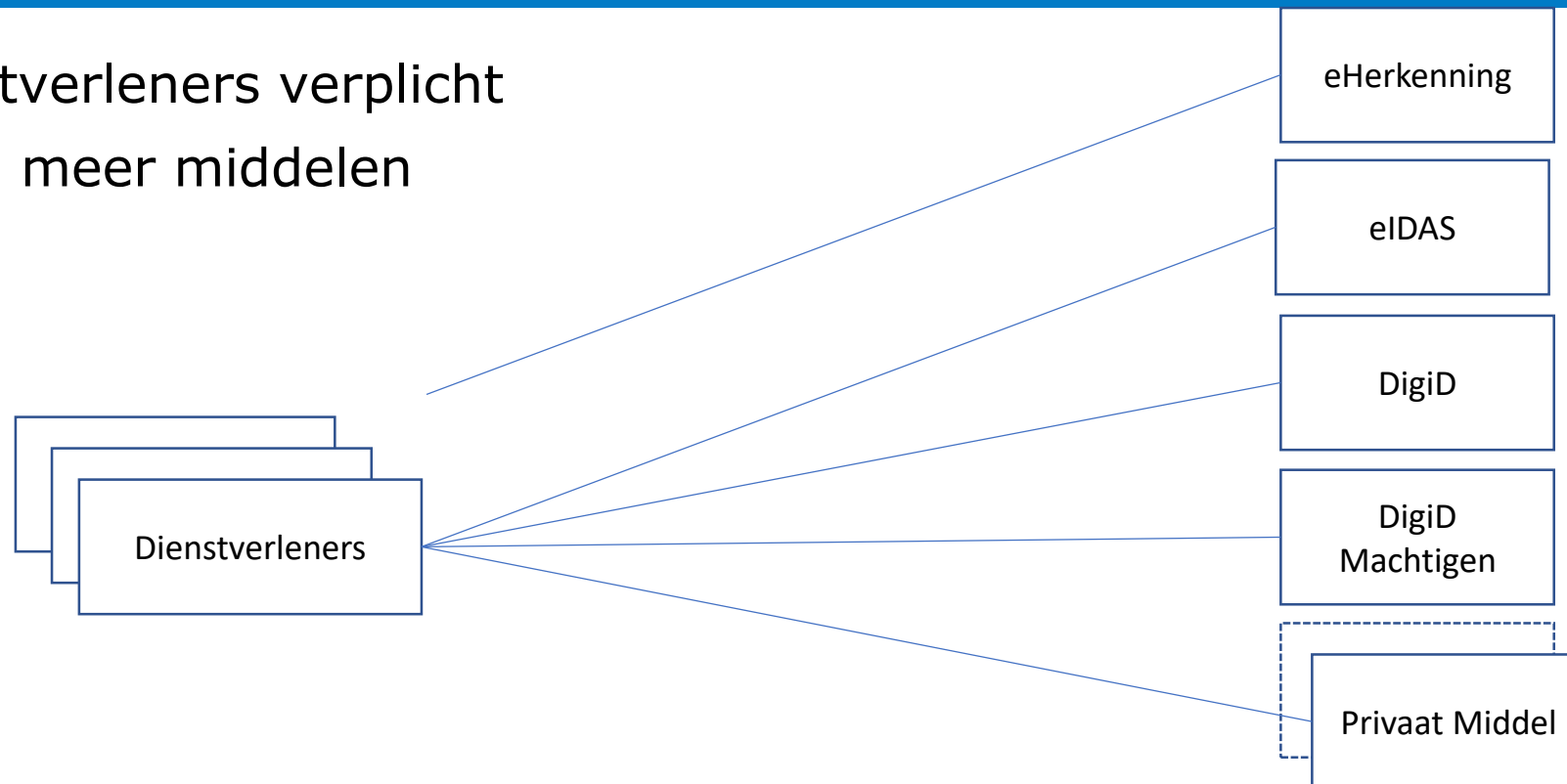
Waar gaat de WDO over? (wie, wat, welke processen worden geraakt)

- Doelen, uitgangspunten, toekomstbestendig, alleen publieke domein
- Verplichtingen voor overheden (publieke dienstverleners):
 - Acceptatieplicht mbt toegelaten eID-middelen. Dus: *geen* eigen/sectorale eID-middelen.
 - Toegelaten worden: publieke (DigiD) *en* private middelen, mits ze voldoen aan eisen (eIDAS gebaseerd)
 - Plicht tot classificeren van hun diensten:
 - *Substantieel* -> bij verwerking persoonsgegevens (bsn), bijv. onderwijs
 - *Hoog* -> bij verwerking bijzondere persoonsgegevens, bijv. medisch
 - Informatiebeveiliging, privacybescherming, bekostiging, standaarden, noodmaatregelen, toezicht
- WDO gaat *niet* over interne (ICT-)infrastructuur en identificatieprocessen



Gevolg van de WDO

- › Resultaat is dat dienstverleners verplicht moeten aansluiten op meer middelen





WDO: waar zit ruimte?

- Tijdelijk toestaan van inlogmiddelen met lager betrouwbaarheidsniveau
- Acceptatie van niet-toegelaten of niet-erkende inlogmiddelen mbt welbepaalde doelgroep
- Acceptatie gebruik publiek middel door zzp'ers/beroepsbeoefenaren
- Gebruik publiek middel buiten publiek domein
- Gebruik publiek middel voor intern systeem
- Acceptatieplicht pas van toepassing na opname organisatie in aansluitschema



..... en de WDO:

- › Is in lijn met Europese wetgeving: eIDAS (sept. 2018)
 - geldt voor aanbestedende organisaties (= overheden)
 - maar: acceptatieplicht geldt alleen mbt diensten/middelen op betrouwbaarheidsniveaus *substantieel* en *hoog*
- › Is AVG *proof*: WDO (privacyregels) en ICT (oa privacy by design)
- › Ontzorgt overheden dmv publieke routeringsvoorziening (BZK)
- › Faseert DigiD laag nog niet uit
- › Noopt tot veel lagere (technische) regelgeving



Planning Wet Digitale Overheid (indicatief)

2020

- › Behandeling WDO in Parlement; svz
- › Streven: 1/7/20 WDO van kracht
- › BZK: rolt ICT-voorzieningen en publieke middelen uit, bereidt toelating private middelen voor, richt beheer en toezicht in
- › Voorbereiding uitvoeringsregelgeving