NORA nodigt je uit bij ICTU

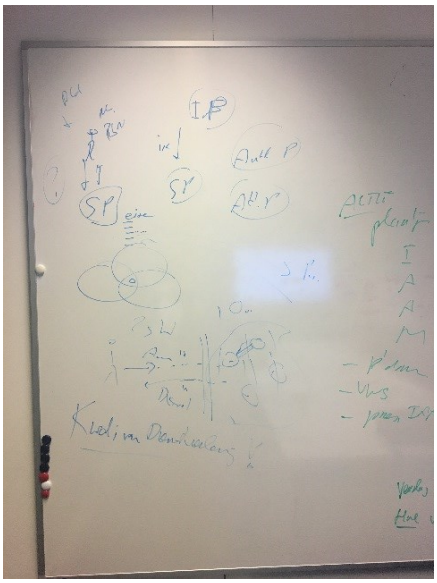
Thema Digitale identificatie en authenticatie

Aanwezigen:

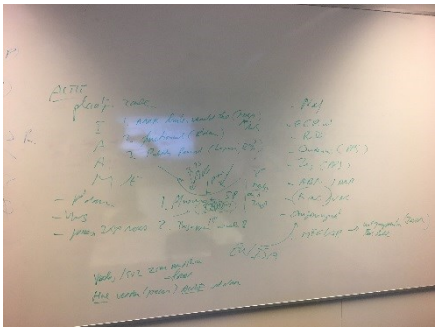
Erwin Reinhoud	Kennisnet
Wim Geurts	Logius
Leon Schipper	Rotterdam
Eric Nijenhuis	UWV
Lieven van der Tas	DJI
Willem Simonis	RvIG
Menno Gmelig Meijling	ICTU
Vincent van de Laar	ICTU
Eric Brouwer	ICTU

Korte inleiding tweede themasessie

De eerste bijeenkomst van dit speerpunt was op 14 november j.l. bij ICTU, tijdens de NORA-middag. Toen is de opdracht geschetst en zijn diverse wensen, ideeën en vragen naar voren gebracht. Het verslag daarvan is aan alle aanwezigen gestuurd en is ook op de NORA gepubliceerd:
https://www.noraonline.nl/wiki/Themasessie_Digitale_Authenticatie_en_identificatie.



Ter voorbereiding op de bijeenkomst van 12 december j.l. is vanuit ICTU een eerste uitwerking gemaakt van de vraag "waar hebben we het precies over?" We hebben dat gedaan in een framework van 4 hoofdvragen waarin we alle 10 inhoudelijke vragen (inclusief subvragen) van de bijeenkomst van 14 november ook konden verwerkt. Daarnaast is ook een eerste beeld geschetst van een streefbeeld, waar op termijn naar toegegroeid zou kunnen worden om dit aspect van de digitale dienstverlening optimaal te regelen. Met een kleine groep (zie bovenstaand) is dit besproken, ook in relatie tot ervaringen vanuit de gemeente Rotterdam (zie de betreffende presentatie).



Naast een goed inhoudelijk gesprek, zijn we een beetje losgegaan op het whiteboard …
En we hebben een paar actiepunten afgesproken, mede ter voorbereiding van de bijeenkomst in januari. Deze acties zijn op de relevante plekken aangegeven.

Doel: *Het wat en waarom van Identificatie en Authenticatie in kaart brengen, opdat we breed gedeelde kennis en beelden krijgen en daarmee alle vraagstukken beter en geprioriteerd kunnen uitwerken om tot gedeelde architectuur oplossingen te komen.*

Doelgroep: *architecten en collega's uit de publieke sector actief betrokken op dit thema.*

1e Resultaat "Waar hebben we het nu precies over?"

We hebben een eerste uitwerking van de begrippen en hun samenhang: in tekst en in beeld.
Met dit onderdeel krijgen we overzicht van waar het domein uit bestaat en wat de verbanden zijn.
We beschouwen dat binnen de context van digitale dienstverlening[1].
En daarbij niet vanuit alleen de belangen van de overheid, maar zo nodig ook die van burgers en bedrijven.

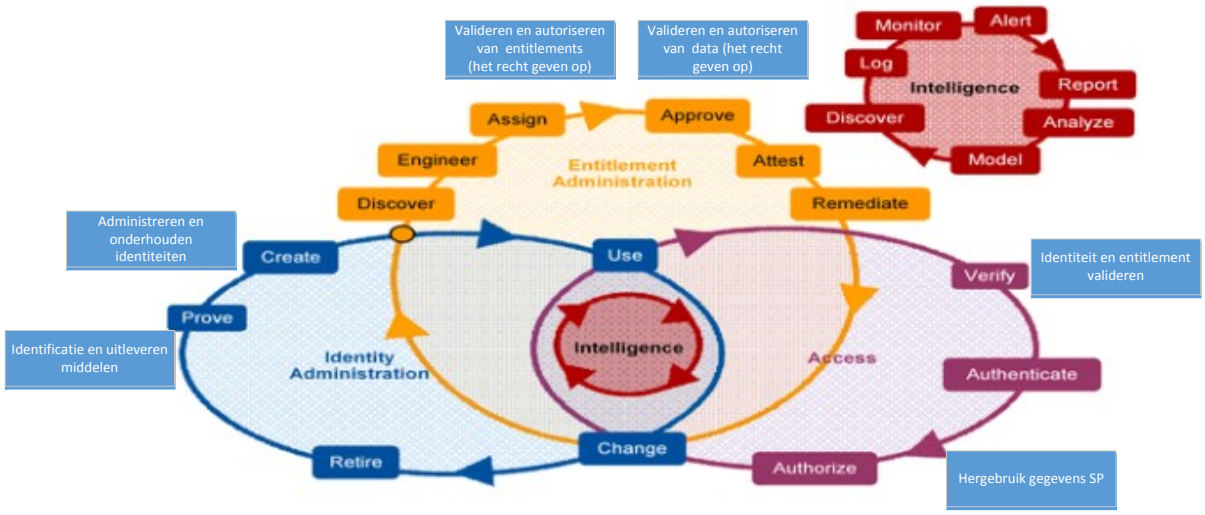
Identificatie, Authenticatie en Autorisatie regelen drie belangrijke voorwaarden voor digitale dienstverlening:

- Identificatie zorgt er voor dat we weten wie je bent;
- Authenticatie zorgt er voor dat we met een bepaalde zekerheid weten dat je ook echt degene bent die je zegt te zijn;
- Autorisatie zorgt er voor dat we weten wat je dan mag (al dan niet door een ander gemachtigd), of juist niet mag.

Als iemand een digitale dienst wil afnemen, dan zal de elektronische identificatie, authenticatie en autorisatie goed geregeld moeten worden om de belangen van zowel de dienstaanbieder als de afnemer te borgen.

Onderstaande plaatje geeft al aardig aan waar het functioneel om gaat.
Het behoeft natuurlijk nog wel een toelichting.
Ook is het niet in het Nederlands.
ACTIE-1: Nagaan of we nog andere aansprekende plaatjes op internet kunnen vinden, onder meer voor:

- communiceren met anderen, buiten deze werkgroep
- onderscheid publiek / privaat



Onderstaande vragen geven aan welke informatiebehoefte bij ons allen hierover bestaat:

1. Identificatie
    a. Hoe weet de dienstaanbieder wie je bent?
    b. Wat is jouw elektronische identiteit?
    c. Ben je een mens of een machine?
    d. Hoe wordt de governance op identiteit geregeld: wie bepaalt / stelt vast? Wie is er in de lead?

2. Authenticatie
    a. En als je zegt wie je bent, met welke zekerheid weet de dienstaanbieder dat dan?
    b. Hoe en waar kan hij jouw elektronische identiteit verifiëren (authenticeren)?

[1] Er zijn natuurlijk ook diensten waar niet van belang is te weten wie de dienst afneemt of wie er eventueel voor betaalt. Denk bijvoorbeeld aan het verstrekken van algemene informatie. In dat geval is Identificatie en / of Authenticatie niet nodig.

c. Authenticatie van wie (burger, ondernemer, etc): hoe wordt de relatie tussen rollen en personen straks vormgegeven?
d. In hoeverre is het wenselijk te differentiëren in niveaus van authenticatie?
e. Komt er een eigen eHerkenning voor ambtenaren (is dat een rol?)?
f. Hoe omgaan met de nieuwe middelen in een grensregio?
g. En met multichannel authenticatie?
h. Het lijkt nu alleen authenticatie.
VOORSTEL: Eerst gaan we breder kijken naar wat IAA voor ons kan betekenen en daarna prioriteren we met uitwerken op basis van concrete behoefte.
i. Waarom alleen digitale authenticatie?
VOORSTEL: Vooralsnog sluiten we eerst aan op "Digitaal, tenzij …" en het niet-digitaal authenticeren wordt op de back-log opgenomen.
j. Ook authenticatie van software en machines?
VOORSTEL: Vooralsnog niet uitwerken, maar op de back-log opnemen.

3. Autorisatie (inclusief machtigen)
   a. En zodra de dienstaanbieder met afdoende zekerheid weet wie je bent, mag je de dienst dan wel afnemen?
   b. Ben je wel geautoriseerd voor deze dienst?
   c. Of mag je eventueel namens een ander die dienst afnemen?
   d. Ben je wellicht gemachtigd door die ander?
   e. Hoe omgaan met een vertegenwoordiger van een burger?
   f. Hoe kan je machtiging over de grens?
   g. Use cases voor machtigen?
   h. Machtigingen zaakgericht of wetsgericht?

4. Wat is nu al mogelijk voor IAA?
   ACTIE-2: De huidige werkwijzen en ook de state-of-the-art invulling van IAA gaan we onderzoeken. (het zijn tevens antwoorden op de vragen 1 t/m 4)

5. In hoeverre is een publiek-private samenwerking NORA-plichtig?
   ACTIE-3: Dit is een algemeen punt, los van IAA, en zal daarom worden uitgezocht door NORA Beheer.
   NB. Door Kabinetsbeleid zijn alleen overheidsorganisaties NORA-plichtig. Er zijn momenteel geen concrete gevallen bekend waar dit PPS-issue speelt.

6. Eenduidigheid in wetgeving en toepassing door juristen van een digitale handtekening
   Hoe kunnen we dat bewerkstelligen?

7. Hoe omgaan met het spanningsveld tussen dienstverleners en aansprakelijkheid nav IAA?

8. Nederlandse versus internationale wetgeving: over welke wetgeving hebben we het dan?
   Denk aan eIDAS.
   ACTIE-4: Uitzoeken welke wet- en regelgeving hierbij van toepassing is.

9. Hoe omgaan met privacy-aspecten (AVG) en informatiebeveiliging (BIR/BIO)?
   VOORSTEL: Vanuit de werkgroep Identificatie en Authenticatie hier vooralsnog geen tijd aan besteden. In de vervolgfase (na mei 2018), kan desgewenst afstemming gestart worden met de betreffende thema-communities.
   Reden hiervoor is het uitganspunt dat de aanbieder van een (digitale) dienst dat moet regelen. Mogelijk dat daar specifieke eisen uit voortkomen voor Identificatie en Authenticatie, maar die zijn momenteel niet bekend. Daarnaast zijn deze aspecten het aandachtspunt van andere werkgroepen, zie onder meer de betreffende NORA-thema's, zodat we dubbel werk moeten voorkomen.

Wat is ons streefbeeld voor IAA?

Onderstaande tekst is de eerste aanzet om te kijken WAT we van IAA nader gaan uitwerken. Een tekst waarmee we anderen kunnen uitleggen welke dingen anders zullen worden wanneer we het streefbeeld voor IAA gaan realiseren. Stel je daarbij het volgende voor:

Dat geregeld zou zijn dat iedere Nederlander (nader te bepalen welke doelgroep precies) tenminste één zodanig betrouwbare elektronische identiteit heeft, dat die daarmee over de gehele wereld, en dus ook in Nederland, digitale diensten van overheden (en zo mogelijk ook van private partijen) kan afnemen.

Dat geregeld zou zijn dat bij die elektronische identiteit ook 1 of meer authenticatie-middelen beschikbaar zijn waarmee door alle betrokken partijen kan worden geverifieerd of degene die zegt een bepaald iemand te zijn dat ook daadwerkelijk is.

En dat geregeld zou zijn dat van elk van die middelen is vastgesteld welke mate van zekerheid dan bestaat dat die bewering juist is.

Als dat allemaal zou zijn geregeld, dan kan elke dienstaanbieder die voor zijn elektronische dienst heeft bepaald met welke zekerheid de identiteit van de dienstafnemer bekend moet zijn, hergebruik (laten) maken van de beschreven identificatie en authenticatie.
En indien dat aan de gestelde eisen voldoet, kan de dienst worden geleverd c.q. afgenomen. Zo nodig kunnen nog meer eisen worden gesteld voordat de dienst kan worden afgenomen. Bijvoorbeeld op basis van rollen, (business)regels, persoonlijke aanvraag of machtigingen.

Waarom is IAA voor ons van belang?

En dit is de eerste tekst waarmee we aan anderen kunnen uitleggen waarom het bovenstaande zo belangrijk is voor onze samenleving. Denk hierbij aan het volgende:

We hebben een wereldwijd stelsel van afspraken waarbij Nationale paspoorten en andere formele reisdocumenten de wereldburgers in staat stellen zich vrij te bewegen over onze planeet.
Zo'n soort afsprakenstelsel is er echter niet voor de digitale reizen die we elke dag maken. We surfen overal heen, doen meer en meer elektronische inkopen en digitaal zaken met de overheid, maar onze elektronische identiteiten zijn op geen stukken na zo betrouwbaar als onze reisdocumenten.
Hierdoor kunnen veel ondernemers en landen niet op voorhand vertrouwen op die elektronische identiteiten (je weet dan immers niet zeker met wie je te maken hebt) en geven daarom maar extra elektronische identiteiten uit die ze zelf wel vertrouwen. Dat is echter omslachtig en zorgt voor het risico dat de burgers te veel identiteiten krijgen, met alle risico's en gevolgen van dien.
Als overheden voor hun burgers geverifieerde identiteiten afgeven, authenticatiemiddelen certificeren en autorisatie- en machtigenvoorzieningen regelen, dan kan dat alle dienstaanbieders daarvan ontlasten. Dienstaanbieders hoeven dan alleen nog de diensten te regelen met bijbehorende authenticatie-eisen. Bijvoorbeeld welk niveau van authenticatie voor die dienst is vereist.

Wie zien we graag betrokken bij het uitwerken van deze vragen?

Binnen mum van tijd konden de aanwezigen aangeven dat ze graag de volgende organisaties een inhoudelijke bijdrage zien leveren:

1. Onderwijs (wereldwijde ervaring met federatieve I en A en met PPS)
2. Zorg (een groot en divers speelveld met PPS)
3. RvIG (beheerder van de BRP en RNI, Self Sovereign Identity)
4. Banken (DNB, ABN e.d. vanwege ambities op gebied van authenticatiemiddelen)
5. VNG en KING / Realisatie (gemeentelijke domein met veel burger-contacten)
6. ECP.nl (publicaties IAM)
7. Naf (samenwerking op thema's en communities)
8. Omgevingswet (grootschalige digitale samenwerking overheid, deels PPS)
9. MFG ArchitectuurRaad (ervaring en behoefte van de grote uitvoerders van de overheid)
10. Europa / ISA (voor aansluiting op internationale ontwikkelingen en -voorzieningen)

ACTIE-5: Betreffende organisaties benaderen voor een bijdrage aan IAA.

Welke stappen moeten we zetten om de beoogde resultaten tijdig te realiseren?
Tijdens ons overleg hebben we geconstateerd dat we meer aandacht zullen moeten besteden aan het proces (en bijbehorende activiteiten) om te borgen dat we de juiste resultaten gaan opleveren en ook in de volgorde waarop dat door betrokkenen gewenst is.
ACTIE-6: Een voorzet maken voor een stappenplan.

Op de agenda voor de eerstvolgende bijeenkomst denken we aan de volgende onderwerpen:
- Bespreken van het stappenplan
- Bespreken van het 1e resultaat "Waar hebben we het nu precies over?"
- Bespreken van het streefbeeld voor IAA
- Besluit nemen over de voorstellen
- De uitkomsten c.q. stand van zaken bespreken van actiepunten

Vervolgbijeenkomsten
In de komende maanden worden werksessies gehouden onder aansturing van Eric Brouwer (namens ICTU werkzaam voor NORA).
De sessies vinden plaats bij de deelnemers van het overleg.
Er hebben zich zo'n 15 actieve deelnemers gemeld.
Voor meer informatie of suggesties, meld je via nora@ictu.nl.

De sessies zijn gepland op:

Data	Tijd	Bij wie?
14 november	13 – 16 uur	ICTU
12 december	14 – 17 uur	ICTU
16 januari	14 – 17 uur	Gemeente Den Haag
20 februari	14 – 17 uur	
20 maart	14 – 17 uur	
17 april	14 – 17 uur	

In de NORA bijeenkomst van 29 mei 2018 (van 13 – 16 uur), worden de (tussen)resultaten gedeeld met belangstellenden.