Healthy Living
Sylviusweg 71
2333 BE Leiden
P.O. Box 2215
2301 CE Leiden
The Netherlands

T +31 88 866 60 00

TNO-rapport

TNO 2022 R10633

Toekomstbestendig maken van Unieke ZorgverlenersIdentificatie (UZI) middelen

Datum	10 januari 2023
Auteur(s)	Jildau Bouwman, Joram Nauta, Geert Kleinhuis, Jins de Jong, Sarah van Drumpt, Kristel Kamstra, Marth Breure, Virag Szijjarto, Sanne Kuijper
Exemplaarnummer	
Oplage	
Aantal pagina's	67 (incl. bijlagen)
Aantal bijlagen	4
Opdrachtgever	VWS
Projectnaam	VWS- gen. voorz. ident.&authenticatie
Projectnummer	060.50449

Inhoudsopgave

1 Inleiding

In de zorg worden steeds meer gegevens digitaal uitgewisseld. Momenteel wordt patiënteninformatie ontsloten voor zorgverleners door zogenaamde Unieke Zorgverlener Identificatiemiddelen (UZI-middelen). De huidige UZI-middelen zijn echter niet volledig geschikt voor de hedendaagse toepassingsmogelijkheden en worden niet altijd als gebruiksvriendelijk ervaren. VWS is daarom gestart met een project dat zich richt op het ontwikkelen van een oplossing zodat nieuwe inlog-middelen de bestaande UZI-middelen op termijn kunnen vervangen. De nieuw te ontwikkelen middelen moeten toekomstbestendig, gebruiksvriendelijk en geschikt voor grootschalig gebruik in het zorgveld zijn. Veiligheid, gebruiksgemak en de behoefte van de gebruikers staan hierbij centraal. Relevant in de besluitvorming zijn ook de systeemkosten van het nieuwe stelsel van middelen.
Toegang tot en het delen van gezondheids- en medische data tussen patiënten en/of medewerkers onderling in de gezondheidszorg is noodzakelijk voor kwalitatief hoogwaardige gezondheidszorg. Tegelijkertijd brengt het delen van de informatie ook zorgen met zich mee over de veiligheid van deze vertrouwelijke en privacygevoelige gegevens. De afgelopen jaren hebben zich verschillende incidenten in de zorg voorgedaan, waarbij onbevoegden toegang hebben gekregen tot privacygevoelige data. Ondertussen zijn de wettelijke eisen aan dataopslag, -toegang en -verwerking verder aangescherpt, de AVG vereist eIDAS hoog als veiligheid niveau voor gezondheidsdata. Op dit moment ligt de Wet Digitale Overheid ter besluitvorming bij de Eerste Kamer. Deze wet regelt dat (semi-)overheid verplicht zijn om identificatiemiddelen van het betrouwbaarheidsniveau ‘substantieel’ of ‘hoog’ te gebruiken om toegang te geven tot onlinediensten waarbij deze betrouwbaarheidsniveaus van toepassing zijn.
Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) heeft TNO gevraagd te onderzoeken hoe het huidige UZI stelsel kan groeien naar een systeem waar identificatie en authenticatiemiddelen op het vereiste hogere betrouwbaarheidsniveau komen. Hierbij is het nadrukkelijk van belang om een werkbare omgeving voor zorgverleners te behouden.
Om te zorgen voor toekomstbestendige identificatie en authenticatiemiddelen in de zorg is eerst geïnventariseerd wat de huidige inlogmiddelen in de zorg zijn en welke betrouwbaarheidsniveaus hierbij horen. Vervolgens is er geanalyseerd welke instapniveau passend is en is er een groeimodel ontwikkeld om naar een hoger betrouwbaarheidsniveau te komen. Hierbij is rekening gehouden met de omvang, het type van de zorgorganisaties, en de financiële impact van de normverschuiving. Ten slotte zijn alleen authenticatieoplossingen meegenomen die beschikbaar zijn zodat de hanteerbaarheid voor de zorgverlener in ieder geval gelijk blijft en waarschijnlijk verbetert.

1.1 Doel onderzoek

Het doel van het onderzoek is om tot een groeimodel te komen tot een toekomst bestendig stelsel voor sterkere authenticatie in de Nederlandse zorg, zonder dat daarbij de werkbaarheid voor de zorgverlener in het geding komt en optimale zorg blijvend kan worden verleend. Er is onderzocht of de huidige UZI-middelen vervangen kunnen worden door een toekomstbestendige oplossing, waarbij gekeken is of er

alternatieven zijn die de huidige oplossing kan vervangen op de gebieden van: techniek, functionaliteit, kosten, beschikbaarheid en betrouwbaarheid.

1.2 Toekomstvisie VWS

VWS heeft voor de toekomstige oplossing van het UZI-register en de uitgifte van bijbehorende middelen de volgende visie vastgesteld.

Voor de juiste zorg op de juiste plek is het randvoorwaardelijk dat zorgprofessionals toegang krijgen tot de juiste (medische) informatie op het juiste moment, waarbij de privacy van patiënten en cliënten gewaarborgd is. Zorgprofessionals kunnen op basis van een betrouwbaar kenmerk uit een authentieke bron digitaal toegang krijgen tot medische gegevens. Dit kenmerk kan door de zorgprofessional gekoppeld worden aan (eigen) identificatiemiddelen die voldoen aan de eisen die door de minister van VWS aan deze middelen worden gesteld. Deze identificatiemiddelen kunnen door zorgprofessionals worden gebruikt voor identificatie, authenticatie, autorisatie, en het verzegelen alsmede ondertekenen van digitale (medische) gegevens.

Voor de toekomst van de UZI-middelen wil VWS toe naar een stelsel waarbij voor de zorgaanbieder keuze ontstaat in het te gebruiken authenticatiemiddel. Dat betekent dat de huidige opzet van het gebruik van identificatie en authenticatiemiddelen moet worden aangepast. De volgende componenten worden onderscheiden en zullen daarmee een plek hebben in de oplossingsrichting:

- *Een register met een uniek nummer per zorgverlener*
  Een door de overheid beheerd register waarin zorgverleners een registratie kunnen krijgen. Met de registratie ontstaat een uniek identificerend nummer dat gekoppeld is aan de zorgverlener (als persoon). Het huidige UZI-register geeft al unieke, identificerende nummers uit. Deze worden in de huidige situatie hard gekoppeld aan een UZI-middel. In de toekomst willen we dit uniek identificerende nummer verstrekken in de vorm van een kenmerk (‘attribuut’).

- *Oplossingen voor authenticatiemiddelen*
  Voor de toekomst zien we als authenticatiemiddelen de door de overheid erkende middelen die beschikbaar komen onder de Wet Digitale Overheid. De uitgifte van huidige UZI-middelen zal daarmee komen te vervallen. De door de overheid erkende middelen zijn zowel de publieke als de private middelen, waaronder DigiD en Europese erkende eIDAS-middelen. Daarnaast is het de wens van het zorgveld dat ook ‘zorgeigen’ authenticatiemiddelen kunnen worden toegepast. Dit zijn middelen die uitgegeven worden door de zorgorganisatie zelf, zoals ziekenhuispassen. Voor alle middelen zal gelden dat ze ten minste moeten voldoen aan bepaald betrouwbaarheidsniveau en een uniek identificerend kenmerk van de handelende persoon moeten kunnen opleveren.

- *Een (ont-)koppelpunt van identiteiten*
  De huidige authenticatiemiddelen, zoals DigiD, leveren na authenticatie een uniek kenmerk op, namelijk het BSN. Het BSN is de sleutel waarmee een burger bekend is bij overheden, uitvoeringsinstanties en organisaties die een wettelijke taak uitoefenen. Het BSN is echter niet de identificerende sleutel die binnen de zorg wordt gebruikt om een zorgprofessional te herkennen: binnen de zorg wordt daartoe het UZI-nummer als uniek identificerend kenmerk gehanteerd. Om gebruik te kunnen maken van authenticatiemiddelen die een BSN opleveren, dient er een

ontkoppeling plaats te vinden waarbij het BSN (als sleutel) wordt omgeruild voor het UZI-nummer. Het UZI-nummer kan vervolgens als uniek identificerend kenmerk (“attribuut”) gebruikt worden. Zo kan een zorgprofessional de digitale authenticatie voor werk- en privézaken gescheiden houden, maar wel hetzelfde authenticatiemiddel naar eigen keuze gebruiken. Bovendien voorkomt deze oplossing het gebruik van BSN’s binnen zorgprocessen waar het gaat om de identificatie van zorgprofessionals.

- *Attribuutregisters met aanvullende kenmerken*
  Voor adequate dienstverlening is een kale identiteit, die enkel bestaat uit een UZI-nummer te beperkt. Zo wordt bij het huidige UZI-middel de ‘rolcode’ beschikbaar gesteld. Naast het register met UZI-nummers zijn ook aanvullende kenmerken uit andere registers, zoals het BIG-nummer, nodig. Waar het gaat om registers onder de verantwoordelijkheid van het ministerie van VWS ligt het voor de hand dat de overheid de koppeling tussen het UZI-nummer en aanvullende kenmerken tot stand zal brengen. Daarnaast zien we mogelijkheden voor de zorg om zelf aanvullende kenmerken te koppelen aan het UZI-nummer, bijvoorbeeld door beroepsregisters met relevante aanvullende kenmerken te ontsluiten via het UZI-nummer van een professional.

- *Een afsprakenstelsel*
  Een afsprakenstelsel is een wettelijk afdwingbare set van specificaties, regels en afspraken die het beoogde systeem reguleert. In het afsprakenstelsel moeten bijvoorbeeld afspraken gemaakt worden op welke manier het nummer vanuit het UZI-register gekoppeld kan worden aan de authenticatiemiddelen, naast bijvoorbeeld afspraken over de manier waarop aanvullende registers gekoppeld kunnen worden aan het UZI-nummer. Ook zal bijvoorbeeld beschreven moeten worden op welke manier het UZI-nummer uit het UZI-register gebruikt kan, of wellicht zelfs moet, worden binnen de zorg. Tot slot worden in het stelsel afspraken gemaakt over technische specificaties en de omgang met storingen, fraude, misbruik, toezicht, handhaving, et cetera.

De oplossingsrichting is tot stand gekomen in samenwerking met het zorgveld. Het zorgveld heeft de oplossingsrichting goed ontvangen en VWS is inmiddels een wetgevingstraject gestart om het nieuwe UZI-stelsel te kunnen implementeren. Totdat de wetgeving in werking treedt, wordt voorgesorteerd op implementatie door zogenaamde proof-of-concepts en pilots uit te voeren. Hiermee wordt het zorgveld voorbereid op implementatie en kan in delen van de zorgsector vooruitlopend op grootschalige implementatie verlichting worden geboden. Met POC’s wordt de oplossingsrichting in een testomgeving technisch beproefd. Beproefde techniek wordt met pilots naar de praktijk gebracht om ervaring in en met het zorgveld op te doen. Daarnaast is deze aanpak van strategisch belang en noodzakelijk voor acceptatie in het zorgveld. In aanloop naar grootschalige implementatie worden verschillende pilots uitgevoerd in delen van het zorgveld waarbij verschillende zorgprofessionals ervaring op kunnen doen met verschillende inlogmiddelen.

1.3 Onderzoeksvragen

Concreet luidt de onderzoeksvraag als volgt:

1) Wat zijn binnen het zorgveld de huidige, beschikbare inlogmiddelen en de bijbehorende betrouwbaarheidsniveaus?
2) Wat is het instapniveau van een groeimodel om naar een hoger betrouwbaarheidsniveau te komen? Hierbij wordt rekening gehouden met
   i) de omvang van de zorgorganisatie;
   ii) het type zorgorganisatie, variërend van apothekers tot ziekenhuis;
   iii) duiding van de financiële impact van de normverschuiving van de huidige situatie naar een hoger betrouwbaarheidsniveau.
3) Hoe blijft de situatie werkbaar voor de zorgverlener en kan de werksituatie verbeterd worden?

1.4 Opdracht aan TNO

TNO heeft in opdracht van VWS de volgende elementen uitgezocht om de UZI-middelen toekomstbestendig te maken.

1) **Inventarisatie zorgpartijen:** Onderzoek naar de status quo van bestaande authenticatiemiddelen, -wensen en -verwachtingen van diverse zorgverleners (10-20 type zorgverleners). Er is een inventarisatie gedaan met verschillende zorgpartijen om te kijken wat ze gebruiken om in te loggen. Van de UMC's heeft TNO al een goed beeld en zijn om deze reden niet opnieuw bevraagd. Er is een uitgebreide vragenlijst opgesteld, zie bijlage A.
2) **Roadmap naar hoger betrouwbaarheidsniveau voor authenticatie**: Een inventarisatie van omgevingsrisico's en relevante ontwikkelingen is uitgewerkt. De verschillende betrouwbaarheidsniveaus zijn in de workshops besproken om te kijken wat haalbaar is.
3) **Kostenscenario's naar aanleiding van inzichten en roadmap**: Er zijn verschillende kosten scenario's op hoofdlijnen uitgewerkt worden om de financiële impact van de normverschuiving van de huidige situatie naar een hoger betrouwbaarheidsniveau voor het zorgveld te duiden.

Gedurende het proces zijn maandelijkse workshops/sprints met diverse expertises gehouden om samen met VWS de randvoorwaarden te bepalen.

1.5 Authenticatie

1.5.1 Overzicht en begrippenlijst

Identificatie is het vaststellen wie iemand is, bijvoorbeeld aan de hand van een paspoort of een emailadres.
Authenticatie is het controleren dat iemand is, wie hij of zij beweert te zijn.
Dit wordt gedaan door iets te tonen dat alleen de geïdentificeerde persoon kan laten zien. Het weten van een geheim wachtwoord is een voorbeeld hiervan. Het getoonde wordt een authenticatiemiddel genoemd.
Een authenticatiefactor is een categorie van authenticatiemiddelen, zie figuur 1, namelijk:

- Iets wat je weet;
- Iets wat je hebt;
- Iets wat je bent, bijvoorbeeld een biometrische factor;
- Ergens waar je bent, bijvoorbeeld een IP-adrescontrole, of
- Iets wat je doet, bijvoorbeeld een plaatje tekenen op een smartphone.

Iets wat je weet	Iets wat je hebt	Iets wat je bent
		
- Wachtwoord - Pincode - Antwoord op geheime vraag	- Smartcard / werknemerspas - App op smartphone - Simkaart - RSA-token - Digitaal certificaat - IRMA	- Vingerafdruk - Gezichtsherkenning - Irisscan

Figuur 1 Overzicht van de meest gangbare authenticatiefactoren en voorbeelden van enkele - middelen.

De laatste twee zijn minder algemeen aanvaard als authenticatiefactor. Iets-wat-je-doet kan vaak samengevoegd worden met iets-wat-je-weet. Ergens-waar-je-bent wordt vaker gebruikt als beheersmaatregel dan als expliciete authenticatiefactor.

Autorisatie is het vaststellen wat iemand mag. Een effectieve autorisatie vereist goede authenticatie. De autorisatie valt verder buiten het bereik van dit onderzoek.

De eIDAS-wet [EU 910/2014] schrijft voor dat er bij het bepalen van het betrouwbaarheidsniveau het noodzakelijk is dat er rekening gehouden wordt met de ISO-norm 29115 en het Quality authenticator scheme van het STORK-project D2.3. De authenticatienorm voor de zorg NEN7512:2015 baseert zich op deze normen. Deze normen worden in acht genomen bij de omschrijving van betrouwbaarheidsniveaus.

In paragraaf 1.5.3 wordt een overzicht gegeven van de mogelijke authenticatiefactoren. Kort samengevat vereist identificatie en authenticatie op niveau hoog een fysieke verschijning of iets gelijkwaardigs tijdens het identificatie- en uitreikingsproces [EU 910/2014 Art. 24], een waterdichte uitreikingsprocedure en een gekwalificeerd elektronisch certificaat met een tweede factor. Deze tweede factor moet een wachtwoord/pin-code of een biometrische factor zijn.

Europese leveranciers van zulke diensten op betrouwbaarheidsniveau hoog staan vermeld op de ‘European Union Trusted Lists’[1]. Deze partijen hebben een certificering en accreditatie om bepaalde vertrouwensdiensten op niveau eIDAS hoog te leveren. Gekwalificeerde elektronische handtekeningen benodigd voor gekwalificeerde certificaten zijn hier een voorbeeld van. Alleen gekwalificeerde elektronische handtekeningen zijn wettelijk en automatisch gelijk aan met de handgeschreven handtekeningen.

1.5.2 Betrouwbaarheidsniveaus in diverse authenticatiestandaarden

Diverse relevante authenticatiestandaarden gebruiken verschillende namen voor de verschillende betrouwbaarheidsniveaus. Echter, in grote lijnen komen de niveaus met elkaar overeen zoals weergegeven in onderstaande tabel 1. Tenzij anders aangegeven zullen de betrouwbaarheidsniveaus uit eIDAS gebruikt worden in dit rapport. Desalniettemin zijn er wel degelijk verschillen te vinden, bevatten niet alle authenticatiestandaarden dezelfde onderwerpen en zijn de eisen niet in elke standaard even scherp geformuleerd. Telkens is geprobeerd de standaard met de meest concrete omschrijvingen te vinden, zonder andere standaarden tegen te spreken om tot concrete oplossingen te kunnen komen.

Een voorbeeld hiervan is de opzet van een sterke-authenticatiesysteem. De eIDAS-wet is technologieneutraal geformuleerd en biedt daardoor minder concrete processen om tot sterke authenticatie te komen. Daarom wordt in paragraaf 1.5.6 in figuur 2 en de tabellen 2 tot en met 9 een versimpeld overzicht van de beoordeling van een authenticatiesysteem volgens Stork gegeven. Dit is het Quality Authentication Assurance-systeem, kortweg QAA.

Tabel 1 Versimpeld overzicht van vergelijkbare betrouwbaarheidsniveaus in enkele authenticatiestandaarden.

Standaard	eIDAS	Stork	NEN7512	ISO 29115
Betrouwbaarheids-niveau		QAA1	Laag	LoA1
	Laag	QAA2	Middel	LoA2
	Substantieel	QAA3	Hoog	LoA3
	Hoog	QAA4	Zeer hoog	LoA4

1.5.3 Authenticatiefactoren

Om een beter beeld te krijgen bij de authenticatiefactoren en -middelen worden ze hieronder besproken. Daarnaast worden enkele relevante aanvullende maatregelen genoemd die voor een bepaald betrouwbaarheidsniveau kunnen zorgen.

Factor: Iets wat je weet

- **Geheime kennis (wachtwoord of PIN-code)** wordt het meeste toegepast. Volgens eIDAS kan dit middel een laag betrouwbaarheidsniveau bieden, maar enkel als er maatregelen worden getroffen (volgens de NEN-EN 12251).

[1] EU Trust Services Dashboard (europa.eu)

Denk hierbij aan een zelfgekozen wachtwoord dat niet gemakkelijk te raden is, nergens in leesbare vorm wordt opgeslagen, nooit in onversleutelde vorm verzonden wordt, en regelmatig en op elk moment te wijzigen is. Bovendien moet de persoon vooraf geregistreerd zijn en zijn identiteit en eventuele kwalificaties gecontroleerd zijn zoals beschreven bij Registratiewijze 2 van de NEN 7512. Enkel als het met een andere authenticatiefactor wordt gecombineerd kan het betrouwbaarheidsniveau hoger worden dan eIDAS laag.

Factor: Iets wat je hebt

- **Fysiek bezit (token)** komen in velen soorten en maten voor, zoals mobiele telefoons, pasjes en sim-kaarten. Tokens zijn fysieke dragers of ontvangers van pincodes voor eenmalige authenticatie, ook wel One Time Passwords (OTP) genoemd. Ze bevatten een geheime sleutel op basis waarvan de pincode gegenereerd of ontvangen wordt. Een voorbeeld hiervan zijn authenticator-apps die eenmalige wachtwoorden genereren op basis van een geheime, unieke QR-code of wachtwoord.

  Voor een eIDAS hoog-classificatie eist de NEN7512 dat het token voldoet aan de NEN-EN 419211. Daarnaast moet het authenticatiemiddel via een fysieke verschijning en middels een waterdichte procedure zijn uitgereikt. De beste bescherming wordt geboden als de token de privésleutel zelf genereert en niet uitgelezen kan worden, zodat het ook niet gekopieerd kan worden. Hierbij is te denken aan een smartcard voor persoonlijk gebruik of een HSM (Hardware Security Module) voor een informatiesysteem. Bovendien moet de token gebruikt worden in combinatie met een wachtwoord, PIN-code of biometrie.

- **Toetsbare verklaring (digitaal certificaat)** wordt toegepast voor de authenticatie van zowel personen, organisaties als systemen. Zulke certificaten worden uitgegeven door een vertrouwde instantie. Deze houdt ze bij en trekt ze zo nodig in. Door middel van een elektronische handtekening van de uitgevende partij is de echtheid na te gaan. Een UZI-pas is een voorbeeld van een drager met een certificaat erop, ondertekend door het CIBG.

  Als het certificaat gekopieerd kan worden, bijvoorbeeld omdat het op een reguliere USB-stick staat, wordt er gesproken van een zacht certificaat in plaats van een hard certificaat, [Annex I van de Directive 1999/93/EC]. Zachte certificaten worden meestal beveiligd met een wachtwoord. Deze certificaten zijn ongeschikt voor authenticatie op betrouwbaarheidsniveau hoog. Dit volgt uit tabel 5 in paragraaf 1.5.6.

  De certificaten opgeslagen op een HSM en toegankelijk zijn via het internet vormen nog een bijzondere categorie. In dit geval is de gebruiker dus niet fysiek in het bezit van de geheime sleutel, maar wel als enige in staat om deze te gebruiken. Zulke oplossingen worden in de eIDAS-wet expliciet geclassificeerd als eIDAS hoog, ook als de toegang tot de HSM met authenticatie op niveau eIDAS substantieel plaatsvindt [EU 910/2014 Art 24.1].

Authenticatie op niveau eIDAS hoog vereist dat de certificaten de naam van de geauthentiseerde bevatten. De certificaten zijn dus persoonsgebonden. Dit betekent dat het authenticatiemiddel niet alleen door bezit aan een persoon gekoppeld is, maar ook via het authenticatiemiddel zelf.

Daarnaast is het voor authenticatie op niveau hoog vereist dat er gekwalificeerde certificaten gebruikt worden. Deze moeten ondertekend worden met gekwalificeerde handtekeningen. Dit betekent dat de uitgever op de EU trusted list[2] moet staan. Bijvoorbeeld het CIBG staat hierop.

Factor: Iets wat je bent

- **Fysiek kenmerk (biometrie)** wordt vaak toegepast als gemakkelijk alternatief voor een pincode. Enkel in bijzondere gevallen kunnen gebruikers verplicht worden om met biometrische middelen te authentiseren[3]. Op vrijwillige basis als vervanging van een pincode is biometrie wel vaak mogelijk.

  Biometrie geeft een laag betrouwbaarheidsniveau, maar gecombineerd met een andere authenticatiefactor kan het een substantieel of hoog betrouwbaarheidsniveau bereikt worden. Veel gebruikers vinden het gebruik van biometrie makkelijker dan het gebruik van een pincode of wachtwoord.

1.5.4 Uitgifteproces

Zoals benoemd in paragraaf 1.5.1 is een fysieke verschijning en een waterdichte uitreiking van authenticatiemiddelen twee belangrijke eisen voor het eIDAS hoog betrouwbaarheidsniveau. In dit overhandigingsproces van authenticatiemiddelen zijn verschillende stappen van belang.
STORK QAA biedt een kader met voorwaarden waaraan voldaan moet worden om van een bepaald betrouwbaarheidsniveau te mogen spreken. Hierin wordt onderscheid gemaakt tussen de registratiefase en elektronische-authenticatiefase. Hieronder wordt kort beschreven welke factoren van belang zijn in deze twee fases.
De **registratie** omvat de volgende criteria.

1. De kwaliteit van de identificatieprocedure, waarbij de gebruiker wordt geïdentificeerd voordat er een authenticatietoken wordt uitgegeven. Het betrouwbaarheidsniveau is afhankelijk van de volgende factoren.
   - Vindt er een fysieke verschijning plaats tijdens de registratie of uitgifte van het certificaat?
   - De kwaliteit van beweringen over de identiteit die tot een unieke identificatie leiden. Een paspoortnummer biedt bijvoorbeeld meer zekerheid dan een geboortedag.
   - De validatie van de beweringen, te bepalen aan hand van de wijze waarop de echtheid bewezen is. Hierbij kan gedacht worden aan emailverificatie, het vergelijken met een officiële identiteitsbron of het controleren van een digitale handtekening.
2. De kwaliteit van het afgifteproces. Het authenticatiemiddel kan afgegeven worden via email, (aangetekende) post of persoonlijk overhandigd worden. Daarnaast is het mogelijk om het authenticatiemiddel via meerdere kanalen af te geven, die naderhand gecombineerd moeten worden. De hoogste zekerheid in het algehele

[2] https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/NL
[3] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6005&showbutton=true&keyword=avg

registratieproces wordt verkregen als de afgifte fysiek wordt afgehandeld, waarbij de identiteit wordt gevalideerd aan de hand van een officieel identiteitsdocument afkomstig van de overheid.

3. De kwaliteit van de entiteit die de identiteitsgegevens afgeeft. Een dergelijke uitgevende entiteit kan bijvoorbeeld een elektronische-identiteitsprovider of een certificeringsinstantie zijn. De organisaties op de EU trusted list hebben een specifieke accreditatie ontvangen om binnen de EU vertrouwensdiensten op het hoogste betrouwbaarheidsniveau te leveren.

Naast de registratiefase is de kwaliteit van de elektronische-authenticatiefase van belang bij het bepalen van het betrouwbaarheidsniveau. Bij de **elektronische authenticatie** wordt het verstrekte identiteitsbewijs geverifieerd op authenticiteit. De kwaliteit van deze fase is afhankelijk van de volgende factoren.

4. Type en robuustheid van de identiteitsgegevens, bijvoorbeeld een gebruikersnaam, persoonsnummer of een certificaatnummer.
5. Beveiliging van het authenticatiemechanisme. Dit verwijst naar de robuustheid van het authenticatiemechanisme. Oftewel: in hoeverre is het mechanisme bestand tegen de in de literatuur beschreven aanvallen. Des te meer bescherming tegen aanvallen wordt geboden, des te hoger de zekerheid dat het om een authentiek identiteitsbewijs gaat.

1.5.4.1 Over de fysieke verschijning tijdens de registratiefase

In de praktijk wordt er in de zorg nog maar weinig gebruik gemaakt van middelen met een hoog betrouwbaarheidsniveau. Eén oorzaak hiervan is dat niet wordt voldaan aan de juiste registratiewijze [Registratiewijze 4 NEN7512]. Deze vereist dat de identiteit van de aanvrager wordt nagegaan door middel van een fysieke verschijning en een controle van een identiteitsdocument. Enkele leveranciers op de EU trusted list hebben dit ingevuld met een ‘digitale fysieke verschijning’. Dit wordt ook als voldoende ervaren voor een hoog betrouwbaarheidsniveau binnen eIDAS..

Eén van de gesproken aanbieders biedt een online intake van een kwartier met onder andere videobeeld en paspoortcontrole. Op basis daarvan geven zij gekwalificeerde certificaten uit als Qualified Trust Service Provider (QTSP) voor vertrouwensdiensten als veilig ondertekenen, versleutelde informatie-uitwisseling, inloggen en archiveren.

Het Europese standaardisatie-instituut werkt aan technische rapporten [ETSI TR 119 460, ETSI TR 119 461] over zulke ‘digitale fysieke verschijningen’. Het valt te verwachten dat dit in de toekomst voldoende zal zijn voor een hoog betrouwbaarheidsniveau.

1.5.5 Huidige authenticatie-eisen

Naast de beschreven standaarden rondom authenticatie, wordt er in de zorg vooral gekeken naar de geldende, bindende NEN-standaarden 7510 en 7512. Daarom worden hieronder de belangrijkste eisen aan authenticatie in de zorg volgens deze normen benoemd.

De NEN 7510-2:2017 stelt in §9.4.1 dat gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, de identiteit van gebruikers behoren vast te stellen door middel van authenticatie met ten minste twee factoren. De NEN 7510-2 bestaat uit beheersmaatregelen die gebruikt kunnen worden om aan de eisen uit de NEN 7510-1 te voldoen [NEN7510-1 §0.6.2], maar niet bindend zijn. De Autoriteit Persoonsgegevens[4] baseert zich op de NEN 7510-2, maar interpreteert deze als bindend.

De NEN 7510-1:2017 is het bindende deel van de NEN 7510. Het is verplicht voor zorgorganisaties om hieraan te voldoen. In bijlage A hiervan zijn beheersmaatregelen uit de NEN 7510-2 normatief opgenomen. Vergelijk bijvoorbeeld NEN 7510-1:2017 A.9.4.1 en NEN 7510-2:2017 §9.4.1. De NEN 7510-1 §6.1.3 schrijft voor dat in een verklaring van toepasselijkheid gerechtvaardigd moet worden waarom bepaalde beheersmaatregelen uit de NEN 7510-2 uitgesloten kunnen worden.
Samengevat betekent dit dat de beheersmaatregelen uit de NEN 7510-2 dus niet verplicht zijn, mits uitgelegd wordt waarom deze niet geïmplementeerd worden en hoe de beoogde doelen uit de NEN 7510-1 alsnog behaald worden.

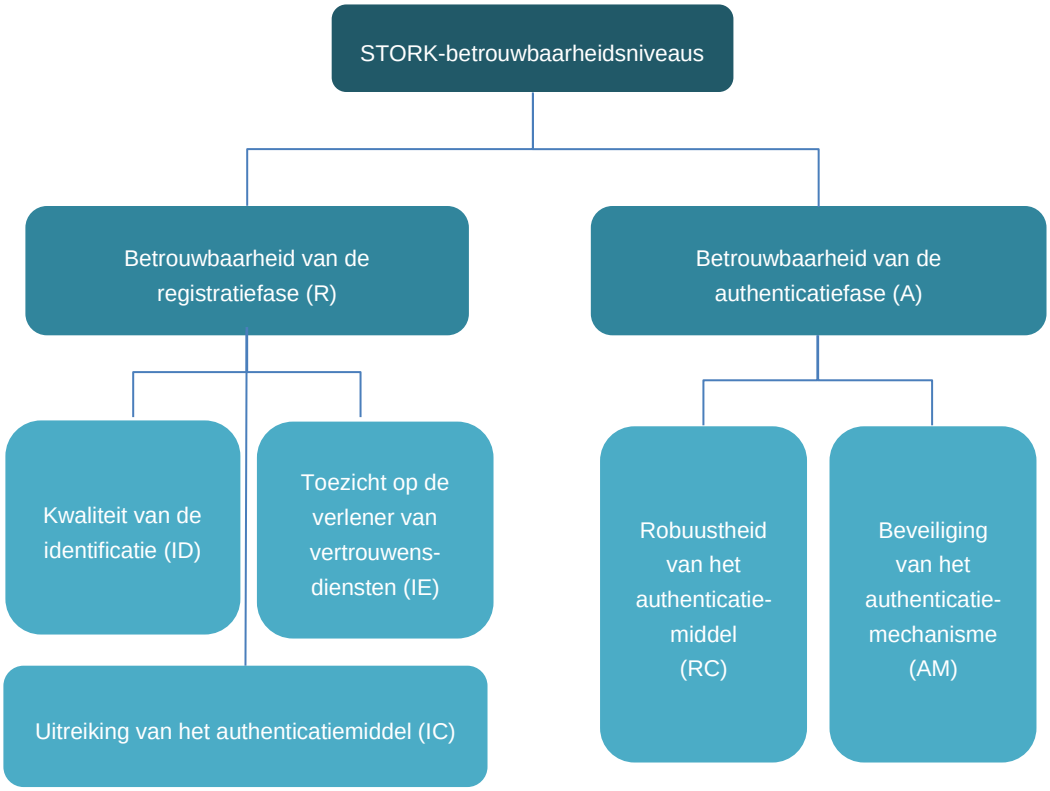
Op de beveiliging van ad-hoc berichten, zoals email- en chatberichten, is de NTA 7516 van toepassing. In §5.6 stelt deze dat voor persoonlijke gezondheidsinformatie authenticatie op niveau eIDAS substantieel vereist is. Voor gegevens waarop het medisch beroepsgeheim van de professional rust, is het betrouwbaarheidsniveau eIDAS hoog vereist. Echter, dit is slechts van toepassing op ad-hoc-uitwisseling van berichten, zoals email of chatapplicaties en niet voor alle systemen.

Interessant om te vermelden is dat het normontwerp NEN 7521 §12.1-3 een hoog betrouwbaarheidsniveau vereist voor de identificatie van een persoon - werknemer of patiënt - die het medisch dossier van een persoon wil raadplegen.

1.5.6 Authenticatie volgens STORK

De onderstaande figuur en tabellen geven een (versimpelde) weergave van de bepaling van een betrouwbaarheidsniveau volgens het Quality Authenticator scheme [Stork D2.3].

[4] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_haga_ziekenhuis.pdf



Figuur 2 Overzicht van het STORK-authenticatiemodel.

Tabel 2 Overzicht van STORK-betrouwbaarheidsniveaus. De gegeven A- en R-scores zijn de benodigde scores om tot een bepaald STORK-betrouwbaarheidsniveau te komen. Voor QAA3, bijvoorbeeld, is een A-score A3 en R-score R3 nodig.

	STORK-betrouwbaarheidsniveau			
	QAA1	QAA2	QAA3	QAA4
R-score (Tabel 6)	R1	R2	R3	R4
A-score (Tabel 3)	A1	A2	A3	A4

Tabel 3 Kwaliteit van de authenticatiefase. De gegeven AM- en RC-scores zijn de benodigde scores om tot een bepaalde kwaliteit van de authenticatiefase te komen. Dit wordt weergegeven met de A-score. Voor A3, bijvoorbeeld, is AM-scores AM3 en RC-scores RC3 nodig.

	Kwaliteit van de authenticatiefase			
	A1	A2	A3	A4
RC-score (Tabel 5)	RC1	RC2	RC3	RC4
AM-score (Tabel 4)	AM1	AM2	AM3	AM4

Tabel 4 Beveiliging van het authenticatiemechanisme.

	Beveiliging van het authenticatiemechanisme			
Het authenticatiemechanisme biedt..	*AM1*	*AM2*	*AM3*	*AM4*
- geen bescherming tegen bekende aanvallen.	*			
- enige bescherming tegen bekende aanvallen.	*	*		
- bescherming tegen de meeste bekende aanvallen.	*	*	*	
- bescherming tegen alle bekende aanvallen. Vergelijkbaar met EAL4+ van de Common Criteria.	*	*	*	*

In tabel 5 is een kleine wijziging aangebracht ten opzichte van de oorspronkelijke tabel [Stork D2.3 tabel 9]. Er is hier expliciet bijgezet dat de certificaten of OTP-tokens met een pincode beveiligd moeten zijn, terwijl in Stork geëist wordt dat de geauthentiseerde bewijst dat zij controle heeft over de sleutel. Dit laatste kan natuurlijk ook door middel van een wachtwoord of een biometrische controle, maar een pincode is het minimale.

Tabel 5 Robuustheid van het authenticatiemiddel. Het verschil tussen harde en zachte certificaten wordt beschreven in paragraaf 1.5.3 onder Toetsbare verklaring.

	Robuustheid van het authenticatiemiddel			
Het authenticatiemechanisme biedt..	*RC1*	*RC2*	*RC3*	*RC4*
Pincode of zwak wachtwoord	*			
Sterk wachtwoord	*	*		
Zachte certificaat of One-time-password token met pincode	*	*	*	
Gekwalificeerde zachte certificaten volgens eIDAS 910/2014 met pincode	*	*	*	
Harde certificaten met pincode	*	*	*	
Gekwalificeerde harde certificaten volgens eIDAS 910/2014 met pincode	*	*	*	*

Tabel 6 Kwaliteit van de registratiefase. De gegeven IC-, ID- en IE-scores zijn de benodigde scores om tot een bepaalde kwaliteit van de registratiefase te komen. Dit wordt weergegeven met de R-score. Voor R3, bijvoorbeeld, is ID-score ID3, IC-score IC3 en IE-score IE3 nodig.

	Kwaliteit van de registratiefase			
	R1	R2	R3	R4
ID-score (Tabel 9)	ID1	ID2	ID3	ID4
IC-score (Tabel 7)	IC1	IC2	IC3	IC4
IE-score (Tabel 8)	IE1	IE2	IE3	IE4

Tabel 7 Uitreiking van het authenticatiemiddel.

	Uitreiking van het authenticatiemiddel			
	IC1	*IC2*	*IC3*	*IC4*
Uitreiking zonder verificatie	*			
Lichte verificatie *- Bijvoorbeeld via de post of een tijdelijke email-link.*	*	*		
Stevige verificatie *- Bijvoorbeeld via de post na controle van het adres.* *- Bijvoorbeeld online na een authenticatie op niveau QAA3.*	*	*	*	
Grondige verificatie *- Bijvoorbeeld een uitreiking na fysieke, persoonlijke verschijning en identificatie.*	*	*	*	*

'*Gekwalificeerd volgens eIDAS 910/2014*' betekent ook dat de uitgever vermeld staat op de EU trusted list [eIDAS 910/2014 Art 23.] De begrippen '*Met overheidsovereenkomst*' en '*Met overheidsaccreditatie of supervisie*' worden in tabel 8 niet verder toegelicht. Ook in Stork D2.3 wordt deze niet verder uitgewerkt. En omdat STORK geschreven is voor authenticatie richting overheden is de overheidsrol niet noodzakelijkerwijze van toepassing buiten dit domein. Ook de ISO29115 en de NEN7512 zijn op dit punt niet eenduidig.

Tabel 8 Toezicht op de verlener van vertrouwens-diensten.

	Toezicht op de verlener van vertrouwensdiensten			
	IE1	*IE2*	*IE3*	*IE4*
Geen toezicht, overeenkomst of accreditatie	*			
Met overheidsovereenkomst	*	*		
Met overheidsaccreditatie of supervisie	*	*	*	
Gekwalificeerd volgens eIDAS 910/2014	*	*	*	*

Tabel 8 Kwaliteit van de identificatie. Voor kwaliteit ID3 mogen of de + of de x gebruikt worden. Er is dus en fysieke (x) en een digitale (+) registratiemogelijkheid. Voor de digitale mogelijkheid gelden zwaardere identificatie-eisen.

	Kwaliteit van de identificatie			
	ID1	*ID2*	*ID3*	*ID4*
Geen fysieke aanwezigheid vereist.	*	*	+	
Eenmalige fysieke verschijning tijdens de registratie	*	*	*	*
Fysieke verschijning bij uitreiking	*	*	*	*
Geen unieke identificatie van de persoon	*			
Unieke identificatie met behulp van publieke gegevens (bijv. adres, geboortedatum, naam)	*	*	x	
Unieke identificatie met persoonlijke gegevens (BSN, paspoortnummer)	*	*	*	*
Geen validatie van de identificatiegegevens	*			
Validatie tegen een geloofwaardige databank.	*	*		
Validatie vereist een digitale handtekening onder de identificatiegegevens	*	*	x	

Validatie vereist een fysiek officieel identiteitsbewijs met handtekening en/of foto	*	*	*	*
Validatie vereist een gekwalificeerde digitale handtekening onder de identificatiegegevens.	*	*	*	*

1.5.7 Voorbeeld van het bepalen van het betrouwbaarheidsniveau van een authenticatiemechanisme

Aan de hand van bovenstaande paragraaf kunnen we het betrouwbaarheidsniveau bepalen van een authenticatiemechanisme.

Een zorgorganisatie geeft RSA-tokens uit om extern een VPN-verbinding op te kunnen zetten met de server. Deze moeten aan de balie aangevraagd worden na controle van de personeelspas en opgave van het bekende adres. Daarna worden deze per aangetekende post verstuurd naar het adres van de medewerker. Om de VPN-verbinding op te zetten moet een PIN-code en de code op de token ingevoerd worden.

Aan de hand van de tabellen in paragraaf 1.5.6 vinden we de volgende scores.
AM3: Recent uitgegeven OTP-tokens bieden bescherming tegen alle gangbare aanvallen.
RC3: Het betreft een OTP-token beschermd met een pincode.
IC3: De token wordt via de post verstuurd na een controle van het adres.
IE3: Bijvoorbeeld de AP houdt enig toezicht op de degelijkheid van het authenticatiemechanisme. Zoals uitgelegd in paragraaf 1.5.6 is dit een mogelijke interpretatie van de gestelde eis.
ID2: Door de personeelspas en het adres te controleren is unieke identificatie gelukt. Echter, de gegevens worden slechts tegen een geloofwaardige databank gecontroleerd, namelijk de eigen personeelsgegevens.

Dit betekent dat dit authenticatiemechanisme voldoet aan de eisen voor Stork QAA2 en het beste als eIDAS laag beoordeeld kan worden.

Met een kleine wijziging kan ook voldaan worden aan de eisen voor eIDAS substantieel.
ID3: Door ook een fysiek officieel identiteitsbewijs met handtekening of foto te controleren wordt voldaan aan de eisen van ID3.

Over het algemeen worden deze standaarden niet direct gebruikt, maar worden deze gebruikt om tot een afsprakenstelsel voor de authenticatie-eisen te komen, zoals bij het Afsprakenstelsel voor de Elektronische Toegangsdiensten[5], dat gebruikt wordt voor eHerkenning.

[5] https://afsprakenstelsel.etoegang.nl/display/as/Startpagina

2 Methodologie

2.1 Strategie

Sterke authenticatie in de zorg vereist dat zorgprofessional de middelen gebruiken zoals ze bedoeld zijn. Omgekeerd betekent dit dat het authenticatieproces aan moet sluiten van de praktijk.
Daarom heeft TNO allereerst een inventarisatie gemaakt van wat de huidige en beschikbare inlogmiddelen met de bijbehorende betrouwbaarheidsniveaus binnen de zorg zijn. Er is hierbij gekozen voor een kwalitatief onderzoek door middel van interviews. Met kwalitatief onderzoek kan er verdiepend op de ervaringen ingegaan worden. Er is gebruik gemaakt van semigestructureerde interviews waarbij vooraf een vragenlijst is opgesteld (bijlagen A en B). Semigestructureerde interviews bieden de mogelijkheid om door te vragen op interessante aspecten.
In de gesprekken met zorgverleners is onderzocht wat hun ervaringen met de huidige inlogmiddelen zijn; welke inlogmiddelen er worden gebruikt en wat zorgmedewerkers van de werkbaarheid van deze inlogmiddelen vinden.
In de gesprekken met IT-leveranciers voor de zorg is onderzocht wat de laatste ontwikkelingen op het gebied van authenticatie zijn en wat de visie van diverse leveranciers op authenticatie in de zorg is.

Vragen, ideeën en problemen die in deze gesprekken en in overleggen met de opdrachtgever opgekomen zijn, zijn in vervolggesprekken onderzocht. Op deze manier is het onderzoek door middel van voortschrijdend inzicht en nieuwe inzichten bijgestuurd.

De informatie verkregen tijdens de interviews is aangevuld met diverse teksten, websites en verdiepingsgesprekken met collega's (zie verwijzingen in de tekst).

2.1.1 Studiepopulatie

Om een goed beeld te krijgen van de bestaande middelen binnen de zorg was het streven om 10-20 verschillende types zorgverleners te interviewen. Op basis van het aantal geregistreerde abonnee-organisaties in het UZI-register, is een selectie van verschillende types zorgverleners gemaakt. Tevens is er rekening gehouden met de grootte van een organisatie. Er zijn zorgverleners van klein (collectief/zelfstandig), middel en grote organisaties gesproken om een representatief beeld binnen het type zorgaanbieder te krijgen. In het totaal zijn er 17 zorgverleners gesproken (bijlage C, tabel 1).
Op basis van de gesproken zorgverleners en meest genoemde softwareleveranciers, zijn er leveranciers benaderd. Tijdens gesprekken met leveranciers kwamen ook andere/nieuwe namen van leveranciers naar boven. Met deze gerefereerde leveranciers is ook gesproken, mits ze interessant waren voor het onderzoek.
In het totaal zijn er 10 leveranciers gesproken (bijlage C, tabel 1).

2.1.2 Interviews

Om aan de juiste gesprekspartners van zorgprofessionals en leveranciers te komen, is gebruik gemaakt van het professionele netwerk van de projectleden. Waar mogelijk is dit aangevuld met het privénetwerk en met contactgegevens die via anderen verkregen zijn. Daarnaast is er via LinkedIn een poster gepubliceerd over het onderzoek en de interviews.

Vervolgens zijn de contactpersonen (zowel zorgprofessionals als leveranciers) via LinkedIn, email en telefoon benaderd met verzoek tot deelname. Bij positieve response is er een videovergadering ingepland met twee TNO-projectmedewerkers en een zorgverlener of softwareleverancier. Alle interviews zijn door minimaal twee TNO-medewerkers afgenomen, waarbij altijd één zorgverlener tegelijkertijd werd gesproken. Dit om te voorkomen dat er sociaal wenselijke antwoorden werden gegeven. Bij interviews met leveranciers is dit minder van belang en werden één of twee respondenten van dezelfde leverancier tegelijkertijd gesproken. De interviews zijn dezelfde dag van afname uitgetypt en verwerkt, waarbij direct de belangrijkste conclusies uit het gesprek in een apart document werden opgeslagen. De interviews zijn geanalyseerd aan de hand van intersubjectiviteit van de zorgprofessionals. Uitgetypte gesprekverslagen zijn bewaard op SharePoint. In een periode van drie maanden zijn de interviews afgenomen. De gegevens uit de interviews zijn gebruikt om tot een groeimodel te komen voor sterkere authenticatie in de Nederlandse zorg. Op verzoek kunnen de geanonimiseerde interviews worden in gezien.

3 Gespreksresultaten

3.1 Studiepopulatie

In het totaal zijn 27 interviews afgenomen; 17 diverse type zorgverleners en 10 leveranciers. Een overzicht van de aantallen en type respondenten is weergegeven in bijlage C, tabel 1.
Er is ook uitvraag gedaan naar de kosten van UZI passen en andere inlogmiddelen, maar deze vraag kon niet worden beantwoord door zorgprofessionals en beperkt door ICT partijen.

3.2 Zorgverleners

De belangrijkste observaties van de gesprekken met de zorgverleners zijn verwerkt in de zogenoemde *Authenticatiematrix* in bijlage C, tabel 2.
Hierin worden per zorgverlener de volgende onderwerpen kort weergegeven.

- Welke diensten gebruikt de zorgverlener?
- Welke inlogmiddelen worden gebruikt per dienst?
- Wat is de geschatte betrouwbaarheid van het inlogmiddel?
- Worden er ook UZI-middelen gebruikt en, zo ja, waarvoor?

Hieronder staan de bevindingen van de gesprekken met de zorgverleners samengevat. Ze zijn opgedeeld in drie onderdelen, namelijk databeveiliging, authenticatie en UZI-pas.

Databeveiliging

- Zorgverleners hebben in het algemeen te weinig kennis; er is nauwelijks voorlichting en educatie rondom databeveiliging en veilig digitaal werken en authenticatie.
- Databeveiliging wordt in het algemeen als belangrijk ervaren, maar heeft geen prioriteit onder zorgverleners.
- Het beroepsgeheim wordt zeer serieus genomen, fysieke databeveiliging ook, maar digitale beveiliging veel minder.
- Op zorgorganisatieniveau is wel kennis in huis en betrokkenheid op het onderwerp.

Authenticatie

- Het betrouwbaarheidsniveau van de authenticatie bij de gebruikte diensten is over het algemeen laag tot substantieel.
  - Laag komt veelal bij EPD’s voor.
  - Incidenteel wordt door gebrek aan beter privémail, Whatsapp en WeTransfer gebruikt.
  - Wachtwoorden en passen worden gedeeld met collega's.
- Jonger zorgpersoneel staat positiever tegenover sterkere authenticatie.
- Er worden door één zorgverlener meerdere verschillende authenticatiediensten gebruikt.
- Ook brief, geprinte informatie en fax worden nog veel gebruikt.
- Zorgverleners hebben bij toekomstige authenticatie voorkeur voor middelen die

- niet snel te verliezen of vergeten zijn, zoals biometrie, een telefoon of sleutelbos;
- snelle authenticatie, zodat de interactie met de patiënt niet verstoord wordt;
- niet meerdere keren inloggen tijdens een consult met een patiënt.

UZI-pas

- UZI-passen worden als duur ervaren met een hoge functionele drempel. Daardoor worden UZI-passen regelmatig door meerdere mensen samen gebruikt.

3.2.1 Huidige authenticatiemethodes

In deze paragraaf benoemen wij enkele middelen en methodes die naar voren kwamen in de gesprekken met de zorgverleners en leveranciers en vermelden daarbij het betrouwbaarheidsniveau. Dit betrouwbaarheidsniveau is enkel gebaseerd op de gebruikte authenticatiemiddelen en beschouwt niet de identificatie en verstrekkingsprocedure, zoals beschreven in hoofdstuk 1. De meest genoemde middelen worden eerst besproken.

De meest gangbare methode voor authenticatie is een gebruikersnaam en wachtwoord. Daarbij wordt vaak voor een optie gekozen om het wachtwoord te verversen na een aantal maanden. Deze 1-factor authenticatie heeft een laag betrouwbaarheidsniveau volgens de eIDAS-norm.
Verder is het onder zorgverleners ook gangbaar om een 2-factor authenticatie te hanteren, te denken aan een wachtwoord in combinatie met een fysiek bezit, zoals een token of een app die telkens een eenmalige pincode genereert. Het betrouwbaarheidsniveau hiervan is substantieel/laag (afhankelijk van de. registratie, uitgifte en beheerproces)).

Zoals uitgelegd in Hoofdstuk 1 gelden er strenge eisen om aan authenticatie op een hoog betrouwbaarheidsniveau te voldoen. Deze eisen worden vaak niet gehaald. Daarnaast worden er nog regelmatig communicatiemiddelen gebruikt zonder dat er authenticatie op het juiste/vereiste authenticatieniveau is, om praktische redenen. Bijvoorbeeld, (grote) bestanden die snel bij een andere zorgverlener moeten aankomen worden via onbeschermde/ ongeautoriseerde applicaties voor bericht- of bestandsverkeer verstuurd, zoals WhatsApp of WeTransfer. Dit soort diensten maken soms gebruik van encryptie voor de inhoud van de berichten/bestanden, maar de meta-data wordt niet beschermd en er is geen controle op de identiteiten van de partijen die de informatie uitwisselen.

Tevens worden er regelmatig biometrische middelen gebruikt zoals vingerafdruk en gezichtsherkenning via de telefoon. In combinatie met andere factoren, zoals een app op de eigen telefoon, is dat soms te classificeren als substantieel (afhankelijk van de registratie, uitgifte en beheerproces middel).

Verder, wordt onder zorgaanbieders af en toe de IRMA-app als nieuw authenticatiemiddel toegepast of onderzocht. Vaak is dit nog in een pilotfase.

Daarnaast zijn de UZI-middelen bij de meeste zorgverleners wel bekend. Echter, de meeste zorgverleners gebruiken ze niet. Het gebruik zit vooral geconcentreerd bij enkele beroepsgroepen zoals apothekers en huisartsen. UZI-passen worden als duur ervaren met een hoge functionele drempel. Daardoor worden UZI-passen regelmatig

door meerdere mensen samen gebruikt. Het middel kent een hoog betrouwbaarheidsniveau, maar wordt regelmatig onzorgvuldig toegepast in de praktijk. Hierdoor is de zekerheid dat de naam op het pasje overeenkomt met de gebruiker veel kleiner dan beoogd. Voorbeelden van zulk onjuist gebruik zijn het gebruik van de pas door meerdere zorgverleners en het achterlaten van de pas in de paslezer, zodat iedereen toegang kan krijgen tot de systemen. De meeste zorgverleners die de pas gebruiken, geven aan dit voornamelijk te gebruiken voor het opvragen van NAW-gegevens. Daarnaast wordt het gebruik voor toegang tot het LSP en VECOZO ook regelmatig genoemd.

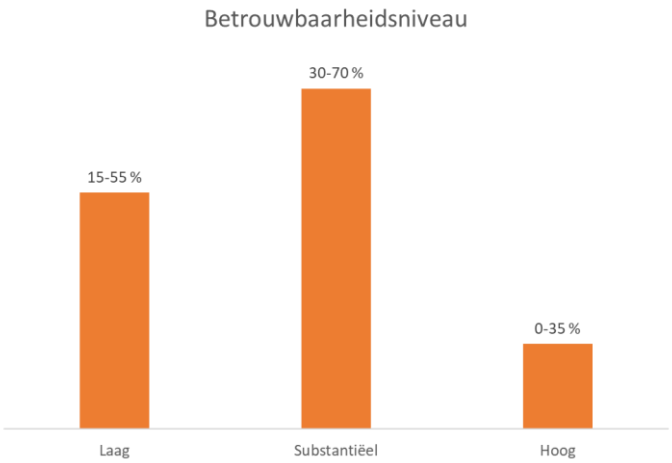
3.2.2 Overzicht van de huidige betrouwbaarheidsniveaus

In de gesprekken hebben de zorgverleners 77 IT-diensten in de zorg beschreven die authenticatie vereisen. Enkele veelgebruikte diensten komen hierin wel meermaals voor. Op basis van de gegeven beschrijving, heeft TNO een inschatting gemaakt van het corresponderende eIDAS-niveau (laag/substantieel/hoog) van de huidig gebruikte middelen. Negen diensten werken met een middel op betrouwbaarheidsniveau hoog, 36 diensten zijn er gevonden die werken met 2-factor authenticatie, afhankelijk van het uitgifteproces, is het betrouwbaarheidsniveau hier laag of substantieel en 25 diensten werken met betrouwbaarheidsniveau laag. Zie voor meer informatie Tabel 10. Meer dan een inschatting is op dit moment niet mogelijk, omdat een vastgesteld toetsingskader voor de middelen nog ontbreekt. Aan de hand hiervan is een schetsend overzicht gemaakt van de betrouwbaarheidsniveaus van authenticatie in de Nederlandse zorg.

De gesprekken met de zorgverleners hebben veel waardevolle inzichten opgeleverd voor de toekomstige authenticatie. Een nadeel van deze methode is dat het relatief arbeidsintensief is, waardoor minder verschillende IT-diensten behandeld kunnen worden. Hierdoor bevatten de in Tabel 11 genoemde percentages aanzienlijke foutmarges.

Tabel 10 Aantal getelde diensten per betrouwbaarheidsniveau.

Betrouwbaarheidsniveau:	N
eIDAS hoog	9
eIDAS substantieel/laag (2-factor authenticatie)	36
eIDAS laag	25
Betrouwbaarheid lager dan eIDAS laag	3
Overige:	
UZI-servercertificaten	4



Figuur 3 Inschatting van het betrouwbaarheidsniveau in het hele zorgveld.

Authenticatie door middel van een wachtwoord + sms-code wordt nog veel gebruikt. Dit is minder veilig[6] dan andere twee-factorauthenticatie en is daarom in de authenticatiematrix op laag/substantieel opgenomen. Voor dit overzicht is deze als substantieel gewaardeerd.
Voor sommige diensten is eIDAS substantieel voldoende, zie NTA 7516, zoals ad-hoc berichtverkeer (chat/mail/etc..) dat niet onder de medische-geheimhoudingsplicht valt.
Omdat TNO geen inzicht heeft in de gebruiksfrequenties per dienst, kan dit overzicht alleen voor aantallen diensten opgesteld worden.

3.3 Leveranciers van zorg-IT

De resultaten met de gesprekken met leveranciers van zorg-IT (bedrijven die pakketten leveren voor registratie van zorg en authenticatie middelen) zijn weergegeven in bijlage C, tabel 3. Hierbij worden per leverancier de volgende vragen beantwoord.

- In welk zorgveld is de leverancier actief?
- Wat voor type dienst wordt geleverd?
- Met welke inlogmiddelen verkrijgt men hier toegang tot?

[6] Zie bijvoorbeeld https://www.infosecurity-magazine.com/news/reddit-breached-after-sms-2fa-fail/.

- Hoe wordt de betrouwbaarheid van dit middel ingeschat? Hierbij is dezelfde benadering gebruikt als bij de zorgverleners, omdat de identificatie- en uitreikingsprocedures door de zorgorganisaties en niet door de IT-leveranciers georganiseerd worden.
- Waar ligt de prioriteit bij de producten en diensten van de IT-leverancier.
- Welke koppelingen met andere diensten zijn besproken?

De onderzoeksbevindingen en de visie rondom sterkere authenticatie uit deze gesprekken worden hieronder samengevat. Ze zijn opgedeeld in vier onderdelen, namelijk landschap, naar eIDAS hoog, kosten en overige bevindingen.

Houding leveranciers

- Leveranciers wachten de ontwikkelingen en vragen van de klant af. Ze zullen niet het initiatief nemen voor sterkere authenticatie om klanten niet af te schrikken. Bij een overgang naar sterkere authenticatie op eigen initiatief zijn leveranciers bang dat dit de werkbaarheid voor klanten verandert en klanten over zullen stappen naar een andere leverancier.
- De klant is de koning en er wordt daarom niets afgedwongen, maar geluisterd naar de behoeftes van de zorgorganisaties.
- Sommige leveranciers beschouwen op dit moment de zorgsector niet als interessante markt, o.a. vanwege de omvangrijke wetgeving, de complexiteit van het zorgdomein en de verplichting om het BSN te verwerken.
- De leveranciers zouden graag meedenken over de toekomstige ontwikkelingen.

Naar eIDAS hoog

- Er zijn passende authenticatieoplossingen op betrouwbaarheidsniveau hoog beschikbaar. De zogenoemde cloudoplossing lijkt een interessante, praktische en werkbare optie. Deze zal hieronder verder beschreven worden.
- Naast cloudoplossingen zijn er ook alternatieven beschikbaar, te denken valt aan yubikeys (een hardwarematige twee-factor authenticatie sleutel, in de vorm van een USB-stick, voor eenvoudige en veilige toegang tot applicaties, netwerken en online services) of smartcards.
- Voor authenticatie op betrouwbaarheidsniveau hoog is het van belang dat iedere zorgverlener een gemakkelijk, persoonlijk middel heeft. Dit vereist een volledig en beschikbaar UZI-register. Iedere zorgverlener die een rol heeft in de zorgverlening en persoonlijk data inziet moet hierin opgenomen zijn.
- Technisch verwachten de leveranciers geen problemen bij het implementeren van sterkere authenticatie.

Kosten

- Leveranciers, en ook zorgverleners hebben en geven geen inzicht in de kosten van sterkere authenticatie.
- Van de cloudoplossingen zijn prijzen beschikbaar, die als startpunt van een kostenberekening kunnen dienen.
- CIBG over de huidige UZI-kosten: Hoe groter de schaal hoe lager de vaste kosten per gebruiker. De vaste kosten bedragen 40% van de huidige prijs. Hiermee is alleen een zeer grove kostenschatting mogelijk.
- Kosten zijn te onderscheiden in kosten voor software, hardware en ondersteunende diensten (zoals persoonlijke verschijning) voor aansluiting op het bredere zorginformatiesysteem (binnen en buiten de organisatie).

Overige bevindingen

- Authenticatiestandaard
  De meeste standaarden schrijven nog een fysieke verschijning tijdens de registratie voor om aan de eisen voor het hoogste betrouwbaarheidsniveau te voldoen. Echter, eIDAS [910/2014 Art. 24)] schrijft dit niet voor. Er wordt gewerkt aan technische invullingen om deze identificatie op afstand mogelijk te maken [ETSI TR 119 460 / ETSI TR 119 461].

3.4 eIDAS hoog met behulp van de cloudoplossing

3.4.1 Overzicht van de oplossing

Een veelbelovende oplossing is het gebruik van een certificaat dat in een beveiligde omgeving- zoals een Hardware Security Module (HSM)- in de cloud is opgeslagen en voor gebruik wordt ondertekend. Deze oplossing is geclassificeerd als eIDAS hoog. Daarnaast is het certificaat te gebruiken vanaf onder andere een smartphone. Dit maakt deze oplossing zeer gebruiksvriendelijk.

Om toegang te krijgen tot deze cloudomgeving is authenticatie op niveau eIDAS substantieel of hoger vereist [EU 910/2014 Art.24]. Door het gebruik van het ondertekende certificaat kan de gebruiker zich hierna authentiseren op niveau eIDAS hoog. In de cloud vindt dus een verhoging van het betrouwbaarheidsniveau plaats[7]. Deze cloud oplossing zou een van de oplossingen kunnen worden binnen het stelsel. Essentieel daarbij is dat deze oplossing zich in het netwerk op de zelfde manier presenteert als fysieke middelen.

3.4.2 Gebruiksgemak voor de zorgverleners

Sommige zorgverleners moeten veel verschillende authenticatiemiddelen beheren voor hun werk. Het beheren van veel verschillende wachtwoorden, pincodes, pasjes en apps beperkt het gebruiksgemak aanzienlijk. Daarnaast leidt het tot hergebruik van pincodes en wachtwoorden, wat een veiligheidsrisico met zich meebrengt.

Toegang tot bovengenoemde cloudomgeving kan ook met behulp van een RSA-token, een smartcard of iets soortgelijks. Deze oplossing kan gecombineerd gebruikt worden met authenticatiecertificaten op smartcards of usb-sleutels en geeft de zorgverlener de kans om te kiezen wat voor hem/haar werkt.

3.4.3 Leveranciersmarkt

In het onderzoek zijn ten minste drie partijen (KPN, Digidentity, Cleverbase) geïdentificeerd die een dienst voor authenticatiemiddelen op niveau eIDAS hoog kunnen leveren. Met twee van deze partijen zijn gesprekken gevoerd, waarin zij aangaven de huidige schaalgrote van de zorg te kunnen bedienen. In een grote pilot zullen deze beloftes moeten worden getoetst.. Door het gebruik van zulke authenticatieoplossingen in de zorg kan de markt hiervoor ook groeien, waardoor het aantal leveranciers toe zou kunnen nemen.

[7] Zie ook S1 van “Eric Verheul, SECDSA: Mobile signing and authentication under classical “sole control”, 2021”, (https://eprint.iacr.org/2021/910)

4 Roadmap van een nieuw authenticatiestelsel

4.1 Inleiding

De roadmap naar een authenticatiestelsel is een ontwikkelplan met de volgende uitgangspunten: gebruiksvriendelijkheid, betrouwbaarheid, keuzevrijheid en betaalbaarheid. Het authenticatiestelsel is cruciaal voor de stip op de horizon: in 2028 gebruikt iedere zorgverlener een persoonlijk inlogmiddel dat voldoet aan betrouwbaarheidsniveau eIDAS Hoog voor (in ieder geval) uitwisseling tussen zorgaanbieders onderling.

In dit hoofdstuk worden de belangrijke thema's binnen de roadmap toegelicht. Deze thema's geven richting aan de roadmap. De roadmap bestaat uit verschillende fases die invulling geven aan deze thema's. Verder zijn er rollen gedefinieerd voor de transitie naar het nieuwe authenticatiestelsel en in het uiteindelijke authenticatiestelsel, die partijen verantwoordelijkheid geven om deze thema's te borgen en gestoeld zijn op de rollen in het huidige stelsel (zie bijlage D).

4.2 Thema's

In de roadmap staan een aantal thema's centraal voor een succesvolle transitie:
- Draagvlak creëren,
- Harmonisatie en standaardisatie,
- Een directe stap naar eIDAS hoog
- Het direct starten met pilots die voorbereiden op een grootschalige transitie.

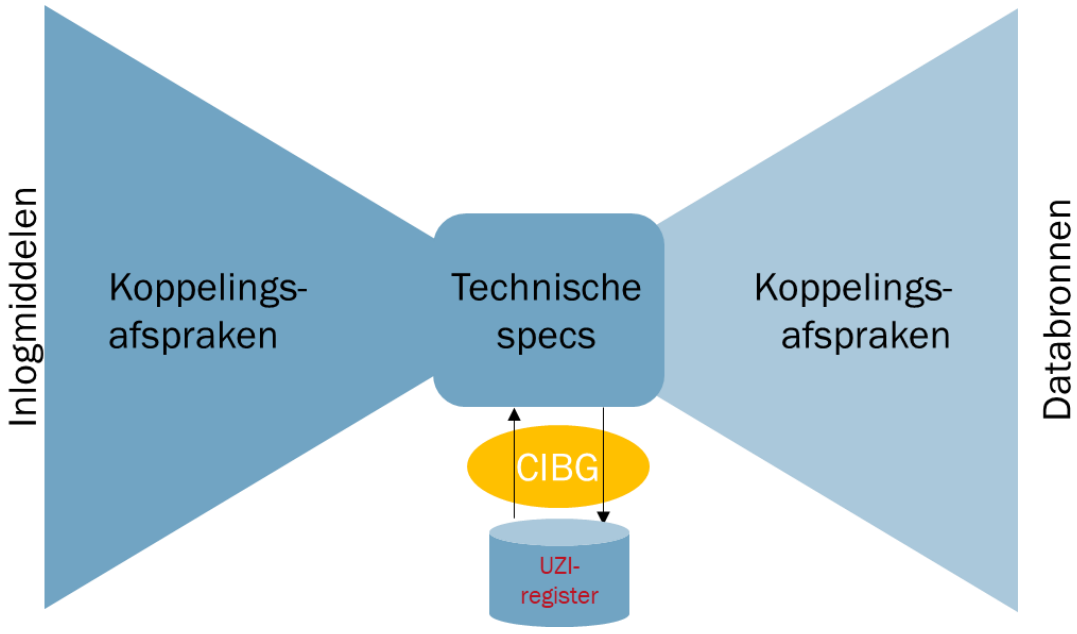
Deze thema's komen voort uit de deskresearch en interviews. Hieronder worden deze thema's toegelicht.

Draagvlak creëren
Onder zorgaanbieders en -professionals wordt de urgentie van een sterke identificatie en authenticatie in hun dagelijkse werkzaamheden onvoldoende ervaren om op een verantwoorde manier gegevens uit te wisselen die voldoen aan de norm eIDAS hoog. Echter, om een systeemtransitie te ondergaan is het essentieel dat de urgentie gevoeld wordt. Als het nut en belang van sterkere authenticatie niet onderkend worden, zal het veilig toepassen van een nieuw authenticatiemiddel met daarbij horende toepassingsregels tot frustratie en onbegrip leiden. Dit zou de implementatie kunnen ondermijnen. Immers, met enkel een betrouwbaar authenticatiemiddel is veilige gegevensuitwisseling niet haalbaar. Gedrag is hierin net zo belangrijk al dan niet belangrijker. TNO adviseert daarom om het belang van veilig digitaal werken onder de aandacht te brengen bij onder meer de eindgebruikers, zowel de privacy-verantwoordelijke alsook de bestuurders bij zorgaanbieders, leveranciers, brancheverenigingen en koepelorganisaties. Verder adviseren wij de rol van sterke authenticatie in veilig werken te benadrukken. Dit besef is belangrijk om de ondersteuning en succesvolle implementatie van sterkere authenticatiemethoden mogelijk te maken.

Harmonisatie door standaardisatie

Een belangrijke belemmering voor het gebruiksgemak van authenticatiemiddelen in de praktijk is de grote diversiteit aan authenticatiemiddelen dat dagelijks nodig is. Zorgverleners kunnen actief zijn in meerdere zorginstellingen en hebben daarnaast ook nog een grote variëteit aan communicatiekanalen te overzien. Hierbij kan gedacht worden aan zorg specifieke mail- en chatapplicaties, declaratieportalen, data-uitwisseling met andere instellingen, et cetera. Deze hebben allemaal eigen authenticatiemiddelen, wat tot veel rompslomp en frustratie leidt. Enige mate van diversiteit aan authenticatiemiddelen is echter noodzakelijk, omdat verschillende situaties andere eisen stellen aan een goedwerkend authenticatiemiddel, daardoor is het gaan naar een situatie van single sign-on (SSO) nog een stap te ver en ook niet zal worden geaccepteerd uit veiligheidsoverwegingen. Om met deze diversiteit om te kunnen gaan, is een stelsel vereist dat overweg kan met alle toegestane authenticatiemiddelen en deze op een gestandaardiseerde manier kan afhandelen. Dit is een structuur die enigszins vergelijkbaar is met die van routeringsdiensten, die onder andere voor patiëntauthenticatie in de zorg al gebruikt worden.

Het voordeel hiervan is dat zorgverleners geen grote verzamelingen authenticatiemiddelen nodig hebben, maar kunnen kiezen uit enkele erkende en toegelaten middelen die voldoen aan het minimum vereiste niveau. Kortom, wordt er met harmonisatie en standaardisatie zowel keuzevrijheid, betrouwbaarheid alsook gebruiksvriendelijkheid geborgd.



Figuur 4 Visualisatie van de werking van het afsprakenstelsel voor het verbinden van inlogmiddelen en databronnen. Door het ontwikkelen van een afsprakenstelsel waarin technische specificaties en manieren van interacteren worden vastgelegd, kan elke geaccepteerd inlogmiddel gebruikt worden om geauthentiseerd te worden voor toegang tot alle relevante databronnen.

Direct naar eIDAS hoog, zonder de tussenstap substantieel

Tijdens de interviews met enkele authenticatieleveranciers (zie bijlage C. Studiepopulatie) kwam naar voren dat een directe stap naar een authenticatielandschap waarin een eIDAS hoog norm gehanteerd wordt, mogelijk is en een tussenstap naar eIDAS substantieel niet nodig. Belangrijk hierbij is te benadrukken dat deze aanname getoetst zal moeten worden in (een) grote pilot(s), zie aanbevelingen). Allereerst zijn authenticatiemiddelen die voldoen aan eIDAS hoog al op kortere termijn te implementeren, met behulp van onder andere een mobiele telefoon. Een mobiele telefoon wordt al op grote schaal gebruikt en wordt als gebruiksvriendelijk ervaren. Er moet wel rekening gehouden worden met het feit dat de telefoon niet altijd geschikt is als enige hulpmiddel. Enerzijds zullen niet alle zorgprofessionals beschikken over een mobiele (werk)telefoon, anderzijds zullen de werkomstandigheden het gebruik ervan niet altijd toelaten, te denken aan een steriele OK omgeving of de magnetische straling tijdens een MRI scan. Hiervoor is het nodig om andere eIDAS hoog authenticatiemiddelen aan te bieden, zoals de al bestaande tokens of passen.

Het grote nadeel van een tussenstap naar eIDAS substantieel is dat er twee keer een transitie nodig is, wat tot weerstand kan leiden. Kortom, TNO adviseert om een tussenstap naar eIDAS substantieel over te slaan om de volgende twee redenen:

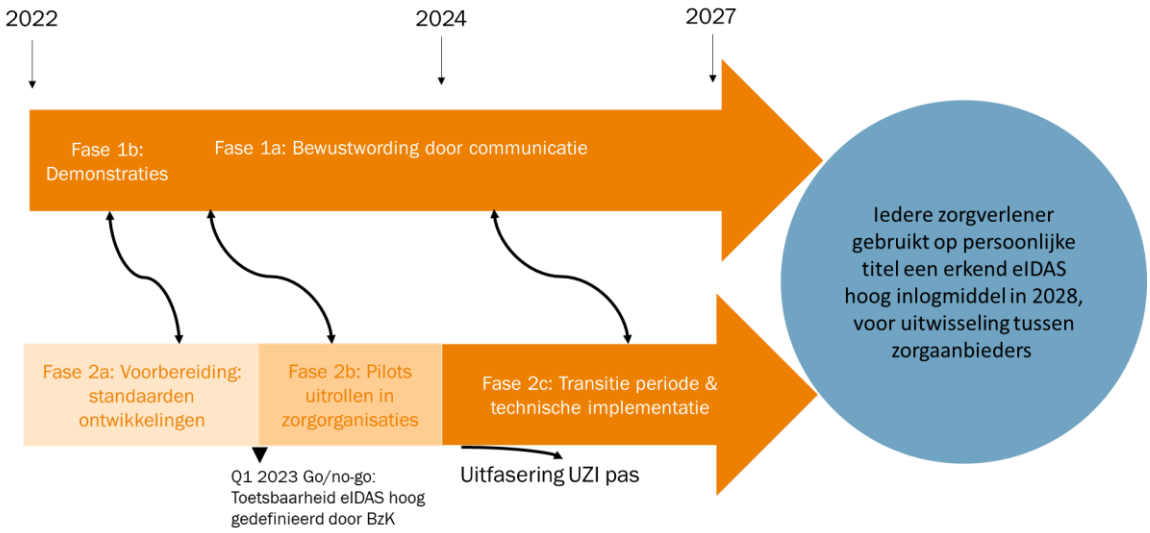
1) Er zijn al technische oplossingen voorhanden die het mogelijk maken op grote schaal authenticatiemiddelen met een eIDAS hoog betrouwbaarheidsniveau te bieden. Dit kan, bijvoorbeeld, met een authenticatiesleutel of door authenticatie met een certificaat opgeslagen op een veilige cloudomgeving, die voor niemand anders toegankelijk is of met een token of een pas. Enkele authenticatieleveranciers geven aan een dergelijk middel voor alle zorgprofessionals te kunnen en willen leveren. Uiteraard is het van belang dit nog verder te valideren in pilots (zie de fases in de volgende paragraaf) en in uitzonderlijke situaties een uitzondering toe te staan (waar dan additionele maatregelen wordt genomen, maar de focus zou moeten zijn op een volledige transitie).
2) Een extra transitiefase van eIDAS laag naar substantieel vraagt om veel extra werk en begrip, wat de vervolgstap naar eIDAS hoog in de weg kan zitten. Daarnaast kan een stap naar substantieel nog gemakkelijk gemaakt worden na de invoering van een hoog niveau, andersom is dit niet aannemelijk.

Direct starten met pilots

Om tot een stelsel te komen waarbij voor de zorgaanbieder keuze ontstaat in het te gebruiken authenticatiemiddel met een hoog betrouwbaarheidsniveau, zullen er grootschalige pilots moeten worden uitgevoerd om te bepalen of de ambities, zoals geformuleerd in de roadmap, ook haalbaar zijn. Dit omvat zowel de pilots om de technische werking te toetsen en te controleren alsook proeven om te bepalen of de transitie naar een nieuw systeem organisatorisch haalbaar is. Werken de plannen van de roadmap niet zoals beoogd, dan zullen de consequenties groot zijn. Situaties kunnen zich voordoen waarbij zorgprofessionals niet kunnen inloggen en daardoor niet bij benodigde informatie kunnen om de juiste zorg op de juiste plek te bieden. Kortom, met de schaalgrootte, de bijkomende risico’s, daarnaast de tijdslijn van de transitie in aanmerking nemende adviseert TNO direct te beginnen met grote pilots; pilots die groot genoeg zijn om te toetsen dat leveranciers de schaalgrootte kunnen leveren die ze aangeven.

4.3 Fases

Een grafische weergave van de verschillende fases die TNO voor zich ziet in de roadmap is te zien in Figuur 5. Deze fases geven invulling aan de thema's zoals hierboven beschreven. Na Fase 2a: 'Voorbereiding: standaarden ontwikkelen' vindt een go/no-go moment plaats, waarin bepaald wordt door de stelselhouder (op advies) of de standaarden een voldoende basis bieden om door te gaan naar de pilot fase. Het is van belang dat er toetsingscriteria komen voor deze pilots, gerelateerd aan de ambitie alle inlogmiddelen op betrouwbaarheidsniveau eIDAS hoog te krijgen. BzK heeft de juiste positie om hier invulling aan te geven.



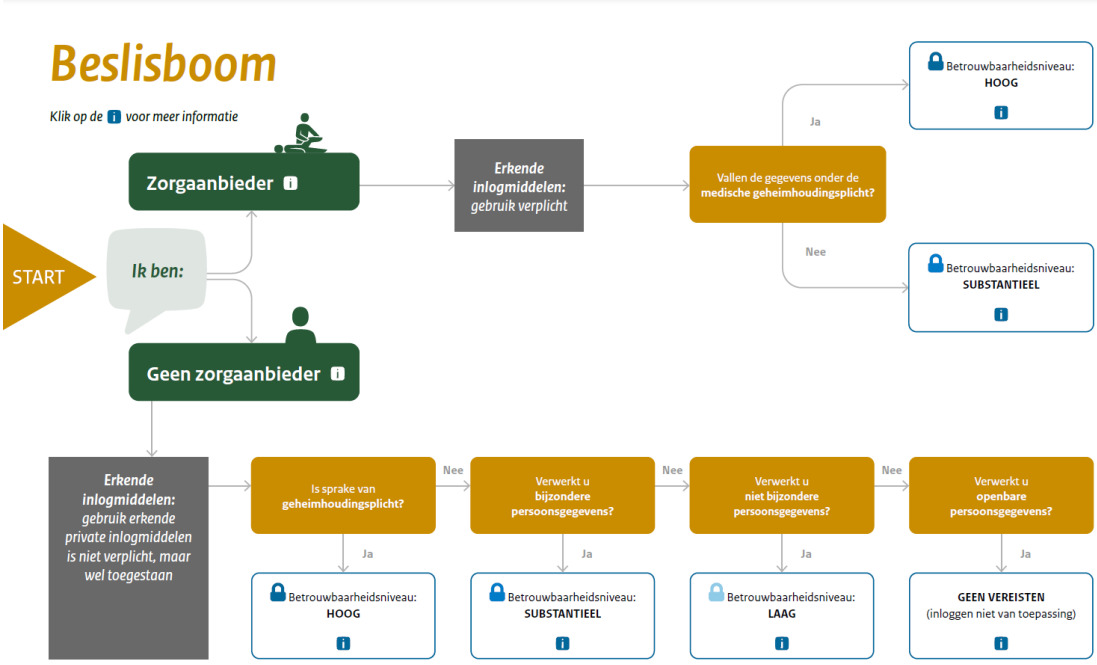
Figuur 5. Fasering van roadmap naar authenticatiestelsel voor de zorg.

Fase 1
Deze fase geeft invulling aan het thema 'Draagvlak creëren' voor het nieuwe authenticatiestelsel. De methodes die hierbij helpen zijn gerichte communicatie, het creëren van bewustwording van het belang van authenticatie, luisteren naar de behoeften en het aantonen hoe het in de praktijk in werkt.

Fase 1a: Bewustwording door communicatie over veilig digitaal werken

Communiceren op maat en vroegtijdig
Communicatie moet gaan leiden tot gedragsverandering. Als de spelers in het nieuwe stelsel goed wordt meegenomen kan frustratie over bureaucratie voorkomen worden. Het is hierbij belangrijk om de verschillende stakeholders op een goede manier te informeren, omdat de manier van werken sterk verschilt per stakeholder. Een algemeen communicatieplan zal hiervoor niet voldoende zijn. Maatwerk in de communicatie is belangrijk, want verschillende stakeholders verkrijgen hun informatie op een andere manier. Voor digitale toegang in de zorg is, bijvoorbeeld, de beslisboom uit figuur 6 ontwikkeld. Soortgelijke communicatie voor andere stakeholders zal nodig zijn voor een goede implementatie van een nieuwe authenticatiestelsel.

Daarnaast is het belangrijk om veilig werken terug te laten komen in het curriculum van de zorgprofessional. Zonder communicatie en bewustwording zal de huidige situatie rondom veilig werken opnieuw optreden.



Figuur 6 Digitale toegang in de zorg. Beslisboom betrouwbaarheidsniveaus en erkende inlogmiddelen. De bovenstaande beslisboom informeert zorgaanbieders over de vereisten voor veilige digitale toegang voor patiënten in de zorg. Bron: Beslisboom betrouwbaarheidsniveaus en erkende inlogmiddelen | Publicatie | Gegevensuitwisseling in de zorg.

Een continue dialoog

Daarnaast zijn er diverse situaties en omstandigheden, waar sterkere authenticatie lastiger is. Hierbij kan gedacht worden aan spoedsituaties, extra hygiënische eisen, maar ook aan de werkbaarheid. Het is daarom verstandig om hierover in gesprek te gaan met de eindgebruikers (zorgaanbieders en -professionals) en de potentiële risico's goed in kaart te brengen.

Betrokkenheid ICT leveranciers

Het advies is om de ICT leveranciers mee te nemen in deze bewustwordingsfase (fase 1a). Op technisch gebied kunnen de ICT-leveranciers helpen om de afnemers van inlogmiddelen de transitie naar eIDAS hoog te laten maken. Leveranciers zijn in staat de klant goed te ondersteunen door middel van communicatie en kennisoverdracht. Daarnaast kunnen zij met behulp van techniek bepaald gedrag stimuleren, te denken aan pop-ups met uitleg over welk gedrag tot veilig werken leidt of instellingsmogelijkheden die de gebruiker bepaald gedrag afdwingen. Dit betekent dat er voortdurende communicatie en controle nodig is om er zeker van te zijn dat iedereen deze stap zet. Echter, de huidige leveranciers komen niet in beweging als de vraag niet verandert ("De klant is koning"). De vraag onder afnemers van inlogmiddelen moet daarvoor veranderen, waarmee dan ook de business case helder

wordt voor de leverancier. Hiervoor is het gevoel van urgentie nodig, wat wederom de noodzaak van communicatie benadrukt. Mogelijk is hier ook regulering nodig, om leveranciers hiertoe te dwingen.

Fase 1b: Demonstraties van verschillende middelen
Het is belangrijk om aan de hand van demonstraties te testen of nieuwe authenticatiemiddelen bij zorgaanbieders en -professionals geadopteerd zullen worden, om:

1) Specificaties op te halen; waar moet het middel aan voldoen?
2) De gebruiksvriendelijkheid te toetsen
3) Specificaties op te halen; waar moet het middel aan voldoen?
4) De adoptie van middelen te testen bij alle stakeholders

Tevens kunnen de kostenprognoses van de leveranciers getest worden. Tegelijkertijd wordt de mogelijk impact voor zorgorganisaties en zelfstandige werkende professionals in de zorg duidelijk; immers met één inlogmiddel kunnen meerdere bronnen en systemen worden benaderd (synergie/substitutie). Hiermee kan in potentie het totaal aantal middelen in een organisatie worden gereduceerd waarmee ook kosten kunnen worden bespaard.

Zonder demonstratie van het concept is het risico aanwezig dat de pilot op gebruiksvriendelijkheid wordt afgewezen. Zonder demonstratie/acceptatie zal er geen transitie plaatsvinden.

Fase 2
Deze fase geeft invulling aan de thema's 'Harmonisatie en standaardisatie', 'Het direct starten met pilots die voorbereiden op een grootschalige transitie' en 'Een directe stap naar eIDAS hoog'. Het advies is om de focus te leggen op het ontwikkelen van een set van standaarden, de standaarden te toetsen aan criteria voor toekomstbestendigheid en het te borgen dat het resulteert in een flexibel stelsel. Verder wordt aangegeven hoe de pilots vorm te geven.

Fase 2a: Voorbereiding: standaarden ontwikkelen
Dienst centraal
Enige vorm van harmonisatie is al zichtbaar bij de UZI-pas, die voor diverse doeleinden gebruikt kan worden. Hierbij staat het middel centraal. In dit voorstel staat een op te zetten of te definiëren dienst (het faciliteren van sterke authenticatie) centraal, die op basis van erkende authenticatiemiddelen met een hoog betrouwbaarheidsniveau, toegang regelt.

Toekomstbestendige standaard(en)
Het is belangrijk bestaande authenticatiestandaarden te actualiseren en toekomstbestendig te maken. TNO adviseert dat de toekomstbestendige standaarden aan de volgende eisen voldoen: de standaarden moeten doelmatig zijn en een toegevoegde waarde hebben, technisch en functioneel interoperabiliteit stimuleren, realiseerbaar, duurzaam en open[8] zijn, en draagvlak hebben. Het afsprakenstelsel waar de standaarden onderdeel van uit maken, zal centraal moeten worden beheerd.

Een flexibel stelsel

[8] Open Standaarden Open Standaarden - Digitale Overheid

Om nieuwe authenticatiemiddelen toe te kunnen laten in het stelsel is het van belang het UZI-register los te koppelen van de UZI-pas en het register compleet te maken. Iedereen die het zorg proces begeleidt, met extra aandacht voor personen die toegang hebben tot persoonlijke (medische) data, dient in het register te staan. Bijvoorbeeld, assistentes dienen vaak nog toegevoegd te worden aan het register. Tot slot kunnen zorgaanbieders ook zorg specifieke middelen, zoals ziekenhuispassen, als authenticatiemiddelen aanbieden en beheren. De erkenning van zorg specifieke middelen binnen het stelsel en de acceptatie door de zorgprofessionals vereisen wederom wel communicatie en controle rondom het authenticatieproces. Een dergelijk flexibel stelsel vraagt de nodige planning en overleg met in ieder geval de zorgaanbieders, ICT-leveranciers, auditoren en inspectie.

Fase 2b: Pilots uitrollen in zorgorganisaties
Aan de hand van pilotstudies met verschillende leveranciers en instellingen kan het aantal leveranciers met geschikte authenticatiemiddelen worden bepaald. Het is belangrijk om te toetsen of het ontworpen systeem doeltreffend is. De pilot studies moet zo ingericht worden dat deze onderwerpen goed getoetst kunnen worden en moeten de eisen van het systeem heel concreet worden gemaakt. Tevens wordt getoetst binnen de pilot of het authenticatiemiddel binnen de tijdslijnen van de roadmap geleverd kan worden, wordt getoetst of voor het merendeel van de beoogde gebruikers de gebruiksvriendelijkheid/acceptatie voldoet, en of het zowel organisatorisch als technisch haalbaar is.

Essentieel voor een geslaagde pilot is niet alleen dat er naar technische implementatie wordt gekeken, maar ook naar de systeemtransitie. TNO adviseert daarom ook naar de samenwerking met alle betrokken partijen te kijken gedurende de pilot en vast te stellen of het nieuwe systeem geen risico’s oplevert. Door pre-concurrentiële samenwerking kunnen zowel marktpartijen als zorgpartijen worden geactiveerd om nieuwe diensten en producten te ontwikkelen die in de volle breedte van de zorg kunnen worden getest. Pre-concurrentiële samenwerking door middel van een Small Business Innovation Research (SBIR) creëert meerdere simultane partijen, platforms en middelen die in de praktijk getest kunnen worden. Partijen worden betaald voor hun inzet (fixed fee). Pre-concurrentiële samenwerking zou ook op basis van een subsidie kunnen, het idee is met name om *unusual suspects* een duwtje te geven. Tevens kan er worden gestuurd op aantal marktpartijen en zorgpartijen, daarnaast kunnen vaste bedragen worden uitgekeerd. De verplichtingen kunnen worden afgestemd op de wensen en behoeften, te denken aan het rapporteren over inzicht in techniek, prijs, schaalbaarheid, synergie-effecten, inrichting ondersteuning. Hiervoor is het van belang dat het business model van het uiteindelijke systeem voor alle partijen helder is.

Na afloop van de pilot studies is:
1) Bevestiging (of niet) dat marktpartijen de middelen/diensten kunnen leveren op de schaal zoals nu verondersteld. Mocht dit niet bevestigd worden dan leidt dit tot een no-go situatie waarvoor een alternatief plan klaar moet liggen (zie verder).
2) De bruikbaarheid/toepasbaarheid van middelen getest in verschillende groepen zorgverleners die de breedte van de zorg representeren, zoals verzorgenden, verpleegkundigen, begeleiders en praktijkondersteuners huisartsenzorg uit de directe zorgverlening.

3) Bekend of er opschalingsrisico's zijn en wat de ondersteuningsbehoeften van gebruikers zijn.
4) Inzicht in (in)compleetheid van het UZI-register.
5) Verkend welke kostenconsequenties zich voordoen voor zorgprofessionals en zorgorganisaties en welke potentiële businessmodellen kunnen worden gehanteerd door aanbieders van oplossingen

N.B. voorwaarde voor succesvolle pilots is de loskoppeling van het UZI-register zodat het bruikbaar is om andere authenticatiemiddelen te voorzien van een zorgidentiteit.

Gedurende de pilot adviseert TNO om een adviesraad te installeren van alle stakeholders die een uiteindelijke rol hebben in het stelsel. We adviseren om de UZI-klankbordgroep hiervoor in te zetten en door te ontwikkelen naar een adviesraad. Daarnaast adviseren wij om de adviesraad in te zetten als autorisator / beslisser (zie hoofdstuk 4.4).

Fase 2c: Transitie periode en technische implementatie
De pilots dienen te voldoen aan criteria die voorafgaande aan de pilots zijn afgestemd met alle betrokkenen. Met name de schaal benodigd voor deze systeemtransitie behoeft een grote pilot. Deze schaal gaat over het aantal alternatieve authenticatiemiddelen en of die genoeg zorgverleners hun dienst kunnen leveren. Daarnaast zullen de pilots ook inzicht moeten geven in de kosten van de transitie en de kosten na transitie. Indien na de pilots duidelijk wordt dat er aan de criteria voldaan kan worden, zullen de volgende onderwerpen geadresseerd moeten worden:

1) <u>(verdere) Bekostiging van de transitie en business case:</u> Er is bekostiging nodig voor de transitie naar een nieuw stelsel. Uit de pilot moet blijken hoe hoog de kosten zijn en hoe groot de compensatie, alsook voor wie compensatie noodzakelijk is. Dit werk zal al gestart moeten worden tijdens de uitvoering van de pilots gezien de grote tijdsdruk van deze transitie. Ook substitutie en synergie-effecten (het vervangen van verschillende uitgifteprocessen, controle en beheersystemen en (deel)systemen door één systeem op eIDAS hoog) is onderdeel van deze discussie. Er zal geïnventariseerd moeten worden wie wat levert en wie wel/niet gecompenseerd kan worden. Bijvoorbeeld de leverancier maakt de kosten; sommigen leveranciers zullen eenmalig leveren en sommigen aan meerdere instellingen. Verder zal duidelijk moeten worden hoe de extra kosten voor zorgverleners gedragen kunnen worden. Het zou bijvoorbeeld opgenomen kunnen worden als onderdeel van de reguliere zorgkosten (als onderdeel in de integrale bekostiging voor prestaties). Er zal een business model moeten worden opgesteld voor na de transitie voor de instandhouding. Het veld kan zal in de vormgeving een rol moeten spelen. Zie ook verder hoofdstuk 5.
2) <u>Rollen:</u> de rollen zullen toebedeeld moeten worden specifiek voor de transitie en opschaling naar een operationeel stelsel (zie paragraaf 4.4). TNO adviseert dat VWS de taken verdeelt en de verantwoordelijke aanwijst en betaalt voor implementatie (transitiemanager). De aangewezen auditor en de instantie die de middelen toe laat in het nieuwe stelsel zullen een lijst met erkende authenticatiemiddelen moeten bepalen die aangeeft met welke middelen zorgverleners aan de slag kunnen.
3) <u>Evaluatie:</u> het is essentieel om te blijven evalueren tijdens en na implementatie. Betrek hierbij de aangestelde adviesraad.

Voldoen de uitkomsten van de pilots onvoldoende aan de criteria dan zal de levensduur van de UZI pas verlengd moeten worden en is het noodzakelijk om te heroriënteren (bijvoorbeeld op een systeem waarbij toch eerst een tussen stap wordt gemaakt naar authenticatiemiddelen op het niveau substantieel). TNO adviseert om voor deze situatie een draaiboek te maken.

4.4 Geïdentificeerde rollen en activiteiten voor de transitie en borging van het nieuwe stelsel

Er zijn rollen gedefinieerd in de transitie naar het nieuwe authenticatiestelsel en het uiteindelijke authenticatiestelsel, die partijen de verantwoordelijkheid geven om de thema's te borgen. Deze rollen komen voort uit een analyse van rollen in de huidige situatie (zie bijlage D), alsook nieuwe rollen die voortkomen uit deskresearch en gesprekken met experts.

De reden van deze introductie van (nieuwe) rollen is de transitie naar een open markt, waarbij keuze uit meerdere authenticatiemiddelen met een eIDAS hoog betrouwbaarheidsniveau de norm is. Om een dergelijke open markt op een efficiënte manier te reguleren zijn besturende, uitvoerende en toezichthoudende rollen en activiteiten van belang (tabel 11).

Tabel 11 Overzicht van geïdentificeerde rollen voor de transitie en borging van het nieuwe stelsel.

Besturend	**Uitvoerend**	**Toezichthoudend**
Stelselverantwoordelijke	Financier (uitvoerend)	Agentschap Authenticatie
Financier (besturend)	Eindgebruiker	Inspectie
Adviseur	Leverancier authenticatiemiddelen	
Autorisator(s) / Beslisser	Softwareleverancier	
Erkenner authenticatiemiddelen	Functioneel beheerder	
	Technisch beheerder	
	Distributeur	
	Auditor	
	Registerbeheerder	

Disclaimer: één partij kan meerdere rollen op zich nemen en vice versa, meerdere partijen kunnen gezamenlijk een rol oppakken.

Besturende rollen:

- **Stelselverantwoordelijke:** is aanjager en facilitator voor het beheer en onderhoud van het stelsel. In dit stelsel worden standaarden met bijbehorende randvoorwaarden gesteld en stippen op de horizon bepaald (spectrum open/gesloten markt, aantal dominante partijen, etc.).
- **Financier (besturend):** bepaalt het financiële model en waarborgt de financiën met name van het afsprakenstelsel, te denken aan een kosten-batenoverweging en een businessmodel.

- **Adviseur**: beschikt over de (inhoudelijke) kennis en levert input (bijvoorbeeld aan de houder en beheerders).
- **Autorisator(s) / Beslisser** (wenselijk om dit te doen via een adviesraad): neemt besluiten op basis van de afgesproken processen ten aanzien van wijzigingsvoorstellen.
- **Erkenner authenticatiemiddelen**: laat authenticatiemiddelen die voldoen aan de eisen toe tot het stelsel.

Uitvoerende rollen:

- **Financier (uitvoerend):** is een actor in het business model.
- **Eindgebruiker:** ieder persoon of rechtspersoon die gebruik maakt van het stelsel en wijzigingsverzoeken kan indienen via hun zorgaanbieder of leverancier. Hier vallen zorgprofessionals/-aanbieders onder.
- **Leverancier authenticatiemiddelen:** biedt middelen aan die moeten voldoen aan de randvoorwaarden van het stelsel.
- **Softwareleverancier:** levert software die van belang is voor het in werking brengen van de authenticatiemiddelen.
- **Functioneel Beheerder:** bewaakt en voert het proces rondom de afhandeling van wijzigingsverzoeken uit omtrent de standaarden binnen het stelsel, faciliteert eisen voor functionele aanpassingen communiceert naar de technisch beheerder. Een standaard is bijvoorbeeld de koppeling van het middel met UZI register.
- **Technisch Beheerder:** de organisatie die de (technische) omgeving beheert waarin de standaarden en randvoorwaarden binnen het stelsel wordt onderhouden en beschikbaar wordt gesteld, daarnaast aanpassingen technisch doorvoert. Hier wordt de functionele specificatie (zoals beschreven bij de functionele beheerder) omgezet naar een technische specificatie.
- **Distributeur** (kan bij meerdere partijen vallen)**:** stelt standaarden en randvoorwaarden van het stelsel beschikbaar, de lijst met middelen die hieraan voldoen en communiceert hierover naar alle betrokkenen.
- **Zorgverlener** (laat) processen en applicaties aanpassen om te voldoen aan het afsprakenstelsel.
- **Autorisator(s)** (wenselijk om dit te doen via een adviesraad)**:** neemt besluiten op basis van de afgesproken processen ten aanzien van wijzigingsvoorstellen.
- **Auditor:** voert audits uit om de zekerheidsniveaus van de middelen te beoordelen.
- **Registerbeheerder:** beheert en onderhoudt register (UZI/BIG).

Toezichthoudende rollen:

- **Agentschap Authenticatie**: controleert de auditor en waarborgt daarmee de ambities van het authenticatiestelsel.
- **Inspectie**: bewaakt de naleving van de regelgeving en verwijzen daarbij naar de standaarden. Hier gaat het om bijvoorbeeld de privacy waarborging en niet om de standaarden binnen het UZI-stelsel.

De besturende rollen, alsook de technisch en functioneel beheerder moeten nationaal zijn zodat interoperabiliteit geborgd blijft.

Rollen en activiteiten tijdens de transitie van het huidige naar het nieuwe stelsel
Om tot het nieuwe stelsel te komen moeten er voorbereidingen getroffen worden. Elk van de bovengenoemde rollen hebben hierin een taak te vervullen. In onderstaand tabel zijn de rollen uitgezet tegen de verschillende fases in de roadmap. De rollen zullen grotendeels ook behouden blijven na implementatie. Deze rollen zijn een voorstel en zijn nog niet afgestemd met de verschillende partijen.

Tabel 12 Besturende rollen.

Rollen	Wie	Fase 1a: Bewustwording	Fase 1b: Technische demonstraties	Fase 2a: Voorbereiding; standaarden & ontwikkelingen	Fase 2b: Praktijk Pilots uitrollen	Fase 2c: Technische implementatie
Eigenaar van de transitie	**VWS**	Eigenaar van de boodschap, initiator van communicatieplan		VWS: toekennen van (nieuwe) rollen, faciliteert gesprek en stelt soft en technische randvoorwaarden	Opdrachtgever van pilots	Eigenaar van de boodschap, initiator van communicatieplan
Eigenaar probleem van financier van transitie	**VWS**	Zorgt dat communicatieplan wordt gefinancierd		Stelt een nieuw financieringsplan samen	Zorgt dat pilot wordt gefinancierd	Zorgt dat uitrol en communicatieplan wordt gefinancierd
Adviseur	**Onderzoeks-organisatie**		Specificeren en toetsen demo	Leveren input voor het actualiseren en toekomstbestendig maken van standaarden	Onderzoeksorganisaties verantwoordelijk (gesteld) voor evaluatie en begeleiding van pilots	
Autorisator(s) / Beslisser	**Adviesraad met afgevaardigden van alle actoren**	Klankbordgroep UZI wordt betrokken		Adviesraad vastgesteld, zij maken besluiten over het doorvoeren van wijzigingen in het nieuwe stelsel	Betrokken bij de evaluatie van de pilots	Monitoren het proces
Erkenner authenticatie-middelen	**CIBG**					laat authenticatiemiddelen met een hoog zekerheidsniveau toe in het stelsel

Tabel 13 Uitvoerende rollen

Rollen	Wie	Fase 1a: Bewustwording	Fase 1b: Technische demonstraties	Fase 2a: Voorbereiding; standaarden & ontwikkelingen	Fase 2b: Praktijk Pilots uitrollen	Fase 2c: Technische implementatie
Financiers in het nieuwe stelsel	**VWS of een andere partij die deze rol krijgt van VWS**			Betrokken bij de ontwikkeling van het financieringsplan	Betrokken bij de uitvoer van de pilots	Financiert instandhouding van middelen in het nieuwe stelsel CIBG: Uitfasering passen & certificaten
Eindgebruiker	**Zorgprofessionals en zorgaanbieders**	Worden actief betrokken bij de boodschap, b.v. via de klankbordgroep	Ontvangen demo ter toetsing en acceptatie	Leveren input voor het actualiseren en toekomstbestendig maken van (de te gebruiken) standaarden	Betrokken bij de uitvoer van de pilots	Passen de nieuwe middelen toe
Leveranciers	**ICT leveranciers**	Worden actief betrokken bij de boodschap, b.v. via de klankbordgroep	Ontwikkelen de demo	Leveren input voor het actualiseren en toekomstbestendig maken van (de te gebruiken) standaarden	Betrokken bij de uitvoer van de pilots	Schalen op / bieden de middelen en services die voldoen aan de normen en standaarden
Functioneel beheerder	**NEN en/of Nictiz Zorg instituut NL**			Faciliteert het actualiseren en ontwikkelen toekomstbestendig standaarden		Starten met operationele taken
Technisch beheerder	**NEN/andere organisatie**			Voeren geactualiseerde en toekomstbestendige standaarden door		Starten met operationele taken
Distributeur	**b.v. beroepsverenigingen, stichtingen, AP**	Voeren het communicatieplan uit		Communiceren (nieuwe) standaarden		Voeren het communicatieplan uit
Auditor	**NEN-geaccrediteerde marktpartijen**				Betrokken bij de evaluatie van de pilots	Begint met audits en koppelt resultaten terug aan de adviesraad
Registerbeheerder	**CIBG**			compleet maken en loskoppelen UZI register		Bieden een volledig register (UZI/BIG) aan
Agentschap Authenticatie	**AT**					controleert de auditor
Inspectie	**AP en/of IGJ**					bewaakt de naleving van de regelgeving en verwijzen daarbij naar de standaarden

5 Financiële consequenties

5.1 Introductie & opbouw van het hoofdstuk

De geschetste veranderingen rondom digitale identificatie binnen de zorg zullen een financiële impact hebben. De verandering die volgt uit de in hoofdstuk 4 beschreven roadmap is in omvang groot; de groei van een groep van de ongeveer 90.000 huidige gebruikers van UZI-passen naar een persoonlijk inlogmiddel voor 1.500.0000 zorgmedewerkers naar een hoger eIDAS betrouwbaarheidsniveau kent financiële consequenties. Dit gecombineerd met een andere rol opvatting van het CIBG, dat verandert van inlogmiddelverstrekker van de huidige UZI-passen en certificaten naar een partij die alleen zorgdraagt voor de juiste registratie van zorgmedewerkers en deze beschikbaar maken voor gekwalificeerde partijen, is fors. Deze rolverandering zorgt voor de introductie van nieuwe partijen die inlogmiddelen kunnen uitgeven alsmede een veranderd (toezicht) stelsel waarbinnen deze partijen moeten functioneren om te kunnen voldoen aan de eisen die gesteld worden aan eIDAS.

Hierdoor raakt de wijziging het gehele zorgstelsel, het aantal gebruikers zal stijgen, er moet een nieuw toezichtstelsel opgezet worden en er zullen (in deze sector) nieuwe marktpartijen nieuwe diensten gaan aanbieden[9]. Tegelijkertijd zijn er in potentie synergie-mogelijkheden; verschillende systemen die zorgmedewerkers nu al gebruiken voor verschillende applicaties en toepassingen kunnen mogelijk worden geharmoniseerd op het vlak van authenticatie. Hiermee kunnen verborgen kosten van authenticatie in allerlei systemen worden geëlimineerd. In de interviews met zorg- en ICT partijen is helaas niet vast komen te staan welke mogelijke besparingen hiermee gemoeid kunnen zijn.

In dit hoofdstuk worden, vanuit de verwachte wijzigingen in het stelsel en de gebruikersgroepen, een eerste doorvertaling gemaakt naar de financiële implicaties. Hiervoor wordt informatie gebruikt die gedurende de onderzoeksperiode beschikbaar is gekomen. Daarnaast zijn een aantal onderbouwde aannames gedaan en besproken in het overleg tussen TNO en de opdrachtgever.

In het eerste subhoofdstuk worden de inschattingen van huidige en toekomstige kosten rondom de UZI pas en digitale identificatie in de zorg beschreven. Hiertoe wordt als eerste een overzicht gemaakt van de huidige operationele manier van werken van partijen en inzicht gegeven in de financiële organisatie van dit systeem. Dit doen we aan de hand van een waardenetwerk met daarin alle rollen en waarde uitwisselingen tussen de rollen.

Op basis van de beschikbare informatie zijn financiële scenario's voor verschillende situaties geschetst en vergeleken om hiermee de vraag "hoeveel zal deze verandering kosten" zo goed als mogelijk te beantwoorden, gegeven de onzekerheden.
In het tweede subhoofdstuk wordt een nieuw waardenetwerk voorgesteld om de werking van het toekomstige systeem inzichtelijk te maken. Dit waardenetwerk geeft

[9] Een belangrijke afhankelijkheid voor de toetreding van nieuwe partijen ligt daarnaast ook in de ontwikkeling van publieke inlogmiddelen, waar het Ministerie van BZK regie voert.

weer op welke manier dit nieuwe stelsel kan werken en laat ook de geldstromen tussen de verschillende rollen zien. Op deze manier wordt inzicht gegeven welke mogelijke manieren van financiering partijen in het zorgsysteem kunnen inzetten om veranderingen voor partijen op te vangen.

5.2 Inschatting van huidige en toekomstige kosten UZI pas -systeem

5.2.1 Waardenetwerk huidig systeem - opbouw

In het huidige systeem kennen we een beperkt aantal partijen dat actief is en kosten draagt in het UZI pas systeem. We identificeren kostendragers en benoemen hun rol en activiteiten in relatie tot het huidige UZI pas-systeem.

CIBG

Beginnend bij het UZI-pas systeem, worden door het CIBG kosten gemaakt voor de verwerking van de aanvraag en het afleveren van de pas/servercertificaat. Deze kosten worden doorberekend in de kostprijs van producten (UZI-passen) en diensten (servercertificaten) en zijn, zoals de website van CIBG aangeeft 'kostendekkend'[10]. De passen worden persoonlijk overhandigd aan een zorgmedewerker. Voor persoonlijke overhandiging vindt er een fysieke identiteitscontrole plaats.

Op basis van de informatie van het CIBG zijn er anno 2021[11] 83.559 UZI passen in omloop. Zonder in te gaan op de soorten passen, geeft deze informatie inzicht in het huidige gebruik bij zorgorganisaties (9.745 organisaties met 60.112 passen)) en zelfstandige werkende zorgprofessionals (23.447 passen). Naast de UZI-passen zijn er 11.887 UZI-servercertificaten door het CIBG uitgegeven.

De kosten die het CIBG maakt voor de uitgifte en beheer van UZI-passen en UZI-servercertificaten bedraagt (voor 2022) € 13,6 miljoen euro[12]. Deze kosten zijn als volgt opgebouwd:

Tabel 14 Uitsplitsing kosten die CIBG maakt voor de UZI passen.

UZI-register & ZOVAR[13]	**2022**	**2021**
Directe personele kosten uitvoering	€ 993.518	€ 975.774
Directe materiële kosten uitvoering	€ 6.090.150	€ 6.127.564
Directe systeemkosten instandhouding	€ 3.919.679	€ 3.803.737
Directe afschrijvingskosten	€ 118.000	€ 118.000
Indirecte kosten	€ 2.477.653	€ 2.339.525
Totaal	**€ 13.599.000**	**€ 13.364.000**

Bron CIBG (april 2022)– verstrekt t.b.v. dit onderzoek/ niet extern te delen

[10] Kosten, geldigheidsduur en facturatie | UZI-pas | UZI-register (uziregister.nl) (geraadpleegd 9-12-2022)
[11] Verstrekt door CIBG 14 dec 2021.
[12] Bron: CIBG – 9 april 2022
[13] ZOVAR (Zorgverzekeraars identificatie en authenticatie register) en UZI zijn twee aparte "labels", waarbij ZOVAR voor zorgverzekeraars is en UZI voor zorgaanbieders. ZOVAR abonnees kunnen alleen een servercertificaat aanvragen. Voor de instandhouding van ZOVAR en de uitgifte van een servercertificaat wordt gebruikgemaakt van dezelfde mensen en systemen. Er wordt geen onderscheid gemaakt in kosten per label.

Zorg
Het gebruik van het systeem door zorgorganisaties en de zelfstandig werkende professionals heeft kostenconsequenties. De UZI pas moet worden gebruikt door deze in een pas-lezer te steken, waardoor een verbinding kan worden gemaakt met de software systemen om toegang te krijgen tot medische gegevens. Het gebruik van servercertificaten heeft daarnaast ook zogenaamd middleware verbindingen nodig waarin de servercertificaten worden gebruikt om de juiste verbindingen tot stand te brengen tussen geautoriseerde partijen om gegevens mee te delen. Het systeem werkt dus pas met de juiste middelen (software-middelware-hardware) hetgeen aan de kant van de gebruiker dus ook kosten met zich meebrengt (zorgverlener (paslezer, N keer) en zorgaanbieder (server certificaten, 1 keer).

In het onderzoek is gesproken met partijen die deze functionele elementen aanbieden door middel van ICT-pakketten aan zorgorganisaties en zelfstandig opererende zorgprofessionals. Deze onderdelen (inloggen met een geautoriseerd inlogmiddel zoals een UZI pas) vormen een beperkt onderdeel van een zorg ICT pakket (bijvoorbeeld een ziekenhuisinformatiesysteem) en is moeilijk af te zonderen van de pakketkosten als geheel. Gedurende het onderzoek zijn leveranciers niet bereid geweest om inzicht te geven in kosten van (delen van) zorg-ICT systemen. Een ander aspect is dat dit onderdeel slechts één van de middelen is die zorgorganisaties en professionals gebruiken om mee te werken. Uit de interviews bleek al dat er uiteenlopende inlogmiddelen en systemen naast elkaar worden gebruikt variërend van fysieke toegangspassen, tot communicatiemiddelen zoals fax, wetransfer, RSA-tokens). De geïnterviewden gaven aan soms wel tot 10 uiteenlopende passen, tokens en andere hulpmiddelen te gebruiken om in verschillende systemen in te loggen of van functionaliteiten in de werkomgeving gebruik te maken. Deze constatering is relevant, omdat bij het verstrekken van een erkend persoonlijk authenticatiemiddel aan iedere zorgmedewerker op een hoger eIDAS niveau, er een aanleiding is om synergiën tussen uiteenlopende middelen op te zoeken.

Door het ontbreken van specifieke kostengegevens van zorg ICT voor het gebruik van UZI middelen (passen en certificaten) heeft TNO besloten om daarom te werken met een aantal werkaannames om de kosten in beeld te brengen. Deze kosten zijn gebaseerd op de interviews met zorgverleners die wel inzicht gaven in de kosten die zij kwijt zijn aan zorg ICT (de prijs van het pakket als geheel) waarna op arbitraire manier een deel van de kosten is toegerekend aan het onderdeel inlogmiddelen. Hiertoe is onder meer gekeken naar prijzen voor individuele componenten zoals UZI pas lezers, alsmede inschattingen van organisaties die hun eigen zorg ICT ontwerpen, beheren en onderhouden en weten welke inspanning het kost om veranderingen door te voeren in systemen.

Er is een categorisering gemaakt op basis van het aantal passen in een zorgorganisatie en is uitgedrukt als kosten per organisatie. Deze indeling is arbitrair maar schaalt goed mee met de beschikbare ICT basis en complexiteit van systemen van software, middleware- en hardware (inclusief paslezers).

Klein:	< 5 passen per organisatie	kosten 500 euro/jaar
Middel	≥ 5 passen en < 20 passen per organisatie	kosten 2.000 euro/jaar
Groot	≥ 20 passen per organisatie	kosten 5.000 euro/jaar

Op basis van de door CIBG verstrekte gegevens zijn de gebruikers gecategoriseerd in deze drie categorieën (7.237 kleine organisaties, 2.254 middel en 227 grote organisaties. De zelfstandig werkende zorgprofessionals (23.447) worden qua omvang geschaard onder de categorie 'klein'. Bij de berekening in tabel 15 zijn deze als aparte groep opgenomen

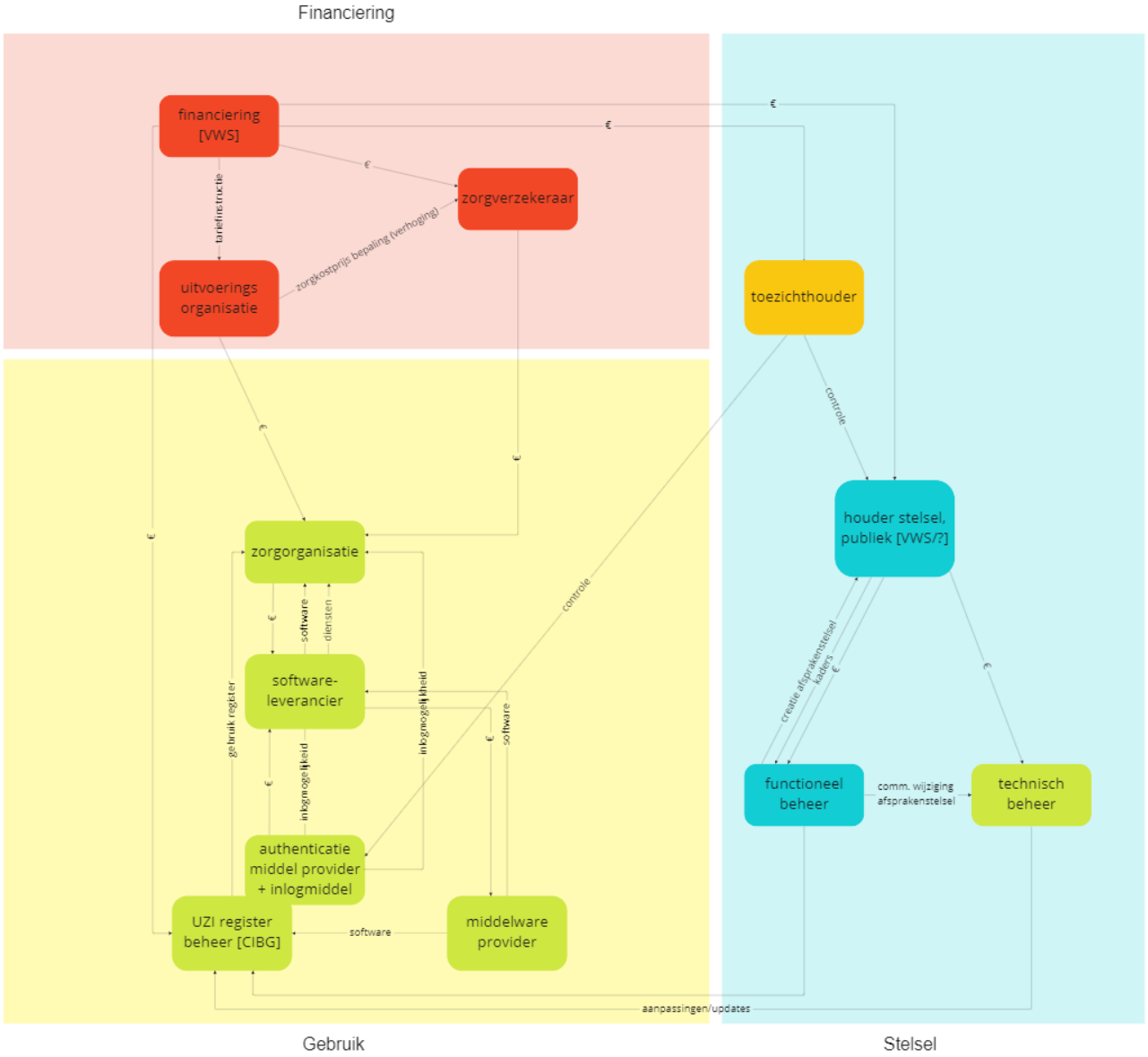
De kosten die zorgorganisaties moeten maken om in het huidige systeem gebruik te kunnen maken van het UZI passysteem zijn voor alle organisaties (op jaarbasis) uitgerekend en bestaat uit de kosten voor de passen (1/3 van de kosten voor passen, omdat passen 3 jaar meegaan) en de zorg ICT (inclusief de afname van server-certificaten die door CIBG worden uitgegeven, als onderdeel van het ICT pakket).

Tabel 15 Kosten gemaakt door zorg voor toepassing van UZI passen.

	abonnee organisaties	categorie		aanname kosten/jaar (€)	Totaal (€)
abonnee org	9.754	7.273	klein	500	€ 3.636.500
		2.254	middel	2000	€ 4.508.000
		227	groot	5000	€ 1.135.000
	zorgverleners (zelfstandig,solistisch werkend)				
passen	23.447		klein	500	€ 11.723.500
pasaanschaf	83.559	(aantal passen)			€ 7.102.515
Totaal					**€ 28.105.515**

De kosten die gemaakt worden in de zorg voor de toepassing van de UZI passen die wordt geschat op basis van voorgaande aannames bedragen ongeveer 28 mln euro per jaar (tabel 16). Deze inschatting van kosten staat los van de overige systemen die worden gebruikt in de zorg waar een persoonlijke authenticatiemiddel een rol speelt om toegang te krijgen tot systemen en faciliteiten (deze zijn voor dit onderzoek out of scope).

Het systeem waarin deze kosten worden gemaakt ziet er als volgt uit:



Figuur 7 Overzicht systeem waarin bovenstaande kosten worden gemaakt.

Het huidige systeem ziet er enigszins complex uit, maar omdat meerdere rollen door dezelfde partij worden uitgevoerd (CIBG), is het in de werkelijkheid overzichtelijk. Een aantal rollen worden uitgevoerd door andere partijen, via een uitbesteding door CIBG.

In het nieuwe systeem komen er een aantal nieuwe rollen bij die beschreven zijn in het vorige hoofdstuk. Eén van de redenen waarom de complexiteit toeneemt in het systeem is dat een deel van de huidige rollen die nu door het CIBG worden ingevuld, door nieuwe partijen vervuld zullen worden. Het nieuwe systeem wordt weergeven in het volgende hoofdstuk.

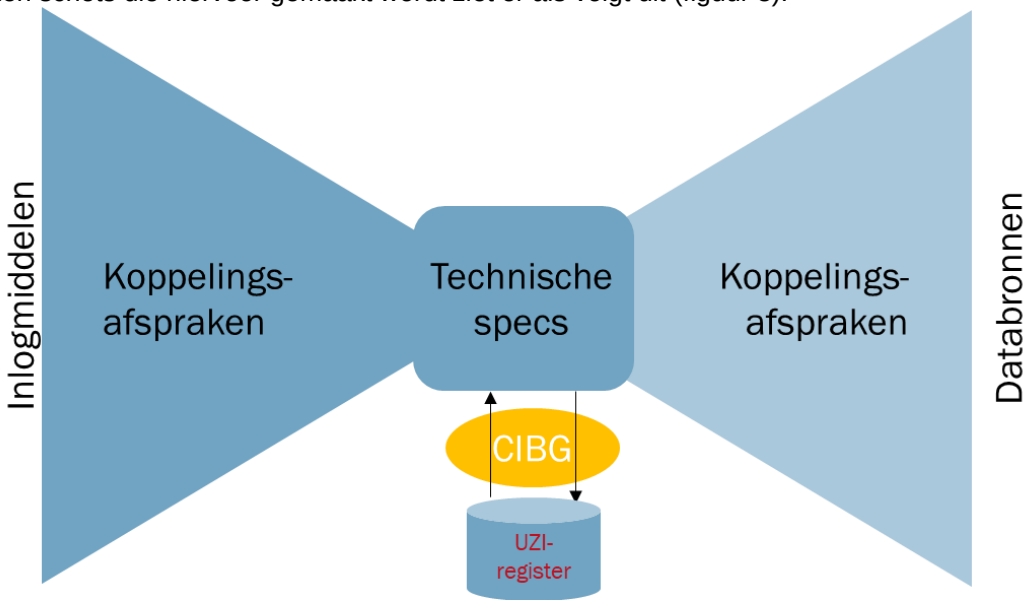
5.2.2 Opbouw & kosten voor nieuwe systeem

Het uitgangspunt voor het nieuwe systeem is dat iedere zorgmedewerker een persoonlijk authenticatiemiddel krijgt op een hoger betrouwbaarheidsniveau. TNO geeft aan dat een overstap naar eIDAS hoog daarbij aan te raden is, zonder tussenstappen naar eIDAS substantieel.

Door de rolverandering van het CIBG; die in de toekomstige situatie niet langer UZI passen en servercertificaten zal uitgeven, dient deze rol en functie op een andere wijze ingevuld te worden. Dit kan gebeuren door andere publieke middelen te voorzien van zorgspecifieke functionaliteiten of door private middelen toe te laten (WDO route). De keuzevrijheid voor het soort authenticatiemiddel ligt bij de zorgorganisatie of de zelfstandig werkende zorgprofessional (keuzevrijheid). Het CIBG behoud de rol van het controleren van de identiteit van de zorgprofessional en het verstrekken van een uniek zorgregistratie nummer aan individuen (het 'register'). Nieuwe middelen zullen moeten worden getoetst en toegelaten tot het systeem

Dit register kan bevraagbaar worden gemaakt waardoor gebruikers zich kunnen identificeren met een authenticatiemiddel waardoor ze worden geautoriseerd om toegang te kunnen krijgen tot medische en persoonlijke gegevens in databronnen die moeten voldoen aan de toegangseisen volgens eIDAS.

Een schets die hiervoor gemaakt wordt ziet er als volgt uit (figuur 8):

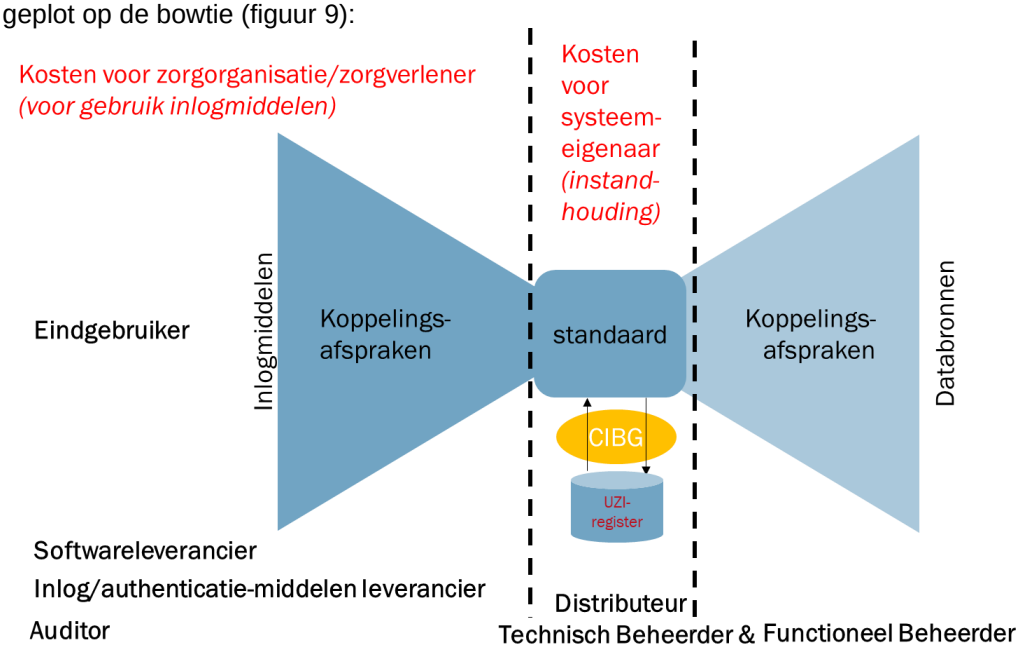


Figuur 8 De rol van het UZI register en de rol van het CIBG bij het nieuwe systeem om via inlogmiddelen toegang te krijgen tot databronnen.

Een gevolg van de verandering van de rol van CIBG (van authenticatiemiddel verstrekker naar alleen de rol van beheerder van het UZI- register) is dat de zorgsector gebruik moet maken van een nieuwe set aan authenticatiemiddelen.

Deze authenticatiemiddelen kunnen zowel publiek beschikbare authenticatiemiddelen zijn (DigiD), als private middelen die onder de WDO moeten worden erkend en/of nog zorgspecifiek toegelaten moeten worden. Deze nieuwe middelen kunnen uiteenlopende verschijningsvormen hebben (van fysiek tot digitaal of een mix) afhankelijk van het na te streven eIDAS niveau en de praktische bruikbaarheid (niet in iedere omgeving is elk middel praktisch bruikbaar). Opgemerkt wordt dat er een belangrijke afhankelijkheid is in de snelheid en implementatie van de WDO door het ministerie van Binnenlandse Zaken.

De rollen die zijn bedacht in sectie 4.4 kunnen op de volgende manier worden geplot op de bowtie (figuur 9):



Figuur 9 Bowtie met rollen en scheiding van kostensoorten (rood).

In bovenstaande figuur 9 is in rood weergegeven welke kosten zorgorganisaties en zelfstandig werkende zorgprofessionals in ieder geval moeten dragen voor het gebruik van in het systeem en een deel van de kosten voor rekening voor het in stand houden van het systeem nodig zijn. Daarnaast zijn er nog kosten voor (organisatie van) het beheer en doorontwikkeling van het stelsel, erkenning, toelating, handhaving e.d (zie rollen hoofdstuk 4)

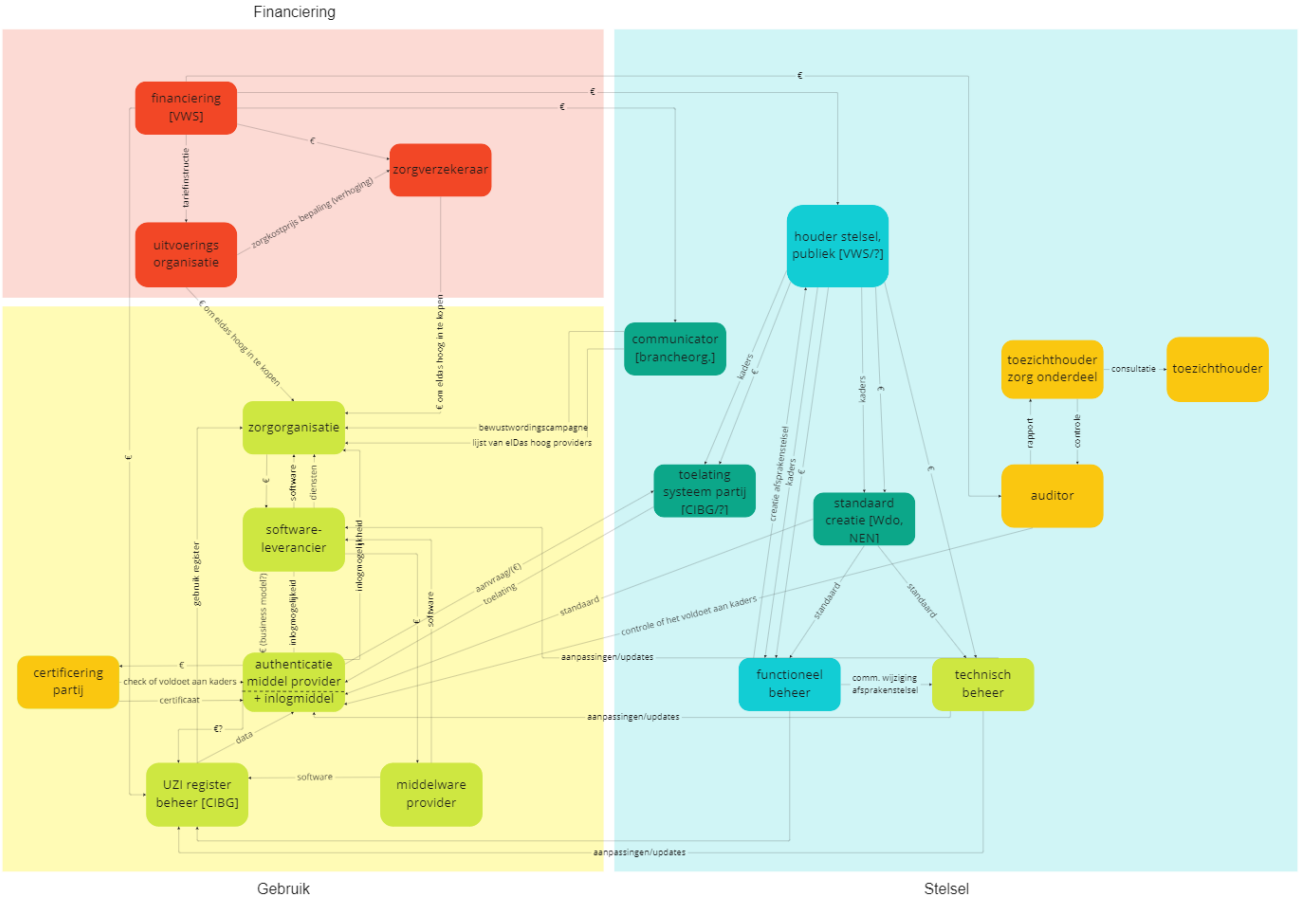
Qua authenticatiemiddelen is het goed om op te merken dat er een ontkoppelpunt zit tussen het authenticatiemiddel (infrastructuur authenticatiemiddel) zelf en de gebruikte zorg ICT-pakket. Op deze manier wordt er voor een zo breed mogelijk pakket aan zorgspecifieke authenticatiemiddelen ruimte geboden in het systeem , die allemaal kunnen koppelen aan de verschillende ICT platform diensten (het gaat hierbij over WDO toegelaten zorgspecifieke inlogmiddelen. Zorgspecifieke middelen mogen worden uitgegeven door zorgaanbieders; en die kunnen kiezen voor private middelen .

Met deze laatste mogelijkheden ligt het dus voor zorgorganisaties in hun eigen vermogen om eigen middelen te verstrekken aan medewerkers (zolang het proces

waarlangs zij dit doen gecertificeerd is en zij toegelaten zijn als authenticatiemiddelverstrekker). Hierdoor liggen mogelijk synergie voordelen en besparingen met andere bestaande systemen voor de hand om digitale en fysieke middelen gezamenlijk te ontsluiten via één systeem. Hierdoor kunnen bijvoorbeeld op de (digitale) werkplek uiteenlopende systemen worden samengevoegd en vereenvoudigd.

5.2.3 Waardenetwerk

Om inzichtelijk te maken hoe het nieuwe systeem eruit zal zien en hoe de kosten en financieringsstromen zouden kunnen lopen is er een waardenetwerk gemaakt (Figuur 10). Hierin staan de rollen die vervuld zullen worden in het nieuwe systeem en de waardeuitwisselingen tussen deze rollen. Deze weergave dient als een praatplaat die gebruikt kan worden om keuzes te maken over het systeem, en is niet een finale weergave van hoe het er uit zal zien.



Figuur 10 Waardenetwerk – rollen en uitwisselingen in het nieuwe systeem.

Een aantal algemene veranderingen rondom rollen in het nieuwe systeem, zoals zichtbaar in de plaat;

- Het rechter blauwe blok rondom het **“stelsel” is ten dele nieuw**, het bestaat in deze vorm in het huidige systeem nog niet. Dit betekent dat nieuwe rollen vervuld zullen moeten worden en dat het optuigen en

operationeel houden van dit stelsel additionele kosten zal brengen in het gehele systeem.
- De rollen in het gele **"gebruik" blok veranderen niet veel** ten opzichte van het huidige systeem. Authenticatie middel providers zullen er wel meer zijn dan nu (op het moment is het alleen UZI-pas) en certificeringspartijen zullen ook een rol spelen, wat weer voor extra kosten zal zorgen.
- Er zijn **geen nieuwe rollen in het rode "financiering" blok,** maar de budgetten waarmee gewerkt wordt zullen wel aangepast moeten worden naar de nieuwe kosten van het systeem.
- **Het aantal eindgebruikers zal significant stijgen.** In de nieuwe situatie zullen veel meer zorgprofessionals een eIDAS hoog inlogmiddel moeten hebben. Hierdoor zal het aantal gebruikers van het huidige 90.000 naar ongeveer 1.500.000 stijgen, wat veel financiële implicaties zal hebben voor het systeem – denk bijv. aan toelatingen, checks, kosten en processen.

Inschatting kosten
In deze sectie geven we een indicatie van de kosten die gemaakt worden in de nieuwe systeem opzet.

CIBG
Net als in de berekening van het oude systeem beginnen we met de beperkte rol van het CIBG. Een verandering is dat het CIBG niet langer inlogmiddelen uitgeeft. Een tweede wijziging is dat het aantal gebruikers zal toenemen. In overleg met het CIBG (september 2022) is een inschatting gegeven van de toekomstige kosten van deze wijzigingen. De geschatte jaarkosten komen uit op ongeveer **8 mln euro** en zijn opgebouwd als volgt:

Tabel 16 Inschatting CIBG kosten in nieuwe rol.

UZI-register	**202X**
Directe personele kosten uitvoering	€ 1.000.000
Directe materiële kosten uitvoering	
Directe systeemkosten instandhouding	€ 4.000.000
Directe afschrijvingskosten	
Indirecte kosten	€ 3.000.000
Totaal	€ 8.000.000

De kosten voor het CIBG nemen dus af. Dit hangt vooral samen met de rolverandering waardoor zij niet zelf meer de materiele kosten voor de uitvoering hoeven te bekostigen. Onder deze post vallen onder meer de kosten technische omgeving om passen/certificaten te produceren, inkoop chips, koerier voor persoonlijke overhandiging, middleware en technische ondersteuning. Deze kosten komen terug op een andere plek in het systeem (en bij andere partijen).

De toename van het aantal gebruikers tot 1.500.000 is geen aanleiding tot hoge aanvullende kosten. De diensten die samenhangen met de uitvoering en

instandhouding gebeuren grotendeels automatisch en zijn niet of minder afhankelijk van het aantal gebruikers.

Authenticatiemiddelverstrekker
Een nieuwe partij is nodig die een authenticatiemiddel gaat verstrekken aan zorgmedewerkers. Deze partij kan zowel een publieke als een privaatrechtelijke achtergrond hebben.

In het onderzoek door TNO is een eerste inschatting gemaakt voor kosten die samenhangen met het verstrekken van authenticatiemiddelen op het niveau eIDAS hoog.

De bandbreedte voor deze middelen wordt geschat op 20-70 euro per medewerker. De bandbreedte is tot stand gekomen op basis van de huidige kosten van het uitvoeringsproces van het CIBG waar de kosten de bovenkant van deze range bestrijkt.

Voor de onderkant van de inschatting is gekeken naar wat mogelijk digitale oplossingen als kostprijs per gebruiker per jaar kunnen rekenen. In gesprekken met marktpartijen worden ramingen gegeven van deze orde grootte. TNO raad aan deze kosten nader te onderzoeken, gegeven de grote bandbreedte en systeemonzekerheden en afhankelijkheid van de invoering van de WDO.

Indien wordt gekozen voor een lager eIDAS niveau dalen de kosten per gebruiker; de bandbreedte die hiervoor wordt gehanteerd bedraagt 5 tot 40 euro per gebruiker.

Tabel 17 Het gebruik van een inlogmiddel voor iedere medewerker in de zorg (schatting).

eIDAS-niveau	Kosten per gebruiker (bandbreedte)		Gebruikers	Kosten	
	Laag (in euro)	Hoog (in euro)	Aantal (#)	Laag (in euro)	Hoog (in euro)
substantieel	5	40	1.500.000	7.500.000	60.000.000
hoog	20	70	1.500.000	30.000.000	105.000.000

Opgemerkt wordt dat er naast kosten voor zorgorganisaties ook inverdieneffecten te verwachten zijn. Dit zijn potentiële besparingen als gevolg van de introductie van één authenticatiemiddel dat kan dienen als ontsluiting voor diverse andere systemen (toegangscontrolesysteem, personeelskaart, etc. etc.) die door het benutten van synergie effecten kunnen worden uit gefaseerd en niet meer (apart) te hoeven worden aangeschaft, onderhouden.

5.2.4 Vervolgvragen voor kosteninschatting

In het waardenetwerk komen ook een aantal keuzepunten naar voren rondom financiering;

1. Gebruik UZI-register gratis of voor een vergoeding

De authenticatiemiddel provider (wat een marktpartij kan zijn) zal gekoppeld worden met het UZI register en daaruit data ophalen. Het businessmodel hierachter staat nog niet vast; zal dit gebruik gratis mogelijk zijn, of moet de authenticatiemiddel provider (AMP) betalen voor dit gebruik? Om een bijdrage te vragen van de AMP zou een manier zijn om de kosten voor het nieuwe stelsel voor een deel bij de markt terug te leggen. Zo zou het budget vanuit VWS wat nodig is voor UZI register beheer kleiner gemaakt kunnen worden. Hierdoor zou de AMP mogelijk wel een hogere prijs kunnen vragen van hun klanten (zorgorganisaties) en daarmee komen de kosten uiteindelijk deels toch weer bij VWS terecht (vergoeding zorgkosten). Om dit tegen te gaan zou het gebruik van het UZI-register centraal gefinancierd kunnen worden.

2. Betaalt de authenticatiemiddel provider een vergoeding voor toelating tot het systeem

Door een vergoeding te laten betalen zou vanuit de marktpartijen inkomsten stromen richting het stelsel. Deze additionele kosten zouden vervolgens hoogstwaarschijnlijk wel doorberekend worden richting de zorginstellingen, waardoor de keuze eigenlijk niet gaat over de hoeveelheid financiering die nodig is vanuit VWS, maar alleen over waar die aan gegeven wordt; aan de zorginstellingen of aan het stelsel. Bij deze keuze moet ook meegenomen worden dat BZK voor Wdo een vorm van toelatingsprijs beoogt, en een dubbele toelatingsprijs is niet wenselijk. Het kan ook overwogen worden om de authenticatiemiddel providers op een andere manier te motiveren, door bijvoorbeeld kosten voor de beoordeling en de audit aan hun door te berekenen.

3. Wie en in welke verdeling dragen de additionele kosten

Authenticatiemiddel providers en certificeringspartijen worden toegevoegd aan het huidige systeem, en dit zal de totale kosten van authenticatie binnen de zorg verhogen. Wel hoeven partijen die al zijn toegelaten tot de WDO geen additionele audit, die zijn dan al voor de WDO uitgevoerd. De kosten die gemaakt worden door de AMP worden doorberekend aan de softwareleveranciers, die het weer doorberekenen aan de zorgorganisaties. Er zal een keuze moeten worden gemaakt over de manier waarop de additionele kosten die bij de zorgorganisaties landen vergoedt zullen worden. Hiervoor bestaan een aantal mogelijkheden, namelijk via de zorgverzekeraar, via een tariefinstructie vanuit VWS richting zorgorganisaties of richting de zorgverzekeraar. Hoe de kosten eerlijk tussen deze twee partijen verdeeld zullen worden moet verder uitgezocht worden.

4. De rol van stelselhouder door VWS of andere organisatie

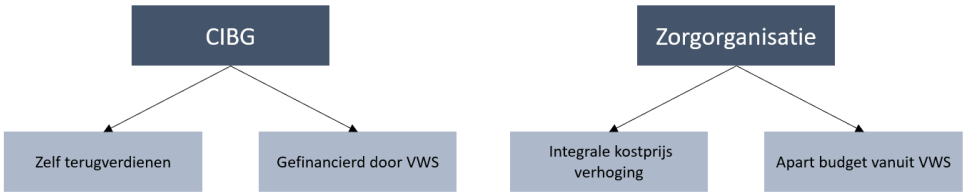
De stelselhouder zal een publieke partij moeten zijn, maar het staat nog niet vast welke partij deze rol op zich zou moeten nemen. Voor de hand liggend zou zijn als VWS dit zou doen, aangezien zij verantwoordelijk zijn voor het opzetten van dit stelsel. Deze taak zou ook uitbesteedt kunnen worden aan een bestaande of nieuwe uitvoeringsorganisatie, hierin zal ook een keuze gemaakt moeten worden.

5.2.5 Doorbelastingscenario's

Het antwoord op de voorgaande keuzepunten zal bepalend zijn voor de werking van het systeem. Er zijn een aantal doorbelastingscenario's opgetekend om mogelijke vormen van financiering te verkennen;

- *Toevoegen aan integrale kostprijs*
- *Extra budget voor zorgorganisaties*
- *Extra budget voor CIBG*
- *Achteraf declaratie voor zorgorganisaties*
- *Hybride vorm van bovenstaande opties*

De scenario's bouwen op twee financieringsmogelijkheden voor CIBG en voor de zorgorganisaties, zoals weergegeven in onderstaand figuur 11.



Figuur 11 Twee financieringsmogelijkheden voor CIBG en voor zorgorganisaties.

Scenario 1: Kosten toevoegen aan integrale kostprijs
In dit scenario zullen de geschatte extra kosten die gemaakt worden door het overstappen op het eIDAS hoog inlogmiddel aan het einde, "achteraf" worden verrekend via de integrale kostprijzen (op basis van productieafspraken tussen zorgorganisatie/verleners en zorgverzekeraars en de richtprijzen van DBC's en ZZP's). In dit geval is te verwachten dat zorgorganisaties op zoek gaan naar synergie tussen de huidige systemen en nieuwe authenticatie manieren, om hun totale authenticatie pakket zo efficiënt mogelijk te maken.

Scenario 2: Extra tijdelijk budget voor zorgorganisaties (vooraf)
In dit scenario zouden zorgorganisaties een apart budget voor een beperkte tijd krijgen van VWS om de stap richting eIDAS hoog inloggen te financieren. Deze manier moedigt de zorgorganisaties aan om daadwerkelijk aan de slag te gaan met implementatie van deze stap, en zorgt er ook voor dat kosten vergoed worden. Ten denken valt hierbij aan vaste bedragen per zorgorganisatie/verlener. Het is wel mogelijk dat de organisaties in dit geval nieuwe eIDAS hoog authenticatiemiddelen en systemen gaan inkopen, maar minder op zoek gaan naar synergiën tussen de nieuwe en huidige systemen, hier worden ze namelijk niet toe gestimuleerd. Dit kan tot nieuwe duurdere, complexere situaties leiden, waarin meerdere authenticatie-systemen tegelijk worden gebruikt, of geheel nieuwe systemen onnodig worden aangeschaft. Een éénmalig extra budget om de aanpassing/overstap te financieren zou dit effect waarschijnlijk niet meedragen.

Scenario 3: Extra budget voor CIBG
Op deze manier hoeven de kosten niet doorbelast te worden aan de andere partijen in het ecosysteem, wat de implementatie veel gemakkelijker maakt voor hen, ze hoeven namelijk niet de schuiven met eigen kosten en budgetten. Een risico van dit scenario is wel dat de partijen (authenticatie middel providers en zorgorganisaties

eveneens) daardoor dus ook geen incentive hebben om met een zo een laag mogelijke prijs te werken. Dit zou ervoor kunnen zorgen dat de additionele kosten die worden gemaakt vanwege deze verandering in totaal hoger zullen zijn dan de minimaal noodzakelijke hoeveelheid.

Scenario 4: Achteraf declaratie voor zorgorganisaties op basis van werkelijke kosten

Een andere mogelijkheid is om de additionele kosten helemaal te laten “doordruppelen” tot bij de zorgorganisaties, en daarna deze kosten te vergoeden door VWS (via de NZa). Een voordeel van deze aanpak is dat alleen de daadwerkelijke kosten worden doorberekend aan VWS, en dus niet een van tevoren ingeschatte budget wordt uitgegeven, wat mogelijk breder is dan de daadwerkelijke kosten. Op deze manier is er goed inzicht te krijgen in hoe duur deze verandering precies is voor zorgorganisaties. Een nadeel is dat deze optie zorgorganisaties niet direct aanspoort om zuinig om te gaan met de kosten van de verandering, omdat ze niet met een vast budget hoeven te werken wanneer ze kiezen tussen de authenticatiemiddel providers. Het is te verwachten dat authenticatiemiddel providers wel enigszins zullen gaan concurreren op prijs in dit scenario, wat een steile toename van de prijzen tegenhoudt. Het is tevens een oplossing die om andere redenen (verantwoording richting VWS of bijvoorbeeld de NZa) niet goed aansluit op de huidige wijze van financiering en verantwoordelijkheden in het stelsel en zorgt voor extra administratieve handelingen.

Scenario 5: Hybride oplossing

In dit geval zou de additionele financiering voor deze veranderstap richting eIDAS hoog op verschillende plaatsen het systeem binnen vloeien. Er kan hier gespeeld worden met combinaties om de juiste mix van voor- en nadelen van elk van de hiervoor beschreven scenario’s te behalen. Een hybride oplossing maakt het systeem complexer, wat op zichzelf ook tot additionele kosten kan leiden (e.g. meerdere processen die in stand moeten worden gehouden, meer soorten aanvragen, verschillende controle punten).

6 Conclusies en aanbevelingen

Het doel van het onderzoek uitgevoerd door TNO is om tot een groeimodel te komen voor sterkere authenticatie in de Nederlandse zorg, zonder dat daarbij de werkbaarheid voor de zorgverlener in het geding komt en optimale zorg blijvend kan worden verleend. Het doel is dat uiterlijk in 2028 iedere zorgverlener een persoonlijk inlogmiddel op betrouwbaarheidsniveau eIDAS hoog gebruikt.
Om de UZI-middelen toekomstbestendig te maken is geïnventariseerd wat de huidige inlogmiddelen en betrouwbaarheidsniveaus in de zorg zijn. Aan de hand hiervan is een groeimodel ontwikkeld om naar een hoger betrouwbaarheidsniveau te komen. Een passend instapniveau voor dit groeimodel is ook onderzocht. Hierbij is rekening gehouden met de omvang, het type van de zorgorganisaties en de financiële impact van de normverschuiving. Ten slotte zijn alleen authenticatieoplossingen meegenomen die beschikbaar zijn zodat de hanteerbaarheid voor de zorgverlener in ieder geval gelijk blijft en waarschijnlijk verbetert.

De belangrijkste bevindingen en aanbevelingen gedurende dit onderzoek zijn hieronder samengevat.

- Om een vendor lock-in te voorkomen is het van belang om de interoperabiliteit te waarborgen door middel van een afsprakenstelsel. Hiermee moet gerealiseerd worden dat elk geaccepteerd inlogmiddel gebruikt kan worden voor authenticatie bij alle relevante databronnen. Als dit afsprakenstelsel breed geïmplementeerd en gebruikt kan worden helpt dit draagvlak te creëren in het zorgveld.

- eIDAS hoog is mogelijk als instapniveau voor het groeimodel. Het is technisch haalbaar en er zijn middelen op de markt verkrijgbaar. Om te bepalen of dit ook voldoende breed beschikbaar is en of het aansluiten bij de behoeften van gebruikers, zijn pilots en demonstraties nodig.

- De middelen op eIDAS hoog zijn beschikbaar bij verschillende leveranciers, die in andere domeinen hebben laten zien dat het mogelijk is om op te schalen naar voldoende beschikbaarheid. Deze middelen worden getoetst door het Agentschap Telecom. Het wordt wel aangeraden om zo spoedig mogelijk een schaalbaarheidstest in het zorgdomein uit te voeren om dit te toetsen. Om vast te stellen of een directe transitie naar eIDAS hoog inderdaad haalbaar is.

- De schaalgrootte, de bijkomende risico’s en de tijdslijn van de transitie in aanmerking nemende adviseert TNO direct te beginnen met pilots.

- Het is cruciaal om draagvlak te creëren door middel van goede communicatie. Dit is essentieel om het menselijk gedrag om veiliger te werken te veranderen. Het advies is om ook de ICT-leveranciers te betrekken bij deze bewustwordingsfase.

- Demonstraties van verschillende middelen is essentieel. Zonder demonstratie van het concept is het risico aanwezig dat de pilot op gebruiksvriendelijkheid

wordt afgewezen. Zonder demonstratie/acceptatie zal er geen transitie plaatsvinden.

- Om nieuwe authenticatiemiddelen toe te kunnen laten tot het stelsel is het van belang het UZI-register los te koppelen van de UZI-pas en het register compleet te maken. TNO ziet een verandering in de rol van het CIBG. Het wordt registerbeheerder in plaats van leverancier van een authenticatiemiddel. Een consequentie van deze veranderende rol is dat er leveranciers van authenticatiemiddelen in het stelsel bijkomen.
- Door de veranderende rol van het CIBG, de introductie van andere authenticatiemiddelproviders en de toename van het aantal controles zal er meer afstemming en overleg nodig zijn (zei rollen hoofdstuk 4).
- Besturende, uitvoerende en toezichthoudende rollen zullen toebedeeld moeten worden specifiek voor de transitie en opschaling naar een operationeel stelsel (zie paragraaf 4.10). TNO adviseert dat VWS de taken verdeeld en de verantwoordelijke aanwijst en betaalt voor implementatie (transitiemanager).
- Het is essentieel om te blijven evalueren tijdens en na implementatie. Betrek hierbij de aangestelde adviesraad.
- Er is bekostiging nodig voor een nieuw systeem, zowel voor de transitie naar het nieuwe systeem als de instandhouding ervan.
- Door uitbreiding van het UZI-register zullen er veel meer individuele authenticatiediensten worden afgenomen. Hierdoor zullen de kosten aanzienlijk toenemen. Op dit moment bedragen de kosten die gemaakt worden in de zorg voor de aanschaf en toepassing van de UZI passen naar schatting 28mln/jaar (tabel 16). Een eerste inschatting voor toekomstige gebruikskosten geeft een range weer tussen de 7,5 en 60 mln per jaar voor eIDAS hoog, waarbij synergie effecten niet zijn meegerekend. Bestaande oplossingen zullen worden uit gefaseerd (binnen de pakketten), het is niet duidelijk wat deze kosten zijn, maar deze kosten zullen lager worden. De systeemkosten voor de uitgifte en beheer van UZI-passen en UZI-servercertificaten dalen naar verwachting licht van (afgerond) 13 miljoen naar circa 8 miljoen.
- Op dit moment laat de veiligheid in de zorgsector te wensen over, dit is een onacceptabel risico. Om voldoende keuzevrijheid en een betrouwbaar gecertificeerd middel aan te kunnen bieden zullen de kosten omhoog gaan. Hiermee zorg je wel dat iedere zorgprofessional een eIDAS hoog authenticatiemiddel gebruikt op persoonlijke titel. Dit zal verplicht moeten worden gesteld, om toch tot dit veiligheidsniveau te komen.

7 Beperkingen onderzoek

Kwalitatief onderzoek gaat gepaard met praktische en theoretische beperkingen. Vanwege de arbeidsintensiteit was het niet mogelijk om alle zorgsectoren te spreken, maar hebben we gezorgd voor een goede doorsnede in het soort gebruiker. Authenticatieniveaus zijn geschat op basis van de middelen. Het is een inschatting gemaakt van de middelen en het betrouwbaarheidsniveau op basis van interviewgesprekken en dit is verder niet geverifieerd. Zorgverleners hebben over het algemeen te weinig inzicht in het proces om dit te beoordelen.

Een tweede beperking is de beperkte beschikbaarheid van inzicht in huidige financiële kosten van inlogmiddelen als onderdeel van het gebruiksproces en het aandeel dat authenticatie en inlogmiddelen hiervan innemen. De toepassing van deze systemen en mogelijkheden voor synergie en substitutie konden niet worden achterhaald. Deze wens naar aanvullende inzicht in en de beperking in de reeds verzamelde gegevens kwam laat in het onderzoek naar voeren.

Ten aanzien van nieuwe te ontwikkelen diensten en businessmodellen bestaat nog veel onzekerheid. Die onzekerheid hangt samen met de invoering van de WDO en de afhankelijkheid van publieke inlogmiddelen die ook in de zorg gebruikt kunnen gaan worden en de effecten die dit heeft op private businessmodellen voor nieuwe dienstverleners. De aantrekkelijkheid van toetreding tot de zorgmarkt door private partijen is sterk afhankelijk van de invoering van de WDO en het risico dat private partijen hierdoor lopen.

8 Ondertekening

Leiden,

ValidSigned by Daan Kloet
on 2023-01-10 16:20:02

Daan Kloet
Research Manager
Microbiology & Systems Biology

TNO

ValidSigned by Jildau Bouwman
on 2023-01-12 09:07:42

Jildau Bouwman
Auteur

A Vragenlijst zorgverleners

Ten behoeve van de gesprekskwaliteit en de volledigheid kunnen er vragen in de lijst staan, waarop we het antwoord al denken te kennen. Deze vragenlijst wordt slechts als leidraad voor het gesprek gebruikt. Begrijpelijkheid en antwoord op de vragen is sterk afhankelijk van de persoon aan wie de vraag wordt gesteld (doelgroep).

Data in de werkomgeving

Technisch en gebruiksgemak

- Waar en hoe bewaren jullie digitale patiëntdata?
- Wat voor HIS/ZIS/... Gebruiken jullie?
- Valt deze informatie onder het medisch beroepsgeheim? Wisselen jullie gegevens uit met andere praktijken/ziekenhuizen/zorgverleners?
- Maken jullie gebruik van het Landelijk SchakelPunt (LSP) en andere uitwisselingssystemen voor de zorg? Hoe ervaren jullie zulke systemen?
- Hoe belangrijk is data-beveiliging in jullie werk? Kun je hier voorbeelden van geven?

Authenticatie in het algemeen

Technisch

- Welke authenticatiemiddelen en inlogmiddelen gebruiken jullie? (Voorbeelden: SMS / Token / Smartcard / Certificaat op smartphone / Biometrie / NFC-functionaliteit op smartphones / Authenticators / Yubikey / anders)
- Waarom gebruiken jullie deze?
- Wat voor authenticatiepassen gebruiken jullie? Weten jullie wat voor passen dit technisch zijn? Waarvoor worden de passen gebruikt? (Toegang tot werkplek/ruimte, gegevensuitwisseling, handtekeningen)
- Wordt er een wachtwoordbeleid gehanteerd? Wordt dit ook technisch afgedwongen?
- Kan er op andere locaties of thuis gewerkt worden? Verloopt de authenticatie dan anders?
- Hoe vaak moet je inloggen?
- Kennen jullie een formele dataclassificatie? Is de authenticatie anders voor verschillende classificatieniveaus?
- Kunnen jullie iets vertellen over de procedure waarmee deze authenticatiemiddelen uitgereikt worden?
- Gebruiken jullie mail- of chatapplicaties in jullie werk? Waar en hoe kunnen jullie hier toegang tot krijgen?

Gebruiksgemak

- Hoe ervaren jullie de authenticatie? Hoeveel tijd ben je ermee kwijt?
- Wat vind je van de authenticatiemiddelen die jullie gebruiken? Makkelijk/moeilijk in gebruik?
- Ervaren jullie weerstanden? In welk opzicht belemmert het jullie in het uitvoeren van jullie werkzaamheden?
- Loop je tegen technische problemen aan tijdens het gebruik?
- Wat zou er beter kunnen?

- Waarom is het niet beter?
- Hoe ziet voor jullie de optimale situatie eruit? Hoeveel tijd zou je eraan willen besteden?
- Gebruiken jullie wel eens andermans inlogmiddelen? Zijn er groepsaccounts? Denk je wel eens na over de gevolgen?
- Sta je open voor het gebruik van andere/betere authenticatie middelen?

De UZI-pas

Technisch

- Gebruiken jullie ook UZI-passen?
- Heeft iedereen een UZI-pas? Wie wel, wie niet? Waarom?
- Waarvoor gebruiken jullie de UZI-pas? (Toegang LSP, digitale handtekening, toegang registers; authenticatie en/of digitale ondertekening)

Gebruiksgemak

- Hoe ervaren jullie het gebruik van de UZI-pas? Makkelijk/moeilijk in gebruik? Loop je ergens tegenaan in het gebruik?
- Wat is er goed aan de UZI-pas?
- Wat zou er aan de UZI-pas mogen veranderen?
- Hebben jullie een idee waarom dat niet veranderd is?
- Zou je de UZI-pas aanbevelen aan anderen?
- Wordt er ook wel eens de UZI-pas van iemand anders gebruikt?

Doorvraag vragen:

- Kun je een voorbeeld geven van..
- Wat bedoel je met…
- Kun je dat toelichten..
- Waarom is dat zo belangrijk voor jou..
- Wat betekent dit voor jou..

B Vragenlijst leveranciers

Ten behoeve van de gesprekskwaliteit en de volledigheid kunnen er vragen in de lijst staan, waarop we het antwoord al denken te kennen. Deze vragenlijst wordt slechts als leidraad voor het gesprek gebruikt. Type vragen, begrijpelijkheid en antwoord op de vragen is sterk afhankelijk van de persoon aan wie de vraag wordt gesteld (doelgroep).

- Kunnen jullie kort uitleggen wat (naam leverancier) doet en hoe het werkt?
- Wat voor EPD's en andere producten levert (naam leverancier)?
- Wat zijn de grootste klantgroepen van (naam leverancier)?
- Is (naam leverancier) al actief in de zorg?
  - Op welke manier?
- Is (naam leverancier) al actief als authenticatiedienst?
  - Waar en hoe bevalt dat?
- Op welke manier zou (naam leverancier) als authenticatiedienst in de zorg kunnen werken?

<u>Data</u>

- Wordt er een formele dataclassificatie gehanteerd bij het ontwerpen van de software?
- Aan welke normen, certificeringen en andere kaders moet deze voldoen?

<u>Technisch</u>

- Beheren jullie de authenticatie in de software zelf of wordt hierbij gebruik gemaakt van externe partijen?
  - Van welke leveranciers maken jullie gebruik? Voor welke diensten?
- Welke authenticatiemiddelen en inlogmiddelen worden er gebruikt om toegang tot het EPD te verkrijgen?
  - (Voorbeelden: SMS / Token / Smartcard / Certificaat op smartphone / Biometrie / NFC-functionaliteit op smartphones / Authenticators / Yubikey / anders)
  - Waarom worden deze gebruikt?
- Wat voor authenticatiepassen worden gebruikt? Weten jullie wat voor chips dit technisch zijn?
- Wordt er een wachtwoordbeleid gehanteerd? Wordt dit ook technisch afgedwongen?
- Kan er op andere locaties of thuis gewerkt worden? Verloopt de authenticatie dan anders?
- Hebben jullie specifieke ontwikkelingen op authenticatiegebied op de agenda staan? Wat voor visie/hoop/ontwikkelingen zien jullie voor (naam leverancier)?
- Op wat voor betrouwbaarheidsniveau vindt de authenticatie van de zorgverleners naar het EPD plaats?
  - Hebben jullie hier een beeld van?
  - Waaraan zou deze moeten voldoen?
  - Proberen jullie hier ook invulling aan te geven?

Gebruiksgemak
- Hoe worden deze authenticatiemiddelen ervaren?
- Wat vindt men van de gebruikte authenticatiemiddelen?
- Wat zou er beter kunnen?
- Krijgen jullie verzoeken voor andere of betere authenticatie?
  - Wat voor trends zijn daarin zichtbaar?
- Ziet (naam leverancier) een spanningsveld tussen sterke authenticatie en werkbaarheid?
  - Hoe kan dat verholpen worden?
- Voelt (naam leverancier) zich verantwoordelijk voor de authenticatie en de daarmee samenhangende beveiliging van de data?

De UZI-middelen

Technisch
- Worden er ook UZI-middelen als authenticatiemiddel gebruikt in jullie software?
  - Waarvoor worden deze gebruikt?
- Kunnen jullie de certificaten koppelen met een ander register?
- Zou het mogelijk zijn om jullie authenticatiemiddelen te koppelen met het UZI-register?
- Zou toegang met iets anders dan een mobiele telefoon ook mogelijk zijn, zodat authenticatie in een steriele omgeving ook mogelijk is?

Gebruiksgemak
- Is het lastig om het gebruik van UZI-authenticatiemiddelen te faciliteren?
- Hoe worden deze door zorgverleners ervaren?
- Wat is er goed aan de UZI-middelen?
- Wat zou er beter kunnen?
  - Wat is er voor nodig om dit te bereiken?

Overige vragen
- Wat onderscheidt jullie van andere authenticatiemiddelen?
- Welke knelpunten zien jullie in het huidige landschap van authenticatiemiddelen?
- Zijn er voorbeelden van authenticatiediensten op niveau eIDAS-hoog die m.b.v. (naam leverancier) (of een alternatief daarvoor) werken?
- Hoe komen we in de zorg mogelijk naar een hoger betrouwbaarheidsniveau?
- Wat voor concessies moeten er mogelijk gedaan worden aan de werkbaarheid (om het betrouwbaarheidsniveau te verhogen)? Wat voor moeilijkheden voorziet (naam leverancier) bij het migreren naar een sterker authenticatieniveau?
  - Welke rol speelt (naam leverancier) hierbij?
- Hoe zou authenticatie met (naam leverancier) op niveau eIDAS hoog eruit zien?
  - Waar worden certificaten en sleutels bewaard?
  - Hoe krijgt de gebruiker daar toegang tot?
  - Wat zijn de belangrijkste veiligheidseisen?
- Is een cloudoplossing gevoeliger voor beschikbaarheidsproblemen?
  - Wat is jullie beschikbaarheid?
- Werken jullie alleen in Nederland of ook Europees/wereldwijd?
  - Hoe groot is de markt voor zulke authenticatieoplossingen en hoeveel concurrenten zijn er?

- Is de omgeving geschikt en gecertificeerd om asymmetrische sleutelparen veilig op te slaan?
  - Zo nee, zien jullie ontwikkelingen in deze richting?
- Wat is jullie huidige capaciteit (in personen / sleutelparen / certificaten)?
- Welke capaciteit verwachten jullie over een jaar te hebben?
- Welke capaciteit zouden jullie over een jaar kunnen hebben?
- Wat gaat sterkere authenticatie kosten?

C Studiepopulatie

Tabel 1. Type en aantal respondenten

Type respondent	Aantal
Zorgverleners	**N**
Apothekers	1
Artsen*	4
Diëtisten	2
Fysiotherapeuten	3
GZ-psychologen	1
Tandartsen	2
Verloskundigen	1
Verpleegkundige/ thuiszorg	2
GGD	1
Totaal zorgverleners	**17**
Leveranciers	
Elektronisch patiëntendossier (EPD)	3
Stichting met meerdere EPD leveranciers	1
Digitale communicatie platform	1
Authenticatieleverancier	2
Identificatie en authenticatie middel	1
Vereniging zorgaanbieders in ICT	1
UZI-middelen	1
Totaal leveranciers	**10**
Totaal aantal respondenten	**27**

* Huisarts, interne geneeskunde, klinisch geriater, neuroloog

Tabel 2. Authenticatiematrix zorgverleners, deel 1.

	Dienst 1	Inlogmiddelen	Betrouwbaarheids niveau	Dienst 2	Inlogmiddelen	Betrouwbaarheids niveau	Dienst 3	Inlogmiddelen	Betrouwbaarheids niveau	Dienst 4	Inlogmiddelen	Betrouwbaarheids niveau	Gebruik UZI	Waarvoor
Fysiotherapeut 1	EPD (Intramed)	wachtwoord	Laag	Extern werken	Wachtwoord + RSA-token	Substantieel	E-Mail	Wachtwoord	Laag				Nee	
Fysiotherapeut 2	EPD (Intramed)	IP-adres + wachtwoord + UZI-certificaat	Laag	Zorgmail	Wachtwoord + Authenticator	Substantieel	Siilo	Pincode + toestelbinding	Substantieel				Ja, UZI certificaat	Ophalen van NAW gegevens
Fysiotherapeut 3	EPD (incura)	wachtwoord + smartphone	Substantieel	Zorgmail	Wachtwoord + Authenticator	Substantieel	Fysiologic	Wachtwoord + smartphone	Laag / Substantieel	EPD (IntraMed)	wachtwoord	Laag	Nee	
Ex-Neuroloog	Citrix	wachtwoord + sms smartphone	Laag / Substantieel	Zorgdomein	Wachtwoord + sms telefoon	Laag / Substantieel	Medimo	Wachtwoord + smartphone	Laag / Substantieel	Wetransfer	Geen	-	Ja, wel gebruikt totdat systeem crashte	Ophalen medicatie gegevens van patienten
Huisarts	EPD (Medicom)	wachtwoord	Laag	EPD op huisartsenpost	UZI-pas + pincode	Hoog							Nee	

Tabel 2. Authenticatiematrix zorgverleners, vervolg.

	Dienst 1	Inlogmiddelen	Betrouwbaarheidsniveau	Dienst 2	Inlogmiddelen	Betrouwbaarheidsniveau	Dienst 3	Inlogmiddelen	Betrouwbaarheidsniveau	Dienst 4	Inlogmiddelen	Betrouwbaarheidsniveau	Gebruik UZI	Waarvoor
Arts ouderenzorg	EPD (Mijncaress)	wachtwoord	Laag	Axioncontinu (Thuiswerkomgeving)	wachtwoord + sms telefoon	Laag / Substantieel	Medimo	Token + gebruikersnaam zonder wachtwoord	Laag	ANWNederland	wachtwoord + sms	Laag / Substantieel	Nee	Toegang tot LSP
Diëtist 1	EPD (Intramed)	wachtwoord	Laag	Zorgmail	wachtwoord + sms	Laag / Substantieel	Sorgente (drinkvoeding)	wachtwoord + sms	Laag / Substantieel	VIPlive/ calculus (met hierin een chatfunctie)	wachtwoord + sms	Laag / Substantieel	Nee	Toegang Vecozo
Diëtist 2	Portavita	wachtwoord + authenticator smartphone	Substantieel	Zorgmail	wachtwoord+ sms telefoon	Laag / Substantieel	Siilio	Smartphone (vingerafdruk)	Substantieel				Ja, UZI pas	Ophalen van patientgegevens, toegang tot Vecozo
Arts interne geneeskunde	EPD (Epic)	pas + pincode of persneelsnummer + wachtwoord	Laag / Substantieel	Mail + extra beveiligingsknop (extra mail met pincode om het te openen)	Wachtwoord	Laag	Fax / CDs	geen	Laag				Nee	
GGD	Citrix	Wachtwoord + sms code via authenitcator generator	substantieel	Identity Hub (CoronaIT)	wachtwoord + federale active directory die bij lokale GGD valideert	Onbekend							Ja	LSP/SBV-Z

Tabel 2. Authenticatiematrix zorgverleners, vervolg.

Apotheker	Farmacon	wachtwoord + gebruikersnaam of UZI pas	Laag (Hoog als UZI, maar vaak niet toegepast)	Zorgmail	wachtwoord	Laag	Medimo (verpleegtehuis)	wachtwoord + sms telefoon of token	Laag / Substantieel	Siillo	pincode	Substantieel	Vecozo	wachtwoord - authenticator
Thuiszorg	Puurvanjou	wachtwoord + RSA-token	Substantieel	Mail	Via PuurVanJou	Substantieel	Point	wachtwoord	Laag	Medicheck	wachtwoord + sms	Laag / Substantieel	Whatsapp	Pincode
Thuiszorg	Nedap op PC	wachtwoord + sms-code/email-code	Laag / Substantieel	Nedap op telefoon/ tablet	pincode	Substantieel	Beveiligde mail	direct via werkomgeving Nedap	Laag	OZOverbind zorg	wachtwoord + sms	Laag / substantieel	MCA-app (Boomer web)	wachtwoord + sms-code
GGZ psycholoog	Intramed	wachtwoord	Laag	Qurentis	wachtwoord	Laag	Carefriend	wachtwoord	Laag	Outlook mail	beveiligd versturen knop, client krijgt mail met link voor code	laag / Substantieel	Embloom	wachtwoord + authenticator
Tandarts 1	EPD (exquise)	wachtwoord (praktijk 1)	Laag	wachtwoord	Zorgmail naar zorgmail niks. zorgmail onbekende ontvanger; indien tel gekoppeld sms indien mail gekoppeld wachtwoord code via mail	Laag	EPD (exquise)	Groepsaccount (praktijk 2)	Geen	Chatfunctie binnen EPD/exquise	zie EPD			
Tandarts 2	Citrix (thuis)	Gebruikersnaam + wachtwoord + code telefoon	substantieel	Citrix (praktijk)	gebruikersnaam +wachtwoord	Laag	Vecozoo	certificaat (persoonlijk)	substieel/ hoog?	LSP	UZI-pas	hoog	Zorgmail	wachtwoord + sms-code
Verbos-kundige	Orpheus	Wachtwoord	Laag	Zorgdomein	Wachtwoord	Laag	Zivver-mail	wachtwoord + sms	Substantieel	Siilo	Pincode + telefoon koppeling	substantieel		

Tabel 3. Authenticatiematrix leveranciers en experts.

	Zorgveld	Dienst	Inlogmiddelen	Betrouwbaarheidsniveau	Prioriteit	Koppeling met andere diensten
Leverancier 1	Paramedisch	EPD	Wachtwoord en authenticator	Substantieel	Gebruiksvriendelijkheid	Zivver, Zorgmail, Zorgdomein
Leverancier 2	Ziekenhuizen	EPD	Meerdere opties (wachtwoord, mobiele app, pasjes, otp-token / UZI-pas)	Laag/Substantieel/Hoog	Gebruiksvriendelijkheid en flexibileit	O.a. authenticatiediensten
Leverancier 3	Ziekenhuizen	EPD	Meerdere opties (wachtwoord, mobiele app, pasjes, otp-token / UZI-pas)	Laag/Substantieel/Hoog	Gebruiksvriendelijkheid en flexibiliteit	O.a. authenticatiediensten
Leverancier 4	CIBG: Zorgbreed	UZI-middelen	UZI-pas / Servercertificaat	Hoog	Regelconform	Diverse
Leverancier 5	Zorgbreed	Digitale communicatie platform	Telefoon + pincode	Substantieel	Privacy en gebruiksgemak	Diverse
Leverancier 6	Zorgbreed	Identificatie en authenticatie middel	Multi step als ondergrens: wachtwoord + sms/authenticator app	Laag/substantieel	Privacy en gebruiksgemak	Diverse
Leverancier 7	Zorgbreed	Stichting met meerdere EPD leveranciers	Diverse	Substantieel	Gebruiksvriendelijkheid en privacy	Diverse
Leverancier 8	Niet actief in de zorgsector	authenticatieleverancier	Signing certificaat, uitgegeven a.d.h.v. een digitale fysieke verschijning	Hoog	Gebruiksvriendelijkheid en privacy	Diverse
Leverancier 9	Zorgbreed (Vereniging)	Vereniging zorgaanbieders in ICT	Telefoon (NFC chip)	Laag/substantieel	Gebruiksvriendelijkheid	Diverse
Leverancier 10	Niet actief in de zorgsector	authenticatieleverancier	Private key op een apparaat + with biometrisch of pincode	Substantieel/Hoog	Privacy en security	Diverse

D Rollen in de huidige situatie

Hieronder worden een aantal partijen uitgelicht die momenteel een rol vervullen binnen het huidige stelsel.

- **VWS:** is het aanspreekpunt voor de AP en wordt beschouwd als de aanjager en facilitator voor het beheer en onderhoud van het stelsel.
- **CIBG:** beheert het UZI-register en BIG-register en geeft de UZI-pas uit, waardoor zij tevens de rol van ICT-leverancier aanneemt.
- **Leveranciers:** hier verstaan wij zowel leverancier van hier verstaan wij zowel leverancier van authenticatiemiddelen als softwareleveranciers onder. Zij nemen de verantwoordelijkheid voor het leveren van producten met gevraagde normen. Ze krijgen ook de gelegenheid om mee te denken over de normen, echter gebeurt dit onvoldoende volgens de NEN-commissie. NEN: *"Op dit moment ontbreekt het vooral aan voldoende participatie van leveranciers."*
- **Zorgprofessional/-aanbieder:** zijn verantwoordelijk voor de kwaliteit van authenticatie en ICT-inkoop. Zij financieren op het moment de authenticatiekosten.
- **AP en IGJ:** bewaakt de naleving van de regelgeving en verwijzen daarbij naar de standaarden.
- **Zorgverzekeraars:** financieren de middelen voor bepaalde beroepsgroepen.