Trust service & Identity proofing practice statement

Voor ”AMP Groep persoonsidentificatie via de app”

Datum document: 26-01-2024

Datum effectief: 29-01-2024

Inhoudsopgave

1 Introductie

Dit document is de Trust Service Practice Statement (TSPS) en Identity Proofing Practice Statement van de AMP Groep persoonsidentificatie dienstverlening via de AMP Groep identificatie app. Het is geen volledige Certification Practice Statement (CPS) omdat de identificatie app alleen betrekking heeft op de aspecten van de identiteitsvaststelling voor het kunnen afgeven van gekwalificeerde certificaten en AMP Groep biedt geen andere certificeringsdiensten aan.

Het doel van dit document is om als basis te dienen voor de naleving van de eIDAS Verordening (EU) nr. 910/2014 en de ETSI-normen ETSI TS 119 461 , ETSI EN 319 401, ETSI EN 319 411-2.

De genoemde eIDAS-verordening definieert identiteitsvaststelling niet als een vertrouwensdienst op zich. In dit document wordt identiteitsvaststelling gedefinieerd als een subset van de Trust Service Component "Registratiedienst" zoals gedefinieerd in de ETSI-norm ETSI EN 319411-2. Het servicecomponent kan een integraal onderdeel zijn van de dienstverlening van de Trust Service Provider (TSP), maar kan ook de taak zijn van een Identity Proofing Service Provider (IPSP).

1.1 Overzicht

Identiteitsvaststelling is het proces waarbij met de vereiste mate van zekerheid wordt geverifieerd dat de identiteit van een aanvrager correct is. AMP Groep heeft een dienst ontwikkeld voor identificatie op afstand (AMP Groep persoonsidentificatie via de app), voor het bewijzen van de identiteit van natuurlijke personen die met vertrouwensdiensten te maken hebben, alsook voor andere doeleinden, zoals de afgifte van elektronische identiteiten, onboarding en "know your customers"-processen (KYC).

Voor de uitvoering van de methode Persoonsidentificatie via de app gebruiken wij de diensten van twee leveranciers/subverwerkers:

Inverid is de leverancier van de ReadID SDK (software development kit), die deel uit maakt van de AMP Groep identificatie app. Binnen de SDK maakt AMP Groep gebruikt van verschillende functionaliteiten. Hieronder de voornaamste functionaliteiten van de ReadID SDK.

- Scannen VIZ (Visual Inspection Zone), scant het ID-document en/of leest de MRZ (Machine Readable Zone). Dit is de sleutel om de NFC (Near field communication) chip te openen.
- Uitlezen en verifiëren van NFC chip. ReadID leest de attributen uit welke aanwezig zijn in de NFC chip en verifieert deze.
- Starten en begeleiding iProov SDK

iProov is de leverancier van Inverid rondom gezichtsverificatie (facial matching) en liveness detectie. iProov maakt gebruik van de foto uit de NFC chip om de Gebruiker

te matchen middels biometrische technieken. Indien het niet mogelijk is om de foto uit de NFC chip te gebruiken en de optische orkestratie is toegestaan dan zal de foto van Gebruiker uitgesneden worden na de VIZ scan om dezelfde vergelijking toe te passen.

AMP Groep verifieert de identiteit van natuurlijke personen in overeenstemming met eIDAS, artikel 24, lid 1, onder d), door gebruik te maken van "andere identificatiemethoden" die een gelijkwaardige zekerheid bieden op het gebied van betrouwbaarheid als fysieke aanwezigheid.

InverID en iProov bieden als leverancier hun eigen eIDAS (Electronic Identities And Trust Services) certificering voor vertrouwensdiensten, uitgegeven door TUV Austria.

1.2 Scope

Dit document (de 'AMP Groep Trust Service & Identity proofing Practice Statement') beschrijft de toegepaste werkwijzen die worden ingezet bij de online identiteitsvaststellingsdienstverlening. Specifiek de werkwijzen die zijn toegepast om te voldoen aan de algemene eisen uit ETSI TS 119 461 en beschrijft de beleids- en beveiligingsvereisten die zijn vastgesteld voor de uitvoering van een "Identity Proofing Service Component" ter ondersteuning van identiteitsvaststelling binnen de Europese regelgeving. Daarbij is rekening gehouden met de volgende aspecten:

- Het is gebaseerd op ETSI EN 319 401, dat gemeenschappelijke vereisten bevat voor alle verleners van vertrouwensdiensten die ’best practices ‘ toepassen voor het gebruik van geselecteerde middelen en toepasselijke technologieën die kan worden gebruikt voor identiteitsvaststelling.

- Het bevat specifieke eisen voor de verificatie van de identiteit van natuurlijke personen.

  De beveiligingseisen van ETSI TS 119 461 hebben betrekking op de meest voorkomende risico's, die vallen onder twee hoofdcategorieën: een aanvrager claimt ten onrechte een identiteit met behulp van vervalste bewijsmiddelen (vervalst bewijs) en een aanvrager maakt gebruik van geldige bewijsmiddelen die verband houden met een andere persoon (impersonatie).

Samenvattend:

- ETSI TS 119 461 v1.1.1 (2021-07): Electronic Signatures and Infrastructures (ESI); Beleid en beveiligingseisen voor onderdelen van vertrouwensdiensten die de identiteit van betrokkenen van vertrouwensdiensten bewijzen voor de identificatiemethode: "AMP Groep persoonsidentificatie via de app", die onbemande identiteitsvaststelling op afstand verschaft (namelijk door middel van de AMP Groep identificatie app), waarbij de communicatie met de aanvrager en de afhandeling geautomatiseerd is (eveneens via de app en de achterliggende systemen).

- Gedeeltelijke certificering van de methode "AMP Groep persoonsidentificatie via de app" volgens ETSI EN 319 411-2 (Registratieservice).

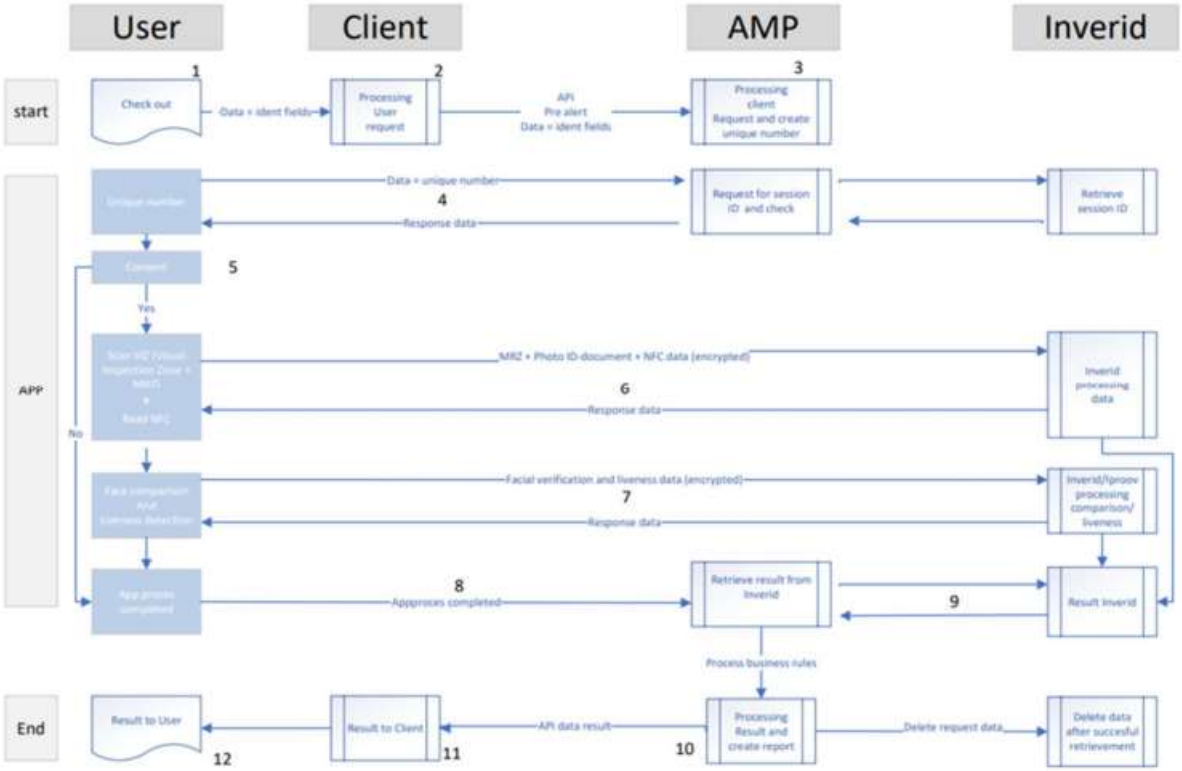
- Bevestiging van gelijkwaardige zekerheid als fysieke aanwezigheid, overeenkomstig Verordening (EU) 910/2014 (eIDAS) art. 24, lid 1, sub d, van de identificatiemethode: "AMP Groep persoonsidentificatie via de app" op basis van beoordeling aan de hand van de toepasselijke eisen van ETSI TS 119 461.

1.3 Identiteitsvaststelling proces

De Methode "AMP Groep persoonsidentificatie via de app" voldoet aan de volgende vereisten voor identiteitsvaststelling, zoals gespecificeerd in ETSI TS 119 461, Hoofdstuk 8:

- 8.1 (initiatie)
- 8.2 (attributen and bewijslast verzamelen)
- 8.3 (attributen and bewijslast validatie)
- 8.4 (binding aan de aanvrager)
- 8.5 (afgifte van bewijs)

Proces:



Stappen	Omschrijving
1	Verzoek Gebruiker aan Opdrachtgever om product/dienst af te nemen, waarbij identificatie noodzakelijk is.
2	Opdrachtgever stuurt verzoek tot identificatie via Restful API naar AMP server.
3	AMP verwerkt het verzoek en creëert een uniek eenmalig online identificatie nummer.
4	Indien online identificatie nummer wordt gebruikt, wordt een unieke sessie gestart binnen de ReadID SDK in de AMP Groep identificatie app.
5	Gebruiker dient akkoord te gaan met het verwerken van persoonlijke data en biometrische gegevens. Indien, gebruiker niet met beide akkoord gaat stopt het online identificatie proces. Het is niet mogelijk om op een later moment alsnog het proces te starten.
6	ReadID SDK communiceert via een beveiligde verbinding direct met de InverID server.
7	iProov (onderdeel van de ReadID SDK) communiceert direct met de InverID server. Alleen de pasfoto wordt gedeeld om deze stap uit te voeren.
8	Op het moment dat alle stappen zijn doorlopen en consent is gegeven, stuurt de app een signaal naar de server van AMP Groep.
9	AMP Groep ontvangt de data van Inverid. Na succesvol ophalen wordt direct een verwijderverzoek ingediend om de data te verwijderen op de server van Inverid.
10	AMP Groep verwerkt de business rules welke zijn overeengekomen met Opdrachtgever.
11	AMP Groep deelt data en resultaat business rules met Opdrachtgever.
12	Gebruiker ontvangt eindresultaat identificatie van Opdrachtgever.

1.4 Identiteitsvaststelling context

De context van identiteitsvaststelling is de reeks externe omstandigheden die het kader bepalen waaraan een identiteitsvaststellingsproces is onderworpen en die eisen en beperkingen kunnen opleggen aan identiteitsvaststelling. Een kernonderdeel van de context van identiteitsvaststelling zijn de wettelijke vereisten die zijn opgelegd aan identiteitsvaststelling voor het gedefinieerde doel door de van toepassing zijnde wetgeving. AMP Groep opdrachtgevers zijn verantwoordelijk voor het waarborgen van naleving van wet en regelgeving volgens hun beoogde context voor identiteitsvaststelling. Het identiteitsvaststellingskader van de persoonsidentificatie via de app zal variëren tussen doelen van identiteitsvaststelling met betrekking tot:

- Het vereiste zekerheidsniveau
- De identiteitskenmerken die moeten worden verzameld, wat betekent dat Attributen verplicht, verboden of optioneel kunnen zijn (bijv. is er wel of geen grondslag voor het verwerken van het Burgerservicenummer)
- De land specifieke nationale wetgeving en overheidsbeleid inzake toepasselijke technologieën (bijvoorbeeld bepaalde identiteitsdocumenten zoals nationale identiteitskaarten uit geselecteerde landen kunnen beperkt zijn; in sommige landen kan validatie van identiteitskenmerken tegen een nationaal bevolkingsregister verplicht zijn, terwijl andere landen geen dergelijke registers hebben; de middelen om te gebruiken voor kenmerk- en bewijsvalidatie en voor binding aan de aanvrager, wat betekent dat bepaalde processtappen verplicht of verboden kunnen zijn; in sommige landen kan fysieke aanwezigheid verplicht zijn voor bepaalde doeleinden van identiteitsvaststelling, of kan externe identiteitsvaststelling beperkt zijn om alleen specifieke gebruiksdoelen toe te staan. Wat betreft bedreigingen voor het verzamelen en valideren van Attributen en bewijzen, zijn de volgende ‘best

practices' van toepassing op ''AMP Groep persoonsidentificatie via de app'': Afhankelijk van de context van de identiteitsvaststelling worden alleen paspoorten, nationale identiteitskaarten, vreemdelingendocumenten en rijbewijzen geaccepteerd omdat in die documenten verzamelde Attributen de persoon uniek identificeren

2 Administratief beleid

2.1 Organisatie

AMP Groep is een logistieke dienstverlener gevestigd in Houten. AMP Groep biedt bezorg- en identificatiedienstverlening aan. Onze opdrachtgevers bestaat uit grotere bedrijven en organisaties zoals de overheid, telecom, finance en farma industrie in Nederland.

2.2 Contactgegevens

AMP Groep
Pakketboot 57
3991 CH Houten
info@ampgroep.nl
www.ampgroep.nl
KvK-nummer 30161122

2.3 Tijd en frequentie van publicatie

De laatste versie van deze Trust service & Identity proofing practice statement is goedgekeurd door het management en staat gepubliceerd op de AMP Groep website.

Dit document wordt periodiek herzien en bijgewerkt in overeenstemming met het AMP Groep-beleid. Goedkeuring en bespreking van de huidige scope vindt jaarlijks plaats, vergelijkbaar met ISO-onderhoud en procedures voor her-certificering.

2.4 Voorwaarden

Deze Trust service & Identity proofing practice statement treedt in werking vanaf de datum van publicatie op de website. Wijzigingen worden van kracht op het moment van publicatie. Deze Trust service & Identity proofing practice statement blijft van kracht totdat deze wordt vervangen door een nieuwe versie.

Toepasselijke algemene voorwaarden voor opdrachtgevers m.b.t. de identiteitsvaststelling op afstand zijn vastgelegd binnen de contracten dan wel de dienstenbeschrijvingen.

3 Definities en afkortingen

3.1 Definities

Definities	Omschrijving
Identificatie app	De app waarmee de identiteitsvaststellingdienstverlening wordt geleverd.
(eind)gebruiker	De natuurlijke persoon die geïdentificeerd wordt.
Opdrachtgever	Het bedrijf die ons de opdracht geeft om de identificatie uit te voeren en waarmee deze dienst contactueel is vastgelegd.
Leverancier	Onderaannemer binnen het identificatieproces die onder de verantwoordelijkheid van AMP Groep vallen.
Attributen	De kenmerken toegewezen aan een persoon die worden uitgelezen vanaf de chip.

3.2 Afkortingen

Afkortingen	Omschrijving
TSPS	Trust service practice statement
IPPS	Identity proofing practice statement
eIDAS	Electronic Identification and Trust Services
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
SOC2	Service Organization Control
BIV	Beschikbaarheid, Integriteit, Vertrouwelijkheid
ICAO	International Civil Aviation Organization
MRZ	Machine Readable Zone
PKI	Public Key Infrastructure
GPA	Genuine Presence Assurance
KvK	Kamer van Koophandel
FAR	False acceptance Rate
FRR	False Rejection Rate

ETSI EN 319 401 (PKI component service: Registration Service)

4 Risicoanalyse

AMP Groep hanteert de methode: risico = kans x impact

Voor het bepalen van de impact worden de volgende aspecten beoordeeld:

- Informatiebeveiliging (BIV)
- Financieel
- Reputatie
- Juridisch
- Kwaliteit

Het risicobeheerproces zorgt voor een op risico's gebaseerde aanpak in alle delen van de organisatie en maakt het mogelijk dat het managementsysteem gebaseerd is op factoren die als relevant zijn geïdentificeerd voor het succes ervan. Op basis hiervan voert AMP Groep jaarlijkse risicoanalyses uit en maakt het ook standaard onderdeel uit van het (ICT) wijzigingenbeheerproces.

5 Interne organisatie

Voor het kwaliteitsmanagementsysteem is AMP groep ISO9001 gecertificeerd.

Voor Informatiebeveiliging is AMP Groep ISO27001 gecertificeerd. De implementatie van het ISO27001 raamwerk zorgt ervoor dat we informatiebeveiliging borgen binnen onze processen, we continue verbeteringen doorvoeren en jaarlijks beoordeeld worden door een onafhankelijke certificerende instantie (BSI Group The Netherlands B.V). De werking van de informatiebeveiligingsmaatregelen wordt jaarlijks gecontroleerd en beoordeeld in een SOC2 type II rapport.

6 Beleid

AMP Groep identificatie app voldoet aan de eIDAS eisen voor identiteitsvaststelling en is gecertificeerd door BSI Group The Netherlands B.V tegen:

- eIDAS Regulation 910/2014
- ETSI EN 319411-2 (Trust Service Component: Registration Service)
- ETSI TS 119 461 voor identiteitsvaststelling van natuurlijke personen (op afstand)

AMP groep hanteert een ‘zero tolerance’ beleid voor discriminatie, seksueel overschrijdend gedrag en pesten, zoals vastgelegd en gecommuniceerd binnen de huisregels.

AMP Groep medewerkers worden jaarlijks getraind op de onderwerpen als informatiebeveiliging en privacy.

De financiële en organisatorische betrouwbaarheid van AMP Groep kan worden bevestigd via openbaar beschikbare jaarverslagen.

Er zijn beleidsregels voor leveranciersbeheer, inkoop, uitbesteding en contractuele relaties geïmplementeerd.

7 HR beveiliging

Het HR indiensttredingsproces van AMP Groep zorgt ervoor dat we mensen aannemen (en als dat van toepassing is, ook onderaannemers) die de juiste expertise, betrouwbaarheid, ervaring en kwalificaties hebben.

Bij AMP Groep volgt iedere medewerkers jaarlijks verplicht een informatiebeveiliging en privacy training.

Iedere medewerker binnen AMP Groep krijgt bij indiensttreding d.m.v. de huisregels de Vertrouwensrol toegewezen. Daarnaast zijn specifieke rollen toegewezen aan gekwalificeerde medewerkers zoals o.a., systeembeheerder, security operator, security officer, functionaris gegevensbescherming.

Bij het toewijzen van rollen en verantwoordelijkheden wordt rekening gehouden met scheiden van taken om conflicterende taken te voorkomen.

Middelen die worden uitgegeven worden bij uitdiensttreding weer ingenomen en rechten worden ontnomen. Voor deze ex-medewerkers blijft de geheimhoudingplicht gelden.

8 Beheer van bedrijfsmiddelen

AMP Groep heeft een beleid voor het beheer van zijn bedrijfsmiddelen. Dit omvat het beheer van software- en hardware, inclusief de hardware in het datacenter. Er wordt een volledige inventaris bijgehouden van alle belangrijke bedrijfsmiddelen. Elk bedrijfsmiddel wordt geclassificeerd en beschermd op basis van de uitgevoerde impactanalyse. De identificatie app is niet geclassificeerd als een "kritieke service".

9 Toegangsbeheer

AMP Groep heeft een toegangsbeleid. Een gebruiker dient enkel toegang te hebben tot systemen of fysieke locaties op basis van de noodzaak vanuit zijn of haar functie (need-to-know/need-to-use principe). De rol van de persoon bepaalt de toegang tot informatie en middelen. Toegang tot informatie en middelen wordt verstrekt/ingetrokken als onderdeel van het in- en uitdienst proces van HR. Logische toegangsrechten worden ieder kwartaal beoordeeld door de systeemeigenaar. Naast het toegepaste wachtwoordbeleid wordt 2FA (Twee Factor Authenticatie) gebruikt voor systemen die vertrouwelijke informatie bevatten, zoals vastgelegd binnen het classificatieschema. Logische toegangslogs worden bewaard en kunnen niet worden gemanipuleerd.

10 Cryptografische beheersmaatregelen

HTTPS (Hypertext Transfer Protocol Secure) en TLS (Transport Layer Security) zijn toegepast binnen het gehele proces van voormelden van data vanuit de opdrachtgever, identificatiedienstverlening via de app en het weer aanleveren van de bewijslast terug aan de opdrachtgever.

11 Fysieke beveiliging

Het pand van AMP Groep en het datacenter voldoen aan de hoogste beveiligingseisen en maatregelen. Dit betekent dat er adequate toegangscontroles, bescherming tegen externe en milieu-bedreigingen, bekabelingsbeveiliging en onderhoud van apparatuur zijn geïmplementeerd.

12 Operationele beveiliging

AMP Groep heeft processen ingericht voor het behandelen van incidenten en het uitvoeren van wijzigingen die voldoen aan de ISO27001 standaard. Het wijzigingenbeheerproces is een gecontroleerd proces waarbij afhankelijk van het risico of proces goedkeuring door directie of security officer wordt toegepast.

Ontwikkelings-, test- en operationele omgevingen zijn gescheiden. Ontwikkelaars volgen ons Veilig ontwikkelen beleid. Het twee paar ogen principe wordt door het systeem afgedwongen voordat we nieuwe ontwikkelingen/wijzigingen op productie live kunnen zetten.

Patches worden minimaal maandelijks en gecontroleerd uitgevoerd. Actuele dreigingen krijgen we automatisch binnen vanuit het Nationaal Cyber Security Centrum.

13 Netwerk beveiliging

De infrastructuur van AMP groep wordt beschermd door firewalls en 24/7 gemonitord. Maandelijks worden kwetsbaarhedenscans uitgevoerd en waar nodig actie op ondernomen. Publiekelijk toegankelijke systemen worden jaarlijks gepentest en mogelijke bevindingen daaruit adequaat opgevolgd. Virusscanning en hardening zijn toegepast om de kans op malware te mitigeren.

14 Incident management

Het Incidentenbeheerproces van AMP Groep omvat elk incident dat een dienstverlening verstoort, of zou kunnen verstoren. Het belangrijkste doel van incidentenbeheerproces is om de normale werking van de dienstverlening zo snel mogelijk te herstellen en de nadelige impact op de bedrijfsactiviteiten te minimaliseren, waardoor wordt gewaarborgd dat de overeengekomen niveaus van servicelevels worden gehandhaafd.

Elke kritieke eIDAS-beveiligingsinbreuk wordt zo snel mogelijk gemeld aan de desbetreffende opdrachtgever voor verdere melding aan de relevante nationale toezichthoudende instantie (bijv. Rijksdienst Digitale Infrastructuur). AMP Groep meldt binnen 4 uur aan de opdrachtgever, zodat de eis van binnen 24 uur melden aan

de toezichthoudende instantie gerealiseerd kan worden. Voor het melden van het incident wordt het eIDAS incidentmelding formulier gebruikt.

15 Bedrijfscontinuïteit

AMP Groep heeft een bedrijfscontinuïteitsplan opgesteld om bij ernstige calamiteiten adequaat herstelwerkzaamheden uit te kunnen voeren. Vanuit de bedrijfs-impactanalyse zijn de kritische systemen en middelen in kaart gebracht en zijn maatregelen geïmplementeerd om de kans op uitval te minimaliseren. De maximaal toegestane uitvaltijd bij een ernstige calamiteit is door de directie vastgesteld op 5 werkdagen. Jaarlijks worden meerdere bedrijfscontinuïteitstesten uitgevoerd om vast te stellen dat we ons vastgestelde beleid waar kunnen maken.

16 Beëindigingsplan

AMP Groep heeft een beëindigingsplan opgesteld dat wordt uitgevoerd als AMP Groep de dienstverlening beëindigt. Doel van het beëindigingsplan is om op een ordelijke manier de dienst over te kunnen dragen, inclusief communicatie naar de entiteiten, in samenwerking met de opdrachtgever.

ETSI TS 119 461 (Hoofdstuk 8/Hoofdstuk 9, toepasselijke vereisten)

17 Eisen voor identiteitsvaststellingsdiensten

17.1 Initiatie

De Gebruiker krijgt het privacy bericht getoond voor de start van het identificatieproces in de online identificatie app van AMP Groep. De Gebruiker dient zowel akkoord te gaan met het verwerken van persoonlijke data als het verwerken van biometrische data. Ook wordt er verwezen naar de privacy verklaring van onze opdrachtgever. De Gebruiker dient akkoord te gaan om het identificatieproces te kunnen starten. Gaat de Gebruiker niet akkoord of is de identificatie via de app niet succesvol, dan is een alternatief proces ‘’Persoonsidentificatie fysiek op locatie’’ mogelijk indien dit proces is afgestemd met de opdrachtgever.

17.2 Verzamelen van attributen en bewijslast

De AMP Groep identificatie app is onderdeel van de AMP online identificatie dienstverlening. Afhankelijk van de identiteitsvaststelling context worden de datagroepen binnen het identiteitsbewijs uitgelezen. Dit is afhankelijk van de overeengekomen afspraken met Opdrachtgever. Daarnaast toetst AMP Groep of de Opdrachtgever voldoende grondslag heeft om alle of een deel van de Attributen terug te ontvangen. Indien het niet noodzakelijk is om het BSN te verwerken zal dit ook niet gedaan worden, echter zit in veel Nederlandse identiteitsbewijzen het BSN verwerkt in de MRZ. In dit geval wordt het BSN alleen gebruikt om de NFC te openen en wordt

het BSN op geen enkele server opgeslagen tijdens het proces, ook niet bij onze leverancier InverID.

17.3 Verzamelen attributen van natuurlijke personen

NFC technologie wordt gebruikt voor het lezen en verifiëren van de chip van het identiteitsdocument dat overeenkomt met ICAO Doc 9303. Dit geldt voor elektronische paspoorten, identiteitskaarten en verblijfskaarten. Ook is hierin vastgesteld of datagroepen verplicht of optioneel zijn. Nederland is een van de weinige landen met een elektronisch rijbewijs, het Nederlands rijbewijs voldoet aan ISO18013. Onderstaande attributen worden verzameld. Het type attribuut geeft aan dat een uitgevende instantie verplicht of optioneel een attribuut kan/moet toevoegen in de NFC chip.

Attribuut	Omschrijving	Type attribuut
Chip Clone detectie	Resultaat van de chip clone detectie	Verplicht
Chip verificatie	Status van de chip verificatie	Verplicht
Geboortedatum	Geboortedatum documenthouder	Verplicht
Datum geldig tot	Datum tot document geldig us	Verplicht
Documentnummer	Unieke documentnummer	Verplicht
Documentcode	Type document (bv. Paspoort)	Verplicht
Land van uitgifte	De code van land van uitgifte	Verplicht
Naam documenthouder	Naam van documenthouder	Verplicht
Voornamen	Voornamen documenthouder	Verplicht
Achternaam	Achternaam documenthouder	Verplicht
Persoonlijk nummer (BSN)	Uniek persoonlijk nummer	Optioneel*
Geboorteplaats	Geboorteplaats documenthouder	Optioneel*
Foto documenthouder	Pasfoto van de documenthouder	Verplicht
Biometrische liveness data	Biometrische data voor vaststellen documenthouder, zoals video en foto	Verplicht

* Indien hier grondslag voor is, dit wordt altijd afgestemd met de Opdrachtgever

17.4 Validatie van attributen en bewijslast

De identiteitsdata wordt optisch verkregen via de MRZ (Machine Readable Zone) middels OCR (Optical Character Recognition) technologie. De MRZ bevat onder andere de achternaam, voornamen en geboortedatum van de gebruiker. In een Nederlands paspoort of identiteitskaart die is uitgegeven tot 30 augustus 2021 staat

het BSN nummer ook in de MRZ code en in de NFC chip. Is het een Nederlands paspoort of identiteitskaart dat op of na 30 augustus 2021 is uitgegeven, dan heeft het paspoort of identiteitskaart een QR-code waarin het BSN staat. Deze QR-code staat op de achterkant van de ID-kaart of op de achterkant van de houderpagina (de pagina met de pasfoto) van het paspoort.

Middels de MRZ wordt de chip gelezen middels NFC (Near Field Communication) technologie. De informatie op de chip wordt geleverd door het uitgevende land van het identiteitsbewijs. De data wordt op deze manier elektronisch en betrouwbaar uitgelezen, hierdoor zijn geen handmatige handelingen vereist.

Na het tot stand brengen van een verbinding vinden de volgende fasen plaats bij het NFC-lezen:

Toegangscontrole: Dit is een beveiligingsmechanisme van de chip om de privacy van de documenthouder te verbeteren. Specifiek voorkomt het skimmen omdat je een toegangsbewijs nodig hebt om toegang te krijgen tot de chipinhoud. Het voorkomt ook afluisteren door het opzetten van een beveiligd versleuteld communicatiekanaal dat wordt gebruikt voor de rest van het proces. De beveiligingsoverwegingen voor de cryptografische protocollen die in deze fase worden gebruikt, vallen buiten het bereik van dit whitepaper. In plaats daarvan is er een blogpost beschikbaar.

Uitlezen van chipinhoud: De chip bestaat uit verschillende bestanden (of datagroepen) die kunnen worden uitgelezen. Sommige bestanden bevatten informatie over de documenthouder, zoals een bestand met de MRZ en een met een

gezichtsafbeelding, terwijl andere cryptografische informatie bevatten voor verificatie.

Protocollen voor kloondetectie worden uitgevoerd door een willekeurige ‘challenge’ naar de chip te sturen en een ‘response’ terug te ontvangen.

De verificatie van paspoortgegevens wordt uitgevoerd door de hashes van verschillende datagroepen uit de chip te valideren, een digitale handtekening over deze hashes te valideren die in het paspoort zijn gelezen, en te controleren tegen een lijst van vertrouwde landcertificaten: een masterlijst. Dit mechanisme wordt passieve authenticatie genoemd. Een succesvolle verificatie betekent dat de gelezen gegevens authentiek zijn. Daarnaast verifieert de server voor kloondetectie de challenge-respons en chip-authenticatie als deze van de gebruiker zijn ontvangen. Verificatie van een challenge-respons gebeurt tegen een door passieve authenticatie beveiligde openbare sleutel. De meeste, maar niet alle identiteitsdocumenten ondersteunen kloondetectie, vooral oudere documenten hebben dit soms niet.

17.5 Gebruik van digitale identiteit als bewijslast

Aan de hand van de ReadID SDK worden digitale identiteitsdocumenten uitgelezen. De AMP Groep identificatie app accepteert ICAO-compliant identiteitsbewijzen (paspoorten, identiteitskaarten en verblijfsvergunningen). Nederlandse rijbewijzen voldoen aan ISO18013. De Opdrachtgever bepaalt of het Nederlands rijbewijs wordt toegestaan.

17.6 Validatie van digitale identiteitsbewijs

Naast het uitlezen van documenten, valideert ReadID of ze voldoen aan de ICAO 9303-standaarden. ReadID heeft hiervoor verschillende certificeringen (https://www.inverid.com/certifications), waaronder de eIDAS-module voor assurance op niveau hoog.

ReadID ondersteunt identiteitsdocumenten die voldoen aan ICAO 9303, met inbegrip van:

- Het Basic Access Control-beveiligingsmechanisme voor toegang tot de chip.
- Het Passieve Authenticatie-beveiligingsmechanisme voor het verifiëren van de authenticiteit van de gelezen gegevens.
- Het Actieve Authenticatie-beveiligingsmechanisme voor het verifiëren van de authenticiteit van de chip, zoals kloondetectie.
- Het chipauthenticatiebeveiligingsmechanisme (EAC-CA) voor kloondetectie.
- Het lezen en interpreteren van DG1 met de MRZ-informatie, DG2 met het gezichtsbeeld, D7 met de geschreven handtekening (indien aanwezig), DG11 met aanvullende persoonlijke informatie (indien aanwezig) en DG12 met aanvullende documentinformatie (indien aanwezig).
- Password Authenticated Connection Establishment (PACE), een opvolger van BAC die gebruikmaakt van modernere cryptografie om een hoger beveiligingsniveau te bieden. Merk op dat de EU de implementatie van PACE door haar lidstaten voor nieuw uitgegeven reisdocumenten vereist. Paspoorten die PACE ondersteunen, ondersteunen ook BAC om compatibel te blijven met de ICAO 9303-standaard, die vereist dat documenten die PACE ondersteunen ook het oudere BAC ondersteunen.

Deze beveiligingsfuncties zijn enkel van toepassing op de ondersteunde digitale identiteitsdocumenten en niet op bijvoorbeeld attestatie of aanvullende gezaghebbende bronnen. Gegevens in doorvoer en in rust worden versleuteld met het standaard TLS-protocol, en er zijn functies voor gegevensintegriteit om de integriteit van opgeslagen gegevens te waarborgen.

17.7 Binden van gebruiker

Naast de functionaliteit voor het verifiëren van identiteitsgegevens en documenten voert de AMP Groep Identificatie app ook verificatie uit van de houder van het identiteitsdocument. Hiermee wordt aangetoond dat de aanvrager van het identiteitsdocument daadwerkelijk de rechtmatige eigenaar van het document is.

De AMP Groep Identificatie app vergelijkt de hoge-resolutie afbeelding van het ID-document uit de NFC chip met GPA (Genuine Presence Assurance) van iProov.
Wat is GPA van iProov?
Het vaststellen van de daadwerkelijke aanwezigheid van een persoon op afstand is van essentieel belang om ervoor te zorgen dat alleen legitieme personen toegang krijgen tot systemen, terwijl fraudeurs en criminelen worden tegengehouden. Het is van groot belang om op een veilige manier te verifiëren dat de gebruiker die zich via hun persoonlijke apparaat authentiseert, daadwerkelijk aanwezig is, zonder blootstelling aan vervalsing of digitale aanvallen.

17.8 Vastleggen van gezichtsfoto van de gebruiker

iProov Echte Aanwezigheidsborging (Genuine Presence Assurance)
Echte Aanwezigheidsborging (GPA) beperkt risico's die voortkomen uit een volledig scala aan aanvallen, waaronder digitale injectie, en is de meest veilige antispoof-technologie. GPA maakt gebruik van een eenmalige biometrische gegevensverstrekking via Flashmark-technologie, die gecontroleerde verlichting gebruikt om te waarborgen dat de persoon die toegang krijgt tot uw systeem de juiste persoon is, een echte persoon is en op dit moment authentiseert. Authentiseren met GPA is een moeiteloze en passieve ervaring, waarbij geen gebruikersacties worden vereist.

17.9 Automatische gezichtsbiometrie

Voor elk resultaat vanuit iProov wordt een binaire score (true/false) teruggeven als resultaat. Periodiek doet iProov testen om de FAR (False acceptance Rate) en FRR (False Rejection Rate) te toetsen en te vergelijken met marktstandaarden.

17.10 Uitgeven bewijslast

Eindgebruikersinformatie wordt teruggegeven via een unieke identificatiecode aan Opdrachtgevers van AMP Groep. Via de koppeling halen Opdrachtgevers de eindgebruikersinformatie op.

Afhankelijk van de context kunnen Opdrachtgevers zowel een PDF downloaden, inclusief afbeelding, als de rauwe data. Configuratieparameters zijn beschikbaar in sectie 19.3 (Geautomatiseerde werking) in dit document.

17.11 Bewijslast van het identiteitsvaststellingsproces

Alle gegevens die zijn uitgelezen van de NFC-chip, inclusief de hoogwaardige foto, hebben een retentieperiode van 21 dagen. Screenshot verzameld tijdens de videoselfie, om te bewijzen dat een persoon een echt mens is, is 14 dagen geldig voor de Opdrachtgever. De gegevens worden opgeslagen in hun oorspronkelijke vorm, bijvoorbeeld ze worden niet gedecodeerd, gedecodeerd of omgezet naar een ander formaat. Tevens wordt ook een leesbare pdf ter beschikking gesteld voor de opdrachtgever. De database is beschermd om de integriteit te waarborgen en alleen geautoriseerd personeel heeft toegang om de database te lezen.

Gegevens worden verwijderd na 14 dagen, in overeenstemming met het gedefinieerde retentiebeleid. Het is vervolgens aan Opdrachtgever om zijn eigen retentie/archiveringsbeleid te implementeren.

De leverancier iProov, voor de stap gezichtsverificatie, heeft afwijkende bewaartermijnen. iProov ontvangt vanuit de ReadID server alleen de pasfoto, geen andere persoonlijke data. Na de gezichtsverificatie wordt een biometrische template 30 dagen bewaard, in het geval van fraude vermoedens is dit langer. De biometrische template kan nooit worden herleid tot de originele foto.

18 Identiteitsvaststelling ‘use cases’

AMP Groep identificatie app voldoet aan de volgende gebruiksscenario zoals gespecificeerd in ETSI TS 119 461:

‘Unattended remote identity proofing’ 9.2.3

Daaruit volgen de procesmaatregelen vanuit hoofdstuk 8:

- 8.1 (initiatie)
- 8.2 (attributen and bewijslast verzamelen)
- 8.3 (attributen and bewijslast validatie)
- 8.4 (binding aan de aanvrager)
- 8.5 (afgifte van bewijs).

18.1 Identiteitsvaststelling van natuurlijke personen

De methode AMP Groep persoonsidentificatie via de app vereist niet:

- fysieke aanwezigheid
- online communicatie met een medewerker

Het identiteitsvaststellingsproces is niet hybride, maar volledig digitaal en geautomatiseerd:

18.2 Identiteitsvaststelling op afstand

De aanvrager ontvangt geautomatiseerde begeleiding gedurende het identiteitsvaststellingsproces. Toegankelijkheid van de AMP Groep identificatie app is alleen mogelijk op het Android en iOS platform. AMP Groep identificatie app biedt zowel in-app tekstuele ondersteuning aan de eindgebruiker (reden voor mislukking/opnieuw proberen), terwijl een lijst met foutcodes naar Opdrachtgever

wordt gestuurd. Een tweedelijns ondersteuning wordt geboden aan de Opdrachtgevers.

Het identificatievaststellingsproces in de AMP Groep identificatie app is gebruiksvriendelijk, intuïtief en kan volledig worden uitgevoerd in minder dan twee minuten. De eindgebruiker voert een unieke identificatiecode in, accepteert de voorwaarden van de opdrachtgever over verwerking van persoonlijke data en biometrische gegevens in de AMP Groep identificatie app, scant digitaal de machine-leesbare zone (MRZ) van het geselecteerde document, controleert de chip via near-field communication (NFC) en voert gezichtsherkenning uit. Succesvolle verificatie is afhankelijk van het voldoen aan de met opdrachtgever overeengekomen business rules. Opdrachtgever kan flexibel beslissen over de volgende stappen:

- Mislukte authenticatie: wel of niet opnieuw proberen (of anders - als fraude wordt gedetecteerd)
- Mislukte authenticatie naar identificatie op locatie (alleen mogelijk in Nederland)
- Geslaagde authenticatie: felicitatiebericht en volgende stappen (bijv. KYC-vragenlijst/eindgebruiker-zelfbeoordeling).

18.3 Geautomatiseerde werking

De methode AMP Groep Persoonsidentificatie via de app voldoet aan ‘Use case’ 9.2.3.4 ‘Automated operation’
zoals gespecificeerd in ETSI TS 119461 Hoofdstuk 8:

- 8.3.2 (validatie van digitaal identiteitsdocument)
- 8.4.3 (binding aan de aanvrager door geautomatiseerde gezichtsbiometrie)