Trust service & Identity proofing practice statement

Voor ”AMP Groep persoonsidentificatie via de app en fysiek op locatie”

Datum document : 15-08-2025

Datum effectief : 01-09-2025

Versie 1.2

Inhoudsopgave

Documenthistorie 3
1 Introductie 4
1.1 Overzicht 4
1.2 Scope 6
1.3 Persoonsidentificatie proces 8
1.4 Identiteitsvaststelling context 13
2 Administratief beleid 14
2.1 Organisatie 14
2.2 Contactgegevens 14
2.3 Tijd en frequentie van publicatie 14
2.4 Voorwaarden 15
2.5 Review & verantwoordelijkheden 15
3 Definities en afkortingen 16
3.1 Definities 16
3.2 Afkortingen 17
4 Risicoanalyse 18
5 Interne organisatie 19
6 Beleid 20
7 HR beveiliging 21
8 Beheer van bedrijfsmiddelen 22
9 Toegangsbeheer 22
10 Cryptografische beheersmaatregelen 23
11 Fysieke beveiliging 23
12 Operationele beveiliging 23
13 Netwerk beveiliging 24
14 Incident management 24
15 Bedrijfscontinuïteit 25
16 Beëindigingsplan 25
17 ETSI TS 119 461 Eisen voor identiteitsvaststellingsdiensten 26
17.1 Identiteitsvaststelling via de app 27

17.2 Identiteitsvaststelling fysiek op locatie 30

Documenthistorie

Versie	Datum	Wijzigingen	Auteur/Verantwoordelijke
1.2	26-08-2025	- Nieuwe paragraaf **2.5 Review & Responsibilities** toegevoegd. - Versiebeheer toegevoegd. - Diverse ETSI-eisen verwerkt in de relevante hoofdstukken.	Melvin van Alem – IT Manager Andy Alen – Compliance Manager
1.1	16-01-2025	Proces **identificatie op locatie** toegevoegd (17.2). - Proces **identificatie op afstand** herschreven (17.1, korter en bondiger).	Melvin van Alem – IT Manager Andy Alen – Compliance Manager Eric Gloudemans – Product Owner IoA
1.0	28-10-2024	Eerste versie	Frank Koning

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 en fysiek op locatie. Het is geen volledige Certification Practice Statement (CPS) omdat de dienstverlening 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 toepasselijke ETSI-normen vanuit ETSI TS 119 461 , ETSI EN 319 401, ETSI EN 319 411-2.

1.1 Overzicht

Persoonsidentificatie 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 persoonsidentificatie op afstand via de app en fysiek op locatie voor het bewijzen van de identiteit van natuurlijke personen die met vertrouwensdiensten te maken hebben.

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.

Voor de uitvoering van de methode **Persoonsidentificatie op locatie** gebruiken wij één IT -leverancier: Oribi ID solutions. De Oribi applicatie(SDK) controleert het getoonde fysieke identiteitsbewijs op echtheid.
Hieronder de voornaamste functionaliteiten van de Oribi applicatie.

- 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. De Oribi applicatie leest de attributen uit welke aanwezig zijn in de NFC chip en verifieert deze.

Gegevens worden vervolgens door AMP verwerkt en overgedragen aan de opdrachtgevers (verwerkersverantwoordelijken). De Oribi applicatie is een hulpmiddel voor onze getrainde identiteitsvaststelling medewerkers, die ook zonder dit hulpmiddel in staat zijn om veilige en vertrouwde identiteitsvaststelling uit te voeren.

1.2 Scope

Dit document (de 'AMP Groep Trust Service & Identity proofing Practice Statement') beschrijft de toegepaste werkwijzen, beleid en veiligheidsmaatregelen die worden ingezet bij de identiteitsvaststellingsdienstverlening voor zowel op afstand via de app als fysiek op locatie.

Specifiek de werkwijzen en maatregelen die zijn toegepast om te voldoen aan de toepasselijke eisen vanuit de Europese regelgeving.

eIDAS Verordening (EU) nr. 910/2014

De verordening stelt eisen aan vertrouwensdienstverleners, zoals aanbieders van elektronische handtekeningen en certificaten voor website-authenticatie. Deze diensten moeten voldoen aan strenge beveiligings- en betrouwbaarheidseisen. AMP groep bevestigd een gelijkwaardige zekerheid voor identiteitsvaststelling via de app als bij de fysieke identificatie op locatie, overeenkomstig art. 24, ~~lid~~paragraaf 1a, sub d.

De eIDAS-verordening definieert identiteitsvaststelling niet als een vertrouwensdienst op zich. In dit document wordt identiteitsvaststelling gedefinieerd als een subset van de Trust Service Componenten "Registration and Subject device provision service". Het service component 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).

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 kunnen worden gebruikt voor identiteitsvaststelling.

ETSI TS 119 461

Beleid en beveiligingseisen voor onderdelen van vertrouwensdiensten die de identiteit van betrokkenen van vertrouwensdiensten bewijzen. Het bevat specifieke eisen voor de verificatie van de identiteit van natuurlijke personen. De eisen hebben

betrekking op de meest voorkomende risico's die vallen onder twee hoofdcategorieën:
Een aanvrager claimt ten onrechte een identiteit met behulp van een vervalst identiteitsbewijs.
Een aanvrager maakt gebruik van een geldig identiteitsbewijs, maar die is van een ander persoon.

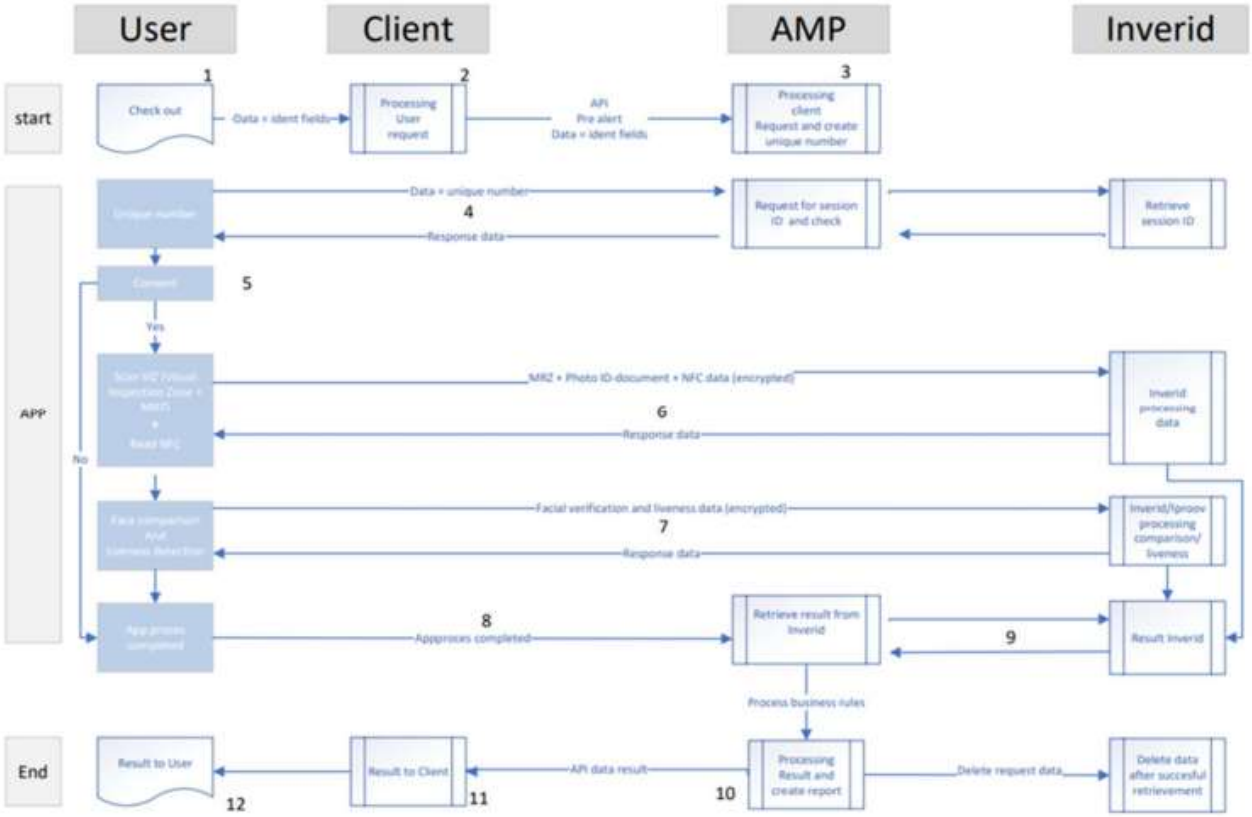
ETSI EN 319 411-2

De norm stelt eisen aan vertrouwensdienstverleners die gekwalificeerde certificaten uitgeven. AMP groep is hierin voor zijn deel verantwoordelijk. Daarom een gedeeltelijke certificering voor de: Registration and subject device provision service.

1.3 Persoonsidentificatie proces

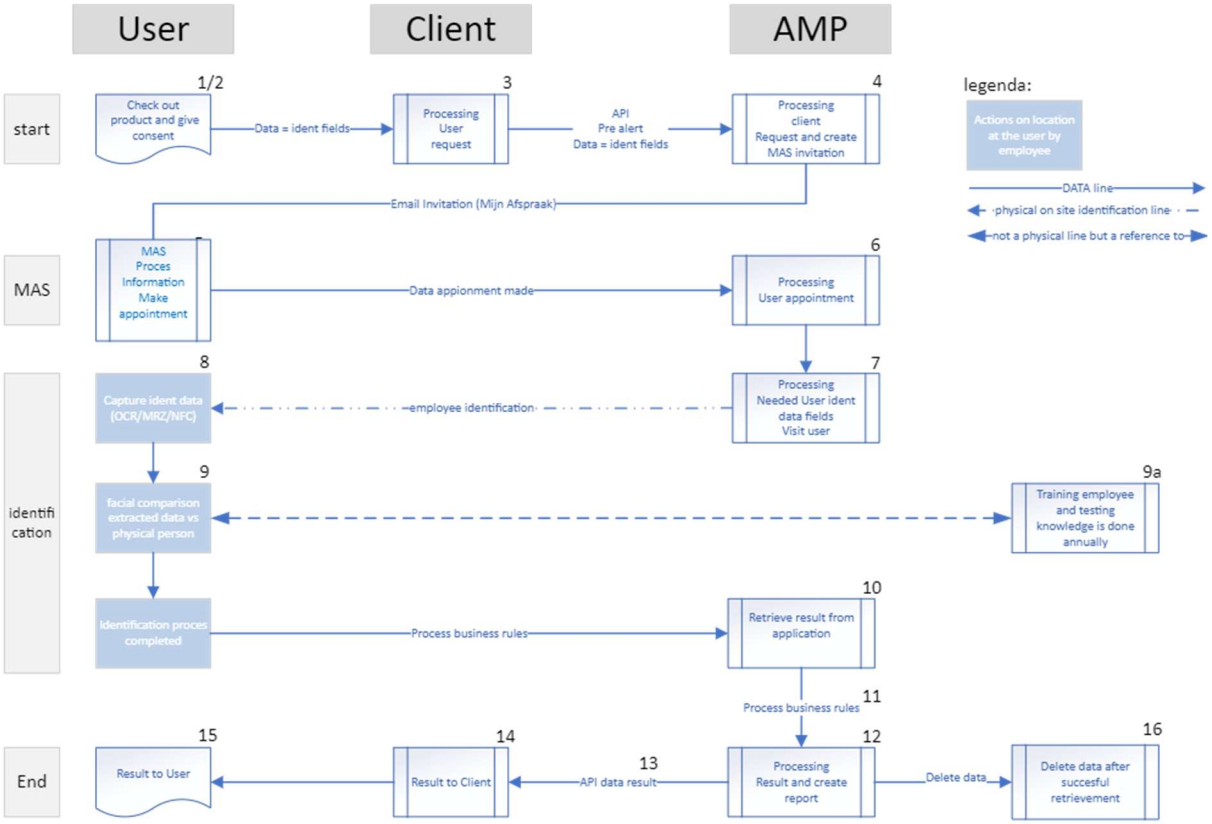
1.3.1 via de app

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 identificatienummer.
4	Indien het identificatienummer 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 identificatieproces. 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 het succesvol ophalen wordt direct een verwijderverzoek ingediend om de data te verwijderen op de server van Inverid.
10	AMP Groep verwerkt de data volgens de business rules welke zijn overeengekomen met Opdrachtgever.
11	AMP Groep deelt de data en resultaat business rules met Opdrachtgever.
12	Gebruiker ontvangt eindresultaat identificatie van Opdrachtgever.

1.3.2 op locatie



Stappen	Omschrijving
1	Verzoek Gebruiker aan Opdrachtgever om product/dienst af te nemen, waarbij identificatie noodzakelijk is.
2	Gebruiker geeft aan de Opdrachtgever akkoord voor het doel en de uitvoering van het proces.
3	Opdrachtgever stuurt verzoek tot identificatie via beveiligde verbinding naar AMP server.
4	AMP verwerkt het verzoek en stuurt de klant een uitnodiging om een afspraak via Mijnafspraak.nl (MAS) te maken voor de identificatie op locatie.
5	Op MAS wordt de Gebruiker geïnformeerd over de belangrijkste voorwaarden voor een succesvolle afhandeling, zoals welke ID-bewijzen worden toegestaan.
6	Gebruiker maakt afspraak voor identificatie op locatie
7	Per proces kan worden ingesteld welke van deze gegevens daadwerkelijk worden verzameld. ID-gegevens die niet nodig zijn voor de identificatie worden niet overgenomen en welke ID-bewijzen worden geaccepteerd Identificatie - Tijdens de fysieke identificatie kunnen de volgende gegevens worden verzameld: Pasfoto, BSN-nummer, nationaliteit, voornamen/voorletters, achternaam, geboortedatum, geboorteplaats, geslacht, documenttype, documentnummer, land v uitgifte, uitgiftedatum, uitgifte instantie, geldigheidsdatum, handtekening, kopie ID-bewijs.
8	Gegevens worden verzameld door het uitlezen van het ID-bewijs middels OCR/ MRZ en/of NFC m.b.v. Oribi software.
9	De identificatiemedewerkers voeren op locatie een gezichtsvergelijking uit a.d.h.v. de foto op het getoonde ID en de Gebruiker. Hiervoor dient de Gebruiker persoonlijk aanwezig te zijn. De identificatiemedewerker krijgt voldoende tijd om de Gebruiker te identificeren.
9a	De identificatiemedewerkers worden getraind om zorgvuldig identificaties uit te kunnen voeren. De training bestaat uit; Technische identificatie (herkennen van echtheidskenmerken van ID-documenten en falsificaten), Tactische identificatie (opvallend gedrag van personen) en Profiling (controle van gezichtskenmerken zoals de vorm van het gezicht, de stand en vorm van de oren, neus en ogen). Jaarlijks wordt de kennis van de identificatiemedewerkers getoetst.
10	Op het moment dat alle stappen succesvol zijn doorlopen, stuurt Mobile Delivery (MD) een signaal naar de server van AMP Groep.
11	AMP Groep verwerkt de business rules welke zijn overeengekomen met Opdrachtgever.

12	Identificatie (succesvol) dan wordt het rapport aangemaakt en de orderdata opgeslagen In het rapport staan de verzamelde ID-gegevens, zoals benoemd in punt 7/ 10 en de datum en tijd waarop de identificatie heeft plaats gevonden en het resultaat van de echtheidscontroles van het ID-bewijs.
13	De data en het rapport wordt via een beveiligde verbinding overgedragen.
14	AMP Groep deelt data en resultaat identificatie met Opdrachtgever.
15	Gebruiker ontvangt eindresultaat identificatie van Opdrachtgever.
16	De verzamelde ID-gegevens worden maximaal 21 dagen bewaard (14 dagen in de database en 7 dagen in de back-up van de database). Op verzoek van de opdrachtgever kan dit eerder worden verwijderd.

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 en op locatie 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). Wat betreft bedreigingen voor het verzamelen en valideren van Attributen en bewijzen, zijn de volgende ‘best practices’ van toepassing: 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 zijn 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.

2.5 Review & verantwoordelijkheden

Het TS&IPPS wordt minimaal één keer per jaar herzien, of eerder indien wet- en regelgeving, interne processen of technologie daar aanleiding toe geven.

- **Product Owner (PO)**
  - Draagt zorg voor de dagelijkse uitvoering en inhoudelijke input.
  - Verzamelt input van betrokken afdelingen en bereidt voorstellen tot wijziging voor.
- **IT Manager**
  - Is eigenaar van dit document en verantwoordelijk voor de inhoud, actualiteit en het initiëren van de review.
  - Coördineert de bijdrage van de Product Owner en andere stakeholders.
- **Compliance Manager**
  - Toetst of het reviewproces conform interne procedures en externe regelgeving wordt uitgevoerd.
  - Registreert de goedgekeurde versie en borgt de bewijslast voor interne en externe audits.
- **Directie**
  - Accordeert de definitieve versie.
  - Draagt de formele eindverantwoordelijkheid richting toezichthouders en opdrachtgevers.

Alle versies worden voorzien van een versienummer, publicatiedatum en akkoordverklaring door de directie.

3 Definities en afkortingen

3.1 Definities

Definities	Omschrijving
Attributen	De kenmerken toegewezen aan een persoon die worden uitgelezen vanaf de chip.
(eind)Gebruiker	De natuurlijke persoon die geïdentificeerd wordt.
Identificatie app	De app waarmee de identiteitsvaststellingdienstverlening wordt geleverd.
Identificatiemedewerker	Medewerker die namens AMP Groep de identificatie op locatie uitvoert
Leverancier	Onderaannemer binnen het identificatieproces die onder de verantwoordelijkheid van AMP Groep vallen.
Mijnafspraak.nl (MAS)	De website waar de eindgebruiker een afspraak voor identificatie in kan plannen
Mobile Delivery (MD)	Combinatie van software en hardware (tablet) waarmee de identificatiemedewerker op een veilige en gestructureerde manier de identificatie kan uitvoeren.
Opdrachtgever	Het bedrijf die ons de opdracht geeft om de identificatie uit te voeren en waarmee deze dienst contactueel is vastgelegd.
Oribi	Software partner

3.2 Afkortingen

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

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. Binnen de verklaring van toepasselijkheid zijn geen maatregelen niet van toepassing verklaard. 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 identiteitsvaststellingsdienstverlening voldoet aan de eIDAS eisen voor identiteitsvaststelling en is gecertificeerd door BSI Group The Netherlands B.V tegen de toepasselijke eisen.

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

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

Er zijn beleidsregels geïmplementeerd voor o.a.: informatiebeveiliging, privacy, kwaliteit, sociaal en duurzaam ondernemen, HR, leveranciers, IT, bedrijfscontinuïteit, fysieke beveiliging, wijzigingen, toegangsrechten

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, kwaliteitsmanager, 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

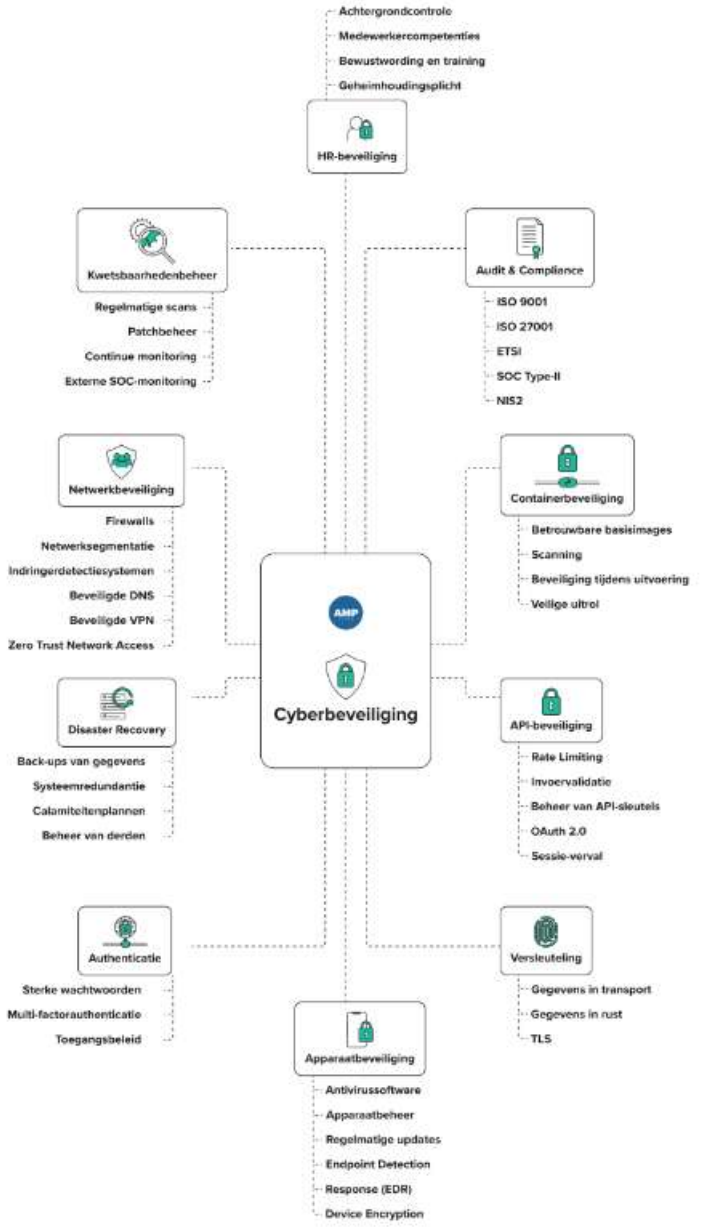
AMP Groep heeft processen ingericht voor het behandelen van incidenten en het uitvoeren van wijzigingen die voldoen aan de ISO27001 standaard. Het wijzigingenbeheerproces is een gecontroleerd proces waarbij afhankelijk van het risico of proces goedkeuring door directie of kwaliteitsmanager wordt toegepast.

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.

17 ETSI TS 119 461 Eisen voor identiteitsvaststellingsdiensten

(Hoofdstuk 8/Hoofdstuk 9, toepasselijke vereisten)

AMP Groep voldoet aan de eisen vanuit de 'use cases' :

- **Unattended remote identity proofing' 9.2.3**
- **Manual Operation 9.2.1.2**
- **Hybrid manual and automated operation 9.2.1.3**

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).

17.1 Identiteitsvaststelling via de app

De methode voor digitale identiteitsvaststelling via de AMP Groep identificatie app is volledig geautomatiseerd en vereist geen fysieke aanwezigheid of contact met een medewerker. Het proces voldoet aan de vereisten van Automated Operation (9.2.3.4).

17.1.1 Initiatie

1. Informatievoorziening:

- De Gebruiker ontvangt via de Opdrachtgever duidelijke informatie over het proces, de voorwaarden en het doel van de identiteitsvaststelling. Deze communicatie bevat de toegestane ID-bewijzen, het doel van het proces en de manier van uitvoering.
- De Gebruiker ontvangt na aanmelding bij AMP een uitnodiging per mail (en evt sms) voor het uitvoeren van de persoonsidentificatie.

2. Toestemming:

De Gebruiker start de identificatie door akkoord te gaan met het verwerken van persoonlijke en biometrische gegevens en het AMP-persoonsidentificatie proces zoals beschreven in dit document. Zonder toestemming stopt het proces automatisch.

3. Verzoekindiening:

De Opdrachtgever stuurt een identificatieverzoek naar de AMP-server via een RESTful API. AMP genereert een uniek identificatienummer en deelt dit met de Gebruiker.

17.1.2 attributen en bewijslast verzamelen

1. Gegevensverzameling:

De Gebruiker voert het identificatienummer in de app in, accepteert de voorwaarden en scant het identiteitsdocument met ReadID SDK. Dit omvat NFC, MRZ en optische controles.

2. Beperking van gegevens:

Alleen de noodzakelijke gegevens worden verzameld op basis van afspraken met de Opdrachtgever, zoals naam, geboortedatum, documentnummer, en pasfoto. Het BSN wordt alleen tijdelijk gebruikt voor NFC-verificatie en niet opgeslagen.

3. Toegestane ID-bewijzen:

Alleen ICAO-compliant identiteitsbewijzen worden geaccepteerd (paspoorten, ID-kaarten en Nederlandse rijbewijzen conform ISO18013).

17.1.3 Attributen en bewijslast validatie

1. Automatische controles:

De ReadID SDK valideert de echtheid van het ID-document via ICAO 9303-standaarden en voert passieve en actieve authenticatie uit. Gegevens worden via een beveiligde verbinding uitgelezen en gecontroleerd. Details over wat wordt gecontroleerd is per opdrachtgever vastgelegd en afgestemd in de zogeheten business rules.

2. Gezichtsverificatie:

De app gebruikt iProov Genuine Presence Assurance (GPA) om de pasfoto te vergelijken met de gebruiker en te garanderen dat deze authentiek is.

17.1.4 Binding aan de aanvrager

1. Gezichtsvergelijking:

Het gezicht van de gebruiker wordt automatisch vergeleken met de pasfoto op de NFC-chip. GPA-technologie minimaliseert risico's op fraude of spoofing.

2. Beveiliging:

Alle biometrische data worden tijdelijk verwerkt en opgeslagen volgens strikte beveiligings- en privacy protocollen.

https://www.iproov.com/wp-content/uploads/2025/03/2024.-MASTER_TSPSiProov-GPA-Liveness-TSPS-Trust-Services-Practice-Statement-v.2.4-_-eIDAS_eID_001.docx-1.pdf

17.1.5 Afgifte van bewijs

1. Rapportage:

Na succesvolle identificatie worden de verzamelde gegevens en resultaten verwerkt en gedeeld met de Opdrachtgever.

2. Veilige overdracht:

Gegevens worden via een beveiligde verbinding overgedragen. AMP Groep verwijdert de data direct na succesvolle overdracht.

3. Opslag en bewaartermijnen:

Gegevens worden maximaal 21 dagen bewaard:

i. 14 dagen in de actieve database.

ii. 7 dagen in de back-up

De Opdrachtgever kan aanvullende retentie- en archiveringsregels toepassen.

Onze gezichtsvergelijking leverancier iProov hanteert afwijkende bewaartermijnen voor niet succesvolle identificaties. Deze bewaartermijnen worden vooraf met onze opdrachtgevers afgestemd.

4. Bijzonderheden i.v.m. de Opdrachtgever:

De Opdrachtgever is verantwoordelijk voor verdere verwerking, zoals eigen archivering of retentiebeleid.

17.2 Identiteitsvaststelling fysiek op locatie

De methode voor identiteitsvaststelling fysiek op locatie door AMP Groep combineert fysieke aanwezigheid met hybride handmatige en geautomatiseerde processen. Dit voldoet aan de vereisten van Manual Operation (9.2.1.2) en Hybrid Manual and Automated Operation (9.2.1.3).

17.2.1 Initiatie

1. **Informatievoorziening**:
    - De Gebruiker ontvangt via de Opdrachtgever duidelijke informatie over het identificatieproces en de voorwaarden. Deze communicatie bevat de toegestane ID-bewijzen, het doel van het proces en de manier van uitvoering.
    - De Gebruiker ontvangt na aanmelding bij AMP een uitnodiging om een afspraak te maken via **Mijnafspraak.nl (MAS)**, waar eveneens de privacyvoorwaarden worden gedeeld.
2. **Toestemming en melding**:
    - De Gebruiker geeft toestemming aan de Opdrachtgever voor het gebruik van persoonlijke en biometrische gegevens.
3. **Verzoekindiening:**
    - De Opdrachtgever stuurt een identificatieverzoek naar de AMP-server via een beveiligde verbinding.

17.2.2 Attributen en bewijslast verzamelen

1. **Gegevensverzameling**:
    - Tijdens de fysieke identificatie worden gegevens verzameld zoals pasfoto, BSN-nummer, nationaliteit, naam, geboortedatum, geboorteplaats, geslacht, documentnummer, uitgifteland en -datum, en de handtekening.
    - Uitlezen gebeurt via **OCR/MRZ** en/of **NFC** met behulp van **Oribi software**. De Oribi SDK valideert de chip van documenten die voldoen aan de standaard zoals beschreven in de ICAO 9303-standaarden. Indien de chip het ondersteunt worden zowel de Actieve als Passieve authenticatie checks uitgevoerd.
2. **Beperking van gegevens**:
    - AMP verzamelt alleen gegevens die noodzakelijk zijn voor identiteitsvaststelling op basis van afspraken met de Opdrachtgever. ID-gegevens die niet nodig zijn, worden niet opgeslagen.
3. **Toegestane ID-bewijzen**:
    - AMP accepteert ICAO-compliant identiteitsdocumenten, zoals paspoorten, ID-kaarten en rijbewijzen, afhankelijk van de afspraken met de Opdrachtgever.

17.2.3 Attributen en bewijslast validatie

1. **Training van identificatiemedewerkers**:
    - De identificatiemedewerkers worden jaarlijks getraind en getoetst op:
        - Technische identificatie: herkennen van echtheidskenmerken en falsificaten.
        - Tactische identificatie: signaleren van opvallend gedrag.
        - Profiling: gezichtskenmerken zoals vorm, stand van ogen, neus en oren.
    - Jaarlijkse herhalingstrainingen zijn verplicht om de kwaliteit en consistentie van identificaties te waarborgen.
2. **Gebruik van Oribi software**:
    - Oribi software biedt nauwkeurige en betrouwbare tools voor het uitlezen en valideren van ID-documenten, inclusief NFC en MRZ-technologie.
    - Details over wat wordt gecontroleerd is per opdrachtgever vastgelegd en afgestemd in de zogeheten business rules.

17.2.4 Binding aan de aanvrager

1. **Gezichtsvergelijking**:
    - De identificatiemedewerker vergelijkt de foto op het ID-document met de fysiek aanwezige Gebruiker.
    - De Gebruiker moet persoonlijk aanwezig zijn.
    - De identificatiemedewerker krijgt voldoende tijd voor het uitvoeren van de verificatie.
    - De identificatiemedewerkers voeren deze stap zorgvuldig uit met behulp van technieken aangeleerd in de verplichte opleiding en jaarlijkse herhalingstrainingen.
2. **Controleproces**:
    - De gezichtsvergelijking maakt gebruik van handmatige en geautomatiseerde controles, indien ondersteund door beschikbare technologieën.
3. **Beveiliging**:
    - Alle biometrische data worden tijdelijk verwerkt en opgeslagen volgens strikte beveiligings- en privacy protocollen.

17.2.5 Afgifte van bewijs

1. **Rapportage**:
    - Na succesvolle identificatie worden de verzamelde gegevens en resultaten verwerkt en gedeeld met de Opdrachtgever.
2. **Veilige overdracht**:
    - Gegevens worden via een beveiligde, versleutelde verbinding overgedragen aan de Opdrachtgever.

- AMP Groep gebruikt standaard **TLS-protocollen** voor datatransport.

3. **Opslag en bewaartermijnen**:
   - De verzamelde gegevens worden opgeslagen in de AMP-database met een maximale retentieperiode van 21 dagen:
     i. 14 dagen in de actieve database.
     ii. 7 dagen in de back-up.
   - Gegevens kunnen op verzoek van de Opdrachtgever eerder worden verwijderd.
   - Gegevens in rust zijn versleuteld en alleen toegankelijk voor geautoriseerd personeel.
4. **Bijzonderheden i.v.m. de Opdrachtgever**:
   - De Opdrachtgever is verantwoordelijk voor verdere verwerking, zoals eigen archivering of retentiebeleid.