Certification Practice Statement (CPS)

Versie: 2.5.1
Datum: 2025-10-01
Status: Gereed
Taal: Nederlands

Wijzigingenblad

Versie	Datum	Omschrijving	Auteur
2.5	15-9-2025	Initiële versie	Marcel Settels
2.5.1	01-10-2025	Update ivm DPIA (bij ZORG-ID Smartcard)	Marcel Settels

1 Introductie

1.1 Overzicht

Achtergrond en aanleiding

Stichting VZVZ Servicecentrum (hierna: VZVZ) is door de Vereniging VZVZ gevraagd om zorgaanbieders te ondersteunen bij de overgang van de door het CIBG uitgegeven UZI-smartcards en elektronische certificaten naar het toekomstige Dezi-stelsel (“De ZorgIdentiteit”), zoals voorzien in de Wet DIAZ (Digitale Identificatie en Authenticatie in de Zorg).

Omdat de behandeling van de Wet DIAZ is vertraagd en invoering per 1 januari 2026 niet haalbaar is, is er sprake van een overgangssituatie. In deze periode biedt VZVZ op vrijwillige basis een tijdelijke ondersteuning voor medewerkers van zorgaanbieders die niet (meer) beschikken over een UZI-medewerkerspas en bijbehorend certificaat.

Rol van VZVZ en ZORG-ID

Deze ondersteuning vindt plaats door middel van de dienst ZORG-ID, waarmee elektronische certificaten namens en in opdracht van zorgaanbieders worden uitgegeven en beheerd. Deze certificaten kunnen:

- Worden gebruikt op een mobiel device (ZORG-ID Mobiel) met minimaal betrouwbaarheidsniveau **“substantieel”**, of
- Worden uitgegeven op een smartcard (ZORG-ID Smartcard) met betrouwbaarheidsniveau **“hoog”**.

VZVZ geeft in opdracht van de zorgaanbieder certificaten uit, die vanuit het eco-systeem ZORG-ID worden gegenereerd en bewaard.

VZVZ brengt voor deze certificaatdienstverlening in beginsel geen kosten in rekening bij zorgaanbieders of medewerkers. Zorgaanbieders en medewerkers maken voor eigen rekening gebruik van de uitgegeven certificaten.

Betrouwbaarheidsniveaus

Op dit moment levert de UZI-medewerkerspas als enige een betrouwbaarheidsniveau hoog, maar dat werkt niet op alle operating systemen die gebruikt worden binnen de zorg. Het doel van ZORG-ID Mobiel is tevens om een bredere toepassing van authenticatie met passend betrouwbaarheidsniveau in de zorg te realiseren, bijvoorbeeld in situaties waarin de UZI-medewerkerspas niet beschikbaar is. ZORG-ID Mobiel levert “substantieel’, ZORG-ID Smartcard is weergegeven voor gebruik op betrouwbaarheidsniveau hoog.

- **Bijlage 1** beschrijft hoe ZORG-ID Mobiel voldoet aan het betrouwbaarheidsniveau “substantieel”.
- **Bijlage 2** beschrijft hoe ZORG-ID Smartcard voldoet aan het betrouwbaarheidsniveau “hoog”.

Verantwoordelijkheden

Het uitgifteproces van certificaten brengt verantwoordelijkheden met zich mee:

- **Zorgaanbieders** zijn verantwoordelijk voor de identificatie van hun medewerkers en het naleven van relevante vereisten.
- **VZVZ (ZORG-ID)** verzorgt de uitgifte, het beheer en de intrekking van certificaten.

Indien één van beide partijen deze verplichtingen niet nakomt, kan dit leiden tot een verlaging van het betrouwbaarheidsniveau naar “substantieel” of “laag”.

Aansprakelijkheid en geschillen

Omdat er sprake is van een vrijwillige overgangssituatie tot het moment dat ZORG-ID of een opvolger officieel als inlogmiddel wordt goedgekeurd binnen het DEZI-stelsel, geldt het volgende:

- De aansprakelijkheid van zowel VZVZ als de zorgaanbieders is over en weer uitgesloten, behoudens voor zover dit wettelijk niet is toegestaan.
- Geschillen worden primair behandeld via een separate geschillenregeling (eventueel arbitrage).
- In het uiterste geval is de rechter te Den Haag bevoegd.

Gebruik binnen het ecosysteem

ZORG-ID maakt onderdeel uit van een geïntegreerd ecosysteem. Het gebruik van certificaten staat nooit op zichzelf, maar is altijd gekoppeld aan:

- Software van een door VZVZ geaccepteerde XIS-leverancier,
- Een specifieke smartcard, of
- Aanvullende software en/of applets.

Zorgaanbieders dienen voorafgaand te beoordelen of de context waarin zij certificaten willen gebruiken geschikt is.

Support en communicatie

Voor hulp bij problemen met certificaten nemen zorgaanbieders contact op met hun softwareleverancier, die indien nodig kan doorzetten naar de supportafdeling van VZVZ (Support | VZVZ | ZORG-ID).

Indien het CIBG besluit de UZI-smartcards of certificaten te beëindigen of de voorwaarden te wijzigen, kan dit gevolgen hebben voor ZORG-ID. VZVZ zal zorgaanbieders en medewerkers hierover informeren via haar website. In het uiterste geval kan dit leiden tot intrekking van uitgegeven certificaten.

Periodieke updates

Dit CPS wordt periodiek bijgewerkt op basis van nieuwe ontwikkelingen en praktijkervaringen. Alleen de meest recente, door VZVZ gepubliceerde versie is geldig; eerdere versies vervallen van rechtswege.

Externe dienstverleners

Voor het uitgifte- en beheerproces maakt VZVZ gebruik van technologie en diensten van AET Mobile Identity Services B.V. Met AET zijn contractuele en juridische waarborgen overeengekomen, waaronder een (sub)verwerkersovereenkomst conform het Uitvoeringsbesluit (EU) 2021/915 en de AVG.

1.2 Documentnaam en identificatie

Het Certification Practice Statement (CPS) van **ZORG-ID** beschrijft op welke wijze invulling wordt gegeven aan de dienstverlening rondom het uitgeven, beheren en intrekken van elektronische certificaten.
Het CPS geeft inzicht in de processen, procedures en beheersingsmaatregelen die door **VZVZ** worden toegepast bij het verstrekken van certificaten (mobiel en smartcard).

Met behulp van dit CPS kunnen zorgaanbieders, medewerkers en andere betrokkenen het vertrouwen bepalen in de door ZORG-ID geleverde diensten.
De algemene indeling van dit CPS volgt het model zoals gepresenteerd in **RFC 3647**, dat internationaal geldt als de facto standaard.

Formeel wordt dit document aangeduid als:

- **Naamgeving**: *20250915 ZORG-ID CPS v25*

- **Versie**: 2.5
- **Object Identifier (OID)**: *2.16.840.1.113883.2.4.3.111.20*
- **Publicatie**: *ww.vzvz.nl/zorg-id/cps*

Het CPS is publiek beschikbaar via de website van VZVZ en kan daarnaast op papier worden opgevraagd bij het secretariaat van VZVZ.

1.3 PKI-deelnemers

De volgende partijen spelen een rol binnen het ZORG-ID PKI-ecosysteem:

- **Certification Authorities (CA's)**: verantwoordelijk voor het daadwerkelijk uitgeven van certificaten. Dit betreft zowel de *Root CA* als de *Issuing CA*.
- **Registration Authorities (RA's)**: verantwoordelijk voor de registratie en identificatie van medewerkers op naam. Dit kan intern of extern zijn, met vastgelegde verantwoordelijkheden.
- **Subscribers**: de natuurlijke personen (medewerkers van zorgaanbieders) aan wie certificaten worden verstrekt.
- **Relying Parties**: zorgaanbieders, leveranciers en andere partijen die op de geldigheid en betrouwbaarheid van de certificaten vertrouwen, onder de voorwaarden zoals in dit CPS beschreven.

1.4 Certificaattoepassingen

De door VZVZ binnen het ZORG-ID uitgegeven certificaten zijn uitsluitend bedoeld voor gebruik binnen de zorgsector, door zorgaanbieders en hun medewerkers (op naam), alsmede door vertrouwende partijen die op deze certificaten vertrouwen.

De certificaten kunnen worden toegepast voor:

- **Authenticatie:** vaststellen van de identiteit van een zorgmedewerker, zorgaanbieder of systeem.
- **Elektronische handtekening:** het plaatsen en verifiëren van digitale handtekeningen in overeenstemming met de geldende wet- en regelgeving.
- **Beveiligde communicatie:** versleuteling en bescherming van gegevensuitwisseling tussen systemen binnen de zorg.

Binnen ZORG-ID zijn de volgende certificaatvormen beschikbaar:

- **ZORG-ID Mobiel** – certificaten voor authenticatie en ondertekening via mobiele apparaten.
- **ZORG-ID Smartcard** – certificaten voor authenticatie en ondertekening via een smartcard.

Certificaten mogen uitsluitend worden gebruikt voor de hierboven beschreven doeleinden. Het gebruik voor andere toepassingen is niet toegestaan, waaronder (maar niet beperkt tot):

- Code signing of distributie van software;
- Gebruik buiten de kaders van zorgcommunicatie of buiten de reikwijdte van de eIDAS-verordening en de Wet DIAZ;
- Gebruik in commerciële of niet-zorggerelateerde omgevingen zonder toestemming van VZVZ.

Testcertificaten worden in principe niet verstrekt aan derden binnen de productieomgeving. Voor interne testdoeleinden kan VZVZ-testmiddelen beschikbaar stellen.

1.5 Beleidsbeheer

De Policy Authority van VZVZ beheert dit CPS. Wijzigingen worden ingedeeld als materieel of niet-materieel en vervolgens beoordeeld door de afdelingen Security en Legal. Na goedkeuring worden de wijzigingen gepubliceerd.

Alle wijzigingen worden uitgevoerd in overeenstemming met de geldende wet- en regelgeving, zoals:

- eIDAS (EU-verordening 910/2014)
- Wet DIAZ
- ETSI-standaarden EN 319 411/412

1.6 Definities en afkortingen

Voor een overzicht van de gebruikte definities en afkortingen wordt verwezen naar Bijlage 3: Definities en afkortingen.

1.7 Correctheid

Hoewel de omschrijving met de grootst mogelijke zorgvuldigheid is gedaan, kunnen er fouten en/of omissies in de Annexes zitten. Het wordt op prijs gesteld indien u deze fouten en/of omissies meldt aan de support afdeling van VZVZ, zodat deze kunnen worden hersteld.

2 Publicatie- en repository verantwoordelijkheden

2.1 Algemene invulling ZORG-ID

De Certification Practice Statement (CPS) van ZORG-ID beschrijft de procedures en verantwoordelijkheden voor het beheer en gebruik van digitale certificaten binnen het ZORG-ID ecosysteem. Het document wordt zodanig gepubliceerd dat alle betrokken partijen gemakkelijk toegang hebben tot de meest actuele informatie over certificaatbeheer, beleidsregels en operationele procedures.

2.2 Publicatie

- **Locatie:** De CPS wordt gepubliceerd op de officiële ZORG-ID website.
- **Beschikbare informatie:** Naast de CPS zelf eveneens beschikbaar:
  - Certificate Revocation Lists (CRL)
  - Online Certificate Status Protocol (OCSP) services
- **Toegankelijkheid:** CRL- en OCSP-gegevens zijn continu online beschikbaar zodat verifiers certificaten in real-time kunnen valideren.

2.3 Geldigheid van de CPS

- **Actuele versie:** Alleen de meest recente, op de website gepubliceerde versie van de CPS is juridisch en operationeel geldig.
- **Oude versies:** Eerdere versies van de CPS zijn uitsluitend voor referentie beschikbaar en vormen geen basis voor certificaatverlening of -gebruik.

2.4 Versiebeheer en revisie

- **Frequentie van revisie:** De CPS wordt minimaal één keer per jaar herzien.
- **Triggers voor revisie:** Naast de jaarlijkse herziening kan een update plaatsvinden wanneer er wijzigingen zijn in:
  - Wet- en regelgeving (bijv. eIDAS, Wet DIAZ)
  - Interne processen of operationele procedures
  - Technologische ontwikkelingen die van invloed zijn op certificaatbeheer of beveiliging
- **Documentatie van wijzigingen:** Elke revisie wordt voorzien van een duidelijke changelog waarin wordt aangegeven:
  - De datum van revisie
  - Versienummer
  - Samenvatting van wijzigingen
- **Goedkeuringsproces:** Wijzigingen worden beoordeeld door de Security- en Legal-afdelingen van ZORG-ID en worden pas gepubliceerd na formele goedkeuring.

2.5 Repository verantwoordelijkheden

- **Beheer:** ZORG-ID is verantwoordelijk voor het beheer van de CPS repository, inclusief CRL- en OCSP-gegevens.
- **Integriteit:** De repository moet zodanig worden beheerd dat:
  - Inhoud niet onbevoegd kan worden aangepast
  - Historische versies kunnen worden geverifieerd (archivering)
  - Distributie veilig en betrouwbaar is
- **Beschikbaarheid:** ZORG-ID draagt zorg voor hoge beschikbaarheid van de repository, zodat certificaatverificatie altijd mogelijk is.

3 Identificatie en authenticatie

3.1 Algemene uitgangspunten

Binnen ZORG-ID wordt een strikt beleid gehanteerd voor de identificatie en authenticatie van gebruikers. Dit beleid is gebaseerd op het waarborgen van integriteit, vertrouwelijkheid en rechtsgeldigheid van digitale certificaten. Het doel is dat elke certificaathouder ondubbelzinnig geïdentificeerd kan worden, zowel op individueel niveau als op organisatorisch niveau.

3.2 Naming (certificaataanduiding)

Voor elk certificaat wordt een uniforme naamgeving gehanteerd. Deze naamgeving bevat de volgende attributen:

- **Volledige naam** van de certificaathouder
- **Functie of rol** binnen de organisatie
- **Zorgaanbieder-ID** van de organisatie waarbij de medewerker werkzaam is

Attribuut	Zorgverlener	Medewerker op naam	Medewerker niet op naam	Server
C (Country)	NL	NL	NL	NL
O (Organization)	Naam abonnee	Naam abonnee	Naam abonnee	Naam abonnee
OU (Org. Unit)	Niet aanwezig	Niet aanwezig	Afdeling	Optioneel afdeling
T (Title)	Aanspreektitel zorgverlener (beroepstitel, opleidingstitel of specialisme)	Nvt	Nvt	Nvt
G (GivenName)	Voornamen	Voornamen	Nvt	Nvt
SN (Surname)	Tussenvoegsel en geboortenaam zorgverlener	Tussenvoegsel en geboortenaam medewerker	Nvt	Nvt
CN (CommonName)	Voornamen, tussenvoegsel en geboortenaam zorgverlener	Voornamen, tussenvoegsel en geboortenaam medewerker	Functienaam medewerker	Systeemnaam
SerialNumber	UZI-nummer	UZI-nummer	UZI-nummer	UZI-nummer

Deze structuur ondersteunt transparantie en traceerbaarheid binnen het zorglandschap en maakt verificatie door derden mogelijk.

3.3 Identiteitsverificatie

De wijze van verificatie is afhankelijk van het type certificaat: smartcard of mobiel certificaat.

Smartcard certificaat (ZORG-ID Smartcard)

- **Uitgifte:** Het smartcardcertificaat wordt fysiek uitgereikt door een **Local Registration Authority (LRA)**.
- **Identificatieniveau:** De verificatie voldoet aan eIDAS “hoog” niveau.
- **Procedure:**
  - De LRA controleert de identiteit van de medewerker op basis van een **geldige UZI-medewerkerspas op naam**.
  - Bij goedkeuring wordt het smartcard certificaat aangemaakt en uitgegeven.
- **Doel:** Waarborgen dat alleen bevoegde personen toegang hebben tot kritische zorgprocessen en gegevens.

Mobiel certificaat (ZORG-ID Mobiel)

- **Uitgifte:** Het certificaat wordt door de zorgaanbieder uitgegeven aan de medewerker.
- **Identificatieniveau:** De verificatie voldoet aan eIDAS “substantieel” niveau.
- **Procedure:**
  - De zorgaanbieder controleert de identiteit van de medewerker volgens interne procedures.
  - Na goedkeuring wordt het mobiele certificaat aan de medewerker gekoppeld.
- **Doel:** Flexibele en veilige toegang tot digitale zorgtoepassingen zonder fysieke smartcard, met een betrouwbaar substantieel identificatieniveau.

3.4 Verificatie van de organisatie

- **Verantwoordelijkheid:** De zorgaanbieder is verantwoordelijk voor de correcte registratie van zijn medewerkers.
- **Controle:** De organisatie moet er zorg voor dragen dat alleen bevoegde medewerkers certificaten ontvangen en dat de registratie actueel blijft.
- **Richtlijn:** Elke wijziging in medewerkersstatus (indiensttreding, functiewijziging, uitdiensttreding) moet direct worden verwerkt in het certificaatbeheer.

3.5 Samengevat

Aspect	Smartcard	Mobiel	Verantwoordelijke organisatie
Identificatieniveau	eIDAS Hoog	eIDAS Substantieel	Zorgaanbieder
Identiteitsverificatie	LRA controle op UZI-medewerkerspas	Interne zorgaanbiederprocedure	Ja, registratie en actualisatie
Toepassing	Kritische toegang, elektronische handtekeningen	Flexibele toegang, digitale applicaties	Ja, continue naleving

4 Operationele eisen certificaatlevenscyclus

4.1 Algemene uitgangspunten

De certificaatlevenscyclus beschrijft alle stappen van aanvraag tot intrekking van digitale certificaten binnen het ZORG-ID ecosysteem. Elke fase heeft duidelijke operationele eisen om de veiligheid, integriteit en betrouwbaarheid van certificaten te waarborgen.

4.2 Aanvraag

- **Kanaal:** Certificaten kunnen worden aangevraagd via:
  - Het **ZORG-ID portal**, of
  - Een **Registration Authority (RA) / Local Registration Authority (LRA)**
- **Identiteitscontrole:** Elke aanvraag vereist verificatie van de identiteit van de aanvrager.
  - Voor smartcards vindt deze controle fysiek plaats door de LRA (zie hoofdstuk 3).
  - Voor mobiele certificaten vindt de controle plaats via interne zorgaanbiederprocessen.

4.3 Uitgifte

Smartcardcertificaat

- Sleutelgeneratie: De private sleutel wordt lokaal gegenereerd op een SSCD (Secure Signature Creation Device) / QSCD (Qualified Signature Creation Device).
- Certificaatafgifte: Na succesvolle verificatie van identiteit wordt het certificaat uitgegeven en gekoppeld aan de private sleutel.

Mobiel certificaat

- Sleutelgeneratie: Sleutel en certificaat worden gegenereerd op een beveiligd mobiel apparaat, conform ETSI EN 319 412 standaard.
- Certificaatafgifte: Het certificaat wordt automatisch gekoppeld aan de gegenereerde sleutel en aan de gebruiker gebonden.

4.4 Acceptatie

- Smartcard: De gebruiker activeert het certificaat door het instellen van een PIN.
- Mobiel: De gebruiker activeert het certificaat door het instellen van een wachtwoord (Pincode) of biometrische verificatie.
- Doel: Zorgen dat alleen de rechtmatige gebruiker toegang heeft tot de private sleutel en het certificaat.

4.5 Verlengen

- **Doel:** Verlengen van een certificaat vóór het verlopen van de geldigheid.
- **Identiteitsverificatie:**
  - **Mobiel certificaat:** Eenvoudige herverificatie, bijvoorbeeld via zorgaanbieder authenticatie.
  - **Smartcard:** Uitgebreide verificatie door LRA, inclusief fysieke aanwezigheid en controle van een nog geldige UZI-medewerkerspas.
- **Procedure:** Na verificatie wordt een nieuw certificaat uitgegeven, gekoppeld aan een nieuwe of bestaande sleutel.

4.6 Intrekking

- **Redenen voor intrekking:**
  - Verlies of diefstal van het apparaat of de smartcard
  - Beëindiging van dienstverband of rol binnen de zorgaanbieder en geen nieuwe werkgever.
  - Compromittering van de private sleutel of certificaat
- **Publicatie:**
  - Intrekking wordt gepubliceerd in de **Certificate Revocation List (CRL)** of via **Online Certificate Status Protocol (OCSP)**
  - **Tijdslimiet:** Binnen **24 uur** na intrekking moet het certificaat onbruikbaar zijn voor verificatie

4.7 Samenvatting certificaatlevenscyclus

Fase	Smartcard (ZORG-ID Smartcard)	Mobiel (ZORG-ID Mobiel)
Aanvraag	RA/LRA met fysieke identiteitscontrole	ZORG-ID portal / zorgaanbieder, interne controle
Uitgifte	Sleutel lokaal gegenereerd op SSCD/QSCD	Sleutel en certificaat gegenereerd op beveiligd mobiel device
Acceptatie	PIN instellen	Wachtwoord of biometrie instellen
Verlengen	Uitgebreide verificatie bij LRA mbv UZI-medewerkerspas	Eenvoudige verificatie via zorgaanbieder
Intrekking	Verlies, diefstal, beëindiging, compromittering	Verlies, diefstal, beëindiging, compromittering
Publicatie	CRL of OCSP binnen 24 uur	CRL of OCSP binnen 24 uur

5 Fysieke, procedurele en personele beveiliging

5.1 Algemene procedures

Om de betrouwbaarheid en veiligheid van de certificeringsautoriteit (CA) te waarborgen, zijn er diverse maatregelen getroffen op het gebied van fysieke beveiliging, personeel, logging en continuïteit. De CA-locaties zijn fysiek beschermd volgens de internationale norm **ETSI EN 319 411-2**, wat betekent dat er strikte eisen gelden voor toegang, bewaking en infrastructuurbeveiliging. Ook het personeel speelt een cruciale rol: medewerkers worden voorafgaand aan hun werkzaamheden zorgvuldig gescreend en krijgen gerichte training om hen bewust te maken van hun verantwoordelijkheden binnen een beveiligde omgeving.

Daarnaast worden alle handelingen binnen de CA-systemen nauwkeurig gelogd. Deze loggegevens vormen de basis voor regelmatige controles, waarbij elke drie jaar een onafhankelijke audit plaatsvindt om de naleving van procedures en beveiligingsrichtlijnen te toetsen. Tot slot zijn er uitgebreide procedures opgesteld voor back-up en disaster recovery. Deze zorgen ervoor dat de dienstverlening ook bij incidenten of calamiteiten kan worden voortgezet, zodat de continuïteit en integriteit van de certificeringsdiensten gewaarborgd blijven.

Security incidenten worden binnen 24 uur teruggekoppeld aan betrokken partijen.

6 Technische beveiligingsmaatregelen

6.1 Sleutelgeneratie en installatie

Sleutels voor CA's worden gegenereerd in HSM's met minimaal FIPS 140-2/3 Level 3 of equivalent. Key ceremonies worden vooraf gescript en volledig gelogd.

Cryptografie:
Smartcard: RSA 3072 / ECC P-384 (hoog)
Mobiel: ECC P-256 (substantieel)

6.2 Sleutelbescherming, back-up en escrow

Private keys verlaten het HSM nooit in plaintext. Back-ups zijn versleuteld en onder M-of-N controle toegankelijk.

Smartcard als SSCD; mobiel device beveiligd volgens **ETSI EN 319 412**.

6.3 Activatiegegevens

PINs en passphrases worden onder two-person integrity beheerd. Resetprocedures vereisen identificatie en logging.

6.4 Computer- en netwerkbeveiliging

Systemen zijn gehard volgens baseline-configuraties. Netwerken zijn gesegmenteerd; beheerkanalen zijn afgeschermd en gemonitord.

- **Fysieke beveiliging:** CA-locaties beveiligd volgens ETSI EN 319 411-2.
- **Personeel:** gescreend en getraind.
- **Logging en auditing:** alle acties gelogd, driejaarlijks geaudit.
- **Back-up / Disaster recovery:** procedures voor continuïteit beschreven.
- **Communicatie:** TLS 1.2+ voor alle CA-interacties.

6.5 Systeemlevenscyclus

Wijzigingen volgen change management met risicobeoordeling en rollbackplan. Binaries worden geverifieerd en waar nodig gesigned.

6.6 Algoritmen en parameters

Toegestane algoritmen: RSA 3072/4096, ECDSA P-256/P-384. Hashfuncties: SHA-256/384. Looptijden per profiel 36 maanden voor mobiel en de smartcard. Migraties worden vastgelegd (crypto-agility).

6.7 Tijdbron en tijdstempels

Systemen synchroniseren op betrouwbare tijdbronnen (bijv. interne NTP met GPS-bron). Afwijkingen worden gemonitord.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Aanvraag

- Via ZORG-ID portal of RA/LRA; identiteitscontrole vereist.

7.2 Uitgifte

- **Smartcard:** sleutel wordt lokaal gegenereerd op SSCD/QSCD. Certificaat uitgegeven na verificatie.
- **Mobiel:** sleutel en certificaat gegenereerd op beveiligd mobiel device, volgens ETSI EN 319 412.

7.3 Acceptatie

- Activering door gebruiker: PIN instellen (smartcard), wachtwoord/biometrie (mobiel).

7.4 Verlengen

- Voor verlopen certificaat; identiteitsverificatie: eenvoudig voor mobiel, uitgebreid voor smartcard.

7.5 Intrekking

- Redenen: verlies, diefstal, beëindiging dienstverband, compromittering.
- Publicatie in CRL of via OCSP binnen 24 uur.

7.6 Certificaatprofiel

- X.509 v3 met extensies: KeyUsage, ExtendedKeyUsage, SubjectAltName.
- ZORG-ID Smartcard → Hoog betrouwbaarheidsniveau, QCP-compliant
- ZORG-ID Mobiel → Substantieel betrouwbaarheidsniveau

8 Conformiteitsaudits en beoordelingen

8.1 Algemene bepalingen

Om de betrouwbaarheid van de certificeringsprocessen te waarborgen, ondergaat de organisatie drie jaarlijks een audit door een onafhankelijke auditor. Deze audit wordt uitgevoerd conform de norm **ETSI EN 319 411**, waarmee wordt gegarandeerd dat de processen en systemen voldoen aan strikte internationale eisen voor betrouwbaarheid, veiligheid en transparantie. Naast deze externe toetsing worden er ook **periodieke interne controles en compliance reviews** uitgevoerd. Deze interne evaluaties zorgen ervoor dat afwijkingen tijdig worden gesignaleerd en dat de organisatie continu blijft voldoen aan de geldende regelgeving en kwaliteitsnormen.

9 Juridische bepalingen

In hoofdstuk 1 zijn de juridische context opgenomen en de juridische bepalingen benoemd.

Bijlage 1: ZORG-ID Mobiel (MOB)

INLEIDING

Deze Annex heeft betrekking op de CPS voor ZORG-ID Mobiel, welke aan de vereisten voldoet van betrouwbaarheidsniveau “substantieel”.

1. *Inschrijving*

Een zorgaanbieder gaat bij activatie van de zorgorganisatie binnen ZORG-ID akkoord met de spelregels die binnen ZORG-ID gelden:

- *De organisatie is een bij het UZI-register geregistreerde zorgaanbieder met een UZI-servercertificaat*
- *Er vindt alleen uitgifte plaats van* identiteiten *op basis van de wettelijk verplichte WID-controle van de zorgmedewerker(s). Andere identiteiten zullen niet uitgegeven worden.*
- *De uitgifte van certificaten en identiteiten vindt plaats onder de verantwoordelijkheid van de zorgaanbieder (LRA). ZORG-ID heeft geen actieve rol hierin.*
- *Bij ZORG-ID Mobiel geeft de zorgaanbieder een identiteitscertificaat uit om deze (eenmalig) op te nemen in de smartphone van de zorgmedewerker*
- *De zorgaanbieder volgt een actief beveiligingsbeleid conform de NEN7510, ISO/IEC 27001; Burgerlijk Wetboek, Arbowet, etc..*

1.1 Aanvraag en registratie .

De kolom ZA geeft weer de verantwoordelijkheid van de zorgaanbieder en de kolom VZVZ geeft de verantwoordelijkheid van VZVZ aan (V = Verantwoordelijk, O = Ondersteunend)

Invulling	**ZA**	**VZVZ**	**eIDAS (informatieve referentie)**
De context waarbinnen de elektronische certificaten worden gebruikt, inclusief de daarbij voorwaarden, alsmede de CPS zijn ter beschikking gesteld (zie spelregels)	V	O	De aanvrager moet bekend zijn met de voorwaarden die aan het gebruik van het elektronische identificatiemiddel zijn verbonden.
De context waarbinnen de elektronische certificaten worden gebruikt, inclusief de daarbij voorwaarden, alsmede de CPS zijn ter beschikking gesteld aan de gebruikers.	V	O	De aanvrager moet bekend zijn met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden.

Gegeven de werkgevers-werknemersrelatie (identificatieplicht) moeten de relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, reeds zijn verzameld.	V	O	De relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, moeten zijn verzameld

1.2 Bewijs en verificatie van identiteit (natuurlijke persoon). In essentie betreft het de medewerker op naam, waarmee de zorgaanbieder een arbeidsrechtelijke relatie heeft.

Invulling	**ZA**	**VZVZ**	**eIDAS (informatieve Referentie)**
De medewerker overlegt het WDO-middel (paspoort, identiteitskaart of rijbewijs) bij de inschrijving (aangaan werkrelatie) bij de zorgaanbieder.	V	O	De persoon kan worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt.
De standaard echtheidscontroles worden uitgevoerd door de werkgever (identificatieplicht).	V	O	Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn.
Het overhandigde WDO-document wordt door de zorgaanbieder gecontroleerd (vis-à-vis).	V	O	Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden verondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is.
Er is een identiteitsdocument overgelegd tijdens een registratieproces ter controle door zorgaanbieder.	V	O	Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het

			document lijkt betrekking te hebben op de persoon die het heeft overgelegd;
Er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt door de zorgaanbieder die de verificatie doet.	V	O	Er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn.

Opmerking: aangezien hier sprake is van een dienstverband tussen de rechtspersoon en de natuurlijke persoon wordt dit vereiste ingevuld door de arbeidsovereenkomst of vergelijkbare werkrelatie en wordt door VZVZ als verplichting gesteld aan de zijde van de zorgaanbieder.

1.3 Bewijs en verificatie van identiteit (rechtspersonen) (niet van toepassing).

Doordat alle organisatie binnen ZORG-ID bij activatie voorzien moeten zijn van een UZI-servercertificaat is impliciet vastgelegd dat het bestaan van deze actieve rechtspersoon is vastgesteld. VZVZ stelt niet nogmaals vast dat het een geldige rechtspersoon is, maar bouwt voor op het werk van het UZI-register.

1.4 Koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen

· ZORG-ID identiteiten worden gekoppeld aan het URA van de betrokken zorgorganisatie; ·

Procedures voor schorsing, wijziging en herroeping zijn van toepassing; Deze wordt uitgevoerd door de administrator of beheerder van de zorgaanbieder, geïdentificeerd door een URA. Administrator-rol en Beheerderrol wordt geheel beheerd door de zorgaanbieder. Binnen ZORG-ID worden alleen relaties gelegd voor medewerkers van de zorgorganisatie die daadwerkelijk een ZORG-ID Identiteit in ontvangst hebben genomen en/of aangegeven hebben dat de identiteit door deze zorgaanbieder mag worden beheerd.

· Delegatie van bevoegdheden kan worden vastgelegd en beheerd (b.v. TaakCode).

Invulling	ZA	VZVZ	eIDAS (Informatieve Referentie)
De zorgaanbieder is verantwoordelijk voor het actueel houden van de eigen Identiteiten. Technisch wordt dit ondersteund door ZORG-ID. Alle in de eIDAS genoemde functies worden ondersteund.	V	O	Het moet mogelijk zijn een koppeling te schorsen en/of te herroepen. De verschillende koppelingsstadia (o.a. activering, schorsing, hernieuwing, herroeping) worden beheerd volgens op nationaal niveau erkende procedures.
In een werkgever werknemer relatie bestaan lokale verantwoordelijkheden. Er is geen sprake van over te dragen gedelegeerde bevoegdheden zoals bedoeld binnen eIDAS. In de toekomst zullen er naar verwachting landelijke bevoegdheden vanuit Dezi zijn. Momenteel zijn uitsluitend lokale verantwoordelijkhe-den instelbaar.	nvt	Nvt	De natuurlijke persoon wiens elektronische identificatiemiddel is gekoppeld aan het elektronische identificatiemiddel van de rechtspersoon kan volgens op nationaal niveau erkende procedures de uitoefening van de koppeling delegeren aan een andere natuurlijke persoon. De delegerende natuurlijke persoon blijft echter aansprakelijk.
De koppeling wordt op de volgende wijze uitgevoerd (cumulatief) (zie volgende rijën):			
Administrators / Beheerders hebben alleen rechten om eigen personeel te beheren.	V	O	De natuurlijke persoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat hij namens die rechtspersoon optreedt.
Een werkgever - werknemersrelatie is van toepassing (wettelijke identificatieplicht).	V	O	De koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures, wat ertoe heeft geleid dat de koppeling in een gezaghebbende bron is geregistreerd.

2. *Beheer van elektronische identificatiemiddelen.*

2.1 Kenmerken en ontwerp van elektronische identificatiemiddelen

Invulling	ZA	VZVZ	eIDAS (Informatieve Referentie)

Het ZORG-ID Mobiel authenticatiemiddel is uitgegeven door de Administrator/ Beheerder. ZORG-ID Mobiel is voorzien van een Pincode.	V	V	Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren.
De uitgegeven mobiele identiteit op de smartphone (bezit) en bijbehorende pincode (kennis) zijn onlosmakelijk met elkaar verbonden.	O	V	Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.
Er wordt gebruik gemaakt van persoonlijke tweefactoren authenticatie	O	V	Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren.
ZORG-ID Mobiel wordt uitgegeven op persoonlijke devices van de medewerker	O	V	Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.

2.2. Uitgifte, uitreiking en activering

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Het proces van uitgifte gaat gepaard met uitgifte van het identificatiemiddel via een QR-code die face-to-face moet worden ‘overhandigd’.	V	O	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld.

2.3 Schorsing, herroeping en reactivering

Invulling	ZA	VZVZ	eIDAS (Informatieve Referentie)
In het ZORG-ID Portaal worden identificatiemiddelen beheerd.	V	O	Het is mogelijk het elektronische identificatiemiddel snel en doeltreffend te schorsen en/ of te herroepen.
In het ZORG-ID Portaal, de zorgsystemen en de infrastructuur zijn voorzien van beveiligingsmaatregelen om dit te voorkomen.	V	O	Er bestaan maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen
Alleen Administrators en Beheerders van identiteiten kunnen identificatiemiddelen heractiveren	V	O	Een elektronisch identificatiemiddel mag slechts worden gereactiveerd indien nog steeds wordt voldaan aan dezelfde betrouwbaarheidsvereisten als die welke voorafgaand aan de schorsing of herroeping van kracht waren

2.4 Verlenging en vervanging.

Invulling	ZA	VZVZ	eIDAS (Informatieve Referentie)
Verlenging en vervanging van het authenticatiemiddel is alleen mogelijk na herauthenticatie bij de zorgaanbieder bij de beheerder of administrator.	V	O	Rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, moet voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau.

3. *Authenticatie*

Dit onderdeel is met name gericht op dreigingen die gepaard gaan met het gebruik van het authenticatiemechanisme. Het vermeldt de vereisten voor elk van de betrouwbaarheidsniveaus. In dit onderdeel wordt ervan uitgegaan dat de controles in overeenstemming zijn met de risico's op het desbetreffende niveau.

3.1 Authenticatiemechanisme

In onderstaande tabel worden de vereisten weergegeven voor het authenticatiemechanisme, door middel waarvan de natuurlijke persoon of rechtspersoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij.

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Binnen ZORG-ID wordt het elektronische identificatiemiddel (zoals een certificaat) cryptografisch gecontroleerd op authenticiteit via digitale handtekeningen. De geldigheidsstatus van het certificaat wordt in real-time geverifieerd via OCSP of CRL. Pas na succesvolle validatie worden de gekoppelde persoonsidentificatiegegevens vrijgegeven.	V	O	Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd.
De persoonsgegevens worden opgeslagen conform verwerkingsovereenkomst getekend, afhankelijk van de locatie, tussen de zorgaanbieder en de softwareleverancier met VZVZ als subverwerker of tussen de zorgaanbieder en VZVZ.	V	O	Indien als onderdeel van het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, wordt die informatie beveiligd ter bescherming tegen verlies en schending, met inbegrip van offlineanalyse.
Het authenticatiemechanisme werkt op basis van public key infrastructure (PKI) infrastructuur en beveiligde verbindingen.	O	V	Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of

			manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel.
In het licht van dynamische authenticatie wordt de verificatie van het elektronische identificatiemiddel real-time en contextafhankelijk uitgevoerd. Dit betekent dat naast het controleren van de geldigheid van het certificaat (via OCSP/CRL), ook actuele factoren zoals tijd, locatie, sessiegedrag of risicoprofiel worden meegenomen. Alleen wanneer het middel technisch geldig is én de context voldoet aan vooraf gedefinieerde authenticatie-eisen, worden persoonsidentificatiegegevens vrijgegeven.	O	V	Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie.
Het authenticatiemechanisme (App, ID, Pincode, ZORG-ID platform) sluit misbruik uit door verschillende lagen van beveiliging (verbindingen, lokale sleutels, HSM toegang, Gebruik persoonscertificaten).	O	V	Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel (ZORG-ID Mobiel)

4 *Beheer en organisatie*

Alle deelnemers die een dienst verlenen op het gebied van elektronische identificatie **in een grensoverschrijdende context** (hierna „aanbieders” genoemd) beschikken over gedocumenteerde methoden en beleid voor het beheer van informatiebeveiliging, benaderingen voor risicobeheersing en andere erkende controlemethoden, zodat zij de bevoegde bestuursorganen van de lidstaten op het gebied van stelsels voor elektronische identificatie garanties kunnen bieden dat in doeltreffende praktijken is voorzien. In onderdeel 2.4 wordt ervan uitgegaan dat alle vereisten/elementen in overeenstemming zijn met de risico's op het desbetreffende niveau.

ZORG-ID is een platform voor een Nederlands Authenticatie. Zorgaanbieders buiten Nederland kunnen geen URA verkrijgen. Mocht ZORG-ID in andere landen of buiten Nederland gebruikt gaan worden , zullen hiervoor aanvullende eisen worden gerealiseerd.

2.4.1 Algemene bepalingen

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
ZORG-ID is een privaat initiatief. ZORG-ID beoogt binnen het Dezi-stelsel toegelaten te worden, waarbij het de bedoeling is dat uiteindelijk wordt voldaan aan betrouwbaarheidsniveau “hoog” conform eIDAS.	nvt	nvt	Aanbieders die een operationele dienst aanbieden die onder deze verordening valt, zijn een overheidsinstantie of een rechtspersoon die door het nationale recht van een lidstaat als zodanig wordt erkend, over een gevestigde organisatie beschikt en volledig operationeel is op alle gebieden die voor de verlening van de diensten relevant zijn.
De zorgaanbieder houdt zich aan de wettelijke verplichtingen van het vaststellen van de identiteiten voor werknemers die binnen een zorgorganisatie werken.	V	O	De aanbieders voldoen aan al hun wettelijke verplichtingen in verband met het verrichten en leveren van de dienst, onder meer wat betreft de soorten informatie die mogen worden gevraagd, de wijze waarop het bewijs van de identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard.
VZVZ is verzekerd voor de bedrijfsrisico’s en wordt gefinancierd door Zorgverzekeraars Nederland en het Ministerie van Volksgezondheid.	O	V	De aanbieders kunnen aantonen dat zij in staat zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen beschikken om hun activiteiten en de dienstverlening voort te zetten.
VZVZ heeft op grond van deze CPS afspraken met de zorgaanbieders	V	O	De aanbieders zijn verantwoordelijk voor het naleven van alle

gemaakt en heeft ook betrekking op andere entiteiten waar diensten zijn uitbesteed waardoor de zorgaanbieders hun verplichtingen kunnen nakomen.			verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden.
ZORG-ID is conform Nederlands recht opgezet.	V	O	Stelsels voor elektronische identificatie die niet volgens nationaal recht zijn opgezet, moeten over een doeltreffend beëindigingsplan beschikken. Dat plan omvat voorzieningen voor de ordelijke stopzetting van de dienstverlening of de voortzetting daarvan door een andere aanbieder, voor de wijze waarop de betrokken autoriteiten en eindgebruikers worden ingelicht, alsook voor de wijze waarop de administratie wordt beschermd, bewaard en vernietigd overeenkomstig het voor het stelsel geldende beleid

2.4.2 Gepubliceerde mededelingen en informatie voor de gebruikers

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
De dienst wordt actueel beschreven op de website www.zorg-id.nl	O	V	Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring.
Procedures staan beschreven op de website www.zorg-id.nl	O	V	Er dient te worden voorzien in passend beleid en passende

			procedures om de gebruikers van de dienst tijdig en op betrouwbare wijze te informeren over elke wijziging van de beschrijving van de dienst, alle toepasselijke voorwaarden en de privacyverklaring
Support- en beheerprocedures zijn toegankelijk via ZORG-ID website.	O	V	Er dient te worden voorzien in passend beleid en passende procedures om verzoeken om informatie volledig en correct te beantwoorden

2.4.3 Beheer van informatiebeveiliging

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
VZVZ beschikt over het NEN 7510 certificaat. Zie verder www.zorg-id.nl	O	V	Er bestaat een doeltreffend beheerssysteem voor informatiebeveiliging dat zorg draagt voor het beheer en de beheersing van informatiebeveiligingsrisico's.
VZVZ beschikt over het NEN 7510 certificaat. Zie verder www.zorg-id.nl	O	V	Het beheerssysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.

2.4.4 Bijhouden van administratie

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
VZVZ beschikt over het NEN 7510 certificaat, waarbij alle vormen van	O	V	Relevante informatie wordt vastgelegd en bewaard met behulp van een doeltreffend

procedures, informatiebeveiliging en gegevensbescherming. Zie voor meer info www.zorg-id.nl.			documentenbeheersysteem, met inachtneming van de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring
ZORG-ID bevat alleen actuele data. De logging wordt bewaard volgens de wettelijke bewaartermijnen (in de systemen 6 maanden).	O	V	De gegevens moeten worden bewaard voor zover dat is toegestaan door het nationale recht of een andere nationale bestuurlijke regeling, en beschermd gedurende de termijn die noodzakelijk is met het oog op financiële controle en onderzoek van beveiligingsinbreuken; na afloop van de bewaringstermijn worden de gegevens veilig vernietigd.

2.4.5 Faciliteiten en personeel.

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Organisatie VZVZ is NEN7510 gecertificeerd. Haar onderaannemer / dienstverlener AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd VZVZ heeft een stelsel van waarborgen afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA/ verwerkersovereenkomst	O	V	Er zijn procedures om te waarborgen dat personeelsleden en sub contractanten voldoende zijn opgeleid en gekwalificeerd en dat zij ervaren zijn in de vaardigheden die vereist zijn voor de taken die zij vervullen.
Organisatie VZVZ is NEN7510 gecertificeerd. AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd	O	V	Er zijn voldoende personeelsleden en sub contractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures.

Organisatie VZVZ is NEN7510 gecertificeerd. AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd VZVZ heeft een stelsel van waarborgen afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA/ verwerkersovereenkomst.	O	V	De voor de dienstverlening gebruikte faciliteiten staan onder permanente controle en worden permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten.
Organisatie VZVZ is NEN7510 gecertificeerd. AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd VZVZ heeft een stelsel van waarborgen afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA/ verwerkersovereenkomst	O	V	De voor de dienstverlening gebruikte faciliteiten zijn zodanig ingericht dat de toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie beperkt is tot bevoegde personeelsleden of subcontractanten.

2.4.6 Technische controles

BlueX eID Management is gecertificeerd als een betrouwbaar systeem volgens CEN/TS 419261:2015 (Beveiligingseisen voor betrouwbare systemen die certificaten en tijdstempels beheren).

CA (Certificate Authority Service) wordt geïmplementeerd met behulp van de Ascertia CA-services: De Ascertia ADSS CA/PKI-server is gecertificeerd volgens Common Criteria (CC) Evaluation Assurance Level 4+ (EAL4+) met ALC_FLR.3 1.

RQSCD (Remote Qualified Signature Creation Device) De ADSS SAM Appliance is Common Criteria EAL4+ gecertificeerd, wat een hoog niveau van IT-beveiliging 1 inhoudt. Het voldoet aan Protection Profile EN 419 241-2, dat specifiek is ontworpen voor Remote Qualified Signature Creation Devices (QSCD's).

HSM-systemen: Common Criteria EAL4+-certificering, eIDAS-beschermingsprofiel EN 419 221-5, eIDAS-beschermingsprofiel EN 419 241-2, eIDAS-artikel 30 en 31-naleving.

Invulling	ZA	VZVZ	eIDAS (Informatieve Referentie)
Cryptografische beveiliging voor alle communicatie is in gericht om de veiligheid te garanderen. Persoonsgegevens die uitgewisseld worden door de infrastructuur zijn encrypt. De data op de servers zijn onderdeel van een DPIA (minimaal aanwezig én beveiligd tegen ongeoorloofde toegang).	O	V	Er is voorzien in proportionele controles ter beheersing van de risico's voor de veiligheid van de diensten, waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkte informatie worden beschermd.
De persoonsgegevens en gevoelige gegevens worden Cryptografisch beveiligd. Alle lijnen en verbindingen zijn beveiligd middels mutual TLS op basis van certificaten. Een Pentest op het gebruik van deze beveiliging is onderdeel van de waarborg.	O	V	De elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, worden beschermd tegen afluisteren, manipuleren en herafspelen.
Gebruik van HSM’s Al het sleutel materiaal is per ‘identiteit’ opgeslagen in een HSM die alleen wordt geopend als aan de toegangsvoorwaarden wordt voldaan. Alleen de eigenaar kan bij dit materiaal.	O	V	De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, is beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is. Er wordt op toegezien dat dergelijk materiaal niet permanent in onversleutelde staat wordt opgeslagen.
De architectuur van ZORG-ID vereist hoge beveiliging. De procedures van monitoring werken 24*7 en onze DAP / SLA hebben garanties voor snelle respons bij incidenten.	O	V	Er zijn procedures die waarborgen dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het

VZVZ heeft een stelsel van waarborgen rondom veiligheid afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA.			risiconiveau, incidenten en veiligheidsinbreuken.
Alle certificaten zijn opgeslagen in HSMs en de database(s) met identiteitsgegevens is beveiligd. . Er vindt geen fysiek transport van sleutelmateriaal plaats. Verwijderen kan niet. Er is wel een CRL waarlangs het sleutelmateriaal geblokkeerd kan worden.	O	V	Alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, worden veilig opgeslagen, vervoerd en verwijderd.
De cryptografisch beveiliging van het sleutelmateriaal vindt plaats middels HSMs. Het management van de HSM's voldoet aan de Europese normen.	O	V	Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.

2.4.7 Compliance en audit

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Er vinden driejaarlijkse audits plaats conform NEN 7510.	O	V	Er vinden periodieke interne audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.
Audits vinden geregeld plaats conform NEN 7510.	O	V	Er vinden periodieke onafhankelijke interne of externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de

			naleving van het desbetreffende beleid te waarborgen.

Bijlage 2: ZORG-ID Smartcard

INLEIDING

Deze Annex heeft betrekking op de CPS voor ZORG-ID Smartcard, welke aan de vereisten voldoet van betrouwbaarheidsniveau “hoog”.

1. *Inschrijving*

Een zorgaanbieder gaat bij activatie van de zorgorganisatie binnen ZORG-ID akkoord met de spelregels die binnen ZORG-ID gelden:

- *De organisatie is een bij het UZI-register geregistreerde zorgaanbieder met een UZI-servercertificaat*
- *Er vindt alleen uitgifte plaats van* identiteiten *op basis van de wettelijk verplichte WID-controle van de zorgmedewerker(s). Andere identiteiten zullen niet uitgegeven worden.*
- *De uitgifte van certificaten en identiteiten vindt plaats onder de verantwoordelijkheid van de zorgaanbieder (LRA). ZORG-ID heeft geen actieve rol hierin.*
- *Bij ZORG-ID Mobiel geeft de zorgaanbieder een identiteitscertificaat uit om deze (eenmalig) op te nemen in de smartphone van de zorgmedewerker*

- *De zorgaanbieder volgt een actief beveiligingsbeleid conform de NEN7510, ISO/IEC 27001; Burgerlijk Wetboek, Arbowet, etc..*

VZVZ ontvangt van AET Europe gegevens (bedrijfsnaam en aankoophoeveelheden) met betrekking tot ZORG-ID gerelateerde aankopen. Deze gegevens worden gebruikt voor het monitoren van KPI’s en het waarborgen van de juiste werking van de ZORG-ID Smartcard faciliteiten. Deze gegevens worden, waar het gaat om persoonsgegevens, verwerkt op grond van het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG). In dit kader hebben VZVZ en AET Europe een afweging gemaakt tussen de belangen van zorgaanbieders en de belangen van VZVZ en AET Europe.

1.1 Aanvraag en registratie.

Invulling	ZA	VZVZ	eIDAS (Informatieve Referentie)
De context waarbinnen de elektronische certificaten en het	V	O	De aanvrager moet bekend zijn met de voorwaarden die aan het gebruik van het

elektronische identificatiemiddel worden gebruikt, inclusief de daarbij voorwaarden, alsmede de CPS zijn ter beschikking gesteld (zie spelregels)			elektronische identificatiemiddel zijn verbonden.
De context waarbinnen de elektronische certificaten worden gebruikt, inclusief de daarbij voorwaarden, alsmede de CPS zijn ter beschikking gesteld.	V	O	De aanvrager moet bekend zijn met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden.
Gegeven de werkgevers-werknemersrelatie (identificatieplicht) moeten de relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, reeds zijn verzameld.	V	O	De relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, moeten zijn verzameld

1.2 Bewijs en verificatie van identiteit (natuurlijke persoon). In essentie betreft het de medewerker op naam, waarmee de zorgaanbieder een arbeidsrechtelijke relatie heeft.

Invulling	**ZA**	**VZVZ**	**eIDAS (informatieve Referentie)**
De medewerker overlegt het WDO-middel (paspoort, identiteitskaart of rijbewijs) bij de inschrijving bij de zorgaanbieder.	V	O	De persoon kan worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt.
De standaard echtheidscontroles worden uitgevoerd door de werkgever. (Identificatieplicht)	V	O	Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn.

Het overhandigde WDO-document wordt door de zorgaanbieder gecontroleerd (vis-à-vis).	V	O	Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden verondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is.
Er is een identiteitsdocument overgelegd tijdens een registratieproces ter controle door zorgaanbieder.	V	O	Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het document lijkt betrekking te hebben op de persoon die het heeft overgelegd;
Deze worden procedureel afgedwongen doordat de zorgaanbieder de verificatie doet volgens bij hem gangbare werkwijzen.	V	O	Er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn.
De ZORG-ID Smartcard is voorzien van de identiteit op basis van de UZI-medewerkerspas van de persoon via een ononderbroken proces tijdens het aanmaken. Hiermee is tevens in deze procedure de identiteit vastgesteld. **Dit is kenmerkend voor ZORG-ID Smartcard**	V	O.	Indien is geverifieerd dat de persoon in het bezit is van een bewijs dat voorzien is van een foto of biometrische gegevens, dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt, wordt het bewijs gecontroleerd op geldigheid aan de hand van een gezaghebbende bron
De UZI-medewerkerspas is de gezaghebbende bron voor het vaststellen van de identiteit. Bij de uitgifte daarvan zijn alle vereiste controles uitgevoerd.	V	O	De door de aanvrager opgegeven identiteit wordt geverifieerd door vergelijking van één of meer fysieke kenmerken van de persoon met een gezaghebbende bron.

Opmerking: aangezien hier sprake is van een dienstverband tussen de rechtspersoon en de natuurlijke persoon wordt dit vereiste ingevuld door de arbeidsovereenkomst en wordt door VZVZ als verplichting gesteld aan de zijde van de zorgaanbieder.

1.3 Bewijs en verificatie van identiteit (rechtspersonen) (niet van toepassing).

Doordat alle organisatie binnen ZORG-ID bij activatie voorzien moeten zijn van een UZI-servercertificaat is impliciet vastgelegd dat het bestaan van deze actieve rechtspersoon is vastgesteld. VZVZ stelt niet nogmaals vast dat het een geldige rechtspersoon is, maar bouwt voor op het werk van het UZI-register.

1.4 Koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen

· ZORG-ID identiteiten worden gekoppeld aan het URA van de betrokken zorgorganisatie; · Procedures voor schorsing, wijziging en herroeping zijn van toepassing; Deze wordt uitgevoerd door de administrator of beheerder van ZORG-ID van de URA. Administrator-rol en Beheerderrol wordt geheel beheerd door de zorgaanbieder. Binnen ZORG-ID worden alleen relaties gelegd voor medewerkers van de zorgorganisatie die daadwerkelijk een ZORG-ID Identiteit in ontvangst hebben genomen en/of aangegeven hebben dat de identiteit door deze zorgaanbieder mag worden beheerd.

· Delegatie van bevoegdheden kan worden vastgelegd en beheerd.

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
De zorgaanbieder is verantwoordelijk voor het actueel houden van de eigen Identiteiten. Technisch wordt dit ondersteund door ZORG-ID. Alle in de eIDAS genoemde functies worden ondersteund.	V	O	Het moet mogelijk zijn een koppeling te schorsen en/of te herroepen. De verschillende koppelingsstadia (o.a. activering, schorsing, hernieuwing, herroeping) worden beheerd volgens op nationaal niveau erkende procedures.
In een werkgever werknemer relatie bestaan lokale verantwoordelijkheden. Er is geen sprake van over te dragen gedelegeerde bevoegdheden zoals bedoeld binnen eIDAS. In de toekomst zullen er naar verwachting landelijke bevoegdheden vanuit Dezi zijn. Momenteel zijn uitsluitend lokale verantwoordelijkhe-den instelbaar.	nvt	Nvt	De natuurlijke persoon wiens elektronische identificatiemiddel is gekoppeld aan het elektronische identificatiemiddel van de rechtspersoon kan volgens op nationaal niveau erkende procedures de uitoefening van de koppeling delegeren aan een andere natuurlijke persoon. De delegerende natuurlijke persoon blijft echter aansprakelijk.

De koppeling wordt op de volgende wijze uitgevoerd (cumulatief)			
Administrators / Beheerders hebben alleen rechten om eigen personeel te beheren.	V	O	De natuurlijke persoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat hij namens die rechtspersoon optreedt.
Uitsluitend op basis van een UZI-medewerkerpas wordt het bewijs van de persoon vastgelegd.	O	V	De koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures, wat ertoe heeft geleid dat de koppeling in een gezaghebbende bron is geregistreerd.
Uitsluitend op basis van een UZI-medewerkerspas wordt het bewijs van de persoon vastgelegd **Dit is kenmerkend voor de ZORG-ID Smartcard**	O	V	Er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau hoog.
Uitsluitend op basis van een UZI-medewerkerspas wordt het bewijs van de persoon vastgelegd **Dit is kenmerkend voor de ZORG-ID Smartcard**	O	V	De koppeling is geverifieerd op basis van een in een nationale context gebruikte unieke identificatiecode die de rechtspersoon vertegenwoordigt, en op basis van uit een gezaghebbende bron afkomstige informatie die op unieke wijze een natuurlijke persoon vertegenwoordigt.

2. *Beheer van elektronische identificatiemiddelen.*

2.1 Kenmerken en ontwerp van elektronische identificatiemiddelen

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
ZORG-ID Smartcard is een fysieke pas beveiligd met een Pincode. Bij uitgifte wordt de pas gekenmerkt met een ondertekend stukje dat met een UZI-medewerkerspas	O	V	Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren.

ZORG-ID Smartcard (PKI-smartcard) is een fysieke pas beveiligd met een Pincode. Bij uitgifte wordt de pas gekenmerkt met een door de UZI-medewerkerspas ondertekend stukje informatie met daarin het UZI-nr van de medewerker.	O	V	Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.
Een PKI-smartcard (Public Key Infrastructure) wordt gebruikt voor veilige authenticatie, digitale handtekeningen en versleuteling. Wanneer zo'n kaart gecertificeerd is volgens Common Criteria EAL4+, biedt deze een hoog niveau van bescherming tegen vervalsingen en identiteitsdiefstal via het volgende mechanisme: *Veilige Sleutelopslag en Sleutelbeheer* • De privésleutels op de smartcard worden veilig opgeslagen en zijn beschermd tegen ongeautoriseerde toegang. • Sleutels worden gegenereerd en beheerd binnen een beveiligde omgeving, waardoor kopiëren of misbruik vrijwel onmogelijk is. *Sterke Authenticatieprotocollen* • PKI-smartcards gebruiken cryptografische challenge-response mechanismen voor authenticatie. • EAL4+ garandeert dat deze protocollen veilig zijn geïmplementeerd en bestand zijn tegen aanvallen zoals replay, man-in-the-middle en brute force.	O	V	Het elektronische identificatiemiddel biedt bescherming tegen kopiëring en vervalsing en tegen aanvallers met een hoog aanvalspotentieel.

Fysieke en Logische Sabotagebestendigheid • EAL4+ gecertificeerde kaarten zijn getest op weerstand tegen fysieke en logische aanvallen. • Dit omvat bescherming tegen side-channel aanvallen zoals stroomanalyse of timingaanvallen, die gebruikt kunnen worden om identiteitssleutels te stelen. **Dit is kenmerkend voor de ZORG-ID Smartcard**			
De ZORG-ID Smartcard is PKI-smartcard. Een PKI-smartcard met Common Criteria EAL4+ certificering beschermt zich tegen oneigenlijk gebruik door derden via een combinatie van fysieke, logische beveiligingsmaatregelen: • De smartcard vereist een persoonlijke pincode of biometrische verificatie voordat deze gebruikt kan worden. • Zonder deze verificatie kunnen derden de kaart niet activeren, zelfs als ze deze fysiek in handen hebben. **Dit is kenmerkend voor de ZORG-ID Smartcard**	O	V	Het elektronische identificatiemiddel is zodanig ontworpen dat het door de persoon aan wie het toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.

2.2. Uitgifte, uitreiking en activering

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Bij het aanmaken van de smartcard wordt door de zorgaanbieder gecontroleerd dat de desbetreffende	V	O	Bij het activeringsproces wordt geverifieerd dat slechts de persoon aan wie het elektronische

medewerker met een geldige UZI-medewerkerspas de smartcard activeert. Het ZORG-ID Portaal en ZORG-ID Desktop app toetsen de geldigheid. **Dit is kenmerkend voor de ZORG-ID Smartcard**			identificatiemiddel toebehoort ervan in het bezit wordt gesteld.

2.3 Schorsing, herroeping en reactivering

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
In het ZORG-ID Portaal worden identificatiemiddelen beheerd.	V	O	Het is mogelijk het elektronische identificatiemiddel snel en doeltreffend te schorsen en/ of te herroepen.
In het ZORG-ID Portaal, de zorgsystemen en de infrastructuur zijn voorzien van beveiligingsmaatregelen om dit te voorkomen.	V	O	Er bestaan maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen
Alleen Administrators en Beheerders van identiteiten kunnen identificatiemiddelen heractiveren	V	O	Een elektronisch identificatiemiddel mag slechts worden gereactiveerd indien nog steeds wordt voldaan aan dezelfde betrouwbaarheidsvereisten als die welke voorafgaand aan de schorsing of herroeping van kracht waren

2.4 Verlenging en vervanging.

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**

Huidige stand van ZORG-ID: Verlenging alleen mogelijk na herauthenticatie. In komende release(s) zal deze functie vereenvoudigd worden.	V	O	Rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, moet voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau.
De zorgaanbieder voert herauthenticatie uit op basis van de identiteitsdocumenten. Deze functies wordt nog vereenvoudigd op basis van de huidige ZORG-ID Smartcard **Dit is Kenmerkend voor ZORG-ID Smartcard**	V	O	Als voor verlenging of vervanging wordt uitgegaan van een geldig elektronisch identificatiemiddel, worden de identiteitsgegevens geverifieerd aan de hand van een gezaghebbende bron.

3. Authenticatie

Dit onderdeel is met name gericht op dreigingen die gepaard gaan met het gebruik van het authenticatiemechanisme. Het vermeldt de vereisten voor elk van de betrouwbaarheidsniveaus. In dit onderdeel wordt ervan uitgegaan dat de controles in overeenstemming zijn met de risico's op het desbetreffende niveau.

3.1 Authenticatiemechanisme

In onderstaande tabel worden de vereisten weergegeven voor het authenticatiemechanisme, door middel waarvan de natuurlijke persoon of rechtspersoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij.

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Binnen ZORG-ID wordt het elektronische identificatiemiddel (zoals een certificaat) cryptografisch gecontroleerd op authenticiteit	V	O	Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische

via digitale handtekeningen. De geldigheidsstatus van het certificaat wordt in real-time geverifieerd via OCSP of CRL. Pas na succesvolle validatie worden de gekoppelde persoonsidentificatiegegevens vrijgegeven.			identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd.
De persoonsgegevens worden opgeslagen conform verwerkingsovereenkomst getekend, afhankelijk van de locatie, tussen de zorgaanbieder en de softwareleverancier met VZVZ als subverwerker of tussen de zorgaanbieder.	V	O	Indien als onderdeel van het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, wordt die informatie beveiligd ter bescherming tegen verlies en schending, met inbegrip van offlineanalyse.
Het authenticatiemechanisme werkt op basis van public key infrastructure (PKI) infrastructuur en beveiligde verbindingen. VZVZ laat hiervoor audits uitvoeren en onderhoudt een DPIA.	O	V	Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel.
In het licht van dynamische authenticatie wordt de verificatie van het elektronische identificatiemiddel real-time en contextafhankelijk uitgevoerd. Dit betekent dat naast het controleren van de geldigheid van het certificaat (via OCSP/CRL). Alleen wanneer het middel technisch geldig is én de context voldoet aan vooraf gedefinieerde authenticatie-eisen, worden persoonsidentificatiegegevens vrijgegeven.	O	V	Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie.
Het authenticatiemechanisme (App, ID, Pincode, ZORG-ID platform) sluit misbruik uit door verschillende lagen van beveiliging	O	V	Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische

(verbindingen, lokale sleutels, HSM toegang, Gebruik persoonscertificaten).			identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel.
De software is geaudit op architectuur en werking, waardoor is verzekerd dat het zeer onwaarschijnlijk is dat de authenticatiemechanismen kunnen worden omzeild. Een PKI-smartcard (Public Key Infrastructure) wordt gebruikt voor veilige authenticatie, digitale handtekeningen en versleuteling. Wanneer zo'n kaart gecertificeerd is volgens Common Criteria EAL4+, biedt deze een hoog niveau van bescherming tegen vervalsingen en identiteitsdiefstal via het volgende mechanisme: *Veilige Sleutelopslag en Sleutelbeheer* • De privésleutels op de smartcard worden veilig opgeslagen en zijn beschermd tegen ongeautoriseerde toegang. • Sleutels worden gegenereerd en beheerd binnen een beveiligde omgeving, waardoor kopiëren of misbruik vrijwel onmogelijk is. *Sterke Authenticatieprotocollen* • PKI-smartcards gebruiken cryptografische challenge-response mechanismen voor authenticatie. • EAL4+ garandeert dat deze protocollen veilig zijn geïmplementeerd en bestand zijn	O	V	Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een hoog aanvalspotentieel.

tegen aanvallen zoals replay, man-in-the-middle en brute force. *Fysieke en Logische Sabotagebestendigheid* • EAL4+ gecertificeerde kaarten zijn getest op weerstand tegen fysieke en logische aanvallen. • Dit omvat bescherming tegen side-channel aanvallen zoals stroomanalyse of timingaanvallen, die gebruikt kunnen worden om identiteitssleutels te stelen. **Dit is kenmerkend voor de ZORG-ID Smartcard**			

4 *Beheer en organisatie*

Alle deelnemers die een dienst verlenen op het gebied van elektronische identificatie **in een grensoverschrijdende context** (hierna „aanbieders” genoemd) beschikken over gedocumenteerde methoden en beleid voor het beheer van informatiebeveiliging, benaderingen voor risicobeheersing en andere erkende controlemethoden, zodat zij de bevoegde bestuursorganen van de lidstaten op het gebied van stelsels voor elektronische identificatie garanties kunnen bieden dat in doeltreffende praktijken is voorzien. In onderdeel 2.4 wordt ervan uitgegaan dat alle vereisten/elementen in overeenstemming zijn met de risico's op het desbetreffende niveau.

ZORG-ID is een platform voor een Nederlands Authenticatie. Zorgaanbieders buiten Nederland kunnen geen URA verkrijgen. Mocht ZORG-ID in andere landen gebruikt gaan worden, zullen hiervoor aanvullende eisen worden gerealiseerd.

2.4.1 Algemene bepalingen

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
ZORG-ID beoogt binnen het Dezi-stelsel toegelaten te worden, waarbij het doel is dat uiteindelijk wordt voldaan aan betrouwbaarheidsniveau “hoog” conform eIDAS.	nvt	nvt	Aanbieders die een operationele dienst aanbieden die onder deze verordening valt, zijn een overheidsinstantie of een rechtspersoon die door het nationale recht van een lidstaat als zodanig wordt erkend, over een gevestigde organisatie

Op dit moment is ZORG-ID nog een privaat middel.			beschikt en volledig operationeel is op alle gebieden die voor de verlening van de diensten relevant zijn.
De zorgaanbieder houdt zich aan de wettelijke verplichtingen van het vaststellen van de identiteiten voor werknemers die binnen een zorgorganisatie werken.	V	O	De aanbieders voldoen aan al hun wettelijke verplichtingen in verband met het verrichten en leveren van de dienst, onder meer wat betreft de soorten informatie die mogen worden gevraagd, de wijze waarop het bewijs van de identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard.
VZVZ is verzekerd voor de bedrijfsrisico's en wordt gefinancierd door Zorgverzekeraars Nederland en het Ministerie van Volksgezondheid.	O	V	De aanbieders kunnen aantonen dat zij in staat zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen beschikken om hun activiteiten en de dienstverlening voort te zetten.
VZVZ heeft op grond van deze CPS afspraken met de zorgaanbieders gemaakt en heeft ook betrekkin op andere entiteiten waar diensten zijn uitbesteed, waardoor de zorgaanbieders hun verplichtingen kunnen nakomen	V	O	De aanbieders zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden.
ZORG-ID is conform Nederlands recht opgezet.	nvt	nvt	Stelsels voor elektronische identificatie die niet volgens nationaal recht zijn opgezet, moeten over een doeltreffend beëindigingsplan beschikken. Dat plan omvat voorzieningen voor de

			ordelijke stopzetting van de dienstverlening of de voortzetting daarvan door een andere aanbieder, voor de wijze waarop de betrokken autoriteiten en eindgebruikers worden ingelicht, alsook voor de wijze waarop de administratie wordt beschermd, bewaard en vernietigd overeenkomstig het voor het stelsel geldende beleid

2.4.2 Gepubliceerde mededelingen en informatie voor de gebruikers

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
De dienst wordt actueel beschreven op de website www.zorg-id.nl	O	V	Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring.
Procedures staan beschreven op de website www.zorg-id.nl	O	V	Er dient te worden voorzien in passend beleid en passende procedures om de gebruikers van de dienst tijdig en op betrouwbare wijze te informeren over elke wijziging van de beschrijving van de dienst, alle toepasselijke voorwaarden en de privacyverklaring
Support- en beheerprocedures zijn toegankelijk via ZORG-ID website.	O	V	Er dient te worden voorzien in passend beleid en passende procedures om verzoeken om informatie volledig en correct te beantwoorden

2.4.3 Beheer van informatiebeveiliging

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**	

VZVZ beschikt over het NEN-7510 certificaat. Zie verder www.zorg-id.nl	O	V	Er bestaat een doeltreffend beheerssysteem voor informatiebeveiliging dat zorg draagt voor het beheer en de beheersing van informatiebeveiligingsrisico's.	
VZVZ beschikt over het NEN 7510 certificaat. Zie overigens via www.zorg-id.nl	O	V	Het beheerssysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.	

2.4.4 Bijhouden van administratie

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
VZVZ beschikt over het NEN 7510 certificaat, waarbij alle vormen van procedures, informatiebeveiliging en gegevensbescherming. Zie voor meer info www.zorg-id.nl.	O	V	Relevante informatie wordt vastgelegd en bewaard met behulp van een doeltreffend documentenbeheersysteem, met inachtneming van de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring
ZORG-ID bevat alleen actuele data. De logging wordt bewaard volgens de wettelijke bewaartermijnen (in de systemen 6 maanden).	O	V	De gegevens moeten worden bewaard voor zover dat is toegestaan door het nationale recht of een andere nationale bestuurlijke regeling, en beschermd gedurende de termijn die noodzakelijk is met het oog op financiële controle en onderzoek van beveiligingsinbreuken; na afloop van de bewaringstermijn worden de gegevens veilig vernietigd.

2.4.5 Faciliteiten en personeel.

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**

Organisatie VZVZ is NEN7510 gecertificeerd. Haar onderaannemer / dienstverlener AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd VZVZ heeft een stelsel van waarborgen afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA/ verwerkersoverenkomst	O	V	Er zijn procedures om te waarborgen dat personeelsleden en sub contractanten voldoende zijn opgeleid en gekwalificeerd en dat zij ervaren zijn in de vaardigheden die vereist zijn voor de taken die zij vervullen.
Organisatie VZVZ is NEN7510 gecertificeerd. AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd VZVZ heeft een stelsel van waarborgen afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA/ verwerkersovereenkomst.	O	V	Er zijn voldoende personeelsleden en sub contractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures.
Organisatie VZVZ is NEN7510 gecertificeerd. AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd. VZVZ heeft een stelsel van waarborgen afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA/ verwerkersovereenkomst	O	V	De voor de dienstverlening gebruikte faciliteiten staan onder permanente controle en worden permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten.
Organisatie VZVZ is NEN7510 gecertificeerd. AET is ISO27001 / ISO9001/ EAL4+ gecertificeerd VZVZ heeft een stelsel van waarborgen afgesloten, d.m.v. arbeidsovereenkomsten en	O	V	De voor de dienstverlening gebruikte faciliteiten zijn zodanig ingericht dat de toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie beperkt is tot bevoegde

overeenkomsten met derden zoals DAP / SLA/ verwerkersovereenkomst			personeelsleden of subcontractanten.

2.4.6 Technische controles

ICM en ACM (identiteitscertificaatbeheerservice, attribuutcertificaatbeheer) worden geïmplementeerd met BlueX eID Management:

BlueX eID Management is gecertificeerd als een betrouwbaar systeem volgens CEN/TS 419261:2015 (Beveiligingseisen voor betrouwbare systemen die certificaten en tijdstempels beheren).

CA (Certificate Authority Service) wordt geïmplementeerd met behulp van de Ascertia CA-services: De Ascertia ADSS CA/PKI-server is gecertificeerd volgens Common Criteria (CC) Evaluation Assurance Level 4+ (EAL4+) met ALC_FLR.3 1.

RQSCD (Remote Qualified Signature Creation Device) De ADSS SAM Appliance is Common Criteria EAL4+ gecertificeerd, wat een hoog niveau van IT-beveiliging 1 biedt. Het voldoet aan Protection Profile EN 419 241-2, dat specifiek is ontworpen voor Remote Qualified Signature Creation Devices (QSCD's).

ZORG-ID smartcard: De SafeSign IC PKI-applet is Common Criteria EAL4+ gecertificeerd op (NXP) JCOP4 P71. Personalisatie van de ZORG-ID smartcard is geïmplementeerd in de ICM (zie ICM voor details).

HSM-systemen: Common Criteria EAL4+-certificering, eIDAS-beschermingsprofiel EN 419 221-5, eIDAS-beschermingsprofiel EN 419 241-2, eIDAS-artikel 30 en 31-naleving.

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Cryptografische beveiliging voor alle communicatie is in gericht om de veiligheid te garanderen. Persoonsgegevens die uitgewisseld worden door de infrastructuur zijn encrypt. De data op de servers zijn onderdeel van een DPIA (minimaal aanwezig én	O	V	Er is voorzien in proportionele controles ter beheersing van de risico's voor de veiligheid van de diensten, waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkte informatie worden beschermd.

beveiligd tegen ongeoorloofde toegang).			
De persoonsgegevens en gevoelige gegevens worden Cryptografisch beveiligd. Alle lijnen en verbindingen zijn beveiligd middels mutual TLS op basis van certificaten. Een Pentest op het gebruik van deze beveiliging is onderdeel van de waarborg.	O	V	De elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, worden beschermd tegen afluisteren, manipuleren en herafspelen.
Gebruik van HSM's Al het sleutel materiaal is per 'identiteit' opgeslagen in een HSM die alleen wordt geopend als aan de toegangsvoorwaarden wordt voldaan. Alleen de eigenaar kan bij dit materiaal.	O	V	De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, is beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is. Er wordt op toegezien dat dergelijk materiaal niet permanent in onversleutelde staat wordt opgeslagen.
De architectuur van ZORG-ID vereist hoge beveiliging. De procedures van monitoring werken 24*7 en onze DAP / SLA hebben garanties voor snelle respons bij incidenten. VZVZ heeft een stelsel van waarborgen rondom veiligheid afgesloten, d.m.v. arbeidsovereenkomsten en overeenkomsten met derden zoals DAP / SLA.	O	V	Er zijn procedures die waarborgen dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken.

Alle certificaten zijn opgeslagen in HSMs en de database(s) met identiteitsgegevens is beveiligd. Er vindt geen fysiek transport van sleutelmateriaal plaats. Verwijderen kan niet. Er is wel een CRL waarlangs het sleutelmateriaal geblokkeerd kan worden.	O	V	Alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, worden veilig opgeslagen, vervoerd en verwijderd.
De cryptografisch beveiliging van het sleutelmateriaal vindt plaats middels HSMs. Het management van de HSM's voldoet aan de Europese normen.	O	V	Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.

2.4.7 Compliance en audit

Invulling	**ZA**	**VZVZ**	**eIDAS (Informatieve Referentie)**
Er vinden driejaarlijkse audits plaats conform NEN 7510.	O	V	Er vinden periodieke onafhankelijke externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.

Bijlage 3: Definities en afkortingen

Bij de samenstelling van de definities van de gehanteerde begrippen zijn de volgende uitgangspunten gehanteerd:

- Er is in een aantal gevallen gekozen voor het gebruik van Engelstalige termen. Reden hiervoor is, dat er vaak geen correcte Nederlandse vertaling voor die Engelstalige term bestaat. Als een Nederlandstalig begrip naast een Engelstalig begrip wordt gebruikt met dezelfde betekenis, staan beide begrippen in de lijst (het meest gangbare begrip is in de lijst opgenomen direct gevolgd door de vertaling die dan cursief is weergegeven);
- Waar het gaat om 'PKI-termen' (PKI = Public Key Infrastructure) is zoveel mogelijk aangesloten bij de algemeen gehanteerde definities van de PKI voor de overheid en in de vakliteratuur over dit onderwerp.

De begrippenlijst bestaat uit drie kolommen: Afkorting, Begrip en Definitie. De sortering is alfabetisch en op de kolom 'Begrip'. In een aantal gevallen is direct na de definitie een toelichting gegeven en, indien van toepassing, de bron van de informatie; als scheiding is een witregel opgenomen.

Afkorting	Begrip	Definitie
AVG	Algemene verordening gegevensbescherming (AVG)	Sinds 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Deze verordening zorgt ervoor dat in de hele EU dezelfde privacywetgeving geldt.
	Betrouwbaarheidsniveau	Definieert het vertrouwen dat een systeem mag hebben in de digitale identiteit van een gebruiker. • Laag: minimale controles, bijvoorbeeld alleen een gebruikersnaam en wachtwoord. • Midden: extra verificatiestappen, zoals verificatie van officiële documenten of een eenmalige code • Hoog: Uitgebreide verificatie, bijvoorbeeld persoonlijk identificeren bij een LRA, gebruik van een smartcard, inclusief documentcontrole en soms biometrie.

CA	Certification Authority	Het onderdeel dat de ondertekening van de certificaten verzorgt en dat door eindgebruikers wordt vertrouwd.
CIBG	CIBG	Het CIBG is een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport, dat belast is met een aantal wettelijke uitvoeringstaken. Zie ook: www.cibg.nl
	Certificaat	Elektronische bevestiging die gegevens voor het verifiëren van een bepaalde persoon verbindt met gegevens over de vertrouwelijkheid en authenticiteit en/of elektronische handtekening en daarmee de identiteit van de persoon bevestigt. Een certificaat is een publiekelijk toegankelijk document dat is uitgegeven door een TSP en dat een aantal door die TSP gecontroleerde gegevens bevat. Een certificaat, bevat tenminste: a) de vermelding dat het certificaat als gekwalificeerd certificaat wordt afgegeven; b) de identificatie en het land van vestiging van de afgevende certificatiedienstverlener; c) de naam van de ondertekenaar; d) ruimte voor een specifiek attribuut van de ondertekenaar, dat indien nodig, afhankelijk van het doel van het gekwalificeerde certificaat, wordt vermeld; e) gegevens voor het verifiëren van de handtekening die overeenstemmen met de gegevens voor het aanmaken van de handtekening die onder controle van de ondertekenaar staan;

		f) vermelding van het tijdstippen van het begin en van het einde van de geldigheidsduur van het gekwalificeerde certificaat; g) de identiteitscode van het gekwalificeerde certificaat; h) de elektronische handtekening van de afgevende certificatiedienstverlener die voldoet aan de criteria van artikel 15a, tweede lid, onderdeel a tot en met d, van Boek 3 van het Burgerlijk Wetboek; i) eventuele beperkingen betreffende het gebruik van het gekwalificeerde certificaat, en j) eventuele grenzen met betrekking tot de waarde van de transacties waarvoor het gekwalificeerde certificaat kan worden gebruikt.
CPS	Certification Practice Statement	Een document dat de gevolgde procedures en getroffen maatregelen over alle aspecten van de dienstverlening beschrijft.
CRL	Certificate Revocation List	Een lijst van ingetrokken (= gerevoceerde) certificaten. De Certificate Revocation List (CRL) is openbaar toegankelijk en raadpleegbaar. De lijst is beschikbaar gesteld door en onder verantwoordelijkheid van .... De CRL is zelf ook elektronisch ondertekend door de CA van ....
ETSI	European Telecommunication Standard Institute	De ETSI is een onafhankelijk instituut op het gebied van standaardisatie voor telecommunicatie.
HSM	Hardware Security Module	Een middel dat de private sleutel(s) van systemen bevat deze sleutel(s) tegen compromittatie beschermt en elektronische ondertekening, authenticatie of ontcijfering uitvoert namens het systeem.

LRA	Local Registration Authority	Een organisatie of instantie die in een PKI-omgeving (Public Key Infrastructure) verantwoordelijk is voor het verifiëren van de identiteit van gebruikers en het initiëren van certificaataanvragen bij een Certificate Authority (CA).
PKI	Public Key Infrastructure	Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op asymmetrische sleutelparen. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.
RA	Registration Authority	Het onderdeel van het UZI-register dat de registratie werkzaamheden uitvoert ter verwerking van de certificaataanvragen.
SSCD/QSCD	Secure Signature Creation Device / Qualified Signature Creation Device	Een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld in artikel 18.17, eerste lid van de Telecommunicatiewet.
TSP	Trusted Service Provider	Een natuurlijk persoon of rechtspersoon die de certificaten afgeeft en/of andere diensten in verband met de elektronische handtekeningen, waaronder identiteit en vertrouwelijkheid, verleent. Het UZI-register is een TSP.
X.509	X.509	Dit is een elektronisch certificaat dat volgens een gestandaardiseerde structuur is opgebouwd