Certificate Policy/

Certificate Practice Statement

1. Inleiding

1.1 Achtergrond

VECOZO is het communicatiepunt voor ketenpartijen in de zorg die hun administratieve processen willen stroomlijnen en optimaliseren. Binnen het administratieve zorgdomein faciliteert VECOZO een digitale omgeving waarin de ketenpartijen snel, eenvoudig en veilig gegevens met elkaar kunnen uitwisselen. Onder meer zorgverzekeraars, zorgaanbieders en gemeenten maken gebruik van VECOZO-diensten, zoals voor het declaratieverkeer en de berichten van zorgtoewijzing.

De digitale omgeving van VECOZO wordt ontsloten met Digitale certificaten (hierna te noemen: certificaten). Een certificaat is een digitaal document dat bestemd is om op uw hardware te worden geïnstalleerd en waarmee wij voor gegevensuitwisseling via internet uw identiteit en authenticiteit vast kunnen stellen.
Een certificaat kan een persoonlijk certificaat zijn (voor één natuurlijk persoon), of een systeemcertificaat (voor gebruik met een webservice).

VECOZO verzorgt de uitgifte, het beheer en het intrekken van certificaten en het blokkeren van gebruikers voor onder andere zorgaanbieders, zorgverzekeraars, gemeenten en derde partijen.

1.2 Leeswijzer

Dit document is een gecombineerde Certificate Policy (CP) en Certificate Practice Statement (CPS). In dit document beschrijven we ons beleid en de procedures rond certificaatbeheer. Dit is van belang voor de gebruikers van onze certificaten.

Uitgeven van een dergelijk document is vereist vanuit WebTrust.

In lijn met WebTrust beschrijft dit document alle onderwerpen als genoemd in Internet X.509 Public Key Infrastructure Certificate Policy en Certification Practices Framework.

1.3 Gebruikersgemeenschap, beleids- structuur en toepassingsgebied

VECOZO treedt op als certificaatdienstverlener. Binnen VECOZO worden de rollen van Registration authority (RA) en Certification authority (CA) onderkend.

1.3.1 Registration authority (RA)

De RA registreert en valideert de certificaataanvragen en intrekkingsverzoeken. Nadat een aanvraag of intrekkingsverzoek is goedgekeurd en is geregistreerd, verstrekt de RA respectievelijk een opdracht tot certificaatgeneratie of tot intrekking aan de Certification authority.

De RA-functie wordt bij VECOZO uitgevoerd door de afdeling Support en Administratie onder verantwoordelijkheid van de manager Business.

1.3.2 Certification authority (CA)

De CA produceert, op verzoek van de RA, VECOZO-certificaten en geeft deze uit aan de eindgebruikers. Daarnaast is de CA verantwoordelijk voor de publicatie van de uitgegeven en ingetrokken certificaten.

Om de CA-diensten te kunnen leveren maakt VECOZO gebruik van de zogenaamde Private Managed PKI (mPKI) dienstverlening[1] van KPN NV (hierna KPN). Dit houdt in dat het technisch beheer van de CA en de directory is uitbesteed aan KPN.

Om de mPKI-dienstverlening te kunnen leveren maakt KPN gebruik van de diensten van een onderaannemer. De CA en de directory staan fysiek bij KPN opgesteld, waarmee VECOZO een contractuele relatie heeft.

[1] Een private mPKI betekent dat VECOZO beschikt over een eigen root-CA cer ficaat, dat niet is ondertekend door een andere CA, zoals bijvoorbeeld die van KPN.

1.3.3 Beleidsstructuur

VECOZO stelt een beleidsstructuur vast waarbinnen besluiten rond de certificaatdienstverlening kunnen of moeten worden genomen.

VECOZO kent een Policy Management Authority (hierna: PMA) en een Algemene Vergadering van Aandeelhouders (hierna: AvA). Het VECOZO Management Team (hierna: MT) treedt op als PMA. De PMA stelt het beleid en de normen vast voor de VECOZO-certificaatdienstverlening.

Voor onderstaande punten is instemming van de AvA van VECOZO vereist:

- Het voornemen om de VECOZO-certificaten voor andere doeleinden dan authenticatie en het plaatsen van digitale handtekeningen te gaan gebruiken (met andere woorden een uitbreiding van het toepassingsgebied).
- Het voornemen om de gebruikers- gemeenschap uit te breiden en/of aan te passen.

1.3.4 Gebruikersgemeenschap

VECOZO stelt een beperkte gebruikersgroep vast die VECOZO-certificaten kan aanvragen. Deze groep bestaat uit twee subgroepen.

De eerste groep bestaat uit de Contractanten en daaraan verbonden de Tekenbevoegd persoon, Hoofdcontactpersoon en Contactpersonen als representanten die een certificaat kunnen aanvragen.
Daarnaast kennen we gebruikers binnen een organisatie. Aanvragen hiervoor worden bij voorkeur via de Contactpersoon en het gebruikersbeheer via de VECOZO-website afgehandeld. De aanvrager wordt dan geauthentiseerd met het eigen certificaat.

- Een *Contractant* is:
  1 een eenmanszaak, personen- vennootschap of rechtspersoon binnen het zorgveld in Nederland, die diensten verleent in het kader van één of meerdere zorgwetten, en derhalve op een veilige, uniforme en digitale wijze gegevens uit wil wisselen met andere partijen in de zorg, of;
  2 een eenmanszaak, personen- vennootschap of rechtspersoon die in de uitoefening van een beroep of bedrijf zelf niet direct inhoudelijke zorg levert maar wel faciliterend is aan de onder i) genoemde partij en/of diens taken overneemt op grond van een of meerdere (verwerkers)overeenkomsten.

Ook Softwarepartijen en enkele overige -aan de zorg gerelateerde - instanties kunnen dus worden aangemerkt als Contractant.
Voor alle typen Contractanten die over een eigen certificaat willen beschikken geldt dat zij een overeenkomst met VECOZO moeten aangaan.

- Een *Tekenbevoegde* is namens de Contractant gerechtigd om een overeenkomst (met VECOZO) te tekenen. Wie dit is, ligt vast in het Handelsregister (KvK).
- Een *Hoofdcontactpersoon* is een door de Contractant gemachtigde medewerker, met een arbeidsrelatie tot de organisatie van Contractant. Deze is het eerste aanspreekpunt voor VECOZO bij verstrekking van informatie (relatiedagen/nieuwsbrieven), incidenten en informatiebeveiliging. De Hoofdcontactpersoon heeft specifieke rechten en plichten.
  VECOZO bepaalt hoeveel het maximum aantal Hoofdcontactpersonen is en op welk organisatieniveau deze worden aangesteld.
- Een *Contactpersoon* heeft dezelfde rechten en plichten als de Hoofdcontactpersoon, maar dan voor een specifiek onderdeel van de onderneming van Contractant (indien van toepassing). Zoals bijvoorbeeld een vestiging. Ook de Contactpersoon heeft een arbeidsrelatie met de organisatie in kwestie.
  De Contactpersoon kan (vooralsnog) méér via Gebruikersbeheer op onze website regelen dan de Tekenbevoegde en de Hoofdcontactpersoon. Het heeft dan ook de voorkeur om zoveel mogelijk via de Contactpersoon op vestigingsniveau te regelen.
- Een *Gebruiker* is een natuurlijke persoon die door middel van een certificaat gebruik kan maken van de Diensten van VECOZO.
  Doorgaans werkt een Gebruiker in (loon)dienst van de Contractant. Het is echter ook mogelijk een certificaat aan te vragen voor Gebruiker die géén deel uitmaakt van de eigen onderneming. Zoals in het geval van inhuur of uitbesteding. Dit is echter uitdrukkelijk onder de eigen verantwoordelijkheid van de Contractant.

Een natuurlijk persoon kan meerdere rollen hebben. Zo kan een Tekenbevoegde ook een Gebruiker zijn.

De tweede groep afnemers zijn de vertrouwende partijen:

- Een Vertrouwende partij is een partij die handelt in vertrouwen op een door VECOZO uitgegeven certificaat middels de dienst VECOZO Single Sign On (hierna: SSO), maar niet noodzakelijk ook Contractant is conform bovenstaande definitie.
- Een Vertrouwende partij gaat een separate overeenkomst aan met VECOZO. VECOZO is voor de door haar aangeboden portaaldiensten zelf ook een Vertrouwende partij.

VECOZO bepaalt het aantal certificaten dat Contractanten en Vertrouwende partijen mogen afnemen.

1.3.5 Toepassingsgebied

VECOZO stelt een beperkt toepassingsgebied voor door haar uitgegeven certificaten vast. Het gebruik van de door VECOZO uitgegeven certificaten is beperkt tot het plaatsen van digitale handtekeningen en authenticatiedoeleinden voor het verkrijgen van toegang tot de Diensten van VECOZO, of voor van het verkrijgen van toegang tot diensten van derden via SSO.

Ten behoeve van het hierboven beschreven toepassingsgebied biedt VECOZO de volgende twee typen certificaten:
Persoonlijk certificaat: Een digitaal certificaat dat is verbonden aan een specifieke Gebruiker voor authenticatie van de betreffende Gebruiker.
Systeemcertificaat: een digitaal certificaat dat is verbonden aan applicaties of systemen van Contractant voor het gebruik van webservices. Het Systeemcertificaat wordt tevens gebruikt voor de Authenticatie van Contractant.

De bepalingen in deze CP/CPS zijn op alle bovengenoemde typen certificaten van toepassing. Indien een bepaling slechts op één type certificaat van toepassing is, dan is dat nadrukkelijk aangegeven.

1.4 Contactgegevens

Het actuele post- en bezoekadres van VECOZO, alsook telefoonnummer en meer informatie over het indienen van incidenten en vragen, vindt u op www.VECOZO.nl.

2. Algemene bepalingen

2.1 Verplichtingen

VECOZO stelt voor zichzelf en de entiteiten binnen de gebruikersgemeenschap vast wat de verplichtingen, verantwoordelijkheden en aansprakelijkheden zijn. Hierbij baseert VECOZO zich op toepasselijke wet- en regelgeving, maar ook op het *Trust Service Principles and Criteria for Certification Authorities Version 2.0*-normenkader.

In deze paragraaf worden de verplichtingen van de gebruikersgemeenschap van de VECOZO-certificaatdienstverlening, gespecificeerd.

2.1.1 Verplichtingen van VECOZO

VECOZO legt zich de volgende verplichtingen op:

- De VECOZO CA en RA opereren conform de in deze CP/CPS gestelde eisen, procedures en maatregelen;
- VECOZO heeft een risicoanalyse uitgevoerd op basis waarvan een informatiebeveiligingsbeleid is opgesteld en beveiligingsmaatregelen zijn getroffen;
- VECOZO heeft passende overeenkomsten afgesloten met bij de certificaatlevenscyclus betrokken leveranciers;
- Deze CP/CPS is in elektronische vorm te vinden op het publieke deel van de website van VECOZO (https://www.vecozo.nl). De CP/CPS wordt tenminste jaarlijks door VECOZO beoordeeld op actualiteit.

2.1.2 Verplichtingen van de Contractanten

VECOZO legt de Gebruikersgemeenschap de volgende verplichtingen op:

- Contractanten (in de rol van Tekenbevoegd persoon, (Hoofd)contactpersoon, Gebruiker of ICT-Beheerder) komen het in deze CP/CPS bepaalde na;
- Tekenbevoegd persoon, (Hoofd)Contactpersoon, Gebruiker en ICT-Beheerder zullen accurate, actuele en volledige informatie verstrekken aan VECOZO;
- De Tekenbevoegde wijst binnen zijn organisatie een beperkt aantal Hoofdcontactpersonen aan (door VECOZO te bepalen hoeveel het maximum aantal is en op welk organisatieniveau zij worden aangesteld);
- Indien zich wijzigingen voordoen van de in het certificaat opgenomen informatie zullen de Tekenbevoegd persoon

en/of Hoofdcontactpersoon en/of Contactpersoon VECOZO hiervan direct op de hoogte stellen;
- Contractanten treffen passende beveiligingsmaatregelen om zo de veiligheid van het certificaat te kunnen garanderen;
- Hoofdcontactpersonen dienen bij VECOZO aan te geven of zij een ICT-Beheerder (derde) betrokken hebben bij de werkzaamheden waarvoor zij het VECOZO certificaat gebruiken;
  - In het geval van ondersteuning bij de uitvoering wordt vastgelegd wie de ICT-Beheerder is, zodat VECOZO die partij te woord kan staan bij eventuele vragen en opmerkingen over certificaten. VECOZO ondersteunt de ICT-Beheerder niet bij inhoudelijke vragen over de diensten.
- Contractanten mogen certificaten alleen gebruiken voor de aangegeven gebruiksdoeleinden zoals is gespecificeerd in het toepassingsgebied in deze CP/CPS;
- Certificaatgegevens (pincode en gebruikersnummer) voor het installeren van het Persoonlijke certificaat worden door de Contractant uitsluitend aan de Gebruiker beschikbaar gesteld;
- Het Systeemcertificaat wordt uitsluitend aan de Contractant ter beschikking gesteld;
- Contractant neemt redelijke zorg in acht om te voorkomen dat de bij het VECOZO-certificaat behorende private sleutel onbevoegd wordt gebruikt. Dit betekent dat Contractant zich verplicht zodanig adequate technische en organisatorische maatregelen te treffen dat de vereiste vertrouwelijkheid van de via VECOZO ontsloten (persoons)gegevens is gewaarborgd. Hierbij moet ten minste gedacht worden aan maatregelen als:
  - een goed beveiligd (“gehardend”) besturingssysteem, dat bovendien is voorzien van actuele beveiligingspatches;
  - een firewall;
  - anti-malware-software voorzien van actuele updates;
  - schermbeveiliging bij inactiviteit van een werkstation.

  Daarnaast registreert Contractant op verzoek van VECOZO de (reeks van) IP-adressen bij het Systeemcertificaat. VECOZO voert hierop een controle uit bij de aanroep van diensten[2];
- Contractant zal meewerken aan een beveiligde toegangsregistratie en -controle, en dat uitsluitend de Gebruiker gebruik mag maken van de bij het certificaat behorende private sleutel waarmee toegang kan worden verkregen tot de VECOZO-diensten en daarmee samenhangend de betreffende (persoons)gegevens;
- In het geval van mogelijke onregelmatigheden zoals verlies of compromitteren van de private sleutel of van de door VECOZO aangeboden Diensten en gegevens, moet VECOZO zo snel mogelijk, doch uiterlijk binnen 24 uur, op de hoogte worden gebracht;
- Contractant neemt kennis van het feit dat activiteiten waarbij gebruik wordt gemaakt van de certificaten in de diensten gelogd worden, voor preventie en detectie van incidenten en fraude.

Rechten en oneigenlijk gebruik
- Rechten zijn gelaagd – een Tekenbevoegde heeft alle rechten die een Hoofdcontactpersoon heeft (en meer), een Hoofdcontactpersoon heeft alle rechten die een Contactpersoon heeft (en meer).
- De rechten van een Gebruiker staan hier los van – dus een Tekenbevoegd persoon, een Hoofdcontactpersoon of een Contactpersoon kan óók een Gebruiker zijn.
- Het recht op gebruik van een certificaat is niet overdraagbaar en mag niet aan derden ter beschikking worden gesteld. Overdracht wordt gezien als oneigenlijk gebruik en kan aanleiding zijn om een certificaat in te trekken.
  - In het geval van een Persoonlijk certificaat mag het certificaat niet aan andere natuurlijke personen worden overgedragen.
  - In het geval van het Systeemcertificaat mag het niet aan andere eenmanszaken, personenvennootschappen en/of (rechts)personen ter beschikking worden gesteld. Dit tenzij VECOZO hiervoor uitdrukkelijk schriftelijk toestemming heeft gegeven. Indien VECOZO constateert dat in strijd met dit lid is gehandeld, handelt Contractant in strijd met de CP/CPS en behoudt VECOZO zich het recht voor het certificaat per direct in te trekken en

[2] Hiervan kan alleen afgeweken worden mits aantoonbaar is dat het op geen enkele wijze mogelijk is (reeksen van) IP-adressen te registreren. In dat geval wordt een alternatieve afspraak overeen gekomen tussen Contractant en VECOZO.

overige passende maatregelen te treffen die VECOZO nodig acht.

Machtigingen

- De Hoofdcontactpersonen zijn door de Tekenbevoegde persoon gemachtigd om:
  - Naar VECOZO het eerste aanspreekpunt te zijn bij verstrekking van informatie(relatiedagen/nieuwsbrieven) en incidenten of datalekken);
  - Contactpersonen te identificeren, aan te vragen, te wijzigen;
  - Toestemmingsverklaringen af te geven en in te trekken aan, onder andere maar niet uitsluitend, tussenpartijen.
- De Contactpersoon is gemachtigd om:
  - Gebruikers te identificeren;
  - aanvragen in te dienen om certificaten voor Gebruikers aan te vragen, te wijzigen, te (de)blokkeren en/of in te trekken;
  - Autorisaties te wijzigen;
    Toestemmingsverklaringen af te geven en in te trekken aan onder andere maar niet uitsluitend tussenpartijen;
  - (Reeks van) IP-adressen te registreren bij het Systeemcertificaat.

- Aanvragen hiervoor worden bij voorkeur via de Contactpersoon en het gebruikersbeheer via de VECOZO-website afgehandeld. De aanvrager wordt dan geauthentiseerd met het eigen certificaat. De Tekenbevoegde en de Hoofdcontactpersoon kunnen deze wijzigingen ook doorvoeren, echter dit dient via een aanvraag van het webformulier te gebeuren.

2.1.3 Verplichtingen van Vertrouwende partijen

De verplichtingen van Vertrouwende partijen, wanneer deze in redelijkheid willen kunnen vertrouwen op een certificaat, zijn:

- Het nakomen van de verplichtingen uit deze CP/CPS;
- De geldigheid of intrekking van het certificaat verifiëren op basis van actuele informatie over intrekking, zoals beschikbaar wordt gesteld aan de Vertrouwende partij;
- Kennis te nemen van alle beperkingen betreffende het gebruik van het certificaat, waarvan de Vertrouwende partij op de hoogte is gebracht;
- De digitale handtekening van certificaten te verifiëren;
- Alle overige voorzorgsmaatregelen te nemen die zijn voorgeschreven in eventuele overeenkomsten en gebruiksvoorwaarden.

2.2 Aansprakelijkheid en verantwoordelijkheid van VECOZO

De aansprakelijkheid van VECOZO is vastgelegd in de overeenkomsten tussen VECOZO en Contractanten, dan wel VECOZO en Vertrouwende partijen. Hetzelfde geldt voor geldigheid en toepasselijkheid, geschillenbeslechting en tarieven.
Op deze overeenkomsten en dienstverlening is het Nederlands recht van toepassing.

2.3 Financiële verantwoordelijkheid

Partijen welke vertrouwen op certificaten uitgegeven door VECOZO vrijwaren VECOZO van elke financiële verplichting, die zou kunnen voortvloeien uit het gebruik van de certificaten en/of het handelen van VECOZO.

Uitgifte van certificaten maakt VECOZO en haar deelorganisaties geen agent, zaakwaarnemer, gevolmachtigde of andere vertegenwoordiger van de Contractant, of Vertrouwende partijen.

2.4 Audit

2.4.1 Object van onderzoek

Alle aspecten van de VECOZO-certificaatdienstverlening worden tijdens een audit door een derde partij beoordeeld. De overige door VECOZO aangeboden diensten en de algemene informatiebeveiliging worden in een separate audit beoordeeld.

2.4.2 Normenkader en auditorganisatie

Voor de audit wordt het *Trust Service Principles and Criteria for Certification Authorities Version 2.0*[2] *als normenkader gehanteerd.*

[2] www.Webtrust.org

VECOZO laat door een externe auditor een onderzoek tegen deze WebTrust-standaard uitvoeren. De audit moet worden uitgevoerd door een auditor die gerechtigd is om formele WebTrust-onderzoeken uit te voeren en een WebTrust-webzegel te verstrekken. De auditor zal op geen enkele wijze verbonden zijn aan VECOZO.

Voor de audit van de informatiebeveiliging en de gegevensverwerking van de diensten van VECOZO wordt door een externe auditor een specifiek normenkader gehanteerd.

2.4.3 Consequenties resultaten audit

Indien tijdens de audits tekortkomingen worden gesignaleerd, zal het VECOZO-management zo spoedig mogelijk correctieve maatregelen treffen en zullen deze maatregelen alsnog door de auditor worden beoordeeld.

2.4.4 Bekendmaking resultaten audit

Indien de WebTrust-audit is afgerond, kan op de website van VECOZO op hoofdlijnen inzicht worden verkregen in de resultaten van de WebTrust-audit door op het WebTrust-zegel te klikken.

2.5 Vertrouwelijkheid

Binnen de VECOZO-certificaatdienstverlening wordt onderstaande informatie vertrouwelijk behandeld:

- *Administratieve gegevens met betrekking tot een aanvraag of verlenging van een certificaat.* Alle gegevens die door of over de Tekenbevoegde, Hoofdcontactpersoon, Contactpersoon en Gebruiker worden verstrekt. Deze gegevens worden bijvoorbeeld tijdens een aanvraag voor een certificaat aan VECOZO verstrekt.
- *Gegevens met betrekking tot intrekking van een certificaat.* Alle gegevens die worden verschaft en vastgelegd ten aanzien van verzoeken tot intrekking van een certificaat. Deze gegevens worden bijvoorbeeld tijdens het indienen van een verzoek tot intrekking van een certificaat aan VECOZO verschaft.

VECOZO leeft bij de verwerking van deze persoonsgegevens de AVG na. Toepasselijke technische en organisatorische maatregelen zijn genomen tegen ongeautoriseerde of onwettige verwerking van persoonsgegevens en tegen onvoorzien verlies, vernietiging of beschadiging van persoonsgegevens.

Op de website van VECOZO is de VECOZO Privacy Statement gepubliceerd. Deze geeft inzicht in de wijze waarop VECOZO persoonsgegevens verwerkt en beschermt.

2.6 Intellectuele eigendomsrechten

De intellectuele eigendomsrechten van de door VECOZO uitgegeven certificaten en de VECOZO CP/CPS berusten bij VECOZO of diens ingeschakelde leverancier(s).

3. Identificatie en authenticatie

VECOZO heeft beleid vastgesteld omtrent identificatie en authenticatie van de entiteiten binnen de gebruikersgemeenschap.

3.1 Identificatie

3.1.1 Identificatie en authenticatie van een Contractant

VECOZO geeft certificaten uit aan Gebruikers (Persoonlijk certificaat) en/of systemen (Systeemcertificaat) die zijn gekoppeld aan een Contractant. Contractant sluit hiertoe eerst een overeenkomst met VECOZO. VECOZO verifieert eerst of de Contractant gerechtigd is gebruik te maken van de (certificaat)diensten van VECOZO.

Om de authenticiteit van de Contractant vast te stellen, vergelijkt VECOZO onder andere de informatie die door de aanvrager is verstrekt met het AGB-bestand of UZOVI-bestand van Vektis en het handelsregister van de Kamer van Koophandel. Indien het om een partij gaat die niet in Vektis wordt geregistreerd maar wel recht heeft op gebruik van de VECOZO-diensten, verifieert VECOZO de aangedragen informatie in het handelsregister van de Kamer van Koophandel.

Wanneer een validatieprocedure niet met succes kan worden afgerond, wijst VECOZO de aanvraag af en worden geen certificaten verstrekt. De Contractant wordt dan meteen op de hoogte gebracht van de mislukte validatie, onder vermelding van de reden van de mislukking. De Contractant kan als gewenst opnieuw een aanvraag indienen.

3.1.2 Identificatie en authenticatie van een Tekenbevoegd persoon

Voor de identificatie van een Tekenbevoegde persoon wordt door VECOZO het Handelsregister van de Kamer van Koophandel gecontroleerd. De Tekenbevoegd persoon dient zich richting VECOZO te legitimeren.

Voor de identificatie en authenticatie van een Tekenbevoegd persoon dienen de volgende gegevens te worden aangeleverd:

- Volledige voorna(a)m(en)
- Voorletters;
- Tussenvoegsels;
- Achternaam;
- Geboortedatum
- Geslacht;
- Telefoonnummer;
- Persoonlijk (zakelijk) e-mail adres.

Identificatie van Tekenbevoegde vindt plaats middels een proces dat een passend beveiligingsniveau heeft. VECOZO streeft er naar meerdere processen te bieden. Ieder proces is voldoende beveiligd op het vereiste niveau van het EIDAS framework.

Meer informatie over de actuele processen staat op www.VECOZO.nl. In een identificatie proces kán worden gevraagd om het tonen van een geldig legitimatiebewijs (paspoort, Nederlandse identiteitskaart, ID-kaart of paspoort uit een EER-land of een Nederlands vreemdelingendocument).

3.1.3 Identificatie en authenticatie van een Hoofdcontactpersoon

De Tekenbevoegde geeft namens de Contractant één of meerdere Hoofdcontactpersonen op die namens de Contractant het gebruikersbeheer kunnen coördineren. Deze Contactpersonen dienen zich naar VECOZO te legitimeren op dezelfde manier als de Tekenbevoegden.

3.1.4 Identificatie en authenticatie van een Contactpersoon

De Hoofdcontactpersoon benoemt de Contactpersonen in een organisatie. De Hoofdcontactpersoon is dan ook verantwoordelijk voor het correct identificeren van deze Contactpersonen.

Hoofdcontactpersonen kunnen daarna certificaten voor Contactpersonen aanvragen. De aanvrager is verantwoordelijk voor het proces waarin de identificatie van deze Contactpersonen plaats vindt.

3.1.5 Identificatie en authenticatie van een Gebruiker

De Contactpersoon beheert de Gebruikers in een organisatie. De Contactpersoon is dan ook verantwoordelijk voor het correct identificeren van deze Gebruikers.
Contactpersonen kunnen daarna certificaten voor Gebruikers aanvragen. De aanvrager is verantwoordelijk voor het proces waarin de identificatie van deze Gebruiker plaats vindt.

3.1.6 Een certificaat aanvragen

De volgende rollen kunnen Gebruikers aanmelden en zo certificaten aanvragen:

- Een Tekenbevoegde;
- Een Hoofdcontactpersoon;
- Een Contactpersoon.

Aanvragen worden bij voorkeur via de Contactpersoon en het gebruikersbeheer via de VECOZO-website afgehandeld. De aanvrager wordt dan geauthentiseerd met het eigen certificaat.

Aanvragen door een Tekenbevoegde, Hoofdcontactpersoon of Contactpersoon kunnen ook middels een papieren stroom worden afgehandeld. Zie voor dat proces www.VECOZO.nl.

3.2 Een certificaat registreren

Alle Gebruikers zijn zelf verantwoordelijk voor het genereren, installeren en vernieuwen van hun certificaat. Ook naamgeving gebeurt, binnen de door VECOZO bepaalde kaders, door Gebruikers.

3.2.1 Soorten naamformaten

Een Gebruiker kan bij het installeren van een persoonlijk certificaat zelf een certificaatnaam ingeven, welke als ’common name’ wordt getoond in het veld ‘subject’ van het betreffende certificaat. Zie hiervoor paragraaf 3.2.3.
Bij een systeemcertificaat wordt in het subject-veld het certificaatnummer opgenomen. Hiervoor wordt verwezen naar hoofdstuk 6 van deze CP/CPS.

3.2.2 Noodzaak voor betekenisvolle namen

Gebruiker hoeft tijdens het installeren van een certificaat geen betekenisvolle naam op te geven. Op basis van de "common name" in het veld "subject" in het certificaat kan VECOZO de identiteit van de Gebruiker vaststellen. Dit geldt niet voor systeemcertificaten omdat dat dit type certificaat niet persoonsgebonden is. Hierbij kan VECOZO op basis van de "common name" de Contractant identificeren.

3.2.3 Uniciteit van namen

VECOZO waarborgt zoveel mogelijk dat een 'common name' in het veld 'subject' slechts eenmaal wordt gebruikt, zodat iedere Gebruiker een unieke naam heeft binnen de VECOZO-gebruikersgemeenschap. Om uniciteit zoveel mogelijk te waarborgen, wordt de 'common name' in het 'subject' van certificaten op onderstaande wijze opgebouwd:

Pos. 1 t/m 7:	Door de gebruiker zelf gekozen karakters. Standaard wordt hier in hoofdletters de eerste voorletter geplaatst plus de eerste zes letters van de achternaam. Als de achternaam korter dan zes karakters is, worden er geen spaties geplaatst.
Pos. 8:	Koppelstreepje.
Pos. 9 t/m 15:	Dagnummer in cijfers, waar nodig een voorloopnul, plus de afkorting van de maand in hoofdletters (JAN, FEB, MRT, APR, MEI, JUN, JUL, AUG, SEP, OKT, NOV, DEC), plus het jaartal van waarin het certificaat gaat verlopen, weergegeven in twee cijfers.
Pos. 16:	Koppelstreepje.
Pos. 17:	Uniek oplopend volgnummer beginnend bij 1, oplopend met 1 (enkel wanneer het certificaat niet direct succesvol kan worden opgehaald).

De "common name" van het systeemcertificaat wordt als volgt opgebouwd:

Pos. 1 t/m 14:	Veertien cijferig gebruikers-nummer. Niet aan te passen door de gebruiker.
Pos. 15:	Koppelstreepje.
Pos. 16 t/m 22:	Dagnummer in cijfers, waar nodig een voorloopnul, plus de afkorting van de maand in hoofdletters (JAN, FEB, MRT, APR, MEI, JUN, JUL, AUG, SEP, OKT, NOV, DEC), plus het jaartal van waarin het certificaat gaat verlopen, weergegeven in twee cijfers.
Pos. 23:	Koppelstreepje.
Pos. 24:	Uniek oplopend volgnummer beginnend bij 1, oplopend met 1 (enkel wanneer het certificaat niet direct succesvol kan worden opgehaald).

3.2.4 Methode om het bezit van de private sleutel aan te tonen

De Gebruiker genereert zelf zijn private sleutel. Bij de generatie dient de Gebruiker gebruik te maken van een betrouwbaar systeem en de noodzakelijke voorzorgsmaatregelen, zoals beschreven in paragraaf 2.1.2 te nemen om inbreuk, verlies, openbaarmaking, wijziging of onbevoegd gebruik van de geheime sleutel te voorkomen. Tijdens het aanvraagproces dient de Gebruiker aan te tonen dat hij beschikt over de private sleutel die behoort bij de publieke sleutel die ter ondertekening wordt aangeboden. Door gebruik te maken van de mPKI-oplossing is technisch middels een challenge gewaarborgd dat de Gebruiker over de juiste private sleutel beschikt.

3.3 Certificaatvernieuwing

VECOZO heeft beleid opgesteld voor zowel het routinematig als niet-routinematig "vernieuwen van certificaten".
Onder "vernieuwen van certificaten" verstaat VECOZO het geautomatiseerd toekennen van een nieuw certificaat met een volledige geldigheidsduur (zie paragraaf 5.4.1), zonder dat een Gebruiker hiervoor een nieuwe aanvraag in hoeft te dienen.
Bij het vernieuwingsproces genereert de Gebruiker een nieuw sleutelpaar en wordt geautomatiseerd een nieuw certificaat toegekend, waarbij het oude certificaat geautomatiseerd wordt ingetrokken. Strikt genomen wordt de geldigheidsduur van een bestaand certificaat dus niet aangepast.

3.3.1 Routinematige vernieuwing

Het vernieuwen van een certificaat voor het aflopen van de geldigheidsduur ervan wordt beschouwd als routinematige vernieuwing. VECOZO stelt de Gebruiker minimaal één

maand voor het aflopen van de geldigheidsduur van het certificaat hiervan op de hoogte door middel van het versturen van een e-mail aan de Gebruiker op een vooraf geregistreerd e-mailadres.

De Gebruiker kan vervolgens op de website van VECOZO zijn certificaat vernieuwen. Hiertoe krijgt de Gebruiker instructies van VECOZO. Tijdens de vernieuwing wordt de authenticiteit van de Gebruiker vastgesteld. Bij persoonlijke certificaten gebeurt dit door de Gebruiker in te laten loggen, bij systeemcertificaten gebeurt dit door de Gebruiker zowel het certificaat als de pincode aan te laten bieden. Tijdens het vernieuwingsproces moet altijd een nieuw sleutelpaar worden gegenereerd en een nieuw certificaat worden aangemaakt. Het is niet mogelijk om de geldigheidsduur van een certificaat te verlengen.

3.3.2 Niet-routinematige vernieuwing

Het vernieuwen van een certificaat na intrekking van een certificaat of wijziging van de certificaatgegevens wordt beschouwd als niet-routinematige vernieuwing. In deze gevallen kan een certificaat vernieuwd worden door het opnieuw ophalen en installeren van een certificaat middels de reeds bekende certificaatgegevens (pincode en gebruikersnummer). Indien de certificaatgegevens niet meer voorhanden zijn dan kunnen deze opnieuw aangevraagd worden.

Voor een persoonlijk certificaat kan dit door de Gebruiker, (Hoofd)Contactpersoon of Teken-bevoegde of ICT-Beheerder worden gedaan. De gegevens van een systeemcertificaat kunnen door de (Hoofd)Contactpersoon en Tekenbevoegde worden opgevraagd. De gegevens worden conform de procedure voor certificaatuitgifte verstrekt.

In het geval van niet-routinematige vernieuwing moet altijd een nieuw sleutelpaar en een nieuw certificaat worden aangemaakt.

3.4 Verzoeken tot (de)blokkering

VECOZO heeft beleid opgesteld voor het blokkeren van Gebruikers en welke vereisten daarbij aan authenticatie worden gesteld. Indien een Gebruiker wordt geblokkeerd, kan deze het certificaat niet meer gebruiken om te authentiseren. Het certificaat wordt niet op de Certificate Revoke List geplaatst. Een blokkade van een gebruiker kan ook weer opgeheven worden.

3.4.1 Authenticatie van (de)blokkerings- verzoeken

In uitzonderlijke gevallen kan de VECOZO RA besluiten een Gebruiker al dan niet tijdelijk te (de)blokkeren, waarna deze het certificaat niet meer kan gebruiken om bij VECOZO te authentiseren. Het is aan de VECOZO RA om in een dergelijke situatie een voor dat moment geschikte authenticatiemethode te kiezen.
Indien een Gebruiker geblokkeerd wordt, ontvangen de Gebruiker en de Contactpersoon of Hoofdcontactpersoon hier een bericht van. Voor instanties waarvan de Contactpersonen toegang hebben tot Gebruikersbeheer is het mogelijk om via Gebruikersbeheer een Gebruiker te deblokkeren.

3.5 Verzoeken tot intrekking

VECOZO heeft beleid opgesteld voor het intrekken van certificaten en welke vereisten daarbij aan authenticatie worden gesteld.
Wanneer een certificaat wordt ingetrokken, wordt deze onherroepelijk op de CRL geplaatst. Het certificaat is daarmee noch voor VECOZO-diensten, noch voor diensten van andere Vertrouwende partijen nog te gebruiken. Nadat een certificaat is ingetrokken, kan dit niet meer opnieuw geldig worden verklaard.

3.5.1 Authenticatie bij intrekkingsverzoeken

Intrekkingsverzoeken dienen gedaan te worden door de Tekenbevoegde, (Hoofd)Contactpersoon, Gebruiker of ICT-Beheerder.

Dergelijke verzoeken worden bij voorkeur door de Contactpersoon gedaan via het gebruikersbeheer via de VECOZO-website. De aanvrager wordt dan geauthentiseerd met het eigen certificaat.

Intrekkingsverzoeken kunnen ook middels een papieren stroom worden afgehandeld, zie voor dat proces www.VECOZO.nl.

4. Operationele eisen

4.1 Aanvraag van certificaten

Aanvragen worden bij voorkeur via de Contactpersoon en het gebruikersbeheer via de VECOZO-website afgehandeld. De aanvrager wordt dan geauthentiseerd met het eigen certificaat.

Aanvragen door een Tekenbevoegde of (Hoofd)Contactpersoon kunnen ook middels een papieren stroom worden afgehandeld. Zie voor dat proces www.VECOZO.nl.

VECOZO controleert de aanvraag voordat de Gebruiker definitief aan wordt gemaakt.

4.2 Uitgifte van certificaten

VECOZO ziet er op toe dat de certificaten op veilige wijze uitgegeven worden om de authenticiteit ervan te handhaven. De procedure voor het uitgeven van certificaten is op een veilige wijze verbonden met de daarbij behorende registratieprocedure, waartoe ook de toelevering behoort van het sleutelpaar dat door de Gebruiker wordt gegenereerd.

VECOZO stuurt de gegevens die benodigd zijn om een certificaat te installeren altijd via gescheiden kanalen naar de aanvrager. Hierbij wordt gebruik gemaakt van de al bij VECOZO bekende gegevens. Bij de initiële aanvraag worden de certificaatgegevens per brief en e-mail verstuurd. Bij vervolgaanvragen via de website kunnen de gegevens van de aanvrager ook deels via de VECOZO-berichtenbox en deels via e-mail worden verstrekt. Bij schriftelijke vervolgaanvragen gebeurt dit per brief of via de VECOZO-berichtenbox in combinatie met een e-mail.

De aanvragers zijn zelf verantwoordelijk voor de interne distributie van de gegevens die benodigd zijn om certificaten te installeren.

VECOZO kan naar eigen goeddunken weigeren een certificaat uit te geven aan eenieder zonder dat dit leidt tot enige vorm van aansprakelijkheid of verantwoordelijkheid voor enige schade of onkosten die het gevolg zijn van een dergelijke weigering.

VECOZO zorgt ervoor dat:

- de door de aanvragers verstrekte gegevens op correcte wijze aan het certificaat worden gekoppeld. Zodra een certificaat is uitgegeven, vervalt echter de plicht van VECOZO om de juistheid van de informatie in een certificaat te (blijven) bewaken en onderzoeken;
- de certificaataanvraag door haar is goedgekeurd en dat adequate validatie heeft plaatsgevonden;
- het certificaat voldoet aan alle in deze CP/CPS gestelde materiële eisen.

4.3 Acceptatie van certificaten

Een Gebruiker wordt geacht een certificaat te hebben geaccepteerd nadat het certificaat door hem is geïnstalleerd op de werkplek.
Door acceptatie van een uitgegeven certificaat verklaart de Gebruiker tegenover VECOZO, alsmede tegenover allen die redelijkerwijs vertrouwen op de informatie in het certificaat, dat gedurende de volledige geldigheidsduur van het certificaat:

- geen enkele onbevoegde persoon toegang heeft gehad tot de geheime sleutel van de gebruiker;
- alle gegevens die de Gebruiker aan VECOZO heeft verstrekt ten behoeve van de onder deze CP/CPS vallende diensten juist en volledig zijn;
- alle in het certificaat verwerkte gegevens juist en volledig zijn;
- het certificaat uitsluitend gebruikt zal worden voor doeleinden die verenigbaar zijn met deze CP/CPS;
- hij akkoord gaat met de voorwaarden in deze CP/CPS;
- hij zijn geheime sleutel goed zal beheren en afdoende voorzorgsmaatregelen zal nemen om verlies, openbaarmaking, wijziging of onbevoegd gebruik te voorkomen, conform hetgeen bepaald is in paragraaf 2.1.2 en in de overeenkomst tussen Contractant en VECOZO;
- hij bij verlies, openbaarmaking, wijziging of onbevoegd gebruik dit zo snel mogelijk kenbaar maakt aan de Contactpersoon, Hoofdcontactpersoon of Tekenbevoegde. De Contactpersoon, Hoofdcontactpersoon of Tekenbevoegde maakt dit vervolgens direct, doch uiterlijk binnen 24 uur, telefonisch of via mail kenbaar aan VECOZO.

Door acceptatie van een certificaat verklaart de Gebruiker dat hij VECOZO zal vrijwaren van enige schade als gevolg van handelingen of verzuimen van gebruiker die leiden tot aansprakelijkheid, schade of benadeling, alsmede eventuele gerechtelijke procedures en daaruit voortvloeiende kosten voor VECOZO, veroorzaakt door het gebruik of de publicatie van een certificaat.

4.4 Intrekking van certificaten en (de)blokkering van gebruikers

VECOZO ondersteunt het (de)blokkeren van gebruikers en het intrekken van certificaten. Indien een Gebruiker wordt geblokkeerd, kan deze het certificaat niet meer gebruiken om te authentiseren. Het certificaat wordt niet op de CRL geplaatst. Een blokkade van een gebruiker kan op een later tijdstip opgeheven worden.

Wanneer een certificaat wordt ingetrokken, wordt deze onherroepelijk op de CRL geplaatst. Het certificaat is daarmee noch voor VECOZO-diensten, noch voor diensten van andere vertrouwende partijen nog te gebruiken. Nadat een certificaat is ingetrokken, kan deze niet meer opnieuw geldig worden verklaard.

4.4.1 Omstandigheden die leiden tot intrekking of blokkering

Onder de volgende omstandigheden moet een certificaat worden ingetrokken:

- Indien de inhoud van het certificaat of een deel daarvan niet meer juist is;
- Indien de private sleutel behorende bij het certificaat verloren is gegaan, is gestolen of is aangetast doordat de private sleutel op enige andere wijze aan inbreuk heeft blootgestaan of (vermoedelijk) is gecompromitteerd;
- Indien een certificaat door een ander(en) wordt gebruikt dan degene voor wie het certificaat is uitgegeven;
- Indien de pincode en het gebruikersnummer van een certificaat (vermoedelijk) zijn gecompromitteerd;
- Indien de Contractant of de Gebruiker niet voldoet aan de verplichtingen zoals deze zijn verwoord in deze CP/CPS of de overeenkomst die met VECOZO is gesloten;
- Indien de overeenkomst tussen de Contractant en VECOZO is ontbonden;
- Wanneer de Contractant is opgehouden te bestaan;
- Bij ontslag of uitdiensttreding van de Gebruiker;
- Bij het overlijden van de Gebruiker;
- Indien het persoonlijke certificaat niet binnen 60 dagen na uitgifte door de Gebruiker is geïnstalleerd. Het VECOZO-systeem blokkeert en verwijdert de betreffende Gebruiker dan automatisch. Het persoonlijke certificaat van de Contactpersoon is hiervan uitgezonderd;
- Indien een Contractant bij Vektis aangeeft dat zij is beëindigd. In dergelijke gevallen worden alle aan de Contractant gekoppelde certificaten zes maanden na de datum van beëindiging automatisch ingetrokken;
- Ter voorkoming van een calamiteit.

Een Gebruiker kan in buitengewone situaties op verzoek geblokkeerd worden (bijvoorbeeld in afwachting van een schriftelijk intrekkingsverzoek in geval van diefstal van een computersysteem). Of VECOZO overgaat tot blokkering is ter beoordeling van de VECOZO RA. Indien een Gebruiker tijdens de inlogprocedure vijf maal een foutief wachtwoord of pincode invoert, wordt de Gebruiker automatisch geblokkeerd.

Indien bij het gebruik van een systeemcertificaat getracht wordt verbinding te maken met VECOZO met een niet geregistreerd IP-adres wordt de toegang geweigerd. In dit geval wordt het systeemcertificaat niet geblokkeerd of ingetrokken, maar de gebruiker kan geen gebruik maken van de VECOZO-dienstverlening tot de juiste (reeks van) IP-adressen zijn geregistreerd.

4.4.2 Wie mag een verzoek tot intrekking of (de)blokkering doen

De volgende personen en entiteiten mogen een verzoek tot intrekking of (de)blokkering doen:

- De Tekenbevoegde;
- De (Hoofd)Contactpersoon;
- De Gebruiker;
- De ICT-Beheerder;
- VECOZO.

Indien een Gebruiker is geblokkeerd omdat de Gebruiker vijf maal een foutief wachtwoord in heeft gevoerd, dan ontvangen de Gebruiker en de Contactpersoon hier een bericht over.
Tekenbevoegde, (Hoofd)Contactpersoon, Gebruiker en ICT-Beheerder kunnen een verzoek doen om de Gebruiker te

deblokkeren. Tevens is het mogelijk voor instanties waarvan de Contactpersoon toegang heeft tot Gebruikersbeheer om via Gebruikersbeheer een Gebruiker te deblokkeren.

4.4.3 Procedure voor een verzoek tot intrekking of blokkering

Tekenbevoegde, (Hoofd)Contactpersoon, Gebrui-ker, ICT-Beheerder en VECOZO kunnen schriftelijk of via het VECOZO-portaal een verzoek tot intrekking indienen. De gebruiker kan het alleen voor zichzelf doen. Zie voor het proces www.VECOZO.nl.

De Contactpersoon kan na inloggen ook rechtstreeks via het VECOZO-portaal certificaten van Contractant intrekken. VECOZO zal de authenticiteit van het intrekkings- of deblokkeringsverzoek valideren conform het bepaalde in paragrafen 3.4.1 en 3.5.1.

Indien de Contractant of VECOZO een verzoek tot intrekking indient, moet de beweegreden worden vastgelegd. Indien aan voorgaande voorwaarden is voldaan, trekt VECOZO uiterlijk vijf werkdagen na ontvangst van het intrekkingsverzoek het certificaat in.

VECOZO beschikt over een automatische koppeling met Vektis. Indien een Contractant beëindiging van AGB-code(s) bij Vektis meldt, wordt dit via deze koppeling geautomatiseerd bij VECOZO gemeld. Zes maanden na ontvangst van het bericht beëindigt VECOZO in beginsel automatisch de certificaten van Contractant. De Contactpersoon van de Contractant ontvangt hier per e-mail bericht over van VECOZO. Daarnaast wordt de Contactpersoon op de hoogte gesteld van het feit dat het betreffende certificaat is ingetrokken. In het geval van faillissement kan door de curator de procedure zoals omschreven op de website van VECOZO gevolgd worden.

Indien VECOZO uit eigen beweging een certificaat intrekt, dan is vooraf toestemming benodigd van een lid van het VECOZO MT tenzij de intrekking conform intern beleid en interne werkafspraken geschiedt. De VECOZO RA mag een certificaat intrekken naar aanleiding van de volgende omstandigheden:

- Een juist geauthentiseerd verzoek van de Tekenbevoegde, (Hoofd)Contactpersoon, ICT-Beheerder of Gebruiker;
- In opdracht van een VECOZO MT-lid;
- Conform vooraf vastgelegd beleid, vastgelegde werkafspraken en afspraken in de overeenkomst met Contractant.

Gezien het bijzondere karakter van het blokkeren van een Gebruiker is hier geen vaste procedure voor. De VECOZO RA beoordeelt ieder verzoek tot (de)blokkering en bepaalt of een certificaat al dan niet ge(de)blokkeerd wordt.

4.4.4 Beschikbaarheid van de intrekkings-/(de)blokkeringsdienst

Ten behoeve van het laten intrekken van een certificaat is de VECOZO RA bereikbaar. De precieze contactgegevens, procedures en openingstijden zijn vermeld op www.VECOZO.nl.

4.4.5 CRL-uitgiftefrequentie

De CRL wordt iedere 12 uur door KPN opnieuw gepubliceerd en wordt elke 24 uur door VECOZO gedownload. Het serienummer van het ingetrokken certificaat en de intrekkingsdatum worden maximaal 25 uur na intrekking gepubliceerd in de CRL.

4.4.6 CRL-controle voorwaarden

VECOZO moet iedere 24 uur een nieuwe CRL downloaden en is verplicht om de authenticiteit van de CRL te verifiëren. Hiertoe moet de elektronische handtekening waarmee de CRL is ondertekend worden geverifieerd.

4.4.7 Andere vormen van publiceren intrekkingstatus

VECOZO hanteert buiten een Certificate Revocation List (CRL) geen andere vormen van publiceren van de intrekkingsstatus. Zo wordt bijvoorbeeld geen gebruik gemaakt van het Online Certificate Status Protocol (OCSP).

4.5 Security auditprocedures

4.5.1 Vastlegging van gebeurtenissen

De belangrijkste activiteiten met betrekking tot certificaatuitgifte die door de medewerkers van VECOZO worden uitgevoerd, worden in de VECOZO-beheerapplicatie en bijbehorende logbestanden vastgelegd. Hiermee wordt

gewaarborgd dat alle gebeurtenissen ten aanzien van de levenscyclus van de certificaten worden vastgelegd. Daarnaast legt VECOZO zelf nog gebeurtenissen vast met betrekking tot de algemene informatiebeveiliging. Hierbij kan worden gedacht aan het installeren van nieuwe software, het aanmaken van accounts en het maken van back-ups.

KPN houdt zelf ook logbestanden bij ten aanzien van de VECOZO CA, zoals gehuisvest bij KPN. Enkele VECOZO-medewerkers kunnen deze logbestanden inzien via een beveiligd online portaal. KPN logt de volgende gebeurtenissen:

- Gebeurtenissen aangaande levenscyclus management van de VECOZO CA en certificaten van Gebruikers, inclusief:
  - Certificaat aanvraag, vernieuwing en intrekking;
  - Succesvolle en gefaalde verwerkingen van bovenstaande gebeurtenissen;
  - Genereren en uitgifte van Certificaten en CRL's.

Bovenstaande logbestanden worden digitaal ondertekend om ongeautoriseerde wijzigingen onmogelijk te maken. Verder logt KPN diverse beveiliging gerelateerde gebeurtenissen. VECOZO heeft contractuele afspraken met KPN omtrent melding van relevante beveiligingsgebeurtenissen.

4.5.2 Notificeren veroorzaker gebeurtenis

Afhankelijk van de aard van een gebeurtenis informeert VECOZO de betrokken Gebruiker(s). Dit ter beoordeling van VECOZO.

4.5.3 Interval vastleggingen

De in paragraaf 4.5.1 beschreven vastleggingen worden direct na het uitvoeren van de betreffende activiteit uitgevoerd. Maandelijks worden deze vastleggingen middels een steekproef geëvalueerd door een daartoe aangewezen medewerker. In geval van incidenten en calamiteiten worden de vastleggingen geanalyseerd.

4.5.4 Bewaartermijn

VECOZO zorgt ervoor dat de vastleggingen met betrekking tot uitgifte en intrekking van certificaten minimaal bewaard blijven gedurende de wettelijk vereiste periode, noodzakelijk voor het leveren van bewijs in een rechtsgang waarbij VECOZO betrokken is.

4.5.5 Bescherming logbestanden

De gebeurtenissen worden op een dusdanige wijze vastgelegd dat de integriteit en de beschikbaarheid van de logbestanden gewaarborgd blijft en dat alleen daartoe geautoriseerde personen de logbestanden kunnen bekijken.

4.5.6 Eisen aan vastlegging datum en tijd van gebeurtenissen

VECOZO synchroniseert de klokken van haar systemen met nauwkeurige tijdsbronnen, waardoor de exacte datum en tijd van gebeurtenissen vast wordt gelegd. Ook KPN draagt zorg hiervoor.

4.5.7 Back-up logbestanden

Van de logbestanden wordt volgens een vast schema en een vaste procedure een back-up gemaakt die gedurende een vastgestelde periode op een veilige locatie wordt bewaard.

4.5.8 Penetratietesten

VECOZO laat haar systemen periodiek door een externe partij op kwetsbaarheden onderzoeken middels penetratietesten. Daarnaast heeft KPN maatregelen getroffen voor het detecteren van kwetsbaarheden in haar systemen.

4.6 Archivering van documenten

VECOZO archiveert tenminste de volgende documenten en informatie:

- De overeenkomst tussen Contractant en VECOZO;
- Certificaataanvragen en alle informatie en documentatie die is gebruikt voor het verifiëren van de certificaataanvraag voor zover dit wettelijk is toegestaan;
- Wijzigingsverzoeken en bijbehorende informatie en documentatie die is gebruikt voor het verifiëren van het wijzigingsverzoek, voor zover dit wettelijk is toegestaan;
- Intrekkingsverzoeken en bijbehorende informatie en documentatie die is gebruikt voor het verifiëren van het intrekkingsverzoek voor zover dit wettelijk is toegestaan.

4.6.1 Bewaartermijn archief

Archieven worden voor de periode van zeven jaar na beëindigen van de overeenkomst bewaard. Hierbij wordt rekening gehouden met de wettelijke vereisten.

4.6.2 Bescherming van archieven

De archieven worden beschermd tegen verlies, vernietiging en vervalsing. Hiertoe heeft VECOZO beveiligingsmaatregelen getroffen.

4.6.3 Opslagfaciliteit

De archieven worden op een veilige locatie bewaard.

4.7 Vernieuwen van sleutels

Het vernieuwen van sleutels dient altijd te worden uitgevoerd conform de procedures die in paragraaf 3.3 zijn gesteld. Onder “vernieuwen van sleutels” verstaat VECOZO het geautomatiseerd toekennen van een nieuw certificaat met een volledige geldigheidsduur (zie paragraaf 5.4.1), zonder dat een Gebruiker hiervoor een nieuwe aanvraag in hoeft te dienen. Bij het vernieuwingsproces genereert de Gebruiker een nieuw sleutelpaar en wordt geautomatiseerd een nieuw certificaat toegekend, waarbij het oude certificaat geautomatiseerd wordt ingetrokken. Strikt genomen wordt de geldigheidsduur van sleutels dus niet aangepast. Bij vernieuwing van een certificaat dient altijd het sleutelpaar te worden vernieuwd.

In het geval het sleutelpaar van de VECOZO CA wordt vernieuwd, zullen alle leden uit de gebruikersgemeenschap van VECOZO hiervan op de hoogte worden gebracht. De communicatie kan via de website van VECOZO en e-mail verlopen.

4.7.1 Continuïteit

Ten behoeve van de waarborging van de continuïteit van de certificaatdienstverlening heeft VECOZO een calamiteiten- en continuïteitsplan opgesteld.

4.7.2 Aantasting

Indien de private sleutel van de VECOZO CA (mogelijk) is gecompromitteerd, wordt het bijbehorende certificaat ingetrokken.
In dat geval stelt VECOZO alle leden uit de gebruikersgemeenschap zo spoedig mogelijk op de hoogte van dit feit. VECOZO geeft hierbij aan dat niet meer kan worden vertrouwd op de uitgegeven VECOZO certificaten en CRL’s. De communicatie kan via de website van VECOZO en e-mail verlopen.

4.8 CA-beëindiging

4.8.1 Berichtgeving aan betrokken partijen

Indien VECOZO de certificaatdienstverlening beëindigt, worden alle leden uit de gebruikersgemeenschap ingelicht en geïnformeerd. De communicatie kan via de website van VECOZO en e-mail verlopen.

4.8.2 Continuïteit van de verplichtingen van VECOZO

Indien VECOZO haar certificaatdienstverlening beëindigt, worden minimaal de volgende activiteiten uitgevoerd:

- de verplichtingen van VECOZO worden overgedragen aan de rechtsopvolger van VECOZO;
- het archief wordt overgedragen aan de rechtsopvolger van VECOZO en blijft beschikbaar voor de betrokken partijen;
- de beëindiging van de dienstverlening wordt gecommuniceerd volgens de procedure beschreven in paragraaf 4.8.1.

4.8.3 Revocatiestatus van de nog geldige en uitgegeven certificaten

Na beëindiging van de certificaatdienstverlening wordt de revocatiestatus van de nog geldige en uitgegeven certificaten overgedragen aan de rechtsopvolger van VECOZO. Indien dit niet mogelijk is en de dienstverlening wordt niet overgenomen, zullen alle dan nog geldige certificaten worden ingetrokken.

5. Beveiliging

5.1 Beveiliging (algemeen)

VECOZO is NEN7510 compliant. VECOZO werkt dus voortdurend aan de beveiliging van de VECOZO-diensten en -certificaatdienstverlening. Door dit dynamische proces is VECOZO gerechtigd maatregelen treffen die (direct) invloed kunnen hebben op het rechtmatig gebruik van de door haar uitgegeven Persoonlijke- en Systeemcertificaten.

In het kader van NEN 7510 worden diverse aspecten van beveiliging doorgelicht, waaronder ook de fysieke, procedurele en personele beveiliging. Maar ook technische (netwerk)beveiliging, back-up en leveranciersmanagement. Ook daarom voldoet de KPN-omgeving aan strenge fysieke, personele en procedurele beveiliging, wat blijkt uit de ISO27001-certificering van KPN.

De totale methodiek (information security management system – ISMS) is risico gebaseerd. Het geheel wordt jaarlijks onafhankelijk geaudit. Het audit rapport wordt ter beschikking gesteld aan de opdrachtgevers van VECOZO.

5.2 Technische beveiliging van het certificaat

VECOZO heeft beleid opgesteld rond technische beveiliging. Hierin wordt onder andere ingegaan op logische toegangsbeveiliging van haar diensten en technische eisen die hier aan gesteld worden, zoals genereren en distribueren van sleutels en certificaten, sleutellengte en geldigheidsduur van certificaten.

5.2.1 Genereren van VECOZO-sleutelpaar

Het genereren en de opslag van de sleutels van VECOZO vindt plaats bij en door KPN onder controleerbare en beheersbare omstandigheden in hardware (zogenaamde Hardware Security Module), volgens een vooraf vastgelegde procedure. De generatie vindt plaats in een fysiek beveiligde KPN-omgeving door personeel in vertrouwelijke functies. Het aantal personeelsleden dat gemachtigd is deze opdracht uit te voeren, is zo klein mogelijk. Het genereren van de sleutels van VECOZO wordt uitgevoerd met een algoritme en sleutellengte die voldoen aan de stand van de techniek. Zie hiervoor de certificaatprofielen in hoofdstuk 6.

5.2.2 Genereren van de eindgebruiker-sleutelparen

De Gebruiker genereert tijdens het aanvraag- en uitgifteproces zelf zijn sleutelpaar. Iedere Gebruiker verklaart dat hijzelf – en niet VECOZO – verantwoordelijk is voor de bescherming van zijn geheime sleutel(s) tegen inbreuk, verlies, openbaarmaking, wijziging of onbevoegd gebruik. De private sleutel is niet overdraagbaar.

5.2.3 Overdracht publieke sleutel van Gebruiker aan VECOZO

De publieke sleutel van de Gebruiker wordt door middel van een versleutelde verbinding aan de VECOZO CA verstuurd. De mPKI-oplossing van KPN draagt er zorg voor dat de publieke sleutel van de Gebruiker op een veilige wijze ondertekend wordt en het certificaat op een veilige wijze aan de Gebruiker wordt geretourneerd.

5.2.4 Overdracht van publieke sleutel van VECOZO aan Gebruikers

Op de website van VECOZO kan het certificaat van de VECOZO CA worden gedownload via https://www.vecozo.nl/certificaten/ en kan de Gebruiker het VECOZO CA-certificaat installeren in zijn browser.

5.2.5 Sleutellengten

VECOZO-sleutels

Voor het sleutelpaar van het VECOZO CA-certificaat worden RSA-sleutels met een sleutellengte van tenminste 2048 bits gebruikt.

Gebruikerssleutels

Voor de sleutelparen van de Gebruikerscertificaten worden RSA-sleutels met een sleutellengte van tenminste 2048 bits gebruikt.

5.2.6 Doelen sleutelgebruik

VECOZO-sleutels

De sleutels van de VECOZO CA mogen alleen worden gebruikt voor het ondertekenen van certificaten en het (offline) ondertekenen van CRL's.

Gebruikerssleutels

De sleutels van Gebruikers mogen alleen worden gebruikt in overeenstemming met het toepassingsgebied en de hiertoe in het certificaat opgenomen extensies.

5.3 Private sleutelbescherming

5.3.1 Standaard cryptografische module

De VECOZO CA private sleutels staan op een Hardware Security Module (HSM) die bij KPN in beheer is. De HSM is FIPS 140-2 level 3 gecertificeerd.

5.3.2 Gebruikers

Voor het verkrijgen van toegang tot VECOZO-diensten middels een persoonlijk certificaat dient een Gebruiker te beschikken over een wachtwoord. Bij verlies van het wachtwoord kan de Gebruiker, de Contactpersoon, de Hoofdcontactpersoon of de Tekenbevoegde dit door VECOZO laten resetten, waarna de Gebruiker zelf een nieuw wachtwoord in kan stellen. Gebruiker dient hiervoor te beschikken over de originele pincode van het certificaat. Is deze niet meer beschikbaar, dan kan de Gebruiker of de

Contactpersoon voor Gebruiker een nieuwe pincode aanvragen. De nieuwe pincode wordt volgens de procedure voor certificaatuitgifte verstrekt.

5.3.3 VECOZO CA

De VECOZO CA is ondergebracht bij KPN. KPN heeft vergaande beveiligingsmaatregelen getroffen op het gebied van logische en fysieke toegangsbeveiliging. KPN is derhalve ISO27001-gecertificeerd.

5.3.4 VECOZO RA

Ten behoeve van de uitvoering van hun functie beschikken, waar nodig, medewerkers van VECOZO over een certificaat dat is beveiligd met een wachtwoord. Hiermee wordt gewaarborgd dat alleen geautoriseerde personen als VECOZO RA kunnen optreden.

5.3.5 Escrow

Zowel de VECOZO sleutels als de sleutels van de Gebruikers worden niet bij een derde escrow agent ondergebracht.

5.3.6 Back-up (eindgebruikers private sleutels)

Gebruikers zijn zelf verantwoordelijk voor het maken van een back-up van hun private sleutel en de te treffen beveiligingsmaatregelen ten aanzien van de back-up, conform het gestelde in de overeenkomst tussen Contractant en VECOZO. VECOZO kan derhalve de private sleutel van de certificaatgebruiker niet herstellen.
Indien een certificaat onverhoopt verloren gaat, kan de Tekenbevoegde of de Hoofdcontactpersoon of de Contactpersoon bij VECOZO een nieuw certificaat aanvragen.

5.3.7 Back-up (VECOZO private sleutels)

VECOZO heeft het beheer van de VECOZO private sleutels uitbesteed aan KPN. Dit geldt ook voor back-up en het daar aan gekoppelde transport en migreren.

De back-up van de sleutels van VECOZO vindt plaats bij en door KPN onder controleerbare en beheersbare omstandigheden
De back-up vindt plaats in een fysiek beveiligde KPN-omgeving door personeel in vertrouwelijke functies. Het aantal personeelsleden dat gemachtigd is deze opdracht uit te voeren, is zo klein mogelijk.

Bij het daadwerkelijk transporteren en migreren van de private sleutels van VECOZO informeert KPN VECOZO. Beide stemmen op dat moment de werkwijze af.

KPN doet een voorstel voor de werkwijze. Transport en migratie vinden plaats in een fysiek beveiligde KPN-omgeving door personeel in vertrouwelijke functies. Het aantal personeelsleden dat gemachtigd is deze opdracht uit te voeren, is zo klein mogelijk. De migratie en back-up wordt getest en door VECOZO akkoord bevonden.

5.3.8 Archivering

Na afloop van de levensduur van het VECOZO CA sleutelpaar wordt deze niet gearchiveerd. De Gebruiker is zelf verantwoordelijk voor het archiveren van zijn sleutelpaar na het aflopen van de geldigheidsduur en de te treffen beveiligingsmaatregelen ten aanzien van de archivering.

5.3.9 Activeren en deactiveren private sleutel VECOZO

Zie paragraaf 5.2.1

5.3.10 Methode van vernietiging

De private sleutel van de VECOZO CA (en kopieën daarvan) worden na afloop van de levensduur op verzoek van VECOZO door KPN op een dusdanige wijze vernietigd dat deze niet meer opnieuw in gebruik kunnen worden genomen. KPN heeft hiervoor een termination plan opgesteld.

De Gebruiker is zelf verantwoordelijk voor de vernietiging van zijn private sleutel.

5.4 Overige aspecten van sleutelpaar-management

5.4.1 Gebruiksduur sleutels

De geldigheidsduur van de VECOZO CA-sleutels en -certificaten is tien jaar. VECOZO draagt er zorg voor dat de sleutels van de VECOZO CA niet worden gebruikt na het einde van hun levenscyclus.

De sleutels en certificaten van Gebruikers hebben een maximale geldigheidsduur van 25 maanden. De Gebruiker mag het certificaat niet na afloop van de geldigheidsduur van het certificaat gebruiken.

5.5 Activeringsgegevens

Het certificaat van de Gebruiker kan alleen worden gedownload wanneer de Gebruiker beschikt over een gebruikersnummer en pincode. Zijn deze niet meer beschikbaar, dan kan de Gebruiker, de Contactpersoon, de Hoofdcontactpersoon of de Tekenbevoegde voor Gebruiker een nieuwe pincode aanvragen. De nieuwe pincode wordt conform de procedure voor certificaatuitgifte verstrekt.

6. Certificaat en CRL-profiel

6.1 Certificaatprofiel

Alle typen certificaten zijn gebaseerd op de X.509v3-standaard. Het verschil tussen persoonlijke- en systeemcertificaten is de vulling van de Common Name. Zie hiervoor paragraaf 3.2.3.

Attribuut	Beschrijving / waarde G3 certificaat	Beschrijving / waarde G4 certificaat
Versie	V3	V3
Serienummer	Uniek serienummer	Uniek serienummer
Algoritme voor handtekening	sha256RSA	sha256RSA
Handtekening hash-algoritme	sha256	sha256
Verlener	CN = VECOZO – G3 O = Vecozo B.V. C = NL	CN = VECOZO – G4 O = Vecozo B.V. C = NL
Geldig van	Ingangsdatum geldigheidsduur certificaat	Ingangsdatum geldigheidsduur certificaat
geldig tot	Einddatum geldigheidsduur certificaat	Einddatum geldigheidsduur certificaat
Onderwerp	E = e-mailadres CN = zie 3.1.3 O = Vecozo B.V.	E = e-mailadres CN = zie 3.1.3 O = Vecozo B.V.
Openbare sleutel	RSA (2048 Bits)	RSA (2048 Bits)
CRL distributiepunten	[1]CRL-distributiepunt Naam van distributiepunt: Volledige naam: URL= http://cert.managedpki.com /crl/VecozoBV/LatestCRL.crl URL= http://crl.vecozo.nl/LatestCRL.crl	[1]CRL-distributiepunt Naam van distributiepunt: Volledige naam: URL= http://mpki.managedpki.com /crl/VECOZOG4LatestCRL.crl URL= http://crl.vecozo.nl/g4/LatestCRL.crl
Identificatie van de onderwerpsleutel	-	-
Sleutel-id van CA	Het sleutel-id van de Certificate Authority	Het sleutel-id van de Certificate Authority
Essentiële beperkingen	Subjecttype=Eindidentiteit Beperking voor padlengte=Geen	Subjecttype=Eindidentiteit Beperking voor padlengte=Geen
Sleutelgebruik	Digitale handtekening, Sleutelcodering (a0)	Digitale handtekening, Sleutelcodering (a0)
Algoritme van vingerafdruk	Sha256RSA	Sha256RSA
Vingerafdruk	Vingerafdruk van het certificaat	Vingerafdruk van het certificaat

Tabel 1: Certificaatprofiel X.509v3 G3 en G4 persoonlijk certificaat

Attribuut	Beschrijving / waarde G3 certificaat	Beschrijving / waarde G4 certificaat
Versie	V3	V3
Serienummer	Uniek serienummer	Uniek serienummer
Algoritme voor handtekening	sha256RSA	sha256RSA
Handtekening hash-algoritme	sha256	sha256
Verlener	CN = VECOZO – G3 O = Vecozo B.V. C = NL	CN = VECOZO – G4 O = Vecozo B.V. C = NL
Geldig van	Ingangsdatum geldigheidsduur certificaat	Ingangsdatum geldigheidsduur certificaat
Geldig tot	Einddatum geldigheidsduur certificaat	Einddatum geldigheidsduur certificaat
Onderwerp	E = e-mailadres CN = Zie 3.1.3 O = Vecozo B.V.	E = e-mailadres CN = Zie 3.1.3 O = Vecozo B.V.
Openbare sleutel	RSA (2048 Bits)	RSA (2048 Bits)
CRL distributiepunten	[1]CRL-distributiepunt Naam van distributiepunt: Volledige naam: URL= http://cert.managedpki.com /crl/VecozoBV/LatestCRL.crl URL= http://crl.vecozo.nl/LatestCRL.crl	[1]CRL-distributiepunt Naam van distributiepunt: Volledige naam: URL= http://mpki.managedpki.com /crl/VECOZOG4LatestCRL.crl URL= http://crl.vecozo.nl/g4/LatestCRL.crl
Identificatie van de onderwerpsleutel	-	-
Sleutel-id van CA	Het sleutel-id van de Certificate Authority	Het sleutel-id van de Certificate Authority
Essentiële beperkingen	Subjecttype=Eindentiteit Beperking voor padlengte=Geen	Subjecttype=Eindentiteit Beperking voor padlengte=Geen
Sleutelgebruik	Digitale handtekening, Sleutelcodering (a0)	Digitale handtekening, Sleutelcodering (a0)
Algoritme van vingerafdruk	Sha256RSA	Sha256RSA
Vingerafdruk	Vingerafdruk van het certificaat	Vingerafdruk van het certificaat

Tabel 2: Certificaatprofiel X.509v3 G3 en G4 systeemcertificaat

6.2 CRL-profiel

Iedere 4 uur wordt door KPN een Certificate Revocation List (CRL) opgesteld en gepubliceerd voor G4 certificaten. Iedere 12 uur wordt door KPN een Certificate Revocation List (CRL) opgesteld en gepubliceerd voor G3 certificaten. Beide CRL's zijn 24 uur geldig. Ten behoeve van de controle van de geldigheid van de certificaten wordt elke 24 uur de door KPN gepubliceerde CRL door VECOZO gedownload en tevens gepubliceerd.

De CRL wordt gepubliceerd op de in het certificaat aangewezen locaties. Informatie over de uitgegeven certificaten is alleen toegankelijk voor VECOZO en vereist een toegangscontrole alvorens hiertoe toegang kan worden verkregen.

6.3 Versienummer CRL

VECOZO geeft X.509 versie 2 CRL's uit.

6.3.1 CRL-velden en CRL-extensies

Tabel 3: CRL-profiel X.509v3 G3- en G4-certificaat

Attribuut	Beschrijving / waarde CRL voor G3	Beschrijving / waarde CRL voor G4
Versie	V2	V2
Verlener	CN = VECOZO – G3 O = Vecozo B.V. C = NL	CN = VECOZO – G4 O = Vecozo B.V. C = NL
Ingangsdatum	Ingangsdatum en –tijdstip van CRL	Ingangsdatum en –tijdstip van CRL
Volgende update	Datum en tijdstip van update CRL	Datum en tijdstip van update CRL
Algortime voor handtekening	sha256RSA	sha256RSA
Handtekening hash-algoritme	sha256	sha256
Sleutel-id van CA	Het sleutel-id van de Certificate Authority	Het sleutel-id van de Certificate Authority
CRL-nummer	Nummer van de gedownloade CRL.	Nummer van de gedownloade CRL.

7. Specificatie van onderhoud op CP/CPS

7.1 Wijzigingsprocedure voor de CP/CPS

7.1.1 Wijzigingen zonder bekendmaking

Wijzigingen in deze CP/CPS van redactionele aard of correcties van kennelijke schrijf- en/of spelfouten kunnen zonder voorafgaande bekendmaking in werking treden.

7.1.2 Wijzigingen waarbij bekendmaking is verplicht

Alle wijzigingen in de CP/CPS die niet onder paragraaf 7.1.1 vallen en die impact hebben op de certificaathouders en -gebruikers, worden minimaal 14 dagen voordat de wijzigingen in werking treden bekend gemaakt aan alle leden uit de gebruikersgemeenschap. De voorgestelde wijzigingen worden op de website van VECOZO gepubliceerd. De wijzigingen en daarmee de nieuwe versie van de CP/CPS treden in werking op het moment dat de nieuwe CP/CPS op de website is gepubliceerd en aan de bekendmakingplicht is voldaan.

7.2 Publicatie van de CP/CPS

De VECOZO CP/CPS is in elektronische vorm te vinden op de website van VECOZO (https://www.vecozo.nl). Voor de contactgegevens wordt verwezen naar paragraaf 1.4.

7.3 Goedkeuringsprocedure voor de CP/CPS

Wijzigingen in de CP/CPS moeten door de PMA worden goedgekeurd. Een uitzondering hierop betreffen de wijzigingen, zoals gedefinieerd in paragraaf 1.3.3, die moeten worden goedgekeurd door de AvA.