



VECOZO

CERTIFICATE POLICY

VOOR VECOZO-CERTIFICATEN IN DE ZORG



Versiebeheer

Nummer	Datum	Opmerkingen	Auteur(s)
1.0	mei 2003	Eerste versie	VECOZO
2.0	september 2004	Tweede versie na PKI-onderzoek en gereedkomen beveiligings- en continuïteitsplannen	VECOZO
2.1	mei 2006	Wijziging adresgegevens	VECOZO
2.2	oktober 2006	Update m.b.t. gewijzigde situatie + tekstuele wijzigingen	VECOZO
2.3	08-04-2009	Geactualiseerd + tekstuele wijzigingen	VECOZO
2.4	16-02-2010	Update mbt intrekken en blokkeren van certificaten.	VECOZO

In dit document wordt regelmatig verwezen naar de CPS van Getronics. U kunt deze via onderstaande URL downloaden:

http://www.pki.getronicspinkroccade.nl/website/files/Getronics_VTN_CPS_v3.1.pdf



Inhoudsopgave

1	Introductie	5
1.1	Overzicht	5
1.2	Gebruikersgemeenschap en toepassingsgebied	6
1.3	Contactgegevens en beleidsstructuur	8
2	Algemene bepalingen	9
2.1	Verplichtingen	9
2.2	Aansprakelijkheid van VECOZO	10
2.3	Financiële verantwoordelijkheid	11
2.4	Interpretatie en handhaving	11
2.5	Tarieven	12
2.6	Publicatie en elektronische opslagplaats	12
2.7	Audit	12
2.8	Vertrouwelijkheid	13
2.9	Intellectuele eigendomsrechten	13
3	Identificatie en authenticatie	14
3.1	Initiële registratie	14
3.2	Certificaatvernieuwing	16
3.3	Verzoeken tot intrekking	16
4	Operationele eisen	17
4.1	Aanvraag van certificaten	17
4.2	Uitgifte van certificaten	17
4.3	Acceptatie van certificaten	17
4.4	Intrekking en blokkeren van certificaten	18
4.5	Security auditprocedures	20
4.6	Archivering van documenten	21
4.7	Vernieuwen van sleutels	21
4.8	Aantasting en continuïteit	21
4.9	CA-beëindiging	22
5	Fysieke, procedurele en personele beveiliging	24
5.1	Algemeen	24
5.2	Fysieke beveiliging	25
5.3	Procedurele beveiliging	25
5.4	Personele beveiliging	26
6	Technische beveiliging	27
6.1	Genereren en installeren van de sleutelparen	27
6.2	Private sleutelbescherming	28



6.3	Overige aspecten van sleutelpaarmanagement	29
6.4	Activeringsgegevens	29
6.5	Computerbeveiligingsmaatregelen	29
6.6	Beheersmaatregelen technische levenscyclus	29
6.7	Netwerkbeveiligingsmaatregelen	29
6.8	Cryptografische module beveiligingsmaatregelen	29
7	Certificaat en CRL-profiel	30
7.1	Certificaatprofiel	30
7.2	CRL-profiel	31
8	Specificatie van onderhoud op CP	32
8.1	Wijzigingsprocedure voor de CP	32
8.2	Publicatie van de CP	32
8.3	Goedkeuringsprocedure voor de CP	32



1 Introductie

1.1 Overzicht

1.1.1 Achtergrond

De certificaatdienstverlening van VECOZO dient ter ondersteuning van veilige elektronische communicatie tussen zorgverleners en de bij VECOZO aangesloten zorgverzekeraars (hierna zorgverzekeraars). VECOZO is specifiek ingericht voor het aanbieden van portaal diensten waarbij ter ondersteuning hiervan diensten worden aangeboden voor de identificatie en authenticatie van gebruikers en het beveiligen van communicatiestromen tussen zorgverleners en zorgverzekeraars. Om dit mogelijk te maken verzorgt VECOZO de uitgifte, het beheer, het blokkeren van gebruikers en het intrekken van digitale certificaten aan zorgverleners, zorgverzekeraars en eventuele derde partijen.

1.1.2 Doel Certificate Policy

De VECOZO Certificate Policy (CP) beschrijft onder welke voorwaarden en waarvoor een VECOZO-certificaat mag worden uitgegeven, beheerd en gebruikt. Het stelt daarmee eisen aan de betrokken partijen en waarborgt daardoor het door VECOZO vastgestelde betrouwbaarheidsniveau. Daarnaast wordt deze CP gebruikt om partijen die gebruik maken van de VECOZO certificaatdienstverlening inzicht te geven in de eisen en werkwijze van VECOZO.

1.1.3 Status

Dit is versie 2.4 van de VECOZO CP. Versie 2.3 is op 8 april 2009 vastgesteld door de Policy Management Authority (het MT) van VECOZO. Deze versie is vervangen door versie 2.4, welke op 16 februari 2010 is vastgesteld.

VECOZO heeft de grootst mogelijke aandacht en zorg besteed aan de gegevens en informatie, die zijn opgenomen in deze CP. Desalniettemin is het mogelijk dat onjuistheden en onvolkomenheden voorkomen. VECOZO aanvaardt geen enkele aansprakelijkheid voor schade als gevolg van deze onjuistheden of onvolkomenheden, noch voor schade die wordt veroorzaakt door het gebruik of de verspreiding van deze CP.

1.1.4 Verhouding tussen CP en Certification Practice Statement

De CP beschrijft welke eisen aan de uitgifte, het beheer en het gebruik van een VECOZO-certificaat worden gesteld. Het VECOZO Certification Practice Statement (CPS), beschrijft daarentegen op welke wijze aan deze eisen tegemoet is gekomen. Vanwege het feit dat het CPS niet publiekelijk beschikbaar is, zal waar nodig in deze CP ook worden beschreven hoe aan bepaalde eisen wordt voldaan.

1.1.5 Structuur

De structuur van deze CP is gebaseerd op het internationaal geaccepteerde RFC 2527¹-raamwerk.

1.1.6 Verwijzingen naar deze CP

De naamgeving van deze CP is VECOZO Certificate Policy, versie 2.4. Aan deze CP is geen Object Identifier (OID) toegewezen en geregistreerd.

¹ RFC 2527, Certificate Policy and Certification Practices Framework, www.ietf.org.



1.1.7 Rolverdeling binnen VECOZO

VECOZO treedt op als certificaatdienstverlener. Binnen VECOZO worden de volgende rollen onderkend:

- *VECOZO Policy Management Authority (PMA)*
De PMA stelt het beleid en de normen vast voor de VECOZO-certificaatdienstverlening. De PMA-functie wordt ingevuld door het VECOZO-management. In paragraaf 1.3.3 wordt nader ingegaan op de beleidsstructuur.
- *VECOZO Certification Authority (CA)*
De CA produceert, op verzoek van de Registration Authority (RA), VECOZO-certificaten en geeft deze uit aan de eindgebruikers. Daarnaast is de CA verantwoordelijk voor de publicatie van de uitgegeven en ingetrokken certificaten.
- *VECOZO Registration Authority (RA)*
De RA registreert en valideert de certificaataanvragen en intrekkingverzoeken. Nadat een aanvraag of intrekkingverzoek is goedgekeurd en is geregistreerd, verstrekt de RA respectievelijk een opdracht tot certificaatgeneratie of tot intrekking aan de CA.

Om de RA- en CA-diensten te kunnen leveren maakt VECOZO gebruik van de zogenaamde Private Managed PKI (PKI) dienstverlening² van Getronics NV (hierna Getronics). Dit houdt in dat het technisch beheer van de CA en de directory is uitbesteed aan Getronics. De RA-functie wordt door VECOZO uitgevoerd.

Om de MPKI-dienstverlening te kunnen leveren werkt Getronics, als dochteronderneming van KPN samen met VeriSign Inc. (hierna VeriSign). De CA en de directory staan fysiek bij Getronics opgesteld. VECOZO heeft een contractuele relatie met KPN.

Ofschoon VECOZO de CA-functie heeft uitbesteed, blijft VECOZO te allen tijde eindverantwoordelijk voor de gehele certificaatdienstverlening.

1.2 Gebruikersgemeenschap en toepassingsgebied

1.2.1 Gebruikersgemeenschap

De partijen binnen de gebruikersgemeenschap van VECOZO zijn certificaathouders, contactpersonen, certificaatgebruikers en vertrouwende partijen.

- Een certificaathouder betreft primair een zorgverlenerspraktijk die minimaal één geldige overeenkomst tot uitwisseling van (persoons)gegevens heeft afgesloten met een zorgverzekeraar. Daarnaast moet een zorgverlener een AGB (Algemeen Gegevens Beheer)-code toegekend hebben gekregen van het landelijk informatiecentrum (Vektis). Daarnaast worden administratiekantoren van aan de zorgverlening gerelateerde instellingen, zorgverzekeraars en overige instanties ook aangemerkt als certificaathouder. Voor administratiekantoren gelden dezelfde uitgangspunten als voor zorgverlenerpraktijken. Voor zorgverzekeraars geldt dat zij een specifieke zorgverzekeraarsovereenkomst met VECOZO moeten aangaan. Onder overige instanties vallen instanties die gebruik maken van VECOZO certificaten om toegang te verkrijgen tot applicaties die door externe partijen worden beheerd. Zij hebben verder geen link met VECOZO; de aanvraag van certificaten verloopt over het algemeen via een bij VECOZO aangesloten zorgverzekeraar. Ten behoeve van de VECOZO-certificaatdienstverlening sluit VECOZO een overeenkomst met de certificaathouder.

² Een private MPKI betekent dat de VECOZO CA niet is ondertekend door een CA van Getronics.



- De contactpersoon treedt namens de certificaathouder op in de communicatie met VECOZO. De contactpersoon vraagt bijvoorbeeld de certificaten aan voor medewerkers van de certificaathouder. Een contactpersoon kan door de certificaathouder worden aangewezen. Alle personen die juridisch namens de certificaathouder tekenbevoegd zijn, zijn automatisch contactpersoon. In alle gevallen is tenminste één contactpersoon ook een certificaatgebruiker. De contactpersoon maakt verder onderdeel uit van de certificaathouder waarmee VECOZO een contract heeft afgesloten.
- Een certificaatgebruiker is de entiteit die als onderwerp is opgenomen in het certificaat en het certificaat daadwerkelijk gebruikt. De certificaatgebruiker maakt onderdeel uit van de certificaathouder waarmee VECOZO een contract heeft afgesloten.
- Een vertrouwende partij is een partij die handelt in vertrouwen op een door VECOZO uitgegeven certificaat. Daarnaast is VECOZO voor de door haar aangeboden portaaldiensten zelf ook een vertrouwende partij.

1.2.2 Toepassingsgebied

Het gebruik van de door VECOZO uitgegeven certificaten is beperkt tot het plaatsen van digitale handtekeningen en authenticatiedoelinden voor communicatie tussen de certificaathouders en de vertrouwende partijen. Deze communicatie verloopt via VECOZO. Certificaathouders worden geauthenticeerd ten behoeve van het verkrijgen van toegang tot VECOZO-portals en daarmee tot de systemen van de zorgverzekeraars of ten behoeve van het verkrijgen van toegang tot diensten van vertrouwende partijen. Voorbeelden van diensten die via VECOZO worden aangeboden zijn de controle op het verzekeringsrecht, het indienen van declaraties en het raadplegen van AGB-codes.

Ten behoeve van het hierboven beschreven toepassingsgebied gebruikt VECOZO de volgende twee typen certificaten:

- *Persoonsgebonden X.509v3-certificaten voor natuurlijke personen*
Deze certificaten worden uitgegeven aan natuurlijke personen die werkzaam zijn bij of voor een certificaathouder. Hierbij wordt gebruik gemaakt van X.509v3 G2-certificaten. In het vervolg zullen deze certificaten worden benoemd als persoonlijke certificaten.
- *X.509v3-servercertificaten voor applicaties c.q. systemen*
Deze certificaten worden uitgegeven ten behoeve van applicaties c.q. systemen van een certificaathouder. De certificaten worden gebruikt voor communicatie tussen applicaties en webservices. Hierbij wordt gebruik gemaakt van X.509v3 G2-certificaten. In het vervolg zullen deze certificaten worden benoemd als systeemcertificaten.

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



1.3 Contactgegevens en beleidsstructuur

1.3.1 Specificatie van de administratieve organisatie

VECOZO B.V.

Postbus 4050

5004 JB Tilburg

Bezoekadres: Abeelstraat 1a, 5038 KE Tilburg

Telefoon: 013 – 4625641

Fax: 013 – 4625640

E-mail: helpdesk@vecozo.com

Internet: www.VECOZO.nl

1.3.2 Contactpersoon

Voor vragen omtrent deze CP kunt u een e-mail sturen aan helpdesk@vecozo.com.

1.3.3 Beleidsstructuur

Ten aanzien van het nemen van beleidsbeslissingen is een tweedeling gemaakt tussen beslissingen die door de aandeelhouders *moeten* worden geaccordeerd en beslissingen die door het VECOZO-management *mogen* worden geaccordeerd. De aandeelhouders komen periodiek tijdens de AvA bijeen.

De AvA moet in ieder geval instemmen met:

- 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 gebruikersgemeenschap uit te breiden c.q. aan te passen.
- Het voornemen om de contractuele relatie met KPN te verbreken en om met een andere partij te gaan samenwerken of het voornemen om de dienstverlening volledig zelf te gaan uitvoeren.

De overige beslissingen kunnen door het VECOZO-management worden genomen. Het VECOZO-management wordt daarom aangemerkt als de VECOZO Policy Management Authority (PMA). Tijdens de AvA legt de PMA verantwoording af over de sinds de voorgaande bijeenkomst genomen beslissingen.



2 Algemene bepalingen

2.1 Verplichtingen

In deze paragraaf worden de verplichtingen van de diverse partijen, die betrokken zijn bij en gebruik maken van de VECOZO-certificaatdienstverlening, gespecificeerd.

2.1.1 Verplichtingen van VECOZO

VECOZO heeft de volgende verplichtingen:

- VECOZO heeft een CP en CPS opgesteld, en heeft de dienstverlening ingericht conform de in deze CP gestelde eisen. Daarnaast waarborgt VECOZO dat het CPS niet strijdig is met deze CP;
- De VECOZO CA en RA opereren conform de in deze CP gestelde eisen en de in het CPS beschreven procedures en maatregelen;
- Het beleid en de procedures die VECOZO hanteert zijn noch direct noch in hun uitwerking discriminerend met Nederlands recht;
- VECOZO dienstverlening is opengesteld voor alle entiteiten die binnen de gebruikersgemeenschap vallen, zoals gedefinieerd in paragraaf 1.2.1;
- VECOZO is een rechtspersoon;
- VECOZO is eindverantwoordelijk voor alle aspecten van het leveren van de certificaatdiensten;
- VECOZO heeft overeenkomsten afgesloten met leveranciers die direct zijn betrokken bij de certificaatlevenscyclus;
- VECOZO heeft een risicoanalyse laten uitvoeren op basis waarvan een informatiebeveiligingsbeleid is opgesteld en beveiligingsmaatregelen zijn getroffen;
- VECOZO dient te beschikken over een managementorgaan, die verantwoordelijk is voor het nemen van beleidsbeslissingen. Zie hiervoor ook paragraaf 1.3.3;
- Wijzigingen in deze CP worden conform de procedures uit hoofdstuk acht goedgekeurd en gepubliceerd.

2.1.2 Verplichtingen van derde partijen

Getronics handelt in overeenstemming met de afgesloten overeenkomst tussen KPN en VECOZO.

2.1.3 Verplichtingen van de contactpersoon, certificaathouder en certificaatgebruiker

De contactpersonen, certificaathouders en certificaatgebruikers hebben de volgende verplichtingen:

- De contactpersoon en certificaathouder zullen, in overeenstemming met de vereisten in deze CP, accurate en volledige informatie verstrekken aan VECOZO;
- Indien zich wijzigingen voordoen van de in het certificaat opgenomen informatie zullen de contactpersoon en/of certificaathouder VECOZO hiervan direct op de hoogte stellen;
- De certificaten mogen alleen worden gebruikt voor de aangegeven gebruiksdoeleinden in het certificaat en zoals is gespecificeerd in het toepassingsgebied;



- Redelijke zorg zal in acht worden genomen om te voorkomen dat de bij het VECOZO-certificaat behorende private sleutel onbevoegd wordt gebruikt. Dit betekent dat de certificaathouder zich verplicht zodanig adequate technische en organisatorische maatregelen te treffen dat de vereiste vertrouwelijkheid van de door de zorgverzekeraar(s) toegankelijk gestelde gegevens is gewaarborgd. Dit houdt tenminste in dat de certificaathouder zal meewerken aan een beveiligde toegangsregistratie en – controle en dat uitsluitend de certificaatgebruiker 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 gegevens van de zorgverzekeraars;
- In het geval van mogelijke onregelmatigheden zoals verlies of compromittering van de private sleutel of van de door de zorgverzekeraar(s) toegankelijk gestelde bestanden c.q. applicaties en gegevens, moet VECOZO zo snel mogelijk op de hoogte worden gebracht;
- De contactpersoon, de certificaathouder en de certificaatgebruiker zullen handelen in overeenstemming met deze CP en de overige voorwaarden die kenbaar zijn gemaakt.

2.1.4 Verplichtingen van de vertrouwende partijen

De verplichtingen van de vertrouwende partijen (de zorgverzekeraars, zorgverleners cq instellingen, derden en VECOZO), wanneer deze in redelijkheid willen kunnen vertrouwen op een certificaat zijn:

- De geldigheid of intrekking van het certificaat verifiëren op basis van actuele informatie over intrekking, zoals beschikbaar is 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;
- Alle overige voorzorgsmaatregelen te nemen die zijn voorgeschreven in eventuele overeenkomsten en gebruiksvoorwaarden.

2.2 Aansprakelijkheid van VECOZO

Tenzij uitdrukkelijk bepaald in een overeenkomst, wijst VECOZO alle waarborgen en verplichtingen van welke aard dan ook af en wijst zij bovendien iedere aansprakelijkheid af voor verzuim en gebrek aan voldoende zorgvuldigheid.

Tenzij uitdrukkelijk vermeld in deze CP verklaart VECOZO:

- Geen garanties te geven voor de nauwkeurigheid, authenticiteit, betrouwbaarheid, volledigheid, gangbaarheid, verhandelbaarheid of geschiktheid van enige informatie die aanwezig is in certificaten;
- Geen aansprakelijkheid te aanvaarden voor verplichtingen die voortkomen uit informatie die aanwezig is in certificaten, op voorwaarde dat de inhoud van deze certificaten wezenlijk conform deze CP is;
- Geen garantie van onweerlegbaarheid te verstrekken voor enig certificaat of daarmee verbonden bericht, anders dan door de wet bepaald;
- Geen garantie te geven voor welke software dan ook.

In geen geval kan VECOZO aansprakelijk worden gesteld voor enige indirecte, speciale, incidentele of gevolgschade of voor verlies van gegevens ten gevolge van:



- Levering of het gebruik van het certificaat;
- Het al dan niet functioneren van certificaten;
- Enige andere transactie of dienst beschreven in deze CP, zelfs indien VECOZO in kennis is gesteld van de mogelijkheid van dergelijke schadevormen.

VECOZO is niet aansprakelijk voor welke schade dan ook die wordt veroorzaakt door:

- a. de installatie en/of het gebruik van het certificaat, dan wel de door de medewerkers van VECOZO geboden ondersteuningsactiviteiten, of
- b. het gebruik door de certificaathouder van de door de zorgverzekeraar(s) toegankelijk gestelde gegevens, bestanden en applicaties.

2.3 Financiële verantwoordelijkheid

2.3.1 Vrijwaring door de deelnemende organisatie binnen VECOZO PKI

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

VECOZO vrijwaart de certificaathouder van alle aanspraken van derden, die gebaseerd zijn op grond van een beweerde inbreuk op een intellectueel eigendomsrecht met betrekking tot het door VECOZO verstrekte certificaat, op voorwaarde dat de certificaathouder:

1. VECOZO van een aanspraak onmiddellijk op de hoogte stelt, en
2. de behandeling van de zaak geheel aan VECOZO overlaat en hiertoe alle medewerking verleent, en aan VECOZO volmacht verleent om zo nodig – op kosten van VECOZO – over de zaak te procederen, en
3. geen verklaringen aflegt, toezeggingen doet, rechten of feiten erkent zonder voorafgaande schriftelijke toestemming van VECOZO, en
4. niet handelt of heeft gehandeld in strijd met de bepalingen in deze CP of in de overeenkomst tot uitwisseling van (persoons)gegevens met de zorgverzekeraar of met de op grond daarvan gemaakte afspraken.

2.3.2 Vertrouwensrelaties

Uitgifte van certificaten maakt VECOZO en haar deelorganisaties geen agent, zaakwaarnemer, gevolmachtigde of andere vertegenwoordiger van de certificaathouder, contactpersoon of vertrouwende partijen.

2.4 Interpretatie en handhaving

2.4.1 Van toepassing zijnde wetgeving

Op deze CP is het Nederlands recht van toepassing.

2.4.2 Geldigheid en toepasselijkheid

Als één of meerdere bepalingen van deze CP bij gerechtelijke uitspraak ongeldig of anderszins niet van toepassing wordt verklaard, laat dit de geldigheid en toepasselijkheid van alle overige bepalingen onverlet.



2.4.3 Geschillenbeslechting

Alle geschillen die ontstaan naar aanleiding van deze CP in de ruimste zin des woords, zullen worden onderworpen aan het oordeel van de arrondissementsrechtbank te Breda, tenzij de betrokken partijen anders overeenkomen. Het geschil moet door een partij schriftelijk per aangetekende brief kenbaar worden gemaakt aan de wederpartij(en).

2.5 Tarieven

VECOZO brengt geen kosten in rekening voor het verkrijgen en gebruik van het certificaat, binnen de gestelde maxima. De betrokken zorgverzekeraars nemen alle kosten op zich (ook weer binnen de gestelde maxima).

2.6 Publicatie en elektronische opslagplaats

2.6.1 Publicatie van VECOZO-informatie

Deze VECOZO CP is in elektronische vorm te vinden op de website van VECOZO (www.vecozo.nl) en kan daarnaast worden opgevraagd bij VECOZO. Voor de contactgegevens wordt verwezen naar paragraaf 1.3. Voor het toesturen van deze VECOZO CP wordt EUR 25,- in rekening gebracht. Het CPS is een vertrouwelijk document en wordt niet buiten de VECOZO-organisatie verstrekt.

2.6.2 Certificaat statusinformatie

De certificaat statusinformatie wordt in een Certification Revocation List (CRL) gepubliceerd. Getronics verzorgt de publicatie van deze CRL in een specifiek voor VECOZO bestemde directory, die niet publiek toegankelijk is. Ten behoeve van de controle van de geldigheid van de certificaten wordt elke 24 uur de door Getronics gepubliceerde CRL door VECOZO gedownload.

2.6.3 Toegangscontrole tot gepubliceerde informatie

De publieke informatie is vrij toegankelijk op de website van VECOZO. De uitgegeven certificaten zijn alleen toegankelijk voor VECOZO en vereisen een toegangscontrole, alvorens hiertoe toegang kan worden verkregen.

2.7 Audit

2.7.1 Object van onderzoek

Alle aspecten van de VECOZO-certificaatdienstverlening worden tijdens een zogenaamde WebTrust-audit door een derde partij beoordeeld. De overige door VECOZO aangeboden diensten, zoals de controle op het verzekeringsrecht en het verwerken van on-line ingediende declaraties en de algemene informatiebeveiliging worden in een separate audit beoordeeld.

2.7.2 Normenkader en auditororganisatie

Voor de WebTrust-audit wordt het WebTrust for CAs-programma³ als normenkader gehanteerd. VECOZO laat door een externe auditor een onderzoek tegen deze WebTrust-standaard uitvoeren. Dit onderzoek kenmerkt zich door een initieel onderzoek en een jaarlijks herhalingsonderzoek. Na drie jaar wordt er weer een nieuw initieel onderzoek uitgevoerd. De audit moet worden uitgevoerd door een auditor die gerechtigd is om formele WebTrust-

³ www.webtrust.org



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 portaal diensten wordt door een externe auditor een specifiek normenkader gehanteerd.

2.7.3 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.

2.7.4 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.

2.8 Vertrouwelijkheid

Binnen de VECOZO-certificaatdienstverlening wordt onderstaande informatie als vertrouwelijk beschouwd:

- *Administratieve gegevens met betrekking tot een aanvraag voor een certificaat*
Alle gegevens die door of over de contactpersoon, certificaathouder en certificaatgebruiker 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 en daadwerkelijke intrekking van een certificaat. Deze gegevens worden bijvoorbeeld tijdens het indienen van een verzoek tot intrekking van een certificaat aan VECOZO verschaft.

Vertrouwelijke informatie is volledig beschermd tegen onthulling zonder de toestemming van de betrokkenen, een rechterlijk bevel of een andere wettelijke grondslag.

VECOZO garandeert dat door hen de Wet Bescherming Persoonsgegevens (WBP) wordt nageleefd voor wat betreft de uitvoering van de certificaatdienstverlening. Toepasselijke technische en organisatorische maatregelen zijn genomen tegen ongeautoriseerde of onwettige verwerking van persoonsgegevens en tegen onvoorzien verlies, vernietiging of beschadiging van persoonsgegevens. Indien de certificaathouder, contactpersoon of certificaatgebruiker dit wenst, kan inzicht worden gegeven in de over hem vastgelegde gegevens. Op de website van VECOZO is de VECOZO privacy policy gepubliceerd.

2.9 Intellectuele eigendomsrechten

De intellectuele eigendomsrechten van de door VECOZO uitgegeven certificaten en de VECOZO Certificate Policy berusten bij VECOZO. VECOZO garandeert geen inbreuk te maken op intellectuele eigendomsrechten van derden.



3 Identificatie en authenticatie

3.1 Initiële registratie

3.1.1 Soorten naamformaten

De weergave van de naam van de certificaatgebruiker in het certificaat moet voldoen aan het veld 'subject' zoals dit is opgenomen in het certificaatprofiel voor VECOZO-certificaten. Bij een systeemcertificaat wordt in het subject-veld het certificaatnummer opgenomen. Hiervoor wordt verwezen naar hoofdstuk zeven van deze CP.

3.1.2 Noodzaak voor betekenisvolle namen

Op basis van het veld 'subject' in het certificaat moet de identiteit van de certificaatgebruiker kunnen worden vastgesteld. Uitzondering is de uitgifte van systeemcertificaten. Reden is dat dit type certificaat niet persoonsgebonden is.

3.1.3 Uniciteit van namen

VECOZO waarborgt zoveel mogelijk dat de naam van een subject slechts eenmaal wordt gebruikt, zodat iedere certificaatgebruiker 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 worden hier in hoofdletters de eerste letter van de voorletters geplaatst plus 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.

De Common Name van het systeemcertificaat wordt als volgt opgebouwd:

Pos. 1 t/m 14: veertien cijferig gebruikersnummer. 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).

3.1.4 Geschillenprocedure inzake naam-claims

In het geval zich een geschil voordoet ten aanzien van naamclaims, zal VECOZO een bindende uitspraak doen jegens de contactpersonen en certificaathouder. Daarnaast heeft VECOZO het recht om een opgegeven naam te wijzigen indien deze in strijd is met het merkenrecht.

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

De certificaatgebruiker genereert zelf zijn private sleutel. Bij de generatie dient de certificaatgebruiker gebruik te maken van een betrouwbaar systeem en de noodzakelijke voorzorgsmaatregelen te nemen om inbreuk, verlies, openbaarmaking, wijziging of onbevoegd gebruik van de geheime sleutel te voorkomen. Tijdens het aanvraagproces dient de certificaatgebruiker 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 gewaarborgd dat de certificaatgebruiker over de juiste private sleutel beschikt.

3.1.6 Authenticatie van een organisatorische entiteit

Binnen de VECOZO-gebruikersgemeenschap is de praktijkhouder (tekenbevoegde van de entiteit) de organisatorische entiteit. VECOZO moet de authenticiteit van de aanvrager verifiëren en moet verifiëren of de aanvrager is gerechtigd om gebruik te mogen maken van de VECOZO-dienstverlening en daarmee samenhangend de VECOZO-certificaatdienstverlening. In de overeenkomst die met de aanvrager wordt afgesloten, zijn de voorwaarden betreffende het gebruik van het certificaat opgenomen.

Om de authenticiteit van de aanvrager vast te stellen, vergelijkt VECOZO onder andere de informatie die door de aanvrager is verstrekt met het AGB-bestand van Vektis. Indien de certificaathouder nog niet in het AGB-bestand is opgenomen, dient de aanvrager contact op te nemen met Vektis. Indien het om een partij gaat die niet in Vektis wordt geregistreerd, wordt er specifiek voor de betreffende partij een contract opgesteld. Wanneer een validatieprocedure niet met succes kan worden afgerond, dan zal VECOZO de certificaataanvraag afwijzen. De aanvrager wordt dan terstond op de hoogte gebracht van de mislukte validatie, onder vermelding van de reden van de mislukking. De aanvrager kan indien gewenst opnieuw een aanvraag indienen.

Gebruikers van certificaten zijn zelf verantwoordelijk voor de rechtsgeldigheid van de informatie die ze verstrekken voor gebruik in de certificaten conform deze CP in iedere jurisdictie waarin deze inhoud kan worden gebruikt of bekeken.

3.1.7 Authenticatie van een persoonlijke identiteit

De certificaathouder geeft een contactpersoon op die namens de certificaathouder certificaten mag aanvragen. Alle personen die juridisch namens de certificaathouder tekenbevoegd zijn, zijn automatisch contactpersoon. Hiermee is bij VECOZO bekend wie namens de certificaathouder certificaten mag aanvragen. VECOZO controleert of de persoon die de certificaten aanvraagt daadwerkelijk contactpersoon van de betreffende certificaathouder is.



3.2 Certificaatvernieuwing

3.2.1 Routinematige vernieuwing

Het vernieuwen van een certificaat voor het aflopen van de geldigheidsduur van een certificaat wordt beschouwd als routinematige vernieuwing. VECOZO stelt de certificaatgebruiker 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 certificaatgebruiker. De certificaatgebruiker kan vervolgens op de website van VECOZO zijn certificaat vernieuwen. Hiertoe krijgt de certificaatgebruiker instructies van VECOZO. Tijdens de vernieuwing wordt de authenticiteit van de certificaatgebruiker 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.

3.2.2 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 alleen maar vernieuwd worden door het aanvragen van een nieuw certificaat conform de beschreven procedures in paragraaf 3.1. In het geval van niet-routinematige vernieuwing moet altijd een nieuw sleutelpaar en een nieuw certificaat worden aangemaakt.

3.3 Verzoeken tot blokkering

3.3.1 Authenticatie van blokkeringsverzoeken

In uitzonderlijke gevallen kan de VECOZO RA besluiten een gebruiker al dan niet tijdelijk te blokkeren, waarna deze het certificaat niet meer kan gebruiken om te authenticeren.

3.4 Verzoeken tot intrekking

3.4.1 Authenticatie van intrekkingverzoeken

Een verzoek tot intrekking mag door de contactpersoon alleen op papier worden ingediend bij VECOZO. Voor aanvragen van zorgverzekeraars kan een uitzondering worden gemaakt, mits deze via e-mail of schriftelijk zijn ingediend. Deze aanvragen worden te allen tijde bewaard. VECOZO is verplicht om te verifiëren of het intrekkingverzoek van de contactpersoon afkomstig is.



4 Operationele eisen

4.1 Aanvraag van certificaten

Voor de aanvraag van certificaten moet een aanvraagformulier worden ingevuld. Dit aanvraagformulier kan via de website van VECOZO of via de helpdesk worden verkregen. De authenticiteit van de aanvraag dient conform paragraaf 3.1.6 en 3.1.7 te worden geverifieerd. Het aanvraagproces dient te worden geïnitieerd door de certificaathouder of de contactpersoon. Het aanvraagformulier dient volledig en juist te worden ingevuld.

Wanneer de contactpersoon cq de certificaathouder certificaten in aanvulling op de initiële aanvraag wil aanvragen, moet hij hiertoe een schriftelijk (post/fax) en ondertekenend verzoek indienen. Zorgverzekeraars kunnen volstaan met het per e-mail versturen van het standaard aanvraagformulier dat ze van onze website kunnen downloaden.

4.2 Uitgifte van certificaten

VECOZO ziet er op toe dat de certificaten op veilige wijze uitgegeven worden teneinde 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 certificaatgebruiker wordt gegenereerd. VECOZO stuurt de contactpersoon een brief (bij zorgverzekeraars een bericht via de VECOZO berichtenbox) en een e-mail. De certificaatgebruiker kan op basis van de informatie die in de brief en e-mail is opgenomen zijn certificaat downloaden. De contactpersoon is zelf verantwoordelijk voor de interne distributie van de informatie die in de brief en de e-mail is opgenomen.

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 garandeert dat:

- De door de aanvrager verstrekte gegevens op correcte wijze in het certificaat worden opgenomen. 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. Certificaathouders en contactpersonen zijn zelf echter verantwoordelijk voor de rechtsgeldigheid van de informatie die ze verstrekken voor gebruik in de certificaten in iedere jurisdictie waarin deze inhoud kan worden gebruikt of bekeken;
- Het certificaat voldoet aan alle in deze CP gestelde materiële eisen.

4.3 Acceptatie van certificaten

Een certificaatgebruiker 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 certificaatgebruiker 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 certificaatgebruiker aan VECOZO heeft verstrekt ten behoeve van de onder deze CP 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;
- Hij akkoord gaat met de voorwaarden in deze CP;
- Hij zijn geheime sleutel goed zal beheren en afdoende voorzorgsmaatregelen zal nemen om verlies, openbaarmaking, wijziging of onbevoegd gebruik te voorkomen;
- Hij bij verlies, openbaarmaking, wijziging of onbevoegd gebruik dit zo snel mogelijk kenbaar maakt aan de contactpersoon. De contactpersoon maakt dit vervolgens direct kenbaar aan VECOZO.

Door acceptatie van een certificaat verklaart de certificaatgebruiker 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 authenticeren. Het certificaat wordt niet op de CRL geplaatst, waardoor eventuele accounts die door vertrouwende partijen aan het certificaat zijn gekoppeld, niet automatisch ook geblokkeerd worden. 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-applicaties, noch voor applicaties van 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 de certificaathouder of de certificaatgebruiker niet voldoet aan de verplichtingen zoals deze zijn verwoord in deze CP of de overeenkomst die met VECOZO is gesloten;
- Bij ontslag of uitdiensttreding van de certificaathouder;



- Bij het overlijden van de certificaatgebruiker of wanneer de bijbehorende certificaathouder is opgehouden te bestaan;
- Ter voorkoming van een calamiteit.
- Indien de pincode en het gebruikersnummer van een certificaat (vermoedelijk) zijn gecompromitteerd.

Een gebruiker kan in buitengewone situaties op verzoek geblokkeerd worden (bijvoorbeeld in afwachting van een schriftelijk intrekkingverzoek in geval van diefstal van een computersysteem). Of VECOZO overgaat tot blokkering is ter beoordeling van de VECOZO RA. Ook kan een gebruiker geblokkeerd worden indien deze geen gebruik meer mag maken van VECOZO-applicaties, maar nog wel van applicaties van vertrouwende partijen. Indien een certificaatgebruiker tijdens de inlogprocedure vijf maal een foutief wachtwoord invoert, wordt de gebruiker automatisch geblokkeerd.

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 contactpersoon;
- VECOZO;
- Getronics (alleen in uitzonderlijke gevallen).

Een bij VECOZO aangesloten partij mag ook een verzoek tot intrekking of blokkering doen. Een melding van een aangesloten partij kan, na nader onderzoek, tot intrekking van het betreffende certificaat of blokkering van de betreffende gebruiker leiden.

Indien een gebruiker is geblokkeerd omdat de gebruiker vijf maal een foutief wachtwoord in heeft gevoerd, dan kan de contactpersoon maar ook de certificaatgebruiker zelf een verzoek doen om de gebruiker te deblokken.

4.4.3 Procedure voor een verzoek tot intrekking of blokkering

De contactpersoon, VECOZO, Getronics of een vertrouwende partij kan schriftelijk een verzoek tot intrekking indienen. VECOZO zal de authenticiteit van dit verzoek en van ieder ander verzoek valideren. Indien de contactpersoon, VECOZO, Getronics of een vertrouwende partij een verzoek tot intrekking indient, moet de beweegreden worden vastgelegd. Het is voor de gebruiker zelf ook mogelijk om via de VECOZO-website een certificaat in te trekken. Bij een persoonlijk certificaat zal de certificaatgebruiker met het in te trekken certificaat in moeten loggen, met een systeemcertificaat dient de gebruiker op de website zowel het certificaat als de oorspronkelijke pincode aan te bieden.

Het serienummer van het ingetrokken certificaat en de intrekkingdatum worden gepubliceerd in de CRL. Daarnaast wordt de contactpersoon op de hoogte gesteld van het feit dat het betreffende certificaat is ingetrokken.

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 intrekings-/blokkeringsdienst

Ten behoeve van het laten intrekken of blokkeren is de VECOZO RA tijdens kantooruren en op werkdagen van 9.00 uur tot 17.00 uur bereikbaar.

4.4.5 CRL-uitgiftefrequentie

De CRL wordt iedere 24 uur door Getronics opnieuw gepubliceerd en wordt elke 24 uur door VECOZO gedownload. De intrekingsstatus is 24 uur per dag / 7 dagen per week beschikbaar waarbij een beschikbaarheidspercentage van 99% wordt geboden en de maximale toegestane uitval bij incidenten en calamiteiten respectievelijk 2 uur en 1 dag is.

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.

4.4.7 Andere vormen van publiceren intrekkingstatus

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

4.5 Security auditprocedures

4.5.1 Vastlegging van gebeurtenissen

De belangrijkste activiteiten die door de medewerkers van VECOZO worden uitgevoerd, worden in de beheerapplicatie en bijbehorende logbestanden vastgelegd. Hiermee wordt gewaarborgd dat alle gebeurtenissen ten aanzien van de levenscyclus van de certificaten worden vastgelegd. De logbestanden worden door Getronics bewaard. Een VECOZO-medewerker, die niet werkzaam is bij de RA, kan de logbestanden bekijken. 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.

Getronics houdt zelf ook logbestanden bij ten aanzien van de VECOZO-dienstverlening en de VECOZO CA, zoals gehuisvest bij Getronics. Meer informatie hieromtrent kan worden gevonden in het CPS van Getronics.

4.5.2 Interval vastleggingen

De in paragraaf 4.5.1 beschreven vastleggingen worden direct na het uitvoeren van de betreffende activiteit uitgevoerd. In geval van incidenten en calamiteiten worden de vastleggingen geanalyseerd.

4.5.3 Bewaartermijn

VECOZO garandeert dat de vastleggingen met betrekking tot certificaten minimaal bewaard blijven gedurende de wettelijk vereiste periode, noodzakelijk voor het leveren van bewijs van certificatie in een rechtsgang.

4.5.4 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.



4.5.5 Back-up logbestanden

Van de logbestanden wordt een back-up gemaakt die op een veilige locatie wordt bewaard.

4.6 Archivering van documenten

VECOZO archiveert tenminste de volgende documenten en informatie:

- De overeenkomst (zowel de overeenkomst met de certificaathouder als de overeenkomst tussen de zorgverzekeraar en de certificaathouder) ten behoeve van een certificaataanvraag;
- Alle informatie en documentatie die is gebruikt voor het verifiëren van de certificaataanvraag;
- Intrekkingsverzoeken en bijbehorende informatie en documentatie die is gebruikt voor het verifiëren van het intrekkingsverzoek.

4.6.1 Bewaartermijn archief

Archieven worden voor de periode van de geldigheidsduur van de overeenkomst bewaard. Hierbij wordt minimaal 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. Er wordt geen back-up gemaakt van het archief waarin de papieren documenten zijn opgeslagen.

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 3.2 zijn gesteld. Bij vernieuwing van een certificaat dient altijd het sleutelpaar te worden vernieuwd.

In het geval het sleutelpaar van de VECOZO CA wordt vernieuwd, zullen de vertrouwende partijen hiervan op de hoogte worden gebracht.

4.8 Aantasting en continuïteit

4.8.1 Continuïteit

Ten behoeve van de waarborging van de continuïteit van de certificaatdienstverlening heeft VECOZO een calamiteiten- en continuïteitsplan opgesteld. VECOZO heeft een aanzienlijk deel van de certificaatdienstverlening uitbesteed aan Getronics, daarom zijn in beide plannen ook uitgangspunten en maatregelen geformuleerd ten aanzien van de leveranciers. Het continuïteitsplan gaat vooral in op het voorkomen van verstoringen. In het continuïteitsplan zijn maatregelen ten aanzien van de volgende onderdelen geformuleerd:

- Telefooncentrale;
- Kantoorautomatiseringsservers;
- Data;



- Externe koppelingen;
- Gebouwen;
- Personeel;
- Systeemontwikkeling en -onderhoud.

Het calamiteitenplan beschrijft de organisatie en de activiteiten die noodzakelijk zijn om snel en afdoende op een buitengewone verstoring van de dienstverlening (calamiteiten) te reageren. In het calamiteitenplan zijn activiteiten en maatregelen ten aanzien van de volgende onderdelen geformuleerd:

- Alarmeringsprocedure;
- Crisisorganisatie;
- Noodplan;
- Uitwijkplan;
- Herstelplan;
- Testplan.

Uiteraard heeft Getronics ook maatregelen ten aanzien van de continuïteit van de dienstverlening getroffen. Meer informatie hieromtrent kan worden gevonden in het CPS van Getronics.

4.8.2 Aantasting

Indien de private sleutel van de VECOZO CA (mogelijk) is gecompromitteerd, wordt het bijbehorende certificaat ingetrokken. In dit 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.

4.9 CA-beëindiging

4.9.1 Berichtgeving aan betrokken partijen

Indien VECOZO de certificaatdienstverlening beëindigt, worden de entiteiten uit de gebruikersgemeenschap ingelicht en geïnformeerd via de website van VECOZO.

4.9.2 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 4.9.1.



4.9.3 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 Fysieke, procedurele en personele beveiliging

5.1 Algemeen

VECOZO heeft een informatiebeveiligingsbeleid (IBB) opgesteld. In dit beleid zijn beleidsuitgangspunten opgesteld ten aanzien van de informatiebeveiliging binnen VECOZO. VECOZO heeft een aanzienlijk deel van de dienstverlening uitbesteed aan Getronics, daarom zijn in het IBB ook uitgangspunten geformuleerd ten aanzien van de informatiebeveiliging bij de leveranciers. Daarnaast is de beveiligingsorganisatie als volgt gespecificeerd:

- *Management*
Het management is verantwoordelijk voor de vaststelling en doen uitvoeren van het IBB. De infrastructuur van de informatiebeveiliging, die nodig is voor het beheren van de beveiliging binnen VECOZO, wordt te allen tijde in stand gehouden. Iedere verandering die invloed zal hebben op het beveiligingsniveau dient te worden goedgekeurd door het management van VECOZO.
- *Leidinggevenden*
De leidinggevenden zijn gedelegeerd verantwoordelijk voor de implementatie en de uitvoering van het IBB.
- *Medewerkers*
De medewerkers zijn persoonlijk verantwoordelijk voor alle aspecten van beveiliging met betrekking tot de functie die zij vervullen. Gebruikers dienen de beveiligingsprocedures te leren en op correcte wijze om te gaan met de ICT-voorzieningen.
- *Beveiligingsfunctionaris*
De beveiligingsfunctionaris vervult een essentiële rol bij het onderhouden en implementeren van het IBB. Hij rapporteert aan het VECOZO-management en houdt tevens toezicht op de algehele werking van het beleid en ondersteunt de implementatie.
- *Audit*
Zie paragraaf 2.7.

Op basis van het IBB heeft VECOZO een risicoanalyse uitgevoerd en de resultaten hiervan vastgelegd en heeft VECOZO, op basis van de Code voor Informatiebeveiliging, een informatiebeveiligingsplan (IBP) opgesteld. In het IBP zijn de door VECOZO getroffen beveiligingsmaatregelen beschreven.

Aangezien VECOZO een gedeelte van de certificaatdienstverlening heeft uitbesteed, wordt op hoofdlijnen aangegeven welke fysieke, procedurele en personele beveiligingsmaatregelen Getronics heeft getroffen. Daarnaast heeft VECOZO in haar IBP maatregelen opgenomen ten aanzien van beveiligingsmaatregelen bij uitbesteding. In navolgende paragrafen wordt vervolgens ingegaan op de beveiliging ten aanzien van VECOZO.

- *Getronics*
De Getronics-omgeving voldoet ook aan strenge fysieke, personele en procedurele beveiliging. Voor nadere informatie omtrent de getroffen beveiligingsmaatregelen wordt verwezen naar het Getronics CPS (hoofdstuk vijf).



5.2 Fysieke beveiliging

In het IBP wordt de fysieke beveiliging uitgebreid geadresseerd. Het doel van, c.q. de eis aan de door VECOZO te treffen maatregelen is het voorkomen van ongeautoriseerde toegang tot locaties, schade of verstoring van de gebouwen, diensten, informatiebedrijfsmiddelen en gegevens. VECOZO heeft hiertoe fysieke beveiligingsmaatregelen getroffen op de volgende aspecten:

- Toegang tot de kritieke ruimten (server ruimte, elektriciteitsvoorziening, ruimte voor opslagmedia en archieven), inclusief richtlijnen voor het werken in kritische ruimten en toegang door externe partijen;
- Beveiliging van ICT-apparatuur. Hieronder valt het plaatsen en beveiligen van apparatuur, stroomvoorziening, beveiliging van voeding en telecommunicatiebekabeling, onderhoud van ICT-apparatuur, afvoeren en hergebruik van ICT-apparatuur, clean desk en clear screen policy en het verwijderen van bedrijfseigendommen.

Daarnaast garandeert VECOZO dat fysieke toegang tot kritieke diensten wordt beheerst en dat fysieke bedreiging van de middelen wordt geminimaliseerd.

5.3 Procedurele beveiliging

In het IBP wordt de procedurele beveiliging uitgebreid geadresseerd. In de navolgende paragrafen wordt hierop nader ingegaan.

5.3.1 Functies

VECOZO handhaaft scheiding in taken en verantwoordelijkheden om het risico van onbevoegde wijziging of misbruik van informatie of diensten te beperken. Hierbij wordt onderscheid gemaakt tussen uitvoerende, beslissende en controlerende taken. Binnen VECOZO wordt verder functiescheiding toegepast tussen systeemontwikkelingsorganisatie, verwerkingsorganisatie, helpdesk en toezicht en controle.

5.3.2 Beheer en beveiliging

In het IBP zijn de volgende maatregelen opgenomen omtrent beheer en beveiliging:

- scheiding van de ontwikkel-, test- en acceptatieomgeving en ontwikkeling en onderhoud van systemen;
- beheerprocedures voor wijzigingen en incidenten;
- netwerkbeheer;
- beheer en beveiliging van media;
- capaciteitsplanning en acceptatie systemen;
- huisregels (maken back-up en bijhouden logboek);
- uitwisseling van informatie en software
- bescherming tegen kwaadaardige software;
- logische toegangsbeveiliging;
- naleving en toezicht.



5.4 Personele beveiliging

In het IBP wordt de personele beveiliging uitgebreid geadresseerd. Het doel van, c.q. de eis aan de door VECOZO te treffen maatregelen is het zo goed mogelijk benutten en op het vereiste niveau houden van de kennis en ervaring van de medewerkers ter bevordering van de beveiliging alsmede het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen. VECOZO heeft hiertoe personele beveiligingsmaatregelen getroffen op de volgende aspecten:

- Beveiligingstaken, (beveiligings)verantwoordelijkheden en vertrouwelijke (gevoelige) functies. Deze zijn gedocumenteerd in functieomschrijvingen waarbij rekening wordt gehouden met de scheiding van taken en bevoegdheden;
- Bij werving evaluatie van personeel met vertrouwelijke functies;
- Opleiding en training van gebruikers;
- Melding van beveiligingsincidenten;
- Procedures voor alle vertrouwelijke en administratieve taken, die invloed hebben op de levering van certificaatsdiensten;
- Onafhankelijkheid en onpartijdigheid van het VECOZO-personeel in vertrouwelijke functies.

5.4.1 Vakkennis, ervaring en kwalificaties

VECOZO zet personeel in dat beschikt over vakkennis, ervaring en kwalificaties die noodzakelijk zijn voor de aangeboden diensten en die toereikend zijn voor de functie. VECOZO heeft hiernaast voldoende personeel in dienst met de noodzakelijke opleiding, training, technische kennis en ervaring voor het soort, de reikwijdte en de hoeveelheid werk dat nodig is voor het leveren van certificaatsdiensten.



6 Technische beveiliging

6.1 Genereren en installeren van de sleutelparen

6.1.1 Genereren van VECOZO-sleutelbaar

Het genereren van de sleutels van VECOZO vindt plaats onder controleerbare en beheersbare omstandigheden in hardware (zogenaamde Hardware Security Module). De generatie vindt plaats in een fysiek beveiligde 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. Aangezien deze activiteit wordt uitgevoerd door Getronics, wordt voor meer informatie verwezen naar het Getronics CPS (hoofdstuk zes).

6.1.2 Genereren van de eindgebruikerssleutelparen

De certificaathouder genereert tijdens het aanvraag- en uitgifteproces zelf zijn sleutelbaar. Iedere gebruiker van een certificaat 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.

6.1.3 Overdracht publieke sleutel van certificaatgebruiker aan VECOZO

De publieke sleutel van de certificaatgebruiker wordt door middel van een versleutelde verbinding aan de VECOZO CA verstuurd.

6.1.4 Overdracht van publieke sleutel van VECOZO aan gebruikers

Op de website van VECOZO kan het certificaat van de VECOZO CA worden gedownload en kan de gebruiker het VECOZO CA-certificaat installeren in zijn browser.

6.1.5 Sleutellengten

Eindgebruikerssleutels

Voor de sleutelparen van de eindgebruikerscertificaten worden RSA-sleutels met een sleutellengte van 1024 bits gebruikt.

VECOZO-sleutels

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

6.1.6 Doelen sleutelgebruik

Eindgebruikerssleutels

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

VECOZO-sleutels

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



6.2 Private sleutelbescherming

6.2.1 Eindgebruikers

Voor het verkrijgen van toegang tot VECOZO-applicaties middels een persoonlijk certificaat, dient een gebruiker te beschikken over een wachtwoord. Bij verlies van het wachtwoord kan de contactpersoon dit door VECOZO laten resetten. Ook kan de gebruiker dit zelf via de VECOZO-website aanvragen.

6.2.2 VECOZO CA

De VECOZO CA is ondergebracht bij Getronics. Getronics heeft vergaande beveiligingsmaatregelen getroffen op het gebied van logische en fysieke toegangsbeveiliging. Hiertoe wordt verwezen naar het CPS van Getronics.

6.2.3 VECOZO RA

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

6.2.4 Escrow

Zowel de VECOZO sleutels als de sleutels van de eindgebruikers worden niet in escrow genomen.

6.2.5 Back-up

Certificaatgebruikers 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. VECOZO kan derhalve de private sleutel van de certificaatgebruiker niet herstellen. Indien een certificaat onverhoopt verloren gaat, kan de contactpersoon bij VECOZO een nieuw certificaat aanvragen.

6.2.6 Archivering

Na afloop van de levensduur van het VECOZO CA sleutelbaar wordt deze niet gearchiveerd.

Certificaatgebruikers zijn zelf verantwoordelijk voor het archiveren van hun sleutelbaar na het aflopen van de geldigheidsduur en de te treffen beveiligingsmaatregelen ten aanzien van de archivering.

6.2.7 Activeren en deactiveren private sleutel VECOZO

Zie paragraaf 6.2.2.

6.2.8 Methode van vernietiging

De private sleutel van de VECOZO CA (en kopieën daarvan) worden na afloop van de levensduur op een dusdanige wijze vernietigd dat deze niet meer opnieuw in gebruik kunnen worden genomen.

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



6.3 Overige aspecten van sleutelpaarmanagement

6.3.1 Gebruiksdur sleutels

De geldigheidsduur van de VECOZO CA-sleutels en -certificaten is vijf jaar. VECOZO garandeert dat de sleutels van de VECOZO CA niet worden gebruikt na het einde van hun levenscyclus.

De sleutels en certificaten van certificaatgebruikers / eindgebruikers hebben een maximale geldigheidsduur van één jaar. De certificaatgebruiker mag het certificaat niet na afloop van de geldigheidsduur van het certificaat gebruiken.

6.4 Activeringsgegevens

Het certificaat van de eindgebruiker kan alleen worden opgehaald wanneer de certificaatgebruiker beschikt over de gebruikerscode en de pincode. Bij verlies van de pincode kan er op verzoek een nieuwe pincode naar de contactpersoon gestuurd worden.

6.5 Computerbeveiligingsmaatregelen

VECOZO garandeert dat toegang tot systeemfuncties voor informatie en applicaties – overeenkomstig het toegangscontrolebeleid – wordt beperkt en dat het VECOZO-systeem voldoende computerbeveiligingsmiddelen biedt voor de scheiding van vertrouwelijke taken, zoals deze door VECOZO zijn onderkend. VECOZO-personeel wordt geïdentificeerd en geauthenticeerd, voordat zij gevoelige applicaties kunnen gebruiken, die te maken hebben met het beheer van certificaten. Daarnaast wordt in hoofdstuk vijf nader ingegaan op de getroffen beveiligingsmaatregelen. Hieronder vallen ook de computerbeveiligingsmaatregelen.

6.6 Beheersmaatregelen technische levenscyclus

VECOZO heeft maatregelen getroffen om te waarborgen dat systeemontwikkeling en -onderhoud op een betrouwbare manier wordt uitgevoerd. Dit onderwerp wordt behandeld in het informatiebeveiligingsplan. Zie hiertoe ook de maatregelen zoals beschreven in hoofdstuk vijf.

6.7 Netwerkbeveiligingsmaatregelen

Beheersmaatregelen zijn geïmplementeerd om de interne netwerkdomeinen van VECOZO te beschermen tegen externe netwerkdomeinen die toegankelijk zijn voor derden. Gevoelige gegevens worden beschermd wanneer zij worden uitgewisseld via netwerken die niet zijn beveiligd. Voortdurende bewakings- en alarmeringsfaciliteiten zijn aangebracht om VECOZO in staat te stellen om niet-geautoriseerde en/of onrechtmatige pogingen om toegang te krijgen tot haar middelen te ontdekken, registreren en er tijdig op te reageren. Daarnaast wordt in hoofdstuk vijf nader ingegaan op de getroffen beveiligingsmaatregelen. Hieronder vallen ook de netwerkbeveiligingsmaatregelen.

6.8 Cryptografische module beveiligingsmaatregelen

Zie paragraaf 6.1.1.



7 Certificaat en CRL-profiel

7.1 Certificaatprofiel

Alle typen certificaten zijn gebaseerd op de X.509v3-standaard. In onderstaande tabel is het certificaatprofiel van de twee typen certificaten weergegeven. Het enige verschil tussen persoonlijke- en systeemcertificaten is de vulling van de Common Name. Zie hiervoor 3.1.3.

Attribuut	Beschrijving / waarde
Versie	V3
Serienummer	Uniek serienummer
Algoritme voor handtekening	-
Verlener	CN = VECOZO - G2 O = Vecozo B.V. C = NL
Geldig van	Ingangsdatum geldigheidsduur certificaat
geldig tot	Einddatum geldigheidsduur certificaat
Onderwerp	E = emailadres CN = zie 3.1.3 OU = Veilige communicatie in de zorg O = Vecozo B.V.
Openbare sleutel	-
Essentiële beperkingen	Subjecttype=Eindidentiteit Beperking voor padlengte=Geen
Sleutelgebruik	Digitale handtekening, Sleutelcodering (a0)
Netscape-certificaatype	SSL Client verificatie(80)
CRL distributiepunten	[1]CRL-distributiepunt Naam van distributiepunt: Volledige naam: URL=http://pki.pinkroccade.com/crl/VecozoBVVeiligecomunicatieindezorg/LatestCRL.crl
2.16.840.1.113733.1.6.9	01 01 ff
Algoritme van vingerafdruk	-
Vingerafdruk	Vingerafdruk van het certificaat

Tabel 1: Certificaatprofiel X.509v3 persoonlijk certificaat

Attribuut	Beschrijving / waarde
Versie	V3
Serienummer	Uniek serienummer
Algoritme voor handtekening	-
Verlener	CN = VECOZO - G2 O = Vecozo B.V. C = NL
Geldig van	Ingangsdatum geldigheidsduur certificaat
Geldig tot	Einddatum geldigheidsduur certificaat



Attribuut	Beschrijving / waarde
Onderwerp	E = e-mailadres CN = Zie 3.1.3 OU = Veilige communicatie in de zorg O = Vecozo B.V.
Openbare sleutel	-
Essentiële beperkingen	Subject Type=End Entity Path Length Constraint=None
Sleutelgebruik	Digitale handtekening, Sleutelcodering (a0)
Netscape-certificaatype	SSL Client Authentication (80)
CRL distributiepunten	[1]CRL-distributiepunt Naam van distributiepunt: Volledige naam: URL=http://pki.pinkroccade.com/crl/VecozoBVVeiligecomunicatieinzorg/LatestCRL.crl
2.16.840.1.113733.1.6.9	01 01 ff
Algoritme van vingerafdruk	-
Vingerafdruk	Vingerafdruk van het certificaat

Tabel 2: Certificaatprofiel X.509v3 systeemcertificaat

CRL-profiel

7.1.1 Versienummer CRL

VECOZO geeft X.509 versie 1 CRL's uit.

7.1.2 CRL-velden en CRL-extensies

Attribuut	Beschrijving / waarde
Versie	V1
Verlener	CN = VECOZO - G2 O = Vecozo B.V. C = NL
Ingangsdatum	Ingangsdatum van CRL
Volgende update	Datum en tijdstip van update CRL
Algoritme voor handtekening	sha1RSA

Tabel 3: CRL-profiel X.509v3 G2-certificaat



8 Specificatie van onderhoud op CP

8.1 Wijzigingsprocedure voor de CP

8.1.1 Wijzigingen zonder bekendmaking

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

8.1.2 Wijzigingen waarbij bekendmaking is verplicht

Alle wijzigingen in de CP die niet onder paragraaf 8.1.1 vallen en die impact hebben op de certificaathouders en -gebruikers, worden minimaal 30 dagen voordat de wijzigingen in werking treden bekend gemaakt aan de VECOZO gebruikersgemeenschap. De voorgestelde wijzigingen worden op de website van VECOZO gepubliceerd. De wijzigingen en daarmee de nieuwe versie van de CP treden in werking op het moment dat de nieuwe CP op de website is gepubliceerd en aan de bekendmakingplicht is voldaan.

8.2 Publicatie van de CP

De VECOZO CP is in elektronische vorm te vinden op de website van VECOZO (www.VECOZO.nl) en kan daarnaast worden opgevraagd bij VECOZO. Voor de contactgegevens wordt verwezen naar paragraaf 1.3. Voor het toesturen van de VECOZO CP wordt EUR 25,- in rekening gebracht.

8.3 Goedkeuringsprocedure voor de CP

Wijzigingen in de CP moeten door de VECOZO Policy Management Authority worden goedgekeurd. Een uitzondering hierop betreffen de wijzigingen, zoals gedefinieerd in paragraaf 1.3.3, die moeten worden goedgekeurd door de AvA.