ABZ

CERTIFICATION PRACTICE STATEMENT

DIGITAAL PASPOORT

versie: 4.3

Zeist, Juni 2015

Afkortingen

ACL	Access Control List
ASP	Application Service Provider
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certification Revocation List
DES	Data Encryption Standard
DIS	Document Information System
GBC	KPN Business Continuity.
http	Hypertext Transfer Protocol
ISO	International Organization for Standardization
I&A	Identificatie & Authenticatie
ITU	International Telecommunications Union
KvK	Kamer van Koophandel
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
NCSC	Nationaal Cyber Security Centrum (voorheen GOVCERT.NL)
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PPC	Persoonlijke Paspoort Code
RA	Registration Authority
RA-O	RA Operator
RA-P	RA Provider
RA-Q	RA Requestor
RC4	Rivest Cipher 4
RFC	Request For Comment
RSA	Rivest, Shamir & Adleman
SHA-2	Secure Hash Algorithm-2
SLA	Service Level Agreement
SMS	Short Message Service
SSL	Secure Sockets Layer
TTP	Trusted Third Party
UPS	Universal Power Supply

Begripsomschrijvingen

ABZ	ABZ, onderdeel van Solera Inc., voorheen ADP Business Services, voorheen ABZ Nederland.
Certification Authority (CA)	Het TTP-onderdeel dat verantwoordelijk is voor het technisch en procedureel beheren van de CA.
CRL	De CRL is een bestand met ingetrokken certificaten dat wordt bijgewerkt nadat een Digitaal Paspoort is ingetrokken. Ook wel zwarte lijst genoemd.
Digitaal Paspoort	Het Digitaal Paspoort is een persoonsgebonden certificaat volgens de ITU-T x.509v3 standaard. (tevens ISO 9594-8 standaard.
Digitaal Paspoort Beheerder	Een door de tekenbevoegde gemachtigde medewerker die online aanvragen voor Digitale Paspoorten kan indienen.
Digitaal Paspoort website	https://dp.abz.nl
Document Information System (DIS)	Systeem waarmee documenten, voorzien van indexgegevens, digitaal worden opgeslagen.
Eind-entiteit	Gebruiker (genoemd in certificaten) en/of Relying Party (vertrouwend op certificaten).
Gebruiker	Persoon die in het certificaat genoemd staat als houder en gebruiker van het certificaat.
Handtekening	Een handtekening op papier of een ingescande handtekening in elektronisch formaat.
Informatieleverancier	Partij die vanuit een beveiligde digitale omgeving informatie aanbiedt.
Machtiging	Het beleggen van de verantwoordelijkheid voor het behandelen van Digitale Paspoort verantwoordelijkheden bij een ander dan de tekenbevoegde. Een machtiging kan zowel via een papieren opdracht als via een digitale opdracht worden verstrekt.
Persoonlijke Paspoort Code (PPC)	Code die gebruikt wordt bij het ophalen, het verlengen en het intrekken van een Digitaal Paspoort. Deze code wordt door ABZ na de aanmeldingsprocedure aan de gebruiker verstrekt.
PKI	Public Key Infrastructure. Dit is het geheel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op public key cryptografie. Berichten worden hierbij versleuteld en ontsleuteld met asymetrische sleutelparen, bestaande uit een openbare “publieke sleutel” en een geheime “privésleutel”. Het doel is het mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.
Post	Daar waar in dit CPS gesproken wordt van ‘post’, wordt hieronder zowel papieren als elektronische post verstaan, hieronder begrepen berichten per SMS.
Privésleutel	Een wiskundige code die strikt geheim moet worden gehouden door de rechtmatige houder ervan en die gebruikt kan worden om een digitale handtekening te creëren of om met de publieke sleutel versleutelde elektronische informatie weer leesbaar te maken.
Publieke sleutel	Een wiskundige code die openbaar wordt gemaakt en waarmee een digitale handtekening kan worden geverifieerd, die gemaakt is met de bijbehorende privésleutel, of waarmee elektronische informatie kan worden versleuteld, die daarna

	alleen leesbaar gemaakt kan worden met de bijbehorende privésleutel.
Registration Authority (RA)	Het organisatieonderdeel dat verantwoordelijk is voor het technisch en procedureel beheren van de RA.
RA-Operator (RA-O)	Het organisatieonderdeel dat verantwoordelijk is voor de administratieve afhandeling van de RA-procedures.
RA-Provider (RA-P)	Het organisatieonderdeel dat verantwoordelijk is voor alle RA-werkzaamheden waarvoor de RA-O niet verantwoordelijk is. De RA-P vormt de interface met de CA-omgeving van waaruit de verschillende opdrachten aan de CA worden uitgezet.
RA-Requestor (RA-Q)	Het organisatieonderdeel dat namens de certificaat houder het certificaat verzoek stelt aan de RA-P.
Rekeningafschrift	Kopie van een afschrift van een Nederlandse bank- of girorekening, dat niet ouder is dan één maand en waarop tenminste leesbaar zijn vermeld naam, adres en woonplaats van de rekeninghouder (organisatie en tekenbevoegde), de datum van het afschrift en het rekeningnummer. Andere informatie dan bovengenoemde mag door de aanvrager onleesbaar worden gemaakt.
Relying Party	Partijen die binnen de PKI vertrouwen op de inhoud van een Digitaal Paspoort.
Repository	Directory waarin alle Digitaal Paspoorten worden gepubliceerd.
Root-certificate	Het root-certificate is het hoogste certificaat in de certificaathiërarchie. Het certificaat wordt gebruikt om de digitale handtekening van de Root CA te verifiëren, welke is aangebracht op het subordinate certificate van de subordinate CA of, indien er geen subordinate CA gebruikt wordt, op de eindgebruikercertificaten. Het root-certificate wordt apart opgeslagen.
Sleutelpaar	Een sleutelpaar is de ‘set’ van twee bij elkaar behorende sleutels, te weten de privésleutel en de publieke sleutel.
SSL	Secure Sockets Layer. Het protocol voor authenticatie en encryptie binnen webservers.
Subordinate CA	De subordinate CA is de CA die de certificaten voor gebruikers creëert en ondertekent. Deze ondertekening kan worden geverifieerd door middel van het subordinate certificate.
Tekenbevoegde	Persoon die bevoegd is de certificaataanvraag te ondertekenen en die eindverantwoordelijk is voor het gebruik van het certificaat in zijn organisatie, of door deze persoon gemachtigd persoon. Tekenbevoegd zijn: a. Bij organisaties die zijn ingeschreven in het handelsregister van de KvK: degene die hierin vermeld staat als tekenbevoegde (gevolmachtigde, bestuurder), dan wel degene die door deze persoon gemachtigd is, of b. Bij organisaties die niet staan ingeschreven in het handelsregister van de KvK: degene die als rekeninghouder vermeld wordt op een recent bank- of giroafschrift van een rekening op naam van de organisatie. Indien het rekeningafschrift alleen een persoonsnaam vermeldt, is in het certificaat de naam van de tekenbevoegde identiek aan die van de organisatie.

Uittreksel handelsregister	Een origineel of online opgevraagd uittreksel uit het handelsregister van de Kamer van Koophandel, niet ouder dan zes maanden.
Wedding Ceremony	De procedure voor het creëren en installeren van een CA. Deze omvat onder andere het creëren van het sleutelmateriaal en, indien van toepassing, het creëren van subordinate CA's door een Root CA. Deze subordinate certificaten kunnen door middel van het Root-certificaat worden geverifieerd.

Vuistregels voor het gebruik van het Digitaal Paspoort

Hieronder zijn de belangrijkste punten met betrekking tot het gebruik van het Digitaal Paspoort samengevat. Deze punten geven een globaal overzicht. Voor een compleet beeld van de verantwoordelijkheden van de gebruiker adviseren wij u het integrale document te raadplegen.

1 Gebruik van het Digitaal Paspoort

Het Digitaal Paspoort van ABZ kan worden gebruikt voor authenticatie van de gebruiker ten behoeve van toegangsautorisatie en voor het digitaal ondertekenen en het versleutelen van elektronische bestanden, zoals bijvoorbeeld e-mail in een business-to-business omgeving. Het betreft een zogenaamd Digidentity L3 certificaat, waarvoor een beperking geldt voor het vertrouwen dat aan het certificaat kan worden gehecht. De aansprakelijkheid van ABZ voor schade is gelimiteerd tot een bedrag van US$ 5000 voor het totaal van alle digitale handtekeningen en/of transacties die betrekking hebben op dat certificaat.

2 Geheimhouden Persoonlijke Paspoort Code, privésleutel en wachtwoord

De gebruiker is verplicht de Persoonlijke Paspoort Code (PPC), de privésleutel en het wachtwoord dat toegang geeft tot de privésleutel op adequate wijze te beschermen. Hiermee wordt onder andere bedoeld dat een sterk wachtwoord gekozen dient te worden en dat dit wachtwoord strikt persoonlijk is. De gebruiker is zich ervan bewust dat de bescherming met name bedoeld is om vervalsing of onjuist gebruik van het Digitaal Paspoort tegen te gaan.

3 Aanvragen van een Digitaal Paspoort

Alleen een tekenbevoegde of een gemachtigde van een organisatie kan een Digitaal Paspoort voor een gebruiker aanvragen. De tekenbevoegdheid van deze persoon moet blijken uit een uittreksel uit het handelsregister van de Kamer van Koophandel of uit een door de tekenbevoegde gegeven machtiging.
Ingeval de organisatie niet in het handelsregister is ingeschreven, moet tekenbevoegdheid blijken uit een kopie van een recent giro- of bankafschrift van de organisatie met daarop, naast de bedrijfsnaam, de naam van de tekenbevoegde. De tekenbevoegde zelf identificeert zich met een kopie van een geldig legitimatiebewijs.

Een tekenbevoegde kan een Digitaal Paspoort Beheerder machtigen om namens hem een Digitaal Paspoort voor gebruikers aan te vragen.

De aanvraag met de benodigde bijlagen moet per post (op papier of elektronisch) worden verstuurd. De verstrekte gegevens moeten correct zijn, de naam van de ondertekenaar en van de organisatie moeten overeenkomen met de namen op het uittreksel uit het handelsregister van de Kamer van Koophandel of op het rekeningafschrift. De handtekening op het aanvraagformulier moet gelijkenis vertonen met de handtekening op het legitimatiebewijs. Wordt hieraan niet geheel voldaan, dan wordt het Digitaal Paspoort niet uitgegeven.

Een Digitaal Paspoort Beheerder met een geldig Digitaal Paspoort kan de aanvraag ook online uitvoeren via de hiertoe door ABZ beschikbaar gestelde website.

4 Accepteren van een Digitaal Paspoort

Voordat het Digitaal Paspoort geinstalleerd kan worden, moet namens de certificaathouder een gebruikersovereenkomst worden geaccepteerd. De gebruiker accepteert de gebruikersovereenkomst (en dus het Digitaal Paspoort) door het proces van het ophalen en installeren van het certificaat op de Digitaal Paspoort site (https://dp.abz.nl) te continueren.

5 Indienen verzoek tot intrekking

Gebruikers kunnen met behulp van hun Persoonlijk Paspoort Code hun eigen Digitaal Paspoort intrekken. Tevens kunnen gebruikers een verzoek indienen bij ABZ tot intrekking van hun Digitaal Paspoort door middel van e-mail, brief of telefoon. Indien door een ander dan de gebruiker een verzoek tot intrekking wordt ingediend, kan dit alleen per brief of e-mail en dient de verzoeker zich te identificeren door middel van een kopie van een geldig legitimatiebewijs. De Digitaal Paspoort Beheerder kan Digitale Paspoorten van andere medewerkers van de organisatie online intrekken.

Inhoudsopgave

Structuur en interpretatie

Inleiding

Voor u ligt het Certification Practice Statement (CPS) ten behoeve van het Digitaal Paspoort, het persoonsgebonden certificaat van ABZ. Het is opgesteld als raamwerk voor dit onderdeel van de TTP-dienstverlening van ABZ en beschrijft de door ABZ geleverde dienst, de gehanteerde procedures en de rechten en plichten van de betrokken partijen.

De vorige versie van het CPS is het mogelijk gemaakt om relevante documenten elektronisch aan te leveren. In deze nieuwe versie is de mogelijkheid voor het versturen van informatie per SMS toegevoegd. Daarnaast is een aantal tekstuele verbeteringen aangebracht.

KPMG Risk Management heeft advies verleend over de gestandaardiseerde structuur waarin het CPS is opgesteld. Daarnaast hebben zij de afzonderlijke bestanddelen van het CPS zoals die door ABZ zijn opgesteld aan een inhoudelijke review onderworpen.

Het document heeft tot doel de bij het Digitaal Paspoort betrokken partijen op de hoogte te stellen van de handelwijze van ABZ en te omschrijven aan welke minimumeisen de betrokken partijen moeten voldoen om gebruik te kunnen maken van het Digitaal Paspoort.

Structuur

De voor dit CPS gehanteerde structuur is gebaseerd op en in overeenstemming met de gestandaardiseerde structuur voor een raamwerk voor een Certificate Policy of een Certification Practice Statement, neergelegd in RFC 2527 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

Status, interpretatie en samenhang met andere documenten.

Dit CPS is opgesteld ten behoeve van het realiseren van betrouwbare dienstverlening rond het Digitaal Paspoort. Deze versie (4.2) van januari 2015 vervangt versie 4.1 van december 2014.

Bij door de door ABZ geleverde TTP-diensten wordt gebruik gemaakt een PKI-omgeving van Digidentity (primair) en een managed PKI-omgeving van KPN Nederland B.V. en Symantec Inc (secundair). In sommige onderdelen van dit CPS wordt naar de specifieke CPS-documenten van deze leveranciers verwezen.

1. INTRODUCTIE

1.1 Overzicht

Het Digitaal Paspoort is bestemd voor het op een veilige manier ontsluiten en benaderen van elektronische diensten in een business to business omgeving. In dit CPS wordt beschreven op welke manier ABZ dit realiseert en welke procedures hiervoor gevolgd worden.

Teneinde het Digitaal Paspoort te kunnen uitgeven en beheren heeft ABZ een infrastructuur ingericht voor het leveren van TTP-diensten.

1.1.1 Betrokken partijen

Voor de benodigde infrastructuur voor het uitgeven van het Digitaal Paspoort wordt gebruik gemaakt van de dienstverlening van Digidentity (primair) en KPN/KPN (secundair).
In de primaire keten treedt Digidentiy op als Certification Authority (CA) op basis van haar eigen root CA.
In de secundaire keten levert KPN de TTP-infrastructuur. De infrastructuur voor de uitgifte van het Digitaal Paspoort maakt deel uit van het Symantec Trust Network (VTN), een wereldwijd netwerk van TTP-infrastructuren.

De TTP-dienstverlening van ABZ met betrekking tot het Digitaal Paspoort kent de volgende rolverdeling:

■ ABZ	- TTP-management
■ ABZ	- Registration Authority (RA)
■ ABZ	- RA-operator
■ Digidentity	- Certification Authority (CA) en RA-provider (primair)
■ ABZ	- Certification Authority (CA) (secundair)
■ KPN	- Certification Authority (CA) (secundair)
■ Digidentity	- Root CA (primair)
■ Symantec	- Root CA (secundair)

1.1.2 Overzicht certificaten

Het Digitaal Paspoort is een zogenaamd digitaal certificaat. Naast het Digitaal Paspoort worden binnen de infrastructuur van de ABZ TTP-dienstverlening een aantal andere digitale certificaten onderkend. Deze zijn noodzakelijk voor de uitvoering en het gebruik van de TTP-dienstverlening. In dit CPS worden de volgende certificaten onderscheiden (zie ook 6.1):[1]

■ Digitaal Paspoort	- Een eindgebruikercertificaat dat op basis van de ABZ TTP-dienstverlening wordt uitgegeven. De gebruiker kan dit certificaat toepassen voor het verkrijgen van toegangsautorisatie en het digitaal ondertekenen en versleutelen van

[1] Ofschoon ABZ, naast het Digitaal Paspoort, eveneens een Bedrijfscertificaat uitgeeft, is dit niet opgenomen in het overzicht. Het Bedrijfscertificaat staat los van de Digitaal Paspoort-dienstverlening. Ten behoeve hiervan is een separaat CPS opgesteld.

elektronische bestanden, zoals bijvoorbeeld e-mail.

- CA-certificaten - De certificaten van Digidentity (primair) en van ABZ, Symantec en KPN (secundair) die worden toegepast voor onder andere het produceren van het Digitaal Paspoort.
- RA-provider-certificaten - De certificaten die door de RA-provider worden toegepast om de CA opdracht te geven tot de productie van een Digitaal Paspoort.

1.1.3 Relatie met andere documenten

Onlosmakelijk verbonden met dit CPS is het CPS van Digidentity. Dit is te verkrijgen op de url http://pki.digidentity.eu/validatie
In geval de secundaire CA in het productie proces treedt, geldt het CPS van KPN. Dit is te verkrijgen op de url
https://certificaat.kpn.com/files/CPS/KPN_STN_CPS_v3.5.pdf
De in dit CPS opgenomen bepalingen zijn in lijn met de regels die gelden voor de Digidentity CA (primair) en het Symantec Trust Network (VTN – secundair). Deze laatste zijn neergelegd in het Symantec CPS. Dit is te verkrijgen op de url https://www.Symantec.com/repository/eca/cps/index.html.

1.2 Identificatie

De naamgeving van het CPS is: DigitaalPaspoortCPSv4.2. Er is geen object identifier toegewezen of geregistreerd.

1.3 Gebruikersgroep en toepassingsbereik

1.3.1 Certification Authority

1. Binnen de PKI is de volgende CA operationeel:
   Tot oktober 2010:
   - Symantec Class II Public Primary Certification Authority

   Vanaf November 2008:
   - Symantec Class II Public Primary Certification Authority - G3 Root
   - KPN Nederland BV
   - TTP Services ABZ Nederland CA

   Vanaf juni 2012:
   - Digidentity L3 Root CA (primair)
   - Symantec Class II Public Primary Certification Authority - G3 Root (secundair)
   - KPN Nederland BV (secundair)
   - TTP Services ABZ Nederland CA (secundair)
2. ABZ handelt conform de bepalingen in dit CPS.
3. ABZ stelt dit CPS beschikbaar aan eind-entiteiten binnen de PKI van ABZ.
4. ABZ verwijst op haar Digitaal Paspoort website naar dit CPS.

1.3.2 Registration Authority

1. Binnen de ABZ-PKI vervult Digidentity (primair) of SaaSplaza (secundair) de rol van RA-provider.

2. Digidentity en SaaSplaza handelen conform de bepalingen in dit CPS.
3. Binnen de ABZ-PKI vervult ABZ de rol van RA-Operator.
   ABZ handelt hierbij conform de bepalingen in dit CPS.

1.3.3 Eind-entiteiten

Binnen de PKI zijn de volgende eind-entiteiten te onderscheiden:

1. Assurantietussenpersonen
2. Verzekeringsmaatschappijen
3. Leasemaatschappijen
4. Expertisebureaus
5. Autoschadebedrijven
6. Gevolmachtigden
7. ABZ en Derden

Al deze eind-entiteiten zijn gebruikers, maar kunnen tegelijkertijd partijen zijn die informatie aanbieden.

1.3.4 Toepassing

1. Het Digitaal Paspoort kan binnen de ABZ-PKI worden gebruikt voor authenticatie van de eind-entiteit ten behoeve van toegangsautorisatie en voor het digitaal ondertekenen en het versleutelen van elektronische bestanden, zoals bijvoorbeeld e-mail.
2. Het Digitaal Paspoort is een Digidentity Level 3 certificaat. Het secundaire Symantec certificaat is een zogenaamd VTN klasse 2-certificaat. De aansprakelijkheid van ABZ voor schade is gelimiteerd tot een bedrag van US$ 5.000 voor het totaal van alle digitale handtekeningen en/of transacties die betrekking hebben op dat certificaat.

1.4 Contactgegevens

1.4.1 Administratie

ABZ is verantwoordelijk voor het beheer, waaronder het wijzigingsbeheer, van dit CPS. Voor vragen of opmerkingen kunt u zich wenden tot de in 1.4.2 genoemde contactpersoon.

1.4.2 Contactpersoon

De volgende persoon bij ABZ is verantwoordelijk voor het beheer, onderhoud, interpretatie en de uitleg van dit CPS.

Bedrijf	ABZ
Straat	Huis ter Heideweg 30
Postcode	3705 LZ
Plaats	Zeist
Postbus	Postbus 124
Postcode	3700 AC
Functionaris	Manager TTP-Services
E-mailadres	TTPmanager@abz.nl

2. JURIDISCHE BEPALINGEN

2.1 Verplichtingen van partijen

2.1.1 Verplichtingen van de CA en de RA

2.1.1.1 Kennisgeving aan gebruiker van uitgifte van een Digitaal Paspoort

Na een correct doorlopen aanmeldingstraject stelt de RA-O de gebruiker op de hoogte van de registratie en van de mogelijkheid een Digitaal Paspoort op te halen. Na het succesvol ophalen van een Digitaal Paspoort ontvangt de gebruiker een elektronische melding.

2.1.1.2 Kennisgeving aan anderen dan gebruiker van uitgifte van een Digitaal Paspoort

De RA-P publiceert Digitale Paspoorten in een Repository die toegankelijk is voor alle gebruikers die hiervoor een contract met ABZ hebben afgesloten.

2.1.1.3 Kennisgeving aan gebruiker van schorsing of intrekking van een Digitaal Paspoort

Digitale Paspoorten kunnen niet worden geschorst. Wordt een Digitaal Paspoort ingetrokken, dan wordt de gebruiker hiervan onmiddellijk door de RA-O op de hoogte gesteld, onder opgave van redenen die aanleiding hebben gegeven tot intrekking.

2.1.1.4 Kennisgeving aan anderen dan gebruiker van schorsing of intrekking van een Digitaal Paspoort

Digitale Paspoorten kunnen niet worden geschorst. In geval van intrekking van een Digitaal Paspoort, worden anderen dan de gebruiker van het Digitaal Paspoort hiervan onmiddellijk door de CA op de hoogte gesteld door de aangepaste Repository (whitelist) en door publicatie van de intrekking op de certificate revocation list (CRL). In het Digitaal Paspoort is het internetadres opgenomen van de plaats waar de CRL gepubliceerd wordt. De in onderdeel 4.4 beschreven procedure is van overeenkomstige toepassing.

2.1.1.5 Nauwkeurigheid van gegevens

Door de publicatie van het Digitaal Paspoort in de Repository garandeert de RA-O aan een ieder die in redelijkheid op de informatie in het Digitaal Paspoort mag vertrouwen, dat de CA het Digitaal Paspoort heeft uitgegeven aan de gebruiker die daarin wordt genoemd en dat de gebruiker het Digitaal Paspoort heeft geaccepteerd.

2.1.1.6 Tijdsinterval tussen aanvraag en uitgifte Digitaal Paspoort

De CA heeft zich verplicht de benodigde activiteiten tussen de aanvraag van een Digitaal Paspoort en de uitgifte ervan binnen een redelijke termijn af te handelen.

Het tijdsinterval tussen het indienen van een aanvraag en een kennisgeving door de RA-O bedraagt maximaal 5 werkdagen.

Het tijdsinterval tussen het ophalen en installeren van een Digitaal Paspoort en de melding daarvan door de RA bedraagt gemiddeld 5 seconden.

2.1.1.7 Intrekking en heruitgifte van certificaten

1. De RA zorgt op verzoek voor intrekking van Digitale Paspoorten. Onderdeel 4.4 geeft aan op welke gronden Digitale Paspoorten kunnen worden ingetrokken.
2. Bij heruitgifte wordt een nieuw certificaat uitgegeven ter vervanging van een certificaat dat niet langer geldig is. Hierbij kunnen de volgende situaties worden onderscheiden:
   a) *Heruitgifte na het verstrijken van de expiratiedatum.* Tot veertien dagen na de expiratiedatum kan de gebruiker met de bestaande PPC een nieuw Digitaal Paspoort ophalen.
   b) *Heruitgifte na intrekking van het Digitaal Paspoort.* Indien een Digitaal Paspoort na intrekking opnieuw wordt uitgegeven, kan de gebruiker deze met de bestaande PPC ophalen. Onderdeel 2.1.1.7.3 is hierbij onverminderd van toepassing.
   c) *Heruitgifte na het verloren gaan van een Digitaal Paspoort.* Indien het Digitaal Paspoort verloren gaat, bijvoorbeeld ingeval de computer waarop het certificaat staat niet meer functioneert en ook alle backups verloren zijn gegaan, kan heruitgifte van het Digitaal Paspoort plaatsvinden. Hiervoor heeft de gebruiker alleen de PPC nodig.
3. Heruitgifte van Digitale Paspoorten vindt niet plaats in geval van compromittering van de gegevens, in geval van fraude of in geval van contractopzegging.

2.1.1.8 Bescherming privésleutel CA

De CA zorgt voor de bescherming van de privésleutel en van de passwords die daar toegang toe bieden, conform het door haar afgegeven CPS. Onderdeel 6 van dit CPS is van overeenkomstige toepassing.

2.1.1.9 Beperkingen ten aanzien van gebruik privésleutel CA

De privésleutel van de CA wordt uitsluitend gebruikt voor certificaat generatie en intrek status, en niet voor enig ander doel. Het gebruik van de privésleutel van de CA is beschreven in het door haar afgegeven CPS.

2.1.2 Verplichtingen van de RA

De RA voert de identificatie van gebruikers, de validatie van intrekkingingsverzoeken en de verificatie van vernieuwingsaanvragen uit conform de bepalingen in dit CPS.

2.1.2.1 Zorgvuldigheid gegevens bij aanmelding van Digitaal Paspoort

De RA-O verplicht zich de gegevens bij aanmelding voor een Digitaal Paspoort conform de bepalingen in onderdeel 3 van dit CPS te verifiëren en te registreren. De RA-O betracht bij deze handelingen alle mogelijke zorgvuldigheid.

2.1.2.2 Zorgplicht ten aanzien van de privésleutel

De RA-P zorgt voor de bescherming van haar privésleutel en van de passwords die daar toegang toe bieden. Onderdeel 6 van dit CPS is van overeenkomstige toepassing.

2.1.2.3 Beperkingen gebruik privésleutel en Digitaal Paspoort

De RA-P zal haar privésleutel slechts gebruiken voor het ondertekenen van certificaataanvragen, overeenkomstig hetgeen bepaald is in onderdeel 1.3 van dit CPS, en voor veilige communicatie tussen de CA en de RA-P.

2.1.2.4 Kennisgeving compromitteren privésleutel

Indien sprake is van compromitteren van de privésleutel (van de RA-requestor) stelt de RA-P de CA en de RA-O onverwijld op de hoogte. De RA-O informeert vervolgens de gebruikers van het Digitaal Paspoort. Het certificaat wordt na compromittatie niet langer gebruikt.

In een dergelijk geval worden de activiteiten van de RA-P direct stilgelegd, totdat nieuwe sleutels zijn gegenereerd. Deze periode beslaat maximaal 48 uur. Gedurende deze periode is het niet mogelijk nieuwe aanvragen te verwerken, en is de gebruiker niet in de gelegenheid zijn Digitaal Paspoort in te trekken. Op verzoek kan ABZ wel overgaan tot intrekking of verlenging.

2.1.3 Verplichtingen van de gebruiker

2.1.3.1 Nauwkeurigheid aangeleverde gegevens bij aanmelding

De tekenbevoegde is verantwoordelijk voor de juistheid van de bij aanmelding aangeleverde gegevens, overeenkomstig de voorwaarden van het Digitaal Paspoort.

2.1.3.2 Bescherming van de privésleutel

Gebruiker zorgt voor een adequate bescherming van de PPC, van de privésleutel en van het password dat daar toegang toe geeft. Gebruiker is zich ervan bewust dat de bescherming met name strekt, zonder daartoe beperkt te zijn, tot het tegengaan van het compromitteren van de PPC, de privésleutel of van het password, waardoor het Digitaal Paspoort onbetrouwbaar zou worden.

2.1.3.3 Beperkingen gebruik privésleutel en Digitaal Paspoort

1. Gebruiker zal de privésleutel en het Digitaal Paspoort slechts gebruiken voor toepassingen zoals die zijn beschreven in dit CPS. Onderdeel 1.3 is van overeenkomstige toepassing.
2. Het is de gebruiker niet toegestaan de privésleutel en het Digitaal Paspoort te gebruiken voor andere dan de in dit CPS uiteengezette toepassingen.

2.1.3.4 Inkennisstelling compromitteren privésleutel

De gebruiker is verplicht ABZ onverwijld in kennis te stellen van het compromitteren van de privésleutel of van het password dat daar toegang toe geeft, conform hetgeen bepaald is in onderdeel 4.4. Bovendien is de gebruiker verplicht onmiddellijk zijn Digitaal Paspoort in te trekken indien hij daartoe redelijkerwijze de mogelijkheid heeft. Het is niet toegestaan het Digitaal Paspoort na compromittatie te gebruiken.

2.1.3.5 Vaststelling identiteit Digitaal Paspoort website

De gebruiker is verplicht de identiteit van de Digitaal Paspoort website, conform de procedure in onderdeel 4.2, te controleren. De gebruiker zal zijn PPC pas op de Digitaal Paspoort website invoeren, nadat met zekerheid is vastgesteld dat de gebruiker daadwerkelijk communiceert met de Digitaal Paspoort website van ABZ.

2.1.3.6 Bevestiging juistheid gegevens

1. Door ingebruikname van het Digitaal Paspoort, conform de procedure in onderdeel 4.3, bevestigt de gebruiker dat de door hem verstrekte en door ABZ verwerkte gegevens juist en volledig zijn.
2. Indien de gebruiker constateert dat de gegevens in het Digitaal Paspoort niet of niet meer correct zijn, is hij verplicht om dit onmiddellijk aan ABZ te melden, conform de procedure in onderdeel 4.4.

2.1.4 Verplichtingen Relying Party

2.1.4.1 Doeleinden waarvoor Digitaal Paspoort kan worden gebruikt

1. Door gebruik te maken van het Digitaal Paspoort erkent de Relying Party op de hoogte te zijn van de bepalingen zoals die zijn opgenomen in dit CPS.
2. Het Digitaal Paspoort mag door een Relying Party slechts worden gebruikt voor de toepassing waarvoor het door ABZ is uitgegeven. Onderdeel 1.3 is van overeenkomstige toepassing.

2.1.4.2 Verantwoordelijkheden ten aanzien van verificatie digitale handtekening

Indien een Relying Party het Digitaal Paspoort gebruikt voor verificatie van een digitale handtekening, is hij verplicht de geldigheid van het Digitaal Paspoort te controleren. Dit kan op basis van de Repository bij ABZ of van de CRL.

2.1.4.3 Verantwoordelijkheden ten aanzien van controleren status schorsing en intrekking

De Relying Party kan slechts rechten ontlenen aan de inhoud van een Digitaal Paspoort, nadat hij de status van de intrekking van het Digitaal Paspoort heeft geverifieerd in de Repository van ABZ of in de CRL. Onderdeel 4.4 van dit CPS is van overeenkomstige toepassing.

Indien de Relying Party om welke reden dan ook de intrekkingsstatus van het Digitaal Paspoort niet heeft geverifieerd, mag niet op de inhoud van het Digitaal Paspoort worden vertrouwd.

2.1.4.4 Acceptatie van limitering van aansprakelijkheid en garanties

De Relying Party accepteert door het gebruik van een Digitaal Paspoort alle limitering van aansprakelijkheid en garanties zoals beschreven in dit CPS, alsmede alle in de algemene leveringsvoorwaarden van ABZ geldende beperkingen van aansprakelijkheid en garanties.

2.1.5 Verplichtingen ten aanzien van de bewaarplaats (Repository)

2.1.5.1 Publiceren uitgegeven Digitale Paspoorten en informatie aangaande intrekking

Uitgegeven Digitale Paspoorten worden door de RA-P gepubliceerd in een Repository. Ingetrokken Digitale Paspoorten worden uit de Repository verwijderd en worden gepubliceerd in de CRL.

2.2 Aansprakelijkheid

2.2.1 Aansprakelijkheid van de CA

2.2.1.1 Garanties

De garanties ten aanzien van de diensten van de CA zijn neergelegd in het CPS van Digidentity (primair) en Symantec en van KPN (secundair).

2.2.1.2 Uitsluiting van aansprakelijkheid

1. ABZ is niet aansprakelijk voor schade, direct of indirect voortvloeiend uit het gebruik van een Digitaal Paspoort niet strokend met doeleinden waarvoor het Digitaal Paspoort wordt uitgegeven.

2. ABZ is niet aansprakelijk voor schade direct of indirect voortvloeiend uit de activiteiten ten aanzien van het uitgeven of intrekken van certificaten. De uitsluiting van aansprakelijkheid voor directe schade is niet van toepassing indien de directe schade te wijten is aan opzet of grove schuld van ABZ.

3. Bovenstaande uitsluiting van aansprakelijkheid is van toepassing voor alle onderdelen van ABZ die bij de TTP-dienstverlening zijn betrokken.

2.2.1.3 Limitering van aansprakelijkheid

De aansprakelijkheid van ABZ voor schade is gelimiteerd tot een bedrag van US$ 5000 voor het totaal van alle digitale handtekeningen en/of transacties die betrekking hebben op dat certificaat.
Vorderingen jegens ABZ vervallen na verloop van 12 maanden na ontstaan van de vordering, tenzij ABZ de vordering heeft erkend.

Indien een Relying Party verzuimt te voldoen aan enige in dit CPS gestelde verplichtingen ten aanzien van verificatie van de validiteit van een Digitaal Paspoort, zoals bijvoorbeeld genoemd in onderdeel 2.1.4.2, sluit ABZ alle aansprakelijkheid uit, behoudens opzet of grove schuld van ABZ.

2.2.1.4 Andere uitsluitingen

Niet van toepassing.

2.2.2 Aansprakelijkheid van de RA

2.2.2.1 Garanties

ABZ staat garant voor het uitvoeren van de RA-O diensten conform dit CPS.

2.2.2.2 Uitsluiting van aansprakelijkheid

1. ABZ is niet aansprakelijkheid voor schade, direct of indirect voortvloeiend uit enig gebruik van een Digitaal Paspoort niet strokend met het toepassingsgebied of met de doeleinden waarvoor het Digitaal Paspoort wordt uitgegeven.
2. ABZ is niet aansprakelijk voor schade direct of indirect voortvloeiend uit de activiteiten ten aanzien van:
   A. de aanmelding voor een Digitaal Paspoort;
   B. de registratie van gebruikers;
   C. de intrekking of schorsing van een Digitaal Paspoort, daarbij inbegrepen alle activiteiten die daarmee verband houden.
3. De uitsluiting van aansprakelijkheid voor directe schade is niet van toepassing indien de directe schade te wijten is aan opzet of grove schuld van ABZ of van een door ABZ voor de Digitaal Paspoort dienstverlening ingezette leverancier.
4. Bovenstaande uitsluiting van aansprakelijkheid is van toepassing voor alle onderdelen van ABZ die bij de TTP-dienstverlening zijn betrokken.

2.2.2.3 Limitering van aansprakelijkheid

De aansprakelijkheid van ABZ voor schade is gelimiteerd tot een bedrag van US$ 5000 voor het totaal van alle digitale handtekeningen en/of transacties die betrekking hebben op dat certificaat.
Vorderingen jegens ABZ vervallen na verloop van 12 maanden na ontstaan van de vordering, tenzij ABZ de vordering heeft erkend.

2.2.2.4 Andere uitsluitingen

Niet van toepassing

2.3 Financiële verantwoordelijkheden

2.3.1 Vrijwaring door Relying Parties

Relying Parties vrijwaren ABZ van aansprakelijkheid, schade, gevolgschade en kosten van derden als gevolg van het verzuimen van de verplichtingen met betrekking tot het gebruik van het Digitaal Paspoort.

2.3.2 Fiduciaire relaties

Het uitgeven van Digitale Paspoorten door ABZ impliceert niet dat ABZ handelt als agent, vertegenwoordigingsbevoegde, noch dat ABZ op enigerlei wijze verantwoordelijk is voor de inhoud van de informatie waar toegang toe wordt verkregen, tenzij dit expliciet door ABZ is bepaald.

2.3.3 Administratieve procedures

Niet van toepassing.

2.4 Overige bepalingen

2.4.1 Toepasselijk recht

Op de bepalingen in dit CPS is het Nederlands recht van toepassing.

2.4.2 Gevolgen ongeldigheid van bepalingen

Indien één van de in dit CPS opgenomen bepalingen in strijd met de wet of een wettelijke bepaling zou blijken te zijn, blijven de overige bepalingen onverminderd van kracht. Indien één van de in dit CPS opgenomen bepalingen in strijd met het Digidentity CPS zou blijken te zijn, dan prevaleert het CPS van Digidentity (secundair: KPN CPS).

2.4.3 Geschillenbeslechting

Een geschil betreffende de totstandkoming, de uitleg of de uitvoering van dit CPS is aanwezig indien een partij dit per aangetekend schrijven aan de wederpartij kenbaar maakt. Betrokken partijen hebben in eerste instantie een inspanningsverplichting om zelf een oplossing te vinden. Indien niet gezamenlijk tot overeenstemming gekomen kan worden zullen voorkomende geschillen kunnen worden voorgelegd aan de bevoegde rechter zoals genoemd in de algemene voorwaarden van ABZ.

2.5 Kosten

Kosten die samenhangen met het gebruik van het Digitaal Paspoort en de aanverwante diensten worden indien van toepassing separaat opgenomen op de website van ABZ (www.abz.nl).

2.5.1 Kosten voor uitgifte Digitaal Paspoort

Zie artikel 2.5.

2.5.2 Kosten voor toegang tot Digitaal Paspoort

Zie artikel 2.5.

2.5.3 Kosten voor raadplegen intrekkingsstatus

Zie artikel 2.5.

2.5.4 Kosten voor andere diensten

Zie artikel 2.5.

2.5.5 Procedure voor teruggave kosten

Zie artikel 2.5.

2.6 Publicatie en bewaarplaats

2.6.1 Publicatie van informatie

1. ABZ publiceert dit CPS op een voor alle eind-entiteiten toegankelijke plaats, te weten http://www.abz.nl.
2. De RA-P publiceert uitgegeven Digitale Paspoorten in een Repository, toegankelijk voor eind-entiteiten die hiertoe een overeenkomst met ABZ hebben afgesloten. Ingetrokken certificaten worden conform artikel 2.1.5.1 uit de Repository verwijderd.
3. De CA biedt te allen tijde informatie over de status van uitgegeven Digitale Paspoorten. Ingetrokken Digitale Paspoorten worden gepubliceerd in een hiervoor bestemde Certificate Revocation List (CRL).
4. De resultaten van de conform artikel 2.7 uitgevoerde audit wordt gepubliceerd op een voor alle eind-entiteiten toegankelijke plaats, te weten http://www.abz.nl.

2.6.2 Intervaltijd publicatie

1. Publicatie van het ABZ-CPS geschiedt conform de bepalingen in onderdeel 8.
2. Publicatie van de CRL vindt plaats conform onderdeel 4.4.

2.6.3 Toegangscontrole tot gepubliceerde informatie

Alle in artikel 2.6.1 genoemde informatie is, met uitzondering van de informatie genoemd in lid 2, vrij toegankelijk voor de in onderdeel 1.3 genoemde eind-entiteiten.

2.7 Audit naleving CPS

2.7.1 Interval uitvoeren Audit

Jaarlijks zal de naleving van het bepaalde in dit CPS door een onafhankelijke EDP-auditor aan een audit worden onderworpen.

2.7.2 Informatie over de EDP-Auditor

De EDP-audit wordt uitgevoerd door een register EDP-auditor (RE) die ingeschreven is in het register van de Nederlandse Orde van Register EDP-Auditors (NOREA)

2.7.3 Relatie Auditor tot partij

De EDP-auditor die de audit uitvoert is uit hoofde van zijn gedrags- en beroepsregels onafhankelijk en onpartijdig bij het uitvoeren van zijn werkzaamheden.

2.7.4 Object van audit

Object van de periodieke audit zijn de naleving van het CPS en bijbehorende procedures en technieken, in opzet, bestaan en werking. Het hierbij gehanteerde normensstelsel wordt per jaar bepaald, op basis van actuele standaarden. De dienstverlening van door ABZ ingeschakelde derden is eveneens onderdeel van de audit.

2.7.5 Consequenties ingeval van onvolkomenheden en gebreken

Indien bij de audit onvolkomenheden en/of gebreken worden geconstateerd, zullen deze zo spoedig mogelijk door ABZ hersteld worden. Hierna wordt voor de desbetreffende onderdelen opnieuw een audit uitgevoerd.

2.7.6 Kennisgeving van resultaten audit

De resultaten van de conform artikel 2.7 uitgevoerde audit wordt gepubliceerd op een voor alle eind-entiteiten toegankelijke plaats, te weten http://www.abz.nl.

2.8 Geheimhouding

2.8.1 Confidentiële informatie

Onder confidentiële informatie wordt verstaan:

1. Persoonsgegevens;
2. Bedrijfsgegevens;
3. Privésleutel gebruikers;
4. Audit logs.

Ingevolge de Wet Bescherming Persoonsgegevens mogen persoonsgegevens slechts gebruikt worden voor het doel waarvoor deze zijn verzameld.

2.8.2 Geen confidentiële informatie

Als niet-confidentiële informatie is aan te merken alle informatie die niet in onderdeel 2.8.1 genoemd is, tenzij dit volgens de Wet Bescherming Persoonsgegevens niet zo is.

2.8.3 Verstrekking van informatie over intrekking/schorsing

Digitale Paspoorten kunnen niet worden geschorst. Informatie over intrekking van een Digitaal Paspoort wordt niet aangemerkt als confidentiële informatie. Onderdeel 2.8.2 is van overeenkomstige toepassing.

2.8.4 Verstrekking opsporingsinstanties en overheidsinstanties

ABZ zal informatie verstrekken aan opsporingsinstanties en overheidsinstanties indien deze informatie wordt gevorderd op grond van een rechterlijk bevel of wettelijk voorschrift.

2.8.5 Inzagerecht

Eind-entiteiten hebben recht op inzage in de over hen geregistreerde gegevens.

2.8.6 Verstrekking op verzoek eigenaar

ABZ zal over eind-entiteiten geregistreerde informatie alleen dan aan derden verstrekken als betreffende eind-entiteit daar nadrukkelijk om heeft verzocht.

2.8.7 Andere gronden voor verstrekking van confidentiële informatie

Niet van toepassing.

2.9 Intellectuele eigendomsrechten

1. Het auteursrecht, evenals alle eventuele andere rechten van industriële en intellectueel eigendom op het Digitaal Paspoort en het CPS, de daarbij behorende technieken en documentatie en andere geschriften alsmede alle rechten tot bescherming van gegevens komen toe aan ABZ of, in het voorkomende geval, aan de leverancier ervan.
2. Eind-entiteiten zullen aanduidingen die betrekking hebben op het auteursrecht of andere rechten van industriële of intellectueel eigendom, niet verwijderen.
3. Eind-entiteiten verplichten zich ABZ onverwijld op de hoogte te stellen van iedere inbreuk op rechten van ABZ of derden met betrekking tot het CPS, de daarbij behorende technieken en documentatie en andere geschriften.

3. IDENTIFICATIE & AUTHENTICATIE

3.1 Initiële registratie

In deze paragraaf wordt de identificatie en authenticatie voor de initiële registratieprocedure aan de orde gesteld.

3.1.1 Naamgeving

Het 'subject' binnen het Digitaal Paspoort is samengesteld uit een aantal velden. Dit zijn de velden E (e-mail), CN (Common Name, Volledige naam), OU=O- (Organisatie), OU (Organisatorische eenheid) en C (Country, Land).

Attribuut	Vereisten*
E	*E-mailadres van gebruiker* Het e-mailadres dient te zijn opgebouwd conform de geldende standaarden (RFC 5322) en het dient een persoonlijk e-mail adres te zijn.
CN	*Volledige naam van de gebruiker (indien de voornaam niet bekend is worden in plaats hiervan de initialen gebruikt)* Gebruiker is altijd een natuurlijk persoon. Beperkingen in de naamgeving binnen het subject zijn niet van toepassing.
OU=O-	*Naam van de organisatie waar gebruiker werkzaam is* De bedrijfsnaam moet voorkomen in het uittreksel handelsregister of op het rekeningafschrift, hetzij als juridische naam, hetzij als de handelsnaam. De bedrijfsgegevens op het aanmeldingsformulier moeten hiermee overeenkomen.
OU	*Primair:* www.digidentity.eu *Secundair:* *Organisatorische eenheid* www.Symantec.com/repository/CPS Incorp by Ref.,LIAB.LTD(c)96
OU	*Organisatorische eenheid* TTP Services ABZ Nederland
O	*Uitgevende partij* Solera Nederland BV
C	*Land van uitgifte* NL

* Invulling van genoemde vereisten gebeurt overeenkomstig de richtlijnen voor naamgeving ingevolge dit CPS (zie met name onderdeel 3.1.5 en 3.1.6).

3.1.2 Zinvolle naamgeving

De Relying Party kan uit de verzameling attributen zoals opgenomen in het Digitaal Paspoort de identiteit van de eind-entiteit, zoals deze is vastgelegd conform artikel 3.1.9, vaststellen.

3.1.3 Regels voor het interpreteren van de naamgeving

Zie onderdeel 3.1.2.

3.1.4 Unieke naamgeving

ABZ draagt zorg voor een unieke identificatie van de gebruiker (zogenaamde distinguished name = subject) in het Digitaal Paspoort. Hierdoor kunnen de afzonderlijke gebruikers op unieke wijze worden geïdentificeerd. Dit wordt op technische wijze gerealiseerd door de combinatie van de verschillende attributen (genoemd in 3.1.1).

3.1.5 Geschillenbeslechting ten aanzien van naamgeving

ABZ behoudt zich het recht voor om bij het inrichten de aangevraagde naam aan te passen indien dit technisch noodzakelijk is. Indien partijen het niet eens zijn met een aanpassing kan hiertegen bezwaar worden gemaakt bij de TTP-manager.

3.1.6 Regels ten aanzien van merkenrechten

ABZ behoudt zich het recht voor wijzigingen aan te brengen aan de attributen zoals de gebruiker deze heeft aangegeven in het aanmeldingsformulier, wanneer deze in strijd kunnen zijn met enig merkenrecht.

3.1.7 Aantonen bezit privésleutel

Ten tijde van de aanvraag van een Digitaal Paspoort dient het bezit van een privésleutel aangetoond te worden. Dit is technisch geïmplementeerd tijdens het proces waarbij de sleutels worden omgezet in een aanvraag, conform de PKCS#10-standaard.

3.1.8 Authenticatie van de organisatie waartoe aanvrager behoort

1. De organisatiegegevens moeten zijn ingevuld op het aanmeldingsformulier. Indien de organisatie is ingeschreven in het handelsregister van de KvK, dan moeten de bedrijfsgegevens die hierin vermeld staan gelijk zijn aan de gegevens op de aanvraag. Indien de organisatie hierin niet is ingeschreven, dienen de bedrijfsgegevens overeen te komen met de gegevens op een kopie van een rekeningafschrift van de organisatie, niet ouder dan één maand. Indien de organisatiegegevens niet correct zijn ingevuld, wordt de aanvraag afgewezen.
2. Het doorgeven van wijzigingen op bedrijfsgegevens dient schriftelijk plaats te vinden. Betreft het een wijziging van de bedrijfsnaam, dan worden de gewijzigde gegevens voordat ze worden doorgevoerd door ABZ geverifieerd door het opnieuw opvragen van een uittreksel uit het handelsregister van de KvK. Alvorens gegevens worden doorgevoerd, wordt het oude certificaat door ABZ ingetrokken.

3.1.9 Authenticatie van individuele eindgebruikers

1. De aanvraag van een Digitaal Paspoort wordt ondertekend door een tekenbevoegde persoon binnen de organisatie waartoe de beoogd houder van het certificaat behoort. Bij online aanvragen wordt de aanvraag ingediend door een door de tekenbevoegde gemachtigde Digitaal Paspoort beheerder.
2. De aanvrager van het Digitaal Paspoort zal de vereiste identificatiemiddelen van de tekenbevoegde overleggen. De vereiste identificatiemiddelen worden vermeld op het aanmeldingsformulier en in sub 2 van onderdeel 3.1.9.1.

3.1.9.1 Vereiste identificatiemiddelen

1. ABZ dient te beschikken over een uittreksel uit het handelsregister van de KvK of, indien een organisatie daar niet is ingeschreven, over een kopie van een recent rekeningafschrift van de organisatie. Het uittreksel uit het handelsregister van de KvK is een origineel uittreksel of een door ABZ opgevraagd uittreksel via KvK Online.
   Indien bij een aanvraag een origineel uittreksel wordt meegezonden, accepteert ABZ dit alleen als het niet ouder is dan zes maanden.
   Indien een organisatie niet in het handelsregister van de KvK is ingeschreven en bij een aanvraag een kopie van een rekeningafschrift wordt meegezonden, mag dit niet ouder zijn dan één maand.
2. Voor de tekenbevoegde accepteert ABZ als geldig legitimatiebewijs:
   A Een kopie van een in Nederland geldig rijbewijs of
   B een kopie van een geldig paspoort
3. ABZ biedt een machtigingsprocedure voor het delegeren van de tekenbevoegdheid. De door de tekenbevoegde gemachtigde persoon dan wel de Digitaal Paspoort beheerder kan hierdoor aanvragen van Digitale Paspoorten initiëren.

3.1.9.2 Authenticatie van tekenbevoegde

1. Na de ontvangst van het aanmeldingsformulier door ABZ gaat dit formulier met alle bescheiden naar de ABZ RA-O. Alleen deze is bevoegd om aanmeldingen in behandeling te nemen. De ABZ RA-O controleert of het formulier is voorzien van een handtekening en of de naam van de ondertekenaar en de organisatie overeenkomt met de namen op het uittreksel uit het handelsregister van de KvK, respectievelijk met de persoonsnaam op de kopie van het rekeningafschrift. Indien deze naam niet overeenkomt, en het niet om een aanvraag door een gemachtigd persoon betreft, wordt de aanvraag afgewezen.
2. De handtekening op het legitimatiebewijs moet gelijkenis vertonen met de handtekening op het aanmeldingsformulier. Indien de handtekening op het legitimatiebewijs (sterk) afwijkt van die op het aanvraagformulier, wordt de aanvraag afgewezen. Tevens moet de naam die staat vermeld op het legitimatiebewijs overeenkomen met de naam van de ondertekenaar. Indien geen kopie van een geldig legitimatiebewijs is meegezonden wordt de aanvraag afgewezen. Indien het legitimatiebewijs van een ander dan de tekenbevoegde is, wordt de aanvraag afgewezen.
3.

Bij een online aanvraag wordt de Digitaal Paspoort Beheerder geauthenticeerd op basis van zijn Digitale Paspoort en op basis van zijn rol als Digitaal Paspoort Beheerder

3.1.9.3 Fysieke representatie

ABZ kent in de procedure geen fysieke representatie.

3.1.9.4 Authenticatie organisatie

Zie onderdeel 3.1.8.

3.2 Routinematige verlenging Digitaal Paspoort

Als routinematige verlenging van het Digitaal Paspoort wordt beschouwd:

- Verlenging Digitaal Paspoort in verband met expiratie. Hierbij wordt een nieuw certificaat uitgegeven op basis van een nieuw gegenereerd sleutelpaar.

De identificatie en authenticatie van gebruikers in geval van een routinematige verlenging van het Digitaal Paspoort gebeurt als volgt:

1. Het Digitaal Paspoort heeft een geldigheidsduur van één jaar. Veertien dagen voor de datum waarop het Digitaal Paspoort expireert wordt de gebruiker middels een e-mailbericht van de expiratie van het Digitaal Paspoort op de hoogte gebracht. De gebruiker is zelf verantwoordelijk voor het verlengen van het Digitaal Paspoort.
2. In het e-mailbericht wordt toegelicht hoe de gebruiker zijn Digitaal Paspoort dient te verlengen en wat de gevolgen zijn als hij dit niet doet. Binnen deze veertien dagen kan de gebruiker zonder een melding te krijgen dat hij reeds een Digitaal Paspoort heeft, het certificaat verlengen. Indien hij dit niet doet, zal hij na de expiratiedatum geen toegang meer krijgen tot omgevingen die beveiligd zijn met het Digitaal Paspoort. De gebruiker wordt geauthenticeerd door middel van een e-mailadres en een PPC. Veertien dagen na expiratie is verlenging niet meer mogelijk, en moet een nieuw Digitaal Paspoort worden aangevraagd.
   Tijdens de geldigheidsduur van het Digitaal Paspoort kan de gebruiker met een geldig Digitaal Paspoort zijn PPC online opvragen. Na het verstrijken van de geldigheidsduur of bij ongeldigheid van het Digitaal Paspoort kan de gebruiker een schriftelijk verzoek bij ABZ indienen voor het opnieuw verstrekken van een Digitaal Paspoort, conform de reguliere aanvraagprocedure.

3.3 Niet-routinematige heruitgifte Digitaal Paspoort

Als niet-routinematige heruitgifte van het Digitaal Paspoort wordt beschouwd:

- Uitgifte van een nieuw Digitaal Paspoort na intrekking, na het verstrijken van de expiratieperiode of na het verloren gaan van het Digitaal Paspoort. Hierbij wordt een nieuw certificaat uitgegeven op basis van een nieuw gegenereerd sleutelpaar.

De identificatie- en authenticatieprocedure van de gebruiker ingeval van niet-routinematige heruitgifte van een Digitaal Paspoort is gelijk aan die van de aanvraag

van een Digitaal Paspoort. Het is alleen mogelijk een verzoek tot heruitgifte schriftelijk in te dienen. Het verzoek kan alleen ondertekend worden door een tekenbevoegde. Een Digitaal Paspoort Beheerder kan een verzoek tot heruitgifte online indienen. Zie voor de gronden die tot intrekking aanleiding geven onderdeel 4.4.

3.4 Verzoek tot intrekking

1. ABZ kent een aantal soorten verzoeken tot intrekking van een Digitaal Paspoort. Onderdeel 4.4 is van overeenkomstige toepassing. Afhankelijk van wie het verzoek tot intrekking afkomstig is, worden verschillende identificatiemiddelen geëist.
2. Gebruikers kunnen met behulp van hun PPC het eigen Digitaal Paspoort intrekken, of ABZ verzoeken hun Digitaal Paspoort in te trekken.
   Tijdens de geldigheidsduur van het Digitaal Paspoort kan de gebruiker met een geldig Digitaal Paspoort zijn PPC online opvragen.
3. Indien door een ander dan de gebruiker een verzoek tot intrekking wordt ingediend, dient de verzoeker zich te identificeren door middel van een kopie van een geldig legitimatiebewijs. Indien dit niet mogelijk is zal ABZ:
   A Niet overgaan tot het intrekken van het Digitaal Paspoort.
   B Het verzoek loggen.
   Onderdeel 4.4 is van overeenkomstige toepassing.
4. ABZ kan een certificaat intrekken ter oplossing van eventueel opgetreden technische storingen.
5. De opzegging van een contract met betrekking tot een Digitaal Paspoort wordt door ABZ tevens als een verzoek tot intrekking van het certificaat beschouwd.

4. OPERATIONELE VEREISTEN

4.1 Aanmelding voor een Digitaal Paspoort

Aanvraag van een Digitaal Paspoort vindt plaats door het daartoe bestemde formulier geheel in te vullen en met de vereiste bijlagen naar ABZ te sturen. Dit formulier is te vinden op de website van ABZ (www.abz.nl). Een Digitaal Paspoort Beheerder kan de aanvraag online indienen. Na goedkeuring van de aanvraag verwerkt ABZ deze in de administratie en worden de gegevens in de Repository opgeslagen.

4.2 Uitgifte van een Digitaal Paspoort

ABZ geeft het Digitaal Paspoort uit. Deze procedure bestaat uit de volgende onderdelen.

1. De gebruiker krijgt van ABZ een Persoonlijke Paspoort Code (PPC) toegestuurd. De gebruiker ontvangt de ene helft van de PPC per post/SMS of van de Digitaal Paspoort Beheerder en de andere helft per e-mail. Met de volledige code kan het Digitaal Paspoort worden opgehaald. Dit gebeurt ofwel met een browser, ofwel met een hiervoor geschikte applicatie.
2. Alvorens de gebruiker zijn PPC op de Digitaal Paspoort-website invoert, controleert de gebruiker de identiteit van de website. Dit doet de gebruiker door het servercertificaat dat op de Digitaal Paspoort-website aanwezig is, te controleren.
3. Het Digitaal Paspoort wordt op de Digitaal Paspoort website aan de gebruiker ter beschikking gesteld, in een pagina die getoond wordt nadat de gebruiker een juist emailadres en PPC heeft ingegeven en daarbij sleutelpaar heeft gegenereerd dat ter ondertekening aan ABZ wordt aangeboden.
4. ABZ genereert (ondertekent) het Digitaal Paspoort behorend bij de publieke sleutel van de gebruiker.

4.3 Acceptatie van een Digitaal Paspoort

1. Voorafgaand aan het ophalen en installeren van het Digitaal Paspoort verschijnt voor de gebruiker een gebruikersovereenkomst. Door vervolgens het proces van het ophalen en installeren van een Digitaal Paspoort op de Digitaal Paspoort site te continueren, accepteert de gebruiker de gebruikersovereenkomst behorend bij het gebruik van het Digitaal Paspoort.
2. Indien een gebruiker deze gebruikersovereenkomst niet accepteert, wordt de procedure afgebroken.

4.4 Intrekking van Digitale Paspoorten

1. Intrekking van een Digitaal Paspoort kan door een gebruiker worden gedaan, en door ABZ op verzoek van de gebruiker of op verzoek van een derde. Ingetrokken certificaten worden gepubliceerd middels een CRL en de betreffende entry wordt uit de Repository verwijderd.
2. De CRL is online beschikbaar op de CA-site (zie ook artikel 4.4.9 e.v.). Na intrekking van een Digitaal Paspoort wordt dit bij de betreffende entry uit de Repository verwijderd.
3. Bij intrekking door ABZ wordt de gebruiker (de betrokken houder van het Digitaal Paspoort) onverwijld in kennis gesteld, voor zover dit redelijkerwijs mogelijk is.

4.4.1 Redenen voor intrekking van een Digitaal Paspoort

1. Digitale Paspoorten dienen te worden ingetrokken in het geval dat de corresponderende privésleutel, of de pincode/passphrase die daar toegang toe geeft, is gecompromitteerd of in geval de informatie die in het Digitaal Paspoort is opgenomen onjuist is (geworden).
2. De volgende omstandigheden zijn altijd aanleiding voor intrekking van het Digitaal Paspoort, zonder daartoe beperkt te zijn:
   A Naamsverandering gebruiker of organisatie.
   B Beëindiging van de arbeidsovereenkomst van de houder van het Digitaal Paspoort.
   C Kennisgeving door derden van misbruik van het Digitaal Paspoort.
   D Kennisgeving van gebruiker dat diens gegevens gecompromitteerd zijn.

4.4.2 Wie kan een verzoek tot intrekking indienen

De volgende personen zijn gerechtigd om een verzoek tot intrekking te doen:

1. Gebruiker
2. Ander dan gebruiker

ABZ kan zelf ook besluiten om een Digitaal Paspoort in te trekken van een gebruiker indien daar gegronde redenen voor bestaan. Dit kan één van de redenen zijn die in onderdeel 4.4.1 is genoemd. Indien dit zich voordoet zal ABZ de gebruiker hiervan op de hoogte stellen onder vermelding van de reden, voor zover dit redelijkerwijs mogelijk is.

4.4.3 Procedure voor verzoek tot intrekking

Door gebruiker

Indien een gebruiker zelf een verzoek tot intrekken van zijn Digitaal Paspoort doet wordt het Digitaal Paspoort direct ingetrokken. Hierbij geldt de volgende procedure:

- Een verzoek tot intrekking van een eigen Digitaal Paspoort kan alleen gedaan worden door middel van:
  1. E-mail, waarbij geldt dat deze verzonden moet zijn vanaf een bij ABZ bekend adres
  2. Brief, met daarop een handtekening die voldoende gelijkenis vertoont met de handtekening die bij ABZ is geregistreerd
  3. Telefonisch, waarbij de verzoeker ter controle door ABZ wordt teruggebeld op het bij ABZ geregistreerde nummer.
- In alle gevallen moet de gebruiker duidelijk vermelden dat het gaat om het intrekken van zijn eigen Digitaal Paspoort, waarbij hij de bedrijfsnaam, gebruikersnaam en e-mailadres (dat bij ABZ bekend moet zijn) moet vermelden.
- De gebruiker is niet verplicht tot het opgeven van een reden.

Door een ander dan de gebruiker

Indien een ander dan de gebruiker een verzoek tot intrekken van zijn Digitaal Paspoort doet, worden eerst de gegevens van deze verzoeker gecontroleerd, alvorens tot intrekking wordt overgegaan. Hierbij geldt de volgende procedure:

- Een verzoek voor het intrekken van een Digitaal Paspoort van een ander kan alleen ingediend worden door middel van brief ofwel online door de Digitaal

Paspoort Beheerder. Het schriftelijke verzoek moet altijd vergezeld gaan van een kopie van een geldig identiteitsbewijs.

- In alle gevallen moet deze persoon ABZ laten weten om welke gebruiker het gaat. Hierbij moet worden vermeld:
  1. de gebruikersnaam
  2. de bedrijfsnaam van de gebruiker wiens Digitaal Paspoort moet worden ingetrokken
  3. indien bekend het e-mailadres van deze gebruiker.
- Zelf is de indiener van het verzoek verplicht om de eigen gegevens (bedrijfsnaam, eigen naam, adres) aan ABZ op te geven.
- De reden voor het verzoek tot intrekking dient duidelijk vermeld worden. Een verzoek tot intrekking van een Digitaal Paspoort zonder een omschrijving van de reden wordt door ABZ niet geaccepteerd.
- Het onderzoek naar de gegevens van de verzoeker wordt door ABZ binnen maximaal tien werkdagen afgerond.
- Indien alle gegevens correct zijn bevonden en de reden tot intrekking is valide, gaat ABZ over tot intrekking van het Digitaal Paspoort, en wordt de betrokken houder van het Digitaal Paspoort op de hoogte gesteld. Het onderzoek en de eventuele intrekking worden door ABZ gelogd.

4.4.4 Geldigheidsperiode van een verzoek tot intrekking

ABZ dient een verzoek tot intrekking binnen 24 uur na het indienen te behandelen.

4.4.5 Redenen voor schorsing van Digitaal Paspoort

ABZ kent geen schorsing van een Digitaal Paspoort.

4.4.6 Indienen verzoek tot schorsing

Niet van toepassing (zie onderdeel 4.4.5).

4.4.7 Procedure verzoek tot schorsing

Niet van toepassing (zie onderdeel 4.4.5).

4.4.8 Schorsingstermijn

Niet van toepassing (zie onderdeel 4.4.5).

4.4.9 Intervalperiode uitgifte CRL

De CRL is een bestand waarin wordt bijgehouden welke Digitale Paspoorten zijn ingetrokken door de CA. De CRL wordt beheerd door Digidentity (primair) of KPN (secundair).

1. Dit bestand is online beschikbaar bij de CA, bijvoorbeeld voor informatieleveranciers die gebruik maken van het Digitaal Paspoort voor autorisatie.
2. De intervalperiode voor het bijwerken van de CRL is maximaal vier uur.
3.

De CRL wordt door Digidentity (primair) of Symantec (secundair) niet gearchiveerd

4.4.10 Vereisten controleren CRL

De CA (Digidentity (primair) of KPN (secundair)) stelt de CRL online beschikbaar.

1. ABZ kent geen vereisten voor controle van de CRL.
2. Informatieleveranciers die gebruik maken van de Repository van ABZ, behoeven de CRL niet te controleren omdat, indien zij hun server juist hebben geconfigureerd, gebruikers automatisch de toegang wordt geblokkeerd op het moment dat een Digitaal Paspoort wordt ingetrokken. ABZ accepteert geen enkele verantwoordelijkheid indien er schade is veroorzaakt door een gebruiker met een Digitaal Paspoort dat door ABZ is ingetrokken.
3. De informatieleverancier kan geen rechten ontlenen aan de CRL zoals deze gepubliceerd wordt door de CA. ABZ accepteert geen enkele verantwoordelijkheid indien er schade is veroorzaakt door een gebruiker met een Digitaal Paspoort dat door ABZ is ingetrokken.

4.4.11 Beschikbaarheid online controle van intrekkingsstatus

Primaire CA

Voor de controle van de intrekkingsstatus via de CRL kent de CA (Digidentity) het volgende mechanisme:
De intrekkingsstatus is online beschikbaar bij de CA op basis van een machinematige controle.
url: http://pki.digidentity.eu/L3/DP/latestCRL.crl

Secundaire CA

Voor de controle van de intrekkingsstatus via de CRL kent de CA (KPN) twee mechanismes:

1. De intrekkingsstatus is online beschikbaar bij de CA op basis van een handmatige controle.
   url: http://crl.managedpki.com/SoleraNederlandBVFinancialServices/LatestCRL.crl

2. Machinematige controle op basis van machine interpretatie van de CRL. De CRL is beschikbaar in verschillende formaten:.x509, .crl en .bin
   http://crl.managedpki.com/SoleraNederlandBVFinancialServices/LatestCRL (PKCS7 formaat)
   http://crl.managedpki.com/SoleraNederlandBVFinancialServices/LatestCRL.crl (DER formaat)
   http://crl.managedpki.com/SoleraNederlandBVFinancialServices/LatestCRL.509.ldif (ldif formaat)

4.4.12 Vereisten online controle van intrekkingsstatus

Deze vereisten zijn beschreven in onderdeel 4.4.10.

4.4.13 Andere vormen van publiceren intrekkingsstatus

De status van het certificaat is ook op te vragen uit de ABZ Repository. Dit verdient zelfs de voorkeur, want de gegevens in de Repository worden vrijwel direct bijgewerkt in geval van intrekking. Het risico dat samenhangt met de intervalperiode voor het publiceren van de CRL wordt hiermee vermeden.

Anders dan een lijst van ingetrokken certificaten (black list = CRL) is de Repository een white list, dat wil zeggen dat alle geldige certificaten hierin gepubliceerd worden. Indien een certificaat niet aanwezig is in de Repository dient dit te worden beschouwd als ingetrokken of als niet bestaand.

4.4.14 Vereisten aan andere publicatievormen van intrekkingsstatus

1. De ABZ Repository is beschikbaar voor een ieder die de geldigheid van een Digitaal Paspoort wil controleren en hiertoe een contract met ABZ heeft afgesloten. Indien een certificaat niet aanwezig is in de Repository dient dit te worden beschouwd als ingetrokken of als niet bestaand.
2. ABZ is niet aansprakelijk als de intrekkingsstatus door technische of andere calamiteiten tijdelijk niet beschikbaar is. ABZ doet in een dergelijke situatie al het mogelijke om de beschikbaarheid van de intrekkingsstatus zo snel als redelijkerwijze mogelijk is te herstellen.

4.4.15 Speciale vereisten publicatie intrekkingsstatus als gevolg van compromitteren privésleutel

In de CRL wordt een onderscheid gemaakt naar de reden van intrekking. De relying party kan daaruit de reden voor intrekking van een Digitaal Paspoort vernemen. Bij het intrekken van een certificaat wordt een keuzelijst gepresenteerd, waaruit de reden voor intrekking kan worden geselecteerd. Compromittering van de privésleutel maakt onderdeel uit van deze lijst.

4.5 Security Audit procedures

4.5.1 Gebeurtenissen die worden gelogd

De volgende gebeurtenissen worden door de RA-P gelogd:

Bij aanvraag:
1. Aanvragen Digitaal Paspoort, dat wil zeggen het door de gebruiker invullen van zijn gegevens op de Digitaal Paspoort site.
2. Procedure na indienen aanvraag
3. Publiceren in de Repository
4. Shutdown/restart van de RA-P componenten.

Bij intrekking:
1. Wie en wanneer
2. Publiceren in de Repository
3. Shutdown/restart van de RA-P componenten.

Bij verlenging:
1. Wie en wanneer
2. Publiceren in de Repository
3. Shutdown/restart van de RA-P componenten.

Overig:
1. Wijzigingen aan infrastructuur
2. Wijzigingen aan software.

4.5.2 Interval uitvoeren loggings

De logging zoals die in 4.5.1 beschreven is, vindt direct plaats met het uitvoeren van de betreffende handeling. Ingeval van calamiteiten worden deze loggings geanalyseerd.

4.5.3 Bewaartermijn Logs

Loggings worden bewaard gedurende een periode van twee jaar. Deze periode is gekozen in verband met de noodzaak te kunnen achterhalen wat de oorspronkelijke gebeurtenissen zijn geweest indien er sprake is van verlenging van het certificaat.

4.5.4 Beveiliging Audit Logs

De logging wordt geschreven door de user waaronder de servers draaien. Alleen een user met de juiste rechten heeft toegang tot de logging.

4.5.5 Audit log backup procedures

Backup van de loggings vindt tenminste drie maal per week plaats en valt samen met de backups van de systemen waarop de software draait.

4.5.6 Opslagfaciliteit van de loggings

De logging wordt opgeslagen op een hoog beschikbaar systeem. Oudere loggingen worden off line opgeslagen.

4.5.7 Kennisgeving van logging gebeurtenis

Wanneer uit de analyse van de logging, conform onderdeel 4.5.2, verdachte of kwaadwillende activiteiten af te leiden zijn, zal onmiddellijk contact met de organisatie waar de veroorzaker werkzaam is worden opgenomen en zal, indien van toepassing, haar of zijn certificaat worden ingetrokken. ABZ behoudt zich het recht voor actie te ondernemen uit hoofde van hetgeen bepaald is in CPS onderdeel 2.

4.6 Archivering van documenten

4.6.1 Gebeurtenissen die worden gearchiveerd

De ABZ RA-O archiveert alle binnenkomende en uitgaande post en alle binnenkomende e-mail zoals:

1. Aanmeldingsformulieren t.b.v. diensten/producten.
2. Bevestiging aanmeldingen t.b.v. diensten/producten.
3. Wijzigingen t.b.v. diensten/producten.
4. Bevestiging wijziging t.b.v. diensten/producten.
5. Opzeggingen t.b.v. diensten/producten.
6. Bevestiging opzegging t.b.v. diensten/producten.
7. Uittreksels handelsregister Kamer van Koophandel.
8. Kopieën rekeningafschriften
9. Kopieën legitimatiebewijzen.

4.6.2 Bewaartermijn archief

Alle bij onderdeel 4.6.1 genoemde documenten worden elektronisch in het Document Informatie Systeem (DIS) gearchiveerd. Alle papieren documenten worden in dozen, op volgorde van scandatum bewaard bij een gespecialiseerde archiefbeheerder. Aan zowel het elektronische als het papieren archief is een bewaartermijn verbonden van vijf jaar.

4.6.3 Beveiliging archief

1. Toegangsbeveiliging elektronisch archief:
   Het DIS draait op een computer waarbij op user-niveau rechten worden verleend. Aan alle ABZ-medewerkers zijn leesrechten verleend. Aan de RA-medewerkers van ABZ zijn tevens schrijfrechten verleend.
2. Toegangsbeveiliging/fysieke beveiliging papieren archief:
   De toegang tot deze ruimte is fysiek beveiligd.
3. Fysieke beveiliging elektronisch archief:
   De machines waarop de documenten zijn opgeslagen staan in een ruimte die fysiek is beveiligd.

4.6.4 Archief backup procedures

Van alle elektronisch gearchiveerde documenten wordt iedere nacht door ABZ een totale backup op tape gezet. Iedere volgende ochtend wordt de laatste backup, van de afgelopen nacht, opgehaald door KPN Business Continuity (GBC) te Lelystad. De kernactiviteit van GBC is het aanbieden van continuïteitsdiensten gericht op de continuïteit van de bedrijfsprocessen van computerafhankelijke organisaties en op de beveiliging van bedrijfsgegevens. Elke tape is bij GBC per direct door ABZ opvraagbaar.

4.6.5 Vereisten voor het tijdstempelen van documenten

1. Alle binnengekomen post wordt door het secretariaat voorzien van een datumstempel.
2. Alle uitgaande post, binnenkomende en uitgaande e-mail worden voorzien van een computer-systeemdatum.

4.6.6 Opslagfaciliteit van archief

De complete backup van het archief wordt opgeslagen bij GBC.

4.6.7 Verkrijgen en verifiëren van gearchiveerde informatie

1. Elk elektronisch document is per klantkaart vanuit het dossier opvraagbaar. Aan elk document wordt een documentnaam en de naam van de behandelaar toegekend.
2. Elk elektronisch document is te verifiëren met de originele documenten.

4.7 Verstrekken publieke sleutels

Voor het verstrekken van de publieke sleutel die deel moet uitmaken van het Digitaal Paspoort gelden de procedures zoals die in onderdeel 3.1 beschreven worden, waarbij opgemerkt moet worden dat de gebruiker zelf verantwoordelijk is voor het

genereren van het sleutelpaar. Indien het gaat om het verstrekken van een nieuwe publieke sleutel, dan zijn ook CPS onderdeel 3.2 en 3.3 van toepassing.

4.8 Compromitteren van de privésleutel en calamiteitenbeheersing

4.8.1 Onbetrouwbaarheid rekencapaciteit, software en data

Indien de rekencapaciteit van de apparatuur waarop de software voor het uitgeven van Digitale Paspoorten draait onvoldoende dreigt te worden, zullen op tijd maatregelen genomen worden om dit te voorkomen. Hierbij moet gedacht worden aan uitbreiding van de bestaande, of aanschaf van nieuwe hardware.

Als de software niet meer betrouwbaar is, zullen, afhankelijk van de oorzaak, de nodige maatregelen genomen worden. Hierbij kan gedacht worden aan:

1. Terugplaatsen backup.
2. Aanbrengen van patches.
3. Aanschaffen en installeren nieuwe software.

Is een upgrade van de sleutellengte noodzakelijk, dan moet mogelijk ook door de gebruiker nieuwe software geïnstalleerd worden.

4.8.2 Intrekking publieke sleutel CA

Ingeval de privésleutel van de CA gecompromitteerd is, wordt het bijbehorende certificaat van de CA ingetrokken. Vervolgens informeert ABZ al haar eind-entiteiten over deze omstandigheden en over de gevolgen op korte en lange termijn.

4.8.3 Compromitteren privésleutel CA

Zie 4.8.2.

4.8.4 Uitwijkmogelijkheden

ABZ heeft jegens haar klanten de verplichting om alles in het werk te stellen om de dienstverlening te garanderen. Dit betekent dat van alle systemen die operationeel zijn ten behoeve van het ondersteunen van klanten, systeem-backups bestaan en er dagelijks backups worden gemaakt van databestanden, zodat in geval van een calamiteit binnen een acceptabele termijn de dienstverlening weer operationeel gemaakt kan worden.

ABZ heeft een Business Continuity Plan (BCP) opgesteld, waarin voor alle onderdelen van de dienstverlening, dus ook voor de Digitaal Paspoort dienstverlening, de maatregelen zijn opgenomen die zijn of worden genomen in geval van een calamiteit. Hiertoe behoren ook de eventuele uitwijkmogelijkheden.

Hetzelfde geldt voor de CA dienstverleners; alle data wordt redundant offsite opgeslagen op een hot standby omgeving, conform ETSI normen.

Indien de primaire CA (Digidentity) door een calamiteit niet in staat is tot levering, wordt de secundaire CA (KPN) geactiveerd, waardoor de certificaat dienstverlening met minimale downtijd kan worden voortgezet.

4.9 Beëindiging van de ABZ Digitaal Paspoort-dienstverlening

ABZ zorgt naar beste vermogen voor de continuïteit van de dienstverlening zolang er geldige Digitale Paspoorten in omloop zijn.
Als er om wat voor reden dan ook (intern of extern) besloten wordt dat ABZ de werkzaamheden rondom het Digitaal Paspoort niet voortzet, zal door haar het CA Termination Plan worden uitgevoerd. Dit Plan houdt in dat ABZ er naar zal streven om:

1. De uitgifte van nieuwe Digitaal Paspoorten direct te staken.
2. Ten minste 3 maanden voor beëindiging van de werkzaamheden alle bedrijven die een Digitaal Paspoort bezitten op de hoogte te stellen van de beëindiging van de werkzaamheden.
3. Ten minste 3 maanden voor beëindiging van de werkzaamheden alle bedrijven die een Digitaal Paspoort bezitten te informeren over de partij die de werkzaamheden zal overnemen, indien een dergelijke partij bekend is.
4. Ten minste 3 maanden voor beëindiging van de werkzaamheden alle informatieleveranciers op de hoogte te stellen van de beëindiging van de werkzaamheden.
5. Samen met de informatieleveranciers binnen deze 3 maanden mee te werken aan de overgang naar de partij die de werkzaamheden van ABZ gaat overnemen, indien een dergelijke partij bekend is.
6. Alle Digitale Paspoorten in te trekken die niet zijn ingetrokken of verlopen aan het einde van deze periode van 3 maanden.
7. Naar redelijkheid en billijkheid het ongemak van onderbreking van de service voor alle bedrijven die een Digitaal Paspoort bezitten te minimaliseren.
8. In redelijkheid zorg te dragen voor bewaring van het bewijs van certificaten, nodig om in rechte bewijs te kunnen leveren, gedurende een redelijke periode.
9. De white list voor certificaat validatie in stand te houden totdat de geldigheidsduur van het laatste certificaat verlopen is.
   Zodra dit het geval is alle ten behoeve van de Digitaal Paspoort dienstverlening door haar gebruikte Private Sleutels te vernietigen of permanent buiten werking te stellen.

ABZ heeft hiertoe een CA Termination Procedure opgesteld en geïmplementeerd.

5. FYSIEKE, PROCEDURELE EN PERSONELE BEVEILIGINGSMAATREGELEN

5.1 Fysieke beveiligingsmaatregelen

5.1.1 Locatie en inrichting

De locaties waar de verschillende onderdelen van de ABZ TTP-dienstverlening zijn ingericht, zijn:

- Digidentity
  Productie - Amsterdam;
  Uitwijk - Rotterdam;
- Symantec Inc.
  Mountain View, Californië (USA);
- KPN
  Apeldoorn/Lelystad;

5.1.2 Fysieke toegang

Hieronder volgt een beschrijving op hoofdlijnen van de beveiliging van de fysieke toegang tot de verschillende omgevingen.

Digidentity	De datacenters zijn alleen toegankelijk voor geautoriseerde personen, met vier lagen van beveiliging, conform ETSI TS 101.456. De toegang tot de computerruimte is beperkt tot hiertoe geautoriseerde medewerkers. Toegang door anderen is alleen toegestaan onder begeleiding en na uitdrukkelijke toestemming. Toegang tot CA-gerelateerde systemen vanuit het Digidentity pand kan alleen worden gerealiseerd vanuit een dedicated computer, die in een kluis is opgeslagen en alleen gebruikt kan worden door middel van een “dual key”-systeem. Van alle handelingen wordt logging bijgehouden.
Symantec Inc.	De CA bevindt zich in een omgeving die voldoet aan strenge fysieke, personele en procedurele beveiligingseisen. Voor nadere informatie aangaande de fysieke toegangsbeveiliging wordt verwezen naar de Symantec Certification Practice Statement, par. 5.1.
KPN	De KPN CA systemen zijn door minimal vier lagen fysieke beveiliging beschermd, waarbij toegang tot een lagere laag noodzakelijk is voor toegang tot een daarboven gelegen laag. Toegangscontrole tot iedere laag is progressief restrictief. Gevoelige operationele CA activiteit, activiteit gerelateerd aan de lifecycle van het certificatie process zoals authenticatie, verificatie en uitgifte, kunnen alleen uitgevoerd worden binnen de meest restricitieve fysieke lagen. Toegang

tot iedere laag is alleen mogelijk met een personeels badge met een proximity kaart. Fysieke toegang wordt gelogd of op video opgenomen. Voor toegang tot hogere lagen wordt twee-factor authenticatie gebruikt, waaronder biometrische. Toegang tot beveiligde ruimtes zonder begeleiding is verboden voor niet gerechtigde medewerkers en bezoekers. Extra beveiligingslagen voor key management beveiliging waarborgen on- en offline opslag van HSM's en keying materiaal. Voor ruimtes die gebruikt worden voor creatie en opslag van cryptografisch materiaal is duale controle vereist, ieder met twee-factor authenticatie, waaronder biometrische. Online HSM's bevinden zich in afgesloten kasten, Offline HSM's worden in afgesloten kluizen en kasten bewaard. Toegang to HSM's en keying materiaal is beperkt conform STN's functiescheiding. Het openen en sluiten van kasten en containers in deze lagen wordt gelogd voor audit doeleinden.

5.1.3 Electriciteitsvoorzieningen en air conditioning

De netwerkcomponenten zijn aangesloten op een UPS en de ruimtes als geheel hebben een noodstroomvoorziening. Tevens zijn de ruimtes voorzien van airconditioning ter controle van de temperatuur en relatieve vochtigheid.

5.1.4 Maatregelen ten aanzien van wateroverlast

In de computerruimtes is geen waterleiding opgenomen. Alle apparatuur is geplaatst op een verhoogde vloer om de kans op wateroverlast tot een minimum te beperken.

5.1.5 Brandbeveiliging

De ruimtes zijn voorzien van een deugdelijke brandblusinstallatie met automatische detectie, die directe sturing hebben op een aantal voorzieningen zodat de opgestelde apparatuur ingeval van brand zo min mogelijk schade ondervindt.

5.1.6 Opslag gegevensdragers

De backups worden opgeslagen in een kluis.
Uitsluitend geautoriseerde medewerkers hebben toegang tot de gemaakte backups.

5.1.7 Afvalverwijdering

ABZ, Digidentity en KPN hebben een overeenkomst met een gespecialiseerd bedrijf voor het verwijderen van papier. Personeel is verplicht papier weg te gooien in gesloten containers die op de afdelingen staan.
Media met gevoelige informatie worden onleesbaar gemaakt alvorens ze verwijderd worden.

5.1.8 Off-site backup

Off-site backups van kritische system data, audit logs en andere gevoelige informatie worden standaard uitgevoerd. De offsite backup media worden op een fysiek veilige wijze opgeslagen.

5.2 Procedurele beveiligingsmaatregelen

5.2.1 Functies en rollen

1. De medewerkers van het Customer Administration van ABZ verzorgen het organisatorische beheer van de ABZ RA. Tevens voeren zij de benodigde administratieve handelingen uit.
2. De operationele RA-functies en het TTP-management zijn ondergebracht bij ABZ.
3. Digidentity verzorgt het technische beheer van de ABZ RA-P en de CA. Secundair zijn dit SaaSplaza en KPN.

5.2.2 Aantal benodigde personen per taak

1. Voor het uitvoeren van organisatorische werkzaamheden is altijd minimaal 1 FTE beschikbaar, conform het bepaalde in onderdeel 5.2.1.
2. Voor het uitvoeren van technische werkzaamheden is altijd minimaal 1 FTE beschikbaar, conform het bepaalde in onderdeel 5.2.1 sub 2.

5.2.3 Identificatie- en authenticatieprocedure voor functies en rollen

De identificatie- en authenticatieprocedures van de functionarissen die ten behoeve van de ABZ TTP-dienstverlening werkzaam zijn, wijken niet af van de reguliere ABZ-procedure bij indiensttreding.
Deze procedures zijn vastgelegd in de HRM-procedures voor indienstname van nieuwe medewerkers. Controle van het identiteitsbewijs en een Verklaring omtrent het Gedrag maken onderdeel uit van deze procedure.

5.3 Personele beveiligingsmaatregelen

5.3.1 Functie-eisen

De functionaris behoort te voldoen aan de eisen zoals beschreven in het door ABZ opgestelde functieprofiel.

5.3.2 Antecedentenonderzoek

Op de medewerkers van ABZ kan een antecedentenonderzoek worden uitgevoerd. Medewerkers wordt gevraagd om een Verklaring omtrent het Gedrag.

5.3.3 Opleidingsvereisten

De medewerkers die werkzaamheden voor de Digitaal Paspoort-dienstverlening uitvoeren, hebben een daartoe bestemde (interne) opleiding gevolgd, inclusief een (intern) examen. Indien ontwikkelingen dit vereisen, worden opfrissings- of vervolgopleidingen georganiseerd.

5.3.4 Opleiding-/cursusfrequentie en vereisten

Zie onderdeel 5.3.3 van dit CPS.

5.3.5 Job rotation-frequentie en loopbaantraject

Niet van toepassing.

5.3.6 Sancties als gevolg van ongeautoriseerd handelen

Indien aannemelijk wordt gemaakt dat personeel van ABZ ongeautoriseerde handelingen heeft verricht, wordt door ABZ onverwijld een intern onderzoek gestart. De bepalingen in onderdeel 2 van dit CPS zijn van overeenkomstige toepassing. Indien ABZ derden inschakelt voor het uitvoeren van de dienstverlening, legt zij deze derden vergelijkbare voorwaarden op.

5.3.7 Functieprofielen

ABZ stelt functieprofielen op voor de bij de ABZ TTP-dienstverlening betrokken medewerkers. Deze functieprofielen worden beheerd en onderhouden door de afdeling HRM. De TTP-manager is betrokken bij het opstellen en onderhouden van functieprofielen voor RA-medewerkers.

5.3.8 Beschikbare documentatie voor personeel

ABZ stelt aan haar personeel alle documentatie en overige hulpmiddelen ter beschikking, die voor het uitoefenen van de in dit CPS genoemde functies benodigd zijn.

6. TECHNISCHE BEVEILIGINGSMAATREGELEN

6.1 Sleutelpaargeneratie en installatie

Deze paragraaf geeft een overzicht van de getroffen technische maatregelen ten aanzien van de sleutelpaargeneratie en -installatie. In de onderstaande tabel wordt een introductie gegeven op de verschillende certificaten en hun eigenschappen die binnen de ABZ TTP-dienstverlening een rol spelen:

Certificaat	Omschrijving
Digitaal Paspoort	Dit certificaat voor de eindgebruiker wordt uitgegeven door ABZ. De gebruiker kan dit certificaat toepassen voor het verkrijgen van toegangsautorisaties en het digitaal ondertekenen en versleutelen van elektronische bestanden, zoals bijvoorbeeld e-mail. De privésleutel is opgeslagen in het systeem van de gebruiker.
CA-certificaten	Dit zijn de CA-certificaten van Digidentity, ABZ, KPN en Symantec. Primair: de CA van Digidentity genereert het ABZ Digitale Paspoort. Secundair: De CA van ABZ genereert het ABZ Digitale Paspoort, de CA van KPN genereert de ABZ CA en de CA van Symantec genereert op zijn beurt het KPN CA-certificaat. CA sleutelpaar generatie is uitgevoerd door meerdere getrainde en vertrouwde medewerkers, waarbij gebruik wordt gemaakt van betrouwbare systemen en processen, en sterke cryptografie is vereist voor de gegenereerde sleutels. Uitgevende Root CA's en alle online KPN en Managed Pki klant CA's die door de crytpografische modules worden gebruikt voor sleutelpaar generatie voldoen aan de eisen van FIPS 140-1 level 3. Alle CA sleutelparen worden gegenereerd in vooraf geplande Key Generation Ceremonies, in overeenstemming met de Key Ceremony Guide en de STN Security and Audit Requirements Guide. Alle activiteiten tijdens de key generation ceremony worden vastgelegd, gedateerd en ondertekend door alle betrokken personen. Deze vastlegging wordt bewaard voor audit en tracking doeleinden. De bewaarperiode wordt bepaald door het KPN management. RA sleutelpaar generatie wordt uitgevoerd door de RA, waarbij gebruik wordt gemaakt van een FIPS 140-1 level 1 gecertificeerde cryptografische module, geleverd door de browsersoftware. Klanten genereren het sleutelpaar dat gebruikt wordt door de Automated Administraion servers. KPN raadt aan om hierbij gebruik te maken van een FIPS 140-1 level 2 of hoger gecertificeerde cryptografische module, geleverd door de browser software, of van een SSCD. Voor server certificaten wordt meestal gebruik gemaakt van de sleutelpaar generator die geleverd wordt door de web server software.Voor eind gebruiker sleutelparen voor gekwalificeerde certificaten wordt gebruik gemaakt van een EAL4+ gecertificeerd SSCD.

6.1.1 Sleutelpaargeneratie

Binnen de ABZ TTP-dienstverlening worden uitsluitend sleutels gebruikt waarvan de sleutellengte voldoet aan de stand van de techniek. Dit minimaliseert de kans dat de privésleutel door middel van crypto-analyse gedestilleerd kan worden.

De generatie van de CA- en RA-sleutelparen vindt plaats onder gecontroleerde omstandigheden welke gepaard gaan met adequate beveiligingsmaatregelen. Voor meer informatie raadpleegt men het Digidentity (primair) of het Symantec en het KPN CPS (secundair).

De generatie van eindgebruikersleutels vindt plaats op het systeem van de gebruiker. Ook de opslag van de privésleutel vindt plaats op het systeem van de gebruiker. De wijze waarop dit gebeurt, is afhankelijk van de gebruikte software, maar vindt in elk geval versleuteld plaats zodat niet iedereen die toegang heeft tot (dat deel van) die machine de informatie kan lezen/gebruiken.

6.1.2 Distributie privésleutel aan gebruiker

Aangezien de privésleutel gegenereerd wordt op de machine van de gebruiker zelf, hoeft de privésleutel niet gedistribueerd te worden.

6.1.3 Distributie publieke sleutel aan CA

De publieke sleutel wordt middels een geëncrypte verbinding naar de CA getransporteerd door deze samen met de informatie die de gebruiker moet identificeren, aan te bieden aan de CA.

Een Digitaal Paspoort wordt uitgegeven indien voldaan is aan de eisen genoemd in onderdeel 3 en de onderdelen 4.1 tot en met 4.3 van dit CPS.

6.1.4 Distributie publieke sleutel CA aan eindgebruikers

De publieke sleutel van de Root CA is opgenomen in het standaard in de internetbrowser opgenomen certificaat van Digidentity (primair) en Symantec (PCA G3) (secundair). De publieke sleutels van de intermediate CA's zijn beschikbaar via de website van ABZ.

6.1.5 Sleutellengten

Voor asymmetrische (publieke en privé) sleutels wordt het RSA cryptosysteem gebruikt met een sleutellengte van minimaal 2048 bits (NB: afhankelijk van de gebruikte browser kan een hogere sleutellengte gebruikt worden).
Als hash-algoritmen gebruikt ABZ de SHA-2.

6.1.6 Generatie parameters publieke sleutels

De parameters die gebruikt worden bij de generatie van de sleutels zijn afhankelijk van en meestal bepaald door de gebruikte browser of applicatie. Indien een keuze mogelijk is wordt geadviseerd een zo groot mogelijke sleutellengte te kiezen.

6.1.7 Kwaliteitscontrole parameters

Niet van toepassing

6.1.8 Hardware/software sleutelgeneratie

De generatie van de CA- en RA-sleutelparen vindt plaats onder gecontroleerde omstandigheden welke gepaard gaan met adequate beveiligingsmaatregelen. De CA- en RA-sleutelgeneratie vindt plaats binnen een hardware module (zie eveneens paragraaf 6.2). Voor meer informatie raadpleegt men het CPS van Digidentity (primair) of van Symantec en KPN (secundair). De gebruikerssleutels worden softwarematig gegenereerd door de gebruikte browser of applicatie.

6.1.9 Gebruik publieke sleutels

De publieke sleutel behorende bij het Digitaal Paspoort van de gebruiker mag uitsluitend gebruikt worden voor de toepassingen beschreven in paragraaf 1.3.4. Dit is ook vastgelegd in het certificaat volgens de “key usage flags” in de extensies van de X.509v3-certificaten.

6.2 Bescherming van de privésleutel

Het beschermen van de privésleutel van de gebruiker is de verantwoordelijkheid van de gebruiker. Deze moet alle redelijkerwijs te verwachten maatregelen nemen om te voorkomen dat de privésleutel gecompromitteerd kan worden.

In verband met de mogelijkheid tot het leveren van bewijs en de mogelijkheid tot verificatie binnen de termijn van de geldigheidsduur van het Digitaal Paspoort, moet de aanvrager (gebruiker) zijn Digitaal Paspoort, zijn privésleutel en de daarvan gemaakte backups op een veilige, betrouwbare en duurzame wijze bewaren zolang deze gegevens juridisch relevant kunnen zijn.

In bepaalde omstandigheden kan het Digitaal Paspoort en de bijbehorende privésleutel van de gebruiker worden ingezet voor de beveiliging van berichten in back-officesystemen. De gewenste authenticatie op persoonsniveau hierbij kan vereisen dat de gebruiker hiervoor de privésleutel voor het aanbrengen van een elektronische handtekening exporteert en voor dit doel overdraagt ter installatie op een server. Hoewel hierbij aandacht zal worden geschonken aan procedures en maatregelen ter beveiliging van de serveromgeving, verleent de gebruiker hieraan medewerking op eigen risico. Het overdragen van de privésleutel ontheft de gebruiker niet van de verplichting de private sleutel adequate wijze te beschermen ingevolge par. 2.1.3.2. Uit hoofde van 2.2.1.2 lid 1 sluit ABZ aansprakelijkheid voor schade die uit dit gebruik voortvloeit nadrukkelijk uit.

6.2.1 Standaarden Cryptografische Module

De door de CA gehanteerde hardware cryptografische module die de privésleutel van de CA bevat, voldoet aan de strengste internationale normen op het gebied van informatiebeveiliging. De primaire en secundaire CA maken gebruik van een cryptografische module welke goedgekeurd is volgens de FIPS 140-2 level 3 standaard.Voor meer informatie raadpleegt men het CPS van Digidentity (primair) en van Symantec en KPN (secundair).

6.2.2 Functiescheiding m.b.t. beheer privésleutel

RA:

Voor de RA geldt dat de RA-operator geen beschikking heeft, noch kan krijgen over de RA-sleutels. Het functioneel beheer van de RA-sleutels wordt uitgevoerd door de RA-provider. De RA-P -functie is opgedeeld in een RA-website en een RA-requestor die ieder een eigen technisch beheer kennen. De RA-website bevat een servercertificaat ten behoeve van identificatie van de RA-website en de sessiebescherming tussen de client en de RA-website. Het servercertificaat is gecertificeerd door Symantec.

De RA-requestor bevat een hardware token met een privésleutel/certificaat ten behoeve van het ondertekenen van de certificaataanvragen naar de Digidentity (KPN)-CA en de sessiebescherming tussen de RA-site en de RA-requestor. De RA-requestor accepteert alleen aanvragen van erkende en vooraf bekende RA-sites. De publieke sleutel is gecertificeerd door Digidentity (KPN). De privésleutel is uitsluitend toegankelijk voor de administrator en het hardware token is afgeschermd met een eigen wachtwoord van hoge kwaliteit. Ieder verzoek tot mutatie door de security officers vereist aanwezigheid en toestemming van de administrator en wordt als zodanig in een logboek vastgelegd.

CA:
Het beheer van de privésleutel van de CA is beschreven in het CPS van Digidentity (primair) en van KPN en Symantec (secundair).

6.2.3 Escrow privésleutel

De privésleutel van de CA wordt niet in escrow gegeven.

6.2.4 Backup privésleutel

Voor backup- en archiveringsdoeleinden worden de privésleutels/certificaat sets van zowel de RA-website als de RA-requestor geëxporteerd en in een cryptografisch bestand opgeslagen dat is beschermd door een wachtwoord. Zij worden op elektronische wijze tweevoudig gebackupt, waarbij één van deze backups opgeslagen wordt in een kluis en de ander bij een externe derde partij. De backup bij de derde partij zal tevens dienen voor archiveringsdoeleinden.

De gebruiker is zelf verantwoordelijk voor het maken en beveiligen van een backup van zijn privésleutel en wordt hier ook op gewezen.

6.2.5 Archivering privésleutel

Zie onderdeel 6.2.4 van dit CPS.

6.2.6 Invoer privésleutel in Cryptografische Module

De prive-sleutel van de RA-site wordt lokaal gegenereerd door twee administrators in bijzijn van twee security-officers en wordt in een softwarematige cryptografische module geladen.De prive-sleutel van de RA-requestor wordt aangemaakt op de Hardware Security Module en daar opgeslagen zonder dat deze op enig moment zichtbaar is voor beheerders of gebruikers.
Indien de gebruiker van een standaard-browser gebruik maakt, wordt de privesleutel lokaal gegenereerd en opgeslagen in de softwarematige cryptografische module.

6.2.7 Activeren privésleutel

De privésleutel van de RA-site wordt geactiveerd door het opstarten van de webserver. De webserver draait onder administrator rechten en behoeft daardoor geen aanwezigheid van security officers. De privésleutel van RA-requestor wordt geactiveerd door het opstarten van de RA-requestor. Er wordt in beide situaties uitgegaan van een hoog niveau van fysieke beveiliging en administrator integriteit.

6.2.8 Buiten werking stelling privésleutel

De privésleutel van de RA-site en van de RA-requestor kan door iedereen die administrator rechten heeft op het systeem worden gedeactiveerd door het stoppen van de server. Er is in dit geval geen vervaltijd.

Voor het systeem bij de gebruiker geldt dat iedereen die de juiste rechten heeft de privésleutel onbruikbaar kan maken of kan verwijderen.

6.2.9 Vernietiging privésleutel

Vernietigen van de privésleutel van de RA-site en van de RA-requestor is mogelijk voor administrators door het geheel herinstalleren van het besturingssysteem. Hierbij wordt ook de software cryptografische module vernieuwd. Verder kan de privésleutel alleen worden vernietigd door gebruik te maken van de sleutelgenerator.

Voor het systeem bij de gebruiker geldt hetzelfde als in onderdeel 6.2.8.

6.3 Overige aspecten van sleutelbeheer

6.3.1 Archivering, buiten werking stelling en vernietiging publieke sleutels

Het archiveren van de privésleutel/certificaat set vindt plaats conform de in 6.2.4 van dit CPS aangegeven methode. Aangezien een certificaat de publieke sleutel bevat zal de publieke sleutel niet separaat worden gearchiveerd.

De publieke sleutel van de RA-site en van de RA-requestor kan buiten werking worden gesteld door of de server te stoppen of het certificaat in te trekken. Voor het stoppen van een server is een administrator bevoegdheid nodig. Voor het intrekken van een certificaat is de revokatie zin nodig. Hierbij geldt dat het enige tijd duurt voordat de certificaten op de CRL verschijnen, echter aanvragen via een RA-requestor met ingetrokken certificaat zullen door de CA niet in behandeling worden genomen.

Op de RA-site en op de RA-requestor kunnen publieke sleutels dan wel certificaten worden vernietigd indien gebruik wordt gemaakt van de passende sleutelgenerator. Dit vereist zowel een administrator bevoegdheid als aanwezigheid van een tweetal security officers.

6.3.2 Periode gebruik publieke/privésleutel

De certificaten van de zowel de RA-site als de RA-requestor zijn 1 jaar geldig. Enige tijd voor het verstrijken van de vervaldatum signaleert de CA de noodzaak van vernieuwing.

Voor de geldigheidsduur van de CA sleutels/certificaten en de wijze van vernieuwing ervan, wordt verwezen naar het CPS van Digidentity (primair) en van Symantec en KPN (secundair).

Een Digitaal Paspoort is 1 jaar geldig. De expiratiedatum wordt bepaald op 1 jaar na uitgifte. Voor het bereiken van de expiratiedatum wordt de gebruiker middels een e-mail bericht geattendeerd op de noodzaak van verlenging van het Digitaal Paspoort.

6.4 Activeringsdata

6.4.1 Generatie en installatie

RA-P:
Generatie vindt plaats in de cryptografische module, waaruit de publieke sleutel wordt geëxporteerd ten einde een certificaat te verkrijgen.
Export van de privésleutel vindt plaats onder vermelding van een PIN per secure token. Er zijn drie tokens beschikbaar, waarvan er minimaal twee nodig zijn voor herinvoer.

De bijbehorende key management applicatie bepaalt de eisen waaraan de PIN moet voldoen.

6.4.2 Bescherming

Het gebruik van een PPC om eventueel geblokkeerde toegang tot de privésleutel van de gebruiker te deblokkeren is niet mogelijk (zie hiervoor ook 6.2.3).

6.4.3 Overige aspecten

Niet van toepassing.

6.5 Computerbeveiligingsmaatregelen

6.5.1 Specifieke technische eisen aan computerbeveiligingsmaatregelen

1. Alle computers die een cruciaal onderdeel vormen van het netwerk hebben een hoge beschikbaarheidsgraad.
2. Systemen zijn alleen toegankelijk indien men beschikt over de daarvoor benodigde wachtwoorden dan wel certificaten. Deze wachtwoorden worden periodiek gewijzigd.

6.5.2 Kwalificatie van de computerbeveiligingsmaatregelen

ABZ stelt hoge kwaliteitseisen aan haar beveiligingsmaatregelen. ABZ en haar partners volgen standaarden als het gaat om computerbeveiligingsmaatregelen. Hierbij volgt ABZ de algemene standaardnormeringen.

6.6 Levenscyclus beveiligingsmaatregelen

6.6.1 Beheersmaatregelen Systeemontwikkeling

Om de beveiliging op een hoog niveau te houden worden de volgende stappen uitgevoerd:

Volgen en bestuderen security alerts van leveranciers en het NCSC.

Afhankelijk van de soort update :

1. Bij patches:
   A. Installeren patches op testomgeving
   B. testen testomgeving
   C. aan de hand van bevindingen eventueel installeren patches.
2. Bij nieuwe versies:
   A. Installeren nieuwe versies op testomgeving
   B. testen testomgeving.
   C. Controleren of de functionaliteit van de nieuwe versie minimaal die van de oude versie evenaart.
   D. Installeren nieuwe versie.
3. Nieuwe software:
   A. Installeren nieuwe software op testomgeving
   B. testen functionaliteit nieuwe software op specifieke eisen
   C. analyseren beveiligingsrisico's
   D. beslissen omtrent invoering nieuwe software
   E. uitvoeren van de benodigde beveiligingsmaatregelen
   F. installeren nieuwe software

Daarnaast kan de behoefte bestaan aan certificaten voor intern gebruik ten behoeve van het testen en monitoren van diensten van ABZ. Hiertoe kan de TTP-manager testmedewerkers schriftelijk toestemming geven om voor een afgebakende periode een of meerdere certificaten te genereren en in te zetten.

6.6.2 Beheersmaatregelen beveiligingsmanagement

ABZ en haar partners voeren periodiek controles uit op haar operationele systemen conform de interne beveiligingsmaatregelen. Hieronder kan mede worden begrepen de controles op de integriteit van de hardware en de software (integrity checks).

6.6.3 Kwalificatie van de genomen levenscyclus beveiligingsmaatregelen

Niet van toepassing.

6.7 Netwerkbeveiligingsmaatregelen

1. Alle computers welke een cruciaal onderdeel vormen van het netwerk hebben een hoge mate van beschikbaarheid.

2. Systemen zijn alleen toegankelijk indien men beschikt over de daarvoor benodigde wachtwoorden dan wel certificaten. Deze wachtwoorden worden periodiek gewijzigd.

6.8 Cryptografische Module

De RA-site maakt gebruik van een softwarematige cryptografische module. De RA-requestor en CA maken gebruik van een FIPS 140-2 Level 3 gecertificeerde Hardware Security Module.

Er wordt gebruik gemaakt van de interne cryptografische module van de browser van de gebruiker.

7. DIGITAAL PASPOORT EN CERTIFICATE REVOCATION LIST FORMAT

7.1 Profiel Digitaal Paspoort

De volgende velden zijn in het x.509v3 Digitaal Paspoort opgenomen:

1. Versienummer
2. Serienummer
3. Encryptievorm handtekening
4. Gegevens over de uitgevende CA
5. Datum begin geldigheid
6. Datum eind geldigheid
7. 'Subject' veld, de opbouw van het subjectveld is beschreven in 3.1.1.
8. De publieke sleutel van de certificaathouder met vermelding van sleutellengte
9. Toegestane gebruiksmogelijkheden
   - Subject Type=End Entity
   - Path Length Constraint=None
10. Locatie CRL
11. Key identifiers voor het subject en voor de authority

7.1.1 Versienummer Digitaal Paspoort

Het Digitaal Paspoort is een certificaat volgens de ITU-T x.509v3 standaard (tevens ISO 9594-8 standaard).

7.1.2 Extensies

In het Digitaal Paspoort worden een vijftal X.509v3 extensies gebruik. Alle in het Digitaal Paspoort gebruikte extensies zijn 'non-critical'. De extensies en hun Object Indentifier zijn:

- Basic Contraints, OID: 2.5.29.19
- Key Usage, OID: 2.5.29.15
- CRL Distribution Points, OID: 2.5.29.31

7.1.3 Algoritme object identifiers

Primair:
De gebruikte algoritmes voor het signeren van de public-key zijn:

1. Assymetrisch: 1 2 840 113549 1 1 1 (PKCS1 met RSA)
2. Hash: 1 2 840 113549 1 1 11 (PKCS 1 SHA-256 met RSA)

Secundair:
De gebruikte algoritmes voor het signeren van de public-key zijn:

1. Asymmetrisch: RSA in overeenstemming met PKCS #1
2. Hash: Het gebruikte algoritme is onder de SHA-2 root (domein Organisatie) sha-2 WithRSAEncryption.

De object identifiers van de gebruikte algoritmen zijn als volgt:

1. PKCS#1 met RSA Encryptie : 1.2.840.113549.1.1.1
2. PKCS#1 SHA-1 met RSA encryptie: 1.2.840.113549.1.1.5

1= iso, 2= member-body, 840 = us, 113549 = rsadsi, 1= pkcs, 1=pkcs-1 (*1)

(*1) Internet X.509 Public Key Infrastructure, Certificate and CRL Profile:
http://tools.ietf.org/html/draft-ietf-pkix-ipki-part1-09.txt
http://www.faqs.org/rfcs/rfc3174.html

7.1.4 Naamgeving

Zie onderdeel 3.1.1.

7.1.5 Naamgevingsbeperkingen

De waarden van de attributen zoals die in de Repository opgeslagen zijn, worden ook gebruikt binnen het subject van het Digitaal Paspoort. Zie 3.1.1.
Het veld “o- “ bevat de naam van het bedrijf waar de gebruiker werkzaam is. Dit volledige veld mag niet langer zijn dan 64 tekens, wat betekent dat de bedrijfsnaam niet langer mag zijn dan 60 tekens.

7.1.6 Certificate Policy object identifiers

Niet van toepassing.

7.1.7 Gebruik van Policy beperking extensie

Niet van toepassing.

7.1.8 Policy qualifiers syntax en semantiek

Niet van toepassing.

7.1.9 Interpretatie van de betekenis van de belangrijkste Certificate Policy extensies

Niet van toepassing.

7.2 Profiel Certificate Revocation List

De CRL van Digidentity kent onderstaand profiel:

Veld	Waarde
Handtekening algoritme	Algoritme voor het ondertekenen van de url. Digidentity CRL’s worden ondertekend met PKCS1 met RSA-encryptie (OID: 1 2 840 113549 1 1 11)
Uitgever	Digidentity BV
Volgende update	Datum waarop de volgende CRL zal worden uitgegeven.
Ingetrokken certificaten	Overzicht van ingetrokken certificaten, middels het serienummer en de intrekkingsdatum

De CRL van Symantec kent onderstaand profiel:

Veld	Waarde
Handtekening algoritme	Algoritme voor het ondertekenen van de url. KPN CRL's worden ondertekend met Sha2 met RSA-encryptie (OID: 1.2.840.113549.1.1.5)
Uitgever	Entiteit die de CRL heeft uitgegeven en ondertekend
Volgende update	Datum waarop de volgende CRL zal worden uitgegeven.
Ingetrokken certificaten	Overzicht van ingetrokken certificaten, middels het serienummer en de intrekkingsdatum

7.2.1 Versienummer CRL

Digidentity en Versign gebruiken geen versienummers bij het publiceren van haar CRL, maar publiceren alleen de meest recente versie. De ingangsdatum van deze versie en de datum van de volgende update van de CRL worden hierbij ook gepubliceerd.
CRL's worden uitgegeven conform de X.509 version 1 standaard.

7.2.2 CRL en CRL-entry extensies

Er worden geen CRL en CRL-entry extensies gebruikt. Zie het CPS van de CA over de opmaak van de CRL.

8. ADMINISTRATIEVE BEPALINGEN

8.1 CPS Veranderingsbeheer

Dit CPS is voorzien van een versienummer, dat is opgebouwd als x.y.z. Veranderingen als genoemd in onderdeel 8.1.1 leiden tot ophoging van “z”, veranderingen als genoemd in onderdeel 8.1.2 leiden tot ophoging van “y” en veranderingen als genoemd in onderdeel 8.1.3 leiden tot ophoging van “x”.

8.1.1 Verandering CPS zonder inkennisstelling

Veranderingen van dit CPS waarbij ABZ niet verplicht is gebruikers hiervan in kennis te stellen zijn:

1. Aanpassingen van gebruikte woordkeuze.
2. Aanpassingen van lay-out.
3. Aanpassingen van stijlfouten.
4. Aanpassingen van tikfouten.
5. Aanpassingen van technologische aspecten, die van geen invloed zijn op de kwaliteit van de TTP dienstverlening.

8.1.2 Verandering CPS met verplichte inkennisstelling

Veranderingen van dit CPS waarbij ABZ verplicht is gebruikers hiervan in kennis te stellen zijn:

- Alle aanpassingen die niet onder onderdeel 8.1.1 vallen, en die niet onder onderdeel 8.1.3 vallen.

Inkennisstelling geschiedt door het plaatsen van een mededeling op de Digitaal Paspoort website en vindt plaats ten minste 30 dagen voorafgaand aan het toepasselijk verklaren van het nieuwe CPS.

8.1.3 Verandering die nieuwe versie van het CPS tot gevolg heeft

Veranderingen van dit CPS die tot gevolg hebben dat het noodzakelijk is een nieuwe versie van het CPS op te stellen zijn, zonder daartoe beperkt te zijn:

1. Structurele verandering van de door ABZ aangeboden TTP-dienstverlening. Deze kan leiden tot noodzakelijke intrekking en heruitgifte van het Digitaal Paspoort.
2. Verandering in de toepassing van het Digitaal Paspoort, zoals beschreven in dit CPS (zie met name onderdeel 1.3).

8.2 Publicatie en inkennisstelling

Deze versie van het CPS (versie 4.3) is geldig vanaf juli 2015. Op de website van ABZ zijn de exacte data van publicatie en in werking treding vermeld.

8.2.1 Onderdelen CPS die niet worden gepubliceerd

Niet van toepassing.

8.2.2 Wijze distributie CPS

Het CPS is toegankelijk op de Digitaal Paspoort website en op de website van ABZ.

8.3 Goedkeuringsprocedures CPS

De TTP-manager bij ABZ is verantwoordelijk voor dit CPS. De procedure voor wijzigingen en goedkeuringen van het CPS is als volgt:

1. Voorstellen tot wijziging kunnen door iedere belanghebbende ingediend worden.
2. De TTP-manager is verantwoordelijk voor de verwerking van de voorstellen. Hij kan zich hierbij laten adviseren door inhoudelijke experts, onder andere op technisch, procedureel, commercieel en juridisch gebied. Uiteindelijk beslist de TTP-manager of een voorstel tot wijziging wordt doorgevoerd.
3. Indien het voorstel is goedgekeurd, laat de TTP-manager het CPS aanpassen. Indien op grond van onderdeel 8.1 van dit CPS voor inwerkingtreding voorafgaande inkennisstelling van de certificaathouders noodzakelijk is, draagt de TTP-manager tevens hiervoor de verantwoordelijkheid.
4. Tijdens de periodieke audit van dit CPS zal worden aangegeven welke wijzigingen hebben plaatsgevonden in de periode vanaf de vorige audit.