PKI overheid

Offerte-aanvraag

Juridische ondersteuning
PKI overheid

COMMUNICEREN IN VERTROUWEN
VERTROUWEN IN COMMUNICEREN

26 mei 2000

Document geschiedenis

Versie	Datum	Status/reden revisie	Auteur
0.1	16/5/2000	Algemene opzet	
0.2	22/5/2000	Concept	
1.0	26/5/2000	Definitieve versie	

PKI overheid

Inhoudsopgave

Algemeen

1.1 Doelstellingen PKI overheid

De doelstelling van de *taskforce PKI overheid* is: "Het realiseren van een werkbare betrouwbare infrastructuur voor PKI-diensten die voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers".

Met PKI-diensten worden diensten bedoeld die direct of indirect bijdragen aan het waarborgen van de authenticiteit (identificatie/oorsprong), integriteit (juistheid) en exclusiviteit (vertrouwelijkheid) van elektronische communicatie en het mogelijk maken om digitale handtekeningen op grote schaal te gebruiken.

Onder een infrastructuur voor PKI-diensten wordt de combinatie van bestuurlijke, organisatorische en technische componenten verstaan die nodig zijn voor het leveren van de PKI-diensten.

De term communicatiebehoefte van de overheid omvat de communicatie binnen drie domeinen, te weten Overheid - Burger, Overheid - Bedrijfsleven en Overheid -Overheid. De communicatie met maatschappelijke instellingen vallen binnen het domein Overheid-Burger.

Met transparantie of uniformiteit wordt bedoeld dat de overheid zicht naar buiten toe met één gezicht presenteert. Er moet voor het bedrijfsleven en de burgers geen technisch onderscheid zijn in de communicatie met de verschillende departementen en/of andere overheidsinstellingen.

1.2 Vraagstelling

De taskforce PKI overheid is dus belast met het invoeren van een infrastructuur die betrouwbare en vertrouwelijke elektronische communicatie mogelijk maakt binnen een breed werkveld.

Bij het definiëren, invoering en het gebruik van PKI-diensten wordt de taskforce geconfronteerd met een aantal specifieke vragen op juridisch gebied. Op dit moment zijn onder meer de volgende punten geïdentificeerd:

Aansprakelijkheid
- Welke mate van aansprakelijkheid komt voort uit de Europese Richtlijn voor de elektronische handtekening en andere relevante wetgeving?
- Hoe kunnen de aansprakelijkheden worden belegd bij en beperkt door de verschillende actoren binnen de PKI?

Elektronische handtekening
- Welke eisen worden gesteld aan een PKI die een geavanceerde elektronische handtekening ondersteunt?
- Welke juridische problemen liggen er bij het invoeren van elektronische handtekeningen in overheidsprocessen (publiekrechtelijk, vormvoorschriften e.d.).
- Welke nationale en internationale ontwikkelingen zijn er op dit gebied en wat is hun belang voor de taskforce?
- Hoe kan, vanuit juridisch oogpunt, (internationale) interoperabiliteit worden bewerkstelligd?

privacy

- Welke eisen worden er gesteld vanuit met name de WBP?

In het kader van deze vraagstelling nodigt Opdrachtgever bedrijven uit offerte uit te brengen om de in paragraaf 1.3 genoemde diensten te leveren.

1.3 Opdrachtformulering

Het is het doel van deze opdracht om specialistische juridische ondersteuning PKI-gebied voor de taskforce PKI overheid te verzorgen. De gevraagde ondersteuning zal onder meer uit de volgende bijdragen bestaan.

a) Juridische PKI-kennis beschikbaar stellen aan de taskforce.

b) Het signaleren van juridische knelpunten en het initiëren van activiteiten om deze op te lossen.

c) Het vertegenwoordigen van de taskforce bij de verschillende wetgevingstrajecten in het kader van de elektronische hantekening

d) Het geven van juridische ondersteuning bij het faciliteren van proefprojecten zowel richting PKI overheid als de verantwoordelijken voor de (externe) projecten.

e) Ondersteuning bij het opstellen van Certification Policies (CP) en Certification Practice Statements (CPS) voor de overheids PKI. (opm: eerste concept juni/juli, 2^{e} versie september)

f) Ondersteuning bij de aanbestedingsprocedures/bestek.

g) Het (inhoudelijk) aansturen van deelstudies op juridisch gebied van de PKI.

h) Het bewaken van de consistentie tussen de diverse deelstudies.

Bij het uitvoeren van deze activiteiten dient te worden samengewerkt met de interne juriste van de taskforce PKI overheid.

Onderdeel van deze opdracht is tevens het uitwisselen van kennis met de taskforceleden en het introduceren van de interne juriste in de specifieke juridische aspecten van PKI.

1.4 Duur van de overeenkomst

De op te leveren producten, de elementen van algemene ondersteuning voor de taskforce PKI overheid, worden bepaald op het moment dat de bijdrage relevant is. In overleg met de projectleider taskforce PKI overheid wordt de specificatie van de deelproducten vastgesteld en wordt de planning van de werkzaamheden, waaronder de datum van oplevering, vastgesteld. De voortgang van de activiteiten wordt in beginsel wekelijks besproken tussen projectleider en opdrachtnemer.

Vooralsnog wordt uitgegaan van een ondersteuning gedurende gemiddeld 2 dagen per week in 2000 vanaf de opdrachtverlening. Een eventuele verlenging van de ondersteuning in 2001 behoort tot de mogelijkheden.

2 Algemene voorwaarden

2.1 Tijdspad offerte

Ten aanzien van de offerteprocedure zal het volgende tijdspad worden gehanteerd:

Fase	Omschrijving	Einddatum
1	Verzenden uitnodiging tot offerte	26 mei 2000
2	Deadline indienen offerte	9 juni 2000
3	Eventuele mondelinge toelichting offertes	12 t/m 16 juni 2000
4	Selectie opdrachtnemer	19 juni 2000

2.2 Indienen offerte

De offerte dient conform bovenstaande tijdsplanning, op 5 juni 2000 (uiterlijk 17.00 uur) bij het onderstaande adres te zijn ontvangen. De offerte wordt in tweevoud verstuurd naar:

Ministerie van Binnenlandse Zaken
T.a.v. [redacted] Taskforce PKI overheid, de heer [redacted]
Postbus 20011
2500 EA Den Haag

Bezoekadres: Herengracht 17-19
Contactpersoon voor inhoudelijke vragen is dhr. [redacted] (tel. [redacted]).

2.3 Afwijkingen offerteaanvraag

Wij verzoeken u uw offerte te laten aansluiten bij onze aanvraag. Afwijkingen op de aanvraag dienen te worden gemotiveerd. Wijzigingen of aanvullingen op onze aanvraag zullen slechts in aanmerking worden genomen voor zover deze van ondergeschikte aard zijn. Niet aangegeven of verklaarde afwijkingen zullen door ons buiten beschouwing kunnen worden gelaten.

2.4 Minimale geldigheidsduur

De offerte zal een minimale geldigheid hebben van 60 dagen na sluitingsdatum. Tijdens die periode heeft zij het karakter van een onherroepelijk aanbod.

2.5 Vertrouwelijkheid

Deze offerteaanvraag zal vertrouwelijk worden behandeld en slechts aan medewerkers worden getoond die voor het uitbrengen van de offerte daarvan kennis moeten nemen. Evenmin zal door u op enigerlei wijze aan derden kennis worden gegeven van het feit dat Opdrachtgever een offerte heeft aangevraagd en/of van de gegevens die in dat verband door Opdrachtgever zijn of worden verstrekt.

De vertrouwelijkheid zal ook worden bewaard wanneer de offerte niet tot de totstandkoming van een overeenkomst zal leiden. Opdrachtgever zal de aan haar uitgebrachte offerte niet aan derden beschikbaar stellen.

2.6 Samenwerking met partners

Er wordt op gewezen dat deze opdracht niet in afzonderlijke kavels wordt verdeeld en dat men zich alleen voor de gehele opdracht kan aanmelden.

2.7 *Kosten offerte*

Aan de offerte zullen voor de Opdrachtgever geen kosten zijn verbonden, ongeacht of de verdere onderhandelingen tot het sluiten van een overeenkomst zullen leiden.

3 Richtlijnen offerte

3.1 Gunningscriteria

Beoordeling van de offerte zal geschieden op basis van de volgende aspecten:

1. Aantoonbare ervaring en kennis van de aangeboden medewerker(s) op de relevante gebieden
2. Inhoudelijke kwaliteit van de aanbieding
3. Prijs van de aanbieding

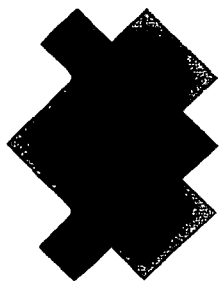
3.3 Kosten

In de offerte worden de kosten van de te leveren producten en diensten door de opdrachtnemer begroot. De kosten worden in Nederlandse valuta uitgedrukt en zijn excl. BTW.

3.4 Beschrijving relevante kennis en ervaring

In uw offerte dient u een beschrijving van de kennis en ervaring van de aangeboden medewerker(s) relevant voor de opdracht op te nemen:

- Overzicht van relevante projecten op het gebied van PKI.
- Overzicht van aanwezige kennis en ervaring op het gebied van PKI.
- Eventuele "derde" opdrachtnemers waarmee wordt samengewerkt (korte beschrijving van kennis en achtergrond van deze opdrachtnemers en welke bijdrage ze leveren aan de aanbieding).



PKI overheid

Offerte-aanvraag

Experimentele PKI voor de taskforce PKI overheid

9 juni 2000

COMMUNICEREN IN VERTRAUWEN IN COMMUNICEREN

PKI overheid

Document geschiedenis

Versie	Datum	Status/reden revisie	Auteur
0.1	17/3/2000	Eerste concept	
0.2	28/3/2000	Algemene delen toegevoegd, relaties met TTP.NL toegevoegd, intern commentaar verwerkt.	
0.3	3/4/2000	Commentaar verwerkt	
0.4	23/5/2000	Verder intern commentaar verwerkt	
1.0	9 juni 2000	Definitieve versie	

PKI overheid

Inhoudsopgave

1. Algemeen

1.1 Doelstellingen

De taskforce PKI overheid is belast met het invoeren van een infrastructuur die betrouwbare en vertrouwelijke elektronische communicatie mogelijk maakt. In de activiteiten is een tweedeling gemaakt: een korte-termijn actielijn gericht op het inrichten van een beperkte PKI in 2000 en een lange-termijn actielijn gericht op het bereiken van een situatie waarbij in 2002 voor vrijwel alle vormen van communicatie en transactie als vanzelfsprekend gebruik zal worden gemaakt van digitale certificaten voor een betrouwbare dienstverlening door middel van de elektronische snelweg.

De doelstelling van de taskforce PKI overheid is: "Het realiseren van een werkbare betrouwbare infrastructuur voor PKI-diensten die voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers".

In het kader van deze doelstelling, werkt de taskforce mee aan experimenten die deel uitmaken van lopende overheidsprojecten en voert in eigen beheer enkele kleinschalige experimenten uit. Hiermee wil de taskforce enerzijds praktijkervaring opdoen met het gebruik van PKI-diensten en anderzijds beschikbare onderdelen van de infrastructuur onderzoeken.

Om deze experimenten te kunnen uitvoeren, dient de taskforce de beschikking te hebben over een operationele PKI die breed inzetbaar is. Ofschoon deze PKI gezien het experimentele karakter geen formele status zal verkrijgen, dient de PKI aan een aantal betrouwbaarheidseisen te voldoen.

Voor de inrichting en de instandhouding van deze experimentele PKI nodigt Opdrachtgever bedrijven uit offerte uit te brengen om de benodigde producten en diensten te leveren.

1.2 Opdrachtformulering

Op basis van de offertes zal de Opdrachtgever een partij selecteren (hierna Opdrachtnemer genoemd) die ten behoeve van de experimentele PKI de volgende diensten zal leveren:

- Inrichten van een PKI en TTP-diensten gericht op het uitgeven en beheren van certificaten
- Technisch beheer van de PKI en TTP-diensten gedurende de periode dat de experimentele PKI operationeel zal zijn
- Ondersteuning bij de inrichting en uitvoering van experimenten

Gezien het karakter dient de gevraagde PKI een breed scala aan proefprojecten en experimenten te kunnen ondersteunen. Zo zullen naar verwachting zowel toepassingen die gebruik maken van smartcards of andere hardware tokens als geheel op sofware gebaseerde toepassingen voorkomen. De registratiefunctie (RA) zal door de taskforce PKI overheid zelf worden uitgevoerd. Daarnaast dient het mogelijk te zijn om extra RA's binnen de verschillende experimenten in te richten.

Dit alles vergt zowel een flexibele PKI infrastructuur als een flexibele houding van de Opdrachtnemer.

1.3 Tijdspad offerte

Ten aanzien van de offerteprocedure zal het volgende tijdspad worden gehanteerd:

Fase	Omschrijving	Einddatum
1	Verzenden offerteaanvraag	16 juni 2000
2	Ontvangst offerte kandidaat Opdrachtnemer bij de Opdrachtgever	30 juni 2000
3	Eventuele mondelinge toelichting door de kandidaat Opdrachtnemer	1e week juli
4	Selectie Opdrachtnemer	2e week juli

1.4 Algemene voorwaarden

De offerte dient conform bovenstaande tijdsplanning, op 30 juni 2000 (uiterlijk 15.00 uur) bij ons in bezit te zijn. De offerte wordt in drievoud verstuurd naar:

Ministerie van Binnenlandse Zaken
T.a.v. [redacted] de heer [redacted]
Postbus 20011
2500 EA Den Haag

Bezoekadres: Herengracht 17-19
Contactpersoon voor inhoudelijke vragen is de heer [redacted].

1.5 Algemene voorwaarden

1.5.1 Afwijkingen offerteaanvraag

Wij verzoeken u uw offerte te laten aansluiten bij onze aanvraag. Afwijkingen op de aanvraag dienen te worden gemotiveerd. Wijzigingen of aanvullingen op onze aanvraag zullen slechts in aanmerking worden genomen voor zover deze van ondergeschikte aard zijn. Niet aangegeven of verklaarde afwijkingen kunnen door ons buiten beschouwing worden gelaten.

1.5.2 Alternatieve voorstellen

Indien u meent door middel van een alternatief minimaal hetzelfde resultaat ten aanzien van de gewenste functies en toepassingsmogelijkheden te kunnen aanbieden dan wordt u verzocht dit in een afzonderlijke bijlage bij uw offerte, te vermelden.

1.5.3 Minimale geldigheidsduur

De offerte zal een minimale geldigheid hebben van 60 dagen na sluitingsdatum. Tijdens die periode heeft zij het karakter van een onherroepelijk aanbod.

1.5.4 Vertrouwelijkheid

Deze offerteaanvraag zal vertrouwelijk worden behandeld en slechts aan medewerkers worden getoond die voor het uitbrengen van de offerte daarvan kennis moeten nemen. Evenmin zal door u op enigerlei wijze aan derden kennis worden gegeven van het feit dat Opdrachtgever een offerte heeft aangevraagd en/of van de gegevens die in dat verband door Opdrachtgever zijn of worden verstrekt.

De vertrouwelijkheid zal ook worden bewaard wanneer de offerte niet tot de totstandkoming van een overeenkomst zal leiden. Hetgeen in bijgevoegde conceptovereenkomst is bepaald omtrent geheimhouding is tevens op de offerteprocedure van toepassing. Opdrachtgever zal de aan haar uitgebrachte offerte niet aan derden beschikbaar stellen.

1.5.5 Samenwerking met partners

Er wordt op gewezen dat deze opdracht niet in afzonderlijke kavels wordt verdeeld en dat men zich alleen voor de gehele opdracht kan aanmelden. De mogelijkheid wordt wel geboden dat meerdere bedrijven zich gezamenlijk voor deze opdracht kunnen aanmelden. Uitgangspunt is dat de offrerende partij als "system integrator" optreedt.

In het geval een samenwerkingsverband zich voor deze opdracht aanmeldt, zal duidelijk moeten zijn aangegeven bij wie de leiding berust en wie daarmee aanspreekpunt is voor BZK.

1.5.6 Kosten offerte

Aan de offerte zullen voor de Opdrachtgever geen kosten zijn verbonden, ongeacht of de verdere onderhandelingen tot het sluiten van een overeenkomst zullen leiden.

2. Details offerteaanvraag

2.1 Uitgangspunten

Uitgangspunt is dat de taskforce PKI overheid zelf de rol van Certification Service Provider (CSP) op zich zal nemen. Logisch gezien is de taskforce dus de CA en RA. De RA functie zal op termijn zowel bij de taskforce zelf als bij de diverse proefprojecten worden belegd.

Ten aanzien van de technische infrastructuur geldt dat de voorkeur wordt gegeven aan maximale outsourcing. Dit betekent dat de voorkeur sterk uitgaat naar aanbiedingen waarbij de technische infrastructuur door de aanbieder gehost wordt (b.v. managed CA of Virtual CA).

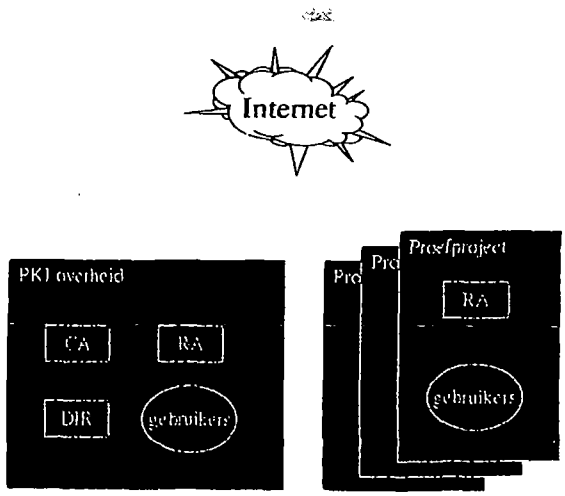
De PKI-diensten dienen optimaal toegankelijk te zijn via het Internet. Dit betreft zowel de toegankelijkheid van de CA/DS diensten vanuit de RA als vanuit de toepassingen van de eindgebruikers (PKI-enabled applicaties).

2.2 Beschrijving van de Infrastructuur

De taskforce PKI overheid zal zelf als CSP optreden. Dit houdt in dat de PKI overheid de functie van CA en RA vervult en zorg draagt voor het beschikbaar stellen van de publieke certificaten via een Directory-dienst. Met deze basis configuratie kunnen de eigen (interne) experimenten worden ondersteund.

PKI overheid treedt daarnaast ook faciliterend op voor externe proefprojecten. De registratiefunctie die hiervoor noodzakelijk is, zal veelal binnen het proefproject zelf worden ingericht. Dit betekent dat het mogelijk moet zijn om flexibel RA's aan de configuratie toe te voegen.

In onderstaande figuur is dit weergegeven.



De verschillende componenten van de PKI dienen via het Internet of een intranet met elkaar op een berouwbare wijze te kunnen communiceren.

2.3 Te leveren producten en diensten

2.3.1 Inrichten van de PKI

Hieronder valt het inrichten van de technische componenten van de PKI alsmede de organisatorische en procedurele componenten voor zoverre die onder de verantwoordelijkheid van Opdrachtnemer vallen (b.v. in geval van outsourcing/hosting).

De volgende diensten vallen hier onder:

- Certificeringsdienst (CA)
  Geschikt voor het creëren van publieke sleutel certificaten voor personen en servers/computers)
- Registratiedienst (RA)
  De technische hulpmiddelen ter ondersteuning van het registratie- en verificatieproces.
- Directory dienst (DS)
  Een adressenlijst ten behoeve van het beschikbaar stellen van publieke sleutel certificaten en aanverwante informatie als CP/CPS.
- Sleutelbeheerdiensten (SB)
  Diensten ten behoeve van het genereren, gebruiken, intrekken en vervangen van sleutelmateriaal voor de CA en (indien van toepassing) de RA en de gebruikers.

2.3.2 Technisch beheer van de PKI gedurende de periode dat de experimentele PKI operationeel zal zijn

Het functioneel en operationeel beheer van de PKI-diensten zal zo veel mogelijk door de Taskforce PKI overheid worden uitgevoerd. De instandhouding van de technische infrastructuur dient door Opdrachtnemer te worden uitgevoerd.
Voor wat betreft hard- en software die door de aanbieder wordt geleverd en bij de taskforce of proefprojecten geïnstalleerd, geldt de eis dat binnen 2 werkdagen na constatering van problemen deze problemen dienen te zijn opgelost.

De experimentele PKI zal minimaal 1 jaar operationeel zijn. Verlenging van de operationele levensduur is echter zeer waarschijnlijk. Hiermee dient in de offerte rekening te worden gehouden.

2.3.3 Ondersteuning bij de inrichting en uitvoering van experimenten

De verwachting is dat nieuwe experimenten zullen leiden tot (beperkte) wijzigingen in de infrastructuur. Bijvoorbeeld het opzetten van een nieuwe RA. Deze wijzigingen dienen adequaat te worden doorgevoerd.

2.4 Eisen en wensen

2.4.1 Algemeen

De taskforce PKI overheid probeert in haar eisen zoveel mogelijk aan te sluiten bij de ontwikkelingen op de Nederlandse en Europese markt. Ten aanzien van de eisen die aan TTP-diensten en dienstverleners kunnen worden gesteld, worden de criteria van het TTP.NL initiatief [TTP.NL1 t/m TTP.NL3] in principe als uitgangspunt genomen.

Voor deze specifieke offerteaanvraag zijn de volgende onderdelen van de TTP.NL criteria van belang:

TTP.NL Part 1, *Requirements and Guidance for the Certification of the Public Key Infrastructure of certification Service Providers*": de onderdelen die in de bijlage zijn aangegeven.

TTP.NL Part 2, *Requirements and Guidance for the Certification of Information Security Management of certification Service Providers*": in zijn geheel.

Gezien het algemene karakter van met name TTP.NL Part 1, is op een aantal punten een nadere specificatie van de eisen geformuleerd. Deze specifieke eisen worden in de volgende paragrafen weergegeven. Daar waar mogelijk is een verwijzing opgenomen naar het relevante TTP.NL criterium.

2.4.2 Certificeringsdiensten en Certificatie Autoriteit (Certification Authority)

Eisen

Weegfactor	Ref.	Eis	Toelichting
10	CA.e1	De CA diensten dienen 24 uur per dag 7 dagen per week beschikbaar te zijn.	Incidentele uitval is acceptabel. Niet-beschikbaarheid t.g.v. problemen met Internet vallen buiten deze eis.
10	CA.e2	De CA dient verschillende Publieke sleutellengtes te kunnen certificeren	De range zal minimaal moeten liggen tussen 512 en 2048 bits.
10	CA.e3	De private sleutel van de CA (signing key)dient goed beveiligd te zijn tegen misbruik.	(CA.w1) Bij voorkeur opslag in tamper proof hardware.
10	CA.e4	De private sleutel van de CA dient goed beveiligd te zijn tegen verlies.	De sleutel dient b.v. in escrow gegeven te worden bij (een) geschikte instantie(s).
10	CA.e5	De omgeving van de CA dient goed beveiligd te zijn.	Dit betreft zowel de techniek als de organisatie van de CA. Aandachtspunten zijn de fysieke, logische en organisatorische maatregelen. Zie TTP.NL part 2.
10	CA.e6	De CA dient een beveiligd communicatiekanaal (vertrouwelijkheid en authenticatie) te bieden met de RAs.	(CA.w2) Dit is bij voorkeur gebaseerd op het gebruik van certificaten.
10	CA.e7	De CA dient de RA te voorzien van statusinformatie over certificaten.	Voorbeelden: - in aanvraag - verificatie accoord - afgewezen aanvraag - verstrekt - ingetrokken (CA.w3) Bij voorkeur alleen statusinformatie over die certificaten die door een specifieke RA zelf zijn aangevraagd.
10	CA.e8	De CA dient de RA de mogelijkheid te bieden zelfstandig certificaten in te trekken.	(CA.w4) Bij voorkeur alleen de mogelijkheid om certificaten in te trekken die door een specifieke RA zelf zijn uitgegeven.

10	CA.e9	De CA dient de lijst met ingetrokken certificaten binnen 24 uur aan te passen en te publiceren indien een certificaat wordt ingetrokken.	(CA.w5) Het verdient de voorkeur indien de lijst direct wordt bijgewerkt (bv. via OCSP).
10	CA.e10	De CA dient over een helpdesk te beschikken die tijdens kantooruren beschikbaar is.	Kantooruren: 08:30-18:00.
10	CA.e11	De CRL dient conform de standaard X.509v2 te zijn.	
10	CA.e12	De sleutellengte van de CA signing key dient minimaal 1024 bits te bedragen.	
10	CA.e13	Het rootcertificaat van de CA dient on-line beschikbaar te zijn voor het downloaden in standaard Microsoft en Netscape cliënt producten.	Zie de lijst met basis cliënt en server applicaties.

Wensen

Weegfactor	Ref.	Wens	Toelichting
2	CA.w1	Bij voorkeur opslag van de CA signing key in tamper proof hardware.	
5	CA.w2	De beveiliging van de communicatie tussen RA en CA is bij voorkeur gebaseerd op het gebruik van certificaten.	
2	CA.w3	Bij voorkeur krijgt een RA alleen statusinformatie over die certificaten die door een specifieke RA zelf zijn aangevraagd.	
2	CA.w4	Bij voorkeur kan een RA alleen die certificaten intrekken die door een specifieke RA zelf zijn uitgegeven.	
2	CA.w5	Het verdient de voorkeur indien de lijst met ingetrokken certificaten (CRL) direct wordt bijgewerkt (bv. via OCSP).	

2.4.3 Registratiediensten en Registratie Autoriteit (Registration Authority)

Eisen

Weegfactor	Ref.	Eis	Toelichting
10	RA.e1	Meerdere RA's dienen te kunnen worden ingericht op verschillende locaties.	
10	RA.e2	De RA dient een beveiligd communicatiekanaal te bieden met de CA.	(RA.w1) Dit is bij voorkeur gebaseerd op het gebruik van certificaten.
10	RA.e3	De RA dient alle functionaliteit te bieden voor het registreren van gebruikers, het aanvragen van certificaten, het	Het beheren van de individuele certificaten vindt plaats door de RA. De rol van de CA daarbij is beperkt tot

		verificatieproces en het uitgeven van certificaten.	het bieden van de geautomatiseerde back-office diensten.
10	RA.e4	Toegang tot de RA functionaliteit dient afgeschermd te zijn voor onbevoegden.	Alleen aangewezen RA-operators mogen toegang verkrijgen. (RA.w2) Toegangsbeveiliging is bij voorkeur gebaseerd op het gebruik van certificaten en tokens.
5	RA.e5	De RA diensten dienen 24 uur per dag 7 dagen per week beschikbaar te zijn.	Incidentele uitval is acceptabel. Niet-beschikbaarheid t.g.v. problemen met Internet vallen buiten deze eis.
10	RA.e6	De RA software dient geschikt te zijn om op een normaal werkstation te worden geïnstalleerd.	Dit betreft een PC met Windows 95/98, eventueel is een NT station acceptabel.
10	RA.e7	De aanvraagprocedure voor certificatie van een publieke sleutel dient er voor te zorgen dat de volgende onderdelen (automatisch) worden gerealiseerd: - beveiligd pad tussen aanvrager en RA (of CA) zodanig dat de integriteit van het aangeleverde materiaal gewaarborgd is - toetsing dat de aanvrager in het bezit is van de bij de te certificeren publieke sleutel behorende private sleutel	Zie b.v. IETF-PKIX RFC 2511

Wensen

Weegfactor	Ref.	Wens	Toelichting
5	RA.w1	Het beveiligde pad tussen RA en CA is bij voorkeur gebaseerd op het gebruik van certificaten.	
2	RA.w2	Toegangsbeveiliging tot de RA is bij voorkeur gebaseerd op het gebruik van certificaten en tokens.	

2.4.4 Directory diensten (DS)

Eisen

Weegfactor	Ref.	Eis	Toelichting
10	D.e1	De DS dient 24 uur per dag 7 dagen per week beschikbaar te zijn.	Incidentele uitval is acceptabel. Niet-beschikbaarheid t.g.v. problemen met Internet vallen buiten deze eis.
10	D.e2	De DS dient voor elke gebruiker via het Internet beschikbaar te zijn.	
10	D.e3	De DS dient zowel de uitgegeven certificaten als de CRL beschikbaar te stellen.	

10	D.e4	De DS dient via LDAP geraadpleegd te kunnen worden.	Dit maakt integratie met de meest voorkomende cliënt software (browsers/e-mail cliënt) mogelijk.
10	D.e5	De DS dient goed beveiligd te zijn tegen ongeautoriseerde wijzigingen.	
10	D.e6	Uitgegeven certificaten en de bijgewerkte CRL dienen binnen 24 uur via de DS te worden gepubliceerd.	Dit betreft de totale tijd tussen uitgifte van een certificaat of aangifte intrekking en het tijdstip waarop het certificaat c.q. de CRL via de DS beschikbaar is.

Wensen

Ref.	Wens	Toelichting

2.4.5 Sleutelbeheerdiensten

Voor de experimenten wordt zowel voorzien in situaties waarbij de private/publieke sleutels door de eindgebruiker zelf (in de applicatie of het token) worden gegenereerd als situaties waarbij het centraal genereren van sleutels wenselijk is. In die gevallen waarbij de sleutels door de gebruikersapplicatie worden gegenereerd, dienen de eisen gezien te worden als een voorwaarde dat de PKI de gestelde eis niet mag blokkeren.

Eisen

Weegfactor	Ref.	Eis	Toelichting
10	SB.e1	Het genereren van publieke/private sleutels voor de gebruikers moet decentraal plaats kunnen vinden.	De gebruikers moeten dus zelf de publieke/private sleutels genereren. (SB.w1) Het is wenselijk dat ook de mogelijkheid bestaat voor centraal genereren van gebruikerssleutels.
10	SB.e2	De volgende algoritmen dienen minimaal te worden ondersteund: - SHA-1/FIPS 180 (hash) - DES/FIPS 46-2 - RSA	Alternatief is de combinatie van RSA (vertrouwelijkheid) en DSA (handtekening). De preferente OIDs zijn: - sha-1WithRsaEncryption - id-dsa-with-sha1 (SB.w2) Het is wenselijk om aparte sleutelparen te hebben voor integriteits/authenticiteitsdiensten en vertrouwelijkheidsdiensten. De Key Usage extentie (zie certificaten) dient dan gebruikt te worden om de functie vast te leggen (zie PKIX RFC 2459) (SB.w3) De mogelijkheid om 3-DES of gelijkwaardig te gebruiken is

wenselijk.

Wensen

Weegfactor	Ref.	Wens	Toelichting
5	SB.w1	Het is wenselijk dat ook de mogelijkheid bestaat voor centraal genereren van gebruikerssleutels.	
5	SB.w2	Het is wenselijk om aparte sleutelparen te hebben voor integriteits/authenticiteitsdiensten en vertrouwelijkheidsdiensten. De Key Usage extentie (zie certificaten) dient dan gebruikt te worden om de functie vast te leggen (zie PKIX RFC 2459)	
2	SB.w3	De mogelijkheid om 3-DES of gelijkwaardig te gebruiken is wenselijk.	

2.4.6 Certificaten

Eisen

Weegfactor	Ref.	Eis	Toelichting
10	C.e1	Certificaten dienen te voldoen aan de standaard X509v3.	
10	C.e2	De volgende typen certificaten dienen te worden ondersteund: - persoonlijke e-mail certificaten conform de S/MIME standaard - persoonlijke certificaten voor gebruik met SSL client-authenticatie - server certificaten voor gebruik met SSL server-authenticatie en encryptie	(C.w1) Ondersteuning van software-signing certificaten is wenselijk (Authenticode/Object signing) (C.w2) Het is wenselijk dat de certificaten zich conformeren aan de profiles als gedefinieerd in PKIX RFC 2459/PKIX ID Qualified Certificates Profile
10	C.e4	De certificaten die worden uitgegeven, dienen minimaal te kunnen worden gebruikt door de meest gebruikte client- en server producten.	Dit betreft m.n. browsers en e-mail clients alsook www- en news servers.
10	C.e5	De geldigheidsduur van certificaten dient per certificaat te kunnen worden gevarieerd.	Eventueel binnen minimale en maximale grenzen.

Wensen

Weegfactor	Ref.	Wens	Toelichting
2	C.w1	Ondersteuning van software-signing certificaten is wenselijk (Authenticode/Object signing)	

2	C.w2	Het is wenselijk dat de certificaten zich conformeren aan de profiles als gedefinieerd in PKIX RFC 2459/PKIX ID Qualified Certificates Profile	
5	C.w3	Het is wenselijk om aparte certificaten uit te kunnen geven voor vertrouwelijkheidsdiensten en authenticatie (digitale handtekening)	Zie ook sleutelbeheer SB.w2.
2	C.w4	De mogelijkheid om attribuutcertificaten te gebruiken is een pre.	
5	C.w5	De mogelijkheid om de inhoud van certificaten per RA te variëren is een pre.	De RA functie zal per experiment bij een organisatie/project belegd worden. Het is wenselijk dat in het uitgegeven certificaat de naam van de RA wordt opgenomen. Ook kan per experiment de behoefte bestaan om eigen velden te definiëren of in te vullen.
5	C.w6	Het gebruik van extensies als gedefinieerd in PKIX RFC 2459 is wenselijk.	Met name: - Certificate Policies extention - Key Usage extention

2.4.7 Tokens

Het (kleinschalig) gebruik van hardware tokens zal onderdeel uitmaken van de experimenten. Hiervoor is het noodzakelijk dat de PKI geschikt is voor het toepassen van tokens.
Het life-cycle beheer van de tokens (pre-personalisatie e.d.) staat daarbij vooralsnog niet centraal.

Eisen

Weegfactor	**Ref.**	**Eis**	**Toelichting**
10	T.e1	Het moet mogelijk zijn om gebruikerscertificaten op hardware tokens op te slaan.	Naast smartcards kunnen ook andere tokens in aanmerking komen.
10	T.e2	Tokens en eventuele benodigde randapparatuur dienen samen te werken met de beveiligingsmogelijkheden van de meest voorkomende (browser/e-mail) cliënt producten.	Zie de lijst met basis client applicaties. Relevante standaarden zijn: - PKCS#11 - Microsoft CAPI - PKCS#15 (opslag certificaten op token)
10	T.e2	Tokens dienen naast de beveiligde opslag ook te voorzien in functionaliteit voor het genereren van publieke/private sleutels.	De private sleutel mag niet buiten het token bestaan.
10	T.e3	Het genereren van de digitale handtekening dient op het token plaats te vinden.	De private sleutel mag niet buiten het token bestaan.

Wensen

Ref.	Wens	Toelichting

2.4.8 Interfaces

Naast de reeds in de vorige secties genoemde eisen aan interfaces, dient de aanbieding te voldoen aan de volgende eisen ten aanzien van interfaces.

Interface DS-secure servers

Secure servers, bijvoorbeeld op SSL gebaseerde www- mail- en news-servers, dienen ten behoeve van client-authenticatie te beschikken over een interface voor het importeren van gebruikerscertificaten in een autorisatie- of toegangscontroledatabase. Hiervoor worden vaak specifieke eisen gesteld aan het formaat van de certificaten (PEM/BER).

Weegfactor	Ref.	Eis	Toelichting
10	I.e1	Een interface dient voorhanden te zijn voor het (eenvoudig) kunnen importeren van gebruikerscertificaten vanuit de Directory Server in secure servers.	Minimaal dient dit interface er te zijn voor de meest gebruikte www-servers.

2.4.9 Bewijs- en Bewaardiensten (Proof and Preservation Services)

Met de Bewijs- en Bewaardienst wordt een onafhankelijke TTP-dienst bedoeld die een handeling en het tijdstip van die handeling, bijvoorbeeld het verzenden en ophalen van e-mail berichten, onweerlegbaar vastlegt.

De Opdrachtnemer dient aan te geven (of en) hoe deze dienst kan worden ingericht en dient een indicatie te geven van de kosten. Deze dienst kan ook via een derde partij worden verleend. In dat geval dient te worden aangegeven welke partij deze dienst kan leveren, tegen welke kosten (indicatief) en er zorg voor te dragen dat de aangeboden PKI gebruikt kan worden met de externe aanbieder van de Bewijs en Bewaardiensten.

3. Richtlijnen offerte

3.1 Gunningscriteria

Beoordeling van de offerte zal geschieden op basis van de volgende aspecten:

1. De mate waarin voldaan wordt aan de gestelde eisen en wensen in paragraaf 2.4. Gezien het experimentele kader en de in ontwikkeling zijnde markt wordt niet vereist dat aan alle in paragraaf 2.4 gestelde eisen wordt voldaan maar wordt een gewogen score bepaald.
    a. Hiertoe dient u per eis en wens aan te geven of de offerte: voldoet (waarde=1)/niet voldoet (waarde=0)(binaire keuze)
    b. In combinatie van de bij de eisen en wensen aangegeven wegingsfactoren zal een totaalscore worden bepaald bestaande uit de som van de individuele scores waarbij de score = waarde*weegfactor/200.
2. Inhoudelijke kwaliteit van de aanbieding
    a. De kwaliteit zal onafhankelijk door 3 personen worden beoordeeld die een score tussen 0 en 100 zullen toekennen waarna de gemiddelde score wordt bepaald. Aspecten die worden beoordeeld, zijn:
        i. Of de combinatie van eisen waaraan voldaan wordt een bruikbare oplossing biedt
        ii. Kwaliteit van het plan van aanpak (o.a. controleerbaarheid, beheersbaarheid, transparantie)
        iii. Aantoonbare ervaring en kennis op de relevante gebieden en de innovatiekracht van de onderneming
        iv. Flexibiliteit van de aangeboden oplossing en de aangeboden ondersteuning
        v. Volledigheid van de offerte
        vi. Het tijdsbestek waarbinnen de PKI wordt opgeleverd
3. Prijs van de aanbieding
    a. Hier aan wordt een score toegekend volgens de formule: 100*(laagste prijs)/(prijs te beoordelen offerte)

De totale score is de som van de scores behaald bij onderdeel 1,2 en 3.

De taskforce PKI overheid houdt zich het recht voor om geen of meerdere offertes te honoreren.

Eisen, wensen en weegfactoren die voor deze offerteaanvraag zijn gehanteerd, zijn niet maatgevend voor eventuele vervolgofferteaanvragen van de taskforce PKI overheid.

3.2 Beschrijving voorstel infrastructuur

De offerte bevat een beschrijving van de door de Opdrachtnemer voorgestelde infrastructuur, met daarin:

- Voorstel voor de functionele en technische infrastructuur.
- Overzicht van de onderdelen van de voorgestelde infrastructuur
- Onderbouwing van de gekozen standaarden

3.3 Beschrijving diensten

De offerte bevat een beschrijving van de (beheer-)diensten die door de Opdrachtnemer worden geleverd, met daarin:

- Beschrijving van de te leveren diensten door Opdrachtnemer, activiteiten, verantwoordelijkheden en benodigde capaciteit.
- Beschrijving van de taken en verantwoordelijkheden die bij de Opdrachtnemer liggen.

3.4 Eisen en wensen

Voor elke in paragraaf 2.3 aangegeven eis en wens dient te worden aangegeven of het voorstel daaraan voldoet (alleen ja/nee aangeven). Daarbij dient verwezen te worden naar de in de tabellen aangegeven referenties. Tevens dient (kort) te worden aangegeven op welke wijze aan de eis of wens wordt voldaan.
Indien niet wordt voldaan aan een eis, dient de reden duidelijk aangegeven te worden. Zo mogelijk dient beschreven te worden op welke alternatieve wijze aan de eis invulling gegeven kan worden. De antwoorden worden gebruikt binnen gunningscriterium 3.1 onderdeel 1.

Tevens wordt gevraagd om in de bijgevoegde lijst met TTP.NL criteria (annex A) aan te geven aan welk criteria de aangeboden PKI voldoet. Indien aan een criterium niet wordt voldaan, dient u aan te geven of dit in de toekomst wel het geval zal zijn of anders waarom u niet aan dit criterium zult voldoen. Deze lijst zal meewegen in de beoordeling van de inhoudelijke kwaliteit va de aanbieding (3.1 onderdeel 2).

3.5 Plan van aanpak

In de offerte moet een plan van aanpak worden opgenomen dat een tijd- en activiteitenplanning bevat. De planning moet zodanig zijn dat de taskforce eind juli 2000 over de experimentele PKI kan beschikken.

Gelet op het speciale karakter van het project (geringe ervaring met toegepaste technologieën), wordt in het plan van aanpak expliciet aandacht besteed aan:

- De wijze waarop ervaringen en kennis opgedaan tijdens de pilot wordt gedeeld met de Opdrachtgever (denk aan documentatie, participatie Opdrachtgever in overleg)
- Beschrijving van witte vlekken en onzekerheden in het ontwerp van de Opdrachtnemer (van architectuur en organisatie) en een analyse van de risico's (technisch, organisatorisch en de maatregelen).
- Voorstel voor de wijze waarop de Opdrachtnemer zijn projectorganisatie inricht.
- Gedetailleerde beschrijving van het tijdspad waarin wordt aangegeven op welk moment welke (deel-)producten en diensten worden opgeleverd en hoe het testen en de acceptatie daarvan plaats zal vinden.
- In uw plan van aanpak dient er aandacht te worden besteed aan de communicatie met de Opdrachtgever.
- Er zal minimaal wekelijks overleg zijn tussen de projectleider van de Opdrachtnemer en de coördinator van de Opdrachtgever. Ter voorbereiding van dit overleg stelt de Opdrachtnemer een voortgangsrapportage op. Daarin wordt aandacht besteed aan de volgende onderwerpen:
  - Realisatie van de afgesproken producten en diensten
  - Realisatie van het afgesproken budget
  - Risico's voor het vervolgtraject

Deze aspecten zullen meewegen in de beoordeling van de inhoudelijke kwaliteit va de aanbieding (3.1 onderdeel 2).

3.6 Kosten

In de offerte worden de kosten van de te leveren producten en diensten door de Opdrachtnemer begroot. Daarbij zijn de volgende uitgangspunten gehanteerd:

- De kostenposten moeten duidelijk zijn gedefinieerd (zodat het de Opdrachtgever duidelijk is welke kostensoorten onder een kostenpost vallen).
- Bij de calculatie van de kosten wordt rekening gehouden met een scenario van 250 tot en met 5000 gebruikers.
- Naast de totale kosten per kostenpost, worden ook de kosten per eenheid aangegeven (rekening houdend met onderstaande tabel).
- De kosten worden in Nederlandse valuta uitgedrukt en zijn excl. BTW.

Bij het opstellen van de begroting wordt door de Opdrachtnemer in ieder geval de kostenposten opgenomen die in onderstaande tabel gegeven zijn. Indien bepaalde kosten niet van toepassing zijn, dient dat te worden aangegeven. Zijn er kosten die niet onder een bepaalde categorie vallen, dan dienen deze apart te worden gespecificeerd.

Produkten/Diensten	**Kostenspecificatie**	**Opmerking**
Certificatie Autoriteit	1. Kosten voor de installatie/inrichting (uurtarief/capaciteit) 2. Service-/abonnementskosten per tijdseenheid 3. Kosten per gebruik	
Registratie Autoriteit	4. Aanschafkosten voor software en/of hardware per RA werkstation. 5. Kosten voor de installatie (uurtarief/capaciteit)	
Directory Dienst	6. Aanschafkosten voor software en/of hardware per RA werkstation. 7. Aanschafkosten voor software en/of hardware per RA werkstation.	Deze post hoeft niet te worden opgenomen indien ze integraal is opgenomen bij de vergoeding voor de TTP diensten
Sleutel Beheer	8. Kosten voor de installatie/inrichting (uurtarief/capaciteit) 9. Service-/abonnementskosten per tijdseenheid of per gebruik.	PKCS#11, indien deze software wordt verrekend in het tarief van de TTP diensten dan hoeft deze post niet te worden opgenomen.

Beheer PKI infrastructuur	10. Kosten per gebruiker 11. Uurtarief per medewerker (kosten per beheermedewerker)	Inclusief een inschatting van de benodigde capaciteit

De optionele onderdelen zullen in eerste instantie niet worden aangeschaft. De op te geven kosten zijn dan ook bedoeld als indicatie.

Optionele onderdelen		
Token	1. Kosten per token 2. Kosten voor beheersysteem	Inclusief eventueel benodigde tokenlezers e.d.
Bewijs en Bewaardienst	3. Kosten voor de installatie/inrichting (uurtarief/capaciteit) 4. Service-/abonnementskosten per tijdseenheid 5. Kosten per gebruik	

Deze lijst zal meewegen in de beoordeling van de kosten va de aanbieding (3.1 onderdeel 3)

3.7 Beschrijving relevante kennis en ervaring

In uw offerte dient u een beschrijving van de kennis en ervaring van de Opdrachtnemer(s) relevant voor de opdracht op te nemen:

- *Eventuele "derde" Opdrachtnemers waarmee wordt samengewerkt (korte beschrijving* van kennis en achtergrond van deze Opdrachtnemers en welke bijdrage ze leveren aan de aanbieding).
- Overzicht van relevante projecten op het gebied van PKI.
- Overzicht van aanwezige kennis en ervaring op het gebied van PKI.

Deze lijst zal meewegen in de beoordeling van de inhoudelijke kwaliteit van de aanbieding (3.1 onderdeel 2)

3.8 Investering van de Opdrachtnemer

De technologieën waarmee in de pilot ervaring wordt opgedaan zijn nieuw en leveren de Opdrachtnemer ook een toegevoegde waarde. U dient in uw offerte aan te geven in welke mate u bereid bent als Opdrachtnemer mede te investeren in deze pilot. U dient aan te geven waar uw bijdrage uit bestaat en onder welke voorwaarden.

Dit onderdeel zal meewegen in de beoordeling van de inhoudelijke kwaliteit va de aanbieding (3.1 onderdeel 2)

Bijlage A1

Kruisverwijzing: eisen tussen experimentele PKI en criteria TTP.NL part 1

Bijlage A.1

Kruisverwijzing tussen de eisen die worden gesteld aan de experimentele PKI en de criteria opgesteld door TTP.NL in part 1" *Requirements and Guidance for the Certification of the Public Key Infrastructure of certification Service Providers".*

De eerste kolom geeft de titel van de control aan. In de tweede kolom wordt met een kruis aangegeven of het specifieke control relevant is voor de door Opdrachtnemer te leveren diensten. De derde kolom geeft een nadere afbakening en een verwijzing naar de eisen en wensen als vastgesteld in de offerteaanvraag.

U dient per control die gemerkt is met een kruis in de kolom 'Opdrachtnemer' aan te geven of u daaraan meent te voldoen. Indien u meent er niet aan te voldoen, dient u een motivatie te geven.

Control uit sectie III van TTP.NL Part 1	**Opdrachtnemer**	**Opmerking**
1.1 Overview		
1.2 Identification	X	Voor zover betrekking op de geleverde diensten.
1.3 Community and Applicability		
1.3.1 Certification authorities		
1.3.2 Registration authorities		
1.3.3 End entities	X	C.e2, C.w1
1.3.4 Applicability	X	C.e1, C.e4, C.w2, C.w3, C.w4
1.4 Contact Details	X	Voor zover betrekking op de geleverde diensten.
1.4.1 Specification administration organization	X	Idem
1.4.2 Contact person	X	Idem
1.4.3 Person determining CPS suitability for the policy		
2. GENERAL PROVISIONS		
2.1 Obligations		
2.1.1 CA obligations	X	Voor zover betrekking op de geleverde diensten.

Control uit sectie III van TTP.NL Part 1	Opdrachtnemer	Opmerking
		CA.e1, CA.e3, CA.e4, CA.e5, CA.e9, CA.e11
2.1.2 RA obligations	X	Voor zover betrekking op de geleverde diensten. RA.e5
2.1.3 Subscriber obligations		
2.1.4 Relying party obligations		
2.1.5 Repository obligations		
2.2 Liability		Voor de experimentele PKI zal geen aansprakelijkheid worden geaccepteerd. De opdrachtnemer is wel aansprakelijk onder de contractvoorwaarden.
2.2.1 CA liability		Idem
2.2.2 RA liability		Idem
2.3 Financial responsibility		Voor de experimentele PKI zal geen aansprakelijkheid worden geaccepteerd.
2.4 Interpretation and Enforcement		
2.4.1 Governing law		
2.4.2 Severability, survival, merger, notice		
2.4.3 Dispute resolution procedures		
2.5 Fees		
2.5.1 Certificate issuance or renewal fees	X	
2.5.2 Certificate access fees	X	
2.5.3 Revocation or status information access fees		
2.5.4 Fees for other services such as policy information		
2.5.5 Refund policy		

Control uit sectie III van TTP.NL Part 1	Opdrachtnemer	Opmerking
2.6 Publication and Repository		
2.6.1 Publication of CSP information	X	Randvoorwaarden t.a.v. de mogelijkheden om informatie te publiceren Minimaal CRL en certificaten. Mogelijk ook CP/CPS. D.e1, D.e3, D.e6
2.6.2 Frequency of publication	X	Ca.e9 Ca.w5
2.6.3 Access controls	X	D.e5
2.6.4 Repositories	X	D.e1, D.e2, D.e3, D.e4, D.e6
2.7 Compliance audit	X	Voor zover het die delen betreft die door de Opdrachtnemer worden geleverd (b.v. CA back-office processen).
2.7.1 Frequency of entity compliance audit	X	Onderdeel uitgewerkt in TTP.NL part 2.
2.7.2 Identity/qualifications of auditor	X	Onderdeel uitgewerkt in TTP.NL part 2.
2.7.3 Auditor's relationship to audited party	X	Onderdeel uitgewerkt in TTP.NL part 2.
2.7.4 Topics covered by audit	X	Onderdeel uitgewerkt in TTP.NL part 2.
2.7.5 Actions taken as a result of deficiency	X	Onderdeel uitgewerkt in TTP.NL part 2.
2.7.6 Communication of results	X	Onderdeel uitgewerkt in TTP.NL part 2.
2.8 Confidentiality	X	Voor zover het die delen betreft die door de Opdrachtnemer worden geleverd (b.v. CA back-office processen).
	X	Idem
2.8.1 Types of information to be kept confidential	X	Idem
2.8.2 Types of information not considered confidential	X	Idem
2.8.3 Disclosure of certificate revocation/suspension information	X	Idem
2.8.4 Release to law enforcement officials	X	Idem
2.8.5 Release as part of civil discovery	X	Idem
2.8.6 Disclosure upon owner's request	X	Idem
2.8.7 Other information release circumstances	X	Idem

Control uit sectie III van TTP.NL Part 1	Opdrachtnemer	Opmerking
2.9 Intellectual Property Rights	X	Voor zover het die delen betreft die door de Opdrachtnemer worden geleverd (b.v. CA back-office processen).
3. IDENTIFICATION AND AUTHENTICATION (34)		
3.1 Initial Registration	X	Randvoorwaarden aangeven. C.e1, C.e2, C.w1, C.w2, C.w5, C.w6
3.1.1 Types of names	X	Idem
3.1.2 Need for names to be meaningful	X	Idem
3.1.3 Rules for interpreting various name forms	X	Idem
3.1.4 Uniqueness of names	X	Idem
3.1.5 Name claim dispute resolution procedure		
3.1.6 Recognition, authentication and role of trademarks		
3.1.7 Method to prove possession of private key	X	Ondersteunende technieken aangeven.
3.1.8 Authentication of organization identity		
3.1.9 Authentication of individual identity		
3.2 Routine Rekey	X	Voor CA en RA rekey de voorwaarden en procedure aangeven. Voor de (end) entity beperkt tot de eventuele technische aspecten.
3.3 Rekey after Revocation	X	Idem
3.4 Revocation Request	X	Voor CA en RA beschrijven. CA.e8 CA.w4
4. OPERATIONAL REQUIREMENTS (34)		
4.1 Certificate Application		

Control uit sectie III van TTP.NL Part 1	Opdrachtnemer	Opmerking
4.2 Certificate Issuance		
4.3 Certificate Acceptance		
4.4 Certificate Suspension and Revocation	X	Mogelijkheden en randvoorwaarden aangeven m.n. ten aanzien van CA en RA certificaten. Suspensie behoeft niet te worden ondersteund.
4.4.1 Circumstances for revocation	X	Idem
4.4.2 Who can request revocation	X	Idem
4.4.3 Procedure for revocation request	X	Idem
4.4.4 Revocation request grace period	X	Idem
4.4.5 Circumstances for suspension	X	Idem
4.4.6 Who can request suspension	X	Idem
4.4.7 Procedure for suspension request	X	Idem
4.4.8 Limits on suspension period	X	Idem
4.4.9 CRL issuance frequency (if applicable)	X	De organisatorische en technische randvoorwaarden aangeven. CA.e9, D.e6, CA.w5
4.4.10 CRL checking requirements	X	De technische randvoorwaarden. D.e2, D.e4,
4.4.11 On-line revocation/status checking availability	X	De technische randvoorwaarden. CA.w5
4.4.12 On-line revocation checking requirements	X	De technische randvoorwaarden. CA.w5
4.4.13 Other forms of revocation advertisements available	X	Beschrijven.
4.4.14 Checking requirements for other forms of revocation advertisements	X	Beschrijven.
4.4.15 Special requirements re key compromise		
4.5 Security Audit Procedures	-	Onderdeel van TTP.NL part 2
4.6 Records Archival	-	Onderdeel van TTP.NL part 2

Control uit sectie III van TTP.NL Part 1	Opdrachtnemer	Opmerking
4.7 Key changeover	X	De organisatorische en technische randvoorwaarden aangeven.
4.8 Compromise and Disaster Recovery	X	voor zover het die delen betreft die door de Opdrachtnemer worden geleverd (b.v. CA back-office). Dit is in TTP.NL part 2 opgenomen.
4.9 CA Termination	X	Voor zover het die delen betreft die door de Opdrachtnemer worden geleverd (b.v. CA back-office).
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS (34)	-	Uitgewerkt in TTP.NL part 2.
5.1 Physical Controls	-	Idem
5.2 Procedural Controls	-	Idem
5.3 Personnel Controls	-	Idem
6. TECHNICAL SECURITY CONTROLS (34)	X	Met name voor zover het die delen betreft die door de Opdrachtnemer worden geleverd (b.v. CA back-office).
6.1 Key Pair Generation and Installation		
6.1.1 Key pair generation	X	Met name de sleutels voor de CA en RA componenten. SB.e1, SB.w3
6.1.2 Private key delivery to entity	X	Beschrijven voor het geval waarbij de private sleutels centraal worden gegenereerd door de CSP.
6.1.3 Public key delivery to certificate issuer	X	Voor alle componenten van belang. RA.e7
6.1.4 CA public key delivery to users	X	Beschrijven.
6.1.5 Key sizes	X	CA.e2, CA.e12, SB.e2, SBw2, SB.w3
6.1.6 Public key parameters generation	X	Met name de sleutels voor de CA en RA componenten en voor het geval waarbij de private sleutels centraal worden gegenereerd door de CSP.
6.1.7 Parameter quality checking	X	Idem. RA.e7

Control uit sectie III van TTP.NL Part 1	Opdrachtnemer	Opmerking
6.1.8 Hardware/software key generation	X	Alleen voor de CA en RA sleutels.
6.1.9 Key usage purposes (as per X.509 v3 key usage field)	X	SB.e2, SB.w2, C.e2, C.w1, C.w2, C.w6
6.2 Private Key Protection		
6.2.1 Standards for cryptographic module	X	Alleen voor de CA en RA sleutels. CA.e3, CA.w1,
6.2.2 Private key (n out of m) multi-person control	X	Idem
6.2.3 Private key escrow	X	Idem
6.2.4 Private key backup	X	Idem
6.2.5 Private key archival	X	Idem
6.2.6 Private key entry into cryptographic module	X	Idem
6.2.7 Method of activating private key	X	Idem
6.2.8 Method of deactivating private key	X	Idem
6.2.9 Method of destroying private key	X	Idem
6.3 Other Aspects of Key Pair Management		
6.3.1 Public key archival	X	Alleen voor de CA en RA sleutels.
6.3.2 Usage periods for the public and private keys	X	C.e5
6.4 Activation Data	X	Alleen voor de CA en RA sleutels en voor het geval waarbij de private sleutels centraal worden gegenereerd door de CSP.
6.4.1 Activation data generation and installation	X	Idem
6.4.2 Activation data protection	X	Idem
6.4.3 Other aspects of activation data	X	Idem
6.5 Computer Security Controls	-	Opgenomen in TTP.NL part 2
6.5.1 Specific computer security technical requirements	-	Idem
6.5.2 Computer security rating	-	Idem
6.6 Life Cycle Technical Controls	-	Opgenomen in TTP.NL part 2
6.6.1 System development controls	-	Idem

Control uit sectie III van TTP.NL Part 1	Opdrachtnemer	Opmerking
6.6.2 Security management controls		Idem
6.6.3 Life cycle security ratings	-	Iderm
6.7 Network Security Controls	-	Opgenomen in TTP.NL part 2
6.8 Cryptographic Module Engineering Controls	X	Voor CA module.
7. CERTIFICATE AND CRL PROFILES		
7.1 Certificate Profile	X	Beschrijven. C.e1, C.e2, C.e4, C.w2, C.w3, C.w5, C.w6
7.2 CRL Profile	X	Beschrijven. CA.e11
8. SPECIFICATION ADMINISTRATION	-	Voor die delen die door Opdrachtnemer worden geleverd. Zie TTP.NL part 3, "General requirements voor CSPs".

| PKI overheid |

Bijlage A2

Kruisverwijzing: eisen tussen experimentele PKI en criteria TTP.NL part 2

Bijlage A.2

Kruisverwijzing tussen de eisen die worden gesteld aan de experimentele PKI en de criteria opgesteld door TTP.NL in part 2", *Requirements and Guidance for the Certification of Information Security Management of certification Service Providers"".*

De tweede kolom geeft de titel van de control aan. In de derde kolom dient u met 'Ja' of 'nee' aan te geven of u daaraan meent te voldoen. Indien u meent er niet aan te voldoen, dient u een motivatie te geven.

Ref.	Control	Voldaan j/n	Opmerking
3	**SECURITY POLICY**		
3.1	Information security policy		
3.1.1	Information security policy document		
3.1.2	Review and evaluation		
4	**SECURITY ORGANIZATION**		
4.1	Information security infrastructure		
4.1.1	Management information security forum		
4.1.2	Information security co-ordination		
4.1.3	Allocation of information security responsibilities		
4.1.4	Authorization process for IT facilities		
4.1.5	Independent review of information security		
4.2	Security of third party access		
4.2.1	Procedures to control third party access		
4.2.2	Identification of risks from third party connections		
4.2.3	Security conditions in third party contracts		
4.3	Outsourcing		
4.3.1	Contracts		
5	**ASSETS CLASSIFICATION AND CONTROL**		
5.1	Accountability for assets		
5.1.1	Accountability for assets		
5.2	Information classification		
5.2.1	Classification guidelines		

Ref.	Control	Voldaan j/n	Opmerking
5.2.2	Classification labeling		
6	**PERSONNEL SECURITY**		
6.1	Security in job definition and resourcing		
6.1.1	Security in job responsibilities		
6.1.2	Personnel screening		
6.1.3	*Confidentiality agreements*		
6.2	User training		
6.2.1	Information security education and training		
6.3	Responding to incidents		
6.3.1	Reporting of security incidents		
6.3.2	Reporting of security weaknesses		
6.3.3	Reporting of software malfunctions		
6.3.4	Incident analysis		
6.3.5	Disciplinary process		
7	**PHYSICAL AND ENVIRONMENTAL SECURITY**		
7.1	Secure areas		
7.1.1	Physical security perimeter		
7.1.2	Physical entry controls		
7.1.3	Securing offices, rooms and facilities		
7.1.4	Working in secure areas		
7.2	Equipment security		
7.2.1	Equipment siting and protection		
7.2.2	Power supplies		
7.2.3	Cabling security		
7.2.4	Equipment's maintenance		
7.2.5	Security of equipment off-premises		
7.2.6	Security disposal of equipment		
7.3	General controls		
7.3.1	Clear desk policy		
7.3.2	Removal of property		

Ref.	Control	Voldaan j/n	Opmerking
8	**COMPUTER AND NETWORK MANAGEMENT**		
8.1	Operational procedures and responsibilities		
8.1.1	Documented operating procedures		
8.1.2	Change control		
8.1.3	Incident management procedures		
8.1.4	Segregation of duties		
8.1.5	Separation of development and operational facilities		
8.1.6	External facilities management		
8.2	System planning and acceptance		
8.2.1	Capacity planning		
8.2.2	System acceptance		
8.3	Protection from malicious software		
8.3.1	Virus controls		
8.4	Housekeeping		
8.4.1	Information back-up		
8.4.2	Operator logs		
8.4.3	Fault logging		
8.5	Network management		
8.5.1	Network controls		
8.6	Media handling and security		
8.6.1	Management of removable computer media		
8.6.2	Disposal of media		
8.6.3	Information handling procedures		
8.6.4	Security of system documentation		
8.7	Exchanges of information and software		
8.7.1	Information and software exchange agreements		
8.7.2	Secure of media in transit		
8.7.3	Electronic commerce security		
8.7.4	Security of electronic mail		
8.7.5	Security of electronic office systems		

Ref.	Control	Voldaan j/n	Opmerking
8.7.6	Publicly available systems		
9	**ACCESS CONTROL**		
9.1	Business requirement for system access		
9.1.1	Access control policy		
9.2	User access management		
9.2.1	User registration		
9.2.2	Privilege management		
9.2.3	User password management		
9.2.4	Review of user access rights		
9.3	User responsibilities		
9.3.1	Password use		
9.3.2	Unattended user equipment		
9.4	Network access control		
9.4.1	Policy on use of network services		
9.4.2	Enforced path		
9.4.3	User authentication for external connections		
9.4.4	Node authentication		
9.4.5	Remote diagnostic port protection		
9.4.6	Segregation in networks		
9.4.7	Network connection control		
9.4.8	Network routing control		
9.4.9	Security of network services		
9.5	Operating system access control		
9.5.1	Automatic terminal identification		
9.5.2	Terminal log-on procedures		
9.5.3	User identifiers		
9.5.4	Password management system		
9.5.5	Use of system utilities		
9.5.6	Duress passwords to safeguard users		
9.5.7	Terminal time-out		

Ref.	Control	Voldaan j/n	Opmerking
9.5.8	Limitation of connection time		
9.6	Application access control		
9.6.1	Information access restriction		
9.6.2	Sensitive system isolation		
9.7	Monitoring system access and use		
9.7.1	Event logging		
9.7.2	Monitoring system use		
9.7.3	Clock synchronization		
9.8	Mobile computing and teleworking		
9.8.1	Mobile computing		
9.8.2	Teleworking		
10	**SYSTEMS DEVELOPMENT AND MAINTENANCE**		
10.1	Security requirement of systems		
10.1.1	Security requirements analysis and specification		
10.2	Security in application systems		
10.2.1	Input data validation		
10.2.2	Control of internal processing		
10.2.3	Message authentication		
10.2.4	Output data validation		
10.3	Cryptographic controls		
10.4	Security of system files		
10.4.1	Control of operational software		
10.4.2	Protection of system test data		
10.4.3	Access control to program source libraries		
10.5	Security in development and support environments		
10.5.1	Change control procedures		
10.5.2	Technical review of operating system changes		
10.5.3	Restrictions on changes to software packages		
10.5.4	Covert channels and Trojan code		
10.5.5	Outsourced software development		

Ref.	Control	Voldaan j/n	Opmerking
11	**BUSINESS CONTINUITY PLANNING**		
11.1	Aspects of business continuity planning		
11.1.1	Business continuity management process		
11.1.2	Business continuity and impact analysis		
11.1.3	Writing and implementing continuity plans		
11.1.4	Business continuity planning framework		
11.1.5	Testing, maintaining and re-assessing business continuity plans		
12	**COMPLIANCE**		
12.1	Compliance with legal requirements		
12.1.1	Identification of applicable legislation		
12.1.2	Intellectual property rights (IPR)		
12.1.3	Safeguarding of organizational records		
12.1.4	Data protection and privacy of personal information		
12.1.5	Prevention of misuse of IT facilities		
12.2	Nvt		
12.3	Reviews of security policy and technical compliance		
12.3.1	Compliance with the security policy		
12.3.2	Technical compliance checking		
12.4	System audit considerations		
12.4.1	System audit considerations		
12.4.2	Protection of system audit tools		

TTP.NL Part 1

REQUIREMENTS and GUIDANCE

for the Certification of

the PUBLIC KEY INFRASTRUCTURE

of Certification Service Providers

Introduction

The text and structure in this document is drawn from the original text of RFC 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (March 1999). Text from SEIS – S10 98/98, (Draft) ABA PKI Evaluation Guidelines and (Draft) ANSI Standard ABA X9.79-199x is taken to formulate recommendations for best practice in support of the requirements of the RFC 2527 specification.
These texts have been amended to suit activities of Certification Service Providers providing services for e-commerce such as issuing qualified certificates for advanced electronic signatures. The alterations in the original text and the new text for the guidance were developed by the Workgroups ACT & Criteria of the TTP.NL project in the Netherlands.

The source of the texts can be identified by the use of different fonts:

- Text of RFC 2527 – with alterations to make it applicable in the field of Certification Service Providers.
  TTP.NL acknowledges The Internet Society's ownership of this material and will revise this document in the event that a new version of the material is published.
- Guidance on the application of the requirements for CSPs is drawn from among other above mentioned sources is written in small font.. TTP.NL is owner of this material and will revise this document when necessary.

The term "shall" is used throughout this document to indicate those provisions which, reflecting the requirements that are mandatory. The term "should" is used to indicate those provisions which, although they constitute guidance for the application of the requirements, are expected to be adopted by a Certification Service Provider. Any variation from the guidance by a Certification Service Provider shall be an exception. Such variations will only be permitted on a case by case basis after the Certification Service Provider has demonstrated to the certification body that the exception meets the relevant requirements clause of the requirements and the intent of the guidance in some equivalent way.

The term 'no stipulation' indicates that the CSP is free to specify how it addressess the item concerned.

II GENERAL

II.1 Scope

This document specifies requirements that a Certification Service Provider shall meet in establishing, implementing and documenting its Public Key Infrastructure.
The specification is based on relevant parts of the (Draft) Scheme for Certification and Accreditation of Certification Service Providers for electronic commerce and communication.
The structure of the section on Detailed Controls is taken from IETF PKIX-4.
SEIS – S10 98/98, (Draft) ABA PKI Evaluation Guidelines and (Draft) ANSI Standard ABA X9.79-199x provide recommendations for best practice in support of the requirements of this specification.
The applicability of the controls was checked in trial certification audits at a number of Certification Service Providers in the Netherlands.

III PUBLIC KEY INFRASTRUCTURE

III.1 General

The Certification Service Provider shall establish and maintain a public key infrastructure. This PKI shall address the identification of Certificate Policy and/or Certification Practice Statement, general provisions in terms of certain legal and business issues involved, the organization's approach to risk management, the degree of assurance required, the selection of control objectives and controls for certification and key management.

III.2 Establishing a public key infrastructure

The following steps shall be undertaken to identify and document the control objectives and controls:

a the CSP shall define a policy addressing its operation, in terms of its CP and CPS;
b the CSP shall define the community and applicability of the public key infrastructure, in terms of the characteristics of the organization, its subscribers and relying parties, and its applications;
c the CSP shall undertake a risk analysis. It shall identify treats to assets, vulnerabilities and impacts on the CSP and shall determine the degree of risk;
d the CSP shall define its legal and business requirements, based on the organizations policy, including legal requirements (concerning data protection), and the level of assurance required;
e the CSP shall select control objectives and controls for its certification processes and its key management processes and technical devices from section 3 for implementation by the CSP. The selection shall be justified;
f the CSP shall compile a Statement of Applicability. This statement shall also record the exclusion of any controls listed in section 3.

III.3 Implementation

The selected control objectives and controls shall be effectively implemented. This shall be verified by reviews.

III.4 Documentation

The documentation shall consist of the following information:

a evidence of the actions undertaken as specified in 2.2;
b a summary of the public key infrastructure, including the organizations policy , the level of assurance, the control objectives and implemented controls, given in the Statement of applicability;

c the procedures adopted to implement the controls as specified in 2.3. These shall describe responsibilities and relevant actions;
d the procedures covering the management and operation of the public key infrastructure. These shall describe responsibilities and relevant actions.

III.5 Document control

The CSP shall establish and maintain procedures for controlling all documentation to ensure that the documentation is:
a readily available;
b periodically reviewed and revised as necessary in line with the organizations policy;
c maintained under version control and made available all locations where operations essential to the effective functioning of the CSP are performed;
d promptly withdrawn when obsolete;
e identified and retained when obsolete and required for legal or knowledge preservation purposes, or both.

Documents shall be legible, dated (together with dates of revision) and readily identifiable, maintained in an orderly manner and retained for a specified period. Procedures and responsibilities shall be established and maintained for the creation and modification of the various types of document.

III.6 Records

Records, being evidence generated as a consequence of the operation of the public key infrastructure shall be maintained to demonstrate compliance with the requirements, as appropriate to the system and to the organization.

The organization shall establish and maintain procedures for identifying, maintaining, retaining and disposing of the records demonstrating compliance.

Records shall be legible, identifiable and traceable to the activity involved. Records shall be stored and maintained in such a way that they are readily retrievable and protected against damage, deterioration or loss.

IV DETAILED PKI CONTROLS FOR CERTIFICATION SERVICE PROVIDERS

Section 3 specifies detailed controls that are relevant for the public key infrastructure of CSPs. The structure of section 3 is in compliance with RFC 2527.
Guidance is selected from SEIS-S10 98/98, from (Draft) ABA PKI Evaluation Guidelines and from (Draft) ANSI Standard ABA X9.79-199x. The applicability of the controls was checked in trial certification audits at a number of Certification Service Providers in the Netherlands.
The CSP shall take all steps necessary to evaluate conformance with this selection of controls in accordance with the requirements of operating a PKI management framework. This shall be verified by reviews in accordance with 2.3.

Detailed controls

(Numbering according to RFC 2527)

1 INTRODUCTION

This section identifies and introduces the set of provisions for the PKI service and indicates the type of entities and applications for which the specification is targeted.

1.1 Overview

Objective: To provide a general introduction to the PKI service.

No stipulation.

1.2 Identification

Objective: To provide unique identification for CSP documentation.

No stipulation.

1.2.1 Unique document identifiers

CSP shall provide unique identifiers for its CP and/or CPS.

1.3 Community and Applicability

Objective: To specifically address in CSP documentation (CP/CPS) whether the responsibilities of a certification authority will be performed by a single entity, or whether they will be performed by separate entities such as a Registration Authority and Certification Management Agents. To specify the applicability of certificates.

1.3.1 Certification authorities

The CP/CPS shall contain a description of the role of a CA within the PKI environment where the CP/CPS is used or within which the CA operates.

Guidance:
In case the CA operates in an open PKI system, its "core" CA functions may not be delegated to other entities or parties, as certain legal obligations and potential liabilities in an open PKI system flow from the issuance of a certificate. Only in a closed PKI system may such CA functions be delegated through contracts with the other entities performing the CA-related functions.

1.3.2 Registration authorities

The CP/CPS shall contain a description of the role of a RA within the PKI environment where the CP/CPS is used.

Guidance:
The CP/CPS must specifically state the type of PKI implementation model that is used and must permit the RA responsibilities and CA responsibilities to be performed by either the same entity or by different entities, unless specific reasons exist for to restrict such opportunity.

1.3.3 End entities

The CP shall contain a description of the types of end entities and their role within the PKI environment.

Guidance:
End entities can be subscribers, relying parties and other parties. -
The CPS should contain a description of the permitted entities that may be subscribers. The subscribers to be certified under this policy may be individuals, organizations, or devices.
The CPS should contain a statement of the beforementioned obligations for subscribers.
The CPS should define the permitted relationships between CA and relying parties. A relying party must either be a subscriber of the CA domain within which the certificate was created, or a subscriber of a CA domain covered by a cross-certification agreement with the originating CA domain
The CPS should contain a description of other parties that may be pertinent to the use or administration of certificates issued under the current specification. It should also specify that:

- the organizational entity representative is responsible for requesting, when required, the revocation or suspension of the certificate held by a subscribed acting on behalf of this organizational entity
- the organizational entity representative must be duly authorized by the organizational entity he represents for requesting the revocation or suspension of the certificate held by a subscribed acting on behalf of this organizational entity.

1.3.4 Applicability

The CP/CPS shall specifically indicate the applications
- for which the issued certificates are suitable.
- for which use of the issued certificates is restricted.
- for which use of the issued certificates is prohibited.

Guidance:
Examples of application in this case are: electronic mail, retail transactions, contracts, travel order, e-government applications etc.). Restricted applications implicitly prohibits all other uses for the certificates.

1.4 Contact Details

Objective: To specifically address in CP/CPS the contact details of the CSP.

1.4.1 Specification administration organization

The CP/CPS shall specifically indicate the name and mailing address of the authority that is responsible for the registration, maintenance, and interpretation of the CP/CPS.

1.4.2 Contact person

The CP/CPS shall also include the name, electronic mail address, telephone number, and fax number of a contact person.

1.4.3 *Person determining CPS suitability for the policy*

No stipulation.

2 GENERAL PROVISIONS

This section contains controls relating to the respective obligations of CAs, RAs, subscribers, and relying parties, and other issues pertaining to law and dispute resolution.

2.1 Obligations

Objective: To describe for each entity type, any applicable provisions regarding the entity's obligations to other entities.

2.1.1 CA obligations

The CSP shall describe the provisions for the CA obligations.

Guidance
Types of obligations:
- CSP shall provide certification and repository services consistent with its CP/CPS;
- CSP meets the obligations and requirements of its CP/CPS;
- CSP publishes its CP/CPS.

2.1.2 RA obligations

The CSP shall describe the provisions for the RA obligations .

Guidance:
Types of obligations:
- CSP shall provide the identification and authentication services consistent with its CP/CPS;
- CSP meets the obligations and requirements of its CP/CPS;
- CSP publishes its CP/CPS.

2.1.3 Subscriber obligations

The CSP shall describe the provisions for the subscriber obligations.

Guidance:
Types of obligations:
- Accuracy of representations in certificate application;
- Protection of the entity's private key;
- Restrictions on private key and certificate use; and
- Notification upon private key compromise.

2.1.4 Relying party obligations

The CSP shall describe the provisions for the relying party obligations.

Guidance:
Types of obligations:
- Purposes for which certificate is used;
- Digital signature verification responsibilities;
- Revocation and suspension checking responsibilities;
- Acknowledgment of applicable liability caps and warranties.

2.1.5 Repository obligations

The CSP shall describe the obligations for the repository obligations.

Guidance:
Timely publication of certificates and revocation information.

2.2 Liability

Objective, To describe for each entity type, any applicable provisions regarding apportionment of liability.

2.2.1 CA liability

The CSP shall describe the provisions for the CA liabilities.

Guidance
Types of liabilities:
- CSP shall specify in its CPS warranties and limitation on warranties;
- CSP shall specify diclaimers and loss limitations per certificate or per transaction;
- CSR shall specify in its CPS other exclusions;
- CSP publishes its CPS.

2.2.2 RA liability

The CSP shall describe the provisions for the RA liabilities.

Guidance
Types of liabilities:
- CSP shall specify in its CPS warranties and limitation on warranties;
- CSP shall specify diclaimers and loss limitations per certificate or per transaction;
- No stipulation on other exclusions;
- CSP publishes its CPS.

2.3 Financial responsibility

Objective: To describe for its CAs, repository and RAs, any applicable provisions regarding financial responsibilities.
See General Requirements for CSPs.

Guidance:
TTP.NL has developed a set of standards for Certification and Accreditation of CSPs.
Financial responsibility is addressed in detail in General Requirements standard for CSPs.

2.4 Interpretation and Enforcement

Objective: To describe the provisions regarding interpretation and enforcement.

2.4.1 Governing law

No stipulation.

Guidance:
Various laws and regulations may apply, depending upon the jurisdiction(s) in which certificates are issued and used. It is the responsibility of the entities concerned to ensure that all applicable laws and regulations of mandatory nature are followed.

2.4.2 Severability, survival, merger, notice

No stipulation.

Guidance:
See 2.4.1.

2.4.3 Dispute resolution procedures

See General Requirements for CSPs.

Guidance:
TTP.NL has developed a set of standards for Certification and Accreditation of CSPs.
Dispute resolution is addressed in detail in General Requirements standard for CSPs, section 7.

2.5 Fees

Objective, To describe any applicable provisions regarding fees charged by its CAs, repositories and RAs.

2.5.1 Certificate issuance or renewal fees

No stipulation.

2.5.2 Certificate access fees

No stipulation.

2.5.3 Revocation or status information access fees

No stipulation.

2.5.4 Fees for other services such as policy information

No stipulation.

2.5.5 Refund policy

No stipulation.

2.6 Publication and Repository

Objective: To describe any applicable provisions regarding publication and repositories.

2.6.1 Publication of CSP information

The CSP shall describe the provisions regarding publication of CSP information.

Guidance:
The CSP shall make publicly available in its repositories its CP/CPSs, its CRLs and its CA-certificates.

CRLs, CPSs and CA-certificates shall be available from the public repository all days, 24 hour per day. Upon system failure, service or other factors which is not under control of the CA, this information service may be unavailable for a maximum period of time defined in the CPS.
Information objects in certificates which are regarded as sensitive personal data of the subscriber shall be handled confidentially. A CSP must never publish copies of issued certificates in publicly available repositories without the express permission of the subscriber.
If copies of issued certificates are published then the CSP shall undertake to inform the subscriber that personal data of the subscriber will be publicly available through access to public data networks.
The CSP shall provide relevant information about issued certificates when necessary to aid in dispute resolution concerning digital signatures.
CRLs shall contain revocation information of all revoked certificates having a validity period at the time of CRL issuance. Information of expired certificates will normally be removed from subsequent CRLs.
CA-certificates for all public CA-keys shall be available in the directory until all certificates, issued with their corresponding private issuing key, has expired.

2.6.2 Frequency of publication

The CSP shall implement CRL publication in accordance with 4.4. and CP/CPS publications in accordance with 8.

2.6.3 Access controls

The CSP shall specify access controls regarding publication and repositories.

Guidance:
There shall be no access controls on the reading of CP/CPS;
Access controls on certificates, certificate status (if provided as a CSP service), or CRLs are optional at the discretion of the CSP;
There shall be appropriate access controls controlling who can write or modify all items mentioned above.

2.6.4 Repositories

The CSP shall make available a repository to publish the information identified in 2.6.1.

Guidance:
Such repository may be operated by the CSP or by a separate organization.

2.7 Compliance audit

Objective: To specify the general procedures to be followed by Certification Bodies that assess CSPs and certify processes and security of CSPs.

See Scheme for Certification and Accreditation of CSPs for electronic commerce and communication, Sections 5 and 6 and Appendices A and B.

Guidance:
TTP.NL has developed a set of standards for Certification and Accreditation of CSPs. COMPLIANCE AUDIT is addressed in detail in the above mentioned scheme.

2.8 Confidentiality

Objective: To specify confidentiality of information.

2.8.1 Types of information to be kept confidential

The CSP shall define types of information that are considered confidential and specify requirements and procedures to address it.

Guidance:
Any personal or corporate information held by CAs or RAs which is not appearing on issued certificates is considered confidential and shall not be released without the prior consent of the subscriber, unless required otherwise by law. All private and secret keys used and handled within the CA operation under this policy are to be kept confidential. Audit logs and records shall not be made available as a whole, except as required by law. Only records of individual transactions may be released according to section 4.6.6.

2.8.2 Types of information not considered confidential

The CSP shall define types of information not considered confidential.

Guidance
Certificates, CRL's and revocation/suspension information are not considered confidential.
Identification information or other personal or corporate information appearing on certificates is not considered confidential, unless statutes or special agreements so dictate.

2.8.3 Disclosure of certificate revocation/suspension information

See 2.8.2

2.8.4 Release to law enforcement officials

According to applicable law.

2.8.5 Release as part of civil discovery

No stipulations.

2.8.6 Disclosure upon owner's request

As stated in 2.8.1.

2.8.7 Other information release circumstances

No stipulations.

2.9 Intellectual Property Rights

Objective: To describe ownership rights of certificates, CPS/CP specifications, names and keys.

No stipulations.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

Objective: To provide names and other forms of identification information for initial registration.

3.1.1 Types of names

The CSP shall specify the types of names it uses within its PKI.

Guidance:
A variety of different kinds of names may legitimately be required for different applications and purposes. Whether one name form or another is chosen to be the primary index into a directory, i.e., the Distinguished Name vs. an Alternate Subject Name, should not in and of itself be viewed as deprecating or derogating one name form in favor of another, as the choice of which name form is used for indexing purposes depends upon the uses of the directory and the desires of the directory owner or administrator, and not necessarily on the Subscriber or the CA. (for example x.500 distinguished name).

3.1.2 Need for names to be meaningful

CSP shall use meaningful names within the PKI .

3.1.3 Rules for interpreting various name forms

No stipulations.

3.1.4 Uniqueness of names

CSP shall use unique names within the PKI .

3.1.5 Name claim dispute resolution procedure

CSP shall have a name claim dispute resolution procedure.

3.1.6 Recognition, authentication and role of trademarks

No stipulations.

3.1.7 Method to prove possession of private key

The CSP shall specify in the CP/CPS that the requesting subscriber proves he has possession of the private key which corresponds to the public key that the subscriber is requesting to be certified.

Guidance:
Evaluators should examine the practices employed by the CSP to prove possession of the private key by the requesting subscriber prior to issuance of a certificate by the CSP. Examples of Proof of Possession Protocols/Processes:
Certificate request & response protocols such as (a) PKCS-10/PKCS-7, (b) PKIX-CRMF (Certificate Request Message Format)
CA private key generation and secure delivery to subscriber

3.1.8 Authentication of organization identity

CSP shall describe a procedure for the authentication of organisation entity.
Guidance:
As part of the CSPs certificate issuance process, the CSP shall exercise appropriate diligence to verify that the requesting entity is in fact who and what they claim to be.

The CSP must require the authorized representative of the requesting organization to (a) supply adequate documentation and/or certifications evidencing valid formation in a jurisdiction providing a means for the CSP to

verify such documentation/certification and (b) meet the requirements for validating an individual.

3.1.9 Authentication of individual identity

CSP shall describe a procedure for the authentication of individual entity.

Guidance:
As part of the CSPs certificate issuance process, the CSP shall exercise appropriate diligence to verify that the requestor is in fact who he/she claims to be.
The CSP must require proof to enable verification of appropriate documentation (passport, driver license etc).

3.2 Routine Rekey

Objective: To describe the identification and authentication procedures for routine rekey for each subject type (CA, RA, and end entity).

3.2.1 Routine Rekey CA, RA and end entity

The CSP shall require that the requesting entity provide the RA (or the CA) with sufficient information to allow the RA (or the CA) to verify the identity of the requesting entity and to identify the certificate to rekey.

Guidance:
The Registration Rekey Request must include at least the Distinguished Name of the requesting entity, the Serial Number of the certificate, and the requested validity period. The CSP can require that the requesting entity digitally signs the certificate rekey data (Registration Rekey Request) using the private key that relates to the public key contained in the requesting entity's existing public key certificate.

3.3 Rekey after Revocation

Objective: To describe the identification and authentication procedures for rekey for each subject type (CA, RA, and end entity) after the subject certificate has been revoked

3.3.1 Rekey after Revocation for CA, RA and end entity

The CSPs policies and procedures for issuing a rekeyed certificate to replace a revoked or expired certificate are the same as those for the initial certificate application process

3.4 Revocation Request

Objective: To describe the identification and authentication procedures for a revocation request.

3.4.1 Revocation request by CA, RA and end entity

The CSP shall specify in the CPS the procedures for a revocation request.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Objective: To state requirements regarding subject enrollment and request for certificate issuance.

4.1.1 Certificate Application

The CSP shall define the decision who can request a certificate in the CP/CPS. That decision will be implemented in accordance with the CPS. The CSP shall define the identification and authentication procedures for entity registration in accordance with its CPS.

4.2 Certificate Issuance

Objective: To state requirements regarding issuance of a certificate and notification to the applicant of such issuance.

4.2.1 Certificate Issuance

The CSP shall adequately verify a certificate request prior to further processing. After successful verification of the certificate application and issuance of the certificate, the CSP shall notify the subscriber that the certificate has been issued.

Guidance:
Certificate issuance process and notification process will be achieved using a mechanism defined in the CPS.

4.3 Certificate Acceptance

Objective: To state requirements regarding acceptance of an issued certificate and for consequent publication of certificates.

4.3.1 Certificate Acceptance

For express acceptance to occur the subscriber must have requested a certificate and the CSP shall act on that request pursuant to the relevant CP/CPS, issue the certificate and notify the subscriber of that fact.

Guidance:
Tests as to whether implied acceptance has occurred include:

- Was there a request for issuance
- Was there express approval of the certificate contents by the subscriber
- Could the user reasonably deny knowing the certificate was available
- Has the subscriber used the certificate
- Could the user reasonably forsee that a relying party would rely on the certificate

4.4 Certificate Suspension and Revocation

Objective: To state requirements for suspension and revocation of certificates.

4.4.1 Circumstances for revocation

The CSP shall specify the circumstances that lead to revocation of a certificate.

Guidance:
Specific reasons for revocation may include:

- Loss of control of private key (key compromise)

- Death or disability of the subscriber
- Theft of loss of the private key or private key container (i.e. smartcard, computer)
- At the authenticated request of the subscriber for any reason
- Use of the certificate in violation of a contractual agreement
- Change in the validity of any material certificate data
- Breach of contract (i.e. nonpayment for service)

4.4.2 Who can request revocation

The CSP shall specify who can request revocation.

Guidance:
Unless otherwise provided by the CP/CPS, only the subscriber, the subscriber's legal representative, executor or legal guardian may request a certificate revocation. A CSP shall initiate a revocation when it has knowledge of facts that constitute grounds for revocation.
In addition to the subscriber, his representatives, executors and guardians, other parties may be designated in a CP/CPS to request revocations. These often include RAs, or parties who attest to the validity of information stated in certificates, for example a personnel officer who might request the revocation of a certificate for an employee, when that employee is terminated. Where the CP/CPS normally requires that revocation requests be signed messages from the subscriber, the CPS often allows RAs to also request revocations, to allow for revocation of certificates where the key is compromised and the subscriber no longer has access to the key.

4.4.3 Procedure for revocation request

The CSP shall specify the procedure how to perform an authenticated revocation request.

Guidance:
Examples of authenticated messages:
- Digitally signed electronic message.
- Telephone communication using authentication (i.e. shared secret)
- Written request, with an authentication procedure

4.4.4 Revocation request grace period

The CSP shall specify the maximum time to process a revocation request.

Guidance:
CSP shall revoke the certificate from a subscriber as soon as it has authenticated information justifying a revocation. The CSP may provide a suspension of the certificate pending the authentication of information received. The subscriber's duties to inform the CSP of an event requiring revocation should be covered in the subscriber's agreement and any documents incorporated therein.

4.4.5 Circumstances for suspension

The CSP shall describe in the CP/CPS under what circumstances a certificate must be suspended.

4.4.6 Who can request suspension

The CSP shall specify in the CP/CPS who may request a certificate suspension.

4.4.7 Procedure for suspension request

The CSP shall have procedures in place and means of rapid communication to facilitate the secure and authenticated suspension of:
- one or more certificates of one or more entities;
- the set of all certificates issued by a CSP based on a single public/private key pair used by a CSP to generate certificates; and

- all certificates issued by a CA, regardless of the public/private key pair used.

4.4.8 Limits on suspension period

The CSP shall specify in the CP/CPS how long a certificate suspension may last.

4.4.9 CRL issuance frequency

The CSP shall specify in the CP/CPS the frequency and timing of CRL issuance. The CRLs shall contain an issue date as well as the date that the next CRL will be issued.

Guidance:
The CSP shall make the method of publication and the sorts of data that will be incorporated into its CRL clear in its CP/CPS. CRLs are the predominant mechanism used for revocation notification. A CRL is a list of revoked certificates. A CRL is signed by a CSP. usually the CSP that issued the revoked certificates, however CSP's can delegate the authority to revoke (that is sign CRLs) certificates to another CSP. CRLs are signed documents, so their authenticity depends on the validation of the signature and not on how they are acquired.

Relying party clients are typically designed to cache copies of CRLs and use those copies until the date that the next CRL will be issued. In some cases, unscheduled "interim" CRLs may be issued, particularly for key compromises.

4.4.10 CRL checking requirements

The CSP shall describe in the CP/CPS the certificate revocation or certificate status checking mechanisms and requirements and the obligations of relying parties to check the status of certificates before relying on the certificates.

Guidance:
In principle, the certification authority that originally issued the certificate should normally carry out certificate revocation. To ensure that the services of certificate revocation are carried out in a proper manner when large numbers of revocations are being issued and the CRL can no longer be managed by a single certification authority, it will be possible for certification authorities to outsource either all or part of its revocation duties as appropriate.

4.4.11 On-line revocation/status checking availability

The CSP shall state if online revocation checking is available.

Guidance:
An example is the automatic checking of a CRL by an application or the use of OCSP.

4.4.12 On-line revocation checking requirements

See 4.4.10.

Guidance:
The proposed IETF On-line Status Protocol (OCSP) standard will provide a standardized protocol for on-line status requests for specific certificates. An OCSP "responder" then provides a signed status response message about the status of the certificate. OCSP responders are trusted entities

4.4.13 Other forms of revocation advertisements available

No stipulations.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulations.

4.4.15 Special requirements re key compromise

The CSP shall describe special requirements in the CP/CPS when the suspension or revocation is the result of private key compromise.

4.5 Security Audit Procedures

Controls are addressed in Information Security Management for CSPs, section 12.

4.6 Records Archival

Controls are addressed in Information Security Management for CSPs, section 12.

4.7 Key changeover

Objective: To describe the requirements for changing (rekeying) the CSPs public key according to the applicable CP/CPS.

4.7.1

The CSP shall provide an uninterrupted CA service to subscribers. The management of the key pair life cycle and key changeover shall be a controlled and managed process.

Guidance:
The CSP shall establish and document a subsequent distribution mechanism. The integrity and authenticity of the CSPs public key and any associated parameters must be maintained throughout the initial distribution process

4.8 Compromise and Disaster Recovery

Objective: To describe the CSPs business continuity plan (in accordance with its CP/CPS or other CSP related security-related documentation) including procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is reestablished either at the original site or a remote hot-site. At a minimum, business continuity planning includes disaster recovery processes for all critical components of a CSP system, including the hardware, software and keys, in the event of a failure of one or more of these components.

See Information Security Management for CSPs, section 11.

4.9 CA Termination

Objective: To describe the requirements relating to procedures for termination and for termination notification of a CSP, including the identity of the custodian of the CSP archival records.
The CSP shall describe CSP termination procedures.

Guidance:

- The CSP shall have policies and procedures to minimize potential disruptions as a result of the cessation of their services.
- The CSPs CP/CPS describes its procedures for termination and for termination notification of a CSP, including the identity of the custodian of the CSP archival records.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical and environmental security

Objective: The CSP shall prevent unauthorised access, damage and interference to business premises and information.
See Information Security Management for CSPs, TTP.NL Part 2, section III paragraph 7.

5.2 Procedural security controls

Objective: The CSP shall prevent loss, damage or compromise of assets and interruption to business activities.
See Information Security Management for CSPs, TTP.NL Part 2, section III paragraphs 8 and 9.

5.3 Personnel security controls

Objective: The CSP shall prevent compromise and theft of information and information processing facilities.
See Information Security Management for CSPs, TTP.NL Part 2, section III paragraph 6.

Guidance:
TTP.NL has developed a set of standards for Certification and Accreditation of CSPs. physical, procedural, and personnel security controls are addressed in detail in the above mentioned standard.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

Objective: To provide technical security controls in order to perform secure key generation and Installation for the PKI components.

6.1.1 Key pair generation

The CSP shall describe who generates the cryptographic keys within the PKI.

Guidance
- Describe key generation per PKI component (CA, RA, LRA, End entity) and indicate key generation location (central, local key generation).

6.1.2 Private key delivery to entity

In case key pairs are generated centrally, the CSP shall deliver private keys to the entity in a secure manner without any compromise.

Guidance
- Only applicable in case key pairs are generated centrally.
- Key delivery shall be performed in a secure manner, in a controlled environment, and protected with adequate security measures.

6.1.3 Public key delivery to certificate issuer

In case key pairs are generated locally, the PKI components shall deliver their (uncertified) public keys to the CSP for certification purposes in a secure manner during which the integrity of the public key is adequately protected.

Guidance
- Only applicable in case key pairs are generated locally.
- The public key shall be delivered by using a secure channel, in a controlled manner, and protected with adequate security measures (key delivery protocol).

6.1.4 CA public key delivery to users

CSP shall deliver or shall make available its public key certificate to the end entities within the PKI.

Guidance:
- CSP shall make available its public key certificate in a public repository or make the public key certificate available in any other manner (integration in end entity software application).
- Availability of the public key certificate is essential in order to facilitate certificate verification by the end entity.

6.1.5 Key sizes

Key sizes for all cryptographic keys (key categories) will be published by the CSP. CSP will make use of key sizes that meet the state of the art in technology and that meet a risk assessment with respect to the indicated key usage.

Guidance:
- CSP shall publish key sizes of the cryptographic keys within the PKI.
- Key sizes on different levels within the PKI may differ. It is important that the key sizes on the different levels within the PKI and for keys with different key usage purposes meet the industry state of the art requirements.

6.1.6 Public key parameters generation

CSP shall describe how the public key parameters (random seed) are generated within the PKI (Random Number Generator) and at which location this is performed.

Guidance
- Key generation uses a prime number generator as specified in an international standard.
- Random number generator/ Pseudo Random number generator.

6.1.7 Parameter quality checking

CSP shall describe the procedure for public key parameter checking.

Guidance
- CSP shall describe whether the quality of the public key parameters is checked and what the requirements are.

6.1.8 Hardware/software key generation

CSP shall describe per PKI component whether the cryptographic keys are generated in software or in hardware.

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

CSP shall describe the key usage purposes of the public key certificates within the PKI.

Guidance
See key usage field specified in the X.509 v3 certificate profile.

6.2 Private Key Protection

Objective: To provide technical security controls in order to perform adequate protection for the private keys within the PKI.

6.2.1 Standards for cryptographic module

CSP shall specify the trustworthiness of the cryptographic module(s) used within the PKI and specify which security standards and which levels the device(s) meet(s).

Guidance:
ITSEC / Common Criteria are selected standards which will be of help in addressing the EU requirement for CSPs to use trustworthy systems. TTP.NL considers to use Evaluation Assurance Levels (EALs) of EAL4 (or ITSEC

equivalent) and downwards to evaluate products and other systemcomponents in CSP's trustworthy systems.

6.2.2 Private key (n out of m) multi-person control

CSP shall specify which of its private keys within the PKI are under multi-person control and what multi-person control rules are.

6.2.3 Private key escrow

CSP shall describe which private keys within the PKI are escrowed.

Guidance:
- Check the escrow form (examples include plaintext, encrypted, split key).
- Check whether escrow takes place in a separate geographical location.
- If applicable, check the name of the escrow agent.
- Check the minimum controls on the escrow system.

6.2.4 Private key backup

CSP shall describe which private keys within the PKI are backed up.

Guidance:
- Check the back-up form (examples include plaintext, encrypted, split key).
- Check whether back-up takes place in a separate geographical location.
- If applicable, check the name of the back-up agent.
- Check the minimum controls on the back-up system.

6.2.5 Private key archival

CSP shall describe which private keys within the PKI are archived.

Guidance:
- Check the archival form (examples include plaintext, encrypted, split key).
- Check whether archival take place in a separate geographical location.
- If applicable, check the name of the archival agent.
- Check the minimum controls on the archival system.

6.2.6 Private key entry into cryptographic module

CSP shall specify the procedure governing private key entry in the cryptographic module.

Guidance:
- Check the form in which the key is stored and which security standards the cryptographic module meets.
- Check who enters the private key in the cryptographic module.
- Check dual person control.
- Check how the private key is stored in the module (i.e., plaintext, encrypted, or split key).

6.2.7 Method of activating private key

CSP shall describe a procedure for activiting the private key.

Guidance:
- Check whether the activation of the private key requires multi-factor authentication.

6.2.8 Method of deactivating private key

CSP shall describe a procedure for deactivating the private key.

Guidance:
- Check whether the deactivation of the private key requires multi-factor authentication.
- Check who can deactivate the private key and how.
- Examples of how private key might be deactivated may include: logout, power off, remove token/key, automatic, or time expiration.

6.2.9 Method of destroying private key

CSP shall specify the private key destruction procedure.

Guidance:
- Check who is authorised to destroy the private key and how. Examples of how might include token surrender, token destruction, or key overwrite, destruction in a secure site.

6.3 Other Aspects of Key Pair Management

Objective: To provide technical security controls in order to perform controlled key archival and public key usage.

6.3.1 Public key archival

The CSP shall specify public key archival procedures.

Guidance:
- Check whether the public key is archived.
- Check who is the archival agent.
- Check what are the security controls on the archival system.

6.3.2 Usage periods for the public and private keys

The CSP shall specify public and private key usage periods.

Guidance:
- Check the usage periods or active lifetimes for the public and the private key respectively.

6.4 Activation Data

Objective: To generate, install and protect activation data (e.g., PINs, passphrases, or a manually-held key shares) in a secure manner.

See: Information Security Management for CSPs (TTP.NL Part 2), section III paragraph 9.5.

Guidance:
Check that activation data refers to data values other than keys that are required to operate cryptographic modules. For each of the entity types (issuing CA, repository, subject CA, RA, and end entity) all of the items listed in 6.1 through 6.3 potentially need to be checked with respect to activation data rather than keys.

6.4.1 Activation data generation and installation

CSP shall describe the procedures for the generation and installation of activation data for the entities within the PKI.

Guidance:
- It is preferable that activation data never be visible to anyone but the individual who will be responsible for activating the system.
- If activation requires m of n individuals, the portions of the activation data should never reside in fewer than m hands.
- Provision for activating the system in the absence of one or more of the activators should be made (i.e., n should be

bigger than m).
- Successful guessing of the activation data should be infeasible. It should not be possible to make and confirm guesses outside the system, and the system should protect against too many incorrect guesses.
- Activation data should be stored only ephemerally and preferably in a form not useable by an intruder. Any residue of the activation should be removed from the system.

6.4.2 Activation data protection

CSP shall describe the procedures for the protection of activation data for the entities within the PKI.

Guidance:
- Splitting the activation data among multiple individuals (e.g., m of n items are needed to activate the system) reduces the level of protection required of any one piece of the data.
- Holders of activation data must be aware of the importance of the activation data.
- In general, the activation data should be memorized rather than written.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer Security Controls

Objective: To describe computer security controls and computer security ratings.

See Information Security Management for CSPs, section III paragraphs 9 and 10.

Guidance:
Computer security controls are addressed in detail in the Information Security Management standard (TTP.NL Part 2). ITSEC / Common Criteria are selected standards which will be of help in addressing the EU requirement for CSPs to use trustworthy systems. TTP.NL considers to use Evaluation Assurance Levels (EALs) of EAL4 (or ITSEC equivalent) and downwards to evaluate products and other systemcomponents in CSP's trustworthy systems.

6.6 Life Cycle Technical Controls

Objective: To describe life cycle technical controls.
See Information Security Management for CSPs (TTP.NL Part 2), section III paragraph 10.

Guidance:
See 6.5.

6.7 Network Security Controls

Objective: To describe network security controls.
See Information Security Management for CSPs (TTP.NL Part 2), section III paragraphs 8 and 9.

Guidance:
See 6.5.

6.8 Cryptographic Module Engineering Controls

Objective: To describe procedures for receiving, installing, and maintaining the cryptographic module.

CSP shall describe the procedures for the device life cycle.

Guidance:
The device life cycle may consist of the following items:
- shipment
- receipt
- pre-use storage
- installation
- usage
- service and repair
- retirement

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

Objective: To provide the certificate profile contents

The CSP shall specify a certificate profile definition.

Guidance:
See the ITU-T *Rec.* X.509 fields.
- Version number(s)
- Certificate extensions
- Algorithm object identifiers
- Name forms
- Name constraints
- Certificate policy Object Identifier
- Usage of Policy Constraints extension
- Policy qualifiers syntax and semantics
- Processing semantics for the critical certificate policy extension

7.2 CRL Profile

Objective: To provide the CRL profile contents

The CSP shall specify a CRL profile definition.

Guidance:
See the ITU-T *Rec.* X.509 fields.
- Version number(s)
- CRL and CRL entry extensions

8. SPECIFICATION ADMINISTRATION

Objective: To specify how the CP/CPS and other documentation will be maintained.

See General Requirements for CSPs.

Guidance:
TTP.NL has developed a set of standards for Certification and Accreditation of CSPs.
Specification administration is addressed in detail in General Requirements standard for CSPs.

0 - 0 - 0

TTP.NL Part 2

REQUIREMENTS and GUIDANCE

for the Certification of

INFORMATION SECURITY MANAGEMENT

of Certification Service Providers

INTRODUCTION

The text in this document is drawn from two main sources: original text of the standards BS7799 Part 1 and 2 and new text of the Guidance on the application of BS7799 as necessary to suit activities of Certification Service Providers issuing qualified certificates for advanced electronic signatures. The alterations in the original text and the new text for the guidance were developed by the Workgroups ACT & Criteria of the TTP.NL project in the Netherlands.

The source of the texts can be identified by the use of different fonts:

- Text of BS7799 – with alterations to make it applicable in the field of Certification Service Providers issuing qualified certificates.
  TTP.NL acknowledges British Standards Institute (BSI's) ownership of this material and will revise this document in the event that BSI publish a new version of the material.
- Guidance on the application of BS7799– for use by Certification Service Providers issuing qualified certificates. TTP.NL is owner of this material and will revise this document when necessary.

The term "shall" is used throughout this document to indicate those provisions which, reflecting the requirements of BS7799 are mandatory. The term "should" is used to indicate those provisions which, although they constitute guidance for the application of the requirements, are expected to be adopted by a Certification Service Provider. Any variation from the guidance by a Certification Service Provider shall be an exception. Such variations will only be permitted on a case by case basis after the Certification Service Provider has demonstrated to the certification body that the exception meets the relevant requirements clause of BS7799 and the intent of the guidance in some equivalent way.

I GENERAL

I.1 Scope

This document specifies requirements that a Certification Service Provider shall meet in establishing, implementing and documenting its information security management.
The specification is based on relevant parts of the (Draft) Scheme for Certification and Accreditation of Certification Service Providers for electronic commerce and communication.
BS 7799-1:1999 gives recommendations for best practice in support of the requirements of this specification.

II INFORMATION SECURITY MANAGEMENT

II.1 General

The CSP shall establish and maintain a documented information security management framework. This shall address the assets to be protected, the CSP's approach to risk management, the control objectives and controls, and the degree of assurance required.

II.2 Establishing an information security management framework

The following steps shall be undertaken to identify and document the control objectives and controls:

a the CSP shall define a policy addressing the operation of its electronic signature certification system;
b the CSP shall define the scope of the electronic signature certification system, in terms of the characteristics of the organization, its location, assets and technology;
c the CSP shall undertake a risk analysis. It shall identify treats to assets, vulnerabilities and impacts on the CSP and shall determine the degree of risk;
d the CSP shall define its own requirements, based on the organizations policy, including legal requirements (concerning data protection), and the level of assurance required;
e the CSP shall select control objectives and controls from section 3 for implementation by the CSP. The selection shall be justified;
f the CSP shall compile a Statement of Applicability. This statement shall also record the exclusion of any controls listed in section 3.

II.3 Implementation

The selected control objectives and controls shall be effectively implemented. This shall be verified by reviews in accordance with 3.12.2.

II.4 Documentation

The documentation shall consist of the following information:

a evidence of the actions undertaken as specified in 2.2;
b a summary of the management framework, including the organizations policy , the level of assurance, the control objectives and implemented controls, given in the Statement of applicability;
c the procedures adopted to implement the controls as specified in 2.3. These shall describe responsibilities and relevant actions;
d the procedures covering the management and operation of the management framework. These shall describe responsibilities and relevant actions.

II.5 Document control

The CSP shall establish and maintain procedures for controlling all documentation to ensure that the documentation is:

a readily available;
b periodically reviewed and revised as necessary in line with the organizations policy;
c maintained under version control and made available all locations where operations essential to the effective functioning of the CSP are performed;
d promptly withdrawn when obsolete;
e identified and retained when obsolete and required for legal or knowledge preservation purposes, or both.

Documents shall be legible, dated (together with dates of revision) and readily identifiable, maintained in an orderly manner and retained for a specified period. Procedures and responsibilities shall be established and maintained for the creation and modification of the various types of document.

II.6 Records

Records, being evidence generated as a consequence of the operation of the management framework shall be maintained to demonstrate compliance with the requirements this selection of BS 7799, as appropriate to the system and to the organization.

The organization shall establish and maintain procedures for identifying, maintaining, retaining and disposing of the records demonstrating compliance.

Records shall be legible, identifiable and traceable to the activity involved. Records shall be stored and maintained in such a way that they are readily retrievable and protected against damage, deterioration or loss.

III DETAILED SECURITY CONTROLS FOR CERTIFICATION SERVICE PROVIDERS

Section 3 specifies relevant controls selected from BS 7799, part 1 addressing information security management of the CSP. The selection is based on experiences with trial certification audits at a number of Certification Service Providers in the Netherlands.
The CSP shall take all steps necessary to evaluate conformance with this selection of controls in accordance with the requirements of operating an electronic signature certification system. This shall be verified by reviews in accordance with 3.12.2.

Detailed controls

1 Scope

2 Terms and definitions

2.1 Information security

2.2 Risk assessment

2.3 Risk management

3 Security policy

3.1 Information security policy

3.1.1 Information security policy document

A written policy document shall be available to all employees responsible for information security.

3.1.2 Review and evaluation

There shall be a defined review process, including responsibilities and review dates, for maintaining the security policy.

Guidance to clause 3

As a minimum, the security policy shall contain the following:

A) definition of information security, it's overall objectives and scope, and the importance of security as an enabling mechanism for information sharing;
B) a statement of management intent, supporting the goals and principles of information security;
C) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, including:
   - compliance with legislative and contractual requirements;
   - security education requirements;
   - prevention and detection of viruses and other malicious software;
   - business continuity management; and
   - the consequences of security policy violations;
D) a definition of general and specific responsibilities for information security management, including reporting security incidents; and
E) references to documentation that may support the policy.

4 Security organization

4.1 Information security infrastructure

Objective. To manage information security within the organization.

4.1.1 Management information security forum

Management direction shall be provided through a suitable high level steering forum.

4.1.2 Information security co-ordination

A large organization shall co-ordinate information security measures through a cross-functional forum.

4.1.3 Allocation of information security responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes shall be explicitly defined.

4.1.4 Authorization process for IT facilities

Installation of IT facilities shall be approved and authorized.

4.1.5 Independent review of information security

Implementation and operation of information security shall be independently reviewed.

4.2 Security of third party access

Objective. To maintain the security of organizational IT facilities and information assets accessed by third parties.

4.2.1 Procedures to control third party access

Procedures shall be documented and implemented to control access to organizational information processing facilities by third parties

4.2.2 Identification of risks from third party connections

The risks associated with access to organizational IT facilities by third parties shall be assessed and appropriate security controls implemented.

4.2.3 Security conditions in third party contracts

Contracts with third parties involving access to organizational IT facilities shall specify security conditions.

4.3 Outsourcing

4.3.1 Contracts

The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and/or desktop environments shall be addressed in a contract agreed between the parties.

5 Assets classification and control

5.1 Accountability for assets

Objective. To maintain appropriate protection of organizational assets.

5.1.1 Accountability for assets

Inventories shall be maintained of all major information and IT assets.

5.2 Information classification

Objective. To ensure that information assets receive an appropriate level of protection.

5.2.1 Classification guidelines

Security classifications should be consistent with business needs, as determined by the risk analysis.

5.2.2 Classification labeling

Classified information and outputs from systems handling organizationally classified data should be labeled appropriately.

6 Personnel security

6.1 Security in job definition and resourcing

Objective. To reduce the risks of human error, theft, fraud or misuse of facilities.

6.1.1 Security in job responsibilities

Job descriptions shall define security roles and responsibilities.

6.1.2 Personnel screening

Applications for employment shall be screened if the job involves access to sensitive information.

6.1.3 Confidentiality agreements

Users of organizational IT facilities shall sign a confidentiality agreement.

Guidance on clause 6.1

The CSP's policies and procedures shall specify the controls on contracting personnel.

6.2 User training

Objective. To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

6.2.1 Information security education and training

All employees of the organization and, where relevant, third party users, shall receive appropriate training in organizational policies and procedures.

6.3 Responding to incidents

Objective. To minimize the damage from security incidents and malfunctions and to monitor and learn from such incidents.

6.3.1 Reporting of security incidents

Security incidents shall be reported through management channels as quickly as possible.

6.3.2 Reporting of security weaknesses

Suspected security weaknesses shall be reported.

6.3.3 Reporting of software malfunctions

Software malfunctions shall be reported.

6.3.4 Incident analysis

Mechanisms shall exist to quantify and monitor the types, volumes and costs of incidents and malfunctions.

6.3.5 Disciplinary process

Security breaches by employees shall be dealt with through a formal disciplinary process.

7 Physical and environmental security

7.1 Secure areas

Objective. To prevent unauthorized access, damage and interference to business premises and information services.

7.1.1 Physical security perimeter

Physical security protection shall be based on defined perimeters (or levels), each increasing the total protection provided.

7.1.2 Physical entry controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized persons have access.

7.1.3 Securing offices, rooms and facilities

Offices, rooms and facilities shall be properly secured.

7.1.4 Working in secure areas

Additional controls and guidelines for working in secure areas are used to enhance the security provided by the physical controls protecting the secure areas.

Guidance to clause 7

As a minimum there shall be four levels of physical security which have been specified from the lowest to highest level of security:

- Level 1 physical security - public area
- Level 2 physical security - controlled environment (i.e., restricted or private area)
- Level 3 physical security - secure environment (comparable to a data center)
- Level 4 physical security - physically secure

7.2 Equipment security

Objective. To prevent loss, damage or compromise of assets and interruption to business activities.

7.2.1 Equipment siting and protection

Equipment shall be sited or protected to reduce the risks of damage, interference and unauthorized access.

7.2.2 Power supplies

Equipment shall be protected from power failures or other electrical disturbances.

7.2.3 Cabling security

Power and telecommunications cabling shall be protected from interception or damage.

7.2.4 Equipment's maintenance

Equipment shall be correctly maintained.

7.2.5 Security of equipment off-premises

Security procedures and controls shall cover the security of equipment used outside an organization's premises.

7.2.6 Security disposal of equipment

Data shall be erased from equipment prior to disposal.

7.3 General controls

Objective. To prevent compromise or theft of information and information processing facilities.

7.3.1 Clear desk policy

The organization shall have a clear desk policy in order to protect information from unauthorized access and loss or damage.

7.3.2 Removal of property

Removal of property belonging to the organization shall require authorization.

8 Computer and network management

8.1 Operational procedures and responsibilities

Objective. To ensures the correct and secure operation of computer and network facilities.

8.1.1 Documented operating procedures

Documented procedures shall be provided for the operation of all computer systems and for systems development, maintenance and testing.

8.1.2 Change control

Changes to information processing facilities and systems shall be controlled.

8.1.3 Incident management procedures

Incident management responsibilities and procedures shall be established to ensure an effective and orderly response to security incidents.

8.1.4 Segregation of duties

Duties shall be segregated in order to minimize the risk of negligent or deliberate system misuse.

8.1.5 Separation of development and operational facilities

Development and testing facilities shall be isolated from operational systems.

8.1.6 External facilities management

Proposals to use an external facilities management service shall identify the full security implications and include appropriate security controls.

8.2 System planning and acceptance

Objective. To minimize the risk of systems failure.

8.2.1 Capacity planning

Capacity requirements shall be monitored to indicate where action is needed to avoid failures due to inadequate resources.

8.2.2 System acceptance

Acceptance criteria for new systems shall be established and suitable tests carried out prior to acceptance.

8.3 Protection from malicious software

Objective. To safeguard the integrity of software and data.

8.3.1 Virus controls

Virus detection and prevention measures and appropriate user awareness procedures shall be implemented.

8.4 Housekeeping

Objective. To maintain the integrity and availability of information services.

8.4.1 Information back-up

Back-up copies of essential business data and software shall be taken regularly. Back-up arrangements for individual systems shall meet the requirements of business continuity plans.

8.4.2 Operator logs

Computer operators shall maintain a log of all work carried out.

8.4.3 Fault logging

Faults shall be reported and corrective action taken.

8.5 Network management

Objective. To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

8.5.1 Network controls

A range of controls shall be established to achieve and maintain security in computer networks.

8.6 Media handling and security

Objective. To prevent damage to assets and interruptions to business activities.

8.6.1 Management of removable computer media

Removable computer media, e.g. tapes, disks, cassettes and printed reports, shall be controlled.

8.6.2 Disposal of media

Computer media shall be disposed of securely and safely when no longer required.

8.6.3 Information handling procedures

Procedures for handling sensitive data shall be established.

8.6.4 Security of system documentation

System documentation shall be protected from unauthorized access.

8.7 Exchanges of information and software

Objective. To prevent loss, unauthorized modification or misuse of information exchanged between organizations.

8.7.1 Information and software exchange agreements

Agreements shall be reached between organizations for the exchange of information and software, which shall specify security controls.

8.7.2 Secure of media in transit

Computer media in transit shall be protected from loss, damage, misuse or unauthorized access.

8.7.3 Electronic commerce security

Special security controls shall be applied to protect electronic commerce.

8.7.4 Security of electronic mail

Controls shall be applied to reduce the business and security risks associated with electronic mail.

8.7.5 Security of electronic office systems

Clear policies and guidelines shall be established to control the business and security risks associated with electronic office systems.

8.7.6 Publicly available systems

There shall be a formal authorization process before information is made publicly available and the integrity of such information is protected to prevent unauthorized modification.

9 Access control

9.1 Business requirement for system access

Objective. To control access to business information.

9.1.1 Access control policy

Access to systems shall be restricted for each user or user group to that defined by documented business requirements.

9.2 User access management

Objective. To prevent unauthorized computer access.

9.2.1 User registration

There shall be a formal user registration and de-registration procedure for access to all multi-user information services.

9.2.2 Privilege management

The use of special privileges shall be restricted and controlled.

9.2.3 User password management

The allocation of user passwords shall be securely controlled by a formal management process.

9.2.4 Review of user access rights

User access rights shall be reviewed at regular intervals by management.

9.3 User responsibilities

Objective. To prevent unauthorized user access.

9.3.1 Password use

Users shall be required to follow good security practices in the selection and use of passwords.

9.3.2 Unattended user equipment

Users shall be required to ensure that unattended equipment has appropriate security protection.

9.4 Network access control

Objective. To prevent unauthorized use of networked services.

9.4.1 Policy on use of network services

Users shall have access only to the services that they are authorized to use.

9.4.2 Enforced path

The route from the user terminal to the computer service shall be controlled by creating and maintaining an enforced path.

9.4.3 User authentication for external connections

Connections by remote users via public, or non-organization, networks shall be authenticated.

9.4.4 Node authentication

Connections by remote computer systems shall be authenticated.

9.4.5 Remote diagnostic port protection

Access to diagnostic ports shall be securely controlled.

9.4.6 Segregation in networks

Large networks shall be divided into separate logical domains.

9.4.7 Network connection control

The connection capability of users on shared networks shall be controlled in line with the documented access control policy for each business application.

9.4.8 Network routing control

Shared networks shall have network routing controls.

9.4.9 Security of network services

A clear description of the security attributes of accessible value-added network services shall be obtained and documented.

9.5 Operating system access control

Objective. To prevent unauthorized computer access.

9.5.1 Automatic terminal identification

Automatic terminal identification shall be implemented to authenticate connections to specific locations.

9.5.2 Terminal log-on procedures

Access to IT services shall be via a secure logon process.

9.5.3 User identifiers

Computer activities shall be traceable to individuals.

9.5.4 Password management system

An effective password system shall be used to authenticate users.

9.5.5 Use of system utilities

Use of system utilities programs shall be restricted and tightly controlled.

9.5.6 Duress passwords to safeguard users

Duress passwords shall be provided where appropriate for users who might be the target of coercion.

9.5.7 Terminal time-out

Inactive terminals in high risk locations or serving high risk systems shall be set to time out, to minimize the risks of access by unauthorized persons.

9.5.8 Limitation of connection time

Restrictions on connection times shall be used to provide additional security for high-risk applications.

9.6 Application access control
Objective. To prevent unauthorized access to information held in computer systems.

9.6.1 Information access restriction
Access to information and application system functions shall be restricted in accordance with the access control policy.

9.6.2 Sensitive system isolation
Sensitive systems shall have a dedicated (isolated) computing environment.

9.7 Monitoring system access and use
Objective. To detect unauthorized activities.

9.7.1 Event logging
Audit trails of security events shall be maintained.

9.7.2 Monitoring system use
Procedures for monitoring system use shall be established and implemented.

9.7.3 Clock synchronization
Computer clocks shall be synchronized for accurate recording.

9.8 Mobile computing and teleworking
Objective. To ensure information security when using mobile computing and teleworking facilities.

9.8.1 Mobile computing
A formal policy shall be in place and appropriate controls are adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.

9.8.2 Teleworking
Policies and procedures shall be developed to authorize and control teleworking activities.

10 Systems development and maintenance

10.1 Security requirement of systems
Objective. To ensure that security is built into IT systems.

10.1.1 Security requirements analysis and specification
An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project.

Guidance to clause 10.1.1

TTP.NL has selected a set of international standards for Certification and Accreditation of CSPs.
ITSEC / Common Criteria are selected standards which will be of help in addressing the EU requirement for CSPs to use trustworthy systems. TTP.NL considers to use Evaluation Assurance Levels (EALs) of EAL4 (or ITSEC equivalent) and downwards to evaluate products and other system components in CSP's trustworthy systems.

10.2 Security in application systems
Objective. To prevent loss, modification or misuse of user data in application systems.

10.2.1 Input data validation

Data input to application systems shall be validated to ensure that it is correct.

10.2.2 Control of internal processing

Data processed by application systems shall be validated.

10.2.3 Message authentication

Message authentication is used for applications where there is a security requirement to protect the integrity of the message contact.

10.2.4 Output data validation

Data output from an application system is validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

10.3 Cryptographic controls

Guidance to 10.3

Controls are addressed in Public Key Infrastructure for CSPs, Section 3.

10.4 Security of system files

Objective. To ensure that IT project and support activities are conducted in a secure manner.

10.4.1 Control of operational software

Strict control shall be exercised over the implementation of software on operational systems.

10.4.2 Protection of system test data

Test data shall be protected and controlled.

10.4.3 Access control to program source libraries

Strict control shall be maintained over access to program source libraries.

10.5 Security in development and support environments

Objective. To maintain the security of application system software and data.

10.5.1 Change control procedures

There shall be formal change control procedures for all stages of the system's lifecycle.

10.5.2 Technical review of operating system changes

The impact of operating system changes on security shall be reviewed and appropriate action taken.

10.5.3 Restrictions on changes to software packages

Modifications to software packages shall be discouraged. Any essential changes shall be strictly controlled.

10.5.4 Covert channels and Trojan code

The purchase, use and modification of software shall be controlled and checked to protect against possible covert channels and Trojan code.

10.5.5 Outsourced software development

Controls shall be applied to secure outsourced software development.

11 Business continuity planning

11.1 Aspects of business continuity planning

Objective. To have plans available to counteract interruptions to business activities.

11.1.1 Business continuity management process

There shall be a managed process in place for developing and maintaining business continuity plans across the organization.

11.1.2 Business continuity and impact analysis

A strategic plan, based on appropriate risk assessment, shall be developed for the overall approach to business continuity.

11.1.3 Writing and implementing continuity plans

Plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.

11.1.4 Business continuity planning framework

A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.

11.1.5 Testing, maintaining and re-assessing business continuity plans

Business continuity plans shall be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.

12 Compliance

12.1 Compliance with legal requirements

Objective. To avoid breaches of any statutory, criminal or civil obligations and of any security needs.

12.1.1 Identification of applicable legislation

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system.

12.1.2 Intellectual property rights (IPR)

Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.

12.1.3 Safeguarding of organizational records

Measures shall be taken to protect important records of an organization from loss, destruction and falsification.

12.1.4 Data protection and privacy of personal information

Measures shall be taken to protect personal information.

12.1.5 Prevention of misuse of IT facilities

Measures shall be taken to prevent the misuse of information processing facilities.

12.2

12.3 Reviews of security policy and technical compliance

Objective. To ensure compliance of systems with organizational security policies and standards

12.3.1 Compliance with the security policy

All areas within the organization shall be subject to regular review to determine the level of compliance with security policies.

12.3.2 Technical compliance checking

Information systems shall be regularly checked for compliance with security implementation standards.

12.4 System audit considerations

Objective. To minimize interference to/from the system audit process.

12.4.1 System audit considerations

Audits of operational systems shall be planned and agreed to minimize the risk of disruptions to business processes.

12.4.2 Protection of system audit tools

Access to system audit tools shall be controlled to prevent any possible misuse or compromise.

o - o - o

TTP.NL Part 3

GENERAL REQUIREMENTS and GUIDANCE

for the Accreditation of

CERTIFICATION SERVICE PROVIDERS

issuing Qualified Certificates

INTRODUCTION

The text in this document is drawn from two main sources: original text of the standard ISO/IEC Guide 65:1996 (to which EN 45011:1998 is identical) and original text of the Guidance on the application of ISO/IEC Guide 65 developed by the International Accreditation Forum (IAF). The Guide 65 text and the IAF Guidance text have been modified as necessary to suit activities of Certification Service Providers issuing qualified certificates for advanced electronic signatures. The alterations in the original texts were developed by the Workgroups ACT & Criteria of the TTP.NL project in the Netherlands.

The source of the texts can be identified by the use of different fonts:

- Text of ISO/IEC Guide 65:1996 (EN 45011:1998) – with alterations to make it applicable in the field of Certification Service Providers issuing qualified certificates.
  TTP.NL acknowledges ISO/IEC's ownership of this material and will revise this document in the event that ISO/IEC publish the material in final form.

- Guidance on the application of ISO/IEC Guide 65:1996 (EN 45011:1998) – with alterations to make it applicable in the field of Certification Service Providers issuing qualified certificates.
  TTP.NL acknowledges IAF's ownership of this material and will revise this document in the event that IAF publish the material in final form.

The term "shall" is used throughout this document to indicate those provisions which, reflecting the requirements of ISO/IEC Guide 65, are mandatory. The term "should" is used to indicate those provisions which, although they constitute guidance for the application of the requirements, are expected to be adopted by a Certification Service Provider. Any variation from the guidance by a Certification Service Provider shall be an exception. Such variations will only be permitted on a case by case basis after the Certification Service Provider has demonstrated to the accreditation body that the exception meets the relevant requirements clause of ISO/IEC Guide 65 and the intent of the guidance in some equivalent way.

1

2 Scope

This document specifies General Requirements that a third party issuing qualified certificates for advanced electronic signatures shall meet if it is to be recognized as competent and reliable.

In these General Requirements the term "Certification Service Provider" is used to cover any body issuing qualified certificates as defined in the proposal for a Directive of the European Parliament and of the Council on a common framework for electronic signatures.

3 References

EN 45011:1998	General requirements for bodies operating product certification systems (*ISO/IEC Guide 65:1996*)
ISO/IEC Guide 2: 1996	General terms and their definitions concerning standardization and related activities
ISO/IEC Guide 65: 1996	General requirements for bodies operating product certification systems
NEN-ISO 10011-1:1990	Richtlijnen voor het uitvoeren van audits voor kwaliteits-systemen - Deel 1: Het uitvoeren van audits
NEN-ISO 10011-2:1991	Richtlijnen voor het uitvoeren van audits voor kwaliteits-systemen - Deel 2: Criteria voor de kwalificatie van auditors voor kwaliteitssystemeñ
NEN-ISO 10011-3:1991	Richtlijnen voor het uitvoeren van audits voor kwaliteits-systemen - Deel 3: Beheer van audit programma's
European Directive	Directive of the European Parliament and of the Council on a Community framework for electronic signatures (26-11-1999).

4 Definitions

For the purposes of these General Requirements, the relevant definitions in the reference documents listed in section 2 above and the following definitions apply:

Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Advanced electronic signature means an electronic signature, which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Signature verification data means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

Certificate means an electronic attestation, which links signature verification data to a person and confirms the identity of that person.

Qualified certificate means a certificate, which meets the requirements laid down in Annex I of the European Electronic Signature Directive and is provided by a certification service provider who fulfils the requirements laid down in Annex II of the European Electronic Signature Directive.

Certification service provider means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Guidance to clause 3

G.3.1 The following definitions apply to the guidance in this document:

Normative document: Document that provides rules, guidelines or characteristics for activities or their results. (ISO/IEC Guide 2).

Standard: Document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree in a given context. (ISO/IEC Guide 2)

5 Certification Service Provider

5.1 General provisions

The structure of the Certification Service Provider shall be such as to foster confidence in its certifications. In particular,

a) *policies and procedures* under which the Certification Service Provider operates shall be non-discriminatory;
b) the Certification Service Provider shall make its services accessible to all applicants whose activities fall within its declared field of operation;
c) the criteria against which the Certification Service Provider performs certification shall be those outlined in specified standards or normative documents;
d) the Certification Service Provider shall confine its requirements, verification and decision on certification to those matters specifically related to the scope of the certification being considered;
e) the Certification Service Provider shall establish and maintain a documented certification system. This documentation shall also address the policy for maintaining a reliable operation, the degree of assurance required, the Information Security Management System, the assets to be protected, the organization's approach to risk management, the control objectives, and *the actually implemented controls.*

Guidance to clause 4.1

G.4.1 Certification Service Providers shall not practice any form of discrimination such as hidden discrimination by speeding up or delaying applications.

G.4.2 Documents cited in clause 4.1.a) that specify requirements for a person or legal entity to obtain and maintain a qualified certificate shall be available to the applicant and to the public. These may include National/Regional/International standards or parts thereof and other normative documents defining activities such as verification of identity as appropriate. Documents developed by the Certification Service Provider should be approved in a process taking into account the views of the significantly interested parties.

G.4.3 When a subjective judgement is required to determine compliance, the Certification Service Provider should document explanatory information in accordance with G.4.2. The detail of the explanation should assure consistent and uniform application of the requirements and related certification decisions.

G.4.4 Clause 4.1.e) of the General Requirements pertains to the requirements for the Public Key Infrastructure processes and the management system for Information Security. The Certification Service Provider shall provide evidence to the satisfaction of the accreditation body of adequately documented and implemented processes for the Public Key Infrastructure and the Information Security Management System.

5.2

5.3 Organization

In order to foster confidence, the Certification Service Provider shall:

a) be impartial;
b) be responsible for decisions relating to its granting, maintaining, and revocation of certificates;
c) identify the management (committee, group or person) which shall have overall responsibility for all of the following:
   1) performance of verification and certification as defined in these General Requirements,
   2) formulation of policy matters relating to the operation of the Certification Service Provider,
   3) decisions on certification,
   4) supervision of the implementation of its policies,
   5) supervision of the finances of the body,
   6) delegation of authority to committees or individuals as required to undertake defined activities on its behalf,
   7) technical basis for granting certification;
d) have documents which demonstrate it is a legal entity;
e) have a documented structure which safeguards impartiality including provisions to ensure the impartiality of the operations of the Certification Service Provider; this structure shall enable the participation of all parties significantly concerned in the development of policies and principles regarding the content and functioning of the certification system;
f) ensure that each decision on certification is taken by a person or persons different from those who carried out the verification;
g) have rights and responsibilities relevant to its certification activities;
h) have adequate arrangements to cover liabilities arising from its operations and/or activities;
i) have the financial stability and resources required for the operation of a certification system;
j) employ a sufficient number of personnel having the necessary education, training, technical knowledge and experience for performing certification functions relating to the type, range and volume of work performed, under a responsible senior executive;
k) have a quality system giving confidence in its ability to operate certification services;
l) have policies and procedures that distinguish between certification services and any other activities in which the Certification Service Provider is engaged;
m) together with its senior executive and staff, be free from any commercial, financial and other pressures which might influence the results of the certification process;
n) have formal rules and structures for the appointment and operation of any committees which are involved in the certification process; such committees shall be free from any commercial, financial and other pressures that might influence decisions; a structure where members are chosen to provide a balance of interests where no single interest predominates will be deemed to satisfy this provision;
o) ensure that activities of related bodies do not affect the confidentiality, objectivity and impartiality of its certifications; the Certification Service Provider shall not provide any other products or services which could compromise the confidentiality, objectivity or impartiality of its certification process and decisions;
p) have policies and procedures for the resolution of complaints, appeals and disputes received from clients or other parties about the handling of certification or any related matters.

Guidance to clause 4.2

G.4.5 Accreditation shall only be granted to a body which is a legal entity as referenced in clause 4.2.d) of the General Requirements, and will be confined to declared scopes, activities and locations. If the activities of the Certification Service Provider are carried out by a legal entity which is part of a larger entity, the links with other parts of the larger entity shall be clearly defined and should demonstrate that no

conflict of interest exists, see guidance G.4.21 to G.4.23 inclusive. Relevant information on activities performed by the other parts of the larger entity shall be documented.

G.4.6 Demonstration that a Certification Service Provider is a legal entity, as required under clause 4.2.d) of the General Requirements, means that if a Certification Service Provider is part of a larger entity, accreditation shall only be granted to the entire legal entity. In such a situation, the structure of the entire legal entity may be subject to audit by the accreditation body in order to pursue specific audit trails and/or review records relating to the Certification Service Provider. The part of the legal entity that forms the actual Certification Service Provider may trade under a distinctive name, which should appear on the accreditation certificate.

G.4.7 For the purposes of clause 4.2.d) of the General Requirements, Certification Service Providers who are part of government, or are government departments, will be deemed to be legal entities on the basis of their governmental status. Such bodies' status and structure shall be formally documented and the body shall comply with all requirements of the General Requirements.

G.4.8 If the Certification Service Provider and its client are both part of government, the two bodies shall not directly report to a person or group having operational responsibility for both. The Certification Service Provider shall, in view of the impartiality requirement, be able to demonstrate how it deals with a case where both itself and its client are part of government. The Certification Service Provider shall demonstrate that the applicant receives no advantage and that impartiality is assured.

G.4.9 Impartiality and independence of the Certification Service Provider should be assured at three levels:

- Strategic and policy;
- Verification of identity.;
- Decisions on certification.

G.4.10 Impartiality, as required by clause 4.2.a) of the General Requirements can only be safeguarded by a structure, as required by clause 4.2.e) of the General Requirements, that enables "the participation of all parties significantly concerned in the development of policies and principles regarding the content and functioning of the certification system".

G.4.11 The structure required by the General Requirements, clause 4.2.e) for the safeguarding of impartiality shall be separate from the management established to meet the requirements of the General Requirements, clause 4.2.c), unless the entire management function is performed by a committee or group that is constituted to enable participation of all parties as required by the General Requirements, clause 4.2.e).

G.4.12 Clause 4.2.e) of the General Requirements is intended to counteract any tendency on the part of the owners of a Certification Service Provider to allow commercial or other considerations to prevent the consistent technically objective provision of its service. Conformity with this clause is particularly relevant when the finance to set up a Certification Service Provider has been provided by a particular interest, which predominates in the shareholding and/or the board of directors.

G.4.13 Clause 2.1.2.e) of the General Requirements requires that the documented structure of the Certification Service Provider has built into it provision for the participation of all the significantly concerned parties. This should normally be through some kind of committee. The structure established should be prescribed in the written constitution of the Certification Service Provider and should not be subject to change without notification to the accreditation body.

G.4.14 Application of clause 4.2.e) of the General Requirements requires judgement on whether all parties significantly concerned in the system are able to participate. What is essential is that all identifiable major interests should be given the opportunity to participate, and that a balance of interests, where no single

interest predominates, is achieved. The members should normally be chosen at least from among representatives of the following groups: customers and suppliers in industry and commerce, regulators, trade bodies, information security management professionals and related professionals, and government. For practical reasons there may be a need to restrict the number of persons.

G.4.15 On request of the committee or equivalent referred to in clause 4.2.e) of the General Requirements, the management responsible for the various functions described in clause 4.2.c) of the General Requirements should provide to that committee or equivalent all the necessary information, including the reasons for all significant decisions, actions, and the selection of persons responsible for particular activities in respect of certification, to enable the Certification Service Provider to ensure proper and impartial certification. If the advice of this committee or equivalent is not respected in any matter by the management, the committee or equivalent shall take appropriate measures, which may include informing the accreditation body.

G.4.16 The Certification Service Provider should be able to demonstrate that supervision of the finances of the body by the responsible management referred to in clause 4.2.c) has included actions to confirm conformity with clause 4.2.i) of the General Requirements.

G.4.17 Decisions to issue or revoke certificates may be taken by one authorized person within the Certification Service Provider or by more than one person, whereby either each person could take separate decisions independently of the others or the persons together could act as a committee. If decisions are taken by a committee, in accordance with clause 4.2.n) of the General Requirements, comprising among others representatives from one or more clients, the operational procedures of the Certification Service Provider should ensure that these representatives do not have a significant influence on decision making. This can for example be assured by the distribution of voting rights or some other equivalent means.

G.4.18 Clause 2.1.2.o) of the General Requirements addresses two separate requirements. First, the Certification Service Provider shall not under any circumstances provide any other products or services which could compromise the confidentiality, objectivity or impartiality of its certification process and decisions. Secondly, although there is no specific restriction on the services or activities a related body may provide, these shall not affect the confidentiality, objectivity or impartiality of the Certification Service Provider.

G.4.19 Activities under clause 4.2.o) of the General Requirements by a related body and certification should never be marketed together and nothing should be stated in marketing material or presentation, written or oral, to give the impression that the two activities are linked.

G.4.20 Nothing should be said by a Certification Service Provider that would suggest that certification would be simpler, easier or less expensive if any specified activities under clause 4.2.o) of the General Requirements were used.

G.4.21 A related body, as referred to in clause 4.2.o) of the General Requirements, is one which is linked to the Certification Service Provider by common ownership, in whole or in part, common directors, contractual arrangement, a common name, informal understanding or other means such that the related body has a vested interest in any certification decision or has a potential ability to influence the process.

G.4.22 The Certification Service Provider should analyze and document the relationship with related bodies to determine the possibilities for conflict of interest with provision of certification and identify those bodies and activities that could, if not subject to appropriate controls, affect confidentiality, objectivity or impartiality.

G.4.23 Certification Service Providers shall demonstrate how they manage their certification business and any other activities so as to eliminate actual conflict of interest and minimize any identified risk to impartiality. The demonstration shall cover all potential sources of conflict of interest, whether they arise from within the Certification Service Provider or from the activities of related bodies. Accreditation bodies

will expect Certification Service Providers to open up these processes for audit. This may include, to the extent practicable and justified, pursuit of audit trails to review records of both the Certification Service Provider and its related bodies for the activity under consideration. In considering the extent of such audit trails, account should be taken of the history of the Certification Service Provider with respect to impartial certification. If evidence of failure to maintain impartiality is found there may be a need to extend the audit trail back into the related bodies to provide assurance that control over potential conflicts of interest has been re-established.

G.4.24 Clause 4.2.c)1) of the General Requirements differentiates between verification and certification. Clause 4.2.f) of the General Requirements requires that each decision on certification is taken by a person or by persons different from those who carried out the verification.

G.4.25 The senior executive, staff and/or personnel mentioned in clause 4.2 of the General Requirements need not necessarily be full-time personnel, but their other employment shall not be such as to compromise their impartiality.

G.4.26 The Certification Service Provider should require all verification subcontractors or external verifiers to give undertakings regarding the marketing of any activities under clause 4.2.o) equivalent to those required by guidance G.4.19 and G.4.20.

G.4.27 The Certification Service Provider should be responsible for ensuring that neither related bodies, nor subcontractors, nor external verifiers operate in breach of the undertakings that they have given. The Certification Service Provider should also be responsible for implementing appropriate corrective action in the event that such a breach is identified.

G.4.28 The policies and procedures referred to in 4.2.p) of the General Requirements should ensure that all disputes and complaints are dealt with in a constructive and timely manner. Where operation of such procedures has not resulted in the acceptable resolution of the matter or where the proposed procedure is unacceptable to the complainant or other parties involved, the procedures of the Certification Service Provider shall provide for an appeals process. The appeals procedure should include provision for the following:

- the opportunity for the appellant to formally present its case;
- provision of an independent element or other means to ensure the impartiality of the appeals process;
- provision to the appellant of a written statement of the appeal findings including the reasons for the decisions reached.

The Certification Service Provider shall ensure that all interested parties are made aware, as and when appropriate, of the existence of the appeals process and the procedures to be followed.

5.4 Operations

The Certification Service Provider shall take all steps necessary to verify by appropriate means the identity of the individual, organization, or entity, and if applicable any specific attributes of the end entity (person, company, server, domain, IP address, etc), to which a qualified certificate is issued.
The Certification Service Provider shall specify the relevant requirements in the form of a publicly available Certification Practice Statement.

Guidance to clause 4.3

G.4.29 Verification of the identity of an individual shall be performed at a face-to-face meeting of the individual with an authorized verifier of the Certification Service Provider. The verifier shall check the identity of the individual by means of a valid official document issued by the appropriate authority in the

country where the individual resides. The document (e.g. passport, identity card, driver license, etc.) shall ensure the identity of the individual and shall include a photograph portrait of the individual. The Certification Service Provider shall keep a record concerning the document presented by the individual.

5.5 Subcontracting

When a Certification Service Provider decides to subcontract work related to the operation of its certification services to an external body or person, a properly documented agreement covering the arrangements including confidentiality and conflict of interest shall be drawn up.

The Certification Service Provider shall:
a) take full responsibility for such subcontracted work and maintain its responsibility for granting, maintaining, and revocation of certificates;
b) ensure that the subcontracted body or person is competent and complies with the applicable provisions of these General Requirements and other standards and guides relevant to the activities, and is not involved either directly or through the person's employer in providing other products or services which could compromise the confidentiality, objectivity or impartiality;
c) obtain the applicant's consent.

Notes
- Where work related to certification has been undertaken prior to the application for certification, the Certification Service Provider may take account of it, provided it can take responsibility as detailed in 4.4 a) and satisfy itself regarding the matters detailed in 4.4 b).
- The requirements given in 4.4 a) and b) are also relevant, by extension, when a Certification Service Provider uses, for granting its own certification, work performed by another Certification Service Provider with which it has signed an agreement.

Guidance to clause 4.4

G.4.30 A Certification Service Provider may issue certificates on the basis of subcontracted verification work carried out by another body, provided that the arrangement with the subcontracted body requires the subcontractor to comply with all relevant requirements of the General Requirements.

G.4.31 The Certification Service Provider shall have contractual arrangements in place for any sub-contracted body performing verification work. The Certification Service Provider shall specify the type of verification required, and shall be able to justify selection of the subcontractor. Where a Certification Service Provider certifies in accordance with guidance G.4.30, it shall have procedures that ensure conformity with all relevant clauses of the General Requirements by subcontracted bodies. If this assurance is based partly or in full on the accreditation of the subcontractor, the scope of accreditation should cover the activities to be carried out under the certification scheme and the Certification Service Provider shall have records available to show that it has checked the status of accreditation of the subcontractor.

G.4.32 Activities carried out by subcontracted bodies shall give the same confidence as those carried out by the Certification Service Provider itself. Evaluation of the verification work and the decision on certification shall be made only by the Certification Service Provider itself, and not by any other body. Where joint verification is undertaken, each Certification Service Provider shall satisfy itself that the whole of the verification has been satisfactorily undertaken by competent personnel.

G.4.33 The first note to clause 4.4 of the General Requirements describes a situation where the Certification Service Provider will be reliant on the verification work of another body. Such reliance needs to be supported by an evaluation of the work undertaken. The Certification Service Provider shall document such an evaluation.
The second note also describes a situation where the Certification Service Provider will be reliant on the verification work of another body. The Certification Service Provider should therefore ensure that information on any verification work on which it relies is updated as appropriate.

5.6 Quality system

4.5.1 The Certification Service Provider's management shall define and document its policy for quality and its objectives for, and commitment to, quality. The management shall ensure that this policy is understood, implemented and maintained at all levels of the organization.

4.5.2 The Certification Service Provider shall operate an effective quality system in accordance with the relevant elements of these General Requirements and appropriate for the type, range and volume of work performed. This quality system shall be documented and the documentation shall be available for use by the staff of the Certification Service Provider.
The Certification Service Provider shall ensure effective implementation of the documented quality system, procedures and instructions. The Certification Service Provider shall designate a person having direct access to its highest executive level who, irrespective of other responsibilities, shall have defined authority for:

a) ensuring that a quality system is established, implemented and maintained in accordance with these General Requirements and
b) reporting on the performance of the quality system to the provider's management for review and as a basis for improvement of the quality of the system.

4.5.3 The quality system shall be documented in a quality manual and associated quality procedures, and the manual shall contain at least the following:

a) a quality policy statement;
b) a brief description of the legal status of the Certification Service Provider, including the names of its owners and, if different, names of the persons who control it;
c) the names, qualifications, experience and terms of reference of the senior executive and other certification personnel, both internal and external;
d) an organization chart showing lines of authority, responsibility and allocation of functions stemming from the senior executive;
e) a description of the organization of the Certification Service Provider, including details of the management (committee, group or person) identified in 4.2 c), its constitution, terms of reference and rules of procedure;
f) the policy and procedures for conducting management reviews;
g) administrative procedures including document control;
h) the operational and functional duties and services pertaining to quality, so that the extent and limits of each person's responsibility are known to all concerned;
i) the procedure for the recruitment, selection and training of personnel of the Certification Service Provider and monitoring of their performance;
j) a list of its approved subcontractors and the procedures for assessing, recording and monitoring their competence;
k) its procedures for handling nonconformities and for assuring the effectiveness of any corrective and preventive action taken;
l) the procedures for evaluating identity and implementing the certification process, including
   1) the conditions for issue, maintaining and revocation of certificates,
   2) controls over the use and application of documents employed in the verification and certification process;
m) the policy and procedure for dealing with appeals, complaints and disputes;
n) its procedures for conducting internal audits, based on the provisions of ISO 10011-1.

Guidance to clause 4.5

G.4.34 Clause 4.5.3.i) of the General Requirements requires the Certification Service Provider to monitor the performance of its own personnel. In addition to other methods of monitoring performance, provision should be made, where applicable, for the periodic witnessing of those activities normally undertaken by personnel at its subcontractors.

G.4.35 The description required by clause 4.5.3.e) of the General Requirements should include an indication of which party or parties each member of a board or a committee is representing.

5.7 Conditions and procedures for granting, maintaining, and revocation of certificates.

4.6.1 The Certification Service Provider shall specify the conditions for granting, maintaining and revocation of certificates.

4.6.2 The Certification Service Provider shall have adequate procedures for granting, maintaining and revocation of certificates.

Guidance to clause 4.6

G.4.36 When the Certificate Service Provider decides to revoke a certificate, it shall publish the revocation information on a publicly available list for an appropriate period of time.

5.8 Internal audits and management reviews

4.7.1 The Certification Service Provider shall conduct periodic internal audits covering all procedures in a planned and systematic matter, to verify that the system is implemented and is effective.

The Certification Service Provider shall ensure that
a) personnel responsible for the area audited are informed of the outcome of the audit;
b) corrective action is taken in a timely and appropriate manner; and
c) the results of the audit are documented.

4.7.2 The Certification Service Provider's management with executive responsibility shall review the system at defined intervals which are sufficiently short to ensure its continuing suitability and effectiveness in satisfying the requirements of these General Requirements and the stated quality policy and objectives. Records of such reviews shall be maintained.

Guidance to clause 4.7

G.4.37 Clause 4.7 of the General Requirements does not mention a specific period in which internal audits and management review of the Certification Service Provider's quality system should take place. Internal audits followed by management reviews of the body's quality system should be carried out at least once each year.

G.4.38 The records of internal audits and management reviews should be made available to the accreditation body on request.

5.9

5.10 Documentation

4.8.1 The Certification Service Provider shall document, update at regular intervals, and make available (through publications, electronic media or other means) on request:

a) information about the authority under which the Certification Service Provider operates;
b) a documented statement of its certification system including its rules and procedures for granting, maintaining, and revocation of certificates;
c) information about the verification and certification process;
d) a description of the means by which the Certification Service Provider obtains financial support and general information on the fees charged to applicants and certified individuals and organizations;
e) a description of the rights and duties of applicants and certified individuals and organizations including requirements, restrictions or limitations on the use of the certification body's logo and on the ways of referring to the certification granted;
f) information on procedures for handling complaints, appeals and disputes;
g) a directory of certificates, describing the scope of certification granted to each.

4.8.2 The Certification Service Provider shall establish and maintain procedures to control all documents and data that relate to its certification functions. These documents shall be reviewed and approved for adequacy by appropriately authorized and competent personnel prior to issuing any documents following initial development or any subsequent amendment or change being made. A listing of all appropriate documents with the respective issue and/or amendment status identified shall be maintained. The distribution of all such documents shall be controlled to ensure that the appropriate documentation is made available to personnel of the Certification Service Provider when they are required to perform any function relating to the activities of the Certification Service Provider.

Guidance to clause 4.8

G.4.39 The information required by clause 4.8.1.c) of the General Requirements should clearly detail the precise basis of certification.

G.4.40 The description of the means by which the Certification Service Provider obtains financial support referred to in clause 4.8.1.d) of the General Requirements should be sufficient to show whether or not the body can retain its impartiality. The description (e.g. financial report) should also demonstrate that the body has sufficient resources to continue its operations.

5.11 Records

4.9.1 The Certification Service Provider shall maintain a record system to suit its particular circumstances and to comply with existing regulations. The records shall demonstrate that the certification procedures have been effectively fulfilled, particularly with respect to application forms, verification reports, and other documents relating to granting, maintaining, and revocation of certificates. The records shall be identified, managed and disposed of in such a way as to ensure the integrity of the process and confidentiality of the information. The records shall be kept for a period of time so that continued confidence may be demonstrated for at least one full certification cycle, or as required by law.

4.9.2 The Certification Service Provider shall have a policy and procedures for retaining records for a period consistent with its contractual, legal or other obligations.
The Certification Service Provider shall have a policy and procedures concerning access to these records consistent with 4.10.1.

Note: The question of the length of time for retention of records requires specific attention in the light of legal circumstances and recognition arrangements.

Guidance to clause 4.9

G.4.41 Certification records shall provide objective evidence of application handling, verification and decision processes having been fulfilled in compliance with the requirements and procedures of the Certification Service Provider.

G.4.42 The Certification Service Provider shall maintain records concerning each certificate issued during a specified period of retention and shall be able to produce such records readily on request of the accreditation body.

5.12 Confidentiality

4.10.1 The Certification Service Provider shall have adequate arrangements consistent with applicable laws to safeguard confidentiality of the information obtained in the course of its certification activities at all levels of its organization, including committees and external bodies or individuals acting on its behalf.

4.10.2 Except as required in these General Requirements or by law, information gained in the course of certification activities about a particular person or organization shall not be disclosed to a third party without the written consent of the person or organization concerned. Where the law requires information to be disclosed to a third party, the person or organization shall be informed of the information provided as permitted by the law.

6 Certification Service Provider personnel

6.1 General

5.1.1 The personnel of the Certification Service Provider shall be competent for the functions they perform.

5.1.2 Clearly documented instructions shall be available to the personnel describing their duties and responsibilities. These instructions shall be maintained up to date.

6.2 Qualification criteria

5.2.1 In order to ensure that verification and certification are carried out effectively and uniformly, the minimum relevant criteria for the competence of personnel shall be defined by the Certification Service Provider.

5.2.2 The Certification Service Provider shall require its personnel involved in the certification process to sign a contract or other document by which they commit themselves to comply with the rules defined by the Certification Service Provider, including those relating to confidentiality and independence from commercial and other interest.
The Certification Service Provider shall ensure that, and document how, any contracted personnel for their own part, and on the part of their employer if any, satisfy all the requirements for personnel outlined in these General Requirements.

5.2.3 Information on the relevant qualifications, training and experience of each member of the personnel involved in the certification process shall be maintained by the Certification Service Provider. Records of training and experience shall be kept up to date, in particular the following:
a) name and address;
b) organization affiliation and position held;
c) educational qualification and professional status;
d) experience and training in each field of the Certification Service Provider's competence;
e) date of most recent updating of records;
f) performance appraisal.

7 Changes in the certification requirements

The Certification Service Provider shall give due notice of any changes it intends to make in its requirements for certification. It shall take account of views expressed by interested parties before deciding on the precise form and effective date of the changes. Following a decision on, and publication of, the changed requirements, it shall verify that each certified person or organization makes any necessary adjustments within such time as, in the opinion of the Certification Service Provider, is reasonable.

8 Appeals, complaints and disputes

7.1 Appeals, complaints and disputes brought before the Certification Service Provider by clients or other parties shall be subject to the procedures of the Certification Service Provider.

7.2 The Certification Service Provider shall:
a) keep a record of all appeals, complaints and disputes, and remedial actions relative to certification;
b) take appropriate corrective and preventive actions;
c) document the actions taken and assess their effectiveness.

Guidance to clause 7

G.7.1 Personnel, including those acting in a managerial capacity, should not be deployed to investigate any appeal, complaint or dispute if they have been involved in activities as described under clause 4.2.o) of the General Requirements towards the appellant in question within the last two years.

G.7.2 Appeals, complaints and disputes represent a source of information as to possible nonconformity. On receipt of a complaint, the Certification Service Provider shall establish and, where appropriate take action on, the cause of any nonconformity found, including any predetermining (or predisposing) factors within the management system of the Certification Service Provider.

G.7.3 The Certification Service Provider should use such investigation to develop remedial / corrective action, which should include measures for:
- minimizing the consequences of any nonconformity;
- restoring conformity with requirements as quickly as practicable;
- preventing recurrence of the nonconformity;
- assessing the effectiveness of the remedial / corrective measures adopted.

o - o - o