KPMG

cutting through complexity™

ITS Global

Certificate Policy
KPMG Assurance Level: Low

OID: 1.3.6.1.4.1.26962.0.0.3.197.0

KPMG Certificate Services

KPMG International Cooperative

20-09-2013

This document contains 49 pages

Document review and approval

Revision history

Version	Author	Date	Revision
0.1	Martin Hilger	19-07-2006	Initial draft (document structure, draft content)
0.2	Martin Hilger	13-09-2006	Updated version
0.3	Martin Hilger / Jeff Carr	14-09-2006	Updated version
0.4	Martin Hilger	27-09-2006	Updated version
0.5	Martin Hilger	04-10-2006	Updated version
0.6	Martin Hilger	20-10-2006	Updated version
0.7	Martin Hilger	20-11-2006	Updated version
1.0	Martin Hilger	12-12-2006	Final review
1.1	Sander Visser	03-06-2009	Updated version and converted to new document template
1.2	Sander Visser	13-07-2009	Updated document based on feedback from Martin Hilger
1.2	Sander Visser	07-08-2009	Updated document based on feedback from Martin Hilger
2013-09-09a	Martin Hilger	09-09-2013	Converted to new template; changes and comments regarding Certificate Services Upgrade
2013-09-13a	Martin Hilger, Miguel Almeida	13-09-2013	Several updates
2013-09-16a	Martin Hilger, Miguel Almeida	16-09-2013	OCSP update
2013-09-20a	Martin Hilger, Miguel Almeida	20-09-2013	Removed all OCSP updates

This document has been reviewed by

	Reviewer	Date Reviewed
1.	Jeff Carr	14-09-2006
2.	Martin Hilger	28-07-2009
3.		
4.		
5.		

This document has been approved by

	Name	Date Approved
1.	Gertjan Koetsier	12-12-2006
2.	Darren Lovell	12-12-2006
3.	Martin Hilger	12-12-2006
4.	Reede Taylor	12-12-2006
5.		

Contents

1 Introduction

The structure of this document is based on the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practice Statement Framework covered in RFC3647.

This document defines the certificate policies for

Table 1: Certificate Types and Assurance Levels

Certificate Name	Enrollment	Purpose
KPMG User Authentication	Autoenrollment	KPMG User Network Authentication Used to authenticate the user and gain access to the KPMG wireless network infrastructure.
KPMG User Authentication-LoadRunner	Autoenrollment	KPMG User eAudit Authentication Used for load testing of eAudit, usually issued in bulk enrollments. Each certificate has a validity period of two weeks.
KPMG Computer Authentication	Autoenrollment	KPMG Computer Network Authentication Used to authenticate the KPMG computers and gain access to the KPMG wireless network infrastructure.
KPMG Computer Authentication v2	Autoenrollment	KPMG Computer Network Authentication This certificate is a variation of the general KPMG Computer Authentication Certificate, enhanced to support eAudit – it has both client and server authentication attributes.
KPMG Computer Authentication Extranet	Autoenrollment	KPMG Extranet Computer Network Authentication A variation of the KPMG Computer Network Authentication certificate for extranet machines. The request is based on command line commands.
KPMG Computer Authentication v2 Extranet	Manual enrollment	KPMG Extranet Computer Network Authentication A variation of the KPMG Computer Network Authentication v2 certificate for extranet machines. The request is based on command line commands.
KPMG Mobile Device User Authentication	Autoenrollment	KPMG User Authentication Used as a Group Certificate to authenticate users accessing KPMG resources using a mobile device.
KPMG Mobile Device Authentication	Manual enrollment	KPMG Device Authentication Used to authenticate KPMG mobile devices. It's used by SCEP to issue individual certificates to mobile devices.
KPMG Low Assurance Wireless Radius Server	Autoenrollment	KPMG Wireless Radius Server *Note: When private key exportable is no longer required for Radius this certificate type will be Medium Assurance*
KPMG Domain Controller Authentication	Autoenrollment	KPMG DC Computer Authentication Allows LDAP traffic to be implemented confidential and secure by using Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology (LDAP over SSL – or LDAPS).
KPMG ConfigMgr OSD Client	Manual enrollment	KPMG internal SCCM OSD Client Used during Operating System Deployment (OSD) when a client boots via PXE or boot media.

The term "assurance" is not intended to convey any representation or warranty as to the availability of CA services offered under the KPMG CS. System maintenance, system repair or factors outside the control of the CA may affect such availability. Member firms and ITS Global running Issuing CAs used for these certificate types do not represent or warrant availability offered under the KPMG CS.

KPMG Assurance Levels are described in the ”Technology Standards for Certificate Services”.

Note: Issuance of a public key certificate under any of these policies does not imply that the subscriber has any authority to conduct business transactions on behalf of the organization operating the CA.

Table 2: Relationship between this CP and other KPMG CS documentation

Relationship between this CP and other KPMG CS documentation
● This CP covers the policies of KPMG Low Assurance certificate types for all CAs participating in KPMG CS. This CP also specifies the responsibilities of participants within KPMG CS. ● Participating member firm Issuing CAs must create separate CPS documents that describe how they will meet the requirements of this CP and other related IT Standards, and how they will implement its practices and controls. ● CPS documents exist for (a) Root and Intermediate CAs and (b) Issuing CA servers in ITS Global and participating member firms. ● Additional supporting documentation is available in the form of IT Standards.

1.1 Overview

The certificates that will be issued under this Certificate Policy (CP) may only be used for verifying the identity of KPMG devices and KPMG users when accessing KPMG networks and other KPMG IT resources.

This Certificate Policy is intended for use by ITS Global and KPMG member firms. It is not intended for use by other organizations. Readers of this document should consult their Issuing Certification Authority if they require further details regarding implementation of this Certificate Policy.

1.2 Document Name and Identification

This Certificate Policy is assigned a unique Object Identifier (OID), which is carried in a standard extension field of an X.509 certificate. By inspecting this field, a Relying Party can verify whether a particular certificate will be suitable for the intended use.

Table 3: Document Name and Identification

Document Name and Identification	
Certificate Policy Name	KPMG Low Assurance
Object Identifier	1.3.6.1.4.1.26962.0.0.3.197.0
Published at	http://cs.ema.kpmg.com/cp/KPMG CS - Certificate Policy KPMG Low Assurance certificates.pdf

1.3 PKI Participants

This policy is designed specifically for KPMG CS infrastructure. Member firms must comply with both the Certificate Policy (herein) and all KPMG CS standards before they will be allowed to use KPMG CS.

1.3.1 Certification Authorities (CA)

Each member firm participating in the KPMG CS must provide Issuing CA services operating in compliance with the relevant CP documents and related IT Standards. Issuing CAs are responsible for: the creation and signing of certificates, binding Subscribers, KPMG CS personnel to the public signature verification keys attributable to them, providing a Certificate Repository and a Certificate Status Service (CSS), publishing a CPS that includes reference to this CP, and for the compliance with this CP by the CA itself.

A member firm may use a contractor to provide some of its operational services related to their CA, however member firms remain responsible and accountable at all times for the operation of their CA.

Note: Cross-certification is not permitted under this CP. However, member firms wishing to establish cross-certifications with external organizations may apply to the KPMG Policy Management Authority (PMA). This authority *is currently vested with ITS Global Enterprise Architecture.*

1.3.2 Registration Authorities (RA)

There is no explicit Registration Authority function defined within the scope of this CP. The KPMG CS Auto-enrollment technology does provide basic RA functionality for the purpose of issuing certificates under this CP.

1.3.3 Subscribers

A CA may only issue certificates to subscribers. KPMG CS has the following end entities as subscribers:

- KPMG users.
  - User Authentication (network authentication for the Global Desktop platform)
  - eAudit User Authentication (bulk certificates for eAudit load testing)
  - Mobile Device User Authentication (group certificate)
- KPMG devices.
  - Computer Authentication (client authentication issued to KPMG laptops and extranet computers)
  - Computer Authentication v2 (client and server authentication, WAN and eAudit. Available for KPMG laptops and extranet computers)
  - Radius Servers used for Wireless Authentication

Note: When private key exportable is no longer required for Radius this certificate type will be Medium Assurance

- Domain Controllers that will be configured to leverage Secure LDAP (LDAPS).
- Mobile Device Authentication (issued via SCEP)
- Configuration Manager OSC clients (for SCCM managed computers authentication)

1.3.4 Relying Parties

With respect to certificates issued under this CP, a Relying Party can only be a subscriber of the KPMG CS.

Individuals or organizations, other than subscribers, are not entitled to rely upon certificates issued by KPMG CS and, any such reliance is done at their own risk.

1.3.5 Other Participants

No stipulation.

1.3.6 Policy Applicability

Certificates issued under this policy relate to KPMG CS only.

1.4 Certificate Usage

The certificates contain public keys that match to private keys for device and user authentication. Certificates for network authentication are intended to be used in verification, authentication, and key agreement mechanisms.

1.4.1 Appropriate Certificate Usage

The certificates may be used for

- Network access to KNET, verifying the identity of KPMG users and devices,
- Mobile device integration and access to Personal Information Manager (PIM) services, verifying the identity of KPMG users and mobile devices,
- Computer access to the SCCM service,
- Wireless Radius Server authentication,
- Domain Controller authentication and encrypted LDAP communication (leveraging SSL/TLS)

1.4.2 Prohibited Certificate Usage

Certificates issued under this policy may not be used for any other purposes, either internally or externally including digital signing, application authentication or encryption.

1.5 Policy Administration

This CP is registered and maintained by ITS Global Enterprise Architecture group. This body will act as the KPMG Policy Management Authority (PMA) defined above, for KPMG CS.

Changes to this CP are subject to the processes defined under the KPMG IT Standards governance model.

All questions concerning this policy should be addressed to the following shared Distribution List:

GO-FM ITS Global Certificate Services (go-fmitsglobalcertif@kpmg.com)

1.6 Definitions and acronyms

1.6.1 Definitions

Activation data – Private data, other than keys, that are required when accessing cryptographic modules.

Certification Authority (CA) – An entity that is trusted to associate a Subject with a public and a private key pair. The CA links the key pair to the Subject by issuing a certificate for the Subject containing the public key as data.

CA Certificate – A certificate for the public key of one CA (the Subscriber CA) issued by another CA (the Issuer CA).

Certificate Management System (CMS) – The system used to issue and manage certificates.

CA System – The CMS and other systems used by a CA.

Certificate – The public key of a Subject, together with related information, digitally signed with the private key of the CA that issued the Certificate.

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certificate Renewal - The act or process by which the validity of the data binding asserted by an existing public key certificate is extended in time by issuing a new certificate. The binding of the public key to the subject and to other data items stays the same.

Certificate Re-key - The act or process by which an existing public key certificate has its public key value changed by issuing a new certificate with a different (new) public key.

Certificate Revocation List (CRL) – A list maintained by a CA of the certificates that it has issued that are revoked before their natural expiration time.

Certification path – An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) – A statement of the practices a CA employs in issuing and managing certificates.

Certificate Status Service (CSS) – The service provided through a CRL repository or an OCSS is jointly called the Certificate Status Service (CSS).

Cross-certification – The process undertaken by CAs to establish a trust relationship, confirmed when each CA issues a certificate for the public key of the other CA. When two CAs are cross-certified, they have agreed to trust and rely on each other's public key certificates and keys as if they had issued them themselves.

Cryptographic module – The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms.

Digital signature – The result of a cryptographic transformation of a message using a private key. A person who has the message and the signature can determine

1 If the signature was created using the private key of the alleged Subject and
2 If the message has been altered since the signature was created.

End Entity – A subscriber, Relying Party, or IT-system (that is not a CA or RA) that uses the keys and certificates created within a PKI.

Entity – An autonomous element within the PKI. This may be a CA, an RA or an end entity.

On-line Certificate Status Protocol (OCSP) – An on-line service that provides timely information regarding the revocation status of a certificate.

Private key – The private part of an asymmetric key pair used for public key encryption techniques. The private key is typically used for creating digital signatures or decrypting messages.

Policy Management Authority (PMA) – A PKI body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs. The ITS Global Enterprise Architecture is assigned responsibility for this role.

Policy CA – A CA assigned by the PMA to sign the CA-certificates of the Tier 3 CAs of the PKI.

Public key – The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages sent to the owner of the private key.

Public Key Infrastructure (PKI) – The entire set of organizations, practices, processes, server platforms, software, and workstations used for the purpose of administering policies, certificates and keys.

Registration Authority (RA) – An entity that has received the responsibility from the CA to identify and authenticate subscribers and to verify their authority to act on behalf of the Subject. The RA does not sign or issue certificates. (For this specific CPS there is no explicit RA function).

Relying Party – A recipient of a certificate who acts in reliance on that certificate and/or a digital signature verified using that certificate.

Repository – A system for storing and distributing certificates or other information relevant to certificates.

Secret key – A key used in symmetric encryption where the sender and receiver of encrypted messages use the same secret key.

Set of provisions – A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Sponsor – A Sponsor is an organizational unit or officer with the authority to nominate a person to be a subscriber of certificates.

Subject – A certificate is assigned to a Subject. The Subject can be the subscriber of the certificate or an organizational role or IT-system for whom the subscriber is responsible and accountable.

Subscriber – The individual to whom the public key certified in a certificate is attributable. Each subscriber must have a Sponsor in the Organization issuing the certificate.

1.6.2 Acronyms

Table 4: Acronyms

Acronym	Abbreviation
cc	country
CA	Certification Authority
CASO	Certification Authority Security Officer
CASA	Certification Authority System Administrator
CAO	Certification Authority Operator
CMS	Certificate Management System
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CS	KPMG Certificate Services
CSS	Certificate Status Service
DC	Domain Component
DN	Distinguished Name
EE	End entity
I&A	Identification and Authentication
IDM	ITS Global Identity Management Team
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
KNET	KPMG Internal Network
KPMG CS	KPMG Certificate Services
O	Organization
OU	Organizational Unit
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PMA	Policy Management Authority
PSE	Personal Security Environment
RA	Registration Authority
RFC	Request for Comments
RSA	A specific Public key algorithm
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1.7 Referenced Documents

Referenced Documents	
Document	**Source**
IT Standard - Technology Certificate Services	KPMG
IT Standard - Technology Network Operating System	KPMG
IT Standard - Specification Desktop Disk Encryption	KPMG
Security Requirements for Log Management	KPMG
Security Requirements for Data Centers	KPMG

2 Publication and Repository Responsibilities

2.1 Repositories

- The CA is responsible for maintaining a CA Repository for publishing certificates, CRLs as well as CP/CPS documents. Certificates and Certificate Status Service must be available to Relying Parties. Therefore, the CA Repository must be available for a high proportion of every 24-hour period.
- The KPMG IT Standards web site will be used for publication of all CS standards documents.

2.2 Publication of Certification Information

These services or parts thereof may be operated by a separate organization or team on behalf of KPMG CS. A CA must:

- Include the URL of the KPMG CS Repository within any certificate it issues.
- Ensure the publication of its CP and its CPSs referencing this policy, digitally signed by an authorized representative of the CA, on the KPMG CS Repository Web Site.
- Ensure that previous versions of the CP and the CPS documents related to KPMG CS are available on KNET.
- Provide a full text version of the CPS when necessary for the purposes of any audit, inspection, or accreditation.
- Publish the address and other relevant access information for its CSS on the KPMG CS Repository Web Site.
- Publish signed CRLs in the KPMG CS repository.
- Ensure that CRLs, CA-certificates and other published certificates are available firmwide in the KPMG CS Repository.
- Ensure that access controls are configured so that only authorized CA personnel can modify the CA Repository.

The CA shall provide relevant information about issued certificates when necessary.

Note: No personally identifiable information above the content needed for authentication should be collected by CAs related to KPMG CS for use in these certificate types.

2.3 Time or Frequency of Publication

- Upon issuance, CA certificates and other certificates must be published promptly in the CA Repository.
- CRLs will be published based on the publishing intervals described in the CPS.
- In case of key compromise CRLs must be created, approved and published immediately.
- When new document versions are made available, these will be reviewed and approved via the IT Standards process prior to being published.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

In accordance with PKIX[1], each Subject must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate Subject Name field. Each Subject may also have alternative names in the Subject AltName extension field.[2]

The DN must be in the form of a X.501 UTF8String and must not be blank.

3.1.2 Need for names to be meaningful

The contents of each certificate Subject Name and Issuer Name fields must be attributable to the authenticated name of the Subject and Issuer. It is recommended that the organization Name component is included in the DN. The organization name must be the official name of the organization.

3.1.3 Anonymity or Pseudonymity of Subscribers

Subscribers must not be anonymous or pseudonymous.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

DNs must be unique among all entities of KPMG CS. For each entity, additional numbers or letters may be appended to the Common Name to ensure the uniqueness of the DN. The capability of Unique Identifier fields to differentiate subscribers with identical names will not be supported.

3.1.6 Recognition, authentication and role of trademarks

The KPMG CS Manager via the IT Standards process reserves the right to make all decisions regarding entity names in all issued certificates.

Role of trademarks: no stipulation, not applicable for these certificate types.

[1] ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459]

[2] The CPS states whether an alternative name of a particular form will be included in the certificate.

3.2 Initial Identity Validation

No specific identity validation for end entities will be carried out under this policy. For the purpose of this policy, existing mandatory HR and IT processes will be considered adequate to provide identification of the individual (for user certificates) and equipment identity (for device certificates).

3.2.1 Method to Prove Possession of Private Key

No stipulation.

3.2.2 Authentication of Organization Identity

No stipulation.

3.2.3 Authentication of Individual Identity

Devices and users are eligible for the respective certificates based on the existence of a valid directory object for the relevant device or user. The relevant CA must keep a record of the type and details of identification used.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The request for renewal of a certificate may only be made by the subscriber (i.e. the subscribed user or device). The CA must authenticate a request for renewal, and the subscriber must authenticate the subsequent response. This may be done by an online method as described in the CPS. A subscriber requesting renewal of a certificate may authenticate the request using the keys corresponding to its valid certificate. When the certificate has expired the request for renewal must be authenticated in the same manner as the initial application of a certificate.

3.3.2 Identification and Authentication for Re-Key after Revocation

When the information contained in a certificate has changed or there is a known or suspected compromise of the private key, a CA must authenticate a request for renewal in the same way as an initial request. The CA must verify any change of the information contained in a certificate before the certificate is issued.

3.4 Identification and Authentication for Revocation Request

The CA must authenticate a request for revocation of a certificate. The CA must establish and make publicly available in its CPS the process by which it addresses such requests and the means by which it will establish the validity of a request.

Requests for revocation of certificates must be logged.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The CA must ensure that all procedures and requirements with respect to an application for a certificate are set out in the CPS. Bulk applications on behalf of subscribers are accepted only from sponsors.

4.1.1 Who Can Submit a Certificate Application

An application for a certificate where a person is the prospective subject and subscriber may be made by the person or by another individual or organization authorized to act on behalf of the prospective subscriber. The application may also be made by the CA, an RA, or by a sponsor coordinating the establishment of an organizational network.

An application for a certificate, where an organization, organizational role or IT-system is the prospective Subject, may be made by a prospective subscriber if the signature of the prospective Subject is attributable to the prospective subscriber for the purposes of accountability and responsibility.

The CA must ensure that each application is done on the basis of an existing network directory object associated with the relevant device or user.

The decision of whether to issue a certificate is at the sole discretion of the CA.

4.1.2 Enrollment Process and Responsibilities

Any information required by the CA in connection with a certificate application must be complete and accurate.

Subscribers must protect their private keys (personal private keys and private keys for Subjects attributable to them) and must take all reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

Relevant user and device certificates must be protected by the KPMG IT Standard - Specification Desktop Disk Encryption.

The subscriber shall use the private keys of subjects attributable to the subscriber only for the purposes identified in the CP.

When a subscriber suspects private key compromise, the subscriber must immediately notify the CA that issued the certificate in a manner specified by that CA.

4.2 Certificate Application Processing

The issuance of a certificate by a CA indicates a complete and final approval of the certificate application by the CA.

4.3 Certificate Issuance

Certificate types under this CP are typically enrolled automatically (exceptions as noted in section 1) therefore no formal acceptance of a certificate is required.

Each member firm that subscribes to the KPMG CS is responsible for the communication and user acceptance for the certificates covered within this CP (Subscriber Agreement).

After all application and approval processes identified in this policy are completed, the Issuing CA will issue the requested certificate to the relevant device or user. There will be no formal notification of the Certificate's issuance.

The procedure used to deliver or make the certificate available to the applicant must be secure and confidential.

4.4 Certificate Acceptance

No stipulation.

4.5 Key Pair and Certificate Usage

These certificate types may not be used for purposes counter to the principles and applications outlined in this CP. Every person using a certificate issued for signing and encryption within the framework of this CP:

- Must verify the validity of the certificate before using it.
- Must use the certificate solely and exclusively for authorized purposes in accordance with this CP.

4.6 Certificate Renewal

Certificate renewal is the act or process of issuing a new certificate to the subscriber by the relevant Issuing CA without changing the old key pair.

The information contained in the certificate must not be changed or modified and there must be no suspicion of compromise to the private key.

The other data items are changed, and the old certificate is revoked, as required by the CPS to support the renewal. If changes go beyond that, the process is a “certificate re-key”.

4.6.1 Circumstances for Certificate Renewal

Application for certificate renewal for user and device certificates under this CP can only be made if the certificate has not yet reached the end of its validity period, and has not been revoked.

4.6.2 Who May Request Renewal

Only the subscriber may request renewal of a certificate.

4.6.3 Processing Certificate Renewal Requests

The processing of certificate renewal requests is conducted in accordance with the provisions of section 4.3 Certificate Issuance. The provisions of section 3.3.1 Identification and Authentication for Routine Re-Key govern the procedures for identification and authentication for certificate renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

The provisions of section 4.3 Certificate Issuance apply.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The provisions of section 4.4 Certificate Acceptance apply.

4.6.6 Publication of the Renewal Certificate by the CA

The provisions of section 4.4 Certificate Acceptance apply.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The provisions of section 4.4 Certificate Acceptance apply.

4.7 Certificate Re-Key

Certificate re-key is the act or process by which an existing certificate has its public key value changed by issuing a new certificate with a different public key. The essence of re-key is that the subject stays the same and a new public key is bound to that subject. Other changes could be made or the old certificate is revoked as required by the CPS and related IT Standards in support of the re-key.

The provisions of section 4.6 Certificate Renewal apply here, with the exception that a new key pair will be used.

4.7.1 Circumstances for Certificate Re-Key

A request for new key certification may be made to expedite certification of a new key pair to

- Replace an existing certificate revoked for a reason other than key compromise.
- Replace an existing certificate revoked for key compromise.

4.7.2 Who May Request Certification of a New Public Key

The Certificate Manager and the end entity may request certification of a new key.

4.7.3 Processing Certificate Re-Keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificates must not be modified. If a change is needed to a certificate, the old certificate must be revoked, and a new certificate must be requested.

4.8.1 Circumstances for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

Certificates must be revoked whenever a CA declares that a previously valid certificate issued by that CA has become invalid; usually stated with a revocation date.

A revocation is announced to potential certificate users by issuing a CRL that mentions the certificate. Revocation and listing on a CRL is only necessary before certificate expiration.

Once a certificate has been revoked, it may not be renewed or extended.

4.9.1 Circumstances for Revocation

An Issuing CA must revoke an end entity certificate when:

- Any of the information in the certificate changes.
- Upon suspected or known compromise of the private key.
- A subscriber or a subject fails to comply with obligations set out in this CP, the relevant CPS, or a Subscriber Agreement.
- A subscriber no longer needs a certificate.
- The CA service is discontinued.
- Relevant CA keys have been compromised.
- Upon request from the subscriber.

Note: when using autoenrollment the revocation of a certificate will result in the automatic enrollment of a new certificate. If the purpose of the revocation is to discontinue a user from using a service the relevant network directory object must either be disabled or have its membership modified (based on existing IT and/or HR processes).

4.9.2 Who Can Request Revocation

The revocation of this certificate type may only be requested by:

- The subscriber in whose name the certificate was issued (acceptance of a revocation request of a certificate is conditional on the successful identification and authentication of the subscriber in accordance with section 3.4 Identification and Authentication for Revocation Request.
- The Sponsor.
- Personnel of the CA.

Revocation of certificates may only be done by the relevant CA. The CA is also allowed to revoke certificates, in case of compromise of a key.

4.9.3 Procedure for Revocation Request

A CA must ensure that all additional procedures and requirements with respect to revocation are set out in the CPS i.e.:

- An authenticated revocation request, and any resulting actions taken by the CA, must be recorded and retained.
- When a certificate is revoked, full justification for the revocation must also be documented.
- When a certificate is revoked, the subscriber may not be informed.
- The revocation shall be published in the CSS.

4.9.4 Revocation Request Grace Period

Should circumstances for revocation of a certificate exist (see section 4.9.1 Circumstances for Revocation), the subscriber must advise the relevant CA immediately, and request revocation of the certificate.

Any action taken as a result of a request for revocation of a certificate must be initiated as soon as possible.

4.9.5 Time within which CA Must Process the Revocation Request

The CA must react as soon as possible but within one working day, to any revocation request received for an end entity certificate under this policy.

4.9.6 Revocation Checking Requirements for Relying Parties

The provisions of section 4.5 Key Pair and Certificate Usage apply. In addition:

- A Relying Party must, before their use, check the status of all certificates in the certificate validation chain against the current CRLs whenever possible.
- A Relying Party must also verify the authenticity and integrity of CRLs whenever possible.

4.9.7 CRL Issuance Frequency

Requirements documented in existing HR and IT processes as well as the high level requirements of section 2.3 Time or Frequency of Publication apply.

4.9.8 Maximum Latency for CRLs

CRLs must be deployed without delay.

4.9.9 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re Key Compromise

Should a private key become compromised, the certificate affected must be revoked immediately.

Should the private key of the relevant CA become compromised, all certificates issued by the CA shall be revoked.

In any key compromise situation, a report must be sent to the Certificate Manager identifiable through the CPS of the relevant CA.

For any CA compromise the KPMG CS Manager and ITS Global Information Security Office must be informed.

4.9.13 Circumstances for Suspension

No stipulation.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The CA shall publish CRLs and certificates on the approved CRL distribution points and AIA locations as per the definitions in the relevant CPS.

4.10.2 Service Availability

CRLs must be available 24/7.

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

- End of subscription is defined by the period of validity as indicated in the certificates under this CP.
- The certificates expire automatically.
- If necessary the certificates can be revoked by the user or the CA.

4.12 Key Escrow and Recovery

No stipulation.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

CPS documents for related CA servers must describe the following physical controls:

- Physical security controls to control access to the CA site.
- Manual or electronic monitoring for intrusion at all times.
- Access to the CA site.
- A site access log.
- Involved removable media and paper containing sensitive plain text information.

The CPS must also include

- A description of the physical CA site. Overall the relevant CA site must be compliant with KPMG *Security Requirements for Data Centers* (as published on the IRSO portal), guidelines and policies.
- Controls for handling of activation data.

A CA must ensure that facilities used for off-site back-up, have the same level of security controls as the primary CA site.

5.2 Procedural Controls

"KPMG CS Processes" describes the approved Role Model for the Assurance Level Model for KPMG CS.

5.2.1 Trusted Roles

No stipulation.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

Personnel controls must be based on ITS Global recommendations and documented in the CPS of the relevant CA.

5.3.1 Qualifications, Experience, and Clearance Requirements

Please refer to the CPS of the relevant CA.

5.3.2 Background Check Procedures

All staff being assigned certificates is subject to normal HR processes and additionally may undergo background check procedures.

5.3.3 Training Requirements

No stipulation.

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions must be identified by the relevant CPS for any unauthorized actions or other violations of KPMG policies and procedures. Disciplinary actions to be considered could include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

Any involvement of independent contractors must be accompanied with:

- Formal Non-Disclosure and Confidentiality Agreements.
- Individual background checks.

5.3.8 Documentation Supplied to Personnel

A CA must make the following documentation available to its subscribers:

- CPs about supported certificate types.
- CPS for all involved CA servers.

5.4 Audit Logging Procedures

The security audit procedures must be compliant with audit procedures defined and approved for KPMG CS and are valid for all KPMG CS-system components.

Please note that where no specific or deviating rules are defined the KPMG “Security Requirements for Log Management” apply.

5.4.1 Types of Events Recorded

Types of events recorded must be in line with audit parameters defined and approved for KPMG CS (see also “KPMG CS Processes”). Additional types may be covered by the relevant CA’s CPS.

5.4.2 Frequency of Processing Log

Frequency of Log processing must be described in the CPS. In general audit logs must be:

- Checked at least quarterly.
- Checked following an alert or anomalous event.

5.4.3 Retention Period for Audit Log

No stipulation.

5.4.4 Protection of Audit Log

Protection of audit logs including manual logs must be described in the CPS. In general audit logs must be appropriately secured to prevent unauthorized viewing, modification, and deletion or other tampering, via the implementation of appropriate physical and logical access controls.

5.4.5 Audit Log Backup Procedures

Audit Log backup procedures must be described in the CPS. In general audit logs and audit summaries must be backed up or copied if in manual form.

5.4.6 Audit Collection System (Internal vs. External)

The audit collection system must be described in the CPS.

5.4.7 Notification to Event-Causing Subject

Notification to event-causing subject will be handled according to the CPS.

5.4.8 Vulnerability Assessments

Vulnerability Assessments will be handled according to the CPS.

In general the relevant CA must be monitored on a 24/7 basis. All unauthorized access attempts must be logged and analyzed.

5.5 Records Archival

No stipulation.

5.6 Key Changeover

No stipulation.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Incident and Compromise Handling Procedures must be identified in the CPS.

In general if the keys of an end entity are lost or compromised, the CA must be informed immediately in order to revoke the certificate.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

The CPS must contain provisions for handling computing resources, software, and/or data corruption.

In general the business owner must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. When a repository is not under the control of the CA, the CA must ensure that any agreement with the repository provides that business continuity procedures be established and documented by the repository.

5.7.3 Entity Private Key Compromise Procedures

Entity private key compromise procedures must be described in the CPS.

In general in case of a compromise of an end entity private key a CA must immediately:

- Request revocation of the relevant certificate issued by the CA.

- Provide appropriate notice.

After addressing the factors that led to key compromise, the CA may generate a new end entity key pair.

5.7.4 Business Continuity Capabilities after a Disaster

A disaster recovery plan must be created for all CAs pertaining to KPMG CS outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. When a repository is not under the control of the CA, the CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

5.8 CA or RA Termination

Termination of a CA is regarded as the situation when all service associated with a logical CA is terminated permanently. This is not the case when the service is transferred from one organization to another, or when the CA-service is passed over from an old CA-key to a new CA-key.

In the event that a CA ceases operation, it must notify its subscribers immediately upon the termination of operations and arrange for the continued retention of the CA’s keys and information. It must also terminate the CSS.

In the event of a change in management of a CA’s operations, the CA must notify all entities for which it has issued certificates.

In the event of a transfer of a CA’s operations to another CA operating at a lower level of assurance, the certificates issued by the CA whose operations are being transferred must be revoked through a CRL signed by that CA prior to the transfer, and terminate the CSS.

The CA archives must be retained in the manner and for the time indicated in section 5.5 Records Archival.

6 Technical Security Controls

This section contains provisions of the public/private key pair management policy for end entities, and the corresponding technical controls.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pair for each subscriber must be generated using the approved Cryptographic Service Providers.

6.1.2 Private Key Delivery to Subscriber

If the prospective certificate holder does not generate the private signing key, KPMG CS shall place the key in storage in a manner that ensures that only the prospective certificate holder has access to it.

6.1.3 Public Key Delivery to Certificate Issuer

No stipulation.

6.1.4 CA Public Key Delivery to Relying Parties

The certificate containing a CA's public signature verification key shall be delivered to subscribers and Designated Certificate Holders, in a secure manner, as documented in the CPS.

6.1.5 Key Sizes

Minimum key size: 1024 bits

Note: it is recommended that Wireless Radius Server and Domain Controller Authentication leverage bigger key sizes.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The purposes for which a key can be used must be restricted by the CA through the Key Usage extension in the certificate. This is a field that indicates the purpose for which the certified public key is used. The certificate must not be used for other purposes than described in this CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The subscriber must protect its private keys from disclosure. When not active, the private key must be stored in encrypted form to protect it from unauthorized use.

As far as cryptographic module controls are concerned please see “IT Standard Process – Certificate Services”.

6.2.1 Cryptographic Module Standards and Controls

No stipulation.

6.2.2 Private Key (n out of m) Multi-Person Control

No stipulation.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

A participant will not be able to backup his/her private key as private keys will be marked as not exportable. However end entity certificates may be subject to local member firm backup procedures or a future global standard for PC Backup.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

No stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

An end entity must be authenticated to the PSE before the activation of the private key.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All Certificates and corresponding keys must have maximum validity periods assigned:

Validity periods for keys are:

Table 5: Certificate Operational Periods and Key Pair Usage Periods

Validity periods	
End-Entity Keys for network user authentication (1024 bits)	1 (one) year
End-Entity Keys for network user authentication-LoadRunner (1024 bits)	2 (two) weeks
End-Entity Keys for network device authentication (1024 bits)	1 (one) year
End-Entity Keys for network device authentication v2 (1024 bits)	1 (one) year
End-Entity Keys for network device authentication (extranet) (1024 bits)	1 (one) year
End-Entity Keys for network device authentication (extranet) v2 (2048 bits)	2 (two) years
End-Entity Keys for mobile device authentication (2048 bits)	2 (two) years
End-Entity Keys for mobile device user authentication (1024 bits)	2 (two) years
End-Entity Keys for low assurance wireless radius server auth. (1024 bits)	1 (one) year
End-Entity Keys for Domain controller authentication (2048 bits)	1 (one) year
End-Entity Keys for Configuration Manager OSD clients' auth. (1024 bits)	2 (two) years

Certificates and keys must not be used after the expiration of the validity periods indicated in this section.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The following requirements apply:

- All KPMG end user (desktop, notebooks) devices under this CP holding user or computer certificates must be equipped with the IT Standard - Specification Desktop Disk Encryption.
- Radius Servers leveraging the relevant device certificate must be compliant with the approved KPMG IT Standards for Wireless technologies and other relevant documentation.
- Domain Controllers and other servers leveraging the relevant device certificates must be compliant with approved KPMG IT Standard - Technology Network Operating System and other relevant documentation.
- Mobile devices managed by an approved mobile device management solution

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

All end entity certificates must reside on approved and supported KPMG OS and application platforms.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The KPMG CS and end entity devices must be protected from attack through any open or general purpose network with which it is connected. Such protection must be provided through the installation of a device configured to allow only the protocols and commands required for the operation of the KPMG CS.

6.8 Time-Stamping

All time stamping of entries created on online CA servers and subscribers must be based on the network time provided by standard time setup of the domain (DC provides the clock for its own domain).

7 Certificate, CRL, and OCSP Profiles

This section specifies the certificate format and the CRL format. Further coding conventions and other specific information regarding the content of required and recommended fields and extensions in certificates and CRLs shall be specified in the CPS.

7.1 Certificate Profile

Certificates will include a reference to the OID for the certificate type identified by this CP within the appropriate field. The CPS or other publicly available document will identify the certificate extensions supported, and the level of support for those extensions.

7.1.1 Version Number(s)

The CA must issue X.509 Version 3 certificates, in accordance with the PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459]. End entity software must support all base (non-extension) X.509 fields.

The values of the base (non-extension) X.509 fields shall be:

Table 6: Certificate base (non-extension) X.509 fields

Field Comment	Content
Version	Version of X.509 certificate, version is 3 (value is 2).
Signature algorithm	sha1RSA (the algorithm used by the CA to sign the certificate).

Issuer	X.501 type distinguished name of CA (CN). It is recommended that the organization name component is included in the name.
	<u>Example:</u>
	CN = KPMG Internal Issuing CA GO01
	C=GO
	ST= Amsterdam
	L= Global Data Centre
	O=KPMG Internal Certificate Services
	OU=KPMG High Assurance CA
	E=go-fmitsglobalcertif@kpmg.com

Validity	Valid from / valid to: The first and last date in the validity period for the certificate.
Subject	Subject name is built from directory information. User certificates: Common Name = UPN Computer certificates: Common Name = DNS name
Public Key	RSA (minimum 1024 Bits – refer to section 6.3.2)

7.1.2 Certificate Extensions

No extension will modify or undermine the use of X.509 base fields.

The following table specifies the values of required certificate extensions and recommends values for some recommended extensions.

Table 7: Certificate Extensions

Extension	Content
Key Usage	End entity certificate options: Digital Signature, Non-Repudiation, Certificate signing, CRL signing. User certificates: Digital Signature Computer certificates: Digital Signature, Key Encipherment (a0)
Application policies	Options as per KPMG CS software. Defined option: ● Client Authentication; or ● Client Authentication and Server authentication, depending on the type of certificate.
Issuance policies	Defined option: ● KPMG Low Assurance (http://cs.ema.kpmg.com/cp/KPMG CS - Certificate Policy KPMG Low Assurance.pdf).
Subject Alt Name	Computer certificate: DNS Name. User certificate: UPN
CRL Distribution Point	KPMG Internal Issuing CA <CC><CN> Example for ITS Global Issuing CA: http://cs.ema.kpmg.com/CRL/KPMG%20Internal%20Issuing%20CA%20GO01.crl ldap:///CN=KPMG%20Internal%20Issuing%20CA%20GO01,CN=<servername>,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=kworld,DC=kpmg,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
Authority Information Access (AIA)	KPMG Internal Issuing CA <CC><CN> Example for ITS Global Issuing CA: http://cs.ema.kpmg.com/CRT/KPMG%20Internal%20Issuing%20CA%20GO01.crt ldap:///CN=KPMG%20Internal%20Issuing%20CA%20GO01,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=kworld,DC=kpmg,DC=com?cACertificate?base?objectClass=certificationAuthority

If further extensions are used, their values and whether they are critical or not shall be specified in the CPS.

7.1.3 Algorithm Object Identifiers

The CA must use and end entities must support, for authentication, the following algorithms:

- RSA – {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 };
- SHA-1 – sha1WithRSAEncryption, {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }.

The CA only issues certificates for keys for these algorithms.

In addition, the CA and end entities must support the algorithms approved by PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459] for verification.

7.1.4 Name Forms

Each DN must be in the form of an X.501 UTF8String.

7.1.5 Name Constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all certificates.

7.1.6 Certificate Policy Object Identifier

The Issuing CA must ensure that the Policy OID is contained within the certificates it issues.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The Issuing CA must populate the Policy Qualifiers extension with the URL of its CP.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

End entity software must support and correctly process the CRL fields and extensions identified in chapter 5 of PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459] as prescribed in the same document.

7.2.1 Version Number(s)

A CA must issue X.509 Version 2 CRLs, in accordance with the PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459].

The values of the fields and entry fields of the X509 Version 2 CRL shall be:

Table 8: CRL Fields

CRL Field Comment	Content
Version	Version of X.509 CRL, version is 2 (value is 1)
Signature and Signature Algorithm	sha-1RSA

Issuer	X.501 type distinguished name of CA (CN). It is recommended that the organization name component is included in the name.
	Example:
	CN = KPMG Internal Issuing CA GO01
	C=GO
	ST= Amsterdam
	L= Global Data Centre
	O=KPMG Internal Certificate Services
	OU=KPMG High Assurance CA

CRL Field Comment	Content
	E=go-fmitsglobalcertif@kpmg.com
Effective date	Date published
Next update	21 days from date published (base CRLs) 10 days from date published (delta CRLs)
Revocation list	**Content**
Revoked Certificate	Serial number of revoked certificate
Revocation Date	Date of revocation

7.2.2 CRL and CRL Entry Extensions

All PKI user software must correctly process all CRL extensions and CRL entry extensions identified in PKIX ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [RFC2459].

The following table gives the stipulations for the extensions and entry extensions:

Table 9: CRL and CRL Entry Extensions

CRL Extension Comment	Content
CRL Number	Sequence number of CRL.
Delta CRL Indicator	Minimum Base CRL Number: contains the sequence number of the base CRL if this CRL is a delta CRL.

7.3 OCSP Profile

No stipulation.

8 Compliance Audit and Other Assessments

A compliance inspection determines whether the CA's performance meets the requirements established by Certificate Policies and Certificate Practice Statements associated with KPMG CS.

8.1 Frequency and Circumstances of Assessment

All CAs shall be subject to a periodic compliance audit which must be carried out at least once per year.

Alternative reviews may be substituted for full compliance audits under the following exceptional circumstances:

- If no changes to policies, procedures, or operations have occurred during the previous year, an assertion to that effect, signed by the cognizant executive, is acceptable instead of a full compliance audit.
- If no significant changes to policies, procedures, or operations have occurred during the previous year, a delta compliance audit is acceptable instead of a full compliance audit.
- However, a full compliance audit must be completed every third year regardless.

8.2 Identity/Qualifications of Assessor

The following information is required from the Assessor:

- Identity of the Auditor.
- Competence of the Auditor to perform audits.
- Experience of the Auditor in auditing PKI systems.
- Familiar with the requirements for the KPMG CS on the issuance and management of certificates.

8.3 Assessor's Relationship to Assessed Entity

This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the KPMG CS.

8.4 Topics Covered by Assessment

The compliance audit for all CAs shall verify that the Operational Authority that is implementing all provisions of the relevant CPS (consistent with this CP) is clearly identified.

A full compliance audit for all CAs covers all aspects within the scope identified above.

Where permitted by section 8.1 Frequency and Circumstances of Assessment, a delta compliance audit in lieu of the full compliance audit may be performed. A delta compliance audit covers all changes to the technical infrastructure, policies, procedures, or operations that have occurred during the previous year. For delta compliance audits all executed changes must be reviewed to confirm that changes have been handled in accordance with the requirements outlined in the relevant IT Standards and KPMG CS documentation. Additionally there must be a complete audit trail of any change (i.e. changes tested in an isolated test environment, test results signed off by 2 individuals, changes to any KPMG CS component as per defined change management procedures).

Additionally the following topics must be addressed in a delta compliance audit even if no changes have occurred since the last full compliance audit:

1 Personnel controls.

2 Separation of Duties.

3 Audit review frequency and scope.

4 Types of events recorded in physical and electronic audit logs.

5 Protection of physical and electronic audit data.

6 Physical security controls.

7 Backup and Archive generation and storage.

8 CA Key Life Cycle Management.

9 Certificate Life Cycle Management.

8.5 Actions Taken as a Result of Deficiency

The inspection results will be submitted to the relevant CA's Manager, the KPMG CS Manager and ITS Global Information Risk and Security Office (IRSO). If irregularities are found, the CA will submit a report for review to the CA Manager, the KPMG CS Manager as to any action the CA will take in response to the inspection report.

Where the CA Manger or the KPMG CS Manager fail to take appropriate action in response to the inspection report, ITS Global Information Risk and Security Office (IRSO) may:

1 Indicate the irregularities, but allow the CA to continue operations until the next programmed inspection.

2 Allow the CA to continue operations for a maximum of thirty (30) days pending correction of any problem prior to revocation.

3 Initiate the revocation process for the CA certificate.

Any decision regarding which of these actions to take will be based on the severity of the irregularities.

8.6 Communications of Results

Inspection information is to be considered sensitive and must not be disclosed for any purpose other than inspection purposes or where required by agreement or by law pursuant to judicial authorization or an express statutory requirement.

The audit report besides a summary must cover the following areas:

- State that the operations of the CAs were evaluated for conformance to the requirements of this CPS and related KPMG CS documentation.
- State that the relevant CPS was evaluated for conformance to this Certificate Policy, KPMG CS IT Standards and other relevant documentation.
- Report the findings of this evaluation to
  - ITS Global Management
  - ITS Global Information Security Office
  - Member firms leveraging KPMG CS

9 Other Business and Legal Matters No stipulation.

9.1 Fees

No stipulation.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

No stipulation.

9.4 Privacy of Personal Information

No stipulation.

9.5 Intellectual Property rights

No stipulation.

9.6 Representations and Warranties

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

No stipulation.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

No stipulation.

9.13 Dispute Resolution Provisions

No stipulation.

9.14 Governing Law

No stipulation.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.

Contact us

Information Risk and Security Office (IRSO)
ITS Global
eMail: go-fmITSGIRSO@kpmg.com