Capstone Asia Pacific Certification Authority Security Guidance Comparative Analysis Report iDA Security Guidelines to WebTrust & ETSI TS 101 456

November 2007

Table of Contents

Executive Summary

We have performed a comparative analysis of the iDA Security Guidelines for Certification Authorities (CAs) to both the WebTrust and ETSI TS 101 456 CA Guidelines to identify where these guides differ in content and requirements. The analysis of WebTrust suggests a more detailed guide is provided in WebTrust but the content is very closely matched. The exceptions are noted in summary below and in detail in the appendix. The ETSI TS 101 456 guide is structured in an easier to match format and is also easier to read in comparison to the WebTrust documentation. Both WebTrust and ETSI TS 101 456 provide good cross references to other standards and relevant documentation, something currently lacking in the iDA documentation. This report may serve as an initial cross reference guide to users in the future.

We have identified a number of prioritised recommendations for iDA to consider in enhancing the current guide and help CAs understand how to interpret the Guide in context to these other international guidelines. We recommend that iDA consider the following steps to improve integration of the current guidelines to those compared:

- Include a cross reference table for WebTrust and ETSI TS 101 456 in the appendix of the guide for quick reference
- Consideration be given to align the iDA Security guide with both Web Trust and ETSI guides relating to the destruction of expired or compromised keys. This is one of the major differences in the guides, however the principle adopted in Singapore does meet the spirit of the other guides in rendering the keys beyond use. Perhaps further emphasis on the containment of the keys may better clarify this issue.
- Consideration be given to include the following items that are currently mentioned in the other guides:
    - Escrow handling of Keys (optional)
    - Clarification of the need and type of audits required to be undertaken
    - Liability guidelines with regard to CAs
    - Certificate Profile – version numbers
    - Indemnification guidance documentation
    - Intellectual Property rights

The detailed recommendations are provided in Appendix A setting out the mapping of the three documents by section.

Background

Public Key Infrastructure (PKI) provides a means for relying parties (meaning, recipients of certificates who act in reliance on those certificates and/or digital signatures verified using those certificates) to know that another individual's or entity's public key actually belongs to that individual/entity. CAs organizations and/or CA functions acting as trusted third parties have been established to address this need.

Comparison of the three CA Guides and the basis for auditing these systems helps to ensure that overall consistency between systems deployed around the region and across the world.

Reliance on the integrity of the Registration Authority (RA) and CA process is critical for the ongoing use of PKI as a secure transaction processing medium. Therefore, it is also beneficial that these processes are considered to provide an acceptable level of common assurance across borders and jurisdictions so that future e-commerce interoperability will not be significantly restricted.

The following documents have been used to perform the comparative analysis and form the basis of the audit and control framework used to assess whether a CA is operating in a secure and well controlled manner.

WEBTRUST SM/TM PROGRAM FOR CERTIFICATION AUTHORITIES VERSION 1.0

This document provides a framework for licensed WebTrust practitioners to assess the adequacy and effectiveness of the controls employed by CAs, the importance of which will continue to increase as the need for third-party authentication increases to provide assurance with respect to e-commerce business activities. As a result of the technical nature of the activities involved in securing of e-commerce transactions, this document also provides a brief overview of PKI using cryptography, trusted third-party concepts, and their increasing use in e-commerce. Confidentiality, authentication, integrity, and non-repudiation are the four most important ingredients required for trust in e-commerce transactions.

ETSI TS 101 456

This document provides the European Union's framework for the practice requirements of CA in the EU. The ETSI TS 101 456 document specifies policy requirements relating to CAs.

It defines policy requirements on the operation and management practices of CAs issuing qualified certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of electronic signatures.

The policy requirements are defined in terms of:

a) the specification of two closely related qualified certificate policies for qualified certificates issued to the public, one requiring the use of a secure-signature-creation device;

b) a framework for the definition of other qualified certificate policies enhancing the above policies or for qualified certificates issued to non-public user groups.

iDA – SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

This guide has been published by the iDA in Singapore as the authoritative guide to security requirements for CAs in Singapore.

Other than this guide, CAs that apply to be licensed will have to be audited for compliance against the Electronic Transactions Act (ETA) in Singapore, ETA related regulations, its Certificate Practices Statement (CPS), and other licensing conditions (e.g. financial soundness) imposed by the Controller of CAs. The auditing team must be independent of the CA that it audits and approved by the Controller. The team must also comprise of a Certified Public Accountant (CPA) and a Certified Information Auditor, either of them must possess sufficient knowledge of PKI.

Scope and Objectives of Work

The scope of this work consisted of a comparative analysis of the audit requirements for an entity under the iDA Security Guidelines to qualify as a licensed CA in Singapore against both the audit requirements under:

a) WebTrust Program for CA version 1.0; and

b) ETSI TS 101 456.v1

The objective of this work is to provide iDA and users of this report, the ability to understand the alignment of iDA security requirements to qualify as a licensed CA against two of the other internationally recognized guidelines. This report aims to provide a reference for users to understand the compliance model and to assist

both the CA and potential auditor in planning and executing such work in the future.

Results and Findings

The analysis of WebTrust suggests a more detailed guide is provided in WebTrust but the content is very closely matched with iDA's Security Guidelines. The style of WebTrust is to provide an illustrative control as a guide whereas the ETSI and iDA guides are more general to allow for a slightly broader interpretation. The ETSI TS 101 456 guide is structured in an easier to match format and is also easier to read than the WebTrust Documentation. Both WebTrust and ETSI TS 101 456 provide good cross references to other standards and relevant documentation, something currently lacking in the iDA documentation.

Where we have found differences of note we have highlighted these and recommended some adjustments where we consider they may help with the overall alignment of the iDA guide to the other two documents. These items are noted in summary of findings below and in detail in the appendix.

The alignment of the audit requirements will allow for a user to adopt the WebTrust audit approach and remain fully compliant with the Singapore CA Security Guidelines. Whilst the WebTrust model is more detailed it addresses all the same items and therefore would allow an auditor to undertake the assessment with assurance that all key elements were addressed. The additional scope that is not required may be eliminated at the discretion of the auditor but then they could not certify against the WebTrust seal. The auditor may have to consider the additional requirements present in the Singapore's ETA and related Regulations for a more comprehensive picture with regards to this additional scope.

Recommendations

We recommend that iDA consider the following steps to improve integration of the current guidelines to those compared:

- Consideration be given to align the iDA Security Guidelines with both WebTrust and ETSI guides relating to the destruction of expired or compromised keys. This is one of the major differences in the guides
- Include a cross reference table for WebTrust and ETSI TS 101 456 in the appendix of the guide for quick reference
- Include the following items in the guide for completeness purposes
    - Escrow handling of Keys (optional)
    - Liability Values outlined for CAs
    - Indemnification to be better outlined
    - Clarification of Audit requirements – need for Audit and type of audit required.
    - Certificate Profile – version numbers,
    - Intellectual Property rights are included
- There are minor issues on developing further guidance in the iDA document that are set out in the appendix for general consideration. These can further improve alignment and clarification, if desired. The issue to consider when deciding to include such items, is whether the iDA wishes to be so prescriptive in every item.

Conclusion

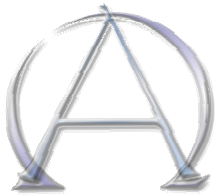
Based on the fieldwork performed we found that the iDA Security Guidelines is a close match to both the WebTrust and ETSI TS 101 456 documents. Whilst the style does differ in each case the core elements are very similar in requirement and standards. A small adjustment to make the alignment more readily identifiable in some cases will help to ensure the guidelines delivers a consistent model in alignment with WebTrust and ETSI TS 101 456.

General

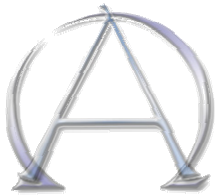
We would like to thank the managers and staff of iDA for their cooperation and support during the review process and we look forward being of assistance to the team in the future.

APPENDIX A: Comparative Analysis Results Summary

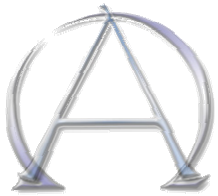
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
MANAGEMENT GUIDELINES			
2.1 – Obligations	Section 6.1 – CA obligations Section 6.2 – Subscriber obligations Section 6.3 – Information for Relying parties **Observation** 1. There are 10 sub clauses in the iDA document covering obligation vs. the ETSI document only requiring the CA to conform with clause 7. 2. Both iDA and ETSI require the following: • The CA is responsible for conformance even if the CA subcontract services to a third party. • The CA shall provide all certification services consistent with its CPS. 3. The iDA document item 2.1.1 notes the outsource request requirements, it also notes the outsource provider has to be audited, this could be infer in the ETSI document but it is not explicit in this regard.	Principle 1 – items 11 and 12: CA and /or RA Obligations **Observation** 1. There are 10 sub clauses in the iDA document covering obligation vs. the WebTrust setting out 8 items. 2. Both iDA and WebTrust require the following: • The CA shall provide all certification services consistent with its CPS. • Both set out obligations pertaining to the revocation of certificates. 3. The iDA document item 2.1.1 notes the outsource request requirements, it also notes the outsource provider has to be audited. 4. Additional item in the iDA document summarises a number of obligation noted in later sections of the guide. It is not clear if this is a complete list and therefore, may be confusing to the reader and hard to maintain in	Consideration could be given to adopting the ETSI approach to simplify this section and to avoid confusion.



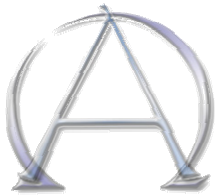
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
	4. Additional item in the iDA document summarises a number a number of obligation noted in later sections of the guide. It is not clear if this is a complete list and therefore, may be confusing to the reader and hard to maintain in the future.	the future. 5. Overall the subject matter is not very closely aligned in this matter , the obligations in both documents are a selection of specific items but do not really address all obligations.	
2.2 – Liability **The iDA statement only requires that the community be informed of the scope and limitation of the CA liability with respect to reliance place on the information contained in the certificate.**	Section 6.4 – Liability (ref. Annex A for potential liability in the use of electronic signatures) **Observation** 1. The ETSI document is more prescriptive making reference to Annexure A – "Potential liability in the use of electronic signature" – it is a conceptual framework to guide potential users of the certificates of the liability attached. 2. However, there is recognition that liability does exist and will be claimed if the CA operates in a negligent manner. The framework also highlights that specific liability will be based on national laws of each member state.	Principle 1 – item 4: Any applicable provisions regarding apportionment of liability. Observation 1. The WebTrust document expressly sets out the limitation of liability to $10,000 per breach of any express warranties made under the CPS and or applicable Certificate Policy (CP). 2. WebTrust also notes that the subscribers will indemnify the CA for actions generally caused by the subscriber's negligent actions.	Both the WebTrust and ETSI have more detail on this matter than the iDA document. Adoption of further guidance may be appropriate to include clarification in the iDA document to indicate that liability is attracted based on the reliance placed by the users of the certificate. The value and limitation of liability may need to be considered by legal counsel. Note *The duties and responsibilities of the Licensed CA are stated within the Electronic Transactions Act (Chapter 88, see Part VIII) and a licensed CA has to be audited against those*



iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
			requirements. *The obligations and liabilities of all parties (including the licensed CA, the subscribers, and relying parties) are elaborated in the licensed CA's CPS and CPs.* *The Liability Values for each type of Certificates issued are specified in the respective CPs.*
2.3 – Certificate Policy and Certificate Practices Statement **The iDA document highlights the requirements of the CA to inform the user community of the CPS and changes to CPS if they occurred. Also a CPS is defined for each class of certificate and each CPS must be uniquely identifiable to the user community.**	Section 7.1 – CPS **Observation** 1. The ETSI commentary is more extensive in this case setting out 8 items of guidance. It is prescriptive in identifying items to be addressed including: • The CA will have CPS addressing all CPs. • The CA will have CPS that identify the obligations of all external organizations supplying services to the CA • The CA will make available the CPS to subscribers and other relying on its certificate	Principle 1 – items 1 and 2: Identification of each CP and CPS for which the CA issues certificates. Principle 1 – item 39: CPS and CP Administration change control and approval procedures. **Observation** 1. The WebTrust approach is similar to the iDA approach both require the disclosure and publication of the CP and CPS. 2. No major differences in these documents noted.	1. iDA should consider expanding the section on CPS and separate policy and practice statement points. 2. The material difference between iDA and ETSI is the need to have CPS for all processes and for the external service provider. This issue should be considered for inclusive in the guide. Note *It is an industry practice for a licensed CA to publish its CPS*

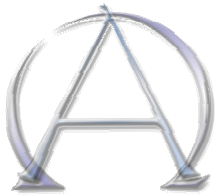


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
	• Senior management of the CA will approve the CPS • Senior management of the CA will have responsibility to ensure the practices are properly implemented • The CPS will be subjected to review process • Terms and conditions on the certificate will be documented in the CPS • The CA will give notice of changes to the CPS to user community		*and CPs, and any changes to the CPS and CPs on its website.* *The CPS coverage and the management of the CPS are in line with the 8 items of guidance published by ESTI.*
2.4 – Security Management **The iDA guide sets out 8 points under the security guide:** • **Requirement for a security policy** • **Personnel to be given policy and made aware of content** • **Security awareness program in place** • **Education in IT security principle and safeguard given** • **Security procedures are**	Section 7.4.1 – Security management **Observation** 1. The ETSI security management guide identifies the following: • Risk assessment to determine what security is required • CA is responsible for all security even if it has outsource elements • A security steering committee is to determine security requirements • Adequate security infrastructure to be maintained at all time • A security policy is in place	Principle 1 – item 43: Physical security controls Principle 1 – item 41: Confidentiality Principle 3 – item 3.2: Security management **Observation** 1. The WebTrust sections on Security Management are spread across a number of areas so mapping is more complex. Primary comparisons on Principle 3 item 3.2 – it identifies 16 points to consider. The following are key: • An Information Security Policy document approved by	The iDA is more prescriptive with regard to overall security awareness and socialization aspect. However, it does not mention outsource party and the responsibility regarding this organization. It is recommended that this be included in the iDA model.



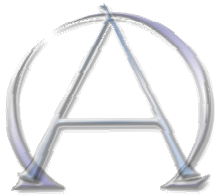
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
documented • **Security level can be checked on a regular basis** • **Incident response procedures capable of tracking security events are in place** • **Forensic evidence of incidents are kept**		management • The Security Policy contains a definition of information security, its overall objectives and scope • The Policy address Managements Intent to support the goals • The Policy contains an explanation of the security Policies, principles and standards and compliance requirements of particular importtance to the organization in particular covering : o Legislative compliance o Security education requirements o Prevention and detection of viruses o BCP o Consequences of Security violations • Policy include responsibility for Information security management including reporting of incidents • Defined review Process 2. The WebTrust guide is more prescriptive in the content of the security policy than the iDA document. 3. Overall the two cover security	

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		management objectives, no material variance is noted,	
2.5 – Risk Management	***NOT AVAILABLE in ETSI*** **Observation** The iDA guide sets out a section on Risk Management this is not covered by the ETSI guide although general comments on risk analysis are made throughout the document e.g. security management section.	***NOT AVAILABLE in WebTrust*** **Observation** The iDA guide sets out a section on Risk Management this is not covered by the WebTrust guide although general comments on risk analysis are made throughout the document.	No recommendation required.
2.5 – Personnel Control **There are 9 items setting out the control of personnel within the iDA document.**	Section 7.4.3 – Personnel security **Observation** 1. The 2 sections are similar in coverage but the approach is different. The iDA document focus is on the detail practice of processing personnel whereas the ETSI is more generic in its approach. This is perhaps to provide for more varied circumstances within the European environment.	Principle 3 – criteria 3.4: Personnel Security **Observation** 1. The 2 sections are similar in coverage but the approach is different. The iDA document focus is on the detail practice of processing personnel. 2. The WebTrust document identifies a number of additional items of note, they include: • Dealing with Contracting personnel including: o Bonding requirements o Contractual requirements including indemnification o Audit and monitoring of contractor personnel	Items for iDA to consider would be the inclusion of: • A conflict of interest related clause which is noted in the ETSI guide. • Skills and experiences requirements for personnel as setout in the ETSI. • Items stated in WebTrust not currently covered in the iDA document as some of these items do address significant security issues pertaining to personnel security too. ***PRIORITY: MODERATE*** *- of*



iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		• Periodic reviews to occur to verify the continued trustworthiness of personnel • A formal disciplinary process in place for employees who violate organizational security policy and procedures • Appropriate and timely actions are taken when employees are terminated so that security is not compromised.	*moderate importance to consider* Note *For the case of the current licensed CA in Singapore, the background, qualifications, experience and security clearance requirements of the personnel are detailed in Section 5.3 of the licensed CA's CPS. Personnel are employed based on qualifications. All staff is subject to background checks and security clearance by the relevant Government authority. Staff should not be deployed in positions where there could potentially be security risk or conflict of interest.*
2.6 – Maintenance of Subscribers	***NOT AVAILABLE in ETSI*** **Observation** There is no specific section in the ETSI guide, however, it is generally address through the operation management section and potentially the BCP section.	Principle 1 – item 14: Subscriber obligations Principle 1 – item 27: Certificate renewal Principle 1 – item 32: Certificate distribution Principle 1 – item 41: Confidentiality	No recommendation required.

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		Observation There is no specific section in the WebTrust guide, however, it is generally address through the various sections noted above.	
2.7 – Incident Management **The iDA document contains 4 items addressing incident management. The key elements include:** • **Need for an incident management plan** • **The plan is tested** • **The incident management plan includes the situation requiring that CA certificates and all related keys be revoked immediately in the event of the lost or compromise of CA certificate key or storage device.** • **The controller will be notified within 24 hours**	Section 7.4.8 – Business continuity management and incident handling Section 7.4.5 (g) – Incident reporting and response **Observation** 1. The ETSI guide does not include a specific section on incident management. However, it is included in a sub section of operation management. 2. The ETSI document is not as prescriptive as the iDA document in setting out the requirements for incident management. However, under operation management section, there are a number of items that are worth considering.	Principle 3 – item 3.6.9 to 3.6.14: Incident reporting and response procedures **Observation** 1. The WebTrust documentation identifies 6 items: • Requirement of a formal Incident management system • Users of CA systems are required to report security incidents • Procedures are in place to report software malfunction • IM procedures are followed and monitored 2. The WebTrust process does not include the requirement to specifically deal with key revocation in the IM sections.	Items within operation management of ETSI that are not identified in the iDA document includes the need for capacity planning to be performed on a regular basis; virus protection maintained up to date; media handling of backup data maintained at the same security level. ***PRIORITY: MODERATE*** *- of moderate importance to consider*
2.8 – Continuity	Section 7.4.8 - Business continuity	Principle 1 – item 44: Business continuity	No recommendation



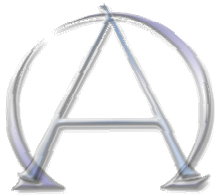
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
Management	management and incident handling **Observation** 1. The iDA and ETSI documents both address business continuity planning and require a documented BCP to be in place. Both documents require the situation of the CA private keys being compromise to be included as part of the BCP. 2. The main differences between the iDA and ETSI documents are that: 3. The iDA appears to mandate the requirement of a hot site whereas ETSI does not make mention of such requirement. 4. The ETSI makes no specific directive on timing of recovery.	management controls Principle 3 - criteria 3.9: Business continuity management **Observation** 1. The iDA and WebTrust documents both address business continuity planning and require a documented BCP to be in place. Both documents require the situation of the CA private keys being compromise to be included as part of the BCP. 2. The main differences between the iDA and WebTrust documents are that: • The iDA appears to mandate the requirement of a hot site. • WebTrust requires a 24 hour recovery time to be stated in the BCP • The CA maintains a recovery site approximately 50 miles from the CA site (May be difficult in Singapore!) • Copies of essential business information and CA systems software are copied every day. 3. iDA's requirements appear to be stronger that Web Trust - so no further requirements needed.	required.

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
CERTIFICATE MANAGEMENT GUIDELINES			
3.1 – Certificate Attributes **There are 7 items in the iDA guide relating to certificate attributes.**	***NOT AVAILABLE in ETSI*** **Observation** There are 7 items in the iDA guide relating to certificate attributes. These are identified generally at various times through the ETSI document but are not capture in a specific section.	Principle 1 – item 36: Certificate profile **Observation** WebTrust sets these out in the Certificate profile section , these attributes are very similar – a one for one check could be made to align them more readily if required for consistency. All key elements are covered.	No recommendation required.
3.2 – Registration **There are three items in the iDA guide related to registration:** • **Authentication require of the applicant** • **Authenticity of official document to be checked** • **Logs to be kept of the registration process**	Section 7.3.1 – Subject registration **Observation** 1. Under the ETSI there are 11 items addressed in the registration section. The ETSI coverage is more prescriptive. 2. The ETSI is explicit in the content of information required setting specific attributes and information required for registration.	Principle 1- item 26: Registration requirements **Observation** The WebTrust approach is very similar – does not mention the audit log here but logs are noted in other areas of WebTrust. Note findings from ETSI.	It may be preferable to apply a more prescriptive set of criteria to this section as it is important to know the key attributes are consistent across various jurisdictions. Currently, it could be subjected to different input based on the guideline provided by the iDA document. ***PRIORITY: MODERATE - of moderate importance to consider***
3.3 – Generation	Section 7.3.3 – Certificate generation	Principle 1 – item 30: Certificate acceptance	No recommendation required.

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
The iDA sets out 2 items on generation: • **Generation in accordance with CPS** • **Accuracy and integrity to be ensure of certificate generation**	**<u>Observation</u>** 1. The ETSI identifies two key elements: • To generate the key in accordance with Directive 1 Annexure H (g) • The key generation procedure securely links to the associated registration, certificate renewal or rekey. 2. Both approaches address the same issue.	Principle 2 – item 2.1.1: Service Integrity CA Key Generation **<u>Observation</u>** Certificates are issued to subscribers upon successful processing of the application and acceptance of the certificate by the subscriber. Certificate format, validity period, extension field and key usage are specified in accordance with the CA' s disclosure certificate profile.	
3.4 – Issuance **The iDA has two statements:** • **A secure communication channel between the CA and subscriber is ensure before exchange is undertaken** • **The CA shall require the subscriber to explicit acknowledge receipt and acceptance of the certificate on issue**	***NOT AVAILABLE in ETSI*** **<u>Observation</u>** 1. The ETSI covers certificate issuance under the certificate generation section. It requires secure communication. However this section does not identify the need for specific acknowledgement at this time, acknowledgement is required as a prerequisite to dissemination.	Principle 1 – item 31: Certificate Issuance **<u>Observation</u>** WebTrust states under criteria section that the certificate is to be generated in a secure remote repository until retrieval by the subscriber. Once retrieved by the subscriber the status is updated to accepted and valid.	The ETSI notes that uniqueness of the certificate's distinguishing name assigned to the subject within a domain of CA is maintained over time to avoid the possibility of confusing two people from the same company with similar names. We recommend that this attribute be included in the certificate of issuance in iDA document. ***PRIORITY: MODERATE*** *- of moderate importance to consider*

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
			Note: *Currently for the licensed CA in Singapore, the CPs and CPS guide the issuance of certificates. No two certificates with the same DN can exist in the CA system. The uniqueness of the certificate's DN is assured via the addition of a serial number, whenever a subject requires more than one certificate.*
3.5 – Publication **5 items were noted in the iDA guide:** • **The CA shall publish its certificates and location of its CPS and repository to its user community using a reliable and trustworthy channel** • **The CA shall publish at least the following information:** o **Company name & registration number**	Section 7.3.5 – Certificate Dissemination **Observation** 1. The ETSI document identifies 5 items under the term dissemination: • Certificate will be available to user • Only certificates with subject consent are published • Terms and conditions of the certificate • Certificate available 24 by 7. • Information is available publicly and internationally. 2. Terms and conditions of the certificates are noted in the ETSI	Principle 1 – item 32: Certificate distribution Principle 2 – item 2.25: Certificate distribution Principle 3 – criteria 3.7: System access management **Observation** 1. WebTrust sets out the publication guide adopting x.500 directory system – the protocol being LDAP. 2. Web Trust also notes the requirement for the Directory to be secured and monitored to ensure the Certificate information is available. 3. The CA maintains controls to provide	No recommendation required.

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
○ **X.500 name** ○ **Internet address** ○ **Telephone number** ○ **CA certificate** ○ **Location of repository** • **Publication of subscriber certificates in repository subject to subscriber consent.** • **Repository must be secured** • **Backup and redundancy in place**	document but not on the iDA publication section. No major differences noted.	reasonable assurance that CA system access is limited to properly authorized individuals.	
3.6 – Renewal **The iDA document identify 3 items of note:** • **Notice of renewal to be provided to subscriber** • **Renewal requested using a secure channel** • **Renewal process the same as new certificate generation**	Section 7.3.2 – Certificate renewal, rekey and update **<u>Observation</u>** 1. The ETSI document focuses on the registration process and is primarily a repeat of the registration section. 2. The iDA appears to be a clearer version – no recommendation require.	Principle 1 – item 27: Certificate renewal Principle 2 – item 2.2.2: Certificate renewal **<u>Observation</u>** WebTrust states that the renewal process is similar to that required for the application of a new certificate, however the subscriber only has to provide information that has changed.	No recommendation required.
3.7 – Certificate suspension **7 items are identified in the iDA document:**	Section 7.3.6 – Certificate revocation and suspension **<u>Observation</u>**	Principle 1 – item 34: Certificate suspension Principle 2 – item 2.2.7: Certificate suspension	The iDA document should also include • a time period for suspended

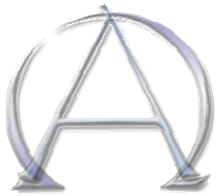


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
• **Suspected or compromised subscriber's private key** • **Certificate suspension submitted via secure communication channel** • **Format of suspension to include reason and time** • **CA to digitally signed suspension certificate** • **CLL updated** • **Subscriber to be notified**	1. The ETSI document notes the following: • Suspension processing should follow the requirements detailed under the CPS process. • All suspension should be processed on receipt • Request should be authenticated • A maximum 24 hours period is set to determine if the certificate should be revoked	**<u>Observation</u>** WebTrust sets out an extensive list of criteria but gives no illustrative controls under this section. The following key elements of the criteria are for consideration in mapping to iDA Security Guidelines: • Circumstances under which a certificate must be suspended. • Identification and authentication procedures required for revocation requests. • Procedures to initiate, authorize and verify a certificate suspension request • Circumstances under which a suspension may be lifted • Authorization required for lifting a suspension • Procedures for rapid communication of the suspension • Procedures to notify the subscriber of the suspension • Whether an external RA is notified for which a suspension was initiated by the RA • How and when the subscribers certificate status information is updated upon certificate	certificate to be revoked. • Authorization process required to lift a suspension • Circumstances under which a suspension are lifted. These are clarification issues – and do not constitute a critical difference. *<u>Note:</u>* *In practice, the licensed CA in Singapore currently has a time period of 6 hours for the maximum delay between receipts of revocation request to revocation status being available.*

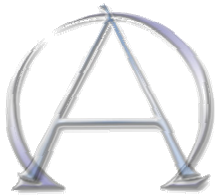
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		suspension and the lifting of the suspension	
3.8 – Certificate revocation **iDA guide contains 9 key elements in relation to certificate revocation:** • **permanent revocation of a certificate will occur if a subscriber request it** • **the CPS will state detail of who can request a revocation** • **Required revocation when detailed circumstances are met (see 3.8.2)** • **Revocation submission must be secured** • **Must include reason and time of revocation** • **CA must digitally sign revocation** • **The revocation must be published once verified** • **Revocation must be protected from change** • **The subscriber must be notified of revocation**	Section 7.3.6 – Certificate revocation and suspension **Observation** 1. The ETSI section on revocation also covers suspension. It covers the same process as that of iDA with no major difference noted. Minor noted variance being ETSI states that once a certificate is revoked, it cannot be reinstated. 2. Although iDA language states permanent revocation which will imply the same outcome.	Principle 1 – item 33: Certificate revocation Principle 2 – item 2.2.6: Certificate revocation **Observation** WebTrust sets out a 9 items under its criteria for certificate revocation. The items are very similar to the items set out above under suspension and are covered by the iDA guide. There is one item noted which relates to a grace period available to the subscriber. This point is not elaborated upon. Under principle 2 there are 12 illustrative controls – addressing the material under principle 1 above. It notes that a suspended certificate will be held on the Certificate Revocation List (CRL) until it is either released, changed to revoked. If nothing happens to the status it will remain as suspended until the end of the life of the certificate.	No recommendation required.

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		Details of the iDA guide are as explicit if not more so in this area so no recommendations are considered necessary.	
3.9 – Archival **The iDA document contains 2 items:** • **Require 7 years of archive and accordance with applicable regulation** • **Digital archival shall be stored indexed and able to be reproduced**	Section 7.4.10 (a) – Compliance with legal requirements Section 7.4.11 (b and f) – Recording of Information Concerning Qualified Certificates **Observation** 1. The ETSI document addresses archive under section 7.4.10 requires document to be retained for statutory purposes and makes reference to the European data protection directive. 2. No major issue noted. iDA requirement is more specific than ETSI	Principle 1 – item 35: Provision of certificate status information **Observation** WebTrust makes not of Archive of CRLs and other certificate information under section 35. The illustrative control indicates that the CA should retain all certificates for a minimum period of 10 years. There is not specific reason for this as a better time frame. It would be expected that the records would be archived in line with local legal regulatory requirements.	No recommendation required.
3.10 – Audit trail **iDA notes 4 items on audit trail:** • **Maintenance of audit trail for certification, registration, generation, issue, renew, suspend, revoke.**	Section 7.4.10 – Recording of information concerning qualified certificates **Observation** 1. The ETSI audit trail section requires all major activities to contain time related information and identifiers. 2. The ETSI audit trail sections are	Principle 1 – item 41: Confidentiality Principle 1 – item 45: Event logging Principle 3 – 11 Event Journaling **Observation** WebTrust sets out the following points under Audit Trail. 1. Information such as Audit trails should be kept confidential	iDA could consider adopting the ETSI or WebTrust audit trail content statement to help ensure consistency in the capture of audit trail information. This is to improve audit guidance it is not a critical

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
• **Audit trails must be protected and available** • **Audit trails need to be reviewed periodically by management** • **Audit trails must be archive for a minimum of 12 months or as required by regulation**	significantly more detailed and specific information required for each transaction type to be held on audit trail.	2. Audit trails should be archived regularly and reviewed. 3. All journal entries include the following elements: • Date and time of the entry • Serial or sequence number of entry (for automatic journal entries) • Kind of entry • Source of entry (for example, terminal, port, location, customer) • Identity of the entity making the journal entry 4. The CA logs the following key life cycle management related events: • CA (and subscriber, if applicable) key generation • Installation of manual cryptographic keys and its outcome (with the identity of the operator) • CA (and subscriber, if applicable) key backup • CA (and subscriber, if applicable) key storage • CA (and subscriber, if	requirement. ***PRIORITY: MODERATE*** *- of moderate importance to consider*

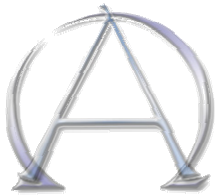


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		applicable) key recovery • CA (and subscriber, if applicable) key escrow activities (optional) • CA key usage • CA (and subscriber, if applicable) key archival • Withdrawal of keying material from service • CA (and subscriber, if applicable) key destruction • Identity of the entity authorizing a key management operation • Identity of the entity handling any keying material (such as key components or keys stored in portable devices or media) • Custody of keys and of devices or media holding keys • Compromise of a private key 5. The CA logs the following cryptographic device life cycle management related events: • Device receipt	

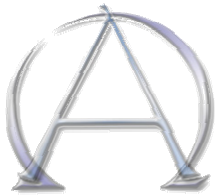


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		• Entering or removing a device from storage • Device usage • Device de-installation • Designation of a device for service and repair • Device retirement	
KEY MANAGEMENT GUIDELINES			
4.1 – Generation **4 items are noted in the iDA documentation:** • **The CA key must be stored under split control** • **Separate key pairs for digital signature and encryption should be generated** • **Key value should be random** • **The subscriber key pair should be approved by the CA if the subscriber generates their own key pair**	Section 7.2.1 – CA key generation **Observation** 1. The ETSI sets out specific security requirements for the key to meet one of three specific criteria: • FIPS pub 140-1[5] level 3 or higher • CED workshop agreement 14167-2[8]; or • A trustworthy system of equivalent EAL4 or high 2. The two documents address different issues under this heading (the items noted under the ETSI section are more closely mapped to section 4.10 of the iDA documentation).	Principle 1 – item 17: CA key pair generation Principle 1 – item 22: Subscriber key pair generation Principle 2 – item 2.1.1: CA Key Generation Principle 2 – item 2.1.9 (1 to 10): CA – provided subscriber key management services **Observation** CA key pair generation, including: • What key sizes are required • What key generation algorithm is required • Whether key generation is performed in hardware or software • What standards are required for the module used to generate the keys (for example, the required ISO 15782-	No recommendation required. Note *Content sections relating to the Cryptography in the iDA document can be found under section 4.1011.*

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		1/FIPS 140-1/ANSI X9.66 level of the module) • For what purposes the key may be used • For what purposes usage of the key should be restricted • The usage periods or active lifetimes for the CA public and the private key, respectively. P2.1.1 - The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with industry standards. P2 2.1.9 - The CA maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with industry standards.	
4.2 – Distribution **The iDA document requires transfer of the key in a secure manner ensuring end to end integrity.**	Section 7.2.3 – CA public key distribution **Observation** 1. The ETSI requires the same objective as those stated in the iDA document.	Principle 1 – item 20: CA public key distribution Principle 2 – item 2.1.3: CA Public key distribution **Observation** CA public key distribution, including a description of how the CA's public key is provided securely to subscribers and relying parties, Illustrative control - The	No recommendation required.

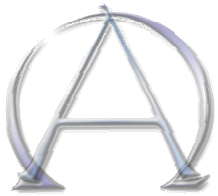


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		CA's public key is delivered in a self-signed certificate to subscribers using an encrypted session between the CA and the subscriber's client software, with an authorization code as a shared secret. Authenticity and integrity protection is based on a MAC key derived from the authorization code.	
4.3 – Storage **The iDA document identifies the following attributes:** • **CA to provide subscriber equipment and storage program facilities to securely store the key.** • **Keys are to be tampered proof with split control** • **The key custodian protects the activation code**	Section 7.2.2 – Certification authority key storage, backup and recovery **Observation** 1. The ETSI guide makes reference again to the FIPS and related security standards for storage and indicates that only trusted personnel may be custodian of the key. 2. Keys are also required to be under dual control in the ETSI guideline.	Principle 2 – item 2.1.2: CA Key storage, backup and recovery Principle 2 – item 2.1.9 (11 to 14): CA – provided subscriber key management services **Observation** The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. 1. The CA's private signing key is stored within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA's business practices (Principle 1, item 17). 2. If the CA private key is not exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or	More detail is provided in WebTrust on the security attributes of the backup and procedures to follow. This may be valuable to include as failures in security of backups are known to be easier targets than the primary data on the network. ***PRIORITY: MODERATE*** *- of moderate importance to consider*



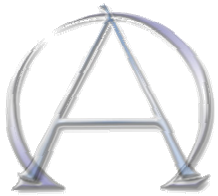
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		backup and recovery, then the CA private key is generated and used within the same cryptographic module and is never exported outside of the cryptographic module. 3. If the CA private key is exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the private key is exported in a secure key management scheme including any of the following: • As cipher text using dual control • As encrypted key fragments using dual control and split knowledge/ownership • In another secure cryptographic module such as a key transportation device using dual control The CA maintains controls to provide reasonable assurance that subscriber private keys stored by the CA remain confidential and maintain their integrity.	
4.4 – Usage	Section 7.2.5 – CA key usage	Principle 2 – item 2.1.5: CA Key usage	Consideration may be given

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
The iDA requires the following key points: • **System software integrity check must be performed before keys are loaded** • **Custody of the keys are under split control**	**Observation** 1. The ETSI states that keys should not be used for any other purpose and keys should reside in only one physical location 2. The ETSI guide is more directed to the actual key usage.	**Observation** 1. The CA maintains controls to provide reasonable assurance that CA keys are used only for their intended functions in their intended locations. • The activation of the CA private signing key is performed using multiparty control (that is, *m* of *n*). • If necessary based on a risk assessment, the activation of the CA private signing key is performed using multi-factor authentication (for example, smart card and password, biometric, and password). 2. The CA maintains controls to provide reasonable assurance that the integrity and authenticity of the CA public key and any associated parameters are maintained during initial and subsequent distribution. 3. The CA provides a mechanism for detecting the modification of the CA's public key during the initial distribution process (for example, using a self-signed certificate). 4. The initial distribution mechanism for the CA's public key is controlled as disclosed in the CA's business	to adopting the ETSI items relating to key usage in the iDA document.

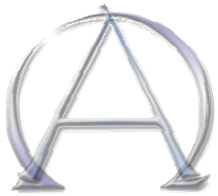


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		practices (Principle 1, item 20). 5. The CA ceases to use a key pair at the end of the crypto-period or when the compromise of the private key is known or suspected	
4.5 – Backup **Private keys shall be backed up to prevent a CA's operation from stopping due to accidental deletion or corruption of keys.** **CA private key backups shall be protected with the same guideless as for CA private key storage** **Separate key custodians**	Section 7.2.2 – CA key storage, backup and recovery **Observation** No major differences noted between the two.	Principle 2 – item 2.1.2: CA Key storage, backup and recovery **Observation** The CA maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. Illustrative controls - • The CA's private signing key is stored within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA's business practices (Principle 1, item 17). • If the CA private key is not exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the CA private key is generated and	No recommendation required.

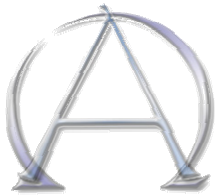
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		used within the same cryptographic module and is never exported outside of the cryptographic module. • If the CA's private signing key is backed up, backup copies of the CA private keys are subject to the same or greater level of security controls as keys currently in use. • If the CA's private signing key is backed up, recovery of the CA private key is conducted in the same secure schema used in the backup process, using dual control.	
4.6 – Key change **Key change in the iDA document identifies the following key items:** • **keys should be changed periodically** • **the validity period shall be defined as per section 4.10.5** • **the CA shall define the key change process that ensures reliability of changeover between old and new**	***NOT AVAILABLE in ETSI*** **Observation** 1. The ETSI makes reference to key change within the life cycle of the key. It is not mentioned as a separate section. 2. The iDA document in this case is more prescriptive.	Principle 1 – item 14, 17, 21,33 and 34: CA Business Practices Disclosure Principle 2 2.2.2 Renewal **Observation** The CA maintains controls to provide reasonable assurance that certificate re-key requests are accurate, authorized, and complete. The CA maintains controls to provide reasonable assurance that certificate renewal requests are accurate, authorized, and complete.	Consideration could be given to timing of change over but this is not essential.



iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
key • **CA shall notify subscriber of any key changes performed automatically**		Key changeover, including a description of the procedures used to provide a new public key to a CA's users • The CA root signing private key has a lifetime of two years and the corresponding public key certificate has a lifetime of four years. Upon the end of the private key's lifetime, a new CA signing key pair is generated and all subsequently issued certificates and CRLs are signed with the new private signing key. The corresponding new CA public key certificate is securely provided to subscribers and relying parties.	
4.7 – Destruction **The iDA document requires all keys to be archived rather than destroyed.**	Section 7.2.6 – End of CA key life cycle **Observation** 1. The ETSI states that private keys are to be destroyed and not to be recoverable 2. There is a difference in this section between the two guide – one would assume the key must be archived for a period of time and then destroyed in a manner that would ensure could not be reverse engineered.	Principle 2 – item 2.1.6: CA Key destruction **Observation** The CA maintains controls to provide reasonable assurance that CA keys are completely destroyed at the end of the key pair life cycle. Illustrative control mentions: • Authorization to destroy a CA private key and how the CA's private key is destroyed (for example, token surrender, token	Key Destruction is favored by both WebTrust and ETSI, however, given the legal requirement in Singapore, regarding archiving, the practical containment of keys is a reasonable approach to take and still meet the spirit of the other two guides. Note: *There is a statutory*

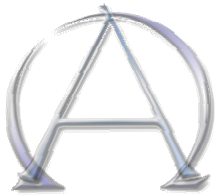


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		destruction, or key overwrite) are limited as disclosed in the CA's business practices (Principle 1, item 17). • All copies and fragments of the CA's private key are destroyed at the end of the key pair life cycle. • If a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed.	*requirement in Singapore for all data to be kept for at least 7 years. Destruction of the CA Private Key would render all CA database not recoverable.* *At the end of the CA key life cycle, iDA Security Guidelines require that the "CA signing private key, all components of the private key and all its backup copies shall be securely archived and stored in a secure location".* *ETSI (section 7.2.6a) specifies, "all copies of the [retired] CA private signing keys shall be destroyed or put beyond use".* *In Singapore's situation, the CA retired CA private keys would be 'put beyond use'.*
4.8 – Key compromise **A procedure shall be pre**	Section 7.4.8 (a and b) – CA Key compromise	Principle 3.9 BCP **Observation**	No recommendation required.

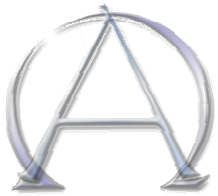


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
established to handle cases where compromise of the CA certification key has occurred. **The CA shall immediately revoke all affected**	**Observation** This item is already dealt with under incident management.	The CA maintains controls to provide reasonable assurance of continuity of operations in the event of the compromise of the CA's private signing key.	
4.9 – CA Key and subscriber encryption key archival **The iDA identifies 3 items:** • **CA public key shall be archived permanently for audit and investigation purposes** • **Subscriber encryption key should be archived for a reasonable timeframe** • **Archival of CA public key and subscriber encryption key shall be protected from unauthorized modification**	***NOT AVAILABLE in ETSI*** **Observation** This section is not covered specifically in the ETSI document but is generally mentioned in section 7.2.2.	Principle 2 – item 2.1.7: Key archival Principle 2 – item 2.1.9 (15 to 17): CA – provided subscriber key management services **Observation** The CA maintains controls to provide reasonable assurance that archived CA keys remain confidential and are never put back into production. • Archived CA keys are subject to the same or greater level of security controls as keys currently in use. • All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site. • Archived keys are never put back into production. • Archived keys are recovered for the shortest time period technically permissible. • Archived keys are periodically	Note that the issue of Key destruction is mentioned again in WebTrust. See commentary under iDA Guidelines section 4.7.

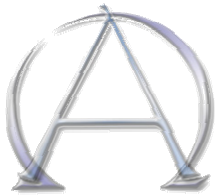
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		verified to ensure that they are properly destroyed at the end of the archive period.	
4.10 – Cryptographic Engineering **The cryptographic processes for the CA operations shall be performed in a hardware cryptographic module that minimally conforms to FIPS 140-1 Security level 3 or FIPS 140 -2 security level 3**	Section 7.2.7 – Lifecycle management of cryptographic hardware used to sign certificates **Observation** 1. The Ida document includes a section on Cryptographic Engineering. These items are referenced to in the ETSI document section 7.2.1 (key generation) and 7.2.2 (key registration). 2. They address the same security requirements of FIPS 140-1 security level 3 for CA cryptographic processes.	Principle 1 – item 18: CA private key protection Principle 1 – item 22: Subscriber key pair generation Principle 2 – item 2.1.9 (1 – 7): CA – provided subscriber key management services **Observation** The CA maintains controls to provide reasonable assurance that subscriber keys generated by the CA (or RA) are generated in accordance with industry standards. Subscriber key generation performed by the CA (or RA) occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA's business practices (Principle 1, item 18).	No recommendation required.
SYSTEMS AND OPERATION GUIDELINES			
5.1 – Physical security **iDA sets out 12 items on physical security. However the major features noted**	Section 7.4.4 – Physical and environmental security **Observation** 1. The ETSI guide identifies 7 key	Principle 1 – item 43: Physical security controls Principle 3 – criteria 3.2: Security management Principle 3 – criteria 3.5: Physical and	We recommend the specific threat items noted in the ETSI documents be considered for inclusion in the iDA documentation.



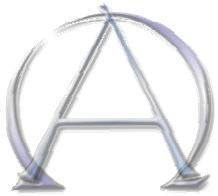
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
include: • **defining major features and setting of responsibilities** • **location of CA not to be publicized** • **security systems in place** • **dual control over access cards and inventory in place** • **cryptographic keys should be physically secured**	elements. The most significant elements are: • Restriction of access to only authorized personnel • Control to avoid lost, damaged or compromised of information • Protection from natural disaster and other specific physical threat 2. The ETSI document identifies a number of physical threats that must be addressed. These include: • Natural disaster, fire, safety factors, failure of support facilities, structural collapse, plumbing leaks, theft, break and enter, disaster recovery. • Additional protection of media taken off site.	environmental security **Observation** Physical security controls, including: • Site location and construction • Physical access controls, including authentication controls to control and restrict access to CA facilities • Power and air conditioning • Water exposures • Fire prevention and protection • Media storage • Waste disposal • Off-site backup	These are more to assist in the audit process for compliance required under this section; it is not essential.
5.2 – System software integrity and control **The iDA document addresses 7 components. The key items require that:** • **System software and application software be verified before use each time.** • **System and application**	***NOT AVAILABLE in ETSI*** **Observation** The ETSI document does not have a specific section addressing system and software integrity control. It is more generally address through the security management section.	Principle 3 – criteria 3.7: System access management Principle 3 – criteria 3.4: Personnel security **Observation** The CA maintains controls to provide reasonable assurance that CA system access is limited to properly authorized individuals. 1. Business requirements for access	No recommendation required.



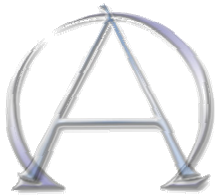
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
software shall minimally conform to common criteria EAL4 or equivalent security level. • **Security critical software that includes the crypto module shall be reviewed by a suitably qualified independent party.**		control are defined and documented in an access control policy which includes at least the following: • Roles and corresponding access permissions • Identification and authentication process for each user • Segregation of duties • Number of persons required to perform specific CA operations (that is, *m of n* rule) 2. The allocation and use of privileges is restricted and controlled. 3. The security attributes of all network services used by the organization are documented by the CA. 4. Use of system utility programs is restricted and tightly controlled.	
5.3 – Change and configuration management **The iDA document identifies 4 items of note:** • **Un-trusted executable should not be loaded** • **Patches reviewed**	Section 7.4.7 – Trustworthy system deployment and maintenance **Observation** 1. The ETSI document addresses change control and configuration under section 7.4.7 (trustworthy system deployment and	Principle 3 – criteria 3.8: Systems development and maintenance **Observation** The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are properly authorized to	Consideration is given that the iDA section includes risk analysis and specific inclusive of the requirement for a formal change control process. WebTrust sets out a whole



iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
thoroughly and tested • **Patches relating to security risk to be promptly loaded** • **Documentation of patches to be maintained up to date**	maintenance). 2. The ETSI recommends: • a risk analysis be carried out to identify services requiring trustworthy system and the level of assurance required. • Change control procedures should exist for releases, modification and emergency software fixes for any operational software. 3. The ETSI approach adopts risk analysis to help target high risk applications and systems. It stipulates that a structure change control process must be in place.	maintain CA system integrity. • Business requirements for new systems or enhancements to existing systems specify the requirements for controls. • Change control procedures exist and are followed for the implementation of software on operational systems. • Change control procedures exist and are followed for scheduled software releases and modifications. • Change control procedures exist and are followed for emergency software fixes. • Test data is protected and controlled • Strict control is maintained over access to program source libraries. • The implementation of changes is strictly controlled by the use of formal change control procedures to minimize the risk of corruption of information systems. • Application systems are reviewed and tested when operating system changes occur. • Modifications to software packages are discouraged and	change control regime – appears a little too prescriptive but has elements of importance for consideration relating to applications being reviewed and tested when operating system changes are made. Emphasis on the importance of strict change control is clearer in WebTrust.

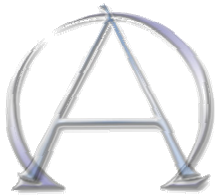


iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		essential changes strictly controlled. • The purchase, use, and modification of software is controlled and checked to protect against possible covert channels and Trojan code. • Controls are in place to secure outsourced software development.	
5.4 – Network and communications security **The iDA has 8 key elements under this section, 2 key points to note are:** • **Security testing and evaluation of network access control of the CA systems should be reviewed by suitably qualified independent party** • **Intrusion detection software tools should be used**	Section 7.4.6 – System access management **Observation** The ETSI document specifically mentions these additional items: • The use of firewalls to protect internal domain • Specific protection of data objects such as deleted files and core dumps.	Principle 3 – criteria 3.7 (8 to 26): System access management – network access control **Observation** The CA maintains controls to provide reasonable assurance that CA system access is limited to properly authorized individuals. • The allocation of passwords is controlled through a formal management process. • Users' access rights are reviewed at regular intervals. • Users are required to follow defined policies and procedures in the selection and use of passwords. • Users are required to ensure that unattended equipment has	This area could be further expanded to include these additional prescription items noted in the ETSI or WebTrust documents.



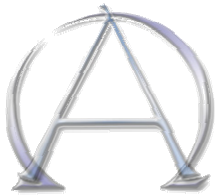
iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
		appropriate protection. • Users are provided direct access only to the services that they have been specifically authorized to use. • The path from the user terminal to computer services is controlled. • If permitted, access by remote users is subject to authentication. • Connections to remote computer systems are authenticated. • Access to diagnostic ports is securely controlled.	
5.5 – Monitoring and audit logs **The iDA document identifies 7 items for monitoring of audit log:** • **Records of the following transactions shall be maintained – registration, certification, publication, suspension, revocation.** • **Records of log file shall be reviewed periodically for unauthorized activities**	**Observation** Refer to ETSI detail requirements for audit trail set out in section 7.4.5(h), 7.4.10 and 7.4.11.	Principle 1 – item 45: Event logging Principle 3 – criteria 3.4: Personnel security Principle 3 – criteria 3.10 (10): Monitoring and compliance Principle 3 – criteria 3.11: Event logging **Observation** Event logging, including the following: How frequently the CA archives event journal data. How frequently event journals are reviewed. • As part of the CA's scheduled system backup procedures, audit trail files are backed up to media on at least a daily basis. Audit trail files are archived by the system	No recommendation required.

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
• **Review of audit trails by oversight personnel** • **Audit logs protected** • **Audit trail retention minimum 12 months** • **Records of significant events kept minimum 12 months or as required by regulation**		administrator on a weekly basis. • Event journals are reviewed at least on a weekly basis by CA management. • The CA maintains controls to provide reasonable assurance that the CA complies with legal requirements. The CA maintains controls to provide reasonable assurance that significant CA environmental, key management, and certificate management events are logged accurately and completely.	
APPLICATION INTEGRATION GUIDELINES			
6.1 – Integrity of signing and verification functions **The iDA document identifies 5 items under this section:** • **Application shall inform user when private key is being accessed** • **User shall be informed if private key is being used for purposed not consistency with that defined as acceptable**	***NOT AVAILABLE in ETSI*** **Observation** The ETSI document does not have a specific section addressing integrity of signing and verification functions. It is more generally address throughout the document – protection of private key is addressed in section 7.2.8 and sections on Certificate Generation.	***NOT AVAILABLE in WEBTRUST*** **Observation** The WebTrust document does not have a specific section addressing integrity of signing and verification functions. It is more generally address throughout the sections on Obligation in Principle 1.	No recommendation required.



iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
by the issuer • Mechanism shall be available to check the integrity of the application for unauthorized modification • Application security risk assessment on the CA software infrastructure should be conducted yearly. • The application should be reviewed by suitably qualified independent party			
6.2 – Protection of private key **The iDA guide specifically identifies the protection of private key to include:** • **Both RA and CA private keys shall be stored in tamper-evidence and tamper-proof devices respectively. It also requires these keys to be protected from unauthorized use or**	***NOT AVAILABLE in ETSI*** **Observation** The ETSI document does not have a specific section addressing protection of private key. It is more generally address throughout the document – protection of private key is addressed in section 7.2.8 and sections on Certificate Generation.	***NOT AVAILABLE in WEBTRUST*** **Observation** The WebTrust document does not have a specific section addressing protection of private key. It is more generally address throughout the sections on Obligation in Principle 1.	No recommendation required.

iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
copy. • **Temporary private key should be securely purged to minimize exposure**			
6.3 – Verification of certificates **The iDA document notes the following key elements for this section:** **1. Application shall verify the validity and authenticity of the certificate by ensuring that:** • **Certificate issuer's signature is valid** • **Certificate is valid i.e. not expired, suspended or revoked; and** • **Certificate extensions flagged as "critical" are being complied with** • **Verification process to trace and verify all components in the certification**	***NOT AVAILABLE in ETSI*** **Observation** The ETSI document does not have a specific section addressing the verification of certificates. It is more generally address through the following sections: • Certificate Generation • Certificate Distribution / Issuance • Certification authority key storage, backup and recovery	***NOT AVAILABLE in WEBTRUST*** **Observation** The WebTrust document does not have a specific section addressing the verification of certificates. It is more generally address through the following sections: • Principle 1 (item 35) – provision of certificate status information; • Principle 2 (item 2.2.8) – Certificate Status Information Processing. Items relating to private keys and issuance are covered in earlier sections on Obligation and Certificate Issuance respectively.	No recommendation required.



iDA Guidelines	Comparative Analysis with ETSI	Comparative analysis with WebTrust	Recommendation
path. 2. Relying party to be informed of the following: • What a particular assurance level means • How the private key associated with the certificate is stored • How entities are verified and issuance process			