Issued

Assessor standard for Bermudan CSP scheme

Ref. tSd 0273

Issue 1.00

2005-01-25

Executive summary

This document contains the proposed processes and deliverables to be put in place in order to support an independent assessment scheme to determine whether CAs that have applied to be certified under the Government's PKI root are compliant with the relevant CPs. It also contains an indication of likely costs for assessment by *tScheme*-Recognised Assessors and of the licence fees likely to be levied by *tScheme* for each compliant CP.

DOCUMENT HISTORY

Status	Issue	Date	Comment	Authorised
tSd	1.00	2005-01-25	First issue, tracked under Document Management procedures. Based on "CSP Standard Final Release221104.doc" from KPMG.	*tScheme* Secretariat

CONTENTS

1. INTRODUCTION

1.1 Background

This document reflects the results of the comparison between the Certification Service Provider (CSP) scheme managed by Ministry of Telecommunications and E-Commerce (MTEC), Bermuda and *tScheme*'s CA Profile (tSd 0102) and associated sub-Profiles, carried out by KPMG.

1.2 Applicable version of CSP scheme

For the purposes of this document, the relevant version of the CSP scheme was that based on the CERTIFICATION SERVICE PROVIDERS (RELEVANT CRITERIA AND SECURITY GUIDELINES) REGULATIONS 2002, an extract shown in figure 1 below.

1999 : 26

THE CERTIFICATION SERVICE PROVIDERS (RELEVANT CRITERIA AND SECURITY GUIDELINES) REGULATIONS 2002

The Minister of Telecommunications and E-Commerce, in exercise of the powers conferred by sections 20 and 32 of the Electronic Transactions Act 1999, makes the following regulations:—

Citation
1 These Regulations may be cited as the Certification Service Providers (Relevant Criteria and Security Guidelines) Regulations 2002.

Relevant criteria
2 For the purposes of section 20 of the Electronic Transactions Act 1999 the relevant criteria are as prescribed in the Code of Practice set out in the First Schedule to these Regulations.

Security guidelines
3 An authorised certification service provider shall, in addition to satisfying the relevant criteria, comply with the security guidelines set out in the Second Schedule to these Regulations.

Commencement
4 These Regulations come into force on ,2002.

Figure 1 - CSP Criteria and Security Guidelines introduction page

The following sections identify the additional criteria that need to be fulfilled during the assessment of a CSP to address the requirements of *tScheme*.

1.3 Applicability to Qualified Certificates

This document does not cover the provision of Qualified Certificate, Advanced Electronic Signatures and/or Secure Signature Creation Devices as defined in the Electronic Signature Directive 1999/93/EC (Dir 99/93). A CSP requiring any of these services to be approved under *tScheme* will need to comply with all related clauses of the applicable *tScheme* Approval Profiles.

1.4 Conflict

In the case of apparent conflict between this document and the related *tScheme* Approval Profile, the Profile has priority. In case of dispute, tScheme Limited will need to be consulted to make a final decision.

2. BASE APPROVAL PROFILE (TSD0111, ISSUE 3.0)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services shall be assessed by *tScheme*-recognised assessors. It identifies the mandatory criteria that all CSPs must satisfy in order to attain *tScheme* approval for this profile.

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
2.1 Usage of non-trusted channels The CSP shall have in place policies and procedures for the usage of non-trusted channels for exchange of information with subscribers and agents (for example postal, telephone and so on).	***MSPP-080***	
2.2 Duress events The CSP shall have in place policies and procedures for detection and management of events by subscribers under duress.	***MSPP-100***	
2.3 Agent's agreement to *tScheme* Assessment When a CSP uses a one or more service components as part of its service a risk assessment should include the analysis of contract with the agent that it agrees to subject its Service or Component to a *tScheme* Assessment or follow-on Assessment check, should the *tScheme*-recognised Assessor decide to do this. Such a check will not be necessary if either the agent's Service has already been approved, or the agent's Component is already recognised as being *tScheme*-Ready, or the Assessor can otherwise be convinced that no Assessment of the agent's Service or Component will be required;	***XPTC-080***	
2.4 Operational Service Each Service Subject to Assessment must be an Operational Service.	***SRPP-005***	

## 2.5 Public Service Description A description of the scope and content of each Service Subject to Assessment, the Public Service Description (PSD), which shall also include a description of the subscriber and expected relying party community to which the Service applies, shall be made publicly available by the CSP.	***SRPP-010***	
## 2.6 Record of Subscriber Agreement The CSP shall record the Subscriber's agreement to the terms and conditions of the Service.	***SRPP-025***	
## 2.7 Publication of a Service Disclosure Statement The items listed in Schedule 2 (item 2.10 of this document) shall clearly and conspicuously be made available by the CSP in a separate Service Policy Disclosure Statement (SPDS) to its community of users, for each Service Subject to Assessment it provides.	***SRPP-290***	
## 2.8 Contracts with other CSPs The contractual relationships with other CSPs (although the details of these contracts may be largely confidential, evidence of any required features specified in Section 3.5 of the Base Profile shall be provided) shall appear either in the Service's Service Practice Statement or in the Assessor's Service Definition.	***SRPP-320***	
## 2.9 Schedule 1 - Enterprise Level Criteria ### 2.9.1 Whenever the term "enterprise" is used in this Schedule, it is qualified to refer either to: a) the enterprise which, or individual who, is actively performing the Trust Service and is responsible for its day to day operation, i.e. the operational enterprise; OR b) the enterprise which controls the operational enterprise, i.e. the controlling parent enterprise; OR c) the enterprise with which the subscriber has a contractual relationship, i.e. the Service offered. Either the operational enterprise or its parent enterprise shall be able to	***N/A***	

demonstrate that it has an appropriate legal status. Specifically, it shall provide:		
2.9.2 Evidence of its establishment / registration (as required by the law of the territory in which it is established);	***N/A***	
2.9.3 In the case of a separately identifiable parent organisation, evidence of the specific relationship between this parent entity and the operational enterprise;	***N/A***	
2.9.4 If the Service offered is neither the operational enterprise nor its parent, it shall similarly demonstrate its legal status;	***N/A***	
2.9.5 The operational enterprise shall demonstrate that it safeguards impartiality of operations by having a documented and distinct management structure and a separately documented set of management policies, controls and procedures for the Trust Services provided;	***N/A***	
2.9.6 The operational enterprise shall demonstrate that it has a quality management system appropriate for the Trust Services it is providing;	***N/A***	
2.9.7 The operational enterprise shall demonstrate that it has a information security management system appropriate for the Trust Services it is providing;	***N/A***	
2.9.8 The operational enterprise shall demonstrate that it has the stability and resources required for supplying electronic Trust Services;	***N/A***	
2.9.9 The operational enterprise shall demonstrate that it employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide electronic Trust Services to the published availability;	***N/A***	
2.9.10 The operational enterprise shall demonstrate that it has a properly documented agreement and contractual relationship in place where the provisioning of Services involves subcontracting, outsourcing or other third party arrangements (see Section 3.5 for more details of this requirement);	***N/A***	

2.9.11 The Service offerer shall demonstrate that it has policies and procedures for the resolution of complaints and disputes from customers received from customers or other parties about the provisioning of electronic Trust Services or any other related matters;		*N/A*	
2.9.12 The Service offerer shall demonstrate that it has adequate arrangements to cover liabilities arising from its operations and/or activities;		*N/A*	
2.9.13 The Service offerer shall supply an address at which legal notices can be served;		*N/A*	
2.10 Schedule 2. Service Policy Disclosure Statement For each SSA, the following information shall clearly and conspicuously be made available by the CSP to its community of subscribers and relying parties. It shall be sufficiently up-to-date and accurate as to not, at any time, mislead subscribers or relying parties:		*N/A*	
2.10.1 CSP contact information:	The name, location and relevant contact information for the CSP.	*N/A*	
2.10.2 Relying Party validation procedures and usage:	A description of the different classes of Service offered by the CSP, corresponding validation procedures, and any restrictions on usage of the Service deliverables.	*N/A*	
2.10.3 Reliance limits:	The reliance limits, if any.	*N/A*	
2.10.4 Obligation of subscribers	The description of, or reference to, the critical subscriber obligations.	*N/A*	
2.10.5 Checking obligations of relying parties:	The extent to which relying parties are obliged to check the status of Service deliverables, and references to further explanation.	*N/A*	
2.10.6 Limited warranty & disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	*N/A*	
2.10.7 Applicable agreements, Service Practice Statement	Identification and references to applicable agreements and Service Policy and Practice	*N/A*	

Service Policy:	statements.		
2.10.8 Privacy policy:	A description of and reference to the applicable privacy policy, if any.	***N/A***	
2.10.9 Refund policy:	A description of and reference to the applicable refund policy, if any.	***N/A***	
2.10.10 Applicable law and dispute resolution:	Statement of the choice of law and dispute resolution mechanism.	***N/A***	
2.10.11 CSP and repository licenses, trust marks, and audit:	Summary of any governmental licenses, seal programs and a description of the audit process and, if applicable, the audit firm.	***N/A***	

3. CERTIFICATE AUTHORITY APPROVAL PROFILE (TSD0102, ISSUE 3.0)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services may be assessed by *tScheme*-recognised assessors. It addresses the provision of a Certification Authority Service and may be one of a selection that a CSP has identified within the definition of its Service Subject to Assessment (SSA).

To be granted *tScheme* Approval for Services that together make up the full Certification Authority Service, whether operated directly by the organisation offering the Certification Authority Service or whether outsourced to various other third parties, the CSP is required to fulfil the additional criteria defined this section, plus those in the following sections relating to the mandatory, constituent services:

- Certificate Generation (see §4);
- Certificate Dissemination (see §5);
- Certificate Status Management (see §6);
- Certificate Status Validation (see §7);
- Registration (see §8).

The provision of a constituent service relating to Signing Key Management (see §9) is optional.

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
3.1 How the constituent parts are delivered For each SSA, the Assessor's Service Definition shall specify how the Service's constituent parts are delivered.	***ASD-010***	
3.2 Record of subscriber obligations: The CSP shall record the Subscriber's agreement to all their defined obligations.	***CP-070***	

## 3.3 Internal audit records: The CSP shall have in place documented internal audit procedures. Records shall be maintained and evidence of their application provided.	***RECS-040***	
## 3.4 Management authority and responsibility: The CSP shall have a high-level management body with final authority and responsibility for approving the Certificate Policy and Certification Practice Statement, including oversight of its proper implementation.	***IPAR-010***	

4. CERTIFICATE GENERATION APPROVAL PROFILE (TSD0104, ISSUE 3.0)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services may be assessed by *tScheme*-recognised assessors. It addresses the provision of a Certificate Generation Service and may be one of a selection that a CSP has identified within the definition of its Service Subject to Assessment.

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
4.1 Destruction of Signing Keys The CAs signing keys stored on its cryptographic hardware are destroyed upon device retirement.	***CC-090***	
4.2 Response Time for Certificate Generation The response times which it offers to properly authenticated authorisations for certificate generation shall be made available to potential users of the Service by being present in either the Service's Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description, as appropriate to their purpose.	***SI-040***	
4.3 CA Algorithm and Key Length Support The CA cryptographic algorithms and key lengths supported shall be made available to potential users of the Service by being present in either the Service's Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description, as appropriate to their purpose.	***SI-060***	
4.4 Conditions of issuance of a new certificate The CSP shall issue a new certificate using the subscriber's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's intended lifetime and no indications exist that the subscriber's private key has been compromised.	***CC-100***	

## 4.5 Actions Taken on Certificate Generation Requests The CSP shall capture and retain records of all certificate generation request, whether such requests are fulfilled or rejected.	***RECS-030***	
## 4.6 Authentication Data The CSP shall capture and retain records of the authentication data relating to the source of a certificate generation authorisation and the information provided with it (e.g. registration data, identity of requesting party, …).	***RECS-060***	
## 4.7 Service Changes Additionally, the CSP shall keep records of any Service-specific changes in status that may affect their claim of conformance with this *tScheme* Approval Profile (or any on which a claim of conformance is based).	***RECS-090***	
## 4.8 Protection of access to records All records shall be protected against unauthorised access and be made available within a reasonable period following a properly justified and authorised request.	***RECS-110***	

5. CERTIFICATE DISSEMINATION APPROVAL PROFILE (TSD0105, ISSUE 3.0)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services may be assessed by *tScheme*-recognised assessors. It addresses the provision of a Certificate Dissemination Service and may be one of a selection that a CSP has identified within the definition of its Service Subject to Assessment (SSA).

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
5.1 Certificate Dissemination under CP The manner in which dissemination is conducted in accordance with the Certificate Policy of the CA shall be made available to potential users of the Service (including relying parties) by being present in either the Service's Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description.	***SI-010***	
5.2 Certificate Dissemination Requests The manner in which requests for the dissemination of certificates may be received and are authenticated shall be made available to potential users of the Service (including relying parties) by being present in either the Service's Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description.	***SI-020***	
5.3 Certificate Dissemination Response The response times which it offers to properly authenticated requests for certificate provision, and where also requested, publication shall be made available to potential users of the Service (including relying parties) by being present in either the Service's Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description.	***SI-030***	

## 5.4 Certificate Dissemination Manner The manner in which Certificates are disseminated (e.g. active 'push' to the subscriber, or passive 'pull' from the subscriber) shall be made available to potential users of the Service (including relying parties) by being present in either the Service's Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description.	***SI-040***	
## 5.5 Certificate Provision Mechanism The CSP shall state clearly the mechanisms by which certificates are provided to subscribers.	***SI-070***	
## 5.6 Certificate Publication Mechanism The CSP shall state clearly the mechanisms by which certificates are published for relying party access.	***SI-080***	
## 5.7 Internal Audit Records The CSP shall show that they have in place appropriate audit procedures to apply self-monitoring and provide evidence of such records where the Service is already Operational.	***RECS-080***	
## 5.8 Access to record protected These records shall be protected against unauthorised access and be made available within a reasonable period following a properly justified and authorised request.	***RECS-090***	

6. CERTIFICATE STATUS MANAGEMENT APPROVAL PROFILE (TSD0106, ISSUE 3.0)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services may be assessed by *tScheme*-recognised assessors. It addresses the provision of a Certificate Status Management Service and may be one of a selection that a CSP has identified within the definition of its Service Subject to Assessment.

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
6.1 Assumptions relating to Certificate Status Services Any assumptions relating to the relationship with associated Certificate Status Services shall appear either in the Service's Service Practice Statement or in the Assessor's Service Definition.	***SI-130***	
6.2 No Reinstatement Once a certificate is definitively revoked (i.e. not suspended), it shall not be reinstated.	***IP-020***	

7. CERTIFICATE STATUS VALIDATION APPROVAL PROFILE (TSD0107, ISSUE 3.0)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services may be assessed by *tScheme*-recognised assessors. It addresses the provision of a Certificate Status Validation Service and may be one of a selection that a CSP has identified within the definition of its Service Subject to Assessment.

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
7.1 Authorisation and authentication of requests The CSP needs to define who is authorised to access a certificate's status and how are they authenticated.	***SI-050***	
7.2 Authorised Certificate Status Management Services The rules governing which Certificate Status Management Services are permitted to notify the service of a change of a certificate's status and how they are authenticated.	***SI-080***	
7.3 Assured integrity The CSP needs to define how the integrity of the status information is assured.	***SI-090***	
7.4 Assured Confidentiality The CSP needs to define how the confidentiality of the request and response is assured.	***SI-100***	
7.5 Process Documentation The validation process shall be fully documented and cover all expected situations, for example how failures are managed and recorded.	***IP-010***	

8. REGISTRATION AUTHORITY APPROVAL PROFILE (TSD0042, ISSUE 3.1)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services may be assessed by *tScheme*-recognised assessors. It addresses the provision of a Registration Service and may be one of a selection that a CSP has identified within the definition of its Service Subject to Assessment.

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
8.1 Proxy Verification If registration proxies are accepted, it is necessary for the CSP to verify the authority of the proxy to act for the registrant concerned. The method of proxy verification shall be shown to be consistent with that of the registrant proper.	***PROX-010***	
8.2 Verification of Registration Information Changes If, subsequent to initial registration and verification, the CSP is informed that any registration information has changed, the CSP shall verify the information.	***RA-030***	
8.3 Agreement on Registration Information Changes If, subsequent to initial registration and verification, the CSP is informed that any registration information has changed, the CSP shall agree it with the subscriber or the subscriber's proxy.	***RA-040***	
8.4 Secure Credential Delivery The resulting credentials shall be delivered using an appropriately secure channel. The scope of the ISMS covering the RA functions may exclude the delivery of credentials where this is covered by the ISMS of a connected Service.	***DC-010***	

## 8.5 All Processes and Expected Situations Documented The registration and verification process shall be fully documented and cover all expected situations, for example how failed verifications are managed and recorded.	***IP-010***	
## 8.6 Maintenance of Records The CSP shall maintain timed and dated records of each registration and verification.	***RECS-010***	
## 8.7 Security of records The Service Provider shall secure from loss, destruction, unauthorised amendment and falsification all records of registration and verification. These records may consist of an electronic or paper tick-sheet type records or copies of source credentials.	***RECS-020***	
## 8.8 Record of all information and documentation used The record shall cover all of the information and documentation used to verify the registrant's identity. Specifically it shall include:	***RECS-030***	
### 8.8.1 Record of document reference numbers Document reference numbers;	***RECS-040***	
### 8.8.2 Record of document validity limitations Any document validity limitations;	***RECS-050***	
### 8.8.3 Record of type of document(s) presented Type of document(s) presented;	***RECS-060***	
### 8.8.4 Record of documentation identification Record of unique identification data, numbers, or a combination thereof, of identification documents, if applicable;	***RECS-070***	
### 8.8.5 Record where applications and document copies stored Storage location of copies of applications and identification documents;	***RECS-080***	

8.8.6 Record of proof of agreement Proof of subscriber acceptance of subscriber agreement;	***RECS-090***	
8.8.7 Record of agreement choices made Any specific choices in the subscriber agreement (e.g. consent to publication of any resulting certificate);	***RECS-100***	
8.8.8 Record of identity of who accepted the application Identity of entity accepting the application;	***RECS-110***	
8.8.9 Record of document validation method Method used to validate identification documents, if any;	***RECS-120***	
8.8.10 Record of receiving and/or transmitting Trust Services Name of receiving Trust Service and/or submitting Trust Service, if applicable;	***RECS-130***	
8.8.11 Proof of consent regarding record retention The Service Provider shall make and document proof of consent from the subscriber regarding record retention.	***RECS-140***	

9. SIGNING KEY PAIR MANAGEMENT APPROVAL PROFILE (TSD0103, ISSUE 3.1)

This Approval Profile is one of a number developed by *tScheme* against which CSPs offering Electronic Trust Services may be assessed by *tScheme*-recognised assessors. It addresses the provision of Key Management Services for private/public key pairs intended to be used for production and verification of digital signatures. The Service may be one of a selection that a CSP has identified within the definition of its Service Subject to Assessment.

The following items are the additional criteria to be covered during the assessment of a CSP:

Item	*tScheme* criterion reference	Status
9.1 Omissions made known The *tScheme* Assessment of a Signing Key Pair Management Service will potentially review the following areas: Signing Key Pair Generation, Signing Key Provision, Verification Key Provision, Signing Capability Provision and Signing Capability Revocation. Not all of these areas need be supported, but omissions shall be made known in an easily understandable way to subscribers.	***CR-020***	
9.2 Signing Key Pair generation and provision If this Service is provided, the following information shall be made available to potential users by being present in either the Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description, as appropriate:	***N/A***	
9.2.1 Algorithms supported Which signing cryptographic algorithms keys can be provided for the service.	***SGSI-020***	
9.2.2 Means of subscriber generation If key pairs are generated by subscribers, how the means of generation are provided, whether in the form of supplied key generation software or hardware or as instructions in the use of third party software or hardware.	***SGSI-030***	
9.2.3 Subscriber generation requirements If key pairs are generated by subscribers, any quality or size requirements which are imposed and verified.	***SGSI-040***	

9.2.4 Authentication and authorisation of key owners How recipients are authenticated and authorised and the method of key provision to a signature creation device, with particular reference to the security of provision.	***SGSI-060***	
9.2.5 Provision of verification key How the corresponding verification key is provided to the subscribers or verifiers.	***SGSI-070***	
9.2.6 Notification of source of information In addition, subscribers shall be explicitly informed of where to find this information.	***SGSI-080***	
9.3 Signing capability provision If this Service is provided, the following information shall be made available to potential users by being present in either the Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description, as appropriate to their purpose:	***N/A***	
9.3.1 Separate signer authentication If separate signer authentication is required in order to release the signing key for use, it shall describe the authentication mechanism, how failures are handled and the scope of an authentication event in terms of the number of signing operations or period of time for which authentication remains valid.	***SCSI-040***	
9.3.2 Multiple signing keys supported The information on whether multiple signing keys are supported and if so, how they are to be selected shall be made available to subscribers.	***SCSI-060***	
9.3.3 Provision for carrying certificates The information on any provision for carrying certificates shall be made available to subscribers.	***SCSI-080***	
9.4 Signing capability revocation If this Service is provided, the following information shall be made available to potential users by being present in either the Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description, as appropriate to their purpose:	***N/A***	
9.4.1 Agents authorised to disable key Which agents have the power and authority to disable use of the subscriber's private key(s) to create signed messages.	***SRSI-010***	

9.4.2 Cause of disablement and how notified Under what circumstances this disablement will be carried out, and how the subscriber will be notified.	***SRSI-020***	
9.4.3 Subscriber request for signing capability removal Any means by which subscribers may request the removal of their own signing capability, in particular when no longer in possession of the signature creation device.	***SRSI-030***	
9.4.4 Subscriber authentication for removal request The means by which a subscriber will be authenticated on requesting removal of own signing capability.	***SRSI-040***	
9.4.5 Disablement liability lag The likely lag between a request for disablement and actual disablement, and the liability of the subscriber for signed messages in the interim.	***SRSI-050***	
9.4.6 Permanence of disablement Whether the disablement is permanent, and if not, how it can be reversed.	***SRSI-060***	
9.4.7 Selectivity of disablement How selective is disablement, such as whether keys can be disabled individually, and what other consequences – if any – this disablement may have on the functioning of devices used to hold the signing keys.	***SRSI-070***	
9.4.8 Existence of signature revocation capability That the signature revocation capability exists, as described to the subscribers;	***SRSI-080***	
9.4.9 Means by which signature revocation achieved Without prejudice to security and commercial confidentiality, the means by which the revocation is achieved;	***SRSI-090***	
9.4.10 Relationship of signature revocation to certificate revocation Whether signing revocation occurs alongside or as a replacement for certificate revocation;	***SRSI-100***	
9.4.11 How signature revocation publicised How signature revocation is publicised, if not via corresponding certificate revocation;	***SRSI-110***	
9.4.12 CSP responsibility for signatures after published revocation What responsibility the CSP will accept for signatures created by keys after any publicised statement that these keys have been disabled.	***SRSI-120***	

10. REFERENCES

[Dir 99/93] EC Directive 1999/93/EC on a Community framework for electronic signatures.

[tSd 0102] Approval Profile for a Certification Authority.

