Issued

Approval Profile for Signing Key Pair Management

Ref. tSd 0103

Issue 3.02

2004-08-26

Executive summary

This document defines the *tScheme* criteria against which organisations must be successfully assessed in order to be eligible for a Grant of Approval or *tScheme*-Ready Status for the provision of Services or Components that enable subscribers to Trust Services to create digital signatures.

QC:
Where text appears in the body of the document in a box headed 'QC' (as is this box) that text relates specifically to Services or Components claiming to offer Services in support of Qualified Certificates (QC), Advanced Electronic Signatures and/or Secure Signature Creation Devices as defined in [DIR 99/93] on a Community framework for electronic signatures, and such Services or Components must fulfil the requirements expressed or indicated within that box.

Individual copies of this document may be downloaded from http://www.*tScheme*.org.

The definitive version of this document is the one available for public download from http://www.*tScheme*.org/ in Adobe Acrobat Reader format. This document is subject to revision so please check that you have the current version.

Please report errors and address comments to Editors@*tScheme*.org.

Copyright: This document may be copied in whole or part for private research and study but not otherwise without the express permission of *tScheme* Limited. All copies must acknowledge *tScheme* Limited's copyright. These restrictions apply to copying in all media.

DOCUMENT HISTORY

Status	Issue	Date	Comment	Authorised
tS	1.00	2001-5-30	First version ratified by the board. This version produced prior to document management procedures introduced 2001-09-21.	*tScheme* Board
tSd	2.00	2001-11-13	Incorporates the following changes: 1. changes reflecting Disposition tS0163 Version 0.03, 2001-07-24. The only substantive change here is that subscriber agreement in bullet 8 of Section 3.2 need no longer be "written", but simply needs to be "prior"; 2. Bullet 6 of Section 3.1 now reflects the fact that a verification key may be provided to verifiers as well as, or instead of, to subscribers; 3. Bullet 22 of the QC paragraphs in Section 3.1 reflects the fact that it is only the private key that needs to be delivered, not the pair; 4. minor editorial changes, including: correction of syntactic errors, incorporation of document maintenance automation, various minor changes in conformance with new document management standards (including the type letter "d" added to the document reference) and the addition of this document history.	*tScheme* Board
tSd	3.00	2002-06-25	Incorporates the following changes: Editorial: 1. Removal of §4 'About evidence'. 2. Incorporation of criteria tagging. 3. Addition of a linked Clause compliance table. 4. Incorporation of *tScheme*-Ready text. 5. A definition of Qualified Electronic Signature has been added in a footnote 6. Minor editorial changes to achieve better consistency across the different Approval Profiles. 7. Reference to 'Model Specification of Service Subject to Assessment' rather than 'Preparing for an Assessment', which also includes removal of opportunity to have more than one Service within the scope of an S3A. Affecting Assessment: 1. Requirements relating to how and to whom Service information is to be presented have been clarified and harmonised across all of the Approval Profiles. Specific forms of presentation are required, and a distinction is now made	*tScheme* Board

© *tScheme* Limited, 2004 - all rights reserved

Status	Issue	Date	Comment	Authorised
			between information that is to be provided to users and information that is to be provided for the Assessors. 2. The "Service Being Provided" requirement has been relaxed to avoid the Catch 22 situation of *tScheme* requiring a Service to be already in use with customers who may not be prepared to use it until it has acquired *tScheme* approval.	
tSd	3.01	2003-03-20	Update 'Date completed' in document properties to put correct date on front page.	*tScheme* Secretariat
tSd	3.02	2004-07-28	Incorporates the following changes: 1. Modify SGSI-010 to cover method of distribution as well as generation; 2. Renumber second instance of SCSI-080 to be SCSI-110.	*tScheme* Secretariat

© *tScheme* Limited, 2004 - all rights reserved

CONTENTS

1. INTRODUCTION 5

1.1 CONVENTIONS 5
1.2 GENERAL 5

2. SCOPE AND RELATION TO OTHER PROFILES. 6

3. CRITERIA 7

3.1 SIGNING KEY PAIR GENERATION AND PROVISION 7
3.1.1 Service information 7
3.1.1.1 Information for users 7
3.1.1.2 Information for Assessors 8
3.1.2 Specific QC criteria 9
3.2 SIGNING CAPABILITY PROVISION 11
3.2.1 Service information 11
3.2.1.1 Information for users 11
3.2.1.2 Information for Assessors 12
3.2.2 Specific QC criteria 12
3.3 SIGNING CAPABILITY REVOCATION 13
3.3.1 Service information 13
3.3.1.1 Information for users 13
3.3.1.2 Information for Assessors 14
3.4 RECORDING 14

4. REFERENCES 15

ANNEX 1. CLAUSE COMPLIANCE LIST 16

© *tScheme* Limited, 2004 - all rights reserved

1. INTRODUCTION

1.1 Conventions

For ease of reference from other documents, each clause is given a tag and a title, adopting the general form of a Common Criteria Protection Profile, as follows:

GENID-000 Text describing the Clause Tag

1.2 General

This Approval Profile is one of a number developed by *tScheme* against which TSPs offering 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 the purpose of producing and verifying digital signatures. The Service may be one of a selection that a TSP has identified within the definition of its Service Subject to Assessment. This Profile shall, as a minimum, be applied in combination with the Base Approval Profile.

Full details of Approval Profiles and the Approval Process may be found on the *tScheme* website.

Definitions of terms and acronyms not defined in this document may be found in the *tScheme* Glossary of Terms

Although the wording of this Approval Profile relates to Assessments for *tScheme* Service Approvals, the Profile is also intended to be applicable to *tScheme*-Ready Assessments. For use in the latter context:

- references to “Service Provider” shall be taken to mean “Component Supplier”;
- references to “Service” shall be taken to mean “Service Component”;
- references to “Service Subject to Assessment”, or SSA, shall be taken to mean “Component Subject to Assessment”, or CSA;
- references to “Specification of Service Subject to Assessment”, or S3A shall be taken to mean “Specification of Service Component Subject to Assessment”, or C3A.

© *tScheme* Limited, 2004 - all rights reserved

2. SCOPE AND RELATION TO OTHER PROFILES.

The criteria given in this Approval Profile are related to the provision of Key Management Services that enable subscribers to Trust Services, or Trust Services themselves to create digital signatures. Specific aspects of these Services include:

1. generation of (or provision of the means of generating) private signing and public signature verification key pairs (each key of which is from now on referred to respectively as: Signing Key and Verification Key);
2. provision of private signing keys, either unassigned[1] or to their rightful[2] subscribers and their protection and control;
3. provision of public verification keys, either unassigned, or to their rightful subscribers, and/or to a Certificate Generation Service;
4. provision to subscribers of the means of creating signatures using the private signing keys;
5. signing capability revocation, i.e. the disablement of private signing keys under the subscriber or TSP's instructions.

This Approval Profile does not address the use of private/public key pairs for any cryptographic purpose other than signing. It does not require the Service to preclude these other uses of the key pairs it manages.

It excludes the provision of Signature Creation Systems and complete Signature Creation Environments[3].

With the exception of the Base Approval Profile, the criteria given in this Approval Profile are not directly related to any other Approval Profiles, i.e. this Profile may be used in isolation and is not dependent upon a successful Assessment against any other Approval Profile.

1 This alludes to the type of Service via which the signing key is placed unassigned on a smart-card, the user of that card being assigned at a later date.

2 "Rightful subscriber" is the subscriber whose identity is bound to the private signing key.

3 These terms are used here in the sense described in [CEN/ISSS WS/E-Sign; N91]

© *tScheme* Limited, 2004 - all rights reserved

3. CRITERIA

The applicability of this Approval Profile shall be described in a "Specification of Service Subject to Assessment" (S3A) as defined in "Model Specification of Service Subject to Assessment".

CR-010 Operational Service

Each SSA shall be an Operational Service (in the sense defined in the *tScheme* Glossary of Terms) supporting the statements given in response to the criteria listed in the relevant sections below.

CR-020 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.

Compliance with this Approval Profile will then be achieved by satisfying the criteria in the succeeding sub-sections.

3.1 Signing Key Pair generation and provision

3.1.1 Service information

3.1.1.1 Information for users

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:

SGSI-010 Generation and distribution methods, key size and quality

- if key pairs are generated by the TSP, the method of generation and distribution, the key size and the cryptographic quality controls applied[4];

SGSI-020 Algorithms supported

- which signing cryptographic algorithms keys can be provided for;

SGSI-030 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-040 Subscriber generation requirements

- if key pairs are generated by subscribers, any quality or size requirements which are imposed and verified;

If a Key Pair Provision Service is provided, subscribers shall be informed of:

4 For example the avoidance of weak keys.

© *tScheme* Limited, 2004 - all rights reserved

SGSI-060 Authentication and authorisation of key owners

- how recipients are authenticated and authorised, and the method of key provision to a signature creation device[5], with particular reference to the security of provision;

SGSI-070 Provision of verification key

- how the corresponding verification key is provided to the subscriber and/or verifiers.

SGSI-080 Notification of source of information

- In addition, subscribers[6], shall be explicitly informed of where to find this information.

3.1.1.2 Information for Assessors

If this Service is provided, the following information shall appear either in the Service Practice Statement or in the Assessor's Service Definition (*tScheme* does not require it to be made generally available):

SGSI-100 Key privacy and integrity

- the methods used to ensure signing key privacy and verification key integrity, particularly how the TSP ensures and demonstrates that neither they nor, though their agency, any third party retain knowledge of the private key.

QC:

In addition, where the TSP is claiming compliance to support the creation of advanced electronic signatures as defined in Article 2/2 of [DIR 99/93], the TSP shall define and document:

SGSI-110/QC Linkage of key pair to subscriber

- the means by which a generated key pair is uniquely linked to a subscriber;

SGSI-120/QC Identification of subscriber

- the manner in which the subscriber can be identified;

SGSI-130/QC No means of signing without key

- the basis for trusting that a signature created with the signing key could not be practically created by any other means;

SGSI-140/QC Key under sole control of subscriber

- the means of ensuring that the signing key is kept under the sole control of the subscriber.

5 As defined in Article 2/5 of [DIR 93/99], consisting of configured software or hardware used to store and apply the signing key.

6 Or in the case of signing keys being provided to a commercial organization for later assignment to individual subscribers, the organization.

© *tScheme* Limited, 2004 - all rights reserved

QC:

In addition, where the TSP is claiming its Signing Key Generation Service is part of a Certification Service complying with the requirements of [DIR 99/93] for the provision of qualified certificates, the TSP shall define and document:

SGSI-150/QC Keys passed to certificate generator reliably

- the means by which the signature verification key of the generated key pair is reliably passed to a certificate generation TSP so as to be uniquely linked to the subscriber;

SGSI-160/QC Subscriber verification prior to receiving certificate

- the means by which the identity of the subscriber is verified prior to generation, or allocation to the subscriber[7], of the certificate (whether before or after the creation of the key pair);

SGSI-170/QC Trusted key generation

- the basis for trust in the systems and products which ensure the cryptographic security of the key generation process;

SGSI-180/QC Non-forgery of certificates and confidentiality of signing key

- the measures taken against forgery of certificates and the means of guaranteeing confidentiality of the signing key during the generation process, even where the TSP performs key generation;

SGSI-190/QC Non-retention or revelation of signing key

- an undertaking not to retain, copy or reveal to third parties the subscriber's signing key.

3.1.2 Specific QC criteria

QC:

In addition, if the Public Service Description claims to support a means of signing (see Signing Capability Provision) which constitutes a Secure Signature Creation Device, as defined by Article 2/6 of [DIR 99/93], then the Service shall additionally meet the requirements of Annex III of [DIR 99/93], specifically the signing key:

SGQC-010/QC Signing key assured and occurs only once

- can practically occur only once and its secrecy is reasonably assured;

SGQC-020/QC Signing key cannot be derived

- cannot, with reasonable assurance, be derived (for instance from the published verification key);

SGQC-030/QC Subscriber can protect against others' use

- can be reliably protected by the subscriber against use by others.

7 This covers the case of certificates being generated containing pseudonyms that are mapped onto real names later.

© *tScheme* Limited, 2004 - all rights reserved

QC:

Also, if the Public Service Description claims that Qualified Electronic[8] Signatures will be able to be performed using private keys. The following criteria will be applied:

If the TSP generates the subscriber keys:

SGQC-040/QC Generation algorithm fit for purpose

- they shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures;

SGQC-050/QC Use algorithm and key length fit for purpose

- they shall be of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of qualified electronic signatures[9];

SGQC-060/QC Secure generation and storage prior to delivery

- they shall be generated and stored securely before delivery to the subscriber.

SGQC-070/QC Key not compromised during delivery to correct subscriber

- the subscriber's private key shall be delivered to the subscriber[10] in a manner such that the privacy of the key is not compromised and on delivery only the subscriber has access to its private key.

If the subscriber generates its own keys, the subscriber shall be obliged through written agreement to:

SGQC-090/QC Subscriber generation algorithm fit for purpose

- generate the keys using an algorithm recognized as being fit for the purposes of qualified electronic signatures;

SGQC-100/QC Subscriber uses algorithm and key length fit for purpose

- use a key length and algorithm that is recognized as being fit for the purposes of qualified electronic signatures.

8 A Qualified Electronic Signature is an Advanced Electronic Signature which is based on a qualified certificate and which is created by a secure-signature-creation device, as defined in article 5.1 of [DIR 99/93].

9 It is currently proposed that the recognition of algorithms, with associated key length, being fit for the purposes of qualified certificates is through a cryptographic advisory panel under the committee identified in article 9 of the [DIR 99/93]

10 Or if not pre-assigned, to the assignment organization for which the TSP is providing the Service.

© *tScheme* Limited, 2004 - all rights reserved

3.2 Signing capability provision

3.2.1 Service information

3.2.1.1 Information for users

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:

SCSI-010 Types and functionality of devices on offer

- the types of signature creation device on offer, including their functionality (especially whether the device supports other functions not related to the performance of electronic signatures);

SCSI-020 Environmental constraints

- the environmental constraints and requirements for operating the signing device;

SCSI-030 Protection of signing key

- how the signing key is protected from unauthorised disclosure or misuse, including any end user management responsibilities;

SCSI-040 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 the authentication remains valid;
- The following information shall be made available to subscribers:

SCSI-050 Strength and integrity of signature creation process

  – the cryptographic strength of the signature creation process and the measures implemented to guard against forgery;

SCSI-060 Multiple signing keys supported?

  – whether multiple signing keys are supported and if so, how they are to be selected;

SCSI-070 Signing event logging

  – any facilities for the logging of signing related events;

SCSI-080 Provision for carrying certificates

  – any provision for carrying certificates.

Subscribers presented with signing keys shall be obliged through prior agreement[11] to:

SCSI-090 Subscribers to exercise care

- exercise reasonable care to avoid unauthorised use of the key;

SCSI-100 Subscriber obligations to notify TSP

- notify the TSP without unreasonable delay, if any of the following occur up to the end of the validity period of the key[12]: the subscriber's private key has been lost, stolen, potentially

11 The level of robustness required of the evidence for this agreement will depend on the commitment the subscriber is making and the level of reliance on the Service.

© *tScheme* Limited, 2004 - all rights reserved

compromised; or control over the subscribers private key has been lost due compromise of activation data (e.g. PIN code) or other reasons.

SCSI-110 Notification of source of information

In addition, subscribers[13] shall be explicitly informed of where to find this information.

3.2.1.2 Information for Assessors

No specific additional information has been identified.

3.2.2 Specific QC criteria

QC:

In addition, if the Public Service Description claims to provide a means of signing which constitutes a Secure Signature Creation Device (SSCD), as defined by Article 2/6 of [DIR 99/93], then the Service shall additionally meet the requirements of Annex III of [DIR 99/93]. Specifically, the TSP shall show that the device ensures that the signing key:

SCQC-110/QC Signing key can occur only once

- can practically occur only once and its secrecy is reasonably assured;

SCQC-120/QC Key cannot be derived or signature forged

- cannot, with reasonable assurance, be derived using currently available technology[14] and the signature is protected against forgery;

SCQC-130/QC Subscriber can protect

- can be reliably protected by the subscriber against use by others;

and that the signature creation device:

SCQC-140/QC Signed data not altered or hidden

- cannot alter the data to be signed nor prevent such data from being presented to the signatory prior to the signature process.

12 As may be indicated in an associated Public Key Certificate.

13 Or in the case of signing keys being provided to a commercial organization for later assignment to individual subscribers, the organization.

14 With some weight being given to predicted developments in cryptanalytic techniques in relation to the anticipated life of the signing keys.

© *tScheme* Limited, 2004 - all rights reserved

The TSP shall also ensure that:

SCQC-150/QC Secure SSCD preparation

- SSCD preparation is securely controlled;

SCQC-160/QC Secure SSCD storage and distribution

- the SSCD is securely stored and distributed;

SCQC-170/QC Secure SSCD deactivation and reactivation

- SSCD deactivation and reactivation is securely controlled;

SCQC-180/QC Secure preparation and distribution of SSCD activation data

- where the SSCD has associated user activation data (e.g. PIN code), the activation data is securely prepared and distributed separately from the SSCD.

3.3 Signing capability revocation

3.3.1 Service information

3.3.1.1 Information for users

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:

SRSI-010 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-020 Cause of disablement and how notified
- under what circumstances this disablement will be carried out, and how the subscriber will be notified;

SRSI-030 Subscriber request for signing capability removal
- any means by which subscribers may request removal of their own signing capability, in particular when no longer in possession of the signature creation device;

SRSI-040 Subscriber authentication for removal request
- the means by which a subscriber will be authenticated on requesting removal of own signing capability;

SRSI-050 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-060 Permanence of disablement
- whether the disablement is permanent, and if not, how it can be reversed;

© *tScheme* Limited, 2004 - all rights reserved

SRSI-070 Selectivity of disablement

- how selective is the 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-080 Existence of signature revocation capability

- that the signature revocation capability exists, as described to the subscribers;

SRSI-090 Means by which signature revocation achieved

- without prejudice to security and commercial confidentiality, the means by which the revocation is achieved;

SRSI-100 Relationship of signature revocation to certificate revocation

- whether signing revocation occurs alongside or as a replacement for certificate revocation;

SRSI-110 How signature revocation publicised

- how signature revocation is publicised, if not via corresponding certificate revocation;

SRSI-120 TSP responsibility for signatures after published revocation

- what responsibility the TSP will accept for signatures created by keys after any publicised statement that these keys have been disabled.

3.3.1.2 Information for Assessors

No specific additional information has been identified.

3.4 Recording

RECS-010 Records of all relevant events

The TSP shall maintain records of all events relating to the life cycle of keys managed and secure them from unauthorised alteration or destruction.

© *tScheme* Limited, 2004 - all rights reserved

4. REFERENCES

[CEN/ISSS WS/E-Sign; N91] "Security Requirements for Signature Creation Systems" Version 3.0 Issued 2000-10-08

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

© *tScheme* Limited, 2004 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for Signing Key Pair Management - clause compliance list

Clause	Description	Compliance
CR-010	Operational Service	
CR-020	Omissions made known	
SGSI-010	Generation and distribution methods, key size and quality	
SGSI-020	Algorithms supported	
SGSI-030	Means of subscriber generation	
SGSI-040	Subscriber generation requirements	
SGSI-060	Authentication and authorisation of key owners	
SGSI-070	Provision of verification key	
SGSI-080	Notification of source of information	
SGSI-100	Key privacy and integrity	
SGSI-110/QC	Linkage of key pair to subscriber	
SGSI-120/QC	Identification of subscriber	
SGSI-130/QC	No means of signing without key	
SGSI-140/QC	Key under sole control of subscriber	
SGSI-150/QC	Keys passed to certificate generator reliably	
SGSI-160/QC	Subscriber verification prior to receiving certificate	
SGSI-170/QC	Trusted key generation	
SGSI-180/QC	Non-forgery of certificates and confidentiality of signing key	
SGSI-190/QC	Non-retention or revelation of signing key	
SGQC-010/QC	Signing key assured and occurs only once	
SGQC-020/QC	Signing key cannot be derived	
SGQC-030/QC	Subscriber can protect against others' use	
SGQC-040/QC	Generation algorithm fit for purpose	

© *tScheme* Limited, 2004 - all rights reserved

Approval Profile for Signing Key Pair Management - clause compliance list

Clause	Description	Compliance
SGQC-050/QC	Use algorithm and key length fit for purpose	
SGQC-060/QC	Secure generation and storage prior to delivery	
SGQC-070/QC	Key not compromised during delivery to correct subscriber	
SGQC-090/QC	Subscriber generation algorithm fit for purpose	
SGQC-100/QC	Subscriber uses algorithm and key length fit for purpose	
SCSI-010	Types and functionality of devices on offer	
SCSI-020	Environmental constraints	
SCSI-030	Protection of signing key	
SCSI-040	Separate signer authentication	
SCSI-050	Strength and integrity of signature creation process	
SCSI-060	Multiple signing keys supported?	
SCSI-070	Signing event logging	
SCSI-080	Provision for carrying certificates	
SCSI-090	Subscribers to exercise care	
SCSI-100	Subscriber obligations to notify TSP	
SCSI-110	Notification of source of information	
SCQC-110/QC	Signing key can occur only once	
SCQC-120/QC	Key cannot be derived or signature forged	
SCQC-130/QC	Subscriber can protect	
SCQC-140/QC	Signed data not altered or hidden	
SCQC-150/QC	Secure SSCD preparation	
SCQC-160/QC	Secure SSCD storage and distribution	
SCQC-170/QC	Secure SSCD deactivation and reactivation	

© *tScheme* Limited, 2004 - all rights reserved

Approval Profile for Signing Key Pair Management - clause compliance list

Clause	Description	Compliance
SCQC-180/QC	Secure preparation and distribution of SSCD activation data	
SRSI-010	Agents authorised to disable key	
SRSI-020	Cause of disablement and how notified	
SRSI-030	Subscriber request for signing capability removal	
SRSI-040	Subscriber authentication for removal request	
SRSI-050	Disablement liability lag	
SRSI-060	Permanence of disablement	
SRSI-070	Selectivity of disablement	
SRSI-080	Existence of signature revocation capability	
SRSI-090	Means by which signature revocation achieved	
SRSI-100	Relationship of signature revocation to certificate revocation	
SRSI-110	How signature revocation publicised	
SRSI-120	TSP responsibility for signatures after published revocation	
RECS-010	Records of all relevant events	

© *tScheme* Limited, 2004 - all rights reserved