Approval Profile for Signing Key Pair Management

Ref. tSd0103

Issue 2.00

2001-11-13

Executive summary

This document defines the *tScheme* criteria against which organisations must be successfully assessed in order to be eligible for approval for the provision of services which 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 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 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

© *tScheme* Limited, 2001 - all rights reserved

CONTENTS

1. INTRODUCTION 4

2. SCOPE AND RELATION TO OTHER PROFILES. 5

3. CRITERIA 6

3.1 SIGNING KEY PAIR GENERATION AND PROVISION 6
3.2 SIGNING CAPABILITY PROVISION 8
3.3 SIGNING CAPABILITY REVOCATION 9
3.4 RECORDING 10

4. ABOUT EVIDENCE 11

5. REFERENCES 12

© *tScheme* Limited, 2001 - all rights reserved

1. INTRODUCTION

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 which a TSP has identified within the definition of its Service(s) Subject to Assessment. This Profile must, 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

© *tScheme* Limited, 2001 - 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 which 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. it 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, 2001 - all rights reserved

3. CRITERIA

The applicability of this Profile to the Service Subject to Assessment must be described in a "Specification of the Service Subject to Assessment" (S3A) as defined in "Preparing for an Assessment".

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 must 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

If these services are provided, the following information must be made available to subscribers and verifiers. In addition, subscribers[4], must be explicitly informed of where to find this information:

1. if key pairs are generated by the TSP, the method of generation, the key size and the cryptographic quality controls applied[5];
2. which signing cryptographic algorithms keys can be provided for;
3. 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, and any quality or size requirements which are imposed and verified;
4. 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.

If no support is provided for key pair generation, the TSP must define and document any quality or size requirements which are imposed and verified on the subscriber-generated keys.

If a Key Pair Provision service is provided, subscribers must be informed of:

5. how recipients are authenticated and authorised, and the method of key provision to a signature creation device[6], with particular reference to the security of provision;
6. how the corresponding verification key is provided to the subscriber and/or verifiers.

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

5 For example the avoidance of weak keys.

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

© *tScheme* Limited, 2001 - all rights reserved

QC:

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

7. the means by which a generated key pair is uniquely linked to a subscriber;
8. the manner in which the subscriber can be identified;
9. the basis for trusting that a signature created with the signing key could not be practically created by any other means;
10. the means of ensuring that the signing key is kept under the sole control of the subscriber.

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 must define and document:

11. 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;
12. 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);
13. the basis for trust in the systems and products which ensure the cryptographic security of the key generation process;
14. 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;
15. an undertaking not to retain, copy or reveal to third parties the subscriber's signing key.

QC:

In addition, if the 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 must additionally meet the requirements of Annex III of [DIR 99/93], specifically the signing key:

16. can practically occur only once and its secrecy is reasonably assured;
17. cannot, with reasonable assurance, be derived (for instance from the published verification key);
18. 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, 2001 - all rights reserved

QC:

Also, if the service description claims that Qualified Electronic Signatures will be able to be performed using private keys. The following criteria will be applied:

If the TSP generates the subscriber keys:

19. they must be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures;
20. they must 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[8];
21. they must be generated and stored securely before delivery to the subscriber.
22. the subscriber's private key must be delivered to the subscriber[9] 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 must be obliged through written agreement to:

23. generate the keys using an algorithm recognized as being fit for the purposes of qualified electronic signatures;
24. use a key length and algorithm which is recognized as being fit for the purposes of qualified electronic signatures.

The TSP must at the time of assessment be providing a service which supports these statements.

3.2 Signing Capability Provision

If this service is provided, subscribers must be informed of:

1. 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);
2. the environmental constraints and requirements for operating the signing device;
3. how the signing key is protected from unauthorised disclosure or misuse, including any end user management responsibilities;
4. if separate signer authentication is required in order to release the Signing Key for use, it should 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;
5. The following information must be made available to subscribers:
   - the cryptographic strength of the signature creation process and the measures implemented to guard against forgery;
   - Whether multiple signing keys are supported and if so, how they are to be selected;
   - any facilities for the logging of signing related events;
   - any provision for carrying certificates.

8 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]

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

© *tScheme* Limited, 2001 - all rights reserved

Subscribers presented with signing keys must be obliged through prior agreement[10] to:

6. exercise reasonable care to avoid unauthorised use of the key;
7. notify the TSP without unreasonable delay, if any of the following occur up to the end of the validity period of the key[11]: the subscriber's private key has been lost, stolen, potentially compromised; or control over the subscribers private key has been lost due compromise of activation data (e.g. PIN code) or other reasons.

QC:

In addition, if the 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 must additionally meet the requirements of Annex III of [DIR 99/93]. Specifically, the TSP must show that the device ensures that the signing key:

8. can practically occur only once and its secrecy is reasonably assured;
9. cannot, with reasonable assurance, be derived using currently available technology[12] and the signature is protected against forgery;
10. can be reliably protected by the subscriber against use by others;

and that the signature creation device:

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

The TSP must also ensure that:

12. SSCD preparation is securely controlled;
13. the SSCD is securely stored and distributed;
14. SSCD deactivation and reactivation is securely controlled;
15. where the SSCD has associated user activation data (e.g. PIN code), the activation data is securely prepared and distributed separately from the SSCD.

The TSP must at the time of assessment be providing a service which supports these statements.

3.3 Signing Capability Revocation

If this service is provided, subscribers must be informed of:

1. which agents have the power and authority to disable use of the subscriber's private key(s) to create signed messages;
2. under what circumstances this disablement will be carried out, and how the subscriber will be notified;
3. 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;

10 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.

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

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

© *tScheme* Limited, 2001 - all rights reserved

4. the means by which a subscriber will be authenticated on requesting removal of own signing capability;
5. the likely lag between a request for disablement and actual disablement, and the liability of the subscriber for signed messages in the interim;
6. whether the disablement is permanent, and if not, how it can be reversed;
7. 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.

In addition, the TSP must make the following information available to subscribers and relying parties:

8. that the signature revocation capability exists, as described to the subscribers;
9. without prejudice to security and commercial confidentiality, the means by which the revocation is achieved;
10. whether signing revocation occurs alongside or as a replacement for certificate revocation;
11. how signature revocation is publicised, if not via corresponding certificate revocation;
12. what responsibility the TSP will accept for signatures created by keys after any publicised statement that these keys have been disabled.

The TSP must at the time of assessment be providing a service which supports these statements.

3.4 Recording

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

© *tScheme* Limited, 2001 - all rights reserved

4. ABOUT EVIDENCE

Most of the evidence required of a TSP is of the same general form whatever the service being assessed. There is some flexibility here, but the specific forms of evidence for each assessment must be agreed with the *tScheme*-recognised Assessor before assessment can start. More information is given in Preparing for an Assessment.

For some Approval Profiles however, there are specific standards[13] that could apply, and to which prior conformance could be demonstrated. Thus, rather than offering point by point evidence, a TSP can offer evidence of already established conformance to appropriate standards. For this Approval Profile, the standards that *tScheme* has identified as being relevant are:

Compliance with Annex III of [DIR 99/93] can be demonstrated by conformance to the following or equivalent standards:

1. [CEN/ISSS WS/E-Sign; N91] - parts related to the SSCD only;
2. [CEN/ISSS WS/E-Sign; N131 & N132];
3. [PKCS #5] - for the interface between the signing capability provision and the Signature Creation System;
4. [DIN V6629]
5. [FIPS-140]

13 Within tScheme's Approval Profiles the term 'standard' is intended to include both formal (de jure) and de facto Standards, recognised industry schemes, and other means of demonstrating levels of performance and practice of similar merit.

© *tScheme* Limited, 2001 - all rights reserved

5. REFERENCES

[DIR.99/93]	EC Directive 1999/93/EC on a Community framework for electronic signatures
[CEN/ISSS WS/E-Sign; N91]	"Security Requirements for Signature Creation Systems" Version 3.0 Issued 2000-10-08
[CEN/ISSS WS/E-Sign; N131 & N132]	"Security Requirements for Secure Signature Creation Devices (version EAL 4 & EAL 4+)
[PKCS #5]	"Cryptographic Token Information Standard" Draft 2 version 1.1 2000-04-27
[DIN V6629]	"Chipcards with Digital Signature Applications/Functions."
[FIPS-140]	FIPS PUB 140-1 (1994 January 11): "Security Requirements for Cryptographic Modules"

© *tScheme* Limited, 2001 - all rights reserved