
Oil & Gas Trust Scheme Requirements

Authors: S. Robinson
Version: 2.0 (Approved)
Date: 01/05/2004

Copyright ©O&G Trust Ruleset 2004. All rights reserved. This document is copyrighted by the O&G Trust Scheme. This document is confidential material, and is intended for use only by O&G Trust Scheme members and authorised agents participating in the O&G Trust Scheme. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes other than those approved by the Oil & Gas Trust Scheme Policy Management Board.

Document Control

Document Ownership

The **Oil & Gas Trust Scheme Policy Management Board** is the entity responsible for the operational policies and procedures described in this document. They are responsible for the ongoing maintenance of this document and for approving all updates and revisions to it.

Document Distribution

This document will be distributed as follows.

Role	Purpose
Oil & Gas Trust Scheme PMB	For approval
Oil & Gas management	For information
All TSP data centre staff	For information

Revision History

Date	Version	Change Made	Department	Person
18/11/03	0.1	Initial draft produced	iSolve Ltd	A. Harris
19/12/03	0.2	Revised draft following initial discussions with TSPs	iSolve Ltd	G. Connell
14/01/04	0.3	Further revisions.	iSolve Ltd	G. Connell
16/01/04	0.4	Inclusion of certificate profile requirements.	iSolve Ltd	G. Connell
23/01/04	0.5	Updates following feedback from TSPs	iSolve Ltd	G. Connell
24/02/04	0.6	Updates following working party review to include: 2.0 removal of liability requirement 2.2 footnote on HMG requirements 2.7 addition of CSV002 for OCSP	iSolve Ltd	G. Connell
05/03/04	1.0	Approved	O&G PMB	S. Robinson
22/04/04	1.1	Updates following consultation to : 2.1 Remove need for url of TSDS in certificate. 2.4 Clarification of fields in certificate. 2.4 Need to include (OGTS) in Subject Organisation Unit field 2.7 Clarify access to OCSP	DTI	S. Robinson
01/05/04	2.0	Approved	O&G PMB	S. Robinson

Standards and Related Documents

<i>Reference</i>	<i>Purpose</i>
HMGVOrg	HMG's Minimum Requirements for Verification of Identity of Organisations
HMGVInd	HMG's Minimum Requirements for Verification of Identity of Individuals
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
TS Base	tScheme Base Approval Profile
TS CA	tScheme Approval Profile for a Certification Authority
TS CD	tScheme Approval Profile for Certificate Dissemination
TS CG	tScheme Approval Profile for Certificate Generation
TS CSM	tScheme Approval Profile for Certificate Status Management
TS CSV	tScheme Approval Profile for Certificate Status Validation
TS SKPM	tScheme Approval Profile for Signing Key Pair Management
TS Reg	tScheme Approval Profile for Registration

Table of Contents

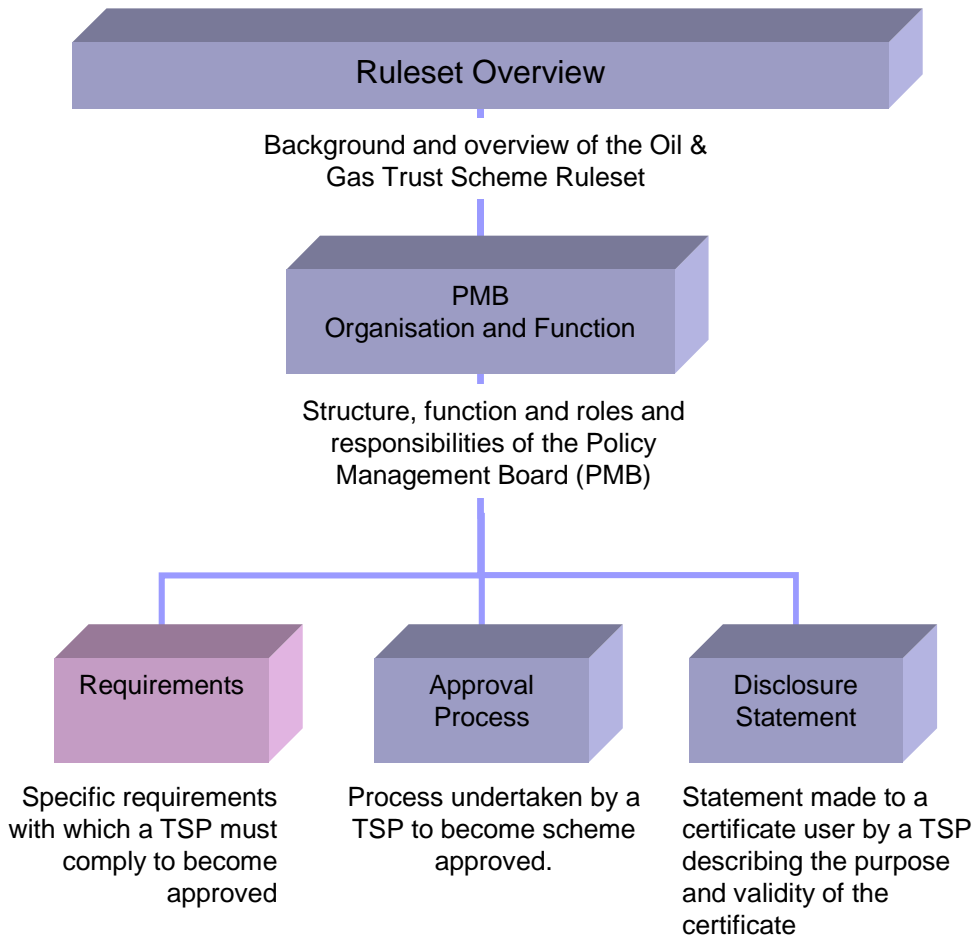
1	<i>Introduction</i>	5
2	<i>Requirements</i>	6
2.1	Base Approval	6
2.2	Certification Authority	6
2.3	Registration	6
2.4	Signing Key Pair Management	6
2.5	Certificate Generation	7
2.6	Certificate Dissemination	8
2.7	Certificate Status Management	8
2.8	Certificate Status Validation	8
3	<i>Compliance Checklist</i>	9

1 Introduction

This Requirements document specifies additional Oil & Gas Trust Scheme requirements that are above and beyond the requirements for tScheme approval. The requirements for tScheme Approval are described in the following documents:

- ◆ tScheme Base Approval Profile
- ◆ tScheme Approval Profile for a Certification Authority
- ◆ tScheme Approval Profile for Certificate Dissemination
- ◆ tScheme Approval Profile for Certificate Generation
- ◆ tScheme Approval Profile for Certificate Status Management
- ◆ tScheme Approval Profile for Certificate Status Validation
- ◆ tScheme Approval Profile for Signing Key Pair Management
- ◆ tScheme Approval Profile for Registration

The diagram below shows the relationship between this Requirements document and the other documents in the Oil & Gas Trust Scheme Ruleset.



2 Requirements

2.1 Certification Authority

The requirements below are those that are additional to those specified in tScheme 's Approval Profile for a Certification Authority.

Req't No	Description	tScheme Reference
CA001	The TSP will make the Oil & Gas Community Trust Service Disclosure Statement (TSDS) available via a URL .	CA App CP-080

2.2 Registration

The requirements below are those that are additional to those specified in tScheme 's Approval Profile For Registration.

Req't No	Description	tScheme Reference
REG001	The verification process must, as a minimum, comply with the Registration Level 2 requirements laid down by the UK Government for the verification of individuals as defined in 'HMG's Minimum Requirements for Verification of Identity of Individuals' and the verification of organisations as defined in 'HMG's Minimum Requirements for Verification of Identity of Organisations'. ¹	Reg App SI-020 Reg App SI-030 Reg App SI-040 Reg App SI-050

2.3 Signing Key Pair Management

The requirements below are those that are additional to those specified in tScheme 's Approval Profile For Signing Key Pair Management.

Req't No	Description	tScheme Reference
SKPM001	All Keys must have a Key length of at least 1024 bits, this relates to both end-user keys and keys in operation at the CA.	SKPM App SGSI-010 CG App SI-060
SKPM002	TSPs must generate their CA Key Pairs in hardware certified to at least FIPS 140-1 level 3.	SKPM App SGSI-060
SKPM003	CA Signing Keys must not exist in plain text outside of the HSM.	SKPM App SGSI-060
SKPM004	Where keys are held in software, adequate organisation policies and practices must be in place to protect the security of keys such that only the authorised or intended user can gain access to the keys.	SKPM App SCSi-010 SKPM App SCSi-020 SKPM App SCSi-030

¹ This does not necessitate TSPs being tScheme approved against the HMG requirements, but a TSP must present evidence as part of the Oil & Gas Trust Scheme Approval Process to demonstrate that its registration process complies with or exceeds these requirements.

2.4 Certificate Generation

The requirements below are those that are additional to those specified in tScheme 's Approval Profile For Certificate Generation.

Req't No	Description	tScheme Reference
CG001	<p>TSPs shall include the fields specified in the table below in end-entity certificates.</p> <p>“Subject – Organisation” should be the company name as registered at Companies House.</p> <p>“Subject – Organisation Unit” should hold an additional indicator (OGTS) after the entry to identify that the certificate has been issued in accordance with the Oil and Gas Trust Scheme, e.g. DTI (OGTS).</p> <p>Dates should be displayed according to eGIF standards.</p> <p>TSPs should avoid setting extension fields to critical to prevent rejection of the certificate by the relying party.</p>	CG App SI-010

Field Name	Description
Version (1, 2 or 3)	The version of the X.509 certificate.
Serial number	Uniquely defines certificate issued by the certificate authority.
Issuer	Identifies the CA that issued certificate. The Distinguished Name (DN) has the following components: CN - Common Name (mandatory) O - Organisation (mandatory) OU - Organisation Unit (mandatory) L - Location (optional) C - Country (mandatory) E - Email (optional) S - State (optional)
Subject	Information about certificate owner. The Distinguished Name (DN) has the following components: CN - Common Name (mandatory) O - Organisation (mandatory) OU - Organisation Unit (mandatory) L - Location (optional) C - Country (mandatory) E - Email (optional) S - State (optional)
Valid from	Start date of certificate period of validity.
Valid to	Ending date of certificate period of validity.
Subject Public Key Info	The subjects public key (1024 bits).
Issuer Unique ID	Uniquely identifies the issuer.
Subject Unique ID	Uniquely identifies the subject.
Signature Algorithm	Contains the identifier for the cryptographic algorithm used by the CA to sign this certificate.
Signature Value	CA signature to confirm certificate validity and authenticity.

2.5 Certificate Dissemination

The requirements below are those that are additional to those specified in tScheme's Approval Profile For Certificate Dissemination.

Req't No	Description	tScheme Reference
CD001	A TSP must make its root and intermediary certificates available to all parties in the Oil and Gas Community of Trust.	CD App SI-010

2.6 Certificate Status Management

The requirements below are those that are additional to those specified in tScheme's Approval Profile For Certificate Status Management.

Req't No	Description	tScheme Reference
CSM001	A TSP must publish a CRL. The CRL must be issued at least once in any 24 hour period. Additionally an OCSP service may be provided.	CSM App SI-090 CSV App SI-070

2.7 Certificate Status Validation

The requirements below are those that are additional to those specified in tScheme's Approval Profile For Certificate Status Validation.

Req't No	Description	tScheme Reference
CSV001	Where an OCSP service is provided it must be made available 24x7. ²	CSV App SI-040 CSV App SI-070
CSV002	Where an OCSP service is provided it must allow unsigned requests for certificate status or an alternative mechanism provided at reasonable cost for applications to make OCSP calls to validate those certificates.	CSV App SI-050

² This means that the general service hours for the OCSP service are 24 hours a day, seven days a week, and it allows for scheduled and emergency outages in accordance with the TSP's SLA.

3 Compliance Checklist

Req't No	Description	Compliance
CA001	URL pointer to Oil & Gas Community of Trust Service Policy Disclosure Statement	
REG001	HMG level 2 verification of individuals and organisations.	
SKPM001	Minimum signing key length of 1024 bits.	
SKPM002	CA keys protected to FIPS 140-1 level 3.	
SKPM003	No plain text versions of signing keys.	
SKPM004	Organisational policies and practices to ensure protection of keys held in software	
CG001	Certificate profile requirements	
CD001	Requirement to make root certificates available.	
CSM001	CRLs to be refreshed at least once every 24hrs	
CSV001	OCSP service to be available 24x7 where used.	
CSV002	Where an OCSP service is provided it must allow unsigned requests for certificate status or an alternative mechanism provided at reasonable cost for applications to make OCSP calls to validate those certificates.	