TRUSTGATE
SECURE TRANSACTION. TRUSTED BUSINESS

MSC Trustgate.com Certificate Policy

Version 4.0

14 January 2021

MSC Trustgate.com.com Sdn. Bhd.
(199901003331)
Suite 2-9, Level 2, Block 4801 CBD Perdana
Jalan Perdana, 63000 Cyberjaya
Selangor Darul Ehsan, Malaysia
Tel: +603 8318 1800
www.msctrustgate.com

MSC Trustgate.com Certificate Policy

Published date: 14 January 2021

Trademark Notices

REVISION HISTORY

This document is the MSC Trustgate.com Certificate Policy. The following revisions have been made to the original document:

No.	Date	Changes	Version
1	April 8, 2019	To add Revision History and include several sections mentioned in Baseline Requirement to replace version 3.3 on 21st Feb 2019.	3.4
2	August 23, 2019	To amend the certificate validity period for DV, OV and AATL to 825 days in Section 6.3.2	3.5
3	January 14th 2021	To amend the content and structure of the CP in accordance with and include all material required by RFC 3647.	4.0

Table of Contents

1. INTRODUCTION

This Certificate Policy (CP) document is the principal statement of policy governing MSC Trustgate.com Sdn Bhd. The CP sets forth the business, legal and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the MSC Trustgate.com ecosystem and providing associated trust services. These requirements protect the security and integrity of MSC Trustgate.com and comprise a single set of rules that apply consistently, thereby providing assurances of uniform trust throughout the MSC Trustgate.com ecosystem. This CP may be updated from time to time as outlined in Section 1.5 Policy Administration. The latest version may be found on the MSC Trustgate.com company repository at www.msctrustgate.com/repositories.

This CP uphold to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. In addition, it upholds to the current and later versions of the requirements of the following schemes:

Name of Law / Policy / Guideline / Requirement Standard	**Location of Source Document**
Malaysia Digital Signature Act 1997	http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20562.pdf
Malaysia Digital Signature Regulation 1998	https://www.mcmc.gov.my/en/legal/acts/digital-signature-act-1997-reprint-2002/digital-signature-regulations-1998
WebTrust for CA Principle and Criteria	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

And for Publicly Trusted Certificate, it upholds to the current and later versions of the requirements of the following scheme

Name of Law / Policy / Guideline / Requirement Standard	**Location of Source Document**
Adobe Approved Trust List Members(AATL)	https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html
Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-document/
CAB Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/

While certain sections are included in this CP according to the structure of RFC 3647, the topic may not necessarily apply to services of MSC Trustgate. These sections state 'No stipulation'. Additional information is presented in subsections of the standard structure where necessary.

CA/Browser Forum requirements are published at https://cabforum.org/. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

This CP is final and binding between MSC Trustgate.com and the Subscriber and/or Relying Party, who uses, relies upon, or attempts to rely upon certification services made available by MSC Trustgate.com.

1.1. Overview

This CP applies to the complete hierarchy of Certificates issued by MSC Trustgate.com. The purpose of this CP is to present the framework in managing its Certificates according to MSC Trustgate.com's own and industry requirements pursuant to the standards. MSC Trustgate.com operates within the scope of the applicable sections of Malaysian Law when delivering its services. This CP aims to document MSC Trustgate.com delivery of certification services and management of the Certificate life cycle of any issued Subordinate CA, client, server, and other purpose end entity Certificates.

This CP is specifically applicable to:

- MSC Trustgate.com Sdn Bhd
- MSC Trustgate.com Sdn Bhd Infrastructure
- MSC Trustgate.com Sdn Bhd Administrators
- MSC Trustgate.com Sdn Bhd Enterprise Customers

A Certification Practice Statement (CPS) complements this CP and states, "*how the Certification Authority adheres to the Certificate Policy*". A CPS provides to an end user with a summary of the processes, procedures, and overall prevailing conditions that MSC Trustgate.com will use in creating and managing such Certificates.

In addition to this CP and the CPS, MSC Trustgate.com maintains additional documented policies which address such issues as:

- Business continuity and disaster recovery
- Security policy
- Personnel policies
- Key management policies
- Registration procedures
- Privacy Policy

All applicable MSC Trustgate.com policies are subject to audit by Malaysian Communications and Multimedia Commission authorised third parties which MSC Trustgate.com highlights on its public facing web site via a WebTrust Seal of Assurance. Additional information can be made available upon request.

1.2. Document name and identification

MSC Trustgate.com Certificates contain object identifier values corresponding to the applicable MSC Trustgate.com Class of Certificate. The OID for MSC Trustgate.com is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) MSC Trustagte.com (45530). MSC Trustgate.com issues certificates and time-stamp tokens containing the following OIDs arcs:

Digitally Signed Object	**Object Identifier (OID)**
Client Certificate	
Class 1 Client Certificates	1.3.6.1.4.1.49530.1.1.1
Class 2 Client Certificates (Generic)	1.3.6.1.4.1.49530.1.1.2
Class 2 Client Certificates (Government)	1.3.6.1.4.1.49530.1.1.2.1

Digitally Signed Object	Object Identifier (OID)
Class 2 Client Certificates (Enterprise)	1.3.6.1.4.1.49530.1.1.2.2
Class 3 Client Certificates	1.3.6.1.4.1.49530.1.1.3
Code Signing Certificates	
Code Signing Certificates	1.3.6.1.4.1.49530.1.2.1
Time Stamping Certificates	
Time Stamping Certificates (Generic)	1.3.6.1.4.1.49530.1.3.1
SSL Certificate	
Domain Validation SSL Certificates	1.3.6.1.4.1.49530.1.4.1
Organisation Validation SSL Certificates	1.3.6.1.4.1.49530.1.5.1
Extended Validation SSL Certificates	1.3.6.1.4.1.49530.1.6.1
Extended Validation Code Signing Certificates	1.3.6.1.4.1.49530.1.6.2
Intranet Validation SSL Certificates	1.3.6.1.4.1.49530.1.7.1

1.2.1. Root Certificates

CERT #	Subject	SHA256 Fingerprint
1	CN = Trustgate Class 1 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	B0FE225E8C0D51FD4AD509C3FD03B34625C0453FD51335436B6B1136AED8805D
2	CN = Trustgate Class 2 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	E2026B5646F49F9671D4318E09094A23CE34C94B5410F19B39D490A761CA65D1
3	CN = Trustgate Class 3 Root Certificate Authority O = MSC Trustgate.com Sdn. Bhd. C = MY	A62C9790F2D112238FE24C352422EAB29C34C3EE5698EE575CDF170188883DE9
4	CN = Trustgate RSA Certification Authority OU = Malaysia Licensed CA No LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	DC7ACA56E0921E3C54E7DA854A13CDE917B3EEC386B8E9D59201F812E4E9B40C
5	CN = Trustgate Time Stamping Authority CA (ECC) OU = Malaysia Licensed CA No LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	FC794E7830873926C16824CBAC867F8EAC7CF28EFC9FF4A465B77E6FD42610B7
6	CN = Trustgate Time Stamping Authority CA OU = Malaysia Licensed CA No LPBP-2/2010 (1) O = MSC Trustgate.com Sdn. Bhd. C = MY	CF74F634C21A6AA376FD264E31EAB031845FFD048D20F9C41AC73C8ED5BC4737
7	CN = MyTrust Class 1 ECC Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	9819A77417A5DF8880C1E52D5F4D72C6E5924460CE568C2DE5AD6199986A8D6E

CERT #	Subject	SHA256 Fingerprint
8	CN = MyTrust Class 2 ECC Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	97351977E28FD6602FE1ADAE58E8994212CB02D995F866D2F5DC41D9E946B855
9	CN = MyTrust Class 3 ECC Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	BFAEC1F8E11BD4840A91472E80040F568970FD48B28F09AF018383AF9B0F9D1F
10	CN = MyTrust Class 1 RSA Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	B9476C3FE5B6385FACE73E8B5265E56F30FFC39E77C9519537C361DC96405787
11	CN = MyTrust Class 2 RSA Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	A788D9F9EBE7648CFED6D8B071382A30780D9719A802731F066F59B32124A8B3
12	CN = MyTrust Class 3 RSA Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	045D810BEE88DF24246081793999E41766272F652837D5B9B909E57BCBCCD149
13	CN = MyTrust Digital ID Root CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd C = MY	D21BECEBF35470585672E8F5721697F71C7CC4D731C4A0FCCDB1A18FCB5691FA

1.2.2. Intermediate Certificate

CERT #	Subject	SHA256 Fingerprint
1	CN = MSC Trustgate.com Individual ID (Mobile) Basic CA OU = Malaysia Licensed CA No LPBP-2/2010(1) O = MSC Trustgate.com Sdn. Bhd. C = MY	D784BA8EA0364AFF850BF55BA490D1526B3F58304807F9D8F1E09CF8D3051560
2	CN = MSC Trustgate.com Class 2 MPKI CA O = MSC Trustgate.com Sdn. Bhd. C = MY	CC6ADC88D783574EA3E4F5114FF3AE4DB5B1470934242C62471B124A419C2F94
3	CN = MSC Trustgate.com Corporate ID (Mobile) CA OU = Malaysia Licensed CA No LPBP-2/2010(1) O = MSC Trustgate.com Sdn. Bhd. C = MY	5210171AF8C5C721B32F2BEEFBDE0331F9876067908F3FD0D589E002F99CF532
4	CN = MSC Trustgate.com Corporate ID (Token) CA OU = Malaysia Licensed CA No LPBP-2/2010(1) O = MSC Trustgate.com Sdn. Bhd. C = MY	A61D795B0EF27E96848585C2187C9476645528697ABE50BA3692F03663F08748
5	CN = MSC Trustgate.com Individual ID (Mobile) CA OU = Malaysia Licensed CA No LPBP-2/2010(1) O = MSC Trustgate.com Sdn. Bhd. C = MY	351B29A7F1354F7FA0F39ED5559A9417A55E1922073332FF0BDBC6DA0D4E62D34
6	CN = MSC Trustgate.com Professional ID (Mobile) CA OU = Malaysia Licensed CA No LPBP-2/2010(1) O = MSC Trustgate.com Sdn. Bhd. C = MY	5243B6A6B861C827B314BBFDE35AE7DF5EBB3F8EF196D35DB2B9CF5EBECBCA04
7	CN = MSC Trustgate.com Professional ID (Token) CA OU = Malaysia Licensed CA No LPBP-2/2010(1) O = MSC Trustgate.com Sdn. Bhd. C = MY	ACB79E7E11B201324313A9AF76A6D09564CEF2ED8DEC6BE6D65FAC1F5F21FA4B
8	CN = Trustgate Class 2 Consumer CA O = MSC Trustgate.com Sdn. Bhd. C = MY	A184B64A106866F751273518382431D23AE042AA6E8552D87540BF8D86FBB51A

CERT #	Subject	SHA256 Fingerprint
9	CN = Trustgate Class 2 MyKey Subscriber CA O = MSC Trustgate.com Sdn. Bhd. C = MY	15D5F8A7B9E73D2B2152F3E2EB44AA06BABD629480F6B4656346ED788448A65D
10	CN = Bank Negara Malaysia Class 2 CA-G3 O = MSC Trustgate.com Sdn. Bhd. C = MY	A4166F2E0125B553E84CBA1B7D240369AB2A5AB1846C0EF14E2332CEBD39E180
11	CN = MAMPU Class 2 CA OU = Authenticated by MSC Trustgate.com Sdn. Bhd. O = Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia C = MY	71C08196ECD864554528C749C9E7C9F4F29E11C68969AE8187E1F6E0BC06D8AE
12	CN = MAMPU Class 2 CA OU = Authenticated by MSC Trustgate.com Sdn. Bhd. O = Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia C = MY	4620E1CD3D0B931441BB25BDB8A7791699F830BB579E6E79A72044E39A5D9E30
13	CN = INTECH-KLIS CA OU = Remote Signing System O = IDAMAN NURANI TECHNOLOGIES SDN. BHD C = MY,	D0D6BA9EA1822C1C57F96F39BEE2A47A431889B7FD4C3BA25FB2200DC1873EBF
14	CN = NCSA O = Majlis Keselamatan Negara C = MY	EC7F4D7E05B60ED09392B0A0081C0B4A2FB165D8CEB6ED20CC44A533DEC539CB
15	CN = RHB-BOARDPAC CA OU = Remote Signing System O = RHB Bank Berhad C = MY	6ACF840E5AD0A768BC84DBD5C4932B65EA9AED0B84069E67FCCD42EFD2EEFABB
16	CN = ABMB-MFA CA OU = Remote Signing System O = Alliance Bank Malaysia Berhad C = MY	B20DA3E95B0554721E74931BE482B42D9458829E776858B43B7F217C81D418EE
17	CN = eCourt ID CA O = Mahkamah Persekutuan Malaysia C = MY	45730651D6DE393CD12595E5F16351AF1297F44847443B01BF4B6C02720E49C1
18	CN = eCourt ID CA O = Mahkamah Persekutuan Malaysia C = MY	CC37D4FEC512879D95BE7F2DBEFED1ABD25A60CA20297CA70FB12C45CC34F353
19	CN = Trustgate Time Stamping Services CA (ECC) O = MSC Trustgate.com Sdn. Bhd. C = MY	67AC1B817817B9C626D6D3E8487A1C7FEC8AA27336D50148580F88BB67FFB7FF
20	CN = Trustgate Time Stamping Services CA O = MSC Trustgate.com Sdn. Bhd. C = MY	091538A9476A4F6A6956F31B133992536881C28323D19B57E2C5D91EB4770B22
21	CN = MyTrust Class 1 ECC Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	4A32CB42C34E023600D0D88CE618263F0BDAA8BC4E27DCC1993A7ADC3193EFB0
22	CN = MyTrust Class 2 ECC Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	F040B8C96223510A3190E0E85233159986BD26187D11C909D65AB8E0D298AA22
23	CN = MyTrust Class 2 ECC Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	475DCD9714F9341629FC499241217144BD659DAE00B83860FC2D5A9C1E2AC7F7
24	CN = Bursa Anywhere CA OU = Remote Signing System O = Bursa Malaysia Berhad C = MY	2D01696CC852C4CE5317778A9FA16BBEA14CDEE10F5FBA91A3B37D8FF52768E5

CERT #	Subject	SHA256 Fingerprint
25	CN = GPKI CA ECC OU = MAMPU, O = MSC Trustgate.com Sdn. Bhd C = MY	567EF5A4C14641BC6B46452540F187B5686407DF4BDD51E5A3B1C79E678F97B8
26	CN = MyTrust Class 3 ECC Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	8EA69844C4A6BDA29FC13FD65A2371E9E689C22C1BF6585432406B527F86730F
27	CN = MyTrust Class 1 RSA Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	9C4CD1AB5BAE1D2D786E56BF9825257AAAD18519C44016170043B94AF61D61CE
28	CN = MyTrust Class 2 RSA Individual CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	F65BFC5FB0D51560AB5B46D52A602B276FDA94E341693799CEB669C76F54DE95
29	CN = MyTrust Class 2 RSA Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	1B1EE0498319BF0A223D4917A41A454D4EA08F44C5C8BD26F65121256377CB6A
30	CN = MyTrust Class 3 RSA Enterprise CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	ADEABEB6A51091CAD7DBCE54EC0C6B4DFADC3ACF16F18311CADCF510E8037366
31	CN = MyTrust RSA Code Signing CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	4F49F31B1E2B4BD4D37659E0F18D438C7CD41DBB970C6B3373B5608C61BBFB44
32	CN = MyTrust RSA SSL CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	B524ABDA93244786185FB291B358A6CAD1012E2F251AD0E0486546993AF416B6
33	CN = MyTrust RSA EV Code Signing CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	70EC99FF806982D8364746CB78106EEBC3FC615FF109A70C4DFC477D44054CAD
34	CN = MyTrust RSA EV SSL CA OU = MyTrust Gateway O = MSC Trustgate.com Sdn. Bhd. C = MY	740D432D12D66D95438305BAC9F054B706524998CEEC2C5E63E409CEBEDD54B6
35	CN = MyTrust Digital ID Class 1 CA OU = MyTrust Gateway, O = MSC Trustgate.com Sdn. Bhd, C = MY	7096769E0A335DADCFB6DEA0DDCEEF47CB1FA3B8709326BACA41514B649CAC8C
36	CN = MyTrust Digital ID Class 2 CA OU = MyTrust Gateway, O = MSC Trustgate.com Sdn. Bhd, C = MY	D42F0C30DD9896F8E0EDED01FC4494F317B7DC7E6530590EDDB4D84228050C99
37	CN = MyTrust Digital ID Class 3 CA OU = MyTrust Gateway, O = MSC Trustgate.com Sdn. Bhd, C = MY	94B349BC4BE13041EA9A47315CE22E0EA327873FADA258EDC99B91F56F0F8439

1.3. PKI participants

1.3.1. Certification authorities

MSC Trustgate.com is a licenced Certification Authority under the purview of Malaysian Communication Multimedia Commission (MCMC) that issues Certificates in accordance with this CPS. As a Certification Authority, MSC Trustgate.com performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation.

MSC Trustgate.com also provides Certificate status information using a Repository in the form of a Certificate Revocation List (CRL) and/or Online Certificate Status Protocol (OCSP) responder. MSC Trustgate.com may also be described by the term "Issuing Authority" or "MSC Trustgate.com" to denote the purpose of issuing Certificates at the request of a Registration Authority (RA) from a subordinate Issuing CA.

The MSC Trustgate.com Policy Board, which is composed of members of the MSC Trustgate.com Sdn Bhd management team and appointed by its Board of Directors, is responsible for maintaining this Certificate Policy relating to all certificates in the hierarchy. Through its Policy Board, MSC Trustgate.com maintains control over the lifecycle and management of the CA.

Some of the tasks associated with Certificate lifecycle are delegated to select, who operate based on a service agreement with MSC Trustgate.com

1.3.2. Registration authorities

In addition to identifying and authenticating Applicants for Certificates, an RA may also initiate or pass along revocation requests for Certificates and requests for re-issuance and renewal (sometimes referred to as re-key) of Certificates. Issuing CAs may act as a Registration Authority for Certificates they issue in which case they are responsible for:

• Accepting, evaluating, approving, or rejecting the registration of Certificate applications; • Registering Subscribers for certification services;

• Providing systems to facilitate the identification of Subscribers (according to the type of Certificate requested);

• Using officially notarised or otherwise authorised documents or sources of information to evaluate and authenticate an Applicant's application;

• Requesting issuance of a Certificate via a multi-factor authentication process following the approval of an application; and

• Initiating the process to revoke a Certificate from the applicable MSC Trustgate.com Subordinate CA or partner Subordinate CA.

Third party Issuing CAs who enter into a contractual relationship with MSC Trustgate.com may operate their own RA and authorize the issuance of Certificates. Third parties must comply with all the requirements of this CP and the terms of their contract which may also refer to additional criteria as recommended by the CA/B Forum. RAs may implement more restrictive vetting practices if their internal policy dictates.

In order to issue certain Certificate types, RAs may need to rely on Certificates issued by third party Certification Authorities or other third-party databases and sources of information Such as government national identity cards such as passwords, eID, and drivers licenses. Where the RA relies on Certificates issued by third party Certification Authorities, Relying Parties are advised to review additional information by referring to such third party's CPS. MSC Trustgate.com Issuing CAs may designate an Enterprise RA to verify Certificate Requests from the Enterprise RA's own organization. In Enterprise RA, the Subscriber's organization shall be validated and predefined, and shall be constrained by system configuration.

1.3.3. Subscribers

Subscribers of Issuing CAs are either directly reliant on the Issuing CA to issue end entity Certificates from a hierarchy managed by the Issuing CA or they are third parties that seek to be issued with an Issuing CA capable of issuing additional Certificates to their own PKI hierarchy. Subscribers are either Legal Entities or natural persons that successfully apply for and receive a Certificate to support their use in transactions, communications, and the application of Digital Signatures. In some cases, individuals are not able to obtain certain Certificate types.

A Subscriber, as used herein, refers to both the Subject of the Certificate and the entity that contracted with the Issuing CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

End entity Subscribers:

• Have ultimate authority over the Private Key corresponding to the Public Key that is listed in a Subscriber's Certificate. A Subscriber may or may not be the Subject of a Certificate (For example, machine or role-based Certificates issued to firewalls, routers, servers, or other devices used within an organization).

Trusted Root Subscribers:

• Set the framework of providing certification services with the CA hierarchy for the benefit of the Subject mentioned in a Certificate;

• Accept and implement the contractual, audit and policy requirements of MSC Trustgate.com Trusted Root services about operational practices and technical implementation:

• Can only be enterprise in-house PKIs. No public PKI services are allowed; and

• MSC Trustgate.com reserves the right to technically constrain the breadth of a domain using subordination (For example, RFC 5280 dNSName Name Constraints).

1.3.4. Relying parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under this CP. A Relying party may or may not also be a Subscriber within MSC Trustgate.com.

1.3.5. Other participants

Other participants include bridge CAs and CAs that cross certify Issuing CAs to provide trust among other PKI communities.

1.4. Certificate usage

A Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1. Appropriate certificate uses

Certificates issued by MSC Trustgate.com complies to DSA 1997 and DSR 1998. These certificates can be used for public domain transactions that require:

- Authentication: The assurance of one's identity - who he/she/it claims to be.
- Integrity: The assurance to an entity that data has not been tempered with.
- Confidentiality: The assurance to an entity that only the intended recipient(s) can read a particular piece of data.
- Non-repudiation: A party cannot deny having digitally signed a data, a transaction, or a document.

1.4.2. Prohibited certificate uses

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorised. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the MSC Trustgate.com Warranty Policy. Certificates do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is free from defect, malware, or virus. In the case of code signing, Certificates do not guarantee that signed code is free from bugs or vulnerabilities.

1.5. Policy administration

1.5.1. Organization administering the document

MSC Trustgate.com Policy Management Authority.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia.

Tel: +603 8318 1800
Fax: +603 8319 1800
Email: legal@msctrustgate.com

1.5.2. Contact person

Attn: Security Officer

MSC Trustgate.com Policy Management Authority.
Suite 2-9, Level 2, CBD Perdana
Jalan Perdana, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia.
Tel: +603 8318 1800
Fax: +603 8319 1800
Email: legal@msctrustgate.com

1.5.3. Person determining CP suitability for the policy

The organization identified in Section 1.5.2 is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the CP /CPS.

1.5.4. CP approval procedures

The PMA approves the CPS and any amendments. Amendments are made after the PMA has reviewed the amendments' consistency with the CPS, by either updating the entire CPS or by publishing an addendum. The PMA determines whether an amendment to this CPS is consistent with the CP, requires notice, or an OID change. See also Section 9.10 and Section 9.12 below.

Amended versions or updates is publicly available at MSC Trustgate.com Repository located at: https://www.msctrustgate.com/repository.htm. Updates supersede any designated or conflicting provisions of the referenced to the previous version of the CPS.

1.6. Definitions and acronyms

"Adobe Approve Trusted List" A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0.

"**Applicant**" means an entity applying for a Certificate.

"**Application Software Vendor**" means a software developer whose software displays or uses MSC Trustgate.com Certificates and distributes MSC Trustgate.com root Certificates.

"**CAB Forum**" is defined in section 1.1.

"**Certificate**" means an electronic document that uses a digital signature to bind a Public Key and an identity.

"**Key Pair**" means a Private Key and associated Public Key.

"**OCSP Responder**" means an online software application operated under the authority of MSC Trustgate.com and connected to its repository for processing certificate status requests.

"**Private Key**" means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

"**Public Key**" means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

"**Qualified Certificate**" means a Certificate that meets the requirements of EU law and is provided by an Issuer CA meeting the requirements of EU law.

"**Relying Party**" means an entity that relies upon either the information contained within a Certificate or a time-stamp token.

"**Relying Party Agreement**" means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using MSC Trustgate.com Repository. The Relying Party Agreement is available for reference through a MSC Trustgate.com online repository.

"**Subscriber**" means either the entity identified as the subject in the Certificate or the entity that is receiving MSC Trustgate.com time-stamping services.

"**Subscriber's Agreement**" means an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

"Trusted Agent"

"**WebTrust**" means the current version of CPA Canada's WebTrust Program for Certification Authorities.

Acronyms

AATL	Adobe Approve Trusted List
CA	Certification Authority
CAA	Certificate Authority Authorization
CAB	"CA/Browser" as in "CAB Forum"
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as "Trading As")
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IGTF	International Grid Trust Federation
ISSO	Information System Security Officer
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
IV	Individual Validated
LEI	Legal Entity Identifier
MICS	Member-Integrated Credential Service (IGTF)
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (e.g. a secret access code)
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
RPS	Registration Practice Statement
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SHA	Secure Hashing Algorithm
SSL	Secure Socket Layer
TSA	Time Stamping Authority
TST	Time-Stamp Token
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

MSC Trustgate.com shall develop, implement, enforce, and annually update CP and/or CPS that describes in detail how the CA implements the latest version of these requirements

2.1. Repositories

MSC Trustgate.com shall publishes all Certificates-related and Certificate Revocation information for issued Certificates, CP, CPS and Relying Party agreements and Subscriber Agreements in public repositories. MSC Trustgate.com shall ensures that revocation data for issued Certificates and its Root Certificates are available through a repository on 24 hours basis and is periodically updated as set forth in this CP.

2.2. Publication of certification information

MSC Trustgate.com publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. MSC Trustgate.com publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 8.1). The Certificate Policy and/or Certification Practice Statement MUST be structured in accordance with RFC 3647 and MUST include all material required by RFC 3647. Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements. It shall clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue. MSC Trustgate.com log all actions taken, if any, consistent with its processing practice.

2.3. Time or frequency of publication

MSC Trustgate.com develop, implement, enforce, and annually update its Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. MSC Trustgate.com indicate conformance with this requirement by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.4. Access controls on repositories

Trustgate MSC Trustgate.com provide unrestricted read access to its Repositories and shall apply logical and physical controls to prevent unauthorised write access to such Repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

To identify a Subscriber, Issuing CAs shall follow naming and identification rules that include types of names assigned to the Subject, such as X.500 distinguished names RFC-822 names and X.400 names. Where DNs (Distinguished Names) are used, CNs (Common Names) must respect name space uniqueness and must not be misleading. RFC2460 (IP version 6) or RFC791 (IP version 4) addresses may be used.

3.1.2. Need for names to be meaningful

When applicable, Issuing CAs shall use distinguished names to identify both the Subject and issuer name of the Certificate. When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.

3.1.3. Anonymity or pseudonymity of subscribers

Issuing CAs may issue end entity anonymous or pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and name space uniqueness is preserved.

3.1.4. Rules for interpreting various name forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5. Uniqueness of names

Issuing CAs may enforce uniqueness within the DN or by requiring that each Certificate include a unique non-sequential serial number with at least 20 bits of entropy.

3.1.6. Recognition, authentication, and role of trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. This CP does not require that an Applicant's right to use a trademark be verified. However, Issuing CAs may reject any applications or require revocation of any Certificate that is part of a dispute.

3.2. Initial identity validation

Issuing CAs may perform identification of the Applicant or for services including CA chaining services using any legal means of communication or investigation necessary to identify the Legal Entity or Individual. Issuing CAs may use the result of a successful Subject DN initial identity validation process to create alternative product offerings by effectively combining elements of previously verified information with alternative, newly verified, information. A suitable account-based challenge response mechanism must be used to authenticate any previously verified information for any returning Applicant provided that the re-verification requirements of Section 3.3.1 are complied with.

3.2.1. Method to prove possession of private key

Subscribers must prove possession of the Private Key corresponding to the Public Key being registered with the Issuing CA. Such a relationship can be proved by, for example, a Digital Signature in the Certificate Signing Request (CSR) in addition to an out-of-band confirmation.

Issuing CAs may accept other Issuing CAs wishing to enter their hierarchy through the Trusted Root program. Following an initial assessment and signing of a specific agreement with the Issuing CA,

the applicant Subordinate CA must also prove possession of the Private Key. CA chaining MSC Trustgate.com CP (Certificate Policy) 34 of 78 Version: 6.4 services do not mandate the physical appearance of the Subscriber representing the Subordinate CA so long as an agreement between the applicant organisation (which has been authenticated) and the Issuing CA has been executed.

For Qualified Certificates where the private key related to the certified public key resides in a QSCD, Subscriber keys must be generated and stored within a recognized Qualified Signature Creation Device (QSCD). The QSCD certification status must be monitored and appropriate measures must be taken if the certification status of a QSCD changes.

3.2.2. Authentication of organization identity

For all Certificates that include an organization identity, Applicants are required to indicate the organization's name and registered or trading address. The legal existence, legal name, legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and provided address of the organization must be verified and any methods used must be highlighted in the CPS.

The authority of the Applicant to request a Certificate on behalf of the organization must be verified in accordance with Section 3.2.5.

3.2.3. Authentication of individual identity

Issuing CAs or RAs shall authenticate Individuals depending upon the class of Certificate as indicated below.

3.2.3.1. Low Assurance

MSC Trustgate.com does not authenticate the identity of the Applicant except required the Applicant to demonstrate control of his/her email address to which the Certificate relates.

3.2.3.2. Medium Assurance

The Applicant may also be required to submit a legible copy of a government issued photo ID (national ID, driving license, passport). Other relevant document may also be required for additional proof. MSC Trustgate.com will authenticate with enough evidence met for IAL 2 in NIST 800-63a for the Subject information such as Country or locality fields are correct.

3.2.3.3. High Assurance

The Applicant may also be required to submit a legible copy of a government issued photo ID (national ID, driving license, passport). Other relevant document may also be required for additional proof. MSC Trustgate.com will authenticate with enough evidence met for IAL 3 in NIST.SP 800-63a for the Subject information such as Country or locality fields are correct.

3.2.4. Non-verified subscriber information

Issuing CAs must validate information to be included within the SubjectDN of a Certificate or clearly indicate within their CPS and within the issued Certificate itself any exceptions that may apply to specific product types or services offered. Issuing CAs may use the Subject:organizationalUnitName as a suitable location to identify non-verified Subscriber information to Relying Parties or to provide any specific disclaimers/notices. In the case of individuals, a unique identifier such as mobile number may be used in conjunction with the individual's legal name.

For all Certificate types where the Issuing CA can explicitly identify a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity the Issuing CA must verify the information and may therefore omit a disclaimer notice.

For all Certificate types where the Issuing CA cannot explicitly verify the identity, e.g. a generic term such as "Marketing," then the Issuing CA may omit the disclaimer that this item is classified as non-

verified Subscriber information as described herein. For IntranetSSL Certificates only, Issuing CAs may rely upon information provided by the Applicant to be included within the subjectAlternativeName, such as internal or non-public DNS names, hostnames, and RFC 1918 IP addresses. Specifically, for SSL/TLS Certificates and Code Signing Certificates, the CA must maintain a process to ensure that Applicants cannot add self-reported information to the subject:organizationalUnitName.

Issuing CAs that provide client authentication, document signing, secure messaging and role-based Certificates may contractually allow Local Registration Authorities to perform validation of data for the following fields so long as an alternative Policy OID is present: Subject:organizationalUnitName and/or Common Name.

3.2.5. Validation of authority

If the Applicantion for a Certificate containing Subject Identity Information is an organization, thenMSC Trustgate.com shall use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

MSC Trustgate.com.com may establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that MSC Trustgate.com deems appropriate.

In addition,MSC Trustgate.com shall establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, thenMSC Trustgate.com shall not accept any certificate requests that are outside this specification.MSC Trustgate.com shall provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6. Criteria for interoperation

No Stipulation.

3.3. Identification and authentication for re-key requests

No Stipulation.

3.3.1. Identification and authentication for routine re-key

No Stipulation.

3.3.2. Identification and authentication for re-key after revocation

No Stipulation.

3.4. Identification and authentication for revocation request

No Stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Issuing CAs shall maintain their own blacklists for individuals from whom or entities from which they will not accept Certificate applications. Blacklists may be based on past history or other sources. In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which the Issuing CA operates may be used to screen unwanted Applicants.

4.1.2. Enrollment process and responsibilities

Issuing CAs shall maintain systems and processes that sufficiently authenticate the Applicant's identify for all Certificate types that present the identity to Relying Parties. Applicants should submit sufficient information to allow Issuing CAs and RAs to successfully perform the required verification. Issuing CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

Issuing CAs shall maintain systems and processes to sufficiently authenticate the Applicant's identify in in compliance with its CPS. Initial identity validation shall be performed by an Issuing CAs validation team or by Registration Authorities under contract as set forth in Section 3.2 of this CP. All communications shall be securely stored along with all information presented directly by the Applicant during the application process. Future identification of repeat Applicants and subsequent authentication checks may be addressed using single (username and password) or multi-factor (Certificate in combination with username/password) authentication principles. MSC Trustgate.com shall validate each server FQDN in publicly trusted SSL certificates against the domain's CAA records. MSC Trustgate.com's CAA issuer domain is "MSC Trustgate.com." If a CAA record exists that does not listMSC Trustgate.com as an authorized CA, MSC Trustgate.com shall not issue the certificate. CAA checking is optional for MSC Trustgate.com Trusted Root customers that issue SSL certificates using Name Constrained CAs.

4.2.2. Approval or rejection of certificate applications

Issuing CAs shall reject applications for Certificates where validation of all items cannot successfully be completed. Assuming all validation steps can be completed successfully following appropriate best practice techniques Issuing CAs shall generally approve the Certificate Request. Issuing CAs may reject applications including for the following reasons:

• Based on potential brand damage to MSC Trustgate.com in accepting the application.

• For Certificates from Applicants who have previously been rejected or have previously violated a provision of a Subscriber Agreement.

Issuing CAs are under no obligation to provide a reason to an Applicant for rejection of a Certificate Request. Issuing MSC Trustgate.com not issue publicly trusted SSL certificates to internal server name or reserved IP addresses.

4.2.3. Time to process certificate applications

Issuing CAs shall ensure that all reasonable methods are used in order to process and evaluate Certificate applications.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

Certificate issuance by MSC Trustgate.com Root CA requires an authorized Trusted Role member from MSC Trustgate.com to deliberately issue a direct command for the Root CA to perform a Certificate signing operation. Issuing CAs shall communicate with any RA accounts capable of causing Certificate issuance using multi-factor authentication. RAs directly operated by the Issuing CA or RAs contracted by the Issuing CA to perform validation shall ensure that all information sent to the CA is verified and authenticated in a secure manner.

4.3.2. Notification to subscriber by the CA of issuance of certificate

The Issuing MSC Trustgate.com notify the Subscriber of the issuance of a Certificate in a convenient and appropriate way based on information submitted during the enrolment process.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

Issuing CAs shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. To avoid this being an open-ended stipulation, Issuing CAs may set a time limit by when the Certificate is deemed to be accepted.

4.4.2. Publication of the certificate by the CA

Issuing CAs may publish a Certificate by sending the Certificate to the Subscriber and/or publishing in a suitable Repository, including to Certificate Transparency Logs.

4.4.3. Notification of certificate issuance by the CA to other entities

RAs, local RA or partners/resellers or MSC Trustgate.com may be informed of the issuance if they were involved in the initial enrolment.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

All Subscribers must protect their Private Key taking care to avoid disclosure to third parties. Issuing CAs must maintain a suitable Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate. Where it is possible to make a back-up of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup. In the case of MSC Trustgate.com's Digital Signing Service, and with the consent of the Subscriber, MSC Trustgate.com shall host, secure, and manage short-lived Certificates and their corresponding Private Keys.

4.5.2. Relying party public key and certificate usage

Issuing CAs must describe the conditions under which Certificates may be relied upon by Relying Parties within their CPS including the appropriate mechanisms available to verify Certificate validity (e.g., CRL or OCSP). Issuing CAs must also offer a Relying Party agreement to Subscribers the content of which should be presented to the Relying Party prior to reliance upon a Certificate from the Issuing CA. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made. Software used by Relying Parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

Certificate renewal is defined as the production of a new Certificate that has the same details as a previously issued Certificate and the same Public Key. Issuing CAs that support renewal must identify the products and services under which renewals can be accepted. An Issuing CA may renew a Certificate so long as:

• The original Certificate to be renewed has not been revoked;

• The Public Key from the original Certificate has not been blacklisted for any reason; and

• All details within the Certificate remain accurate and no new or additional validation is required.

Issuing CAs may renew Certificates which have either been previously renewed or previously rekeyed (subject to the points above). The original Certificate may be revoked after renewal is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

4.6.2. Who may request renewal

An Issuing CA may accept a renewal request provided that it is authorized by the original Subscriber through a suitable Certificate lifecycle account challenge response. A Certificate signing request is not mandatory, however if one is used then it must contain the same Public Key.

4.6.3. Processing certificate renewal requests

An Issuing CA may request additional information before processing a renewal request.

4.6.4. Notification of new certificate issuance to subscriber

As per 4.3.2

4.6.5. Conduct constituting acceptance of a renewal certificate

As per 4.4.1

4.6.6. Publication of the renewal certificate by the CA

As per 4.4.2

4.6.7. Notification of certificate issuance by the CA to other entities

No Stipulation

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

Certificate re-key is the process in which a subscriber can obtain a new certificate to replace an old certificate that:

• Contains the same information (identity, domains etc.) as the old certificate,

• Has the same expiry date (not After date) as the old certificate,

• Contains a different public key as the old certificate.

If a Certificate is re-keyed prior to the 'Not After' date, and the new certificate is given the same 'Not After' date as the old certificate, this process is referred to as Certificate reissue.

Issuing CAs that support re-keying must identify the products and services under which re-keys can be accepted. An Issuing CA may re-key a Certificate as long as:

• The original Certificate to be re-keyed has not been revoked;

• The new public key has not been blacklisted for any reason; and

• All details within the Certificate remain accurate and no new or additional validation is required.

Issuing CAs may re-key Certificates which have either been previously renewed or previously rekeyed (subject to the points above). The original Certificate may be revoked after re-key is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

4.7.2. Who may request certification of a new public key

An Issuing CA may accept a re-key request provided that it is authorized by either the original Subscriber, or an organization administrator who retains responsibility for the Private Key on behalf of a Subscriber through a suitable Certificate lifecycle account challenge response. A Certificate signing request is mandatory with any new Public Key.

4.7.3. Processing certificate re-keying requests

An Issuing CA may request additional information before processing a re-key or reissue request and may re-validate the Subscriber subject to re-verification of any previously validated data. In the case of a reissuance, authentication through a suitable challenge response mechanism is acceptable.

4.7.4. Notification of new certificate issuance to subscriber

As per 4.3.2

4.7.5. Conduct constituting acceptance of a re-keyed certificate

As per 4.4.1

4.7.6. Publication of the re-keyed certificate by the CA

As per 4.4.2

4.7.7. Notification of certificate issuance by the CA to other entities

No stipulation

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

Certificate modification is defined as the production of a new Certificate that has details which differ from a previously issued Certificate. The new modified Certificate may or may not have a new Public Key and may or may not have a new 'Not After' date.

• Issuing CAs shall treat modification in the same was a 'New' issuance.

• Issuing CAs may modify Certificates that have either been previously renewed or previously re-keyed. The original Certificate may be revoked after modification is complete, however, the original Certificate must not be further renewed, re-keyed or modified.

4.8.2. Who may request certificate modification

As per 4.1

4.8.3. Processing certificate modification requests

As per 4.2

4.8.4. Notification of new certificate issuance to subscriber

As per 4.3.2

4.8.5. Conduct constituting acceptance of modified certificate

As per 4.4.1

4.8.6. Publication of the modified certificate by the CA

As per 4.4.2

4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

Certificate revocation is a process whereby the serial number of a Certificate is effectively blacklisted by adding the serial number and the date of the revocation to a Certificate Revocation List (CRL). The CRL itself will then be digitally signed with the same Private Key which originally signed the Certificate to be revoked. Adding a serial number to the CRL allows Relying Parties to establish that the lifecycle of a Certificate has ended. Issuing CAs may remove serial numbers once a Certificate has normally expired to promote more efficient CRL file size management. Prior to performing a revocation, Issuing CAs will verify the authenticity of the revocation request.

Revocation of a Subscriber's Certificate is performed within twenty-four (24) hours under the following circumstances:

1. The Subscriber requests in writing (to MSC Trustgate.com which provided the Certificate) that they wish to revoke the Certificate;

2. The Subscriber notifies MSC Trustgate.com that the original Certificate Request was not authorized and does not retroactively grant authorization;

3. MSC Trustgate.com obtains reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise

4. MSC Trustgate.com receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use, and/or unexpected termination of a subscriber's or subject's agreement or business functions;

5. MSC Trustgate.com obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

6. In case of PSD2 Certificates, MSC Trustgate.com receives an authenticated revocation request (or authenticates a revocation request) that originated from the NCA which has authorized or registered the payment service provider, and which includes a valid reason for revocation. Valid reasons for revocation include when the authorization of the PSP has been revoked or any PSP role included in the certificate has been revoked.

4.9.2. Who can request revocation

Issuing CAs and RAs will accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organization named in the Certificate. Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify MSC Trustgate.com of a suspected reasonable cause to revoke a Certificate. Additionally, for PSD2 Certificates, revocation request can originate from the NCA which has authorized or registered the payment service provider. MSC Trustgate.com CP (Certificate Policy) 50 of 78 Version: 6.4 Issuing CAs may also at their own discretion revoke Certificates including Certificates that are issued to other cross signed Issuing CAs.

4.9.3. Procedure for revocation request

Due to the nature of revocation requests and the need for efficiency, Issuing CAs and RAs may provide automated mechanisms for requesting and authenticating revocation requests; for example, through an account which issued the Certificate that is requested to be revoked. RAs may also provide manual backup processes in the event that automated revocation methods are not possible. Issuing CAs and RAs will record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved. Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs may be published immediately or they may be published as defined within the Issuing CA's CPS. Issuing CAs and RAs shall prepare methods for Subscribers, Relying Parties, Application Software Suppliers, and other third parties to submit Certificate Revocation request. Issuing CAs and RAs may or may not revoke in response to this request. See section 4.9.5 for detail of actions required for Issuing CAs and RAs for making this decision.

4.9.4. Revocation request grace period

For SSL and codesigning certificates, MSC Trustgate.com does not support a revocation request grace period. For all other certificates, the revocation request grace period is the time available for a Subscriber to take any necessary actions themselves in order to request revocation of a suspected Key Compromise, use of a weak key or discovery of inaccurate information within an issued Certificate. Issuing CAs should allow Subscribers a maximum of 48 hours to take appropriate action to revoke or take appropriate action on behalf of Subscribers.

4.9.5. Time within which CA must process the revocation request

Issuing CAs shall begin investigating Certificate Problem Reports within twenty-four (24) hours of receipt of the report. All revocation requests for end entity Certificates, both those generated automatically via user accounts and those initiated by the Issuing CA itself, must be processed within a maximum of 30 minutes of receipt. Issuing CAs that cross sign other CAs should process a revocation request within 24 hours of a confirmation of Compromise and an ARL should be published within 12 hours of any off-line ARL key ceremony. Issuing CAs and RAs shall maintain 24 x 7 ability to respond internally to a high-priority Certificate Problem Report through report abuse channel and, where appropriate, forward such a complaint to law enforcement authorities, and/or

revoke a Certificate that is the subject of such a complaint. Issuing CAs and RAs shall begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

Issuing CAs and RAs shall decide whether revocation or other action is warranted based on at least following criteria:

• The nature of the alleged problem;

• The number of reports received about a particular Certificate or Subscriber;

• The entity making the complaint; and

• Relevant legislation.

For Qualified Certificates, actual revocation status shall be published/available through all revocation mechanisms within 60 minutes after the revocation decision and will never be reverted.

4.9.6. Revocation checking requirement for relying parties

Prior to relying on a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid. Relying Parties will need to consult CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). Issuing CAs may include all applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process.

4.9.7. CRL issuance frequency

All Issuing CAs must meet the requirements of the Baseline Requirements and the EV Guidelines (if applicable). In addition, Issuing CAs that operate offline shall publish a CRL every 3 months. Issuing CAs that operate online must publish CRLs at least every 7 days and value of nextUpdate fields is not more than 10 days beyond the value of the thisUpdate. For Subordinate CA Certificates, CRL is updated at least once every 12 months and within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than 12 months beyond the value of the thisUpdate field.

4.9.8. Maximum latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.9.9. On-line revocation/status checking availability

Issuing CAs that support OCSP responses in addition to CRLs shall provide response times no longer than 10 seconds under normal network operating conditions. Issuing CAs' OCSP responses shall conforms to RFC6960 and/or RFC5019. OCSP responses shall be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. On-line revocation checking requirements

For the status of Subscriber Certificates: • Issuing MSC Trustgate.com update information provided via an OCSP at least every four days. OCSP responses from this service will not exceed an expiration time of seven days. For the status of Subordinate CA Certificates: • Issuing MSC Trustgate.com update information provided via an OCSP at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate. OCSP Responders that receive a request for status of a Certificate that has not been issued, shall not respond with a "good" status for such Certificates. OCSP Responders for CAs which are not Technically Constrained, in line with Section 7.1.5, shall not respond with a "good" status for such Certificates. Issuing MSC Trustgate.com require OCSP

requests to contain the following data: • Protocol version • Service request • Target Certificate identifier

4.9.11. Other forms of revocation advertisements available

If the Subscriber Certificate is for a high-traffic FQDN, Issuing CA may choose to rely on stapling, in accordance with RFC4366, to distribute its OCSP responses. In this case, Issuing MSC Trustgate.com ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. Issuing MSC Trustgate.com enforce this requirement on the Subscriber contractually through the Subscriber Agreement or Terms of Use, or by technical review measures implemented by the CA.

4.9.12. Special requirements re key compromise

Issuing CAs and related Registration Authorities shall use commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where the Issuing CA at their own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed Issuing CAs shall revoke Issuing CA Certificates or Subscriber end entity Certificates and publish a revised CRL within 24 hours.

4.9.13. Circumstances for suspension

Certificate suspension is only allowed for Client certificates. Certificate suspension is not allowed for any other types of end entity Certificates. Certificate suspension is strictly forbidden for SSL certificates and Qualified Certificates

4.9.14. Who can request suspension

No Stipulation

4.9.15. Procedure for suspension request

No Stipulation

4.9.16. Limits on suspension period

No Stipulation

4.10. Certificate status services

4.10.1. Operational characteristics

MSC Trustgate.com must not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.10.2. Service availability

MSC Trustgate.com shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions. MSC Trustgate.com shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by MSC Trustgate.com. MSC Trustgate.com shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3. Optional features

No Stipulation.

4.11. End of subscription

No Stipulation

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

No Stipulation

4.12.2. Session key encapsulation and recovery policy and practices

No Stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

Issuing CAs shall have physical and environmental security policies for systems used for Certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g., power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls should be implemented to avoid loss, damage or Compromise of assets and interruption to business activities and theft of information and information processing facilities.

5.1.1. Site location and construction

Issuing CAs shall ensure that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference, and the protections provided should be commensurate with the identified risks in risk analysis plans.

5.1.2. Physical access

Issuing CAs shall ensure that the facilities used for Certificate life cycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee should always accompany any unauthorized person entering a physically secured area. Physical protections should be achieved through the creation of clearly defined security perimeters (i.e., physical barriers) around the systems hosting the CA operations. No parts of the CA premises shall be shared with other organizations within this perimeter.

5.1.3. Power and air conditioning

Issuing CAs should ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4. Water exposures

Issuing CAs should ensure that the CA system is protected from water exposure

5.1.5. Fire prevention and protection

Issuing CAs should ensure that the CA system is protected with a fire suppression system.

5.1.6. Media storage

Issuing CAs should ensure that any media used is securely handled to protect it from damage, theft and unauthorized access. Media management procedures should be protected against obsolescence and deterioration of the media within a defined period of time. Records are required to be retained. All media should be handled securely in accordance with requirements of the information asset classification scheme and media containing sensitive data must be securely disposed of when no longer required.

5.1.7. Waste disposal

Issuing CAs should ensure that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8. Off-site backup

Issuing CAs should ensure that full system backups of the Certificate issuance system are sufficient to recover from system failures and are made periodically, as defined in the Issuing CA's CPS. Back-

up copies of essential business information and software must be taken regularly. Adequate back-up facilities must be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. At least one full backup copy must be stored at an offsite location (at a location separate from the Certificate issuance equipment). Backups should be stored at a site with physical and procedural controls commensurate to that of the operational facility.

5.2. Procedural controls

5.2.1. Trusted roles

Issuing CAs should ensure that all operators and administrators including Vetting Agents are acting in the capacity of a trusted role. Trusted roles are such that no conflict of interest is possible, and the roles are distributed such that no single person can circumvent the security of the CA system. MSC Trustgate.com may subscribe certificates for MSC Trustgate.com affiliate companies, or persons identified in association with these companies (as a subject). MSC Trustgate.com affiliate companies include MSC Trustgate.com's parent and subsidiary companies, as well and other companies that share a same parent company as MSC Trustgate.com. Trusted roles include but are not limited to the following:

• Developers: Responsible for development of CA systems.

• Security Manager: overall responsibility for administering the implementation of the CA's security practices, cryptographic key life cycle management functions (e.g., key component custodians);

• Administrator: approval of the generation, revocation, and suspension of certificates;

• System Engineer: installation, configuration, and maintenance of the CA systems, viewing and maintenance of CA system archives and audit logs;

• Operator: day-to-day operation of CA systems and system backup and recovery;

• Key Manager: cryptographic key life cycle management functions (e.g., key component custodians).

5.2.2. Number of persons required per task

Issuing CAs shall state the number of persons required per task within their CPS. The goal is to guarantee the trust for all CA services (Key Pair generation, Certificate generation, and revocation) so that any malicious activity would require collusion. Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1 above.

5.2.3. Identification and authentication for each role

Before appointing a person to a trusted role, Issuing CAs shall run a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA. The CPS should describe the mechanisms that are used to identify and authenticate people appointed to trusted roles.

5.2.4. Roles requiring separation of duties

No Stipulation

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, MSC Trustgate.com verify the identity and trustworthiness of such person.

5.3.2. Background check procedures

Prior to commencement of employment in a Trusted Role, MSC Trustgate.com conducts background checks which include the following:

• confirmation of previous employment,

• check of professional reference,

• confirmation of the highest or most relevant educational degree obtained,

• search of criminal records (local, state, or provincial, and national),

• check of credit/financial records,

• search of driver's license records, and

• search of QIIS records

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, MSC Trustgate.com will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

5.3.3. Training requirements

MSC Trustgate.com provide all personnel performing information verification duties with skills-training Sanctions for unauthorized actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of MSC Trustgate.com policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.4. Independent contractor requirements

MSC Trustgate.com verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.5. Documentation supplied to personnel

MSC Trustgate.com.com shall provide its employees the requisite training, this CPS, CP and all relevant documentations such as technical operational and administrative needed to perform their job responsibilities competently and satisfactorily.

5.4. Audit logging procedures

5.4.1. Types of events recorded

MSC Trustgate.com.com and its RA shall record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. MSC

Trustgate.com shall make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

5.4.2. Frequency of processing log

Audit log files shall be generated for all events relating to the security and services of the Issuing CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. Issuing MSC Trustgate.com record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. Issuing MSC Trustgate.com make these records available to its Qualified Auditor as proof of the CA's compliance with associated CA audit scheme stipulated in introduction.

Issuing MSC Trustgate.com record at least the following events:

CA key life cycle management events, including:

• Key generation, backup, storage, recovery, archival, and destruction;

• Cryptographic device life cycle management events; and

• CA system equipment configuration.

CA and Subscriber Certificate life cycle management events, including:

• Certificate Requests, renewal, and re-key requests, and revocation for both successful and unsuccessful attempts; • All Certificates issued including revoked and expired Certificates;

• All verification activities stipulated in this CPS;

• Date, time, phone number used, persons spoken to, and end results of verification telephone calls;

• Acceptance and rejection of Certificate Requests;

• Issuance of Certificates; and

• Generation of Certificate Revocation Lists and OCSP entries including failed read-and write operations on the Certificate and CRL directory as well as actual CRLs.

Security events, including:

• Successful and unsuccessful PKI system access attempts;

• PKI and security system actions performed;

• Security profile changes;

• System crashes, hardware failures, and other anomalies;

• Firewall and router activities; and

• Entries to and exits from the CA facility

Log entries includes the following elements;

1. Date and time of entry;

2. Identity of the person making the journal entry; and

3. Description of the entry.

5.4.3. Retention period for audit log

Audit log records are held for a period of time as appropriate to provide necessary legal evidence in accordance with any applicable legislation.

5.4.4. Protection of audit log

Events are logged with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, tampering or destroyed. The audit log files are protected to ensure that only individuals with authorised trusted access are able to perform any operations without modifying integrity, authenticity, and confidentiality of the data.

5.4.5. Audit log backup procedures

Incremental backups of audit logs are created daily, and full backups shall be performed weekly by authorised Trusted Personnel. The backup is stored in a secure location (e.g., file proof safe).

5.4.6. Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network, and operating system level. Manually generated audit data is recorded by MSC Trustgate.com personnel.

5.4.7. Notification to event-causing subject

No stipulation.

5.4.8. Vulnerability assessments

MSC Trustgate.com's security program shall include an annual Risk Assessment that:

a) Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

c) Assesses the sufficiency of the policies, procedures, information

5.5. Records archival

5.5.1. Types of records archived

No stipulation

5.5.2. Retention period for archive

MSC Trustgate.com retain all documentation relating to certificate requests and the verification thereof,

and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3. Protection of archive

No Stipulation.

5.5.4. Archive backup procedures

No Stipulation.

5.5.5. Requirements for time-stamping of records

All entries in the log files shall contain time and date information at which the event occurred

5.5.6. Archive collection system (internal or external)

The archive collection system shall comply with the requirements in Section 5.

5.5.7. Procedures to obtain and verify archive information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified by checking the readability of the information.

5.6. Key changeover

No Stipulation.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

Issuing CAs shall establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or Compromise the Issuing CA services. Issuing CAs should carry out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution, etc.). This business continuity is included in the scope of the audit process as described in Section 8 to validate which operations should be first restored after a disaster and the recovery plan. Issuing CA personnel that serve in a trusted role and operational role should be specially trained to operate according to procedures defined in the disaster recovery plan for business-critical operations.

If an Issuing CA detects a potential hacking attempt or another form of Compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, the Issuing CA should assess the scope of potential damage in order to determine if the CA or RA system needs to be rebuilt, if only some Certificates need to be revoked, and/or if a CA hierarchy needs to

be declared as Compromised. The CA disaster recovery plan should highlight which services should be maintained (for example, revocation and Certificate status information).

5.7.2. Computing resources, software, and/or data are corrupted

If any equipment is damaged or rendered inoperative, but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to the Issuing CA's disaster recovery plan.

5.7.3. Entity private key compromise procedures

In the event an Issuing CA Private Key is Compromised, lost, destroyed, or suspected to be Compromised:

• The Issuing MSC Trustgate.com, after investigation of the problem, decide whether the Issuing CA Certificate should be revoked. If so, then:

o All the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity; and

o A new Issuing CA Key Pair shall be generated, or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates.

5.7.4. Business continuity capabilities after a disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability.

5.8. CA or RA termination

When it is necessary to terminate an Issuing CA or RA activities, the impact of the termination must be minimized as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing CA and/or Registration Authority Agreements. Issuing CAs must specify the procedures they will follow when terminating all or a portion of their Digital Certificate issuance and management operations. The procedures must, at a minimum: • ensure that any disruption caused by the termination of an Issuing CA is minimised as much as possible;

- ensure that archived records of the Issuing CA are retained;
- ensure that prompt notification of termination is provided to Subscribers, Authorised
- Relying Parties, Application Software Providers, and other relevant stakeholders in
- MSC Trustgate.com certificate lifecycles;
- ensure Certificate status information services are provided and maintained for the
- applicable period after termination, including, if applicable, transferring Certificate status
- information services to another GMO Internet Group entity;
- ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the
- time of termination is maintained;
- notify all auditors including the eIDAS Conformity Assessment Body; and
- notify the Belgian eIDAS supervisory body (FPS Economy, SMEs, Self-employed and
- Energy - Quality and Safety) and other relevant Government and Certification bodies under
- applicable laws and related regulations.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

For Root CA Key Pairs, MSC Trustgate.com shall performs following controls; 1. prepares and follows a Key Generation Script, 2. has a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and

3. has a Qualified Auditor issue a report opining that MSC Trustgate.com followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

In other CA Key Pairs, issuing MSC Trustgate.com performs following controls;

1. Generates the keys in a physically secured environment as described in Section 5.1 and 5.2.2. of Certificate Policy and/or Certification Practice Statement;

2. Generates the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;

3. Generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;

4. Log its CA key generation activities; and

5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

For Subscriber keys generated by issuing CA, Key generation must be performed in a secure cryptographic device that meets FIPS 140-2 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6. Issuing MSC Trustgate.com also reject a certificate request if it has a known weak Private Key. Issuing CAs shall generate all issuing Key Pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. External witnesses (Ideally an independent auditor who normally performs audits on a regular basis) should be present or the ceremony must be videotaped/recorded. Issuing CA key generation is carried out within a device which is at least certified to FIPS 140-2 level 3 or above.

Subscriber key generation by MSC Trustgate.com is performed in a secure cryptographic device meeting FIPS 140-2 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

6.1.2. Private key delivery to subscriber

Issuing CAs that create Private Keys on behalf of Subscribers may do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. The cryptographic algorithms regarding Public/Private key generation (encryption, sign, cryptographic hash, RNG or PRNG etc.) were approved by FIPS, the Public/Private key generation algorithm is also specified in FIPS 186-4. The generated Public/Private key is encrypted with PIN code which was provided by the Subscriber. The encrypted Public/Private key will be delivered in TLS session, authenticated by the password pre-registered by an administrator of the Subscriber.

6.1.3. Public key delivery to certificate issuer

Issuing CAs shall only accept Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2.1 of this CP

6.1.4. CA public key delivery to relying parties

Issuing CAs shall ensure that Public Key delivery to Relying Parties is undertaken in such a way as to prevent substitution attacks. This may include working with commercial browsers and platform operators to embed Root Certificate Public Keys into root stores and operating systems. Issuing CA Public Keys may be delivered by the Subscriber in the form of a chain of Certificates or via a Repository operated by the Issuing CA and referenced within the profile of the issued Certificate

6.1.5. Key sizes

MSC Trustgate.com follows NIST Special Publication 800-133 (2012) - Recommendation for Cryptographic Key Generation - for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Issuing CAs and end entity Certificates delivered to Subscribers. Any Subordinate CAs in the Trusted Root program, outside of the direct control of MSC Trustgate.com are contractually obligated to use the same best practices.

MSC Trustgate.com selects from the following Key Sizes/Hashes for Root Certificates, Issuing CA Certificates and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the Baseline Requirements and EV Guidelines: SSL Certificates must meet Baseline Requirements Section 6.1.5 on algorithm type and key size.

6.1.6. Public key parameters generation and quality checking

Issuing CAs shall generate Key Pairs in accordance with FIPS 186 and shall use reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission. Issuing CAs shall reference Baseline Requirements Section 6.1.6 on quality checking.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

Issuing CAs shall set key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (See Section 7.1). Private Keys corresponding to Root Certificates shall not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;

2. Certificates for Subordinate CAs and Cross Certificates;

3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and

4. Certificates for OCSP Response verification.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Issuing CAs shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. Issuing CAs shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1. Cryptographic module standards and controls

Issuing CAs shall ensure that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection. Issuing CAs that require Subscribers to use FIPS 140-2 level 2 or above systems for Private Key protection must contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection. This can be achieved, for example, through limitation to a suitable CSP (Cryptographic Service Provider) tied to a known FIPS compliant hardware platform as part of the enrolment process.

6.2.2. Private key (n out of m) multi-person control

Issuing CAs shall activate Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this Private Key multi-person controls are strongly authenticated (i.e. token with PIN code).

6.2.3. Private key escrow

Issuing CAs shall not escrow CA Private Keys for any reason.

6.2.4. Private key backup

Issuing CAs shall back up Private Keys under the same multi-person control as the original Private Key for disaster recovery plan purposes.

6.2.5. Private key archival

With the exception of Digital Signing Service, Issuing CAs shall not archive Private Keys and must ensure that any temporary location where a Private Key may have existed in any memory location during the generation process is purged.

6.2.6. Private key transfer into or from a cryptographic module

Issuing CA Private Keys must be generated, activated, and stored in Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they must be encrypted. Private Keys must never exist in plain text outside of a cryptographic module. If MSC Trustgate.com becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the MSC Trustgate.com shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7. Private key storage on cryptographic module

Issuing CAs shall store Private Keys on at least a FIPS 140-2 level 3 device

6.2.8. Method of activating private key

Issuing CAs are responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9. Method of deactivating private key

Issuing CAs shall ensure that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time, an Issuing CA's Hardware Security Module is on-line and operational it is only used to sign Certificates and

CRL/OCSPs from an authenticated RA. When a CA is no longer operational, its Private Keys are removed from the Hardware Security Module.

6.2.10. Method of destroying private key

Issuing CA Private Keys must be destroyed when they are no longer needed or when the Certificate to which they correspond have expired or are revoked. Destroying Private Keys requires Issuing CAs to destroy all associated CA secret activation data in the HSM in such a manner that no information can be used to deduce any part of the Private Key.

Private Keys generated by MSC Trustgate.com are stored in GCC in PKCS 12 format until the Key Pairs are picked up by the Subscriber. When the Subscriber acknowledge the receipt of the Key Pair or when 30 days has passed after the key generation, the Subscriber Key Pair is automatically deleted from GCC. Subscriber Private Keys are not stored in any other systems.

6.2.11. Cryptographic Module Capabilities

See Section 6.2.1

6.3. Other aspects of key pair management

6.3.1. Public key archival

Issuing CAs must archive Public Keys from Certificates.

6.3.2. Certificate operational periods and key pair usage periods

6.4. Activation data

6.4.1. Activation data generation and installation

Generation and use of Issuing CA activation data used to activate Issuing CA Private Keys shall be made during a key ceremony (Refer to Section 6.1.1). Activation data shall be generated automatically by the appropriate HSM and delivered to a shareholder who must be a person in trusted role. The delivery method must maintain the confidentiality and the integrity of the activation data.

6.4.2. Activation data protection

Issuing CA activation data must be protected from disclosure through a combination of cryptographic and physical access control mechanisms. Issuing CA activation data must be stored on smart cards.

6.4.3. Other aspects of activation data

Issuing CA activation data must only be held by Issuing CA personnel in trusted roles.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

The following computer security functions must be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Issuing CA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide discretionary access control with least privilege;
- Provide security audit capability (protected in integrity);

• Prohibit object re-use;

• Require use of strong password policy;

• Require use of cryptography for session communication;

• Require trusted path for identification and authentication;

• Provide means for malicious code protection;

• Provide means to maintain software and firmware integrity;

• Provide domain isolation and partitioning different systems and processes; and

• Provide self-protection for the operating system.

6.5.2. Computer security rating

All the Issuing CA PKI component software has to be compliant with the requirements of the protection profile from a suitable entity.

6.6. Life cycle technical controls

6.6.1. System development controls

The system development controls for the Issuing CA are as follows:

• Use software that has been designed and developed under a formal, documented development methodology;

• Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);

• Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;

• All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;

• The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation;

• Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are installed on the equipment and are obtained from sources authorized by local policy. Issuing CA hardware and software are scanned for malicious code on first use and periodically thereafter; and

• Hardware and software updates are purchased or developed in the same manner as original equipment; and are installed by trusted and trained personnel in a defined manner.

6.6.2. Security management controls

The configuration of the Issuing CA system as well as any modifications and upgrades are documented and controlled by the Issuing CA management. There is a mechanism for detecting unauthorized modification to the Issuing CA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the Issuing CA system. The Issuing CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3. Life cycle security controls

Issuing CA monitors the maintenance scheme requirements in order to maintain the level of trust of software and hardware that are evaluated and certified.

6.7. Network security controls

Issuing CA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of security guards, firewalls and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8. Time-stamping

All Issuing CA components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

7.1.1. Version number(s)

Issuing CAs shall issue Certificates in compliance with X.509 Version 3.

7.1.2. Certificate extensions

Issuing CAs shall issue Certificates in compliance with RFC 5280 and applicable best practice including compliance to the current CA/B Forum Baseline Requirements sections 7.2.1.1 through 7.2.1.5. Criticality shall also follow best practice and where possible prevent unnecessary risks to Relying Parties when applied to name constraints

7.1.3. Algorithm object identifiers

MSC Trustgate.com not issue Subscriber Certificates utilizing the SHA-1 algorithm. The CA may continue to use their existing SHA-1 Root Certificates. However, SHA-2 Subscriber certificates should not chain up to a SHA-1 Subordinate CA Certificate.

7.1.4. Name forms

Issuing CAs must issue Certificates with name forms compliant to RFC 5280 and section 7.1.4 of CA/B Forum Baseline Requirements for SSL, EV Code Signing Certificates that chain up to Publicly Trusted Root.

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.5. Name constraints

Issuing CAs may issue Subordinate CA Certificates with name constraints and mark as critical where necessary. When name constraints are NOT set on a Subordinate CA, such CA must be subject for full audit specified in section 8.0 of this document.

MSC Trustgate.com may issue Subordinate CA Certificates with name constraints where necessary and mark as critical where necessary as part of the Trusted Root program.

7.1.6. Certificate policy object identifier

MSC Trustgate.com follows Section 7.1.6 of CA/B Forum Baseline Requirements

7.1.7. Usage of Policy Constraints extension

No stipulation

7.1.8. Policy qualifiers syntax and semantics

No stipulation

7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation

7.2. CRL profile

7.2.1. Version number(s)

MSC Trustgate.com.com shall issue X.509 Version 2 CRLs in compliance with RFC 5280.

7.2.2. CRL and CRL entry extensions

No Stipulation.

7.3. OCSP profile

No Stipulation.

7.3.1. Version number(s)

No Stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

MSC Trustgate.com at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;

2. Comply with these Requirements;

3. Comply with the audit requirements set forth in this section; and

4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1. Frequency or circumstances of assessment

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with Section 7.1.5 and audited in line with Section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.1, then no pre-issuance readiness assessment is necessary. If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.1, then, before issuing Publicly-Trusted Certificates, MSC Trustgate.com successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.1. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

8.2. Identity/qualifications of assessor

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;

2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1);

3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;

4. For audits conducted in accordance with any one of the ETSI standards - accredited in accordance with ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits;

5. For audits conducted in accordance with the WebTrust standard - licensed by WebTrust;

6. Bound by law, government regulation, or professional code of ethics; and

7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/ Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3. Assessor's relationship to assessed entity

MSC Trustgate.com.com chooses an auditor/assessor who is completely independent from MSC Trustgate.com.

8.4. Topics covered by assessment

MSC Trustgate.com undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities v2.0;

2. A national scheme that audits conformance to ETSI TS 102 042;

3. A scheme that audits conformance to ISO 21188:2006; or

4. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

The audit MUST be conducted by a Qualified Auditor, as specified in Section 8.2. If a Delegated Third Party is not currently audited in accordance with Section 8 and is not an Enterprise RA, then prior to certificate issuance MSC Trustgate.com ensure that the domain control validation process required under Section 3.2.2.4 or IP address verification under 3.2.2.5 has been properly performed by the Delegated Third Party by either

(1) using an out-of-band mechanism involving at least one human who is acting either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request or (

2) performing the domain control validation process itself. If the CA is not using one of the above procedures and the Delegated Third Party is not an Enterprise RA, then MSC Trustgate.com obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.1, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement.

If the opinion is that the Delegated Third Party does not comply, then MSC Trustgate.com not allow the Delegated Third Party to continue performing delegated functions. The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit). However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years. Actions taken because of deficiency MSC Trustgate.com shall follow the same process if presented with a material non-compliance by external auditors and create a suitable corrective action plan to remove the deficiency.

8.5. Actions taken as a result of deficiency

No Stipulation

8.6. Communication of results

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1. MSC Trustgate.com make the Audit Report publicly available. The CA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. For both government and commercial CAs, the CA SHOULD make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, MSC Trustgate.com provide an explanatory letter signed by the Qualified Auditor.

The Audit Report MUST contain at least the following clearly-labelled information:

1. name of the organization being audited;

2. name and address of the organization performing the audit;

3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;

4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);

5. a list of the CA policy documents, with version numbers, referenced during the audit;

6. whether the audit assessed a period of time or a point in time;

7. the start date and end date of the Audit Period, for those that cover a period of time;

8. the point in time date, for those that are for a point in time;

9. the date the report was issued, which will necessarily be after the end date or point in time date; and

10. (for audits conducted in accordance with any of the ETSI standards) a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part 1 (General Requirements), and/or Part 2 (Requirements for Trust Service Providers). pg. 85

11. (for audits conducted in accordance with any of the ETSI standards) a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as this document, and the version used.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and the MSC Trustgate.com ensure it is publicly available.

The Audit Report MUST be available as a PDF and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7. Self-Audits

During the period in which the CA issues Certificates, the MSC Trustgate.com monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.1, the MSC Trustgate.com strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The MSC Trustgate.com review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

The MSC Trustgate.com internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate MSC Trustgate.com monitor adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practice Statement. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the MSC Trustgate.com ensure all applicable CP are met.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate issuance or renewal fees

No Stipulation

9.1.2. Certificate access fees

No Stipulation

9.1.3. Revocation or status information access fees

No Stipulation

9.1.4. Fees for other services

No Stipulation

9.1.5. Refund policy

Neither MSC Trustgate.com nor any RAs operating under MSC Trustgate.com or any Resellers provide any refunds for Certificates or services provided in respect to Certificates.

9.2. Financial responsibility

9.2.1. Insurance coverage

No Stipulation.

9.2.2. Other assets

No Stipulation.

9.2.3. Insurance or warranty coverage for end-entities

No Stipulation

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

No Stipulation.

9.3.2. Information not within the scope of confidential information

No Stipulation

9.3.3. Responsibility to protect confidential information

No Stipulation.

9.4. Privacy of personal information

9.4.1. Privacy plan

No Stipulation

9.4.2. Information treated as private

No Stipulation

9.4.3. Information not deemed private

No Stipulation.

9.4.4. Responsibility to protect private information

No Stipulation.

9.4.5. Notice and consent to use private information

No Stipulation.

9.4.6. Disclosure pursuant to judicial or administrative process

No Stipulation.

9.4.7. Other information disclosure circumstances

No Stipulation.

9.5. Intellectual property rights

No Stipulation.

9.6. Representations and warranties

9.6.1. CA representations and warranties

No Stipulation.

9.6.2. RA representations and warranties

No Stipulation.

9.6.3. Subscriber representations and warranties

No Stipulation.

9.6.4. Relying party representations and warranties

No Stipulation.

9.6.5. Representations and warranties of other participants

No Stipulation.

9.7. Disclaimers of warranties

No Stipulation.

9.8. Limitations of liability

No Stipulation.

9.9. Indemnities

No Stipulation.

9.10. Term and termination

9.10.1. Term

No Stipulation.

9.10.2. Termination

No Stipulation.

9.10.3. Effect of termination and survival

No Stipulation.

9.11. Individual notices and communications with participants

No Stipulation.

9.12. Amendments

9.12.1. Procedure for amendment

No Stipulation.

9.12.2. Notification mechanism and period

No Stipulation.

9.12.3. Circumstances under which OID must be changed

No Stipulation.

9.13. Dispute resolution provisions

No Stipulation.

9.14. Governing law

No Stipulation.

9.15. Compliance with applicable law

No Stipulation.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

No Stipulation.

9.16.2. Assignment

No Stipulation.

9.16.3. Severability

No Stipulation.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No Stipulation.

9.16.5. Force Majeure

No Stipulation.

9.17. Other provisions

No Stipulation.