

Short Form Certificate Policy



Australian Government

Medicare Australia

Medicare Australia Site Certificates Communities of Interest (CoI) Certificate Policy (CP)
for Site Certificates issued under the
Medicare Australia Organisation Certification
Authority (Medicare Australia OCA) V1.6

February 2007

Copyright Notice:

This document contains information protected by copyright. © Commonwealth of Australia

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the Copyright Act 1968, all other rights are reserved. Requests and enquiries concerning reproduction and rights should be addressed to The Manager, Media, Marketing and Communications Branch, Medicare Australia National Office, PO Box 1001 Tuggeranong DC ACT 2901.

Contact

Medicare Australia
Locked Bag 6666
Tuggeranong DC ACT 2901
AUSTRALIA

This Document has been authorised by the Medicare Australia Policy Management Authority:

_____ Date: _____
General Manager or nominee, Information Technology Services Division, Medicare Australia

Introduction

This is the Certificate Policy for Site Certificates issued to practices and entities known to Medicare Australia (for example, government departments and agencies; health and welfare services providers) to enable them to conduct secure transactions and data exchange with Medicare Australia and other parties in relation to programs authorised or approved by Medicare Australia or within an entity's Community of Interest recognised by Medicare Australia.

The document is structured and numbered according to the *Gatekeeper Short Form Certificate Policy Template*.

This CP should be read in conjunction with the Medicare Australia Organisation Certification Authority Certification Practice Statement (Medicare Australia OCA CPS).

Terminology

Site Certificate means a Certificate issued under this CP.

Site means:

- a) the site location of any practice registered by Medicare Australia for a Medicare Australia program. The practice may be referred to as a Registered Medicare Australia Practice or practice and includes Pharmacies and aged care providers (however described); and
- b) any site of an entity, where that entity is recognised by Medicare Australia as a member of a Medicare Australia recognised Community of Interest and is known to Medicare Australia and where Medicare Australia is the Relationship Organisation.

• Certificate Policy Clauses

CP Identification

Certificates issued under this CP shall bear the Policy OID:

1.2.36.174030967.1.6.1.1

(where "174030967" is the last 9 digits of Medicare Australia's Australian Business Number).

1. INTRODUCTION

Practices and entities who wish to undertake secure electronic transmissions:

- with Medicare Australia and /or access to data held by Medicare Australia; and / or
- within a Community of Interest

may require a site certificate (Site Certificate).

The Relationship model (also referred to as Known Customer PKI) streamlines the enrolment of practices and entities for a Site Certificate.

The Site Certificate has a unique Policy OID.

The Relationship Organisation for this CP is Medicare Australia.

The Relationship Organisation Units (ROU) are:

- program area(s) in Medicare Australia responsible for programs accessible by practices using Site Certificates; and
- entities who are members of a Community of Interest.

The Relationship Organisation Unit Operators (ROUOs) are:

- Medicare Australia personnel (for Medicare Australia) who accept and manage the registration of practices); or
- personnel of the entities who are members of the Community of Interest who accept and manage the registration of entities

to participate in a program using the practice or entity's Site Certificate.

1.1 PKI Participants

1.1.1 Certification Authority

All Certificates issued under this CP shall be produced by the Medicare Australia Organisation Certification Authority (Medicare Australia OCA).

Refer to the Medicare Australia Organisation Certification Authority Practice Statement (Medicare Australia OCA CPS) for further information on applicable practices and procedures for Certificates issued under this CP.

1.1.2. Relationship Organisation

Medicare Australia is the Relationship Organisation (Medicare Australia RO) in the Health Sector PKI.

1.1.3. Relationship Organisation Unit

There are separately identified Relationship Organisation Units (ROUs) within the Medicare Australia RO, usually one ROU for each Community of Interest (CoI) in the Health Sector PKI operated by Medicare Australia.

The ROU has responsibilities in the CoI in managing the Subscribers in that CoI.

The various program areas in Medicare Australia are the ROUs for the participating practices.

The entities in a Medicare Australia recognised CoI are the ROUs for the participating entities.

1.1.4 Certificate Controllers

Certificate Controllers are Medicare Australia RO personnel with responsibilities for management of Certificates.

All Certificate Controllers operating under this CP are duly authorised representatives of Medicare Australia.

Certificate Controllers may not be located within the various program areas of Medicare Australia. Certificate Controllers are Medicare Australia personnel who may be located outside of the program areas.

1.1.5 Relationship Organisation Unit Operators

Relationship Organisation Unit Operators (ROUOs) who are Medicare Australia personnel within the relevant program CoI are located within Medicare Australia.

ROUOs who are personnel of an entity within a relevant CoI are located within that entity.

ROUOs within any CoI are not Certificate Controllers.

All ROUOs operate in accordance with the processes and procedures set out in the Medicare Australia OCA CPS and this CP.

1.1.6. Subscribers

All Subscribers for Site Certificates shall be either:

- practices registered with a Medicare Australia program and known to Medicare Australia as such according to an application for participation in a Medicare Australia program, or
- an entity which is known to Medicare Australia and is a member of a recognised Medicare Australia Community of Interest.

A person, who is authorised by a practice or entity to bind the practice or entity, must enter into the Subscriber agreement for a Site Certificate which is known as the *Medicare Australia Communities of Interest Site Certificate Terms and Conditions of Use*.

1.1.7. Relying Parties

The Relying Party under this CP, in relation to Medicare Australia program CoIs, is Medicare Australia, as receiver of transactions secured using the Site Certificates.

The Relying Party under this CP, in relation to entities known to Medicare Australia and who are in a recognised Medicare Australia CoI, is the other entity in the CoI who is the receiver of transactions secured using the Site Certificates.

There is no Relying Party Agreement under this CP.

Parties who rely on Certificates issued under this CP and who do not have a written agreement with Medicare Australia relating to transactions with Medicare Australia, or who undertake transactions that are not authorised or approved by Medicare Australia rely on such certificates at their own risk.

1.2 Certificate Use

1.2.1 Appropriate Certificate Uses

Key Pairs and Certificates issued under this CP are to be used by Sites to secure transactions for programs and services authorised or approved by Medicare Australia.

1.2.2 Prohibited Certificate Uses

There are no prohibited certificate uses. Parties using the Site Certificates for any transaction other than transactions authorised or approved by Medicare Australia do so at their own risk.

1.3 Definitions and Acronyms

Definitions and Acronyms are in the Health Sector PKI Glossary at www.medicareaustralia.gov.au.

2. IDENTIFICATION AND AUTHENTICATION OF USERS

2.1 Naming of Subscribers

Subscribers (termed 'Certificate Subjects' in the x.509 definition) under this CP will be named (and the uniqueness of their names will be assured) consistent with the name recognised by Medicare Australia through its relationship with the Subscriber. This may include the name by which Medicare Australia has recognised the entity as a member of a CoI or the name under which the entity is registered as a Subscriber.

2.2 Identification and authentication of the Subscriber at registration

Subscribers under this CP will be identified and authenticated by:

- Medicare Australia ROUs responsible for registering practices for Medicare Australia programs and services; or
- In each CoI, the entity's ROU responsible for registering that entity for a Site Certificate in the Health Sector PKI operated by Medicare Australia.

2.3 Identification and authentication of the Subscriber at renewal

Subscribers under this CP shall be identified and authenticated and the Certificate renewed automatically provided that

- if the Site is a Registered Medicare Australia Practice, its registration status with the relevant ROU has not changed, or
- if the Site is an entity recognised by Medicare Australia in a Medicare Australia CoI, its registration status with that entity's ROU has not changed.

Note: all certificate renewals under this CP involve re-keying.

2.4 Identification and authentication of revocation request

Revocation of certificates under this CP shall only be requested by:

- ROUOs in the event that the Subscriber becomes ineligible to remain as a Registered Medicare Australia Practice or entity recognised by Medicare Australia as a member of a Medicare Australia recognised CoI; or
- The Subscriber by written notice; or
- Certificate Controllers.

3. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

3.1. Certificate creation

3.1.1. Enrolment process and responsibilities

Where a Site is a Registered Medicare Australia Practice, the Site may be enrolled automatically for Certificates by Certificate Controllers on the basis of that registration.

Where a Site is a not a Registered Medicare Australia Practice, the practice may apply to the relevant ROU for the CoI of the Medicare Australia program or service to be registered for that program or service and to be enrolled for Site Certificates when registration as a Registered Medicare Australia Practice occurs.

Where a Site is a not a Registered Medicare Australia Practice, the entity, being a member of a Medicare Australia CoI and responsible for that Site, may apply to the Medicare Australia RO Certificate Controllers to be enrolled for Site Certificates.

All applications made a practice and an entity are the responsibility of the practice or entity through its authorised contact person (however described).

3.1.2. Publication of the certificate by the CA

Certificates issued under this CP will be published in the Healthcare Public Directory.

Revocation status of Certificates issued under this CP will be published in the Healthcare Public Directory.

3.2. Key Pair and Certificate Usage

3.2.1 Key pair generation and installation

The Subscriber Key Pairs and Certificates issued under this CP shall be generated by a Certificate Controller using accredited software.

The signing key and Certificate will be stored in a password protected PKCS#12 file separate from the encryption key and Certificate. These PKCS#12 files are stored in electronic medium¹ and posted as instructed by the ROUO.

¹ 'electronic medium' includes floppy disk, CD or other medium in which data can be stored electronically.

A passphrase to access the keys and Certificates will be generated and posted separately to the Subscriber.

3.3. Certificate renewal

Certificates issued under this CP shall be renewed automatically by the Certificate Controllers.

In the case of a Registered Medicare Australia Practice, the Certificate shall be renewed automatically after checking its status or on advice from the ROUOs, provided the status of the Registered Medicare Australia Practice has not changed.

In the case of an entity, the Certificate shall be renewed automatically after checking its status or on advice from the ROUOs, provided the status of the entity has not changed.

Refer to clause 2.3 for details of identification and authentication.

3.4. Certificate revocation

Certificates issued under this CP may be revoked by Medicare Australia in its absolute discretion, including but not limited to:

- after loss, destruction or theft of the Site Certificate;
- in the event of de-registration of the practice (however described) whether in relation to participation in any Medicare Australia program or not;
- in the event of any Approvals (however described) relating to the practice being cancelled by Medicare Australia;
- in the event any Approval Number(s) (however described) relating to the practice being cancelled by Medicare Australia;
- in the event that the entity ceases to exist or be recognised by Medicare Australia or ceases to be a member of a Medicare Australia recognised Col.

3.5 Certificate status services

3.5.1 Operational characteristics

Details of Operational Characteristics are not provided.

3.5.2 Service availability

Service availability for the Certificate Revocation List (CRL) is substantially 24 x 7 at www.certificates-australia.com.au.

3.5.3 Optional features

Details of Optional Features are not provided.

4. REGISTRATION OPERATIONAL CONTROLS

4.1 Personnel controls

All Certificate Controllers under this CP shall be authorised representatives of Medicare Australia.

4.2 Logical and Technological controls

Certificate requests will be processed by the authorised Certificate Controllers of Medicare Australia in accordance with the security provisions of the Medicare Australia OCA CPS.

4.3 Physical controls

Certificate requests will be processed by Authorised Certificate Controllers in accordance with the security provisions of the Medicare Australia OCA CPS.

4.4 Business continuity of the Relationship Organisation

As Medicare Australia (the Relationship Organisation under this CP) is a statutory agency under the *Medicare Australia Act 1973*, its continuation depends on continuance in force of the *Medicare Australia Act 1973* or by other Acts of the Commonwealth Parliament made pursuant to government policy.

Changes in legislation or government policy will provide for business continuity of the RO in accordance with policy as determined by the government.

4.5 Relationship Organisation termination

As Medicare Australia is a statutory agency under the *Medicare Australia Act 1973*, its termination or change of entity status is through amendment to the *Medicare Australia Act 1973* or by other Acts of the Commonwealth Parliament made pursuant to changes in government policy.

5. CERTIFICATE, CRL AND OCSP PROFILES

5.1 Certificate profile – Site Encipherment Certificate

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V3	M	
1.2. Serial Number	A positive integer that uniquely identifies the Certificate.	M	
1.3. Signature Algorithm	SHA-1 RSA, SHA-1 hashing algorithm using the RSA signing algorithm.	M	
1.4. Issuer Distinguished Name		M	
1.4.1. Country (C)	AU	M	
1.4.2. Organization (O)	GOV	M	
1.4.3. Organization Unit (OU)	Medicare Australia	M	
1.4.3. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.5. Validity			
1.5.1. Not Before	The date that the Certificate is valid from (system time at certificate issuance). YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later.	M	
1.5.2. Not After	The date that the Certificate is valid until. 5 years from Start Validity, i.e. certificate issuance. YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later	M	
1.6. Subject			
1.6.1. Country (C)	AU	M	
1.6.2. State (St)	<STATE>	M	
1.6.3. Locality (L)	<Suburb Name>	M	
1.6.4. Organization (O)	<Trading Name <Locality>>	M	
1.6.5. Organisation Unit (OU))	<Trading Name <Locality>>	M	
1.6.6. Common Name (CN)	<Trading Name <Locality>> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 2048 bits.	M	
2. X.509v3 Extensions			
2.1. Authority Key Identifier		M	Non-Critical
2.1.1. Key Identifier	SHA-1 hash (60 bits) of the Issuer's public key.		
2.1.2. AuthorityCertIssuer	Not present		
2.1.3. AuthorityCertSerialNumber	Not present		
2.2. Subject Key Identifier	SHA-1 hash (60 bits) of the Subject's public key.	M	Non-Critical
2.3. Key Usage		M	Critical
2.3.1. Digital Signature	NOT SET		
2.3.2. Non Repudiation	NOT SET		
2.3.3. Key Encipherment	SET		
2.3.4. Data Encipherment	NOT SET		
2.3.5. Key Agreement	NOT SET		
2.3.6. Key Certificate Signature	Not Selected		
2.3.7. CRL Signature	Not Selected		
2.4. Extended Key Usage	Not applicable		Non-Critical
2.5. Certificate Policies			Non-Critical
2.5.1. Policy Identifier	1.2.36.174030967.1.6.1.1		
2.5.1.1. Policy Qualifier ID	User Notice		
2.5.1.2. User Notice	Certificates issued under this CP must be relied on by entities within the Community of Interest, unless otherwise agreed, and not for purposes other than those permitted by this CP.		
2.5.1.3. Policy Qualifier ID	CPS URI		

Field	Content	Mandatory	Critical*
2.5.1.4. CPS URI	http://www.medicareaustralia.gov.au/		
2.6. Subject Alternate Names			Non-Critical
2.6.1. rfc822Name	<email address>	O	
2.7. Basic Constraints			
2.7.1. Subject Type	Not CA		Critical
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			
2.8.1. Access Description	Not present		
2.8.1.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.4.1)		Non-Critical
2.8.1.2. Alternative Name	URL=http://ocsp.certificates-australia.com.au/maoca.ppk		
2.9 CRL Distribution Point			
2.9.1 URL	http://www.certificates-australia.com.au/cgi-bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU		Non-Critical
3.0 Other Fields - Generic ²			
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	
3.0.2 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.174030967.0.4)	< Healthcare Provider Identifier >	O	
3.0.3 Generic IA5 String: Medicare Identifier (OID=1.2.36.174030967.0.5)	< Medicare Identifier >	O	
3.0.4 Generic IA5 String: Location ID (OID=1.2.36.174030967.1.6.2.1)	< Location ID >	O	
3.0.5 Generic IA5 String: Pharmacy Approval Number (OID=1.2.36.174030967.0.6)	< Pharmacy Approval Number >	O	

5.2 Certificate profile –Site Signing Certificate

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V3	M	
1.2. Serial Number	A positive integer that uniquely identifies the Certificate.	M	
1.3. Signature Algorithm	SHA-1 RSA, SHA-1 hashing algorithm using the RSA signing algorithm.	M	
1.4. Issuer Distinguished Name		M	
1.4.1. Country (C)	AU	M	
1.4.2. Organization (O)	Medicare Australia	M	
1.4.3. Organization Unit (OU)	Medicare Australia	M	
1.4.4. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.5. Validity			
1.5.1. Not Before	The date that the Certificate is valid from (system time at certificate issuance). YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later.	M	

² These Certificate extension OID references are expected to be common to all CoI Certificate Policies, and may have applicability to this CoI.

Field	Content	Mandatory	Critical*
1.5.2. Not After	The date that the Certificate is valid until. 5 years from Start Validity, i.e. certificate issuance. YYMMDDHHMMSSZ encoded as UTCTime for dates up to 2049 and encoded as GeneralizedTime for dates in 2050 or later	M	
1.6. Subject			
1.6.1. Country (C)	AU	M	
1.6.2. State (St)	<STATE>	M	
1.6.3. Locality (L)	<Suburb Name>	M	
1.6.4. Organization (O)	<Trading Name <Locality>>	M	
1.6.5. Organisation Unit (OU)	<Trading Name <Locality>>	M	
1.6.6. Common Name (CN)	<Trading Name <Locality>> :RA Number	M	
1.7. Subject Public Key Info	RSA Public Key of 2048 bits.	M	
2. X.509v3 Extensions			
2.1. Authority Key Identifier		M	Non-Critical
2.1.1. Key Identifier	SHA-1 hash (60 bits) of the Issuer's public key.		
2.1.2. AuthorityCertIssuer	Not present		
2.1.3. AuthorityCertSerialNumber	Not present		
2.2. Subject Key Identifier	SHA-1 hash (60 bits) of the Subject's public key.	M	Non-Critical
2.3. Key Usage		M	Critical
2.3.1. Digital Signature	SET		
2.3.2. Non Repudiation	NOT SET		
2.3.3. Key Encipherment	NOT SET		
2.3.4. Data Encipherment	NOT SET		
2.3.5. Key Agreement	NOT SET		
2.3.6. Key Certificate Signature	Not Selected		
2.3.7. CRL Signature	Not Selected		
2.4. Extended Key Usage	Not applicable		Non-Critical
2.5. Certificate Policies			Non-Critical
2.5.1. Policy Identifier	1.2.36.174030967.1.6.1.1		
2.5.1.1. Policy Qualifier ID	User Notice		
2.5.1.2. User Notice	Certificates issued under this CP must be relied on by entities within the Community of Interest, unless otherwise agreed, and not for purposes other than those permitted by this CP.		
2.5.1.3. Policy Qualifier ID	CPS URI		
2.5.1.4. CPS URI	http://www.medicareaustralia.gov.au/		
2.6. Subject Alternate Names			Non-Critical
2.6.1. rfc822Name	<email address>	O	
2.7. Basic Constraints			
2.7.1. Subject Type	Not CA		Critical
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			
2.8.1. Access Description	Not present		
2.8.1.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.4.1)		Non-Critical
2.8.1.2. Alternative Name	URL=http://ocsp.certificates-australia.com.au/maoca.pfx		
2.9 CRL Distribution Point			
2.9.1 URL	http://www.certificates-australia.com.au/cgi-bin/getcrl_health.pl?DN=cn%3DMedicare%20Australia%20Organisation%20Certification%20Authority%2Co%3DMedicare%20Australia%2Cc%3DAU		Non-Critical
3.0 Other Fields - Generic ³			

³ These Certificate extension OID references are expected to be common to all CoI Certificate Policies, and may have applicability to this CoI.

Field	Content	Mandatory	Critical*
3.0.1 Generic IA5 String: RA Number (OID=1.2.36.73665175.1.10009)	< RA Number >	M	
3.0.2 Generic IA5 String: Healthcare Provider Identifier (OID=1.2.36.174030967.0.4)	< Healthcare Provider Identifier >	O	
3.0.3 Generic IA5 String: Medicare Identifier (OID=1.2.36.174030967.0.5)	< Medicare Identifier >	O	
3.0.4 Generic IA5 String: Location ID (OID=1.2.36.174030967.1.6.2.1)	< Location ID >	O	
3.0.4 Generic IA5 String: Pharmacy Approval Number (OID=1.2.36.174030967.0.6)	< Pharmacy Approval Number >	O	

5.3 Medicare Australia OCA CRL Profile

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V2	M	
1.2. Signature Algorithm	sha1RSA	M	
1.3. Issuer Distinguished Name		M	
1.3.1. Country (C)	AU	M	
1.3.2. Organization (O)	GOV	M	
1.3.3. Organisational Unit (OU)	Medicare Australia		
1.3.3. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.4 Validity		M	
1.4.1 Effective Date			
1.4.2 Next Update			
1.5 CRL Number		M	
2. X.509v3 Extensions			
2.1. Authority Key Identifier		M	Non-Critical
2.1.1. Key Identifier	SHA-1 hash (60 bits) of the Issuer's public key		

Frequency of issuing	60 minutes		
Grace Period	60 minutes		

5.4 Medicare Australia OCA OCSP Profile

Field	Content	Mandatory	Critical*
1. X.509v1 Field			N/A
1.1. Version	V3	M	
1.2. Serial Number	Unique value assigned by the Issuing CA	M	
1.3. Signature Algorithm	SHA-1 with RSA Signature	M	
1.4. Issuer Distinguished Name		M	
1.4.1. Country (C)	AU	M	
1.4.2. Organization (O)	GOV	M	
1.4.3. Organisational Unit (OU)	Medicare Australia		
1.4.4. Common Name (CN)	Medicare Australia Organisation Certification Authority	M	
1.5. Validity	5 years		
1.5.1. Not Before	Issue date	M	

Field	Content	Mandatory	Critical*
1.5.2. Not After	Expiry date	M	
1.6. Subject			
1.6.1. Country (C)	AU	M	
1.6.2. Organization (O)	GOV	M	
1.6.3. Organizational Unit (OU)	Medicare Australia		
1.6.4. Common Name (CN)	Medicare Australia OCA OCSP Responder	M	
1.7. Subject Public Key Info	Public Key encoded in accordance with RFC2459 & PKCS#1- 2048 bits	M	
2. X.509v3 Extensions			
2.1. Authority Key Identifier	SHA-1 hash (60 bits) of the Issuer's public key	M	Non-Critical
2.1.1. Key Identifier	The Key Identifier of the Issuer of this Certificate – 60 bit		
2.1.2. AuthorityCertIssuer	Not present		
2.1.3. AuthorityCertSerialNumber	Not present		
2.2. Subject Key Identifier	SHA-1 hash (60 bits) of the Subject's public key	M	Non-Critical
2.3. Key Usage		M	Critical
2.3.1. Digital Signature	SET		
2.3.2. Non Repudiation	Not Selected		
2.3.3. Key Encipherment	Not Selected		
2.3.4. Data Encipherment	Not Selected		
2.3.5. Key Agreement	Not Selected		
2.3.6. Key Certificate Signature	Not Selected		
2.3.7. CRL Signature	Not Selected		
2.4. Extended Key Usage			Non-Critical
2.4.1. OCSP Signing	1.3.6.1.5.5.7.3.9		
2.5. Certificate Policies			
2.5.1. Policy Identifier	Not present		
2.5.1.1. Policy Qualifier ID	Not present		
2.5.1.2. User Notice	Not present		
2.5.1.3. Policy Qualifier ID	Not present		
2.5.1.4. User Notice	Not present		
2.6. Subject Alternate Names			Non-Critical
2.6.1. rfc822Name	NA		
2.7. Basic Constraints			
2.7.1. Subject Type	End Entity		N/A
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access			
2.8.1. Access Description	Not present		
2.8.1.1. Access Method	Not present		Non-Critical
2.8.1.2. Alternative Name	Not present		
3. No Check Extension (generic extension)			