



NCDC OBJECT IDENTIFIER ALLOCATION

VERSION 1.6

Copyright © 2009 National Center for Digital Certification, Kingdom of Saudi Arabia. This document is intended for use only by the National Center for Digital Certification and authorized Saudi National PKI participants. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes without prior written consent.

Control Page

Author(s)		
Name	Functional Section, Department	Signature/Date
Parag Parikh Chirag Patel	Senior IS Security Consultant, MIS	June 10 th 2008

Reviewed by		
Name	Functional Section, Department	Signature/Date
Mohammed Al-Ghamdi	Assistant Director, NCDC	January 27 th 2009

Approved by		
Name	Functional Section, Department	Signature/Date
Mohammed Al-Ghamdi	Assistant Director, NCDC	January 27 th 2009

Document Amendment Record			
Change No.	Date	Prepared by	Brief Explanation
1.0	April 01 st , 2008	Parag Parikh	Document Draft
1.1	June 09 th , 2008	Parag Parikh	Revision after receiving actual OID
1.2	June 10 th , 2008	Parag Parikh	Removal of NPA subnodes; Final Approval
1.3	July 09 th , 2008	Parag Parikh	Document Update to add Root CA CP/CPS, and, Government CSP CP/CPS
1.4	November 25 th , 2008	Parag Parikh	Finalize OID structure
1.5	January 26 th , 2009	Parag Parikh / Chirag Patel	New OID Structure
1.6	March 28 th , 2009	Chirag Patel	Added new OID under Government CA- Directory Extension

Table of Contents

Control Page	2
Table of Contents	3
Table of Figures	3
1. Abbreviations	4
2. Document Updates	4
3. Introduction	5
4. Object Identifiers (OIDs)	5
5. Object Identifiers allocated to MCIT/NCDC	6
5.1 THE NCDC OID	6
6. Object Identifiers allocated within NCDC	6
2.16.682.1.101.5000.1 PUBLIC KEY INFRASTRUCTURE	8
2.16.682.1.101.5000.1.1 NATIONAL POLICY AUTHORITY	9
2.16.682.1.101.5000.1.2 SAUDI NATIONAL ROOT CA	10
2.16.682.1.101.5000.1.3 GOVERNMENT CERTIFICATION AUTHORITIES	11
2.16.682.1.101.5000.1.4 LICENSED CERTIFICATION AUTHORITIES	14
2.16.682.1.101.5000.1.5 CERTIFICATE SERVICE PROVIDERS	14
7. Appendix A	15

Table of Figures

Figure1: OID Hierarchy.....	7
Figure2: NPA OID Structure	9
Figure3: Saudi National Root CA OID Structure.....	10
Figure4: Government CAs OID Structure.....	11
Figure5: Level1 CAs basic minimum OID Structure.....	15

1. Abbreviations

Abbreviation	Description
CA	Certification Authority
CP	Certificate Policy, used interchangeably with “Policy”
CPS	Certificate Practice Statement
PDS	PKI Disclosure Statement
CSP	Certificate Service Provider
ARL	Authority Revocation List
CRL	Certificate Revocation List
KSA	Kingdom of Saudi Arabia
DN	Distinguished Name
FIPS	Federal Information Processing Standards
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
SASO	Saudi Arabian Standards Organization
OCSF	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKIX	Public key Infrastructure X.509 standard
PMA	Policy Management Authority
NPA	National Policy Authority
NRCA	National Root Certification Authority
RA	Registration Authority
RFC	Request For Comments
MCIT	Ministry of Communication & IT
NCDC	National Center for Digital Certification
SSC	Shared Services Center
MIS	Al-Moammar Information Systems Co.

2. Document Updates

This is a dynamic document and specific details about the OID Allocation can be published on NCDC website. Alternatively, the NCDC OID Allocation can be published and updated on <http://www.oid-info.com/cgi-bin/display?tree=2.16.682> website. This document should be updated by NCDC on every change to the OID allocation, including addition/assignment of OID's and Retirement of OID's.

3. Introduction

During the design and build phases of the NCDC-SSC PKI Project, it was required that MCIT/NCDC has been allocated a globally unique object identifier (OID) to uniquely identify NCDC PKI objects within certificates. This document defines the OID that has been allocated to MCIT/NCDC, and should be used to catalogue and allocate the OIDs used throughout NCDC in the future.

4. Object Identifiers (OIDs)

OIDs provide a standard mechanism for uniquely identifying an object. Examples of objects, in the context of the NCDC PKI Project, include certificate policies, encryption algorithms, directory attributes, certificate extensions, etc.

OIDs are obtained by registering the information object in an OID tree. The tree consists of nodes arranged hierarchically. Each node has just one superior node, but may have many subordinate nodes. Each connection between any two nodes is represented by an integer. The OID for an object is the concatenation of the integers along the path from the root of the tree to the node for the object of interest. This numbering scheme ensures that each object represented as a node in the OID tree has a unique and unambiguous identifier.

Further information about OIDs can be found at <http://www.alvestrand.no/objectid/index.html> and <http://asn1.elibel.tm.fr/en/oid/index.htm>.

5. Object Identifiers allocated to MCIT/NCDC

MCIT/NCDC has exclusive authority to allocate OIDs in the tree below the OID allocated to it by the Saudi Arabian Standards Organization (SASO).

5.1 The NCDC OID

The following OID has been allocated to MCIT/NCDC by SASO:

2.16.682.1.101.5000

{joint-iso-itu-t(2) country(16) sa(682) sa-organizations(1) government-organizations(101) ncdc(5000)}

The OID was issued to Mr. Mohammed Edan Al-Ghamdi (mghamdi@mcit.gov.sa), acting on behalf of NCDC. This information can be verified at any time by consulting the OID Information website at <http://www.oid-info.com/get/2.16.682.1.101.5000> or <http://www.oid-info.com/cgi-bin/display?oid=2.16.682.1.101.5000&submit=Tree+display>

6. Object Identifiers allocated within NCDC

This section of the document will define the OIDs that have been allocated within NCDC. To ensure that unique OIDs are allocated throughout the NCDC-SSC, it is vital that the following guidelines are followed:

- All OIDs are allocated by the single authority listed as responsible for the NCDC OID. The current contact can be found on <http://www.oid-info.com/get/2.16.682.1.101.5000>. At the time of writing this document, the current contact is Mr. Mohammed Edan Al-Ghamdi.
- OIDs must never be re-used, as this may cause unforeseen problems within applications that rely on them. Once an OID is no longer used with NCDC-SSC, it can be marked as “retired” within this document.
- All object identifiers allocated within NCDC-SSC begin with the NCDC OID **2.16.682.1.101.5000**.

The OID Hierarchy has been allocated as below:

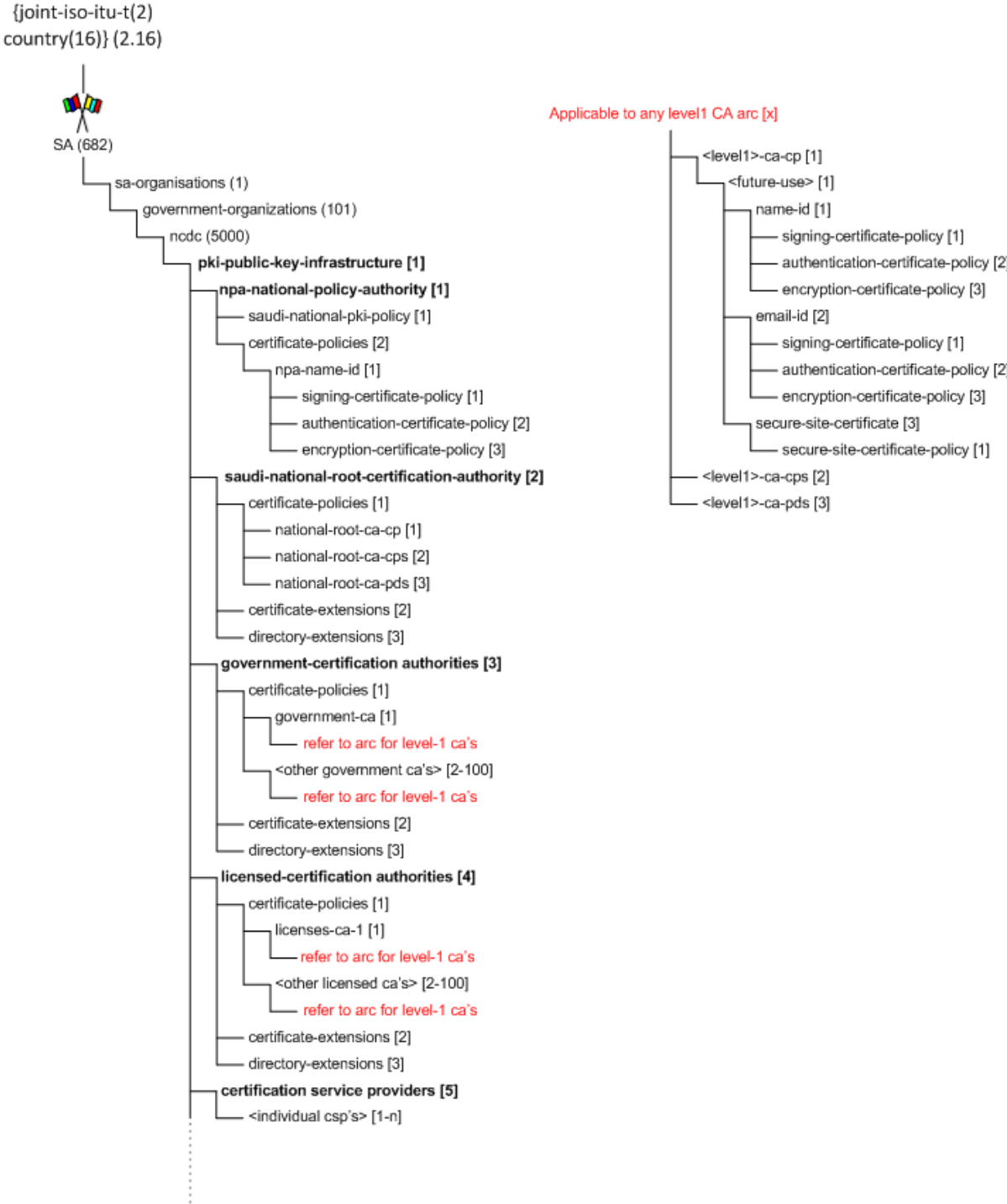


Figure1: OID Hierarchy

Node	Name	Description	OID Administrator	Current Status
2.16.682.1.101.5000.1	Public Key Infrastructure	OIDs in this part of the tree are used for the design, implementation and management of Public Key Infrastructures hosted by NCDC-SSC.	Mr. Mohammed Edan Al-Ghamdi	Valid

2.16.682.1.101.5000.1 Public Key Infrastructure

The OID for the Public Key Infrastructures within NCDC-SSC is 2.16.682.1.101.5000.1. Subnodes of the PKI are allocated as follows:

Node	Name	Description	OID Administrator	Current Status
2.16.682.1.101.5000.1.1	National Policy Authority	OIDs in this part of the tree are used by the National Policy Authority for publishing the relevant documentation	Mr. Mohammed Edan Al-Ghamdi	Valid
2.16.682.1.101.5000.1.2	Saudi National Root CA	OIDs in this part of the tree are used by the Saudi National Root CA	Mr. Mohammed Edan Al-Ghamdi	Valid
2.16.682.1.101.5000.1.3	Government Certification Authorities	OIDs in this part of the tree are used by the Government CAs	Mr. Mohammed Edan Al-Ghamdi	Valid
2.16.682.1.101.5000.1.4	Licensed Certification Authorities	OIDs in this part of the tree are used by the Licensed CAs	Mr. Mohammed Edan Al-Ghamdi	Valid
2.16.682.1.101.5000.1.5	Certification Service providers	OIDs in this part of the tree are used for the CSPs	Mr. Mohammed Edan Al-Ghamdi	Valid

2.16.682.1.101.5000.1.1 National Policy Authority

The OID for the National Policy Authority within NCDC-SSC is 2.16.682.1.101.5000.1.1. Subnodes of the NPA are shown below:

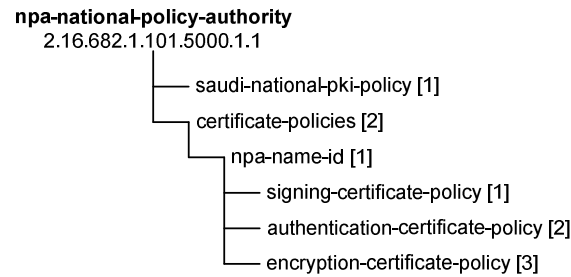


Figure2: NPA OID Structure

Name	OID	Description	OID Administrator	Current Status
Saudi National PKI Policy	2.16.682.1.101.5000.1.1.1	This OID has been assigned to the Saudi National PKI Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Certificate Policies	2.16.682.1.101.5000.1.1.2	OID that uniquely identifies the Certificate Policies applicable to the NPA	Mr. Mohammed Edan Al-Ghamdi	Valid
NPA Name ID	2.16.682.1.101.5000.1.1.2.1	OID that uniquely identifies the Certificate Policies applicable to the NPA Certificate type Name ID	Mr. Mohammed Edan Al-Ghamdi	Valid
Signing Certificate Policy	2.16.682.1.101.5000.1.1.2.1.1	OID identifying NPA Name ID – Signing Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Authentication Certificate Policy	2.16.682.1.101.5000.1.1.2.1.2	OID identifying NPA Name ID – Authentication Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Encryption Certificate Policy	2.16.682.1.101.5000.1.1.2.1.3	OID identifying NPA Name ID – Encryption Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid

2.16.682.1.101.5000.1.2 Saudi National Root CA

The OID for the Saudi National Root CA within NCDC-SSC is 2.16.682.1.101.5000.1.2. Subnodes of the Saudi National Root CA are shown below:

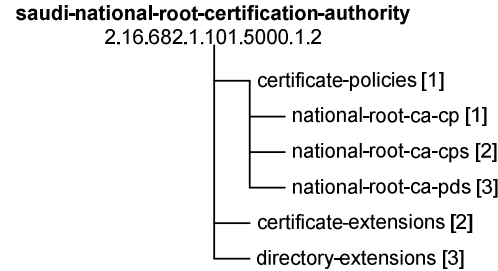


Figure3: Saudi National Root CA OID Structure

Name	OID	Description	OID Administrator	Current Status
Certificate Policies	2.16.682.1.101.5000.1.2.1	OID that uniquely identifies the Certificate Policies applicable to the Saudi NRCA	Mr. Mohammed Edan Al-Ghamdi	Valid
National Root CA CP	2.16.682.1.101.5000.1.2.1.1	OID that uniquely identifies the Saudi NRCA - CP Document	Mr. Mohammed Edan Al-Ghamdi	Valid
National Root CA CPS	2.16.682.1.101.5000.1.2.1.2	OID that uniquely identifies the Saudi NRCA - CPS Document	Mr. Mohammed Edan Al-Ghamdi	Valid
National Root CA PDS	2.16.682.1.101.5000.1.2.1.3	OID that uniquely identifies the Saudi NRCA - PDS Document	Mr. Mohammed Edan Al-Ghamdi	Valid
Certificate Extensions	2.16.682.1.101.5000.1.2.2	OID Arc formed for future assignment of custom certificate extensions for the Saudi NRCA	Mr. Mohammed Edan Al-Ghamdi	Valid
Directory Extensions	2.16.682.1.101.5000.1.2.3	OID Arc formed for future assignment of custom directory extensions for the Saudi NRCA	Mr. Mohammed Edan Al-Ghamdi	Valid

2.16.682.1.101.5000.1.3 Government Certification Authorities

The OID Arc for the Government Certification Authorities within NCDC-SSC is 2.16.682.1.101.5000.1.3. Subnodes of the Government Certification Authorities are shown below:

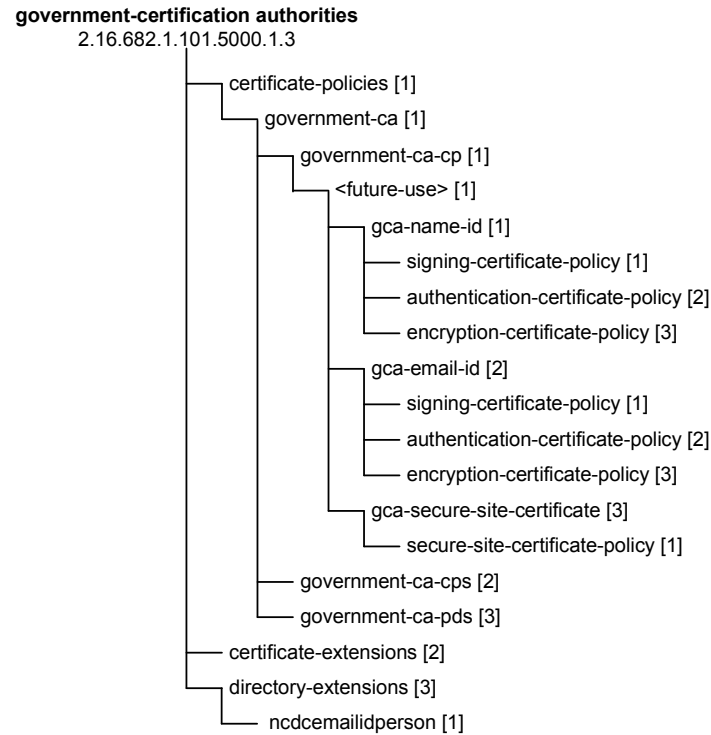


Figure4: Government CAs OID Structure

Name	OID	Description	OID Administrator	Current Status
Certificate Policies	2.16.682.1.101.5000.1.3.1	OID that uniquely identifies the Certificate Policies arc applicable to the Government CAs	Mr. Mohammed Edan Al-Ghamdi	Valid
Government CA	2.16.682.1.101.5000.1.3.1.1	OID that uniquely identifies the NCDC Government CA	Mr. Mohammed Edan Al-Ghamdi	Valid
Government CA CP	2.16.682.1.101.5000.1.3.1.1.1	OID that uniquely identifies the NCDC Government CA - CP Document	Mr. Mohammed Edan Al-Ghamdi	Valid
<future-use>	2.16.682.1.101.5000.1.3.1.1.1.1	Reserved for Future Use	Mr. Mohammed Edan Al-Ghamdi	Valid
Name ID	2.16.682.1.101.5000.1.3.1.1.1.1.1	OID that uniquely identifies the Certificate Policies applicable to the Government CA Certificate type Name ID	Mr. Mohammed Edan Al-Ghamdi	Valid
Signing Certificate Policy	2.16.682.1.101.5000.1.3.1.1.1.1.1.1	OID identifying Government CA Name ID – Signing Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Authentication Certificate Policy	2.16.682.1.101.5000.1.3.1.1.1.1.1.2	OID identifying Government CA Name ID – Authentication Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Encryption Certificate Policy	2.16.682.1.101.5000.1.3.1.1.1.1.1.3	OID identifying Government CA Name ID – Encryption Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Email ID	2.16.682.1.101.5000.1.3.1.1.1.1.2	OID that uniquely identifies the Certificate Policies applicable to the Government CA Certificate type Email ID	Mr. Mohammed Edan Al-Ghamdi	Valid
Signing Certificate Policy	2.16.682.1.101.5000.1.3.1.1.1.1.2.1	OID identifying Government CA Email ID – Signing Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid

Name	OID	Description	OID Administrator	Current Status
Authentication Certificate Policy	2.16.682.1.101.5000.1.3.1.1.1.1.2.2	OID identifying Government CA Email ID – Authentication Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Encryption Certificate Policy	2.16.682.1.101.5000.1.3.1.1.1.1.2.3	OID identifying Government CA Email ID – Encryption Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Secure Site Certificate	2.16.682.1.101.5000.1.3.1.1.1.1.3	OID that uniquely identifies the Certificate Policies applicable to the Government CA Certificate type – Secure Site Certificate	Mr. Mohammed Edan Al-Ghamdi	Valid
Secure Site Certificate Policy	2.16.682.1.101.5000.1.3.1.1.1.1.3.1	OID identifying Government CA Secure Site Certificate Policy	Mr. Mohammed Edan Al-Ghamdi	Valid
Government CA CPS	2.16.682.1.101.5000.1.3.1.1.2	OID that uniquely identifies the NCDC Government CA - CPS Document	Mr. Mohammed Edan Al-Ghamdi	Valid
Government CA PDS	2.16.682.1.101.5000.1.3.1.1.3	OID that uniquely identifies the NCDC Government CA - PDS Document	Mr. Mohammed Edan Al-Ghamdi	Valid
Certificate Extensions	2.16.682.1.101.5000.1.3.2	OID Arc formed for future assignment of custom certificate extensions for the Government Certification Authorities	Mr. Mohammed Edan Al-Ghamdi	Valid
Directory Extensions	2.16.682.1.101.5000.1.3.3	OID Arc formed for future assignment of custom directory extensions for the Government Certification Authorities	Mr. Mohammed Edan Al-Ghamdi	Valid
ncdcemailidperson	2.16.682.1.101.5000.1.3.3.1	OID that uniquely identifies NCDC Email ID Person object class	Mr. Mohammed Edan Al-Ghamdi	Valid

Notes:

1. Current NCDC Government CA has been assigned the OID {2.16.682.1.101.5000.1.3.1.1}. All future government CAs should be assigned OIDs from {2.16.682.1.101.5000.1.3.1.2} - {2.16.682.1.101.5000.1.3.1.100}
2. Every level 1 CA, under the Saudi NRCA should maintain the basic structure shown in [Appendix A](#)

2.16.682.1.101.5000.1.4 Licensed Certification Authorities

The OID Arc for the Licensed Certification Authorities within NCDC-SSC is 2.16.682.1.101.5000.1.4.

No licensed CAs have been established at the time of writing this document.

Structure shown for licensed CAs in [Figure 1](#) should be observed.

Notes:

1. Licensed CAs should be assigned the OIDs from {2.16.682.1.101.5000.1.4.1.1} - {2.16.682.1.101.5000.1.4.1.100}
2. Every level 1 CA, under the Saudi NRCA should maintain the basic structure shown in [Appendix A](#)

2.16.682.1.101.5000.1.5 Certificate Service Providers

The OID Arc for the Saudi PKI Certificate Service Providers is 2.16.682.1.101.5000.1.5.

No CSPs have been established at the time of writing this document.

Structure for CSPs is shown in [Figure 1](#)

Saudi PKI Certificate Service Providers should be assigned OIDs from {2.16.682.1.101.5000.1.5.1.1} - {2.16.682.1.101.5000.1.5.1.<n>}

7. Appendix A

All future Government CAs should be assigned OIDs from {2.16.682.1.101.5000.1.3.1.2} - {2.16.682.1.101.5000.1.3.1.100}

All future Licensed CAs should be assigned OIDs from {2.16.682.1.101.5000.1.4.1.1} - {2.16.682.1.101.5000.1.4.1.100}

Each level 1 CA Arc should follow the basic minimum structure shown below:

Applicable to any level1 CA arc [x]

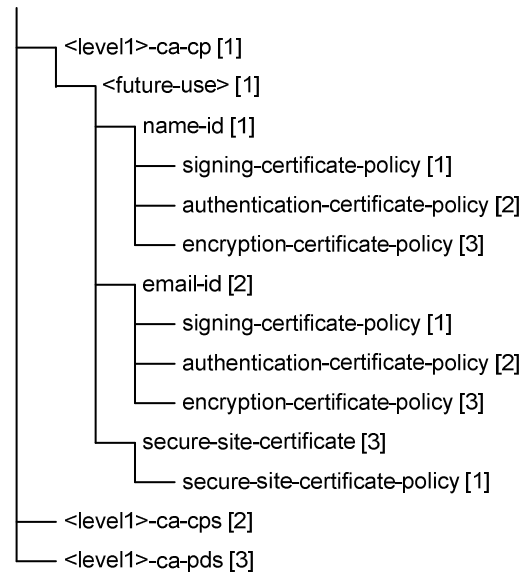


Figure5: Level1 CAs basic minimum OID Structure

For reference and understanding, please refer to the [Government Certification Authorities](#) section, where Government CA has been assigned the basic minimum structure as shown above.