



Actalis Object Identifiers (OIDs)

Author:	Riccardo Minet Actalis S.p.A.	_____	_____
			Data
Verified by:	Egidio Casati Actalis S.p.A.	_____	_____
			Data
	Fulvio Parisi Actalis S.p.A.	_____	_____
			Data
Approved by:	Adriano Santoni Actalis S.p.A.	_____	_____
			Data
		_____	_____
			Data
Document code:	013OID	- 2008	- 1 - 08
	<i>Project/Service</i>	<i>Year</i>	<i>Doc N.</i> <i>Version</i>
Distribution class:	PUBLIC		

HISTORY OF MODIFICATIONS

From release 1 to release 2	
Par. 4	Added policies for GTA Schema Trust Authority (STA) Policy
From release 2 to release 3	
Par. 4	Added C-Travel certificate policy
From release 3 to release 4	
Par. 4	Added Authentication certificate policy (CNS)
From release 4 to release 5	
Par. 3	Added Outsourced CA Certificate Policy Arc
Par. 4	Added CRS-SISS Project Outsourced CA Certificates Policy
From release 5 to release 6	
Par. 4	Added MHP Signing Certificates Policy
From release 6 to release 7	
Par. 3	Added LDAP ObjectClass identifiers
From release 7 to release 8	
Par. 3	Added Time-Stamps functional arc
Par. 4	Added Actalis Time-Stamps Policy

INDEX

1. SCOPE OF THIS DOCUMENT	3
1.1 Normative References	3
1.2 Definitions	3
2. PUBLIC ARC	4
3. FUNCTIONAL ARCS	5
3.1 OID Assignment Rules	5
3.1.1 Actalis Certificate Policy OIDs	5
3.1.2 Actalis Certificate Extension OIDs	5
3.1.3 Actalis Protocols	5
3.1.4 Actalis Extended Key Usages (EKU)	6
3.1.5 Outsourced CA Certificate Policy OIDs	6
3.1.6 LDAP ObjectClass identifiers.....	6
3.1.7 Actalis Time-Stamps Policy OIDs	7
4. CURRENTLY ASSIGNED OIDS	7
5. ADMINISTRATION	8

1. SCOPE OF THIS DOCUMENT

Object identifiers (OIDs) are globally unique identifiers used in a number of data objects and protocols including X.509 certificates, Internet protocols, directories, etc.

Actalis uses a number of OIDs to ensure uniqueness and provide identity. This document provides the policy on how these OIDs shall be allocated.

1.1 Normative References

- [1] ITU-T Rec. X.680 - X.693 (07/02) "Abstract Notation One (ASN.1)"
- [2] RFC 1778 "The String Representation of Standard Attribute Syntaxes" IETF, March 1995
- [3] RFC 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" IETF, March 1999
- [4] ANS X9.79-1:2001 "Public Key Infrastructure - Practice and Policy Framework" January 2001

1.2 Definitions

Certificate Policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

2. PUBLIC ARC

The Actalis OID schema is divided into two parts:



Actalis has obtained its public OID from British Standard Institutions according with ISO 6523
The public arc is split up as follows:

- A:* ISO (International Standards Organization) code: (1)
- B:* ISO Identified Organization: (3)
- C:* Actalis identifier: (159)

Therefore Actalis' public arc is:

1.3.159

3. FUNCTIONAL ARCS

In order to manage the private arc, functional arcs shall be assigned under the public arc with individual values for functional arcs.

Currently assigned functional arcs are:

- Actalis Certificate Policies (CPs)
- X.509 Private Certificate Extensions
- Actalis Specific Protocols
- Actalis Specific Extended Key Usages
- Outsourced CA Certificate Policies (CPs)

3.1 OID Assignment Rules

All objects within the structure will be numbered according to the rules in this section. Private arcs shall only be used in conjunction with the authorized Actalis public arc above.

3.1.1 Actalis Certificate Policy OIDs

CP OIDs shall have the following format:

Public Arc (1.3.159)	Private Arc (1.Y.Z)
-----------------------------	----------------------------

Where:

- Y: is a Certificate Policy number is allocated by the PAA
- Z: is a Certificate Policy Version No

3.1.2 Actalis Certificate Extension OIDs

Certificate Extension OIDs shall have the following format:

Public Arc (1.3.159)	Private Arc (2.Y.Z)
-----------------------------	----------------------------

Where:

- Y: Is a Private Extension Type (Pilot=1, Production=2, Test=3)
- Z: Is a Private Extension ID allocated by the PAA

3.1.3 Actalis Protocols

Actalis proprietary protocols shall be assigned OIDs according to the format below:

Public Arc (1.3.159)	Private Arc (4.Y)
-----------------------------	--------------------------

Where:

Y: is a unique protocol number allocated by Actalis

3.1.4 Actalis Extended Key Usages (EKU)

Actalis proprietary EKUs shall be assigned OIDs according to the format below:

Public Arc (1.3.159)	Private Arc (5.Y)
-----------------------------	--------------------------

Where:

Y: is a unique EKU number allocated by Actalis

3.1.5 Outsourced CA Certificate Policy OIDs

CP OIDs shall have the following format:

Public Arc (1.3.159)	Private Arc (6.W.X.Y.Z)
-----------------------------	--------------------------------

Where:

W: is a unique number allocated by Actalis that identify the outsourced CA
X, Y, Z: are numbers defined in accordance with the outsourced CA's Policy schema

3.1.6 LDAP ObjectClass identifiers

Actalis proprietary ObjectClass shall be assigned OIDs according to the format below:

Public Arc (1.3.159)	Private Arc (7.W.X.Y.Z)
-----------------------------	--------------------------------

Where:

W: is a unique number allocated by Actalis that identify the ObjectClass identifier
X, Y, Z: are numbers defined in accordance with the outsourced CA's Policy schema

3.1.7 Actalis Time-Stamps Policy OIDs

Time-Stamps Policy OIDs shall have the following format:

Public Arc (1.3.159)	Private Arc (8.Y.Z)
----------------------	---------------------

Where:

- Y: is a Policy number is allocated by the PAA
- Z: is a Policy Version No

4. CURRENTLY ASSIGNED OIDS

- 1.3.159.1.1.1 Actalis Certification Authority - Qualified Certificates Policy - Version 1
- 1.3.159.1.2.1 Actalis Certification Authority - Root Authority Certificates Policy -Version 1
- 1.3.159.1.3.1 Actalis Certification Authority - Class A Certificates Policy - Version 1
- 1.3.159.1.4.1 Actalis Certification Authority - Server Authentication Certificates Policy - Version 1
- 1.3.159.1.5.1 Actalis Certification Authority - Qualified Certificates with usage limitations Policy - Version 1
- 1.3.159.1.6.1 Actalis TimeStamping Authority - Root Certificate Policy - Version 1
- 1.3.159.1.8.1 Actalis GTA Schema Trust Authority (STA) Policy - Version 1
- 1.3.159.1.9.1 Actalis Certification Authority - C-Travel Certificates Policy - Version 1
- 1.3.159.1.10.1 Actalis Certification Authority - Authentication Certificates Policy - Version 1
- 1.3.159.1.11.1 Actalis Certification Authority - Client Authentication Certificates Policy - Version 1
- 1.3.159.1.12.1 Actalis Certification Authority - OCSP Validation Certificates Policy - Version 1
- 1.3.159.1.13.1 Actalis Certification Authority - Authentication Certificates Policy – Fiscal Code Verification - Version 1
- 1.3.159.1.14.1 Actalis Certification Authority – MHP signing certificates - Version 1
- 1.3.159.6.1.* CNS-Regione Lombardia - Authentication Certificates Policies
- 1.3.159.6.2.1 CNS-Regione Friuli - Authentication Certificates Policy – Version 1
- 1.3.159.8.1.1 Actalis Time-Stamps Policy – Version 1

5. ADMINISTRATION

For comments o requests please contact:

Riccardo Minet
ACTALIS S.p.A.
Via T.Taramelli, 26
20124 - Milano
ITALY

e-mail: riccardo.minet@actalis.it