Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Platform Services – Trust Backend
Swiss Government PKI

SecOff,14.11.2023

Swiss Government PKI

Object Identifiers (OID)

Projektname

Projektnummer

Version **4.45**

Status	in Arbeit	in Prüfung	genehmigt zur Nutzung
	☐	☐	☑

Beteiligter Personenkreis	
Autoren:	J. Weber, Hans W. Kramer, C. Enke
Genehmigung:	PKI Management Board
Benützer/Anwender:	PKI
zur Information/Kenntnis:	SecOff PKI

Änderungskontrolle, Prüfung, Genehmigung			
Version	**Wann**	**Wer**	**Beschreibung**
v1.0	18.01.2006	Ramon Keller, Softlab	OIDs aus den Dokumenten zusammengetragen
v1.1	19.01.2006	Johann Wiss, BIT	ePass OIDs ergänzt
v1.3	31.03.2006	Ramon Keller, Softlab	OID für Digitalen Tachographen bei AdminCA-CD-T ergänzt
v1.4	03.04.2006	Johann Wiss, BIT	OIDs für KlasseC-Enterprise
V1.5	11.04.2006	Ramon Keller, Softlab	OID für SSL Organizational Client Policy der AdminCA-CD-T ergänzt
V1.6	03.05.2006	Marcel Suter, Softlab	OID der AdminCA-A-T01 ergänzt
V1.7	11.08.2006	Marcel Suter, Softlab	OID der AdminCA-A-T01 TSA ergänzt
V1.8	22.01.2007	Ramon Keller, Softlab	OID für Klasse C Office Automation Policy der AdminCA-CD-T01 reserviert.
V1.9	23.2.2007	Ramon Keller, Softlab	OID für Klasse C Domain Controller Policy der AdminCA-CD-T01 reserviert.
V1.10	29.8.2007	Ramon Keller, Softlab	OIDs für AgencyIdentifier Extension (AmtsID) in Organisations-zertifikaten und OID für sedex organisational Client Policy der AdminCA-CD-T01 reserviert.
V1.11	25.01.2008	Marcel Suter, Cirquent	OIDs Gruppenmailboxen der AdminCA-CD-T01 reserviert.
V1.12	04.02.2008	Ramon Keller, Cirquent	Policy OIDs der vAdminCA-CD-T01 ergänzt
V1.13	04.06.2009	Ramon Keller, Cirquent	Policy OIDs und Extension OIDs für eDoc Systemplattform re-serviert
V1.14	05.01.2010	HW Kramer, BIT	Policy OIDs und Extension OIDs für MRTD 10 reserviert
V1.15	21.09.2010	Marcel Suter	Policy OIDs und Extension OIDs für BP Reserviert
V1.16	21.09.2010	Marcel Suter	Policy OIDs für Protocol
V1.17	27.06.2011	Antonio Alessio	Policy OID für SPOC reserviert
V1.18	23.04.2012	Marcel Suter	Policy OID für Enhanced CA 02
V1.19	26.04.2012	Jürgen Weber, BIT	Policy OID für aRegular CA 01 (Acceptance)
V1.20	30.04.2012	Jürgen Weber, BIT	OIDs für ZKV LDAP Attribute Types

V1.21	22.05.2012	Jürgen Weber, BIT	Policy OID für Regular CA 01 (Production)
V1.2	24.09.2012	Marcel Suter, BIT	Policy OID für EnterpriseCC
V1.23	27.03.2013	Marcel Suter, BIT	Policy OID für Authentication Klasse B MobileID
V1.24	11.10.2013	Pascal Joye, BIT	Policy OID für LRA Station (ab Windows 7 System)
V1.25	20.03.2014	SuMa, BIT	Policy OID ZKV
V1.26	14.04.2014	SuMa, BIT	Policy OID SEDEX
V1.27	14.04.2014	SuMa, BIT	Updated Web SSL OID and removed unused sections
V1.28	18.08.2014	Jürgen Weber, BIT	Added SSL Web client policy Added SSL Web server/client policy
V2.0	18.08.2014	Jürgen Weber, BIT	Updated CI
V2.2	19.09.2014	Jürgen Weber, BIT	Policy OID für RAaaS Server Policy OID für RaaaS Client
V2.3	11.12.2014	Jürgen Weber, BIT	Added OID Client Auth (no public trust)
V2.4	27.01.2014	Jürgen Weber, BIT	Added EV SSL policies
V2.5	04.02.2015	Jürgen Weber, BIT	Added Process-Authentication EJPD SSO Portal
V2.6	01.04.2015	Pascal Joye, BIT	Added Standard C-Class Products
V2.7	11.05.2015	Marcel Suter	Added End user CP OIDs for Enhanced CA 02 (Auth/Cipher/Dsig) different from Enhanced CA 01
V2.8	12.05.2015	Robert Dietschi	Added DFS OIDs for Acceptance & Development
V2.9	21.05.2015	Marcel Suter	Added OID Card Printer, BKI
V3.0	19.06.2015	Hans W. Kramer	Added OID Person Authentication/Signature, Person Authentication/Signature/Encryption, Person Signature/Encryption
V3.1	19.06.2015	Hans W. Kramer	Added OID Organization Authentication/Signature, Organization Authentication/Signature/Encryption, Organization Signature/Encryption
V3.2	19.06.2015	Hans W. Kramer	Added OID System Authentication, System Authentication/Signature, System Authentication/Signature/Encryption, System Signature/Encryption
V3.3	15.07.2015	Hans W. Kramer	Added OID Elcom MATCH Client Authentication/Signature

V3.4	10.11.2015	Antonio Alessio	Added OID Organization Signature
V3.5	26.11.2015	Jürgen Weber	Added OID System Signature
V.3.6	08.12.2015	Jürgen Weber	Added EJPD – eSchKG Verbund Added Class C – System Encryption Added SSL CA 01 – Domain Controller
V.3.7	18.02.2016	Alessio Antonio	Added Governikus Core Signature Certificate Added Governikus OSCI Transport Encryption Certificate Added Governikus OSCI Transport Signature Certificate Added Governikus Core Timestamp Certificate
V3.8	29.03.2016	Jürgen Weber	Added Swiss Government Root CA III Added Swiss Government Public Trust Standard CA 02 Added EE CP issued by SG Public Trust Standard CA 02
V3.9	04.04.2016	Jürgen Weber	Added Swiss Government Public Trust EV CA 02 Added EE CP issued by SG Public Trust EV CA 02
V4.0	29.04.2016	Pascal Joye	Added 2 x Code Signing
V4.1	04.05.2016	Jürgen Weber	Added Code Signing OCSP Responder policies
V4.2	22.07.2016	Beatrice Metaj	Added OID Class B Prestaged Authentication Only Added OIDs for OCSP Responder on issuing CAs - SG QualifiedCA01 - SG EnhancedCA01 - SG EnhancedCA02 - SG RegularCA01 - SG SSLCA01
V4.3	28.09.2016	Beatrice Metaj	Added OID for Groupmailbox Certificates only Sign/Enc
V4.4	02.11.2016	Jürgen Weber	Added OID for SG Root CA III OCSP Responder policy
V4.5	09.01.2017	Beatrice Metaj	Added OID for Personal Cert. Authentication Only on Enhanced CA01 (non-prestaged)
V4.6	18.01.2017	Beatrice Metaj	Added OIDs for Class B prestaged on SG Enhanced CA 01 Added OID Prestaged Authentication only on Enhanced CA 01
V4.7	19.04.2017	Beatrice Metaj	Added OID for Class A Signature on Qualified CA01 with ZertEs 2017 adaptation

			Added OID for Electronic Seal on Regulated CA01 Added OID for Class A Signature on Regulated CA01 with Zer-tEs 2017 adaptation
V4.8	17.07.2017	Beatrice Metaj	Added OID for Added Swiss Government Public Trust Standard CA 02 Browser Compatible
V4.9	02.08.2017	Antonio Alessio	Added OID for Swiss Government Public Trust Standard CA 02 Root-signed by QuoVadis
V4.10	23.08.2017	Jürgen Weber	Public Trust Standard Browser Compatible Server/Client Authentication SAN
V4.11	19.08.2017	Beatrice Metaj	Public Trust Standard Browser Compatible Server/Client Authentication SAN >2048KB
V4.12	3.10.2017	KH	Added Swiss Government Public Trust Standard CA 03
V4.13	10.10.2017	KH	Added EE CP issued by SG Public Trust Standard CA 03 Server Authentication
V4.14	10.10.2017	KH	Added Public Trust Standard CA03 OCSP Responder Signing
V4.15	02.11.2017	Beatrice Metaj	Added Armasuisse Policy for noManApp TEPLAS
V4.16	26.07.2018	Beatrice Metaj	Added OID for CP/CPS Smart Tachographs NG Kap. 1.11
V4.17	25.09.2018	Beatrice Metaj	Added new Root IV: • OID for Swiss Government Root CA IV – Top level Kap. 1.2 and CPS OID Kap. 1.3 • OID for OCSP Responder Signing Kap. 1.7 • OID for Swiss Government Regulated CA01 Kap 1.7
V4.18	31.10.2018	Cornelia Enke	Added new OCSP Responder CP for: 2.48 OCSP-Responder-RootCAI 22.64 OCSP-Responder-RootCAII 62.18 OCSP-Responder PTSTCA02BC
V4.19	13.02.2019	Cornelia Enke	Korrigiert von 22.64 zu 22.65 OCSP-Responder-RootCAII
V4.20	12.03.2019	Cornelia Enke	Regulated CA02 ergänzt
V4.21	13.03.2019	Antonio Alessio	Authentication Enhanced CA 02 prestaged LRAO

V4.22	20.03.2019	Cornelia Enke	Korrektur unter 1.7 – Ausstellung der Blattzertifikate unter Regulated CA02
V4.23	01.07.2019	Jürgen Weber	Added: 22.66 – EESSI Digital Signature Certificate
V4.24	02.09.2019	Jürgen Weber	Added: 3.2.50: Authentication only Enhanced CA 02 (pre-staged)
V4.25	18.12.2019	Cornelia Enke	Added: ClassC PersonSign (22.67) ClassC PersonEnc (22.68)
V4.26	20.01.2020	Jürgen Weber	Added: 2.51 - SCMS Bund Auth EnhancedCA02 Added: 2.52 - SCMS Bund Enc EnhancedCA02 Added: 2.53 - SCMS Bund DSig EnhancedCA02 Added: 2.54 - SCMS Bund Auth only EnhancedCA02 Added: 2.55 - SCMS Bund Auth 90-Days EnhancedCA02 Added: 2.66 - **--- NOT IN USE --- (gesperrt für EESSI)**
V4.27	12.02.2020	Cornelia Enke	Addded: FreeDN Policy für Klasse A
V4.28	25.03.2020	Jürgen Weber	Added: EETS-B2B Authentication
V4.29	27.03.2020	Cornelia Enke	Added: FUB Zusatzkarte Auh. Only (2.16.756.1.17.3.2.67)
V4.30	05.08.2020	Cornelia Enke	OIDs auf die keine Zertifikate mehr ausgestellt werden sind ~~durchgestrichen~~ dargestellt. Dekommissionierung Qualified CA01
V4.31	28.10.2020	Cornelia Enke	Neuausstellung von issuing CAs im Rahmen Lifecycle • Enhanced CA03 • Enhanced CA04 • Enhanced CA05 • Regular CA 02

			• Regulated CA03
V4.32	2.11.2020	Hans Kramer	Added BIT TLS Inspection CA 1
V4.33	03.11.2020	Cornelia Enke	Added “geregeltes Behördenzertifikat – neu”
V4.34	20.01.2020	Cornelia Enke	Added: • OCSP Responder Enhanced CA03 • OCSP Responder Enhanced CA04 • OCSP Responder Enhanced CA05 • OCSP Responder Regular CA02 • OCSP Responder Regulated CA03 Decomissioning: • PTSTCA02 • PTSTCA03 • PTCSSTCA02
V4.35	10.05.2021	Cornelia Enke	Added: GGG Policy OID unter RootCAIV
V4.36	02.08.2021	Cornelia Enke	Added Polivy OID für Klasse C Organisationszertifikat unter RegularCA02
V4.37	22.10.2021	Hans Kramer	End Entity Policy OID for Regular CA02
V4.38	03.03.2022	Cornelia Enke	End Entity Policy OID for Electronic Seal on Regulated CA03 (qcp-l-H)
V4.39	27.04.2022	Cornelia Enke	End Entity Policies für RegulatedCA03 ergänzt
V4.40	15.06.2022	Pascal Joye	Update Document Header (Platform Services – Trust Backend)
V4.41	30.06.2022	Mario Lovisi	Add Entry Policy OID for ZKV (Zollkundenverwaltung)
V.4.42	23.1.2023	Hans Kramer	Modified {id-adminpki}.2.10, {id-adminpki}.2.11, {id-adminpki}.2.15 to match issued certificates.
V 4.43	31.1.2023	Hans Kramer	Modified {id-adminpki}.5.2.13 to match issued certificates and standards.
V 4.44	17.2.2023	Hans Kramer	Removed document classification, based on discussion with PO TRB.

V4.45	14.11.23	Cornelia Enke	Review and cleanup for RegularCA02 policies

Inhaltsverzeichnis

1 Object Identifiers

1.1 Swiss Government PKI Top OID

Für das Projekt Swiss Government PKI (SG PKI) ist folgender OID als Top definiert:

2.16.756.1.17.3

Dieser OID wird im Folgenden mit {`id-adminpki`} substituiert.

1.2 Subsidiäre Identifier

Tabelle 1: Toplevel' OIDs

Object Identifier	Certification Authority	Verwendung
{id-adminpki}.1.x	SG Root CA I	Certificate Practise Statements (CPSs) of Swiss Government Root CA I (Produktion) Obsoletes AdminCA-AB-Txx
{id-adminpki}.2.x	SG Sub CA	Certificate Policies (CPs)
{id-adminpki}.3.x	SG Sub CA	Certificate Extensions
{id-adminpki}.11.x	SG aRoot CA I	Certificate Practise Statements (CPSs) of Swiss Government Root aCA I (Abnahme) Obsoletes VAdminCA-AB-Txx
{id-adminpki}.12.x	SG Sub aCA	Certificate Policies (CPs)
{id-adminpki}.13.x	SG Sub aCA	Certificate Extensions
{id-adminpki}.21.x	AdminCA-CD-Txx	Certificate Practise Statements (CPSs)
{id-adminpki}.22.x	AdminCA-CD-Txx	Certificate Policies (CPs)
{id-adminpki}.23.x	AdminCA-CD-Txx	Certificate Extensions

Object Identifier	Certification Authority	Verwendung
{id-adminpki}.31.x	VAdminCA-CD-Txx	Certificate Practise Statements (CPSs)
{id-adminpki}.32.x	VAdminCA-CD-Txx	Certificate Policies (CPs)
{id-adminpki}.33.x	VAdminCA-CD-Txx	Certificate Extensions
{id-adminpki}.41.x	AdminCA-CD-Exx	Certificate Practise Statements (CPSs)
{id-adminpki}.42.x	AdminCA-CD-Exx	Certificate Policies (CPs)
{id-adminpki}.43.x	AdminCA-CD-Exx	Certificate Extensions
{id-adminpki}.51.x	VAdminCA-CD-Exx	Certificate Practise Statements (CPSs)
{id-adminpki}.52.x	VAdminCA-CD-Exx	Certificate Policies (CPs)
{id-adminpki}.53.x	VAdminCA-CD-Exx	Certificate Extensions
{id-adminpki}.61.x	SG Root CA III	Certificate Practise Statements (CPSs)
{id-adminpki}.62.x	SG Root CA III	Certificate Policies (CPs)
{id-adminpki}.63.x	SG Root CA III	Certificate Extensions
{id-adminpki}.5.x	SG Root CA IV	Certificate Practise Statements (CPSs) of Swiss Government Root CA IV (Produktion)

1.3 SG Root CA's

Tabelle 2: SG Sub CA's OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.1.0	CPS	SG Root CA I Obsoletes: Admin-Root-CA
{id-adminpki}.21.0	*CPS*	*Admin-CA-Class2 - OBSOLETE -*
{id-adminpki}.21.1	CPS	SG Root CA II Obsoletes: AdminCA-CD-T01
{id-adminpki}.61.0	CPS	SG Root CA III
{id-adminpki}.5.0	CPS	SG Root CA IV CPS

1.4 SG Root CA I Sub CA's

Tabelle 3: SG Root CA I Sub CA's OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.1.1	*CPS*	*Admin-CA1 - OBSOLETE -*
{id-adminpki}.1.2	*CPS*	*Admin-CA2 - OBSOLETE -*
{id-adminpki}.1.3	CPS	SG Enhanced CA 01 Obsoletes: Admin-CA3
{id-adminpki}.1.4	CPS	~~SG Qualified CA 01~~ ~~Obsoletes: AdminCA-A-T01~~ *Dekommissioniert am 24.06.2020*
{id-adminpki}.1.5	CP	SG Enhanced CA 02
{id-adminpki}.1.6	CP	SG Enhanced CA 03
{id-adminpki}.1.7	CP	SG Enhanced CA 04
{id-adminpki}.1.8	CP	SG Enhanced CA 05
{id-adminpki}.2.0	CP	Test

Object Identifier	Typ	Verwendung
{id-adminpki}.2.1	CP	Encryption
{id-adminpki}.2.2	CP	Signing
{id-adminpki}.2.3	CP	Authentication / WebRAO
{id-adminpki}.2.4	CP	System
{id-adminpki}.2.5	CP	Authentication (file)
{id-adminpki}.2.6	CP	System (file)
{id-adminpki}.2.7	CP	WebRAO (fixed-end)
{id-adminpki}.2.8	CP	WebserverCertAdmin
{id-adminpki}.2.9	CP	System client auth
{id-adminpki}.2.10	CP	~~Encryption (Admin-CA3)~~ Encryption EnhancedCA01 or EnhancedCA02
{id-adminpki}.2.11	CP	~~Signing (Admin-CA3)~~ Digital Signature EnhancedCA01 or EnhancedCA02
~~{id-adminpki}.2.12~~	~~CP~~	~~Authentication (Admin-CA3)~~
~~{id-adminpki}.2.13~~	~~CP~~	~~WebRAO (Admin-CA3)~~
~~{id-adminpki}.2.14~~	~~CP~~	~~WebserverCertAdmin (Admin-CA3)~~
{id-adminpki}.2.15	CP	~~Authentication (Admin-CA3 ohne UPN)~~ Authentication EnhancedCA01 or EnhancedCA02
~~{id-adminpki}.2.16~~	~~CP~~	~~LRA Officer AdminCA-A-T01~~
~~{id-adminpki}.2.17~~	~~CP~~	~~EE Qualified Digital Signature~~
~~{id-adminpki}.2.17.1~~	~~CP~~	~~EE Qualified Digital Signature FreeDN~~
~~{id-adminpki}.2.17.2~~	~~CP~~	~~EE Qualified Digital Signature PreassignedDN~~
~~{id-adminpki}.2.17.3.1~~	~~CP~~	~~EE Qualified Digital Signature PresetDN (eZivi)~~
~~{id-adminpki}.2.18~~	~~CP~~	~~TSA (AdminCA-A-T01)~~
{id-adminpki}.2.19	CP	SPOC (ePass10)
~~{id-adminpki}.2.20~~	~~CP~~	~~Authentication with MobileID~~
{id-adminpki}.2.30	CP	Authentication Enhanced CA 02 (FUB)
{id-adminpki}.2.31	CP	DSig Enhanced CA 02 (FUB)

Object Identifier	Typ	Verwendung
{id-adminpki}.2.32	CP	Cipher Enhanced CA 02 (FUB)
{id-adminpki}.2.33	CP	Authentication Enhanced CA 02
{id-adminpki}.2.34	CP	DSig Enhanced CA 02
{id-adminpki}.2.35	CP	Cipher Enhanced CA 02
{id-adminpki}.2.36	CP	Prestaged Authentication only Enhanced CA 02
~~{id-adminpki}.2.37~~	~~CP~~	~~QualifiedCA01 OCSP Responder Signing~~
{id-adminpki}.2.38	CP	EnhancedCA01 OCSP Responder Signing
{id-adminpki}.2.39	CP	EnhancedCA02 OCSP Responder Signing
{id-adminpki}.2.40	CP	Authentication only Enhanced CA 01 (non-prestaged)
{id-adminpki}.2.41	CP	Authentication Enhanced CA 01 prestaged
{id-adminpki}.2.42	CP	DSig Enhanced CA 01 prestaged
{id-adminpki}.2.43	CP	Cipher Enhanced CA 01 prestaged
{id-adminpki}.2.44	CP	Authentication only Enhanced CA 01 Prestaged
~~{id-adminpki}.2.45~~	~~CP~~	~~Qualified Signature on Qualified CA01 with new ZertEs 2017 adaptation~~
~~{id-adminpki}.2.46~~	~~CP~~	~~Electronic Seal on Regulated CA01~~
~~{id-adminpki}.2.47~~	~~CP~~	~~Qualified Signature on Regulated CA01 with new ZertEs 2017 adaptation~~
~~{id-adminpki}.2.47~~	~~CP~~	~~Qualified Signature on Regulated CA01 with new ZertEs 2017 adaptation~~
{id-adminpki}.2.48	CP	OCSP-Responder-RootCAI
{id-adminpki}.2.49	CP	Authentication Enhanced CA 02 prestaged LRAO
{id-adminpki}.2.50	CP	Authentication only Enhanced CA 02 (prestaged)
{id-adminpki}.2.51	CP	SCMS Bund Auth EnhancedCA02
{id-adminpki}.2.52	CP	SCMS Bund Enc EnhancedCA02
{id-adminpki}.2.53	CP	SCMS Bund DSig EnhancedCA02
{id-adminpki}.2.54	CP	SCMS Bund Auth only EnhancedCA02
{id-adminpki}.2.55	CP	SCMS Bund Auth 90-Days EnhancedCA02

Object Identifier	Typ	Verwendung
{id-adminpki}.2.66	CP	**(gesperrt für EESSI – Root II)**
{id-adminpki}.2.67	CP	FUB Zusatzkarten Auth only
{id-adminpki}.2.68	CP	Enhanced-CA-03- OCSP-Responder
{id-adminpki}.2.69	CP	Enhanced-CA-04-OCSP-Responder
{id-adminpki}.2.70	CP	Enhanced-CA-05-OCSP-Responder

1.5 SG Root CA II Sub CA's

Tabelle 4: SG Root CA II Sub CA's OIDs

Object Identifier			Typ	Verwendung
Production	**Acceptance**	**Reference / Development**		
{id-adminpki} : 2.16.756.1.17.3				
{id-adminpki}.21.1			CPS	Swiss Government Regular CA 01
{id-adminpki}.21.2			CPS	Swiss Government SSL CA01
~~{id-adminpki}.21.3~~			~~CPS~~	~~Swiss Government EV SSL CA01~~
{id-adminpki}.22.1			CP	SSL Client
{id-adminpki}.22.2			CP	WebRAO
{id-adminpki}.22.3			CP	WebServer
{id-adminpki}.22.4			CP	System
{id-adminpki}.22.5			CP	Codesigning
{id-adminpki}.22.6			CP	System (file)
{id-adminpki}.22.7			CP	System (E-Mail)
{id-adminpki}.22.8			CP	E-Dec
{id-adminpki}.22.9			CP	PKIEntity
{id-adminpki}.22.10			CP	AV (Anwendungsverantwortlicher)
{id-adminpki}.22.11			CP	UPI
{id-adminpki}.22.12			CP	DFS-CA Operator
{id-adminpki}.22.13			CP	DFS-CA Service Admin
{id-adminpki}.22.14			CP	DFS-CA Entity
{id-adminpki}.22.15			CP	DFS-CIA Entity

Object Identifier			Typ	Verwendung
Production	**Acceptance**	**Reference / Development**		
{id-adminpki} : 2.16.756.1.17.3				
{id-adminpki}.22.16			CP	DFS-CP Entity
{id-adminpki}.22.17			CP	SSL Organizational Client
{id-adminpki}.22.18			CP	Office Automation Client (Klasse C)
{id-adminpki}.22.19			CP	Microsoft Domain Controller (Klasse C)
{id-adminpki}.22.20			CP	Sedex Organisational Client
{id-adminpki}.22.21			CP	OSCI Infrastructure
~~{id-adminpki}.22.22~~			~~CP~~	~~Gruppenmailboxen (Sign/Enc/Auth)~~
{id-adminpki}.22.23			CP	eDoc Systemplattform
{id-adminpki}.22.24			CP	LRA Station
{id-adminpki}.22.25			CP	ZKV Anwendungen
{id-adminpki}.22.26			CP	SSL Web server authentication only
{id-adminpki}.22.27			CP	SSL Web client authentication only
{id-adminpki}.22.28			CP	SSL Web server/client authentication
{id-adminpki}.22.29			CP	RAaaS Server
{id-adminpki}.22.30			CP	RAaaS Client
{id-adminpki}.22.31			CP	Client Auth (no public trust)
{id-adminpki}.22.32			CP	EV SSL Web server authentication only
{id-adminpki}.22.33			CP	EV SSL Web client authentication only
{id-adminpki}.22.34			CP	EV SSL Web server/client authentication
{id-adminpki}.22.35			CP	Process-Authentication EJPD SSO Portal
{id-adminpki}.22.36			CP	Person Authentication
{id-adminpki}.22.37			CP	Organization Authentication
{id-adminpki}.22.38			CP	Card Printer
{id-adminpki}.22.39			CP	Bulk Key Generator

Object Identifier			Typ	Verwendung
Production	**Acceptance**	**Reference / Development**		
{id-adminpki} : 2.16.756.1.17.3				
{id-adminpki}.22.40			CP	Person Authentication/Signature
{id-adminpki}.22.41			CP	Person Authentication/Signature/Encryption
{id-adminpki}.22.42			CP	Person Signature/Encryption
{id-adminpki}.22.43			CP	Organization Authentication/Signature
{id-adminpki}.22.44			CP	Organization Authentication/Signature/Encryption
{id-adminpki}.22.45			CP	Organization Signature/Encryption
{id-adminpki}.22.46			CP	System Authentication
{id-adminpki}.22.47			CP	System Authentication/Signature
{id-adminpki}.22.48			CP	System Authentication/Signature/Encryption
{id-adminpki}.22.49			CP	System Signature/Encryption
{id-adminpki}.22.50			CP	Elcom MATCH Client Authentication/Signature
{id-adminpki}.22.51			CP	EV Codesigning
{id-adminpki}.22.52			CP	Organization Signature
{id-adminpki}.22.53			CP	System Signature
{id-adminpki}.22.54			CP	EJPD – eSchKG Verbund
{id-adminpki}.22.55			CP	Class C - System Encryption
{id-adminpki}.22.56			CP	SSL CA 01 – Domain Controller
{id-adminpki}.22.57			CP	Governikus Core Signature Certificate
{id-adminpki}.22.58			CP	Governikus OSCI Transport Encryption Certificate
{id-adminpki}.22.59			CP	Governikus OSCI Transport Signature Certificate
{id-adminpki}.22.60			CP	Governikus Core Timestamp Certificate
{id-adminpki}.22.61			CP	CITES System Dsig, Auth, Enc
{id-adminpki}.22.62			CP	RegularCA01 OCSP Responder Signing
{id-adminpki}.22.63			CP	SSLCA01 OCSP Responder Signing

Object Identifier			Typ	Verwendung
Production	**Acceptance**	**Reference / Development**		
{id-adminpki} : 2.16.756.1.17.3				
{id-adminpki}.22.64			CP	Gruppenmailboxen (Sign/Enc)
{id-adminpki}.22.65			CP	OCSP-Responder-RootCAII
{id-adminpki}.22.66			CP	EESSI Digital Signature Certificate (siehe {id-adminpki}.2.66)
{id-adminpki}.22.67			CP	Person Signature
{id-adminpki}.22.68			CP	Person Encryption
{id-adminpki}.22.69			CP	EETS-B2B Authentication
{id-adminpki}.23.1			Extension	RDN Suffix
{id-adminpki}.23.2			Extension	PKI Entity Type (CAIFs, CAIFc, OM, KAS, KAO)
{id-adminpki}.23.3			Extension	Registration Officer Rolle (AV, ADMIN)
{id-adminpki}.23.4			Extension	*DFS Extensions*
{id-adminpki}.23.4.1	{id-adminpki}.33.4.1	{id-adminpki}.23.4.1	Extension	DFS: CA-Operator Mandator ID (CH, FL)
{id-adminpki}.23.4.2	{id-adminpki}.33.4.2	{id-adminpki}.23.4.2	Extension	DFS: CA-Service Admin Mandator ID (CH, FL)
{id-adminpki}.23.4.3	{id-adminpki}.33.4.3	{id-adminpki}.23.4.3	Extension	DFS: CA Mandator ID (CH, FL)
{id-adminpki}.23.4.4	{id-adminpki}.33.4.4	{id-adminpki}.23.4.4	Extension	DFS: CIA Mandator ID (CH, FL)
{id-adminpki}.23.4.5	{id-adminpki}.33.4.5	{id-adminpki}.23.4.5	Extension	DFS: CP Mandator ID (CH, FL)
{id-adminpki}.23.5			Extension	AgencyIdentifier (CH ID: id-adminpki-bv-amtid)
{id-adminpki}.23.6			Extension	OSCI Participant GUID (id-adminpki -osci-guid)
{id-adminpki}.23.7	-	-	Extension	EJPD_SYSP_APPLICANT (eDoc Systemplattform Applicant)
{id-adminpki}.23.8			Extension	SEDEX internal v3 extension

1.6 SG Root CA III Sub CA's

Tabelle 5: SG Root CA III Sub CA's OIDs

Object Identifier			Typ	Verwendung
Production	**Acceptance**	**Reference / Development**		
{id-adminpki} : 2.16.756.1.17.3				
{id-adminpki}.61.1			CPS	Swiss Government Public Trust Standard CA 02
{id-adminpki}.61.2			CPS	Swiss Government Public Trust EV CA 02
{id-adminpki}.61.3			CPS	Swiss Government Public Codesigning Standard CA 02
{id-adminpki}.61.4			CPS	Swiss Government Public Codesigning EV CA 02
{id-adminpki}.61.5			CPS	Swiss Government Public Trust Standard CA 02 Root-signed by QuoVadis
{id-adminpki}.61.6			CPS	Swiss Government Public Trust Standard CA 03
{id-adminpki}.61.7			CPS	Swiss Government Regular CA 02
~~{id-adminpki}.62.1~~			~~CP~~	~~Public Trust Standard Server Authentication~~
~~{id-adminpki}.62.2~~			~~CP~~	~~Public Trust Standard Client Authentication~~
~~{id-adminpki}.62.3~~			~~CP~~	~~Public Trust Standard Server/Client Authentication~~
~~{id-adminpki}.62.4~~			~~CP~~	~~Public Trust EV Server Authentication~~
~~{id-adminpki}.62.5~~			~~CP~~	~~Public Trust EV Client Authentication~~
~~{id-adminpki}.62.6~~			~~CP~~	~~Public Trust EV Server/Client Authentication~~
~~{id-adminpki}.62.7~~			~~CP~~	~~Public Trust Standard OCSP Responder Signing~~
~~{id-adminpki}.62.8~~			~~CP~~	~~Public Trust EV OCSP Responder Signing~~
~~{id-adminpki}.62.9~~			~~CP~~	~~Public Trust Code Signing~~
~~{id-adminpki}.62.10~~			~~CP~~	~~Public Trust EV Code Signing~~

~~{id-adminpki}.62.11~~			~~CP~~	~~OCSP Responder PTSTCSCA01 (Public Trust Standard CS OCSP Responder Signing)~~
~~{id-adminpki}.62.12~~			~~CP~~	~~OCSP Responder PTEVCSCA02 (Public Trust EV CS OCSP Responder Signing)~~
~~{id-adminpki}.62.13~~			~~CP~~	~~SG Root CA III OCSP Responder Signing~~
~~{id-adminpki}.62.14~~			~~CP~~	~~Public Trust Standard Browser Compatible Server/Client Authentication~~
~~{id-adminpki}.62.15~~			~~CP~~	~~Public Trust Standard Browser Compatible Server/Client Authentication SAN~~
~~{id-adminpki}.62.16~~			~~CP~~	~~Public Trust Standard Browser Compatible Server/Client Authentication SAN >2048KB~~
~~{id-adminpki}.62.17~~			~~CP~~	~~Public Trust Standard CA03 Server Authentication~~
~~{id-adminpki}.62.18~~			~~CP~~	~~OCSP-Responder PTSTCA02BC~~
{id-adminpki}.62.19			CP	RegularCA02-OCSP-Responder
~~{id-adminpki}.62.20~~			~~CP~~	~~Regular CA02 Organization Authentication~~
{id-adminpki}.62.20			CP	Person Authentication (RegularCA02)
{id-adminpki}.62.21			CP	Person Signature (RegularCA02)
{id-adminpki}.62.22			CP	Person Encryption (RegularCA02)
{id-adminpki}.62.23			CP	Organization Authentication (RegularCA02)
{id-adminpki}.62.24			CP	Organzation Signature (RegularCA02)
{id-adminpki}.62.25			CP	Organization Encryption (RegularCA02)
{id-adminpki}.62.26			CP	System Authentication (RegularCA02)
{id-adminpki}.62.27			CP	System Signature (RegularCA02)
{id-adminpki}.62.28			CP	System Encryption (RegularCA02)
{id-adminpki}.62.29			CP	ZKV (Zollkundenverwaltung) Authentication and Encryption (RegularCA02)
{id-adminpki}.62.30			CP	eDoc Systemplattform (RegularCA02)
{id-adminpki}.62.31			CP	Sedex Organisational Client Backend (RegularCA02)
{id-adminpki}.62.32			CP	Process-Authentication EJPD SSO Portal (RegularCA02)
{id-adminpki}.62.33			CP	Organization Authentication/Signature/Encryption

				(RegularCA02)
{id-adminpki}.62.34			CP	Gruppenmailboxen (Sign/Enc)(RegularCA02)
{id-adminpki}.62.35			CP	System Authentication/Signature/Encryption (RegularCA02)
{id-adminpki}.62.36			CP	System Signature/Encryption (RegularCA02)
{id-adminpki}.62.37			CP	Elcom MATCH Client Authentication/Signature (RegularCA02)
{id-adminpki}.62.38			CP	EJPD – eSchKG Verbund (RegularCA02)
{id-adminpki}.62.39			CP	CITES System Dsig, Auth, Enc (RegularCA02)

1.7 SG Root CA IV Sub CA's

Object Identifier			Typ	Verwendung
Production				
{id-adminpki} : 2.16.756.1.17.3				
{id-adminpki}.5.1.1			CP	SG Regulated CA01 – Issuing CA
{id-adminpki}.5.1.2			CP	SG Regulated CA02 – Issuing CA

{id-adminpki}.5.1.3			CP	SG Regulated CA03 – Issuing CA
{id-adminpki}.5.2.1			CP	OCSP-Responder-RegulatedCA02
{id-adminpki}.5.2.2			CP	Electronic Seal on Regulated CA02 (qcp-l-qscd)
{id-adminpki}.5.2.3			CP	Qualified Signature on Regulated CA02 with new ZertEs 2017 adaptation (qcp-n-qscd)
{id-adminpki}.5.2.4			CP	TSA Token (qcp-l-qscd)
{id-adminpki}.5.2.5			CP	OCSP-Responder-RootCAIV
{id-adminpki}.5.2.6			CP	Qualified Signature on Regulated CA02 with new ZertEs 2017 adaptation (qcp-n-qscd) with ***FreeDN***
{id-adminpki}.5.2.7			CP	Geregeltes Behördenzeritikat “neu” – Regulated CA02
{id-adminpki}.5.2.8			CP	Electronic Seal on Regulated CA03 (qcp-l-qscd)
{id-adminpki}.5.2.9			CP	Qualified Signature on Regulated CA03 with new ZertEs 2017 adaptation (qcp-n-qscd)
{id-adminpki}.5.2.10			CP	TSA Token (qcp-l-qscd) on Regulated CA03
{id-adminpki}.5.2.11			CP	Regulated-CA03-OCSP-Responder
{id-adminpki}.5.2.12			CP	Qualified Signature on Regulated CA02 with new ZertEs 2017 adaptation (qcp-n-qscd) with ***FreeDN***
{id-adminpki}.5.2.13			CP	Qualified Signature on Regulated ~~CA03~~ CA02 with new ZertEs 2017 adaptation ~~(qcp-n-HSM)~~ (qcp-n-qscd)
{id-adminpki}.5.2.14			CP	Qualified Signature on Regulated CA02 for GGG (qcp-n-HSM)
{id-adminpki}.5.2.15			CP	Electronic Seal on Regulated CA03 (qcp-l-HSM)

1.8 AdminPKI-KlasseC-Enterprise

Tabelle 6: AdminPKI-KlasseC-Enterprise

Object Identifier	**Typ**	**Verwendung**

Object Identifier	Typ	Verwendung
{id-adminpki}.41.0	CPS	Admin-C-Root01
{id-adminpki}.41.1	CPS	Admin-CE-Intra01, Admin-CE-EDA01, Admin-CE-EVD01
{id-adminpki}.41.2	CPS	KlasseCC-Enterprise (2.16.756.1.17.3.41.2.1)
{id-adminpki}.42.0	Policy	Test
{id-adminpki}.42.1	Policy	Encryption EMail
{id-adminpki}.42.2	Policy	Signing Email
{id-adminpki}.42.3	Policy	DC
{id-adminpki}.42.4	Policy	IPSec
{id-adminpki}.42.5	Policy	Armasuisse Volume Activation Process
{id-adminpki}.42.6	Policy	Armasuisse TEPLAS
{id-adminpki}.43.0	Extension	

1.9 CSCA (Country Signing CA für den ePass 06)

Tabelle 7: ePass 06 OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.51.0	CPS	
{id-adminpki}.52.1	CP	CP CSCA
{id-adminpki}.52.2	CP	CP Signing Server, Document Signer
{id-adminpki}.53.1	Extension	

1.10 CSCA (Country Signing CA) für das MRTD 10

Tabelle 8: CSCA/MRTD 10 OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.61.0	CPS	
{id-adminpki}.62.1	CP	CP/CPS, CSCA, Signing Server, Document Signer, Master-List Signer
{id-adminpki}.62.2	CP	Reserved for future use
{id-adminpki}.63.1	Extension	

1.11 CVCA (Country Verifying CA) für das MRTD 10

Tabelle 9: CVCA/MRTD 10 OIDs

Object Identifier	Typ	Verwendung

Object Identifier	Typ	Verwendung
{id-adminpki}.71.0	CPS	
{id-adminpki}.72.1	CP	CP CVCA
{id-adminpki}.72.2	CP	CP DV Document Verifier
{id-adminpki}.73.1	Extension	

1.12 FKR New Generation – SMART TACHOGRAPHS

Tabelle 10: FKR New Generation - Smart Tachographs

Object Identifier	Typ	Verwendung
{id-adminpki}.81.0	CPS	
{id-adminpki}.82.1	CP	SMART TACHOGRAPHS SUISSE CP AND CPS
{id-adminpki}.82.2	CP	SMART TACHOGRAPHS FL CP AND CPS

1.13 BIT TLS Inspection CA 1

Tabelle 11: BIT TLS Inspection CA 1

Object Identifier	Typ	Verwendung
{id-adminpki}.91.0	CPS	
{id-adminpki}.92.1	CP	BIT TLS Inspection CA 1 CP AND CPS

Object Identifier	Typ	Verwendung

2 AdminPKI BluePrint Top Level OID

The OIDs get reorganized in a tree level following the extension v3 depth. They are organized on the same level as they are in the section 1.

Tabelle 11: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung
2.16.756.1.17.3.100	Top Level	AdminPKI BP

2.1 AdminPKI BluePrint Top Level OID Production

The OIDs get numbered all similarly following this value {id-adminpki}.100.0

Tabelle 12: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung
2.16.756.1.17.3.100.**0**	Top Level	AdminPKI BP Production

2.2 AdminPKI BluePrint Top Level OID Acceptance

The OIDs get numbered all similarly following this value {id-adminpki}.100.1

Tabelle 13: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung
2.16.756.1.17.3.100.**1**	Top Level	AdminPKI BP Acceptance

2.3 AdminPKI BluePrint Top Level OID Reference

The OIDs get numbered all similarly following this value {id-adminpki}.100.2

Tabelle 14: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung

Object Identifier	Typ	Verwendung
2.16.756.1.17.3.100.**2**	Top Level	AdminPKI BP Reference

2.4 AdminPKI TN OID s

The protocol OIDs for TN.

Tabelle 15: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung
2.16.756.1.17.3.100.**3**	Top Level	Top Level protocol
2.16.756.1.17.3.100.**3.1**	X509	X50x types
2.16.756.1.17.3.100.**3.1**	TN Top Level	Top level types
2.16.756.1.17.3.100.**3.2**	TN Protocol	Protocol types
2.16.756.1.17.3.100.**3.3**	TN Types	TN types
2.16.756.1.17.3.100.**3.4**	X50x types	X50x types

2.5 AdminPKI BluePrint

Tabelle 16: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung
2.16.756.1.17.3.100.x.y	Top Level	All extensions follow depth first numbering at this point

2.5.1 AdminPKI BluePrint Entities

All OIDs that deal with the PKI entities (aka CAO, KAO, etc)

Tabelle 17: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.100.x.50	Entities	All OIDs that are related to PKI entities. That is, all

Object Identifier	Typ	Verwendung
		internal certificates and tokens that get used within the various components and not necessariliy published to the outside world.

Tabelle 18: AdminPKI BluePrint OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.100.x.50.1	CAO	Represents a CAO in the BP world

2.5.2 Swiss Government Regular CA 01 (Production)

Tabelle 197: Swiss Government Regular CA 01 OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.100.0.0	CPS	Swiss Government Regular CA 01
{id-adminpki}.100.0.4	CP	System Policy
{id-adminpki}.100.0.8	CP	e-Dec

2.5.3 Swiss Government aRegular CA 01 (Acceptance)

Tabelle 207: Swiss Government aRegular CA 01 OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.100.1.0	CPS	Swiss Government aRegular CA 01
{id-adminpki}.100.1.4	CP	System Policy
{id-adminpki}.100.1.8	CP	e-Dec
{id-adminpki}.100.1.9	CP	Group Mail Box

2.5.4 LDAP ZKV (Acceptance)

All LDAP Attribute Type OIDs that deal with the ZKV application

Tabelle 218: Swiss Government aRegular CA 01 OIDs

Object Identifier	Typ	Verwendung
{id-adminpki}.100.1.500.1	LDAP	adminEDECContactMail
{id-adminpki}.100.1.500.2	LDAP	adminEDECSerialNum
{id-adminpki}.100.1.500.3	LDAP	adminEDECP12
{id-adminpki}.100.1.500.4	LDAP	adminEDECCertCreationDate
{id-adminpki}.100.1.500.5	LDAP	adminEDECCertRevocationDate
{id-adminpki}.100.1.500.6	LDAP	adminEDECStatus
{id-adminpki}.100.1.500.7	LDAP	adminEDECError

3 Anhang

3.1 Tabellenverzeichnis

--- Ende des Dokumentes ---