Public Key Service

Schnittstellenbeschreibung LDAP-Service

Version: 2.1
Stand: 03.08.2015
Status: Freigegeben

Business flexibility T · · Systems · · ·

Impressum

Herausgeber

T-Systems International GmbH

Dateiname	Dokumentennummer	Dokumentenbezeichnung
PKS LDAP-Server v2.1.doc	[Hier Dok-Nr. eingeben]	[Hier Bezeichnung eingeben]

Version	Stand	Status
2.1	03.08.2015	Freigegeben

Kurzinfo

Dieses Dokument beschreibt die COMMON-PKI-konforme Schnittstelle zum PKS-LDAP-Server

Inhaltsverzeichnis

1 Einleitung

Für die Speicherung der Zertifikatsdaten und der Sperrliste in dem LDAP-Verzeichnis von TeleSec werden nur Standard-Objektklassen verwendet, die mit Hilfe von Hilfsklassen um die benötigten Attribute erweitert werden.

Das Grundgerüst für den Aufbau der Objektklassen zur Speicherung der Zertifikatsdaten und der CRL ist in [RFC 4523] festgelegt. In dieser RFC werden die zwei Hilfsklassen PkiCa und PkiUser definiert, die an eine Standard-Objektklasse angehängt werden müssen. Zusätzlich wird die Hilfsklasse PkiUserData definiert, die es erlaubt zusätzliche Standard-Attribute zu einem Benutzereintrag hinzuzufügen.

Die beiden Hilfsklassen PkiCa und PkiUser enthalten Attribute, mit denen alle PKI-spezifischen Informationen (Zertifikate, Sperrlisten, CrossZertifikatpaare) gespeichert werden können. Die Hilfsklasse PkiUser für die Speicherung der PKI-spezifischen Daten eines Endbenutzers enthält nur ein dem Benutzer zugeordnetes Zertifikat. Die Einträge der Zertifizierungsstellen können ebenfalls Zertifikate enthalten, zusätzlich können aber auch Sperrlisten und Crosszertifikatpaare gespeichert werden.

In Kapitel 2.1 wird die Hilfsklasse PkiUser zur Speicherung der Daten von Endbenutzern beschrieben, während Kapitel 2.2 eine Beschreibung der Hilfsklasse PkiCa enthält, in der die zu einer Zertifizierungsstelle gehörenden Daten gespeichert werden. Die Hilfsklasse PkiUserData zur Speicherung zusätzlicher Attribute zu einem Benutzereintrag wird in Kapitel 2.3 erläutert. Die Verwendung der Hilfsklassen kann aus den Kapitel 3 und 4 entnommen werden. Der genaue Aufbau des gesamten Verzeichnisses wird in Kapitel 5 beschrieben.

2 Aufbau der Hilfsklassen

2.1 Aubau der Hilfsklasse PkiUser

Name der Objektklasse: pkiUser

Objekt Id (OID): 2.5.6.21

Attribute in der Hilfsklasse:

- userCertificate;binary: Benutzerzertifikat.

2.2 Aufbau der Hilfsklasse PkiCa

Name der Objektklasse: pkiCa

Objekt-Id (OID): 2.5.6.22

Attribute der Hilfsklasse:

- certificateRevocationList: Sperrliste, die Konform zur Norm X.509 ist.
- caCertificate;binary: Zertifikat einer Zertifizierungsstelle.

2.3 Aufbau der Hilfsklasse PkiUserData

Name der Objektklasse: pkiUser

Objekt-Id (OID): 0.2.262.1.10.3.6

Attribute der Hilfsklasse:

- businessCategory: Arbeitsgebiet des Benutzers
- countryName: Heimatland des Benutzers
- givenName: Vorname der Benutzers
- localityName: Wohnort des Benutzers
- mail: E-Mail-Adresse des Benutzers
- organizationalUnitName: Organisationseinheit des Benutzers
- organizationName: Organisation des Benutzers
- postalCode: Postleitzahl des Wohnortes
- streetAddress: Straße des Benutzers am Wohnort
- title: Titel des Benutzers

3 Aufbau der Benutzereinträge

Benutzereinträge werden mit Hilfe der Objektklasse Person und den Hilfsklassen PkiUser und PkiUserData im Verzeichnis abgelegt. Die Attribute CommonName, SurName und UserCertificate;binary sind immer vorhanden, alle anderen Attribute sind optional.

3.1 Der Aufbau des DN für den Benutzereintrag

Der DistinguishedName (DN) eines Eintrages gibt eindeutig die Position des Eintrages in dem Directory Information Tree (DIT) wieder. Er muß daher eindeutig sein. Der DN eines Eintrages hat die Struktur cn=..., ou=..., o=..., c=... (z.B. c=DE, o=Deutsche Telekom AG, ou=TeleSec CA 1, cn=Maier WilhelmSER:1). Da der CommonName des Benutzers mit in den DN eingeht, muß dieser eindeutig gemacht werden. Dazu wird bei der Zertifizierungsstelle eine eindeutige Seriennummer für jedes Zertifikat vergeben. Diese entspricht der Zertifikatsseriennummer. Mit dem Vorsatz SER: wird diese Seriennummer an den CommonName im DN angehängt

3.2 Beispiel für den Aufbau eines Endbenutzer-Eintrages

DN:	CN=Maier Wilhelm SER:2,
	OU=TeleSec CA 1, O=Telekom, C=DE
Objektklasse:	pkiUserData
	pkiUser
	person
	top
Attribute:	

commonName:	Maier, WilhelmSER:2
country:	c=DE
surname:	Maier, Wilhelm
userCertificate ;binary:	binär, ASN.1-kodiert

4 Aufbau der Einträge der Zertifizierungsstelle

Die Einträge der Zertifizierungsstelle werden in zwei Bereiche aufgeteilt. Root-Zertifikate und Sperrlisten werden mit der Objektklasse Organization und der Hilfsklasse PkiCa im Verzeichnisbaum unterhalb von Country abgelegt. Die CA-Zertifikate der Zertifizierungsstelle für das Ausstellen von Zertifikaten, den Verzeichnisdienst und den Zeitstempeldienst werden in der Objektklasse OrganizationalUnit zusammen mit der Hilfsklasse PkiCa gespeichert.

4.1 Der Aufbau des DN für den Eintrag der CA

Der DN setzt sich aus den namengebenden Attributen der einzelnen Knotenpunkte zusammen, die auf dem Weg vom obersten Knoten bis zum gewünschten Eintrag durchlaufen werden. Im Verzeichnisdienst des Public Key Service befinden sich diese Daten in dem Knoten o=Deutsche Telekom AG, c=de. Neben diesen übergeordneten Einträgen gibt es darunter einen Eintrag für jedes Ca-Zertifikat. Der DN eines Eintrages einer CA hat bei dem oben beschriebenen Aufbau eines Verzeichnisses immer die Struktur ou=..., o=..., c=... (z.B. c=DE, o=Deutsche Telekom AG, cn=TeleSec CA 1).

4.2 Beispiel für den übergeordneten Eintrag der Zertifizierungsstelle

DN:	O=Deutsche Telekom AG, C=DE		
Objekklasse:	pkiCa		
	organization		
	top		
Attribute:	organizationName:	Deutsche Telekom AG	

4.3 Beispiel für einen Eintrag mit CA-Zertifikat zur Zertifikatsaustellung

DN:	OU=Telesec CA 1:PN, O=Deutsche Telekom AG, C=DE		
Objekklasse:	pkiCa		
	organizationalUnit		
	top		
Attribute:		OrganizationalUnitName:	Telesec CA 1:PN
		caCertificate;binary:	binär, ASN.1-kodiert

5 Aufbau des Verzeichnisses

Das LDAP-Verzeichnis ist so aufgebaut sein, dass eine Zuordnung der Zertifikate zum ausgebenden CA-Zertifikat gewährleistet ist. Der Aufbau basiert daher auf dem Herausgeberfeld des Zertifikats.

Bei dem Aufbau der Verzeichnisstruktur werden nur Attribute und Objektklassen aus dem Standard verwendet werden. Zu diesen Objektklassen werden die benötigten zusätzlichen Attribute mittels Hilfsklassen hinzugefügt. Für die Speicherung der Zertifikate und der Listen wird eine Standard-Objektklasse (Organization, OrganizationalUnit oder Person) verwendet , an welche die in der RFC 2587 beschriebenen Hilfsklassen PkiCa bzw. PkiUser angefügt werden. Zusätzliche Standard-Attribute für die Benutzer-Einträge können mit der Hilfsklasse pkiUserData eingefügt werden.

Der Aufbau des Verzeichnisses erfolgt zertifikatsorientiert, d.h. jedes Zertifikat wird in einem einzelnen Eintrag im Verzeichnis gespeichert. Die Zertifikate werden immer unterhalb des CA-Zertifikates abgespeichert, von dem sie digital signiert wurden.

Die Sperrlisten werden in dem Knoten Organization abgespeichert.

Der Verzeichnisbaum hat den folgenden Aufbau:

C=DE

O=Deutsche Telekom AG

OU=TeleSec CA 1

CN=Benutzer-CommonName SER: 1

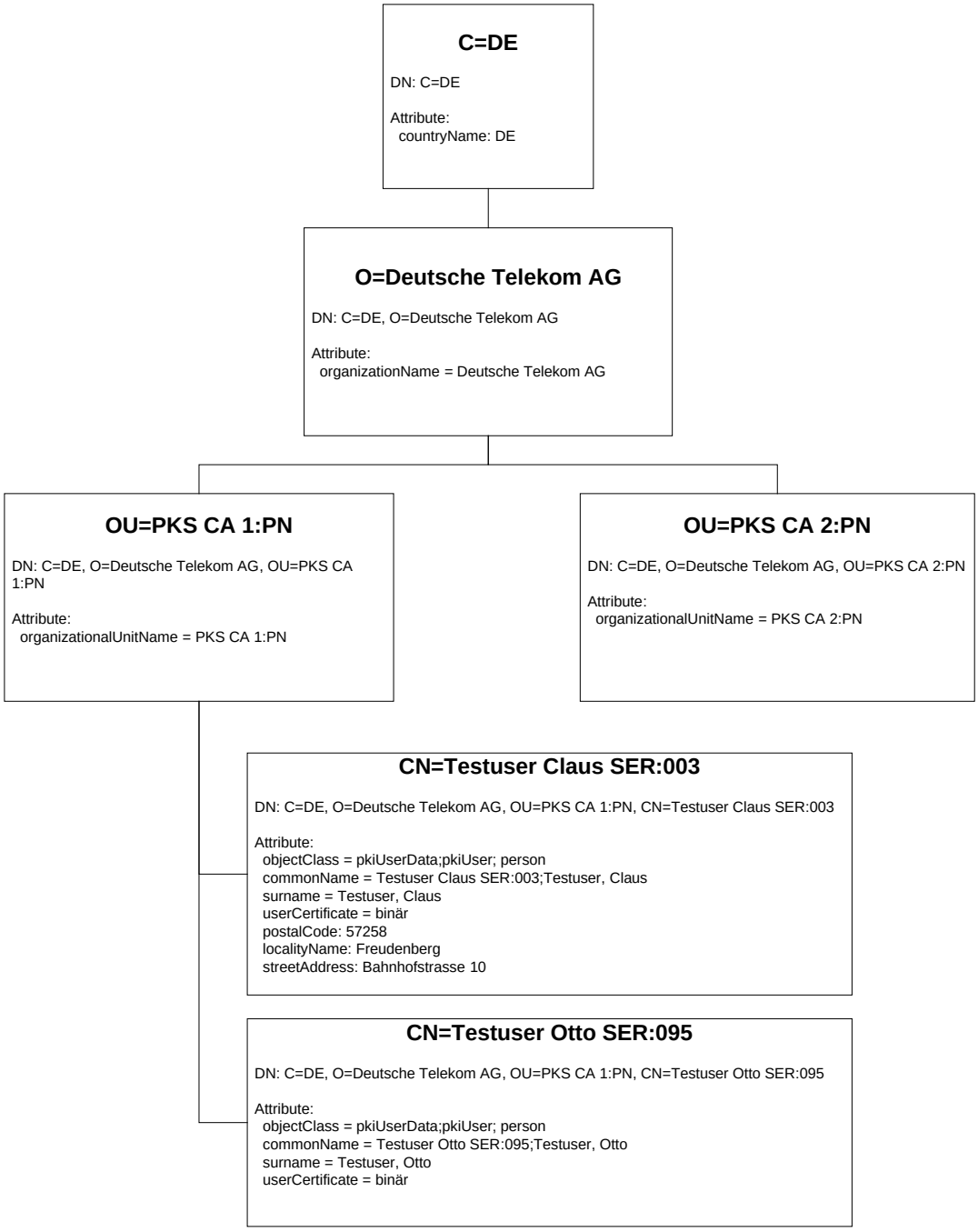
CN=Benutzer-CommonName SER: 2

OU=TeleSec CA 2

CN=Benutzer-CommonName 1:PN

...

In der folgenden Abbildung wird der Aufbau des Verzeichnisses zusätzlich an einem Beispiel graphisch dargestellt.



Quellenverzeichnis

[COMMON-PKI] COMMON-PKI Core Specification, Version 2.0, 20. Januar 2009

[RFC4523] MK. Zeilenga, Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates, June 2006