deutsches forschungsnetz

Zertifikatprofile in der DFN-PKI

(Sicherheitsniveau Global)

In der DFN-PKI werden Zertifikatprofile mit verschiedenen, fest vorgegebenen X.509v3 Zertifikaterweiterungen unterstützt.

Zertifikate für Datenverarbeitungssysteme

Zertifikate für Datenverarbeitungssysteme enthalten als CommonName und SubjectAltname immer mindestens einen voll qualifizierten Domainnamen (FQDN).

Alle Zertifikate für Datenverarbeitungssysteme enthalten die folgenden Erweiterungen:

authorityInfoAccess	Wert cAIssuer: URL des CA-Zertifikats Wert OCSP: URL des OCSP-Responders der DFN-PKI (http://ocsp.pca.dfn.de/OCSP-Server/OCSP)
authorityKeyIdentifier	Bezeichner des Schlüssels des ausstellenden CA-Zertifikats
basicConstraint	CA:FALSE
certificatePolicies	OID 2.23.140.1.2.2 OID 1.3.6.1.4.1.22177.300.30 OID 1.3.6.1.4.1.22177.300.1.1.4 OIDs der aktuell gültigen CP und CPS Dokumente der DFN-PKI
cRLDistributionPoints	URL der Sperrliste
subjectAltName	Erlaubte Namenstypen: dNSName iPAddress
subjectKeyIdentifier	Bezeichner des Schlüssels des Zertifikats

Die einzelnen Profile unterscheiden sich in der keyUsage, der extendedKeyUsage und in zusätzlichen Erweiterungen.

Profilname	**keyUsage**	**extendedKeyUsage**	**zusätzliche Erweiterungen**
802.1X Client	digitalSignature, keyEncipherment	clientAuth, serverAuth	
Domain Controller	digitalSignature, keyEncipherment	clientAuth, serverAuth, Microsoft Smartcard Logon, KDCAuth (Das Wurzelzertifikat muss in Windows für diese extendedKeyUsage separat freigeschaltet werden!)	Microsoft Enroll Certtype: DomainController
Exchange Server	digitalSignature, keyEncipherment	clientAuth, serverAuth, emailProtection	
LDAP Server	digitalSignature, keyEncipherment	clientAuth, serverAuth	

Profilname	keyUsage	extendedKeyUsage	zusätzliche Erweiterungen
Mail Server	digitalSignature, keyEncipherment	clientAuth, serverAuth	
Radius Server	digitalSignature, keyEncipherment	clientAuth, serverAuth	
Shibboleth IdP SP	digitalSignature, keyEncipherment	clientAuth, serverAuth	
VoIP Server	digitalSignature, keyEncipherment	clientAuth, serverAuth	
VPN Server	digitalSignature, keyEncipherment	serverAuth	
Web Server	digitalSignature, keyEncipherment	serverAuth	
Webserver MustStaple	digitalSignature, keyEncipherment	serverAuth	tlsFeature: statusRequest(5)
Web Server SOAP	digitalSignature, keyEncipherment	serverAuth	

Zertifikate für Benutzer

Zertifikate für Benutzer enthalten als CommonName immer den Namen einer natürlichen Person, ein Pseudonym oder einen Gruppennamen.

Alle Zertifikate für Benutzer enthalten die folgende Erweiterung:

authorityInfoAccess	Wert cAIssuer: URL des CA-Zertifikats Wert OCSP: URL des OCSP-Responders der DFN-PKI (http://ocsp.pca.dfn.de/OCSP-Server/OCSP)
authorityKeyIdentifier	Bezeichner des Schlüssels des ausstellenden CA-Zertifikats
basicConstraint	CA:FALSE
certificatePolicies	OID 1.3.6.1.4.1.22177.300.1.1.4 OIDs der aktuell gültigen CP und CPS Dokumente der DFN-PKI
cRLDistributionPoints	URL der Sperrliste
subjectAltName (optional)	Erlaubte Namenstypen: otherName vom Typ microsoftUserPrincipalName rfc822Name uniformResourceIdentifier
subjectKeyIdentifier	Bezeichner des Schlüssels des Zertifikats

Die einzelnen Profile unterscheiden sich in der keyUsage, der extendedKeyUsage und in zusätzlichen Erweiterungen.

Profilname	keyUsage	extendedKeyUsage
802.1X User	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection
Code Signing	digitalSignature	codeSigning (Für CodeSigning in Windows muss das Wurzelzertifikat

		separat freigeschaltet werden!)
Mitarbeiter	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection
RA Operator	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection
Smartcard	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection
Smartcard Encrypt	keyEncipherment	emailProtection
Smartcard Logon	digitalSignature	clientAuth, 1.3.6.1.4.1.311.20.2.2
Smartcard Sign	nonRepudiation, digitalSignature	emailProtection
Smartcard Sign and Logon	nonRepudiation, digitalSignature	clientAuth, emailProtection, 1.3.6.1.4.1.311.20.2.2
Student	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection
TrustedDisk	digitalSignature, keyEncipherment	1.3.6.1.4.1.30205.13.1.1
User	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection
UserAuth	digitalSignature, keyEncipherment	clientAuth
UserEMail	nonRepudiation, digitalSignature, keyEncipherment	emailProtection
UserEncrypt	keyEncipherment	emailProtection
UserSign	nonRepudiation, digitalSignature,	emailProtection
UserSignAuth	nonRepudiation, digitalSignature,	clientAuth, emailProtection
User SOAP	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection
VPN User	nonRepudiation, digitalSignature, keyEncipherment	clientAuth, emailProtection

Verwendete Object Identifier

Zertifikaterweiterung	Wert aus der Zertifikaterweiterung	Zugehöriger Objekt Identifikator (OID)
AuthorityInfoAccess		1.3.6.1.5.5.7.1.1
	caIssuers	1.3.6.1.5.5.7.48.2
	OCSP	1.3.6.1.5.5.7.48.1
AuthorityKeyIdentifier		2.5.29.35
BasicConstraints		2.5.29.19
CertificatePolicies		2.5.29.32
CRLDistributionPoints		2.5.29.31
ExtendedKeyUsage		2.5.29.37
	serverAuth	1.3.6.1.5.5.7.3.1
	clientAuth	1.3.6.1.5.5.7.3.2
	codeSigning	1.3.6.1.5.5.7.3.3
	emailProtection	1.3.6.1.5.5.7.3.4
	Microsoft Smartcard Logon	1.3.6.1.4.1.311.20.2.2
	KDCAuth	1.3.6.1.5.2.3.5
	TrustedDisk	1.3.6.1.4.1.30205.13.1.1
KeyUsage		2.5.29.15
	digitalSignature	
	keyEncipherment	
	nonRepudiation	
Microsoft Enroll Certtype (Microsoft Certificate Template)		1.3.6.1.4.1.311.20.2
SubjectAltName		2.5.29.17
SubjectKeyIdentifier		2.5.29.14
tlsFeature		1.3.6.1.5.5.7.1.24
	status_request (5)	