deutsches forschungsnetz

Zertifikatprofile der eduroam-ca in der DFN-PKI

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

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
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**
RADIUS Server	digitalSignature, keyEncipherment	clientAuth, serverAuth	certificatePolicies = 1.3.6.1.4.1.22177.100.1.1, 1.3.6.1.4.1.22177.100.1.2
RadSec Client	digitalSignature, keyEncipherment	clientAuth, serverAuth	certificatePolices = 1.3.6.1.4.1.22177.100.1.2
RadSec Client Server	digitalSignature, keyEncipherment	clientAuth, serverAuth	certificatePolicies = 1.3.6.1.4.1.22177.100.1.1, 1.3.6.1.4.1.22177.100.1.2
RadSec Server	digitalSignature, keyEncipherment	serverAuth	certificatePolicies = 1.3.6.1.4.1.22177.100.1.1