

Verba Seal PKI Token / Verba Seal HSM G3

Профил за сертификат на краен корисник

Квалификуван сертификат за правно лице издаден на локално QSCD

Name	Value
Version	V3
Serial Number	<>
Signature algorithm	Sha256RSA
Signature hash algorithm	Sha256
Issuer	CN = KIBSTrust Issuing Qseal CA G3 2.5.4.97 = NTRMK-5529581 OU = KIBSTrust Services O = KIBS AD Skopje C = MK
Valid from	<Date of signing 00:00:00 GMT>
Valid to	<Date of signing + 1 day + (365 or 730 or 1095 days) at 23:59:59 GMT>
Subject	CN = Legal Person's name. (short name) O = Issuer organization name who made subscriber identification 2.5.4.97 = NTR<Country code>-NTRnumber Identification of the Subscriber organization different from the organization name OU = Issuer organization unit name (optional) OU = VAT - <VATNumber> (optional) C = 2 character ISO 3166 country code
Public key	RSA (2048 bits)
Public Key parameters	05 00
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl3.kibstrust.com/KIBSTrustIssuingQsealCAG3.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.16305.1.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.kibstrust.com/repository/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.16305.1.2.5.5.3 [3]Certificate Policy: Policy Identifier=0.4.0.194112.1.3
Key Usage	Digital Signature, Non-Repudiation (c0)
Subject Key Identifier	<>
Authority Key Identifier	KeyID=e0b0e64bb05e5f53cf95dbff17b747c4227432a9
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Subject Alternative Name	RFC822 Name=<e-mail address>

<p>Qualified Certificate Statements</p>	<p>etsiQcsCompliance 0.4.0.1862.1.1 etsiQcsQcSSCD 0.4.0.1862.1.4 etsiQcPDS 0.4.0.1862.1.5 PDS Location (EN) https://www.kibstrust.com/repository/docs/PDSG3-EN.pdf PDS Location (MK) https://www.kibstrust.com/repository/docs/PDSG3-MK.pdf etsiQcType 0.4.0.1862.1.6 etsiQcTypeEsign 0.4.0.1862.1.6.2</p>
<p>Authority Information Access</p>	<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp3.kibstrust.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://cacerts.kibstrust.com/KIBSTrustIssuingQsealCAG3.crt</p>
<p>Thumbprint</p>	<p><></p>

Verba Seal PKI Token G2

Профил за сертификат на краен корисник

Квалификуван сертификат за правно лице издаден на QSCD

Name	Value
Version	V3
Serial Number	<>
Signature algorithm	Sha256RSA
Signature hash algorithm	Sha256
Issuer	CN = KIBSTrust Issuing Qseal CA G2 2.5.4.97 = NTRMK-5529581 OU = KIBSTrust Services O = KIBS AD Skopje C = MK
Valid from	<Date of signing 00:00:00 GMT>
Valid to	<Date of signing + 1 day + (365 or 730 or 1095 days) at 23:59:59 GMT>
Subject	CN = <i>Legal Person's name. (short name)</i> O = <i>Issuer organization name who made subscriber identification</i> 2.5.4.97 = NTR <Country code>- <i>NTRnumber Identification of the Subscriber organization different from the organization name</i> OU = <i>Issuer organization unit name (optional)</i> OU = <i>VAT - <VATNumber> (optional)</i> C = <i>2 character ISO 3166 country code</i>
Public key	RSA (2048 bits)
Public Key parameters	05 00
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.kibstrust.com/qSealG2.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.16305.1.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.kibstrust.com/repository/cps [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.16305.1.2.5.2.3 [3]Certificate Policy: Policy Identifier=0.4.0.194112.1.3
Key Usage	Digital Signature, Non-Repudiation (c0)
Subject Key Identifier	<>
Authority Key Identifier	KeyID=264aabd306a8e9d270da7104b631504785a9094d
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Subject Alternative Name	RFC822 Name=<e-mail address>

Qualified Certificate Statements	etsiQcsCompliance 0.4.0.1862.1.1 etsiQcsQcSSCD 0.4.0.1862.1.4 etsiQcPDS 0.4.0.1862.1.5 PDS Location (EN) https://www.kibstrust.com/repository/docs/PDSG2-EN.pdf PDS Location (MK) https://www.kibstrust.com/repository/docs/PDSG2-MK.pdf etsiQcType 0.4.0.1862.1.6 etsiQcTypeEsign 0.4.0.1862.1.6.2
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp2.kibstrust.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://www.kibstrust.com/repository/certs/CA-qSeal-G2.crt
Thumbprint	<>