Signet TSA: Profile of Signet TSA certificate and Signet TSA time stamp

Signet TSA - Qualified Time Stamp Authority

This document contains information about the TSA certificate used at Signet TSA and the profile used for time stamps.

Certificate profile for the Signet TSA time stamping certificate

x.509 Fields	
Version	V3
Serial Number	Allocated automatically by the Fullgilt audkenni CA
Issuer	
Country (C)	IS
Organization (O)	Audkenni ehf.
OrganizationIdentifier	NTRIS-5210002790
Serialnumber	5210002790
Common Name (CN)	Fullgilt audkenni 2021
Subject	
Country (C)	IS
Organization (O)	Advania Ísland ehf.
OrganizationIdentifier	NTRIS-5902697199
Serialnumber	5902697199
Common Name (CN)	Signet TSA [Current Year, i.e. 2022]
Validity	*6 years*
Signature Algorithm	*SHA256WITHRSA*
Key Length	*3072 bit*
x.509 Extensions	
Key Usage	Critical
Digital Signature	*Selected*
Non-Repudiation	*Selected*
Extended Key Usage	*Critical*
Time Stamping (1.3.6.1.5.5.7.3.8)	*Selected*
Basic Constraints	Critical
Subject Type	Subject is not a CA
Path Length Constraint	None
Authority Key Identifier	Not Critical
Subject Key Identifier	Not Critical
Certificate Policies	*Not Critical*
Policy Identifier OID's	2.16.352.1.2.1.1.2 0.4.0.2042.1.2 2.16.352.1.2.14.2

User Notice Explicit Text	Time-Stamping Unit
CPS Pointer	https://repo.audkenni.is/cps
CRL Distribution Point	Non Critical
Distribution Point URI	http://crl.audkenni.is/FA2021/latest.crl
Authority Information Access	Non Critical
Authority Information Access value	Authority Information Access [1]: Access Method: OCSP (1.3.6.1.5.5.7.48.1) Access Location: URI: http://ocsp.audkenni.is Authority Information Access [2]: Access Method: CA Issuers (1.3.6.1.5.5.7.48.2) Access Location: URI: http://cdp.islandsrot.is/skilriki/FA2021.p7b
Private Key Usage Period	Critical
Validity	Not Before: [Issuing date & time GMT] Not After: [1 year and 42 days after Issuing date & time GMT]

Signet TSA time stamp Profile

reqPolicy	True /supported
nonce	True /supported
certReq	True /supported
policy	0.4.0.2023.1.1
genTime	Date + hour + min + sec i.e. :2022-07-29 12:42:49
accuracy	Secs: 1 - Millis: 0 - Micros: 0
Fraction of a second in time stamp token	FALSE / Not supported
ordering	FALSE / Not supported
Qualified statement	EuCompliance Object ID: 0.4.0.19422.1.1
SHA hash functions	SHA 256 & SHA 512 supported
Time Source	Use time obtained from the server's clock