ADVANCED ELECTRONIC SEAL CERTIFICATE POLICY

Global Trusted Sign

Document Reference | PL17_GTS_V3

TABLE OF CONTENTS

1. References	EU Regulation No. 910/2014 (Art. 8, Section 4, Annex I, Annex II) ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 412-1 PD CENTS 419 241 :2014 RFC 5280: Internet X.509 PKI - Certificate and CRL Profile, 2008 RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003.
2. Associated Documents	PC21_GTS - Advanced Certificate Issuance Process PC22_GTS - Advanced Certificate Revocation Process
3. Distribution List	Interested parties in the GTS trust hierarchy
4. Document History	03-04-2019 | Version 1 10-03-2020 | Version 2 18-09-2020 | Version 3
5. Document Classification	D | Public

6. Revision Record

Version Number	Created	Approved	Reason
	18-09-2020	18-09-2020	
3	**AdmSeg**	**Management Group**	Update of GTS Trust Group and registrations.
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 18-09-2020 08:58:59	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 18-09-2020 09:00:59	

7. Introduction

This document aims to present the Advanced Electronic Seal Certificate Policy of the Global Trusted Sign Root Certification Authority, as a qualified trust service provider in the context of Regulation 910/2014 (hereinafter referred to as GTS CA).

This document is public and intended for the GTS CA working groups and third parties responsible for auditing the GTS CA.

It is suggested that the reader knows the concepts of cryptography, public-key infrastructures and electronic signature.

8. General Context

This document focuses on the definition of profiles of Advanced Electronic Seal Certificates issued by the GTS NQ CA (Global Trusted Sign Advanced Certification Authority), enabling the assurance of liability of the certificates. This document is not intended to appoint legal rules or obligations, but rather to inform in a simple and direct way the general public, including people without technical or legal knowledge.

The certificates issued by the GTS CA contain a reference to the GTS CA Certification Practice Statement (CPS), being the CPS supplemented by this Certificate Policy.

The present document is referred to as "Advanced Electronic Seal Certificate Policy".

Document information	
Version of the document	3
Status of the document	Approved
OID **"Object identifier"**	1.3.6.1.4.1.50302.1.1.2.7.1.0
Issuance Date	18th September 2020
Validity	18th September 2021
Location	https://pki.globaltrustedsign.com/index.html

9. Identification and Authentication

9.1. Name Allocation

The allocation of names proceeds as follows:

Attribute	Code	Value
Country	C	<Holder's country>
Organization	O	<Legal name of the organization>
Common Name	CN	<Name of the organization for which it is known>
Organization Identifier	OrganizationIdentifier	Unique identifier of the legal person, other than the name of the organization. (2.5.4.97) VAT format<country's code>-<TIN of the legal person> (According to 5.1.4 of the ETSI 319 412-1)

9.2. Use of the Certificate and Pair of Keys by the holder

The natural or legal person identified by the DN (Distinguished Name) is the holder of the Advanced Electronic Seal Certificate (check 9.1. Names Allocation). The certificate issued according to this policy complies with the terms established on the applicable Portuguese Law.

10. Certificate Profiles

10.1. Certificate Profile

The public key - private key pair is associated with a holder (natural or legal person) whose main use is digital signature. The user of the public key trusts the respective private key and this trust is given through the use of X.509 v3 digital certificates (connecting the holder and the public key). The GTS CA digitally signs the digital certificate, making sure that the holder has the private key (proof of possession of the private key).

Certificates issued by the GTS Advanced Certification Authority:

- Have a validity of 1, 2 or 3 years, stated in their content.
- Are signed by the GTS Advanced Certification Authority.
- Are distributed through public systems.
- Can be stored in any type of storage units.

Security services requiring the public key of the user may need to validate the entire GTS CA chain of trust (Certificate of the GTS Root Certification Authority and the Certificate of the Advanced Certification Authority). These certificates are public and can be checked by any security service (https://pki.globaltrustedsign.com/index.html).

The storage of keys involved in all signature processes or generation of certificates by the GTS Certification Authority in in the possession of the certificate holder, as this certificate is downloaded by the holder, thus meeting the requirements set forth in the ETSI standards.

The profile of the Advanced Electronic Seal certificate meets the ETSI 319 412 standards.

10.1.1. Version Number

The certificate ***version*** field describes the version used in the certificate encryption. In this profile, version 3 (v3) is used.

10.1.2. Certificate Extensions

X.509 v3 certificates provide methods to associate attributes with users or public keys, as well as to manage the certification hierarchy.

10.1.3. Issuance of Advanced Electronic Seal Certificates

Certificate Component	Value	Type	Remarks
Version	V3	M	
Serial Number	<Assigned by the GTS Certification Authority to each certificate>	M	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	"Global Trusted Sign NQ Certification Authority 02"		
Validity			Validity of the Certificate
Valid from	<Date of issuance>		
Valid to	<Date of issuance + 1, 2 or 3 years>		Maximum validity of 1, 2 or 3 years
Subject		M	
Country (C)	<Country>		Nationality of the certificate's holder
OrganizationIdentifier	<Unique identifier of the legal person>	M	Unique identifier of the legal person, other than the name of the Organization. (2.5.4.97) VAT format<country's code>-<TIN of the legal person> (According to 5.1.4 of the ETSI 319 412-1)
Organization (O)	<Name of the organization>		Name of the organization
Common Name (CN)	<Name of the organization for which it is known>		Name of the organization for which it is known
Subject Public Key Info		M	
Algorithm	rsaEncryption (OID: 1.2.840.113549.1.1.1)		Public key algorithm
subjectPublicKey	<Public key>		Certificate's public key

Certificate Component	Value	Type	Remarks
Authority Key Identifier		M	
keyIdentifier	160-bit hash		It enables to identify the public key corresponding to the private key of the certificate
Subject Key Identifier	160-bit hash	M	Identifier of the certificate's key
Key Usage		M	
Digital Signature	"0" selected		
Non-Repudiation	"1" selected		
Key Encipherment	"0" selected		
Data Encipherment	"0" selected		
Key Agreement	"0" selected		
Key Certificate Signature	"0" selected		
CRL Signature	"0" selected		
Encipher Only	"0" selected		
Decipher Only	"0" selected		
Certificate Policies		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.2.7.1.0 Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identifier and location of the Certification Practice Statement of the GTS NQ CA
Basic Constraints		M	
Subject Type	End Entity		Certificate intended to End-Entities
PathLenConstraint	None		
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/subca_nq/gts_subcanq02_crl.crl		Location of the GTS NQ CA Certificate Revocation List

Certificate Component	Value	Type	Remarks
[2]	distributionPoint: https://pki02.globaltrustedsign.com/subca_nq/gts_subcanq02_crl.crl		Secondary location of the GTS NQ CA Certificate Revocation List
Authority Information Access		M	
[1] accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)		Certificate validation service
[1] accessLocation	http://ocsp-nq.globaltrustedsign.com/		OCSP service location
[2] accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parameter used to identify the GTS NQ CA certificate and build the chain of trust.
[2] accessLocation	https://pki.globaltrustedsign.com/subca_nq/gts_subcanq02.crt		Location of the GTS NQ CA Certificate
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Algorithm used to create the certificate's signature
Signature Value	<It contains the digital signature issued by the NQCA>	M	Signature of the certificate

10.1.4. Algorithm OID

The certificate ***signatureAlgorithm*** field contains the cryptographic algorithm OID used by the GTS CA to sign the certificate (1.2.840.113549.1.1.11 - sha256WithRSAEncryption).

10.1.5. Names Constraints

In order to ensure total interoperability between applications that use digital certificates, it is recommended to use only alphanumeric characters without accents, space, underline, minus symbol and full stop ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') on X.500 directory entries.

10.1.6. Policy Constraints Extension

Not applicable.