POLÍTICA DE CERTIFICADOS PARA AUTENTICAÇÃO DE SÍTIOS WEB (SSL EXTENDED VALIDATION)

Global Trusted Sign

Referência do Documento | PL03_GTS_V6

ÍNDICE

1. Referências	Regulamento 910/2014 | 45.1; Anexo IV ETSI EN 319 411-1 | 6.6.3; 6.2.3; 6.3.7 ETSI EN 319 411-2 | 6.6.3; 6.2.3; 6.3.7 BRG CA/Browser Forum | 6.1.6; 6.1.7; 7.1 Browser Forum EV Guidelines v1.6.8
2. Documentos Associados	PC03_GTS - Processo de Emissão de Certificados para Autenticação de Sítios Web PC15_GTS - Processo de Revogação de Certificados para Autenticação de Sítios Web DP02_GTS - Declaração de Práticas de Certificação da EC GTS DP04_GTS - PKI Disclosure Statement CA GTS - EN
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	31-07-2017 | Versão 1 18-08-2017 | Versão 2 25-08-2017 | Versão 3 31-01-2019 | Versão 4 09-03-2020 | Versão 5 04-11-2020 | Versão 6
5. Classificação do Documento	D | Público

6. Registo da Revisão

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	04-11-2020	**04-11-2020**	
6	**AdmSeg**	**Grupo de Gestão**	Atualização de AdmSeg
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 04-11-2020 17:22:33	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 04-11-2020 17:24:02	

7. Introdução

O presente documento tem como objetivo apresentar a Política de Certificados para autenticação de Sítios Web (SSL *Extended Validation*) da Entidade Certificadora da Global Trusted Sign, enquanto prestadora de serviços qualificados no âmbito do regulamento 910/2014 (adiante designada por EC GTS).

O presente documento apresenta-se disponível publicamente e é destinado a todos os participantes que se relacionem, de alguma forma, com a Entidade Certificadora da GTS.

No âmbito da presente declaração de práticas assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica.

8. Contexto Geral

O objetivo do presente documento é a definição do perfil dos Certificados de Autenticação de Sítios Web (SSL *Extended Validation*) emitidos pela EC GTS (Entidade de Certificação da Global Trusted Sign).

Os certificados emitidos pela EC GTS contêm uma referência à Declaração de Práticas de Certificação da EC GTS (DPC), sendo a DPC completada pela presente Política de Certificados.

O presente documento designa-se "Politica de Certificados para Autenticação de Sítios Web (SSL *Extented Validation*)".

Informação do Documento	
Versão do Documento	6
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.2.2.1.0
Data de Emissão	04 de novembro de 2020
Validade	04 de novembro de 2021
Localização	https://pki.globaltrustedsign.com/index.html

9. dentificação e Autenticação

9.1. Atribuição de Nomes

A atribuição de nomes segue a convenção:

Atributo	Código	Valor
Country	C	<País>
Locality Name	L	<Localidade>
Organization	O	<Nome da Organização>
Common Name	CN	<Fully Qualified Domain Name do Servidor Web >
Postal Code	POSTALCODE	<Código postal da Organização>
Street Address	STREET	<Morada da Organização>
Street Address	STREET	<Localidade relativa ao código postal da organização>
Serial Number	SERIALNUMBER	<Identificador único da organização>
Business Category	BUSINESSCATEGORY	<Setor de atividade da organização>
Jurisdiction Country Name	JURISDICTIONOFINCORPORATIONCOUNTRYNAME	<País onde a organização decorre a sua atividade>
Jurisdiction State Or Province Name	JURISDICTIONOFINCORPORATIONSTATEORPROVINCENAME	<Província onde a organização decorre a sua atividade>
Jurisdiction Locality Name	JURISDICTIONOFINCORPORATIONLOCALITYNAME	<Localidade onde a organização decorre a sua atividade>

9.2. Uso do certificado e par de chaves pelo titular

A EC GTS é uma entidade emissora de certificados para sítios web. O nome qualificado do domínio do serviço ou sítio web está contido campo ***Common Name*** do certificado, sendo este certificado usado para o estabelecimento de uma ligação segura SSL/TLS.

10. Perfis de Certificado

10.1. Perfil de Certificado

Par chave pública – chave privada está associado a um titular cujo principal uso é a utilização mecanismos de cifra e assinatura digital. O utilizador da chave pública confia na respetiva chave privada sendo esta confiança dada através do uso de certificados digitais X.509 v3 (fazendo uma ligação do titular com chave pública). A EC GTS assina digitalmente o certificado digital, certificando-se que o titular possui a chave privada (prova de posse da chave privada).

Os certificados emitidos pela EC GTS:

- Têm um limite de validade (1 ano), indicado no seu conteúdo.
- São assinados pela EC GTS.
- São distribuídos através de sistemas públicos.
- Podem ser guardados em qualquer tipo de unidades de armazenamento.

Serviços de segurança que requeiram a chave pública do utilizador podem precisar de validar toda a cadeia de confiança da EC GTS (Certificado da Entidade de Certificação da GTS e Certificado da Entidade de Certificação de Raiz da GTS). Estes certificados são públicos e podem ser consultados por qualquer serviço de segurança (https://pki.globaltrustedsign.com/index.html).

A emissão deste certificado a ser publicado contém a si inerente a introdução de dois domínios para o site do cliente, utilizando as versões www e não www do URL (por exemplo, "http://www.example.com" e "http://example.com").

O armazenamento das chaves envolvidas em todos os processos de assinatura ou geração de certificados pela Entidade de Certificação da GTS são guardados num Dispositivo Seguro de Hardware (HSM) certificado e que cumpre os requisitos definidos nas normas ETSI.

O perfil do certificado de autenticação de sítios web está de acordo com o conjunto de standards ETSI 319 412 e com as recomendações do CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates.

10.1.1. Número da Versão

O campo "version" do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é 3 (V3).

10.1.2. Extensões do Certificado

As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

10.1.3. Emissão de Certificados de Autenticação de Sítios Web (SSL *Extended Validation*)

Componente do Certificado	Valor	Tipo	Comentários
Version	V3	M	
Serial Number	<atribuído pela EC a cada certificado>	M	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Assinatura de certificado
Issuer		M	
Country (C)	"PT"		
Organization (O)	"ACIN-iCloud Solutions, Lda"		
Organization Unit (OU)	"Global Trusted Sign"		
Common Name (CN)	Global Trusted Sign Certification Authority 001		Nome da Entidade Certificadora responsável pela emissão de certificados de autenticação de sítios web da EC GTS
Validity		M	Validade do Certificado
Valid from	<data de emissão>		
Valid to	<data de emissão + 1 ano>		Validade máxima de 1 ano.
Subject		m	
Country (C)	<País>		País onde se encontra a entidade
Locality Name (L)	<Localidade>		Localidade onde se encontra filiada a Organização
Organization (O)	<Nome da Organização>		Nome legal da Organização
Common Name (CN)	<Fully Qualified Domain Name do Servidor Web >		

PostalCode	<Código postal da Organização>		
STREET	<Morada da Organização>		
STREET	<Localidade relativa ao código postal da organização>		
SERIALNUMBER	<Identificador único da organização>		De acordo com o documento *Guidelines for the Issuance and Management Of Extended Validation Certificates* capítulo 9.2.6: Subject:serialNumber
	<País onde a organização decorre a sua atividade>		De acordo com o documento *Guidelines for the Issuance and Management Of Extended Validation Certificates* capítulo 9.2.5: subject: jurisdictionCountryName
Subject Business Category Field	<Setor de atividade da organização. Valores possíveis são: "*Private Organization*" "*Government Entity*" "*Business Entity*" "*Non-Commercial Entity*">		De acordo com o documento *Guidelines for the Issuance and Management Of Extended Validation Certificates* capítulo 9.2.4: subject:businessCategory
Subject Public Key Info		M	
algorithm	rsaEncryption (OID: 1.2.840.113549.1.1.1)		Algoritmo da chave pública
subjectPublicKey	<Chave Pública>		Chave pública do certificado
Authority Key Identifier		M	
keyID	160 bit hash		Permite identificar a chave pública correspondente à chave privada do certificado
Subject Key Identifier	160 bit hash	M	Identificador da chave do certificado
Key Usage		M	
Digital Signature	"1" selecionado		
Non Repudiation	"0" selecionado		
Key Encipherment	"1" selecionado		
Data Encipherment	"1" selecionado		

Key Agreement	"0" selecionado		
Key Certificate Signature	"0" selecionado		
CRL Signature	"0" selecionado		
Encipher Only	"0" selecionado		
Decipher Only	"0" selecionado		
Certificate Policies		M	
[1]	policyIdentifier: 1.3.6.1.4.1.50302.1.1.2.2.1.0 Policy Qualifier Id=CPS cPSuri: https://pki.globaltrustedsign.com/index.html		Identificador e localização da Declaração de Práticas de Certificação da EC GTS
[2]	Policy Qualifier Id=2.23.140.1.1		Identificador da política de certificados do CA/B Forum para os certificados *Extended Validation*
Subject Alternative Name		O	
GeneralName	DNS=<fully qualified domain name do servidor Web>		Máximo 7 Domínios. Não pode ter domínios *Wildcard*
Basic Constraints		M	Esta extensão é marcada Crítica
Subject Type	End Entity		Certificado destinado a Entidades Finais
PathLenConstraint	None		
Extended Key Usage		M	
KeyPurposeID	Server Authentication		OID 1.3.6.1.5.5.7.3.1
keyPurposeID	Client Authentication		OID 1.3.6.1.5.5.7.3.2
CRLDistributionPoints		M	
[1]	distributionPoint: https://pki.globaltrustedsign.com/subca/gts_subca_crl.crl		Localização da Lista de Revogação de Certificados da EC GTS
[2]	distributionPoint: https://pki02.globaltrustedsign.com/subca/gts_subca_crl.crl		Localização secundária da Lista de Revogação de Certificados da EC GTS

Authority Information Access		M	
accessMethod	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)		Parâmetro usado para identificar o end-point do serviço OCSP
accessLocation	http://ocsp.globaltrustedsign.com/		Localização do serviço OCSP
accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)		Parâmetro usado para identificar o certificado da EC GTS e construir a cadeia de confiança.
accessLocation	https://pki.globaltrustedsign.com/subca/gts_subca.crt		Localização do certificado da EC GTS
Qualified Certificate Statements		M	
id-etsi-qcs-QcCompliance	*<Extensão presente>*		A presença do QCStatement afirma que o certificado é um certificado qualificado emitido de acordo com Regulação Europeia (EU) No 910/2014
id-etsi-qcs-QcType	id-etsi-qcs-QcType 3 Certificate for website authentication defined in Regulation (EU) No 910/2014		Certificado para Autenticação de sítios Web como definido na Regulação Europeia (EU) No 910/2014
Id-etsi-qcs-QcPDS	Id-etsi-qcs-QcPDS en: https://pki.globaltrustedsign.com/index.html pt: https://pki.globaltrustedsign.com/index.html		Este QCStatement contém URLs para declarações de divulgação de princípios EC GTS (PDS)
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	M	Algoritmo usado para a criação da assinatura do certificado
Signature Value	<contém a assinatura digital emitida pela CA>	m	Assinatura do certificado

10.1.4. OID do Algoritmo

O campo "signatureAlgorithm" do certificado contém o OID do algoritmo criptográfico utilizado pela PSQ GTS para assinar o certificado. O algoritmo usado é sha256WithRSAEncryption que tem o OID 1.2.840.113549.1.1.11.

10.1.5. Condicionamento nos Nomes

Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se (mas não se obriga) a que apenas caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') sejam utilizados em entradas do Diretório X.500.

10.1.6. OID e sintaxe da Política de Certificados

A extensão "certificate policies" contém a sequência de um ou mais termos informativos sobre a política, cada um dos quais consiste num identificador da política e qualificadores opcionais.

A sintaxe da sub-extensão "Policy Qualifier" não tem nenhum requisito imposto pelo RFC 3647, no entanto, a EC GTS usa o qualifier cPSuri para indicar o URL das Políticas de Certificados usadas para a emissão de certificados.

A variável opcional Policy Qualified ID (1.3.6.1.5.5.7.2.1) diz respeito ao mecanismo para distribuir mais informação sobre as políticas de certificados.

A variável cPSuri representa um URL onde pode ser encontrada a Política de Certificados de Autenticação de Sítios Web da EC GTS.

10.1.7. Utilização da extensão Policy Constraints

Não aplicável.