SISP – SOCIEDADE INTERBANCÁRIA E SISTEMAS DE PAGAMENTO

POLITICA DE CERTIFICADO

DE

VALIDAÇÃO CRONOLÓGICA DA SISP

Código:	PLRC006
Versão:	1.0
Data da versão:	30/06/2019
Criado por:	SISP
Aprovado por:	Director Geral
Nível de confidencialidade:	PÚBLICO

Histórico das alterações

Data	Versão	Criado por	Descrição da alteração
30/06/2019	1.0	SISP	Criação

Índice

1. INTRODUÇÃO

1.1. Objectivos

O objectivo deste documento é definir o perfil de Certificados de Validação Cronologica emitido pela SISP TSA – SISP Timestamp Authority.

1.2. Publico Alvo

Este documento é público e destina-se a todos quantos se relacionam com a Entidade de Certificação SISP TSA, em particular os Auditores e Colaboradores da SISP.

1.3. Estrutura do documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focados antes de proceder com a leitura do documento.

Este documento complementa a Declaração de Práticas de Validação Cronologica da Entidade Certificadora SISP TSA, presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

2. DOCUMENTOS DE REFERÊNCIA

- Declaração de Pratica de Validação Cronológica

3. CONTEXTO

O presente documento tem como objectivo a definição de um conjunto de parâmetros que definem o perfil dos Certificados de Validação Cronológica emitidos na pela PKI da SISP, permitindo assim garantir a fiabilidade do serviço de Validação Cronológica disponilizado pela SISP. Não se pretende nomear regras legais ou obrigações, mas antes informar pelo que se pretende que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

3.1. Visão Geral

Esta Política satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da SISP TSA.

3.2. Identificação do documento

Este documento constitui a Politica de Certificados de Validação Cronologica da SISP TSA cujo o OID associado é, o 2.16.132.1.2.2.3.1.

É identificado pelos dados constantes na tabela seguinte e, é actualizado sempre que se mostrar necessario:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	2.16.132.1.2.2.3.1
Data de Emissão	30/06/2019
Validade	1 Ano
Localização	https://pki.sisp.cv/

4. IDENTIFICAÇÃO E AUTENTICAÇÃO

4.1. Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela DPC.

O Certificado de Validação Cronológica é identificado por um nome único (DN – Distinguished Name) de acordo com standard X.500.

O nome único do certificado de Validação Cronológica é identificado pelos seguintes componentes:

Atributo	Codigo	Valor
Country	C	CV
Organization	O	ICP-CV
Organization Unit	OU	SISP – Sociedade Interbacaria e Sistemas de Pagamentos
Common Name	CN	Entidade Certificadora de Validação Cronológica da SISP

4.2. Uso do certificado e par de chaves pelo titular

A SISP é a titular do Certificado de Validação Cronológica, sendo o mesmo emitido para a Entidade Certificadora de Validação Cronológica da PKI da SISP. A chave privada associada a este tipo de certificados é utilizada para assinar as respostas a pedidos de validações cronológicas (aposição de selos temporais), garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

5. PERFIL DE CERTIFICADO VALIDAÇÃO CRONOLÓGICA (TSU)

5.1. Perfil de Certificado

O perfil dos certificados de Validação Cronológica está de acordo com os requisitos da ICP-CV e com os seguintes standards:

a) *RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP;*
b) *ETSI EN 419 421 v1.1.1, Policy and Security Requirements for Trust Service Providers issuing*
c) *Time-Stamps;*
d) *ETSI EN 419 422 v1.1.1, Time-stamping protocol and time-stamp profiles;*
e) *RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile;*
f) *Legislação caboverdiana.*

Componente do Certificado	Componente do Certificado	Secção no RFC5280	Valor	Tipo	Comentários
tbsCertificate	**Version**	4.1.2.1	3	m	O valor 3 identifica a utilização de certificados ITU-T X.509 versão 3
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	1.16.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.4	 "CV" "ICP-CV" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" <nome da subca>	m	Designação Oficial da ECVC da SISP
	Validity Not Before Not After	4.1.2.5	 <data de emissão> <data de emissão + 5 anos e 4 meses>	m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralisedTime* Validade maxima de 6 anos.
	Subject Country (C) Organization (O) Organization Unit (OU) Common Name (CN)	4.1.2.6	 "CV" "ICP-CV" "SISP-Sociedade Interbancaria e Sistemas de Pagamentos" "SISP TSA Signer<nn>"	m	Designação Official da TSU da SISP <nnnn> número da TSU
	Select Public Key Info Algorithm subjectPublic Key	4.1.2.7	 1.2.840.113549.1.1.1 <Chave Pública com modulus n de 2048 bits>	m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman). O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.24

	Unique Identifiers	4.1.2.8		m	O “unique identifiers” está presente para permitir a possibilidade de reutilizar os nomes do subject e/ou issuer 20
	X509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier KeyIdentifier	4.2.1.1	O key Identifier é composto pela hash de 160-bit SHA-256 do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	O key Identifier é composto pela hash de 160-bit SHA-256 m do valor da BIT STRING do subjectPublicKey (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage Digital Signature Non Repudiation Key Enciphermen t Data Enciphermen t Key Agreement Key Certificate Signature CRL Signature Encipher Only Decipher Only	4.2.1.3	 “0” seleccionado “1” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado “0” seleccionado	mc	Esta extensão é marcada CRÍTICA
	Cerificate Policies policyIdentifier policyQualifiers	4.2.1.4	 2.16.132.1.3.2.3.1 <policyQualifierID> cPSuri: https://pki.sisp.cv	m m m	Identificador da Declaração de Práticas de Certificação da EC de TSA da SISP (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Declaração de Práticas de Certificação publicada pela SISPTSA. O apontador está na forma de um URL."
	policyIdentifier policyQualifiers		2.16.132.1.2.2.3.1 <policyQualifierID> cPSuri: https://pki.sisp.cv	m m	Identificador da Politica de Certificados da EC de TSA da SISP (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo cPSuri contém um apontador para a Politica de Certificados publicada pela SISPTSA. O apontador está na forma de um URL."

	Qualifiedn Certificate Statement id-qcs-pkixQCSyntax-v2		1.3.6.1.5.5.7.1.3 Id-etsi-tsts-EuQCompliance=”0.4.0.19422.1.1” Text= “By inclusion of this statement the issuer claims that this time-stamp token is issued as a qualified electronic time-stamp ”	m	A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile e ETSI
	CRLDistributionPoints distributionPoint	4.2.1.13	http://crl.sisp.cv/sisptsa.crl	m m	URL para aceder a CRL
	Extended Ket Usage Timestamping	4.2.1.12	1.3.6.1.5.5.7.3.8	c	Descrição do OID: id-kp-timeStamping indica que o certificado é utilizado para ligar um objeto a uma hora e data obtida de uma fonte fiável de tempo
	Internet Certificate Extensions				.
	Authority Information Access accessMethod accessLocation	4.2.2.1	1.3.6.1.5.5.7.48.2 http://ocsp.sisp.cv/	o o o	Esta extensão TEM de ser crítica1. Valor do OID: (id-ad-ocsp) URL para aceder ao OCSP
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 20
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

5.2. Numero da versão

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

5.3. 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.

5.4. OID do Algoritmo

O campo "signatureAlgorithm" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 1.16.840.113549.1.1.11 (sha256WithRSAEncryption).

5.5. Formato dos Nomes

Tal como definido na secção 4.1.

5.6. Condicionamento nos Nomes

Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se a que apenas carateres 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. A utilização de carateres acentuados será da única responsabilidade do Grupo de Trabalho de Gestão da PKI da SISP.

5.7. OID da Politica 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.

Os qualificadores opcionais ("*policyQualifIierID*: 2.16.132.1.2.2.3" e "*cPSuri*") apontam para o URL onde pode ser encontrada a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*" e para o URL desta política, identificado pelo *policyIdentifier*.

5.8. Utilização da extensão Policy Constraints

Nada a assinalar.

5.9. Sintaxe e semantica do qualificador de politica

A extensão "certificate policies" contém um tipo de qualificador de política a ser utilizado pelos emissores dos certificados e pelos escritores da política de certificados. O tipo de qualificador é o "cPSuri" que contém um apontador, na forma de URL, para a Declaração de Práticas de Certificação publicada pela EC e, um apontador, na forma de URL, para a Politica de Certificados.

5.10. Semântica de processamento para a extensão critica Certicate Policies

Nada a assinalar.

6. REFERÊNCIAS BIBLIOGRÁFICAS

[1] ARME, Declaração de Práticas de Certificação da EC Raiz de Cabo Verde.

[2] ARME, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança.

[3] Portaria nº 2/2008, de 28 de Janeiro;

[4] Decreto-Lei nº44/2009 de 9 de Novembro;

[5] Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;

[6] Decreto-Lei nº 33 /2007, de 24 de Setembro;

[7] Portaria nº 4/2008

[8] FIPS 140-2. 1994, *Security Requirements for Cryptographic Modules.*

10] ETSI EN 419 421 v1.1.1, *Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*

[11] ETSI EN 419 422 v1.1.1, *Time-stamping protocol and time-stamp profiles*

[12] RFC 3161. 2001, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).*

[13] RFC 3628. 2003, *Policy Requirements for Time-Stamping Authorities (TSAs).*