Consulta Pública 01/2024

Modernização da ICP-Brasil

Janeiro de 2024

Após a realização de diversas reuniões, no final do ano de 2023, para apresentação e debate acerca de temas para modernização da ICP-Brasil, o ITI lança esta consulta pública como ferramenta para contribuição ampla a respeito das ideias aqui apresentadas.

Com o objetivo de padronizar os processos de identificação eletrônica de pessoas físicas e jurídicas, bem como estabelecer normas aplicáveis aos serviços de confiança, a União Europeia estabeleceu o Regulamento (UE) Nº 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, também conhecido como eIDAS (*Electronic Identification and Trust Services*).

Essa regulamentação apresenta conceitos, regras de interoperabilidade e requisitos de segurança para serviços de confiança, notadamente, certificados digitais de assinatura e selo eletrônico. Como se observa, o regulamento tem similaridades com as práticas estabelecidas na ICP-Brasil, já tendo inclusive servido de base para o aperfeiçoamento normativo da própria ICP-Brasil, como foi o caso da implementação da Lista de Prestadores de Serviços de Confiança (LPSC), que tomou como base as Listas de Confiança implementadas seguindo os requisitos do eIDAS na União Europeia.

Entre as implementações propostas no eIDAS e ainda não implementadas da ICP-Brasil está a utilização dos selos eletrônicos, os quais devem garantir a origem e a integridade de um documento eletrônico, servindo de prova da emissão do documento por uma determinada pessoa jurídica. Selo eletrônico é semelhante ao certificado de assinatura eletrônica, com a diferença de ser utilizado apenas por pessoas jurídicas e não ter um titular designado, sendo considerado análogo a um carimbo físico.

No esboço da discussão sobre a implementação do selo eletrônico, considerando a necessidade de alinhamento com a prática internacional e objetivando simplificar e deixar mais claro o perfil dos diferentes tipos de certificado, o debate passou a incluir novos tipos de certificados digitais no âmbito da ICP-Brasil, assim como a revisão dos tipos já estabelecidos.

Nesse contexto, insere-se a proposta de alteração normativa que visa a extinção de certificado de assinatura de pessoa jurídica, uma vez que se entende que um ente pessoa jurídica sempre será representado, conforme os poderes estabelecidos, por uma ou mais pessoas físicas. Além disso, a obrigatoriedade de haver um responsável pelo uso do certificado, pessoa física, associado dentro do certificado de PJ, induz poderes de representação a esse responsável que nem sempre condiz com o objetivo ou adequação de uso do certificado.

A AC Raiz da ICP-Brasil propõe, dessa maneira, a implementação do certificado digital de selo eletrônico em substituição ao certificado do tipo A1, com emissão exclusiva em hardware e para pessoa jurídica, mantendo o certificado de assinatura do tipo A3, que passa a ser de emissão apenas para pessoa física.

A proposta institui, também, o certificado digital do tipo SSL/TLS *Webtrust*, para atendimento exclusivo aos requisitos *Webtrust*; o certificado digital de aplicações especiais em software; e o certificado digital de aplicações especiais em hardware. Sendo os dois últimos destinados ao uso em equipamentos, servidores, aplicações e dispositivos IOT.

Somadas à proposta de simplificação e adequação normativa, as estatísticas de emissão de certificados dos últimos anos apresentam dados que colocam em evidência a necessidade de extinção do certificado do tipo A2, cuja última emissão ocorreu em 2016, dos certificados de sigilo (S1 a S4), que somam apenas 9 emissões desde 2020, e do A3 para pessoa jurídica, que não chegou a 4% do total de emissões neste ano de 2023.

Visando a simplificação dos perfis de certificados, vislumbra-se a desobrigação de alguns campos *otherName* e a extinção de outros, como, por exemplo, os correspondentes aos dados de pessoa física em certificado emitido para pessoa jurídica. Além disso, muitos campos *otherName* trazem qualificações dos titulares, não identificando esses. As ACs emissoras não possuem competência para gestão desses qualificadores.

A seguir são apresentadas:

Tabela com a proposta de tipos de certificado ICP-Brasil e os respectivos propósitos de uso;

Tabela com a indicação das mídias armazenadoras de chaves criptográficas e prazos de validade dos certificados; e

Tabela com a estatística de emissão de certificados ICP-Brasil desde 2010.

Proposta de tipos de certificado ICP-Brasil

Tipo de Certificado	OID	Propósito de Uso
~~**Assinatura Digital - A1**~~	~~2.16.76.1.2.1.*n*~~	Confirmação de identidade e assinatura de documentos eletrônicos com verificação de autoria e integridade de suas informações.
~~**Assinatura Digital - A2**~~	~~2.16.76.1.2.2.*n*~~	
Assinatura Digital - A3	2.16.76.1.2.3.*n*	
Assinatura Digital - A4	2.16.76.1.2.4.*n*	
~~**Sigilo - S1**~~	~~2.16.76.1.2.101.*n*~~	Cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.
~~**Sigilo - S2**~~	~~2.16.76.1.2.102.*n*~~	
~~**Sigilo - S3**~~	~~2.16.76.1.2.103.*n*~~	
~~**Sigilo - S4**~~	~~2.16.76.1.2.104.*n*~~	
Selo Eletrônico - SE	2.16.76.1.2.203.*n*	Garantia de origem e integridade de um documento eletrônico, servindo de prova da emissão do documento por uma pessoa jurídica.
Carimbo do tempo - T3	2.16.76.1.2.303.*n*	Assinatura de carimbos do tempo de ACT.
Carimbo do tempo - T4	2.16.76.1.2.304.*n*	
Aplicações Especiais em Software - AE-S	2.16.76.1.2.401.*n*	Uso em equipamentos, servidores, aplicações e dispositivos IOT.
Aplicações Especiais em Hardware - AE-H	2.16.76.1.2.402.*n*	
Cupom Fiscal Eletrônico - A CF-e-SAT	2.16.76.1.2.500.*n*	Assinatura de Cupom Fiscal Eletrônico – CF-e.
Objeto Metrológico - OM-BR	2.16.76.1.2.550.*n*	Uso exclusivo em equipamentos metrológicos regulamentados pelo Inmetro.
SSL/TLS Webtrust	-	Autenticação de servidores e aplicações em ambiente Web, de acordo com os princípios e critérios WebTrust.

Mídias armazenadoras de chaves criptográficas e prazos de validade dos certificados

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)	Período Máximo de Validade do Certificado (em anos)
~~**A1 e S1**~~	~~Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima~~	~~1~~
AE-S	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima	1
~~**A2 e S2**~~	~~Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica~~	~~2~~
A3, ~~S3~~, T3 e SE	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO	5
A4, ~~S4~~, T4 e AE-H	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO	11 (para cadeias hierárquicas completas em Curvas Elípticas) 6 (para as demais hierarquias)
A CF-e-SAT	Hardware criptográfico.	5
OM-BR	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO	10
SSL/TLS WebTrust	Conforme os princípios e critérios **Webtrust**	Conforme os princípios e critérios **Webtrust**

Emissão de certificados ICP-Brasil desde 2010

ANO	A1_pf	A1_pj	A1_eqp	A2_pf	A2_pj	A2_eqp	A3_pf	A3_pj	A4_pf	A4_pj	A4_ eqp	S1_pf	S1_pj	S1_eqp	S2_pf	S2_pj	S2_eqp	S3_pf	S3_pj	S3_eqp	S4_pf	S4_pj	S4_eqp	T3	T4	Total Ano
2010	31.098	276.318	1.518	-	-	1	388.122	506.434	7	-	1	-	288	4	-	-	-	-	299	1	-	-	-	-	-	1.204.095
2011	50.657	503.242	2.293	-	1	21	428.130	952.810	2	1	2	-	44	4	-	-	-	-	22	1	-	2	2	-	-	1.937.269
2012	79.755	629.435	2.422	-	-	-	460.242	932.587	11	-	-	-	22	1	-	-	-	-	2	1	-	-	-	2	-	2.107.224
2013	79.862	694.092	2.484	3	-	-	634.612	818.314	37	-	-	-	8	-	-	-	-	-	10	2	-	-	-	9	1	2.229.434
2014	111.687	884.284	3.798	-	-	-	596.345	957.618	11	-	-	1	2	-	-	-	-	-	3	-	-	-	-	15	-	2.553.764
2015	145.109	1.088.277	4.111	10	-	-	976.470	1.062.689	21	-	-	1	-	1	-	-	-	-	1	-	-	-	-	3.847	-	3.280.537
2016	154.713	1.225.257	4.040	4	-	-	953.485	888.939	16	-	-	2	-	1	-	-	-	-	-	-	-	-	-	7	-	3.226.464
2017	178.764	1.485.778	3.372	-	-	-	977.248	944.985	21	1	-	-	-	2	-	-	-	-	1	-	-	-	-	5	-	3.590.177
2018	281.591	2.026.902	4.141	-	-	-	1.106.968	997.485	15	-	-	3	-	1	-	-	-	-	1	-	-	-	-	6	-	4.417.122
2019	701.779	2.516.706	3.491	-	-	-	1.432.128	819.120	13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	12	-	5.494.826
2020	1.357.685	3.026.579	2.477	-	-	-	1.055.319	589.373	92	-	-	-	2	-	-	-	-	-	1	-	-	-	-	7	-	6.071.145
2021	1.855.109	3.783.736	1.619	-	-	-	1.256.520	577.587	527	-	-	1	-	-	-	-	-	-	1	-	-	-	-	5	-	7.494.841
2022	2.111.206	4.506.451	879	-	-	-	1.415.274	435.752	224	-	2	-	-	-	-	-	-	-	-	3	-	-	-	9	-	8.486.225
2023	1.304.755	2.965.352	622	-	-	-	817.920	211.310	1	-	-	-	-	-	-	-	-	-	1	-	-	-	-	16	-	5.304.775
Total	**8.455.031**	**25.631.436**	**37.380**	**17**	**1**	**22**	**12.528.032**	**10.701.685**	**998**	**2**	**5**	**8**	**366**	**14**	**-**	**-**	**-**	**-**	**342**	**8**	**-**	**2**	**2**	**3.940**	**1**	**57.464.230**