PROCEDIMENTOS OPERACIONAIS MÍNIMOS PARA OS

PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL

PSC VALID

Versão 1.0
Junho de 2019

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprova a alteração	Item Alterado	Descrição da Alteração
1.0	26/06/2019	Não se Aplica	Não se aplica	Criação do Requisitos Operacionais Mínimos do Prestador de Serviço de Confiança – PSC VALID – Versão 1.0

LISTA DE ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo de Tempo
AES	Advanced Encryption Standard
APF	Administração Pública Federal
CAdES	CMS Advanced Electronic Signature
CTR	Counter Mode
DPPSC	Declaração de Prática do Prestador de Serviço de Confiança
EAT	Entidade de Auditoria do Tempo – ICP-Brasil
ETSI	European Telecommunications Standards Institute
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-Based One-Time Password
HSM	Hardware Security Module
HTTPS	Hyper Text Transfer Protocol Secure
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IETF	Internet Engineering Task Force
ITI	Instituto Nacional de Tecnologia da Informação
KMIP	Key Management Interoperability Protocol
LPA	Lista de Políticas de Assinatura Aprovadas
LPSC	Lista de Prestadores de Serviço de Confiança
OATH	Open Authentication
PAdES	PDF Advanced Electronic Signature

PCO	Planejamento de Capacidade Operacional
PIN	Personal Identification Number
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PKCS	Public Key Cryptography Standards
PUK	PIN Unlock
RFC	Request for Comments
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOTP	Time-based One-Time Password algorithm
TRC	Teorema do Resto Chinês
TTLV	Tag, type, length, value
XAdES	XML Advanced Electronic Signatures
XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

1. DISPOSIÇÕES GERAIS

1.1. Este documento tem por finalidade regulamentar os requisitos mínimos de segurança e os procedimentos operacionais a serem adotados pelos Prestadores de Serviço de Confiança Valid (PSC VALID).

A estrutura deste documento está baseado no DOC - ICP - 17[12] e no DOC - ICP - 17.01[10]. As referências a formulários presentes neste documento deverão ser estendidos também como referências a outras formas que o PSC VALID ou entidades vinculadas a ela possam vir a adotar.

1.2. Suplementa, para o PSC VALID, os regulamentos contidos nos documentos DOC-ICP-03 [1], DOC-ICP-04 [2], DOC-ICP-08 [3] e DOC-ICP-09 [4], tomando como base também a Política de Segurança da ICP-Brasil – DOC-ICP-02 [5].

1.3. Os requisitos contidos neste documento foram apresentados quando do credenciamento do PSC VALID para armazenamento de chaves privadas dos usuários finais ou serviços de assinaturas digitais, verificação de assinaturas digitais, se for o caso, ou ambos e mantidos atualizados durante seu funcionamento enquanto estiver credenciada na ICP-Brasil.

1.4. O PSC VALID possui uma Política de Segurança da Informação composta por diretrizes, normas e procedimentos que descrevem os controles de segurança que devem ser seguidos em suas dependências e atividades, em consonância com o DOC-ICP-02 [5].

1.5. Um exemplar da Política de Segurança da Informação, no formato impresso, está disponível para consulta no Nível 1 (vide regulamento no item 3) de segurança do PSC VALID.
1.6. A Política de Segurança da Informação do PSC VALID é seguida por todo pessoal envolvido nas atividades realizadas pelo PSC, do seu próprio quadro ou contratado.

1.7. Este documento define normas operacionais e de segurança que devem ser aplicadas nas áreas internas do PSC VALID, assim como no trânsito de informações, armazenamento de chaves privadas, serviços de assinatura digital e verificação de assinatura digital e materiais com entidades externas.

1.8. A seguir são informados os requisitos que devem ser observados quanto a segurança de pessoal, segurança física, segurança lógica, segurança de rede, requisitos mínimos para armazenamento de chaves privadas, serviços de assinatura digital e verificação de assinatura digital, classificação da informação, salvaguarda de ativos da informação, gerenciamento de riscos, plano de continuidade de negócios, análise de registros de eventos e plano de capacidade operacional.

2. SEGURANÇA PESSOAL

2.1 O PSC VALID possui uma Política de Gestão de Pessoas que dispõe sobre os processos de contratação, demissão, descrição de cargos, avaliação de desempenho e capacitação.

2.2 A comprovação da capacidade técnica do pessoal envolvido nos serviços prestados pelo PSC VALID está à disposição para eventuais auditorias e fiscalizações.

2.3 Todo pessoal envolvido nas atividades realizadas pelo PSC VALID, do próprio quadro ou contratado, realiza a assinatura de um termo, com garantias jurídicas, que garante o sigilo das informações internas e de terceiros, mesmo após a demissão ou o término do contrato.

2.4 O termo de sigilo da informação possui cláusula explícita de responsabilização nos casos de quebra de regras ou regulamentos da ICP-Brasil.

2.5 Aplicar-se-á o termo de sigilo de informações a quaisquer outras entidades que porventura tenham acesso às informações internas e de terceiros originárias dos projetos coordenados pelo PSC VALID.

2.6 O PSC VALID possui procedimentos formais de apuração e responsabilização em caso de descumprimento das regras estabelecidas pelas suas políticas ou pelas normas da ICP-Brasil.

2.7 O quadro de pessoal do PSC VALID e contratados possui um dossiê contendo os seguintes documentos:

a) Contrato de trabalho ou cópia das páginas da carteira de trabalho onde conste o registro da contratação, termo de posse de servidor ou comprovante de situação funcional;
b) Comprovante da verificação de antecedentes criminais;
c) Comprovante da verificação de situação de crédito;
d) Comprovante da verificação de histórico de empregos anteriores;
e) Comprovação de residência;
f) Comprovação de capacidade técnica;
g) Resultado da entrevista inicial, com a assinatura do entrevistador;
h) Declaração em que afirma conhecer as suas atribuições e em que assume o dever de cumprir as regras aplicáveis da ICP-Brasil;
i) Termo de sigilo.

2.8 Não serão admitidos estagiários no exercício fim das atividades do PSC.

2.9 Quando do desligamento, o referido dossiê contém os seguintes documentos:

a) Evidências de exclusão dos acessos físico e lógico nos ambientes do PSC VALID;

b) Declaração assinada pelo empregado ou servidor de que não possui pendências, conforme previsto no item 7.3.10 do DOC-ICP-02 [5].

3. SEGURANÇA FÍSICA

3.1. Disposições Gerais de Segurança Física

3.1.1. Níveis de acesso

3.1.1.1. São definidos pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes do PSC VALID.

3.1.1.1.1. O primeiro nível – ou nível 1 – situar-se após a primeira barreira de acesso às instalações do PSC. O ambiente de nível 1 desempenha a função de interface com cliente ou fornecedores que necessitam comparecer ao PSC.

3.1.1.1.2. O segundo nível – ou nível 2 – é interno ao primeiro e requer a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo do PSC. A passagem do primeiro para o segundo nível exige a identificação por meio eletrônico e o uso de crachá. Especificações nível 2:

a) O ambiente de nível 2 é separado do nível 1 por paredes divisórias de alvenaria. Não existem janelas qualquer outro tipo de abertura para o exterior, exceto a porta de acesso;

b) O acesso a este nível é permitido apenas às pessoas que trabalhem diretamente com as atividades de serviços de armazenamento dos certificados para usuários finais, serviços de assinatura digital e verificação da assinatura digital ou ao pessoal responsável pela manutenção de sistemas e equipamentos do PSC como administradores de rede e técnicos de suporte de informática. Demais funcionários do PSC VALID ou do possível ambiente que esta compartilhe não acessam este nível;

c) Preferencialmente, nobreaks, geradores e outros componentes da infraestrutura física deverão estar abrigados neste nível, para evitar acessos ao ambiente de nível 3 por parte de prestadores de serviços de manutenção;

d) Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do PSC a partir do nível 2;

3.1.1.1.3. O terceiro nível – ou nível 3 é o primeiro nível a abrigar material e atividades sensíveis da operação do PSC VALID. Qualquer atividade relativa ao armazenamento de certificados digitais dos usuários, serviços de assinatura digital e verificação da assinatura digital é realizada a partir deste nível, onde somente pessoas autorizadas podem permanecer. Especificações nível 3:

a) No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: senha individual e identificação biométrica;

b) As paredes que delimitam o ambiente de nível 3 são constituídas de alvenaria e não possui forro ou pisos falsos. Não existem janelas ou qualquer outro tipo de abertura para o exterior, exceto a porta de acesso;

c) Existe uma porta única de acesso ao ambiente de nível 3, que abre somente depois que o funcionário tenha se autenticado eletronicamente no sistema de controle de acesso. A porta é dotada de dobradiças que permitam a abertura para o lado externo, de forma a facilitar a saída e dificultar a entrada no ambiente, bem como de mecanismo para fechamento automático, para evitar que permaneça aberta mais tempo do que o necessário.

3.1.1.1.4. Não se aplica.

3.1.1.1.5. O quarto nível – ou nível 4 – interior ao terceiro, é onde ocorrem todas as atividades especialmente sensíveis da operação do armazenamento de chaves e de assinatura digital do PSC VALID. Todos os sistemas e equipamentos necessários a essas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas, onde a permanência delas é exigida enquanto o ambiente estiver ocupado.

3.1.1.1.6. No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esse ambiente de nível 4 – que constitui a chamadas sala cofre - possui proteção contra interferência eletromagnética externa.

3.1.1.1.7. A sala-cofre foi construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

3.1.1.2. Poderão existir no PSC VALID vários ambientes de quarto nível para abrigar e segregar, quando for o caso:

a) Equipamentos de produção on-line; e

b) Equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

3.1.1.3. Todos os servidores e elementos de infraestrutura e proteção do segmento de rede, tais como roteadores, hubs, switches e firewalls:

a) Operam em ambiente com segurança equivalente, no mínimo, ao quarto nível citado neste documento;

b) Possuem acesso lógico restrito por meio de sistema de autenticação e autorização de acesso.

3.1.1.4. O PSC VALID atende aos seguintes requisitos:

a) O ambiente físico do PSC VALID possui dispositivos que autêntica e registra o acesso de pessoas informando data e hora desses acessos;

b) O PSC VALID possui imagens que garantam a identificação de pessoas quando do acesso físico em qualquer parte de seu ambiente;

c) Realiza mandatoriamente o sincronismo de data e hora entre os mecanismos de segurança física, garantindo a trilha de auditoria entre dispositivos de controle de acesso físico e de imagem;

d) Todos que transitam no ambiente físico do PSC VALID portam crachás de identificação, inclusive os visitantes;

e) Só é permitido o trânsito de material de terceiros pelos ambientes físicos do PSC VALID mediante registro, garantindo a trilha de auditoria com informações de onde o material passou, a data e hora que ocorreu o trânsito e quem foi o responsável por sua manipulação;

f) O PSC VALID possui dispositivos de prevenção e controle de incêndios, temperatura, umidade, iluminação e oscilação na corrente elétrica em todo seu ambiente físico;

g) Todo material crítico inservível, descartável ou não mais utilizável recebe tratamento especial de destruição, garantindo o sigilo das informações lá contidas. O equipamento enviado para manutenção tem seus dados apagados, de forma irreversível, antes de ser retirado do ambiente físico do PSC VALID;

h) Os computadores pessoais, servidores e dispositivos de rede, e seus respectivos softwares, são inventariados com informações que permitam a identificação inequívoca;

i) Em caso de inoperância dos sistemas automáticos, o controle de acesso físico é realizado provisoriamente por meio de um livro de registro onde constam os dados de quem acessou, a data, hora e o motivo do acesso;

j) O PSC VALID possui mecanismos que garantem a continuidade do fornecimento de energia nas áreas críticas, mantendo os ativos críticos de informação em funcionamento até que todos os processos e dados sejam assegurados caso o fornecimento de emergência se esgote;

l) Para armazenamento de chaves privadas para usuários finais, o PSC VALID possui

dois ambientes físicos, sendo obrigatoriamente um para operação e outro para contingência;

m) O PSC VALID utiliza o nível 4 da AC VALID, Integrante da ICP-Brasil, para abrigar o hardware criptográfico que armazena as chaves privadas dos usuários finais, assim como os serviços de autenticação. Este equipamento está armazenado em gabinete cadeado, cuja chave do cadeado está em posse de funcionário distinto dos perfis lógicos do PSC, segregados dos que operam o ambiente da AC;

n) Todos os equipamentos e ambiente computacional utilizados no PSC possuem sua data e horário sincronizados com a EAT.

4. SEGURANÇA LÓGICA

4.1 O acesso lógico ao ambiente computacional do PSC VALID se dá, no mínimo, mediante usuário individual e senha, que deve ser trocada periodicamente;

4.2 Todos os equipamentos do parque computacional possuem controle de forma a permitir somente o acesso lógico a pessoas autorizadas;

4.3 Os equipamentos possuem mecanismos de bloqueio de sessão inativa;

4.4 O PSC VALID possui explicitamente a política de cadastro, suspensão e remoção de usuários em seu ambiente computacional. Os usuários estão cadastrados em perfis de acesso que permite privilégio mínimo para realização de suas atividades;

4.5 Os usuários especiais (a exemplo do root e do administrador) de sistemas operacionais, do hardware criptográfico, do banco de dados e de aplicações em geral possuem senhas segregadas de forma que o acesso lógico a esses ambientes se dá por, pelo menos, duas pessoas autorizadas;

4.6 Todo equipamento do PSC VALID possui log ativo e seu horário sincronizado com uma fonte confiável de tempo da ICP-Brasil;

4.7 As informações como log, trilhas de auditoria (do armazenamento de chaves privadas e serviço de assinatura), registros de acesso (físico e lógico) e imagens possuem cópia de segurança cujo armazenamento é de 6 anos;

4.8 Os softwares dos sistemas operacionais, os antivírus e aplicativos de segurança são mantidos atualizados;

4.9 É vedado qualquer tipo de acesso remoto dos operadores do PSC VALID ao ambiente de nível 3.

5. SEGURANÇA DE REDE

5.1 O tráfego das informações no ambiente de rede possui proteção contra danos ou perdas, bem como acesso, uso ou exposição indevidos;

5.2 Não são admitidos acessos externos à rede interna do PSC VALID. As tentativas de acessos externo são inibidas e monitoradas por meio de aplicativos que criam barreiras e filtros de acesso, assim como mecanismos de detecção de intrusão;

5.3 5.3 O PSC VALID aplica testes de segurança na rede interna e externa com aplicativos especializados com periodicidade de, no mínimo, uma vez a cada mês. Os testes na rede são documentados e as vulnerabilidades detectadas corrigidas.

6. REQUISITOS PARA ARMAZENAMENTO DE CHAVES PRIVADAS

6.1. Armazenamento das chaves e certificados digitais

6.1.1 As chaves privadas dos usuários finais, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em hardware criptográficos, estão armazenadas dentro dos espaços (slots), ou equivalente, da fronteira criptográfica e segurança física de um HSM com certificação Inmetro válida no âmbito da ICP-Brasil, endereçados por conta de usuário;

6.1.2 Esse acesso ou comando de exportação às chaves privadas dos usuários é de uso, conhecimento e controle exclusivo do titular, sem a possibilidade de ingresso por outros titulares no mesmo HSM, qualquer funcionário do PSC VALID ou dependentes de outras chaves criptográficas;

6.1.3. O PSC VALID provê mecanismos de duplo fator de autenticação ao titular para acesso à chave privada, sendo um fator dentro da fronteira criptográfica do HSM e outro dentro do ambiente seguro e primeira interface de comunicação com HSM ou ambos dentro da fronteira criptográfica do HSM. Cada fator possui uma classe diferente (conhecimento, posse ou biometria). Os mecanismos de autenticação empregam método ou protocolo de validação que realiza a proteção da transmissão e dos dados de

autenticação por meio de criptografia. Essa funcionalidade é apensada aos requisitos técnicos na manutenção da homologação dos HSM e são:

a) Senhas (PIN/PUK): segundo regras da ICP-Brasil;

b) OTP: segundo regras da RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP);

c) Biometria: segundo regras da ICP-Brasil;

d) Certificado de atributo: segundo regras da ICP-Brasil;

e) *Push Notification:* segundo regras do XMPP *extension protocol* ou semelhante;

f) Outras autenticações semânticas em acordo com o DOC-ICP-17.01 [12] e previamente aprovadas pela AC Raíz.

6.1.4 O PSC VALID realiza, em outro ambiente físico de contingência, a cópia das chaves dos usuários finais, observados os mesmos requisitos de armazenamento do ambiente principal. A entrada do ambiente de contingência ocorre em até 48 horas.

6.1.5 Os espaços para armazenamento das chaves privadas dos usuários finais são liberados, desde que não haja renovação por parte do mesmo ou a revogação da chave, entretanto, são mantidos os registros de armazenamento das chaves conforme Declaração de Prática do Prestador de Serviço de Confiança VALID– DPPSC VALID.

6.2 Protocolos

6.2.1 Os HSMs certificados na ICP-Brasil SUPORTAM a interface PKCS#11, atendendo às exigências de especificação da ICP-Brasil, além dos relatados nesse documento, os seguintes requisitos:

a) Gerar chaves simétricas especificando os componentes de chaves simétricas em texto claro;

• Gerar par de chaves especificando os componentes de chaves assimétricas em texto claro. Por exemplo os componentes Módulo, Expoente público, tamanho em bits, etc;

• Gerar objeto de chaves especificando os componentes de chaves assimétricas (no mínimo chave pública) em texto claro. Por exemplo os componentes: Módulo, Expoente público, Expoente Privada em forma reduzida ou em forma de TRC (Teorema de Resto Chinês);

• Cifrar e decifrar chaves especificando os componentes de chaves simétricas ou assimétrica em texto claro;

• Exportar e importar chaves (PKCS#12) especificando os componentes de chaves assimétricas privadas criptografados;

• Assinar conteúdo especificando os componentes de chaves assimétricas públicas em texto claro;

• Verificar assinatura especificando os componentes de chaves assimétricas públicas em texto claro.

b) O módulo criptográfico suportam as seguintes chamadas de PKCS#11 (Cryptoki):

- C_Initalize
- C_Finalize
- C_OpenSession
- C_CloseSession
- C_Init_Token
- C_Init_PIN
- C_Login
- C_Logout
- C_CreateObject
- C_DestroyObject
- C_GetAttributeValue
- C_SetAttributeValue
- C_EncryptInit
- C_Encrypt
- C_DecryptInit
- C_Decrypt
- C_DigestInit
- C_Digest
- C_DigestKey
- C_SignInit
- C_Sign
- C_VerifyInit
- C_Verify
- C_GenerateKey
- C_GenerateKeyPair
- C_DeriveKey
- C_GenerateRandom
- C_WrapKey
- C_UnwrapKey

c) É obrigatória a implementação das seguintes funções:

• C_GenerateKey especificando templates de chaves simétricas;

• C_GenerateKeyPair especificando templates de chaves assimétricas;

• C_Sign para realizar assinatura de um conteúdo;

• C_Verify para verificar a assinatura de um conteúdo;

• C_Encrypt para cifrar um dado com uma chave já construída;

• C_Decrypt para decifrar um dado com uma chave já construída;

• C_CreateObject especificando templates de chaves assimétricas (no mínimo chave pública);

• C_DestroyObject especificando o handle do objeto.

6.2.2 Os HSMs utilizados pelo PSC VALID utilizam o protocolo Key Management Interoperability Protocol – KMIP, versão 1.3 ou superior, devendo seguir, além dos relatados nesse documento, os seguintes requisitos:

6.2.2.1 O PSC VALID um conjunto de operações que se aplicam aos objetos gerenciados, relacionados ao conjunto normativo do PSC e ao ciclo de vida das chaves, que por sua vez consistem em atributos, como mostrado, em exemplo, na tabela a seguir:

Operações do Protocolo	Objetos Gerenciados	Atributos dos Objetos
Create	Certificate	Unique Identifier
Create Key Pair	Symmetric Key	Name
Register	Public Key	Object Type
Re-key	Private Key	Cryptographic Algorithm
Derive Key	Split Key	Cryptographic Length
Certify	Secret Data	Cryptographic Parameters
Re-certify	Key Block (para chaves) ou Value (para certificados)	Certificate Type
Locate		Certificate Issuer
Check		Certificate Subject
Get		Digest
Get Attributes		Operation Policy Name
Get Attribute List		Cryptographic Usage Mask
Add Attribute		Lease Time
Modify Attribute		Usage Limits

Delete Attribute		State
Obtain Lease		Initial Date
Get Usage Allocation		Activation Date
Activate		Process Start Date
Revoke		Protect Stop Date
Destroy		Deactivation Date
Archive		Destroy Date
Recover		Compromise Occurrence Date
Validate		Compromise Date
Query		Revocation Reason
Cancel		Archive Date
Poll		Object Group
		Link
		Application Specific ID
		Contact Information
		Last Change Date
		Custom Attribute

6.2.2.2 Os objetos base são:

a) Os componentes dos objetos gerenciados.

i. Atributo: identificado pelo seu nome;

ii. Key Block, contém o valor da chave;

b) Os elementos do protocolo de mensagens;

c) Os parâmetros das operações.

6.2.2.3 Os objetos criptográficos gerenciáveis são:

a) Certificado, com o tipo e valor;

b) Chave simétrica, com o Key Block;

c) Chave Pública, com o Key Block;

d) Chave Privada, com o Key Block;

e) Chave Dividida, com o par e o Key Block;

f) Dados Reservados, com o tipo e o Key Block.

6.2.2.4 Os atributos contêm os metadados de um objeto gerenciável, nos quais:

a) Número identificador único, estado, entre outros;

b) Os atributos devem ser pesquisados com a operação “locate”.

6.2.2.5 Os atributos são configurados, modificados e apagados quando a especificação KMIP permitir esses pelo cliente.

6.2.2.6 Os valores das estruturas de codificações (TTLV, definição dos valores, Text String, Structure, Byte String, Integer, Big Integer, Long Integer, Boolean, Date-Time e Enumerations), dos campos dos objetos, dos atributos, dos formatos e conteúdo das mensagens, da manipulação de erros e dos parâmetros (solicitação e resposta) das operações cliente/servidor devem seguir integralmente o estabelecido neste documento e no Key Management Interoperability Protocol Specification Version 1.3, OASIS Standard, 27 December 2016, ou versionamento superior.

NOTA 1: O ITI poderá requisitar aos PSC VALID em credenciamento ou credenciados testes dos modelos descritos, ou outras versões, nos sítios https://www.snia.org/forums/ssif/kmip, http://docs.oasisopen.org/kmip/profiles/v1.3/csd01/kmip-profiles-v1.3-csd01.html ou equivalente.

6.2.2.11 As soluções do PSC VALID devem garantir a portabilidade da chave privada do usuário conforme o descritivo:

a) Glossário:

CPrUi: Chave privada do usuário 'i', armazenada no HSM 1, a ser exportada e importada para o HSM 2; CPrHe 2 : Chave privada do HSM 2, a ser utilizada para importação de chaves privadas de usuários gravadas no HSM 1;

CPuHe 2 : Chave Pública do HSM 2, utilizada para exportação de chaves privadas de usuários armazenadas no HSM 1, a serem importadas pelo HSM 2.

CPuHe 2 deve ser armazenada no repositório do ITI, seguindo procedimentos já estabelecidos (CPuHe 2 pode ser transformada em um certificado digital;

CSi: Chave simétrica a ser gerada pelo HSM 1, para exportação da chave privada do usuário 'i', CPrUi. CSi é utilizada para cifração da chave privada do usuário 'i';

Algos: Algoritmo criptográfico simétrico, de sigilo, pode ser o AES ou Serpent, com modo de operação CTR e tamanho de chave 256 bits.

b) Usuário deve solicitar, assinando digitalmente, uma requisição, que estará disponível no sítio do PSC VALID, de portabilidade de sua chave privada, de exportação no PSC atual e de importação no PSC de destino.

c) Os PSCs receberão essa requisição e autorizarão essa portabilidade com os três perfis (administrador, auditor e operador). Assim que receber a autorização do usuário, PSC 1 e PSC 2 devem iniciar os procedimentos de exportação e importação.

d) Os PSCs devem estabelecer uma conexão ponta a ponta em um canal seguro de comunicação (HTTPS com dupla autenticação por certificado digital ICP-Brasil).

e) Modo Operacional:

i. Procedimentos preliminares:

[a] Cada PSC gera um par de chaves ([CPuHe , CPrHe] - pública e privada) em cada um de seus HSMs. Este par tem como propósito prover portabilidade entre HSMs de quaisquer PSCs. Este par de chaves deve ser utilizado em possível exportação de chaves privadas de usuário, CprUi e também na assinatura das requisições para envelopamento utilizando a sua chave pública. Por analogia, para a chave CPuHe, 'C' significa 'Chave', Pu chave Pública, e He significa chave gerada pelo HSM para exportação de chave do usuário 'i', CPrUi. De forma similar, CPrHe e CPrUi têm significados equivalentes;

[b] CPuHe é armazenada em repositório do ITI, e CPrHe é mantida no HSM de origem;

ii. Para Exportação de chaves privadas dos usuários contidas no HSM 1 para o HSM 2:

[c] No PSC VALID importa-se para o HSM 1 a chave pública do HSM 2, CPuHe 2 , do repositório do ITI;

[d] No HSM 1 gera-se uma chave de sessão simétrica, CSi, distinta, para cada chave privada de usuário a ser exportada; [e] No HSM 1 cifra-se a chave simétrica, CSi, com a chave pública do HSM 2, CPuHe 2 , de destino, para exportação da chave do usuário 'i', CPrUi;

[e] No HSM 1 cifra-se a chave simétrica, CSi, com a chave pública do HSM 2, CPuHe 2 , de destino, para exportação da chave do usuário 'i', CPrUi;

[f] No HSM 1 cifra-se a chave privada do usuário 'i', CPrUi, antes do procedimento de exportação de chaves, com a chave simétrica gerada, CSi, com o algoritmo de sigilo padrão AES ou Serpent, com o modo de operação CTR e tamanho de chave de 256 bits;

[g] No HSM 1 apaga-se cada chave de sessão simétrica gerada, CSi, após o procedimento de cifração do item 'f' ter sido executado;

[h] Após a cifração da chave privada do usuário 'i', CPrUi, ter sido realizada com sucesso, exporta-se essa chave, e a chave Csi cifrada, para o HSM 2;

iii. Para importação de chaves privadas dos usuários contidas no HSM 1 para o HSM 2:

[i] O administrador do HSM 2, de destino, cria novo usuário e o habilita;

[j] O usuário importa do HSM 1 sua chave privada e a chave simétrica cifrada, itens 'e' e 'f';

[k] No HSM 2, de destino, recebe-se a chave privada CPrUi e a chave simétrica CSi cifradas, do usuário 'i';
[l] No HSM 2 decifra-se a chave simétrica, CSi, com a chave privada do HSM 2, CPrHe 2 ;

[m] Em seguida, no HSM 2 decifra-se a chave privada do usuário 'i', CPrUi, que estava no HSM 1, com a chave simétrica CSi, com o algoritmo criptográfico padrão AES ou Serpent, com o modo de operação CTR

e tamanho de chave de 256 bits; [n] No HSM 2 grava-se a chave privada do usuário 'i', CPrUi, já decifrada, e importada do HSM 1;

[o] No HSM 2 destrói-se a chave simétrica CSi;

[p] O PSC 2 encaminha para o PSC 1 mensagem indicando que a importação ocorreu satisfatoriamente. Então, o HSM 1 apaga a chave privada do usuário 'i', CPrUi

6.3. Rede

6.3.1 Foi arquitetado um pool de HSM para operação, replicação e gerenciamento das chaves dos usuários finais, seguindo, além dos relatados no DOC-ICP-17.01 [12], os seguintes requisitos.

a) Especificação e estabelecimento de uma comunicação segura (sessão SSL/TLS) ou equivalente entre os HSMs;

b) Os HSMs poderão estar em ambientes distintos desde que os mecanismos de acesso e segurança se mantenham os descritos neste documento.

6.3.2. O PSC VALID, no âmbito da ICP-Brasil, atende aos critérios mínimos de 99,99% de “nível de tempo de atividade” (*uptime*) a ser verificado por mês.

6.4. Requisitos para serviços de confiança de uso de chaves privadas

6.4.1. Definições para Interface de Serviços de Confiança

6.4.1.1 O PSC VALID utiliza o protocolo TLS, definido pela RFC 5246, para comunicação com serviços de confiança.

6.4.1.2 É utilizado o framework OAuth 2.0 (RFC 6749 e RFC 7636) para implementação da interface aos serviços de confiança dos PSC.

6.4.1.3 Adicionalmente, poderá ser implementada outra interface para os serviços de confiança, desde que o PSC proveja o software necessário para possibilitar ao titular o uso das suas chaves privadas de forma segura.

6.4.2. Definições para URI de base para Serviços de Confiança

6.4.2.1 A URI de base – URI-base - define o estilo e formato dos endereços HTTPS de serviços de confiança. A URI de base contém número correspondendo à versão de API definida pela ICP-Brasil.

6.4.2.2 Este documento trata da versão “v0” de API para PSC.

6.4.2.3 A URI-base utilizado pelo PSC VALID é:

Exemplo de URI-base: http://nuvem.validcertificadora.com.br/v0

6.4.3. Autorização e Autenticação para Requisição de Serviços

6.4.3.1. Fluxo Básico para Uso de Serviços de Confiança. Seguindo o fluxo de autorização estabelecido pela RFC 6749, o uso de chaves privadas em PSC é precedido de solicitação bem sucedida, por parte de aplicações, dos seguintes serviços:

a) Requisição de Código de Autorização

b) Requisição de Token de Acesso

c) Serviço de assinatura utilizando chave de usuários:

6.4.3.2. Trânsito de Fatores de Autenticação

As aplicações não coletam fatores de autenticação do usuário. Para este fim, o PSC VALID comunica-se diretamente com equipamento do usuário, previamente identificado e cadastrado junto ao PSC de forma segura. Excetua-se desta regra o Serviço “Autorização com Credenciais do Titular”.

6.4.3.3. Autenticação de Aplicações de Assinatura

Para obter acesso aos serviços de confiança, o PSC VALID implementa o Serviço de Cadastro de Aplicação com Certificado ICP-Brasil para SSL. O PSC VALID poderá também implementar Serviços de Confiança Opcionais para Cadastro de Aplicação sem Certificado, Token de Acesso para Aplicações e Manutenção de Aplicações. O PSC VALID poderá implementar, para as aplicações, outros métodos de acesso aos seus serviços, com rastreabilidade e riscos associados avaliados.

6.4.4. Relação de Serviços de Confiança Disponibilizados pelo PSC VALID:

a) Serviços de Confiança Obrigatórios:

I. Código de Autorização;
II. Token de Acesso;
III. Assinatura;
IV. Cadastro de Aplicação com Certificado;
V. Listagem de Certificados do Titular
VI. Localização de Titular

b) Serviços de Confiança Opcionais:

I. Cadastro de Aplicação sem Certificado;
II. Token de Acesso para Aplicação;
III. Manutenção de Aplicação;
IV. Autorização com Credenciais do Titular.

6.4.5. Detalhamento de Serviços de Confiança Obrigatórios

6.4.5.1. Serviços de Autorização

6.4.5.1.1. Código de Autorização (Authorization Code Request)

Serviço para obter do titular a autorização de uso da sua chave privada.

Path	http://nuvem.validcertificadora.com.br/v0/oauth/authorize>
Método HTTPS	GET;
Parâmetros da requisição	concatenados após o Path como parâmetros http query, usando o formato "application/x-www-form-urlencoded": ○ response_type: obrigatório, valor "code"; ○ client_id: obrigatório, contendo a identificação da aplicação; ○ redirect_uri; opcional, contendo a URI para redirecionar o usuário de volta para a aplicação de origem. A URI deve estar na lista de URI's autorizadas para a aplicação. Deve ser URL ENCODED. Se não informado, será considerada a primeira URI cadastrada para a aplicação; ○ state: opcional, é retornado sem modificações para aplicação de origem; ○ lifetime: opcional, indica o tempo de vida desejado para o token a ser gerado. Inteiro, em segundos; ○ scope: opcional, se não informado, será considerado "single_signature". (Ver lista de escopos abaixo). Possíveis valores para o parâmetro: single_signature: token que permite a assinatura de apenas um conteúdo (hash), sendo invalidado após a sua utilização; multi_signature: token que permite a assinatura de múltiplos hashes em uma única requisição, sendo invalidado após a sua utilização; signature_session: token de sessão OAuth que permite várias assinaturas em várias chamadas a API, desde que o token esteja dentro do prazo de validade ou que não tenha sido revogado pela aplicação ou pelo usuário. ○ code_challenge: obrigatório, ver RFC 7636 ○ code_challenge_method: obrigatório, valor “S256” (ver RFC 7636).

b) Resposta da Requisição de Código de Autorização:

É retornado um URI de redirecionamento com dois parâmetros http query, usando o formato "application/x-www-form-urlencoded":

code	obrigatório, código de autorização gerado pelo PSC, a ser usado na solicitação do token de acesso

state	obrigatório caso tenha sido informado na requisição, deverá conter o que foi enviado na requisição.

Se o usuário não autorizar a solicitação, o PSC VALID retorna para aplicação cliente através de sua redirect_uri os seguintes parâmetros via http query, usando o formato "application/x-www-formurlencoded":

code	error: obrigatório, com o valor “user_denied”
state	obrigatório caso tenha sido informado na requisição, deverá conter o que foi enviado na requisição.

6.4.5.1.2. Token de Acesso

Após a obtenção de código de autorização, o token de acesso deve ser solicitado com parâmetros no formato "application/x-www-form-urlencoded":

a) Solicitação:

Path	http://nuvem.validcertificadora.com.br/v0/oauth/token>
Método HTTPS	POST
Parâmetros da requisição	formato "application/x-www-form-urlencoded" ○ grant_type: obrigatório, valor "authorization_code"; ○ client_id: obrigatório, contendo a identificação da aplicação; ○ client_secret: opcional, sendo obrigatório se a aplicação não utilizar certificado ICPBrasil; ○ code: comtem o código de autorização retornado do Serviço Código de Autorização como redirect_uri; ○ redirect_uri: opcional, deve ser igual ao informado no Serviço Código de Autorização; ○ code_verifier: obrigatório, correspondendo a code_challenge enviado na Requisição de Código de Autorização, ver RFC 7636.

b) Resposta da Requisição de Token de Acesso:

Parâmetros de retorno	formato "application/json;charset=UTF-8" ○ access_token: obrigatório, valor do token de acesso; ○ token_type: obrigatório, valor "Bearer"; ○ expires_in: obrigatório, valor inteiro com validade do token em segundos. Não deve ultrapassar o valor 300 (5 minutos); ○ scope: opcional, deve ser informado se o escopo retornado for diferente do solicitado pela aplicação.

Obs.: Não será permitido o *refresh_token*.

6.4.5.2. Assinatura

Os parâmetros com conteúdo a ser assinado e assinaturas deverão conter valores em hexadecimal.

Se o escopo do token permitir apenas uma assinatura (*sigle_signature*) e for informado mais de um conteúdo, uma mensagem de erro deve ser retornada.

a) Solicitação

Path	http://nuvem.validcertificadora.com.br/v0/oauth/signature>
Método HTTPS	POST
Cabeçalho	○ Content-type: application/json; ○ Accept: application/json; ○ Authorization: Bearer access_token;
Parâmetros	formato "application/json;charset=UTF-8": ○ certificate_alias": identificador da chave; ○ hashes: conjunto com valores a serem assinados. Cada elemento do conjunto conterá: id: identificador do conteúdo a ser assinado; alias: forma legível do identificador do conteúdo; hash: conteúdo a ser assinado

b) Resposta da Requisição de Assinatura:

Parâmetros	formato "application/json;charset=UTF-8" : ○ status: obrigatório, “success" para sucesso; ○ message: obrigatório, mensagem com informações adicionais; ○ id: identificador do conteúdo assinado; raw_signature: valor numérico em base64 da assinatura produzida

6.4.5.4. Cadastro de Aplicação com Certificado

Serviço para cadastro de uma aplicação junto ao PSC, sendo que a aplicação utilizará um certificado SSL ICP-Brasil para assinar os dados enviados, substituindo neste caso o Serviço de Cadastro de Aplicação.

a) Solicitação

Path	http://nuvem.validcertificadora.com.br/v0/oauth/application_cert>
Método	POST
HTTPS	
Cabeçalho	○ Content-type : application/json ; ○ Accept : application/json ;
Parâmetros	formato "application/json;charset=UTF-8": ○ signed_info, estrutura de dados assinada com certificado SSL ICP-Brasil, contendo: name, obrigatório, nome da aplicação; comments, obrigatório, descrição da aplicação; redirect_uris, obrigatório, URI’s autorizadas para redirecionamento (para serviços de requisição de autorização). Devem ser oriundas da URL Base do certificado de equipamento apresentado, sendo vedada a utilização de fragments

b) Resposta do Serviço de Cadastro de Aplicação com Certificado:

Parâmetros	formato "application/json;charset=UTF-8": ○ status, obrigatório, “success" para sucesso; ○ message, obrigatório, mensagem com informações adicionais.

6.4.6 Detalhamento de Serviços de Confiança Opcionais

6.4.6.1 Cadastro de Aplicação sem Certificado

Serviço para cadastro de uma aplicação junto ao PSC VALID. É obrigatório para todas as aplicações que utilizarem serviços de autorização sem certificados ICP-Brasil.

a) Solicitação

Path	http://nuvem.validcertificadora.com.br/v0/oauth/application>
Método HTTPS	POST
Cabeçalho	○ Content-type : application/json ; ○ Accept : application/json ;
Parâmetros	formato "application/json;charset=UTF-8": ○ client_id : obrigatório, CNPJ base da aplicação (antes da "/"); ○ client_secret : obrigatório, senha/segredo da aplicação; ○ name : obrigatório, nome/descrição da aplicação;

b) Resposta da Requisição de Cadastro de Aplicação

Parâmetros	formato "application/json;charset=UTF-8": ○ status: obrigatório, “success" para sucesso; ○ message: obrigatório, mensagem com informações adicionais.

6.4.6.2. Serviços de Manutenção de Cadastro de Aplicação

Serviço para manutenção das informações armazenadas de uma aplicação no PSC. É obrigatório para todas as aplicações que utilizarem serviços de autorização não identificadas por certificados ICP-Brasil para SSL.

6.4.6.2.1. Token de Acesso para Aplicação Requisição para que uma aplicação obtenha token de acesso para manutenção de seu cadastro junto ao PSC.

a) Solicitação

Método HTTPS	POST;
Path	http://nuvem.validcertificadora.com.br/v0/oauth/client_token>

Parâmetros da requisição	concatenados após o Path como parâmetros http query, usando o formato "application/x-www-form-urlencoded": ○ grant_type, obrigatório, valor "client_credentials"; ○ client_id, obrigatório, contendo a identificação da aplicação; ○ client_secret, obrigatório se a aplicação não utilizar certificado SSL ICP-Brasil; ○ lifetime, opcional, validade desejada para o token a ser gerado, deve conter valor Inteiro, em segundos.

b) Resposta da Requisição de Token de Acesso para Aplicações:

Parâmetros de retorno	formato "application/json;charset=UTF-8" : ○ access_token, obrigatório, valor do token de acesso; ○ token_type, obrigatório, valor "Bearer"; ○ expires_in, opcional, validade do token em segundos.

6.4.6.2.2. Manutenção de Aplicação Serviço para atualização de informações de uma aplicação. Requer um token de acesso para aplicações, enviado no parâmetro de cabeçalho “Authorization”.

Path	http://nuvem.validcertificadora.com.br/v0/oauth/client_maintenance>
Método HTTPS	PUT
Cabeçalho	○ Content-type: application/json; ○ Accept: application/json; ○ Authorization: Bearer access_token (“Bearer” concatenado espaço e access_token);
Parâmetros	formato "application/json;charset=UTF-8": ○ client_id, obrigatório, CNPJ base da aplicacao (antes da "/"); ○ client_secret, opcional, nova senha da aplicacao; ○ name, opcional, nome da aplicação; ○ comments, opcional, observações gerais de uso da aplicação; ○ redirect_uris, opcional, URI’s autorizadas para redirecionamento (para requisição de código de autorização).

b) Resposta da Requisição de Manutenção de Aplicações

Parâmetros de retorno	formato "application/json;charset=UTF-8": ○ status, obrigatório, “success" para sucesso; ○ message, obrigatório, mensagem com informações adicionais.

6.4.6.3 Autorização com Credenciais do Titular Serviço para obter, do titular, autorização de uso da sua chave privada, com solicitação de fatores de autenticação.

6.4.6.3.1 No mínimo um fator de autenticação obtido deve ser válido para uma única solicitação de autorização (OTP- one-time password). Os fatores de autenticação deverão ter seus valores concatenados e enviados no parâmetro “password”.

a) Solicitação

Path	http://nuvem.validcertificadora.com.br/v0/oauth/pwd_authorize>
Método HTTPS	POST
Cabeçalho	○ Content-type: application/json; ○ Accept: application/json;
Parâmetros	formato "application/json;charset=UTF-8": ○ grant_type, obrigatório, valor "password”; ○ client_id, obrigatório, identificação da aplicação; ○ client_secret, opcional, sendo obrigatório apenas quando a aplicação não utilizar certificado ICP-Brasil; ○ username, obrigatório, identificação do usuário por meio de CPF ou CNPJ; ○ password, obrigatório, valor da concatenação de fatores de autenticação informadas pelo usuário; ○ lifetime, opcional, indica o tempo de vida desejado para o token a ser gerado, valor inteiro, em segundos. Não deve ultrapassar o valor 300 (5 minutos); ○ scope, opcional, se não informado será considerado "single_signature". (ver lista de escopos para Serviço de Código de Autorização).

b) Resposta da Requisição de Manutenção de Aplicações

Parâmetros de retorno	formato "application/json;charset=UTF-8": o access_token, obrigatório, valor do token de acesso; o token_type, obrigatório, valor "Bearer"; o expires_in, obrigatório, validade do token em segundos. Não deve ultrapassar o valor 300 (5 minutos); o scope, opcional, informado apenas se o escopo retornado for diferente do solicitado pela aplicação.

6.5 Lista de Prestador de Serviço de Confiança – LPSC

6.5.1 A Lista de Prestadores de Serviço de Confiança – LPSC contém as entidades credenciadas no âmbito da ICP-Brasil como Prestadores de Serviço de Confiança - PSC. A LPSC será publicada pela AC Raiz e atualizada no prazo máximo de 180 dias.

6.5.2 A LPSC será publicada no repositório da AC Raiz em versão textual, para leitura humana, e em XML, para processamento por máquina.

6.5.3 A autenticidade e a integridade da versão processável por máquina da lista compilada é

assegurada por meio de uma assinatura digital XMLDSig suportada por um certificado digital do ITI.

6.5.4 As versões da LPSC e o certificado que assina a LPSC serão publicados no repositório da AC

Raiz, disponível em: http://www.iti.gov.br/repositorio

6.5.5 A autenticidade e integridade da lista compilada devem ser verificadas pelas partes confiáveis antes de qualquer uso.

6.5.6 A LPSC é codificada em XML, em conformidade com a estrutura proposta pelo padrão ETSI TS 102 231, e contém os seguintes dados:

a) a informação do esquema (SchemeInformation), onde são apresentados os dados de identificação do emissor, o ITI, e a data da próxima atualização (NextUpdate) da lista;

b) a lista de prestadores de serviço (TrustServiceProviderList), que contém uma entrada (TrustServiceProvider) para cada PSC credenciado junto à ICP-Brasil; e

c) assinatura digital no formato XMLdSIG.

7. SERVIÇO DE ASSINATURA DIGITAL, VERIFICAÇÃO DE ASSINATURA DIGITAL.

7.1. Introdução

7.2.Criação de Assinaturas

7.1.1. Os requisitos a seguir foram baseadas nos padrões para criação e validação de assinaturas definidas nas especificações do ETSI.

7.2.Criação de Assinaturas

7.2.1. O objetivo da criação de assinaturas é para gerar uma assinatura cobrindo um documento eletrônico (texto, som, imagem, entre outros) do assinante, o certificado de assinatura ou uma referência a esse certificado, bem como os atributos da assinatura que suportam essa assinatura.

7.2.2. Um modelo funcional básico de um ambiente para a criação de assinaturas se constitui por:

• signatário que quer criar uma assinatura em um documento eletrônico;

• um aplicativo condutor que representa um ambiente de usuário (por exemplo, um aplicativo de negócios) que o assinante usa para acessar a funcionalidade de assinatura; e

• um sistema de criação de assinatura, que implementa a funcionalidade de assinatura.

7.2.3. Antes de iniciar o procedimento de assinatura o sistema deve verificar a validade do certificado. Ao receber o retorno da assinatura o sistema deve bater a resposta com a chave pública.

NOTA: O envolvimento humano de um signatário nem sempre é necessário. A assinatura pode ser um processo automatizado e implementado na aplicação no ambiente do usuário.

7.3. Dispositivos para criação de assinaturas

7.3.1. São sistemas ou equipamentos configurados para implementar códigos e/ou outros mecanismos que possibilitem ativação da chave privada do signatário para a criação das assinaturas digitais.

7.3.2. Os dispositivos para criação de assinatura contém os certificados de assinatura ou possuírem uma referência inequívoca a eles. Devem, ainda, verificar os dados de autenticação do assinante.

7.3.3. Os equipamentos para criação de assinaturas possuem certificação Inmetro válida no âmbito da ICP-Brasil, conforme definido no conjunto de documentos DOC-ICP-10 [6], no documento DOC-ICP-01.01 [7], neste documento e seus complementares.

7.4. Interface da aplicação com o dispositivo de criação de assinaturas

7.4.1. A interface entre a aplicação de assinatura e o dispositivo ou equipamento de criação garante que, somente com a autenticação do titular do certificado, que deve ter controle exclusivo da chave privada, seja possível requerer a criação dos dados de uma assinatura digital.

7.4.2. O uso do dispositivo de criação exige que o usuário insira dados específicos de autenticação do assinante. Toda informação trocada entre a aplicação e o dispositivo trafega de forma criptografada.

7.4.3. Mais de um mecanismo de autenticação é aplicado para fornecer uma garantia de autenticação suficiente.

7.4.4. O mecanismo de autenticação do signatário evita ataques de representação.

Nota 1: A natureza dos mecanismos de autenticação e os dados de autenticação do assinante são determinados pelo dispositivo de criação de assinaturas. Existem padrões para diferentes interfaces, tipos dispositivos ou equipamentos e mecanismos de autenticação.

Nota 2: Em alguns casos, o uso de dados de autenticação do signatário será obrigatório e outros requisitos sobre a natureza dos mecanismos de autenticação e as interfaces podem ser impostas.

7.5. Suítes de Assinatura

7.5.1. Todos os algoritmos e tamanho de chaves envolvidos no cálculo de qualquer elemento da assinatura digital encontram-se definidos no documento DOC-ICP-01.01 [7].

7.6. Formatos de Assinaturas

7.6.1. A ICP-Brasil padroniza as assinaturas digitais baseadas em políticas explícitas de assinatura. As políticas de assinatura preveem os formatos CAdES, XAdES e PAdES.

7.6.2. Todos os formatos e perfis de assinatura digital no âmbito da ICP-Brasil estão definidos no conjunto de documentos DOC-ICP-15 [8] e seus complementares.

7.6.3. O PSC VALID implementa assinaturas digitais baseadas nas políticas de assinatura padronizadas e aprovadas na ICP-Brasil.

7.7. Assinatura com Carimbo do Tempo

7.7.1. Uma assinatura digital com carimbo do tempo evidencia que a assinatura digital já existia na data contida no carimbo do tempo. Os carimbos do tempo são emitidos pelas Autoridades de Carimbo do Tempo (ACT) credenciadas na ICP-Brasil e fornece data/hora como uma propriedade não assinada adicionada à uma assinatura digital.

7.7.2. A ICP-Brasil define no documento DOC-ICP-11 [9] o modelo de carimbo do tempo adotado em sua infraestrutura.

7.7.3. As políticas de assinatura regulamentadas no âmbito da ICP-Brasil definem o uso de carimbo do tempo.

7.8. Validação de Assinaturas

7.8.1. O processo de validação de uma assinatura digital é realizado contra uma política explícita de assinatura digital, que consiste de um conjunto de restrições de validação, denominada Política de Assinatura, gerando um relatório com indicação da situação de validação (Válida, Inválida ou Indeterminada), fornecendo os detalhes da validação técnica de cada uma das restrições aplicáveis, que podem ser relevantes para a aplicação demandante na interpretação dos resultados.

7.8.2. Na ICP-Brasil, conforme disposto no documento DOC-ICP-15 [8], uma assinatura digital é criada pelo signatário de acordo com uma política de assinatura. A validade de uma assinatura digital é avaliada pelo verificador utilizando a mesma política de assinatura usada na criação dessa assinatura digital. O item 7.6.2, acima, define os formatos e perfis regulamentados no âmbito da ICP-Brasil.

7.8.3. Os requisitos para geração e verificação de assinaturas digitais no âmbito da ICP-Brasil estão descritos no documento DOC-ICP-15.01 [10].

7.8.4. A AC Raiz gerencia as Políticas de Assinatura na ICP-Brasil, conforme definido no Anexo 3 do DOC-ICP-15.03 [11]. No processo de validação de uma assinatura digital, deve-se verificar a validade das Políticas de Assinatura por meio da Lista de Políticas de Assinatura Aprovadas (LPA), publicada no repositório da AC Raiz.

7.9. Acordo de Nível de Serviço

7.9.1. O acordo de nível de serviço para todos os serviços credenciados do PSC VALID são de no mínimo 99,99%.

8. CLASSIFICAÇÃO DA INFORMAÇÃO

8.1. Toda informação gerada e custodiada pelo PSC VALID recebe classificação segundo o seu teor crítico e grau de confidencialidade, de acordo com a Política de Classificação de Informação.

8.2. A classificação da informação no PSC VALID é realizada independente da mídia onde se encontra armazenada ou o meio pelo qual é trafegada.

8.3. A classificação da informação está definida em documento próprio.

9. SALVAGUARDA DE ATIVOS DA INFORMAÇÃO

9.1. O PSC VALID, em sua Política de Segurança da Informação, define como é realizado a salvaguarda de ativos de informação no formato eletrônico, também denominado backup.

9.2. A salvaguarda de ativos da informação possui descrita as formas de execução dos seguintes processos:

a) Procedimentos de backup;

b) Indicações de uso dos métodos de backup;

c) Tabela de temporalidade;

d) Local e restrições de armazenamento e salvaguarda em função da fase de uso; e) Tipos de mídia;

f) Controles ambientais do armazenamento;

g) Controles de segurança;

h) Teste de restauração de backup.

9.3 O PSC VALID possui política de recebimento, manipulação, depósito e descarte de materiais de terceiros.

10. GERENCIAMENTO DE RISCOS

O PSC VALID possui um processo de gerenciamento de riscos, atualizado, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados atualizado, no mínimo, anualmente.

11. PLANO DE CONTINUIDADE DE NEGÓCIOS

O PSC VALID possui um Plano de Continuidade do Negócio – PCN implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio em caso de inoperância total ou parcial de seu ambiente.

12. ANÁLISES DE REGISTRO DE EVENTOS

Todos os registros de eventos (logs, trilhas de auditorias e imagens) são analisados, no mínimo, mensalmente e um relatório é gerado com assinatura do responsável pelo PSC VALID. Todos os registros da transação biométrica por parte do PSC VALID são guardados por um período de 6 anos.

13. PLANO DE CAPACIDADE OPERACIONAL

O PSC VALID elaborou e mantem atualizado anualmente um Plano de Capacidade Operacional – PCO para determinar a capacidade de produção atual e futura com níveis de desempenho satisfatórios para responder a novas demandas, fornecendo níveis adequados de serviços aos usuários, visando dimensionar os sistemas para suportar o crescimento orgânico, picos de utilização e sazonalidades.

O PCO do PSC VALID possui, no mínimo:

a) Níveis de serviços requeridos pelos usuários determinados;

b) Análise da capacidade de processamento de dados instalada; e

c) Dimensionamento da capacidade necessária de infraestrutura, hardware, comunicação de dados e link de internet para atender os níveis de serviços atuais e futuros.

14. DOCUMENTOS DA ICP-BRASIL REFERENCIADOS

14.1. Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram:

Ref.	Nome do Documento	Código
[1]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[4]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[5]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[6]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL	DOC-ICP-10
[8]	VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL	DOC-ICP-15
[9]	VISÃO GERAL DO SISTEMA DE CARIMBOS DO TEMPO NA ICP-BRASIL	DOC-ICP-11

14.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do Documento	Código
[7]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[10]	REQUISITOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL	DOC-ICP-15.01
[11]	REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL	DOC-ICP-15.03

[12]	PROCEDIMENTOS OPERACIONAIS MÍNIMOS PARA OS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17.01

15. REFERÊNCIAS

- ✓ 15. REFERÊNCIAS
- ✓ BRASIL, Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para
- ✓ credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e
- ✓ dispõe sobre o Núcleo de Segurança e Credenciamento.
- ✓ RFC 6238, IETF - TOTP: Time-Based One-Time Password Algorithm
- ✓ RFC 6287, IETF - OCRA: OATH Challenge-Response Algorithm
- ✓ RFC 4226 - HOTP: An HMAC-Based One-Time Password Algorithm
- ✓ ETSI TS 102 231 - Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trustservice status information; V3.1.2 (2009-12)
  Regulation (EU) 910/2014 - relativo à identificação eletrônica e aos serviços de confiança para as transações eletrônicas no mercado interno Europeu.