VeriSign Trust Network
Políticas de Certificados

Versão 1.3

Data efetiva: 31 de março de 2004

VeriSign, Inc. 487 E. Middlefield Road Mountain View, CA 94043 USA +1 650.961.7500 http//:www.verisign.com

Políticas de Certificados VeriSign Trust Network

Data de revisão: 31 de Março de 2004

Avisos de marcas comerciais

Agradecimentos

A VeriSign agradece pela inestimável assistência de J.F. Sauriol do Labcal Technologies Inc. (http://www.labcal.com) com os elementos técnicos e estrutura das Políticas de Certificados da VeriSign Trust Network A VeriSign também gostaria de agradecer aos inúmeros revisores que participaram do documento, especializados nas mais diversas áreas de administração, direito, política e tecnologia.

Índice

1. INTRODUÇÃO

Observação: os termos capitalizados nesta Política de Certificado são termos definidos, com denotações específicas. Consulte a Seção 9 para uma lista das definições:

VeriSign, Inc. (“VeriSign) é líder no fornecimento de serviços de infra-estrutura confiável para sites da web, empresas, provedores de serviços de comércio eletrônico e indivíduos. O nome de domínio, certificado digital e serviços de pagamento de uma empresa oferecem uma infra-estrutura web de identificação, autenticação e transação essencial para o comércio eletrônico , exigem para realizar operações e comunicações seguras.

A VeriSign fornece certificados digitais (“Certificados”) para aplicações com fio e sem fio, através de uma infra-estrutura de chave pública global (“PKI”), conhecida como VeriSign Trust NetworkSM (“VTN”), bem como uma base de marca privada. A VeriSign criou a Rede de Confiança da VeriSign (“ VTN”) para acomodar uma grande comunidade pública de usuários, com as mais variadas necessidades em comunicação e segurança da informação. A VeriSign oferece os serviços VTN junto com uma rede global de empresas afiliadas (“Afiliadas”), espalhadas no mundo todo.

Este documento, doravante referido como “’PC”, intitula-se “As Políticas de Certificado da Rede de Confiança da VeriSign”. Este PC é a principal declaração de política que rege a VTN. A PC define as exigências comerciais, legais e técnicas para aprovação, emissão, gestão, utilização, revogação e renovação de Certificados digitais dentro da Rede de Confiança da VeriSign, oferecendo serviços associados e de confiança. Estes requisitos, denominados “Padrões VTN”, protegem a segurança e integridade da Rede de Confiança da VeriSign. Os Padrões VTN consistem em um grupo simples de regras que se aplicam consistentemente por toda VTN, fornecendo assim a segurança de confiança uniforme por toda a rede.

A rede VTN inclui três classes de Certificados, Classes 1-3. A PC descreve como estas três Classes correspondem às três classes de aplicativos com requisitos comuns de segurança. Esta PC consistem em um único documento que define três políticas de certificado, correspondente às três Classes. A versão atual da PC identifica os Padrões VTN aplicáveis a cada Classe.

Os autores deste documento são membros da Autoridade em Gerenciamento de Políticas da Rede de Confiança da VeriSign (“PMA”). A PMA é responsável pela proposta de mudanças na PC, atualização do documento e solicitação de comentários sobre a PC. A PMA também supervisiona a conformidade com os requisitos desta PC.

1.1. Visão Geral

A PC estabelece os requisitos para a Rede de Confiança da VeriSign, porém não a rede propriamente dita. A PC rege o uso da VTN por todos os indivíduos e entidades participantes da VTN (coletivamente, “Participantes da VTN”). Além disso, a VeriSign e todas as Afiliadas devem seguir os requisitos da PC. A VeriSign, bem como cada Afiliada, tem autoridade sobre parte da VTN. A parte da VTN controlada pela VeriSign ou por uma Afiliada é denominada “Subdomínio” da VTN. Um Subdomínio de uma Afiliada consistem em uma parte da VTN sob seu controle. Um Subdomínio de uma Afiliada inclui entidades a ela subordinadas como seus Clientes, Assinantes e Parte Confiante. Entretanto, a PC atual como um documento guarda-chuva, estabelecendo os padrões VTN de linha de base para toda a rede VTN.

A PC não é valida para serviços externos à VTN. Por exemplo, a VeriSign e certas Afiliadas oferecem serviços de rótulos privados, com os quais as organizações criam suas próprias hierarquias privadas fora da VTN, aprovam aplicativos certificados, e terceirizam a VeriSign ou Afiliada para as funções secundárias de emissão, gerenciamento, revogação e renovação de certificados. Uma vez que a PC aplica-se somente à VTN, ela não se aplica a estas hierarquias privadas.

(a) Função de uma PC de VTN e Outros Documentos sobre Práticas

A PC descreve em um plano geral, a infra-estrutura comercial, legal e técnica de uma rede VTN. Dentre outros, ela descreve, especificamente:

– • Aplicativos adequados para cada classe de Certificado, bem como os níveis associados de segurança.

– • Obrigações das Autoridades Certificadores, Autoridades de Registro, Assinantes e Parte Confiante.

– • Todas as disposições legais que devem ser cobertas nos Contratos de Assinante VTN e Contratos com Parte Confiante,

– • Requisitos para auditoria e análises relacionadas às práticas e segurança.

– • Métodos de confirmação de identidade dos Solicitantes a Certificação para cada Classe de Certificado,

– • Procedimentos operacionais para serviços de ciclo de vida do Certificado: Aplicações, emissão, aceitação, revogação e renovação de Certificados,

– • Procedimentos de segurança operacional para o registro de auditorias, retenção de registros e recuperação de desastres,

– • Administração física, de pessoal; gerenciamento de chaves e segurança lógica,

– • Certificado e conteúdo da Lista de Revogação de Certificados, e

– • Administração da PC, incluindo métodos de emenda.

Todavia, a PC é o primeiro de uma série de documentos relevantes à VTN. Estes outros documentos incluem:

• Documentos antigos de âmbito operacional e de segurança que complementam a PC, fornecendo requisitos mais detalhados, tais como: - Política de Segurança Física da VeriSign, que determina os princípios de segurança que regem a infra-estrutura da VTN,

- O Guia de Requisitos para Segurança e Auditoria, que descreve requisitos detalhados para a VeriSign e Afiliadas, com relação à segurança de pessoal, física, de telecomunicações, lógica e de gerenciamento de chave criptográfica,

- Guia de Práticas de Requisitos Legais da Afiliada, que define os requisitos para a Afiliada determinar a funcionalidade de uma série de práticas e documentos legais que são aceitáveis em um idioma local, cumprem com a legislação local e refletem certos procedimentos localizados, e para determinar uma política privada e plano de validação descrevendo como as Afiliadas autenticarão indivíduos e organizações para cada classe e tipo de Certificados que planejam oferecer, e

- Guia de Referência , que apresenta, em detalhes, os principais requisitos operacionais de gerenciamento.

. • "Declaração de Práticas de Certificação." A VeriSign e cada Afiliada terão uma DPC. Enquanto a PC determina os requisitos (Padrões da VTN), a DPC explica como a VeriSign ou Afiliada emprega as práticas e procedimentos que atendem a este requisitos.

. • Contratos secundários impostos pela VeriSign ou Afiliada. Estes contratos devem VINCULAR Clientes, Assinantes e Parte Confiante à VeriSign ou Afiliada. Dentre outras coisas, o contrato determina Padrões VTN a estes Participantes da VNT e em alguns casos, determinam práticas específicas sobre como os Padrões da VTN devem ser atendidos.

Em muitos casos, a PC baseia-se neste documentos secundários para Padrões VTN específicos e detalhados, onde inclui as especificações na PC que comprometeriam a segurança da rede VTN. A Figura 1 mostra a relação entre a PC e outros documentos normativos.

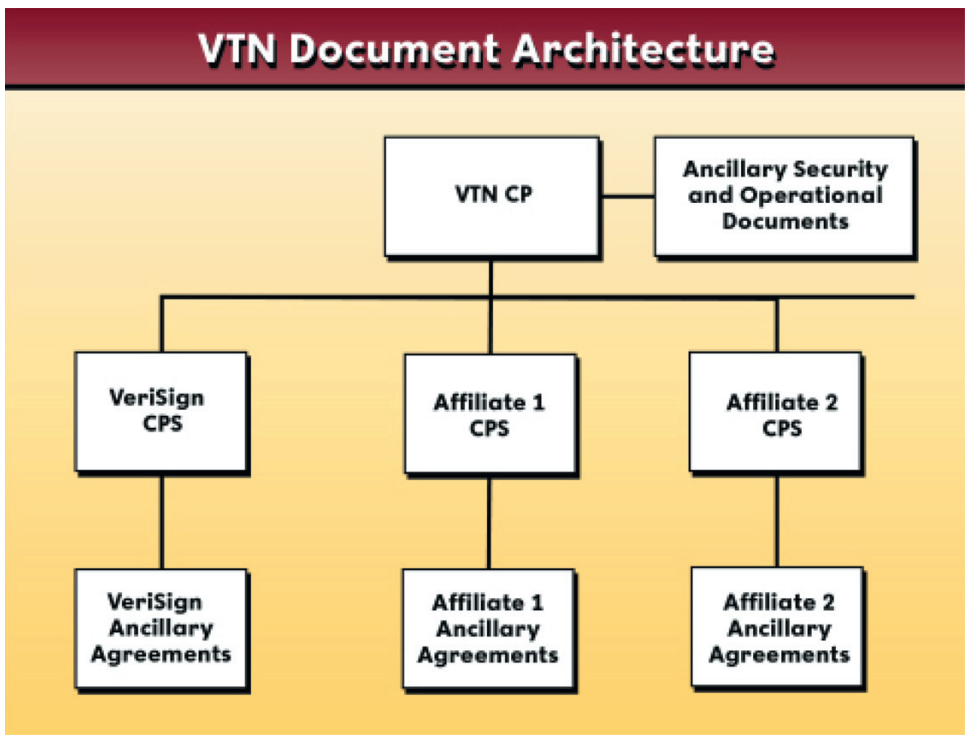

Figura 1 - Arquitetura de Documentos VTN

Conforme mostrado na Figura 1, a PC é cume da arquitetura de documentos VTN, e define Padrões VTN de alto nível. Documentos correlatos de segurança e operação complementam a PC na determinação de Padrões VTN mais

detalhados. A VeriSign e cada Afiliada possui um DPC que descreve como os Padrões VTN são atendidos. Finalmente, a VeriSign e cada Afiliada usam os contratos e documentos correlatos para determinar os requisitos aos Participantes da VTN.

A VeriSign e a PMA atualizam a PC e os documentos operacionais e de segurança secundários da VTN. Em comparação, a VeriSign e cada Afiliada mantém suas próprias DCPs e contratos secundários. Cada Afiliada deve escolher e atualizar uma DPC, e também definir um conjunto de contratos secundários como uma condições de início e continuação das operações como uma Afiliada participante da VTN. Estes documentos devem ser revisados e aprovados pela PMA.

A Tabela 1 é uma matriz que exibe vários documentos de práticas VTN, estejam eles disponíveis publicamente ou em suas instalações. A lista na tabela 1 não deve ser exaustiva. Observe que os documentos não divulgados publicamente são confidenciais, para preservar a segurança da VTN.

Documentos	Status	Onde estão disponíveis ao público
Políticas de Certificados VeriSign Trust Network	Público	Repositório VeriSign, de acordo com PC § 8.2.2. Consultar https: //www.verisign.com/repository
Documentos Operacionais e de Segurança Secundários da VTN		
Política de Segurança de Informação da Verisign	Confidencial	N/A
Política de Segurança Física da Verisign	Confidencial	N/A
Manual de Requisitos de Segurança e Auditoria	Confidencial	N/A
Manual de Referência de Cerimônia de Chave	Confidencial	N/A
Compêndio de Administrador de PKI Gerenciada	Público	https://www.verisign.com/ enterprise/library/index.html
Manual de Administrador de Serviços de Gerenciamento de Chave de PKI Gerenciada	Público	https://www.verisign.com/ enterprise/library/index.html
Documentos Específicos da VeriSign		
Declaração de Práticas de Certificação da VeriSign	Público	Repositório VeriSign, de acordo com DPC § 2.6.1. Consultar https://www.verisign.com/ repository
Acordos secundários e auxiliares da VeriSign (Contratos de PKI Gerenciada, Contratos de Assinante, e Contratos de Partes Confiantes)	Público, incluindo contratos de PKI Gerenciada Lite, mas não os Contratos de PKI Gerenciada, que são confidenciais	Repositório VeriSign, de acordo com DPC § 2.6.1. Consultar https://www.verisign.com/ repository

Tabela 1 Ð Disponibilidade de Documentos de Práticas

(b) Histórico dos Certificados Digitais e a Hierarquia VTN

Esta PC assume que o leitor está familiarizado com Assinaturas Digitais, Infra-estrutura de Chave Pública - ICP (em inglês, PKIs) e a rede de confiança da Verisign, VTN. Caso contrário, a VeriSign recomenda que o leitor receba treinamento no uso de criptografia de chave pública e infra-estrutura de chave pública, como implementado na VTN. Acesse http://www.verisign.com para informações educacionais e treinamento. Os representantes de atendimento ao cliente da VeriSign oferecem assistência adicional (customer_service@verisign.com). E finalmente, a seguir um breve resumo dos papéis dos diferentes participantes da rede VTN.

No coração da VTN, existe uma hierarquia de entidades chamadas “Autoridades Certificadoras”, ou “ACs”. As ACs são Parte Confiante de confiança que facilitam a confirmação da ligação entre uma chave pública e uma identidade e/ou outros atributos de um indivíduo, organização ou dispositivo que é o Titular do Certificado. (Titulares de Certificados são o mesmo que Assinantes, exceto no caso de dispositivos, onde o Assinante é o proprietário do dispositivo e que possui um certificado.)

"AC" é um termo guarda-chuva que se refere às autoridades emissoras de certificados a Assinantes ou outras ACs de hierarquia superior. Uma subcategoria de AC é a Autoridade Primária de Certificação ("APC"). As APCs atuam como raízes na VTN; uma APC corresponde a cada Classe de Certificado. Uma AC pode ser uma AC VeriSign, o que significa que ela pertence e é operada pela VeriSign. Por exemplo todas as APCs são ACs Verisign. Outras ACs que não são entidades da VeriSign, tais como ACs de Afiliadas ou de determinados Clientes.

As ACs às vezes delegam as funções de configuração de identidade a uma ou mais "Autoridades de Registro", ou ARs. As ARs estabelecem os procedimentos de inscrição em nome da AC, recebem as Solicitações de Certificado, confirmam a identidade dos Solicitantes ao Certificado e aprovam ou rejeitam solicitações de certificado.. As ARs também pode iniciar a revogação de Certificado, mediante solicitação de um Assinante ou outros, embora a própria AC possa realizar a revogação, incluindo o Certificado em uma lista de revogação de certificados ("LCR"), ou indicando que um Certificado foi revogado no repositório de ACs.

Assinantes são indivíduos ou organizações que obtém Certificados para usos em suas aplicações. Por exemplo, indivíduos podem usar um certificado para enviar um e-mail assinado digitalmente a Parte Confiante. Uma organização pode usar um certificado, por exemplo, ou um servidor para criar uma sessão segura com um navegador da Internet, usando SSL (Secure Socket Layer). O SSL cria um canal seguro entre um navegador e um servidor da web. O SSL autentica o servidor para o cliente, oferece integridade de mensagens e codifica a comunicação entre o servidor e o cliente.

Parte Confiante são indivíduos ou organizações que utilizam certificados de outrem para certa aplicação. Por exemplo, o destinatário de uma mensagem de e-mail com assinatura digital pode usar o certificado do remetente para verificar a assinatura digital. Além disso, o remetente de um e-mail codificado pode usar o certificado do destinatário para codificar uma chave, que por sua vez é usada para codificar a mensagem. Somente o destinatário que possui a chave pública correspondente à chave pública no Certificado pode obter a chave, e assim, decodificar a mensagem.

Antes de um Assinante obter um Certificado ele deve primeiro se inscrever como Solicitante de Certificado. Os candidatos a certificado devem completar o processo de inscrição estabelecido por uma AC ou R, no qual a Solicitação de Certificado é apresentada à AC ou AR. Em resposta à solicitação de certificado, a AC ou AR confirma a identidade e/ou atributos do Solicitante de Certificado e aprova ou rejeita a solicitação. Em caso de aprovação, um Certificado é emitido ao candidato.

Após a emissão, a AC disponibiliza o Certificado ao candidato. Na maioria dos casos, um Solicitante de Certificado recupera um certificado Cliente, acessando uma página da web específica que carrega o certificado no software. Como alternativa, o Certificado pode ser entregue ao Solicitante, que deverá carregá-lo em seu software. Tal recuperação e/ou carregamento de um Certificado em software constitui a aceitação do Certificado, ao passo que o Solicitante se torna um Assinante, a menos que mesmo tenha manifestado prévia aceitação. O Assinante deve revisar o Certificado e notificar a AC ou AR sobre erros em seu conteúdo após receber acesso ao Certificado. O novo Assinante concorda com os termos e obrigações determinados no Contrato do Assinante.

(c) Conformidade com os Padrões Aplicáveis

A estrutura desta PC corresponde, em geral, à Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, conhecida como RFC 2527 da IETF (Internet Engineering Task Force) uma agência de normatização da Internet. Este documento serve para definir três "políticas de certificado" dentro do escopo do RFC 2527. A estrutura do RFC 2527 framework se tornou um padrão na indústria de infra-estrutura de chave pública. Esta PC cumpre com a estrutura do RFC 2527, para fazer o mapeamento de políticas e comparações, avaliações e interoperações mais fáceis para pessoas usando ou considerando utilizar os serviços da rede VTN.

A PC da VeriSign baseia-se na estrutura do RFC 2527 onde possível, não obstante algumas poucas variações em títulos e detalhes tornaram-se necessárias devido à complexidade dos modelos de negócios da VTN. Enquanto a VeriSign pretende continuar a política de adesão ao RFC 2527 no futuro, a VeriSign se reserva o direito de variar da estrutura RFC 2527 conforme necessário, por exemplo, para melhorar qualidade da PC ou sua adequabilidade à rede VTN. Adicionalmente, a estrutura da PC não pode corresponder a versões futuras da RFC 2527.

(d) Interoperação com Outras PKIs

A VeriSign poderá considerar a interoperação com outras PKIs, conforme o caso. O PMA é responsável pela aprovação ou reprovação de solicitações das interoperações. Esta interoperação inclui, porém não se limita a tipos específicos de certificação cruzada. A certificação cruzada pode incluir a emissão de Certificados ou o recebimento de Certificados cruzados. A VeriSign considerará a interoperação com uma hierarquia para uma classe específica de Certificados pela avaliação de fatores que incluem, mas não se limitam a:

. • O grau em que a PKI de Parte Confiante oferece funções substancialmente similares e o nível de segurança e confiabilidade em comparação aos serviços para aquela Classe de Certificados,

. • O nível de melhoria trazido com a interoperação em benefício dos serviços VTN para Afiliadas, Clientes, Assinantes e Parte Confiante,

. • A capacidade de PKIs interoperáveis em oferecer suporte ao conjunto extenso e robusto de serviços de ciclo de vida de forma contínua, e

. • A necessidade empresarial por tal interoperabilidade.

Para tal, é necessária a execução de um contrato de interoperação.

1.1.1. Visão Geral da Política

A VeriSign oferece três classes distintas de serviços de certificação, Classes 1-3, para Internet com ou sem fio e outras redes. Cada nível, ou classe, de Certificado oferece uma funcionalidade específica e recursos de segurança que correspondem a um nível específico de confiança. Os participantes da VTN escolhe quais Classes de Certificados desejam ou necessitam. Conforme a VeriSign observa novos padrões de utilização e demanda de mercado, ela considera o fornecimento de novas classes ou tipos de Certificados.

Os Certificados de Classe 1, emitidos apenas para indivíduos, oferece o nível mais baixo de segurança dentro da VTN. Eles oferecem garantias de que o nome exclusivo do Assinante é único e inequívoco dentro do Subdomínio da VeriSign ou de uma Afiliada, assegurando ainda que determinado endereço de e-mail está associado a uma chave pública.. Eles são adequados para assinaturas digitais, codificação e controle de acesso a transações não-comerciais ou de baixo valor, onde a prova de identificação não se faz necessária.

Os Certificados de Classe 2, também emitidos apenas para indivíduos, oferece um nível médio de segurança dentro da rede VTN. Eles oferecem a segurança da identidade do Assinante, baseada em uma comparação de informações enviadas pelo Solicitante de Certificado, comparadas às informações em registros comerciais e bancos de dados, ou no banco de dados do serviço de verificação de identidade aprovado pela VeriSign. Eles podem ser usados em assinaturas digitais, codificação e controle de acesso, incluindo uma prova de identidade em transações de valor médio.

Os certificados de Classe 3 oferecem o mais alto nível de segurança dentro da rede VTN. Eles são emitidos a indivíduos, organizações e Administradores de ACs e ARs. Os Certificados de Classe 3 para Indivíduos pode ser usado para assinaturas digitais, codificação e controle de acesso, incluindo uma prova de identidade em transações de alto valor. Esses certificados de Classe 3 oferecem a garantia da identidade do Assinante baseado na presença pessoal (física) do Assinante perante uma pessoa que confirma sua identidade, utilizando um atestado de idoneidade emitido pelo governo federal, e outra credencial de identificação. Os demais certificados de Classe 3 para organizações são emitidos para dispositivos que oferecem autenticação, integridade de mensagens, software e conteúdo, além da criptografia de confidencialidade. Oferecem ainda garantias da identidade do Assinante baseada em uma confirmação de que a empresa do Assinante existe de fato, que sua organização autorizou a Solicitação de Certificado, e que a pessoa que envia a Solicitação de Certificado em nome do Assinante teve sua autorização para faze-lo.

“Certificados de Classe 3 Organizacional ASB” (veja § 1.1.2.2.1 da PC) são emitidos para uma organização, para uso por um representante devidamente autorizado, que utiliza o Certificado em nome da organização. O representante pode usar os Certificados para assinaturas digitais, criptografia e controle de acesso. OS Certificados de Classe Organizacional ASB oferecem a garantia não somente de uma chave pública vinculada a uma organização privada, mas também que a pessoa controlando a chave privada da organização está autorizada a agir em nome da empresa em transações que utilizam a chave privada correspondente à chave pública no Certificado.

Em geral, todas as três classes de Certificados VTN resumem-se em duas categorias, PKI de Varejo e PKI Gerenciada. Os Certificados Individuais são Certificados emitidos pela VeriSign ou sua Afiliada, agindo como uma AC para indivíduos e organizações que fazem solicitações individuais à VeriSign ou uma Afiliada através de seu website. Os Certificados de PKI Gerenciada baseiam-se em uma Solicitação de4 Certificado aprovada por um Cliente de PKI Gerenciada, que firma um Contrato de PKI Gerenciada com a VeriSign ou uma Afiliada, para a emissão de determinada quantidade de Certificados (veja a PC § 1.1.2.1.1).

Além de Certificados de PKI de Varejo e Gerenciada, os Certificados da VTN são emitidos a Clientes Gateway, Administradores de ACs e ARs, e através do Centro de Serviços de Autenticação. Os Clientes Gateway são ACs que utilizam o software de Certificado do servidor da Microsoft ou Netscape, que foram incluídos na rede VTN em virtude de um Certificado emitido ao Cliente Gateway pela VeriSign. Os Clientes Gateway usam servidores de Certificados para emitir certificados a Assinantes. Para mais informações sobre o Gateway, veja o § 1.1.2.1.5 da PC. Certificados de Administrador são emitidos para Administradores de ACs ou ARs, permitindo-lhes realizar funções administrativas em nome da AC ou AR. Conforme o programa do Centro de Serviço de Autenticação, a VeriSign ou Afiliada confirmam a identidade de um Solicitante de Certificado em nome de uma organização, tal como em transações interempresariais (B2B). Para mais informações sobre o Centro de Serviço de Autenticação, veja o § 1.1.2.2.1 da PC.

A Tabela 2 define as propriedades de cada classe de Certificado, baseados em sua emissão a indivíduos ou organizações, oferecidos como PKIs de Varejo ou Gerenciadas, oferecidos através do programa do Centro de Serviços de Autenticação ou Gateway, ou emitidos pelo Administrador.

Classe	Emitido para	Serviços sob os quais Certificados são Disponível	Confirmação de Identidade do Solicitante de Certificado (§§ 3.1.8.1 da PC) 3.1.9)	Solicitações implementadas ou contempladas por Usuários (PC § 1.3.4.1)
Classe 1	Indivíduos	Varejo	Pesquisa de nome e endereço de e-mail para garantir que o nome significativo é exclusivo e inequívoco.	modestamente melhorar a segurança do e-mail através de confidencialidade criptografia, assinaturas digitais e controle de acesso baseado na Web, onde a prova de identidade não se faz necessária. Solicitações que exigem um baixo nível de de segurança em comparação as outras Classes, como navegação na Internet sem fins comerciais e e-mail.
		PKI Gerenciada e Gateway	Pesquisa de nome e endereço de e-mail como na Classe 1 Varejo além da documentação e bancos de dados internos de verificação para confirmar o Certificado com o credenciamento do Requerente junto ao Cliente de PKI Gerenciada ou Cliente Gateway como uma Afiliada Indivíduos.	
Classe 2	Indivíduos	Varejo e Centro de Serviços de Autenticação	Igual à Classe 1 Varejo, além da verificação de informações de registro automatizadas ou fora de banda com um ou mais bancos de dados de Parte Confiante ou fontes comparáveis.	Melhora a segurança do e-mail por meio da criptografia de confidencialidade, assinaturas digitais para autenticação e controle de acesso baseado na Web. Solicitações

Classe	Emitido para	Serviços com Certificados Disponíveis	Confirmação de Identidade do Solicitante de Certificado (§§ 3.1.8.1 , 3.19 da PC)	Solicitações implementadas ou contempladas pelos Usuários (§ 1.3.4.1 da PC)
		PKI Gerenciada	Igual à Classe 1 Varejo, além da verificação de documentação e bancos de dados internos para confirmar a identidade do Solicitante de Certificado(por ex.., documentação e recursos humanos) e que o Solicitante é afiliado ao Cliente de PKI Gerenciada.	que exijam um nível médio de segurança, em comparação com as demais Classes, como e-mails de um indivíduo, entre empresas, assinaturas on-line, aplicativos de conta e substituição de senha.
Classe 3	Indivíduos	Varejo	Mesmo que a classe 1 Varejo, além da presença pessoal e verificação de uma ou mais credenciais de identificação.	Melhora a segurança do e-mail por meio da criptografia de confidencialidade, assinaturas digitais para autenticação e controle de acesso baseado na Web. Aplicativos que exijam um alto nível de segurança, em comparação com as demais Classes, transações bancárias on-line, acesso a bancos de dados corporativos, e troca de informações confidenciais.
		Administradores	Procedimentos especializados de confirmação, dependendo do tipo de Administrador. A identidade do Administrador e a organização utilizando o Administrador são confirmadas. Veja também § 5.2.3 da PC.	Funções do administrador.
	Organizações	Varejo	Verificação de banco de dados de Parte Confiante ou outros documentos que comprovem o direito de uso do nome da organização. Inspeção de validação por telefone (ou procedimento similar), para confirmar informações e autorização da Solicitação de Certificado. Em caso de Certificados de servidores da web, a confirmação que o Solicitante de Certificado tem o direito de usar o nome do domínio no Certificado.	Autenticação de servidor (alguns exemplos sendo web, ftp ou diretório), sessões seguras de SSL/TLS, criptografia de confidencialidade e (quando em comunicação com outros servidores) autenticação de cliente (Secure Server ID, OFS e autenticação e integridades de software e outros conteúdos (IDs Digitais de Assinatura de Código e Conteúdo).

Classe	Emitido para	Serviços para os quais os Certificados Disponível	Confirmação de Certificado Identidade do Solicitante (§§ 3.1.8.1 , 3.19 da PC)	Solicitações implementadas ou contempladas pelos Usuários (§ 1.3.4.1 da PC)
		- Centro de Serviços de Autenticação	Verificação de banco de dados de Parte Confiante ou outra documentação comprobatória da existência da organização. Inspeção de validação por telefone (ou procedimento similar) para que a organização confirme o emprego e autoridade do representante empresarial, e para que este possa confirmar sua Solicitação de Certificado. Carta de confirmação de envio da Solicitação de Certificado é enviada ao representante..	Melhora a segurança do e-mail enviado em nome de uma organização por meio da criptografia de confidencialidade, assinaturas digitais para autenticação e controle de acesso baseado na Web. Solicitações exigindo um alto nível de de segurança em comparação com as outras Classes, como obter acesso a uma extranet B2B ou realizar transação de alto valor em uma transação B2B.
		PKI Gerenciada	Validação de PKI Gerenciada para Cliente SSL ou PKI Gerenciada para Cliente SSL Premium Edition como na Classe 3 Organizacional, Varejo além da validação do Administrador da PKI Gerenciada.	Automação de servidor, criptografia de confidencialidade e, (na comunicação com outros servidores capacitados) autenticação de cliente (Secure Server ID e Global Server ID).

Tabela 2 - Propriedades de Certificado que Afetam a Confiança

As especificações para Classes de Certificados nesta PC definem o nível mínimo de segurança fornecido para cada Classe. Por exemplo, qualquer Certificado de Classe 1 pode ser usado para assinaturas digitais, criptografia, controle de acesso onde a comprovação de identidade não é necessária, isto é, para aplicações que exigem baixos níveis de segurança. Entretanto, por contrato ou dentro de ambientes específicos (tais como ambiente inter-empresarial), os participantes da rede VTN podem usar procedimentos de validação mais consistentes que aqueles fornecidos nesta PC, ou utilizar Certificados para aplicações mais seguras que aquelas descritas nos §§ 1.1.1, 1.3.4.1 da PC. Tal utilização estará limitada a tais entidades e sujeitas aos parágrafos 2.2.1.2, 2.2.2.2 da PC, e estas entidades responsabilizar-se-ão por qualquer dano ou prejuízo causado pela (má) utilização.

1.1.2. Escopo de Serviços da VTN Suite

A rede VTN oferece uma série de serviços para ajudar na implantação, gerenciamento e uso dos Certificados. Esta seção fornece uma descrição geral de cada um destes serviços. Para mais informações sobre estes programas, consulte o site da VeriSign na Internet http://www.verisign.com. Todos os serviços estão sujeitos a contratos específicos com a VeriSign ou Afiliada.

1.1.2.1. Serviços de Distribuição de Certificados

1.1.2.1.1. PKI Gerenciada VeriSign®

A PKI Gerenciada da VeriSign é um serviço completo de PKI gerenciada que permite a Clientes corporativos da VeriSign e suas Afiliadas a fornecer Certificados a indivíduos, bem como funcionários, parceiros, fornecedores e clientes, como também em dispositivos como servidores,

roteadores e firewalls. A PKI Gerenciada possibilita às empresas o envio seguro de mensagens, proteção de intranet, extranet, rede virtual privada (VPN) e aplicações de comércio eletrônico. Usando a PKI Gerenciada, uma empresa pode realizar o gerenciamento de ciclo de vida de um Certificado e explorar a alta disponibilidade dos serviços de processamento de Certificados da VeriSign e suas Afiliadas, sem assumir a tarefa de projetar, fornecer, terceirizar pessoal e fazer a manutenção de sua própria PKI. A VeriSign expandiu seus serviços de PKI Gerenciada com o Go Secure!SM, um conjunto de serviços plug-and-play, feitos para acelerar a forma com que as empresas implantam aplicações de segurança para comércio eletrônico, incluindo aplicativos clientes de e-mail e navegação, diretórios, serviços de rede virtual privada, servidores da Web e soluções de planejamento de recursos corporativos. PKI Gerenciada é, em seu âmago, um serviço de terceirização. Os Clientes da VeriSign ou suas Afiliadas que obtém uma PKI Gerenciada VeriSign (“Clientes de PKI Gerenciada”) são classificados em três categorias. Primeiro, alguns Clientes de Gerenciada (“Clientes de PKI Gerenciada”) fornecem Certificados clientes para se tornar uma Autoridade Certificadora na rede VTN. PKI Gerenciada - Clientes de PKI Gerenciada realizam as funções de ‘interface’ de aprovação ou reprovação de Solicitação de Certificados da AR, usando a funcionalidade da PKI Gerenciada. As funções das ARs são um sub-conjunto de funções da AC. Ao mesmo tempo, o Cliente de PKI Gerenciada pode dinamizar a infra-estrutura segura de PKI da Rede de Confiança VeriSign, terceirizando todas as funções “secundárias” de emissão, revogação, gerenciamento e renovação de Certificados para a VeriSign ou uma Afiliada. (Para uma discussão sobre Afiliadas e Centros de Processamento, veja o § 1.1.2.1.2 da PC).

A segunda categoria de Cliente de PKI Gerenciada (“Clientes de PKI Gerenciada e PKI Gerenciada Lite”) utiliza a PKI Gerenciada Lite, que oferece segurança para pequenas empresas e organizações do que os Cliente de PKI Gerenciada tradicional Os Clientes de PKI Gerenciada Lite se tornam Autoridades de Registro associadas a uma AC da VeriSign ou Afiliada, que é compartilhada entre os Clientes de PKI Gerenciada Lite da VeriSign ou de uma Afiliada para aquela classe específica de Certificados. Os Clientes de PKI Gerenciada Lite, similar aos Clientes de KI Gerenciada, aprovam ou rejeitam Solicitações de Certificado usando a funcionalidade de PKI Gerenciada, como também solicitam a revogação e renovação de Certificados. Como para os Clientes de PKI Gerenciada, a ou outro Centro de Processamento realiza as funções secundárias de emissão, gerenciamento, revogação e renovação de Certificados.

As categorias finais de Clientes de PKI Gerenciada aprovam Solicitações de Certificado para Certificados de servidores, conhecidos como IDs de Servidores Seguros (Secure Server ID) (“PKI Gerenciada para Clientes SSL”) e para certificados de servidor conhecidos como ID de Servidor Global (“Clientes de PKI Gerenciada para Servidor Global”). (Para uma discussão sobre as diferenças entre as IDs de Servidor Seguro e IDs de Servidor Global, consulte o § 1.3.4.1.3.2. da PC) PKI Gerenciada para Clientes SSL e PKI Gerenciada para Clientes SSL Premium Edition se tornam Autoridades de Registro associadas à uma Autoridade Certificadora da VeriSign, que é compartilhada entre todas as PKIs Gerenciadas da VTN para Clientes SSL ou PKI Gerenciada para Clientes SSL Premium Edition. PKI Gerenciada para Clientes SSL e PKI Gerenciada para Clientes SSL Premium Edition, como outro Clientes de PKI Gerenciada, aprovam ou rejeitam Solicitações de Certificado usando a funcionalidade de PKI Gerenciada, como também solicitam a revogação e renovação de Certificados. Além disso, como em outros Certificados de PKI Gerenciada, a VeriSign realiza todas as funções secundárias de emissão, gerenciamento, revogação e renovação de Certificados.

Clientes de PKI Gerenciada e Clientes de PKI Gerenciada Lite não têm permissão para aprovar Solicitações de Certificado de qualquer pessoal que não seja Indivíduos Afiliados, exceto como indicado abaixo.. Clientes de PKI Gerenciada não podem aprovar Solicitações de Certificado para Certificados da VTN emitidos para o público em geral. O Centro de Serviços de Autenticação oferece uma solução para organizações que desejam obter Certificados para indivíduos não-afiliados e representantes da empresa. Consulte o § 1.1.2.2.1 da PC.

Além disso, a VeriSign oferece um serviço quer amplia o escopo da afiliação permitida na PKI Gerenciada, denominado “Two-Tier Authentication Service”, ou Serviço de Autenticação

de Nível Duplo. Os Clientes de PKI Gerenciada talvez desejem obter Certificados para uma base de usuários que eles não conhecem, porém realizam transações com tais usuários. Por exemplo, um fabricante e Cliente de PKI Gerenciada pode quere distribuir Certificados, não para seus próprios funcionário, mas para funcionários de revendedoras de seus produtos. Os funcionários da fábrica conhecem os revendedores, mas não o dono/fabricante. O Serviço de Autenticação de Nível Duplo permitirá ao fabricante distribuir Certificados aos funcionários dessas revendedoras.

De forma específica, o Serviço de Autenticação de Nível Duplo possibilita a um Cliente de PKI Gerenciada, como o fabricante, a delegar funções de AR às organizações com as quais ele tem um relacionamento comercial, como as revendedoras neste exemplo. Essas organizações devem celebrar um contrato, aprovado pela VeriSign ou uma Afiliada, confirmando esta delegação e solicitando que se cumpram as obrigações da RA. Os Solicitantes ao Certificado devem ser Indivíduos Afiliados em relação a estas organizações.

Uma PKI Gerenciada para Cliente SSL ou PKI Gerenciada para Cliente SSL Premium Edition pode apenas aprovar Solicitações de Certificado de servidores dentro de suas próprias organizações. PKI Gerenciada para Clientes SSL e PKI Gerenciada para Clientes SSL Premium Edition não têm permissão para aprovar Solicitações de Certificado de Classe 3 de qualquer servidor fora de suas respectivas organizações, tampouco podem emitir Certificados para o público em geral.

1.1.2.1.2. Programa de Afiliação VeriSign

A VTN expande os serviços de certificação e PKI da VeriSign em âmbito global.. A VeriSign fechou parcerias com os principais provedores de comércio eletrônico no mundo todo, para oferecer serviços, atendimento e suporte localizados ao Cliente. Este provedores, Afiliadas da VeriSign atuam como Parte Confiante de confiança dentro da rede VTN, tornando-a uma rede de confiança interoperável e global, constituída por um sistema de provedores de serviços de autenticação distribuídos no mundo todo. Afiliadas da VeriSign são empresas líderes nos setores de tecnologia, telecomunicações e serviços financeiros em seus respectivos países ou territórios. As Afiliadas acrescentam a infra-estrutura computacional, experiência em telecomunicações, centros de atendimento ao cliente e suporte a dados 7 dias por semana, 24 horas ao dia, integração de sistemas e processamento de transações seguras à tecnologia de emissão de Certificados VeriSign, tornando-se ACs e ARs dentro da rede VTN.

As Afiliadas oferecem presença local da VTN em seus respectivos países ou territórios. Eles comercializam os serviços VTN em seus países ou territórios. Além disso, as Afiliadas captam Clientes e Assinantes, celebram contratos com vários participantes da VTN e oferecem suporte ao cliente a seus Clientes e Assinantes..

O Programa de Afiliação da VeriSign comporta dois tipos de Afiliadas. Primeiro, as Afiliadas se tornam “Centros de Processamento”, criando uma hospedagem segura de instalações, dentre outras coisas, sistemas de ACs, incluindo módulos de criptografia portando chaves privadas para uso na emissão de Certificados. Os Centros de Processamento atuam como ACs na VTN, realizando todos os serviços de ciclo de vida de Certificados, como a emissão, gerenciamento, revogação e renovação de certificados. Eles também oferece serviços de ciclo de vida pra seus Clientes de Gerenciada ou Clientes de PKI Gerenciada de outros Centros de Serviço a ele subordinados.

Depois, as Afiliadas se tornam “Centros de Serviço”, o que não implementa uma instalação para serviços de ciclo de vida de certificado e funções secundárias. Em vez disso, os Centros de Serviço aprovam ou rejeitam Solicitações de Certificado, no caso de Certificados de Varejo, ou no caso de Certificados de PKI Gerenciada, os centros de serviço coordenam com um Centro de Processamento o fornecimento de serviços secundários de ciclo de vida de Certificados aos Clientes de PKI Gerenciada. Afiliadas - Centros de Serviço que oferecem Certificados a clientes (Centros de Atendimento ao Cliente) se tornam ACs dentro da VTN, porém terceirizam as funções secundárias com a VeriSign ou outro Centro de Processamento. Ao fornecer Certificados de servidor, os Centros de Serviço passam a ser Autoridades de Registro (ARs) dentro da VTN, de uma AC VeriSign que emite IDs de Servidor Seguro e IDs de Servidor Global. Estes Centros

de Serviço (Centros de Serviços para Servidores) realizam as funções de aprovação e reprovação Solicitações de Certificado para IDs de Servidor Seguro ou IDs de Servidor Global. Os Centros de Serviço também podem fornecer serviços de PKI Gerenciada da VeriSign a outros Clientes de PKI Gerenciada. Estes Clientes de PKI Gerenciada celebram um contrato de PKI Gerenciada com o Centro de Serviço, que por sua vez, conforme seu contrato com a VeriSign ou outro Centro de Processamento organiza com o Centro de Processamento para fornecer serviços secundários de ciclo de vida de Certificados a estes Clientes de PKI Gerenciada.

Afiliadas, sejam elas Centros de Processamento ou Centros de Serviço, têm a opção de atuar em três frentes de negócios, "Consumidor", "Web Site" e "Empresa". "Consumidor" refere-se às Afiliadas que oferecem Certificados de Varejo Classe 1, 2 ou 3 em seus sites a Solicitantes ao Certificado. Os Centros de Processamento na linha de negócio Consumidor são ACs, enquanto os Centros de Serviço na linha de negócios Consumidor passam a ser ARs. "Web Site" refere-se a Afiliadas que fornecem IDs de Servidor Segurou e/ou IDs de Servidor Global na forma de Certificados de Varejo fornecidos diretamente às organizações que se inscrevem no site da Afiliada. Todas as Afiliadas atuantes no ramo de negócios de "Web Site" são Autoridades de Registro para uma Autoridade Certificadora VeriSign, embora possam ser Centros de Processamento em uma ou mais linhas de negócio.

"Empresa" refere-se a Afiliadas que oferecem serviços de PKI Gerenciada VeriSign a seus Clientes. Estas Afiliadas, seja um Centro de Processamento ou um Centro de Serviço, obtém Clientes de PKI Gerenciada, e celebram o contrato de PKI Gerenciada adequado para a prestação de serviços secundários. A linha de negócios Empresa é, por sua vez, dividida em duas linhas de negócio: Empresa-cliente e Empresa-servidor. Os negócios da Empresa-cliente concentram-se em organizações que desejam obter Certificados-clientes, que podem vir a ser Clientes de PKI Gerenciada ou Clientes de PKI Gerenciada Lite, através da celebração do Contrato de PKI Gerenciada com uma Afiliada. Se a Afiliada é um Centro de Processamento, ela, então, realiza suas próprias funções secundárias para estes Clientes de PKI Gerenciada. Em comparação, um Centro de Serviço, de acordo com seu contrato com o Centro de Processamento, atribui ao Centro de Processamento as funções secundárias para os Clientes de PKI Gerenciada ou Clientes de PKI Gerenciada Lite do Centro de Serviço.

Com relação a negócios servidor Corporativo, as organizações de desejam obter IDs de Servidor Seguro ou IDs de Servidor Global podem ser tornar PKIs Gerenciadas para Clientes SSL ou Clientes SSL Premium Edition, celebrando um Contrato de PKI Gerenciada com a Afiliada.

As Afiliadas que atuam na área de negócios de servidores Corporativos são Centros de Serviço, que terceirizam com a VeriSign as obrigações de execução de serviços de PKI Gerenciada para estes Clientes de PKI Gerenciada.

Uma Afiliada pode ter tanto um Centro de Serviço como um Centro de Processamento. Por exemplo, uma Afiliada por optar por emitir Certificados de sua instalação segura como um Centro de Processamento na linha de negócios para Consumidor, porém aprovam Solicitações de Certificado para Certificados-servidor como um Centro de Serviço na linha de negócios para Web Site.

1.1.2.1.3. Programa Universal do Centro de Serviço Universal e Outros Programas para Revendedores

A VeriSign e Afiliadas (previamente autorizado por escrito pela VeriSign) podem desenvolver um programa para a realização de contratos com entidades que anunciam seus serviços a mercados específicos ("Revendedores"). Além disso, O Programa Universal de Centros de Serviços permite que "Centros de Serviço Universais" promovam os serviços da VeriSign em mercados específicos usando uma plataforma de software especializada para o gerenciamento de implantação de PKI complexo. Os Centros de Serviço Universais são importantes provedores de serviços que vendem PKIs Gerenciadas e serviços relacionados a seus Clientes de PKI Gerenciada e administram as implementações das PKIs desses Clientes usando a plataforma de software do Programa Universal de Centro de Serviços. Os Revendedores e Centros de Serviço Universais devem cumprir com as exigências impostas pela VeriSign e Afiliadas, através de suas PCs, contratos secundários e outros documentos como referência.

Os Centros de Serviço Universal não se tornam automaticamente Autoridades Certificadoras. Em vez disso, seus Clientes de PKI Gerenciada se tornam ACs, e é dever do Centro de Serviços Universal obter Clientes, firmar com eles os contratos apropriados e fornecer suporte ao cliente

1.1.2.1.4. O programa Web Host

O Programa Web Host permite que empresas atuem como host ("Web Host") de sites de clientes, para gerenciar os processos de ciclo de vida das IDs de Servidor Seguro de varejo e IDs de Servidor Global para seus clientes. Um Web Host pode ser um provedor de serviços da Internet, um integrador de sistemas, um Revendedor, um consultor técnico, um provedor de serviços de aplicativo, ou similar. O Programa Web Host oferece a funcionalidade de gerenciamento de pedido feita conforme as necessidades da organização do Web, para um gerenciamento de ciclo de vida simplificado.

O Programa WebHost permite que Web Hosts inscrevam-se para IDs de Servidor Seguro e IDs de Servidor Global em nome de Assinantes (usuários final), que são clientes desses Web Hosts. Embora ajudem no processo de inscrição (veja § 4.1.1 da PC), os Web Hosts não executam funções de validação, que são feitas por um Centro de Processamento ou Centro de Serviços.

Além disso, os Web Hosts não são os Assinantes de IDs de Servidor Seguro e IDs de Servidor Global. Os clientes de Web Hosts obtém estes Certificados como os verdadeiros Assinantes e são responsáveis pelo cumprimento das obrigações do Assinante, conforme o Contrato do Assinante. Os Web Hosts têm uma obrigação em fornecer o contrato de assinante aplicável a seus clientes, para informá-los de suas obrigações.

1.1.2.1.5. VeriSign Gateway Services

O software de servidor de Certificados da Netscape e Microsoft permite que as organizações tenham suas próprias autoridades certificadoras. Em geral, estas organizações podem estabelecer suas ACs dentro de uma hierarquia privada, não podem interoperar com outro domínios sem uma interoperação ou organização de distribuição de raiz. Entretanto, os serviços Gateway permitem a estas ACs entrar na VTN, e conseqüentemente, permitir que seus usuários interoperem com Parte Confiante da VTN no mundo.

Os clientes Gateway se tornam ACs dentro da VTN quando um Cliente Gateway firma um contrato adequado com VeriSign ou uma Afiliada, onde uma de suas ACs VTN emitem um Certificado de Gateway ao Cliente Gateway O Certificado de Gateway certifica a chave pública do Cliente Gateway. Portanto, quando um Terceiro obtém um Certificado emitido por um Cliente Gateway, este Terceiro é capaz de validar uma cadeia de certificados com a ajuda dos Certificados PCA VTN incorporado ao software do terceiro. Sendo assim, os serviços Gateway tornam desnecessário para um Cliente Gateway distribuir um Certificado de raiz com assinatura própria a partir de sua AC.

Depois de emitido o Certificado Gateway, um Cliente Gateway é relacionado a um Centro de Processamento. A partir de uma instalação de segurança, ele emite, gerencia e revoga Certificados. Os Assinantes devem ser Indivíduos Afiliados com relação ao Cliente Gateway. . No momento, o programa Gateway cobre apenas Certificados de Classe 1. Portanto, os requisitos de segurança de Clientes Gateway são mais brandos que os Centros de Processamento, que emite múltiplas classes de Certificados.

1.1.2.2. Serviços de Certificação de Valor Agregado

1.1.2.2.1. Serviços de Autenticação

A VeriSign e Afiliadas oferecem serviços de autenticação para empresas, como um acréscimo benéfico aos serviços de PKI Gerenciada. Nestes serviços, a VeriSign ou a Afiliada confirmarão a identidade do Solicitantes ao Certificado em nome dos clientes Este tipo de serviço executa funções de autenticação para os Clientes de PKI Gerenciada de forma terceirizada. Estes Clientes de PKI Gerenciada pode terceirizar a autenticação de toda ou parte de sua base de

usuários Assinantes. Comércios e empresar que já conhecem parte de seus usuários podem considerar útil terceirizar a autenticação de uma parte desconhecida de sua base de usuários. A execução de serviços terceirizados de autenticação estará sujeita a um contrato com a VeriSign ou Afiliada.

Ao ponto em que a VeriSign ou uma Afiliada conduz certas atividades de autenticação para Clientes de PKI Gerenciada, onde a VeriSign ou uma Afiliada seriam obrigadas a cumprir com as obrigações desta PC do Cliente de PKI Gerenciada em seu nome. O cumprimento dessas obrigações não exime o Cliente de PKI Gerenciada de suas obrigações na PC, ao ponto em que o Cliente de PKI Gerenciada detém as responsabilidades de autenticação para parte de sua base de usuários ou outras funções, tais como iniciar solicitações de revogação.

Outro serviço de autenticação de valor agregado é o programa do Centro de Serviços de Autenticação da VeriSign ("VeriSign Authentication Service Bureau"). Este programa possibilita que a VeriSign e Afiliadas confirmem a identidade dos Assinantes em nome de uma organização. A VeriSign e Afiliadas oferecem este serviço à organizações como operadores de extranets ou mercados B2B ou B2C através de um contrato adequado para estes serviços ("Clientes ASB"). No programa do Centro de Serviços de Autenticação, a VeriSign e Afiliadas oferecem Certificados individuais de Classe 2 ("Certificados ABS Individuais Classe 2") e Certificados corporativos de Classe 3 usados somente por representantes autorizados de organizações interagindo com o Cliente ASB ("Certificados ASB Corporativos de Classe 3"). Uma vez que a VeriSign ou a Afiliada fornece serviços de autenticação como um terceirizador, o Cliente ASB se livra da despesa e trabalho de implementar a política, tecnologia e pessoal necessário para confirmar a identidade de Solicitantes a Certificado desconhecidos.

Como a PKI Gerenciada , o Centro de Serviços de Autenticação é um serviço terceirizado. Os Clientes ASB assinam um contrato com a VeriSign ou uma afiliada para se tornar uma AC. Esta AC emite certificados comercializados em conjunto, indicando que o Cliente ASB é uma AC. O Cliente ASB, porém, terceiriza a maioria das funções de AC, tanto primárias como secundárias à VeriSign ou Afiliada. A única função de AC que o Cliente ASB mantém é a obrigação de iniciar a revogação de Certificados emitidos pela AC do Cliente ASB, conforme rege o parágrafo 4.4.1.1 da PC, embora a VeriSign ou a Afiliada também possam processar solicitações de revogação e comunica-las diretamente. Com exceção da obrigação do Cliente ASB em iniciar a revogação, a VeriSign ou a Afiliada realizam todas as confirmações de identidade e serviços de ciclo de vida de Certificado para o cliente ASB. A VeriSign ou a Afiliada quando oferecem serviços do Bureau de Autenticação ("Provedor ASB") Authentication Service Bureau services ("ASB Provider") atuam como AR para o cliente ASB. Um Provedor ASB pode ser um Centro de Processamento ou Centro de Serviço.

1.1.2.2.2. Serviço de Cartório Digital VeriSign

O "Serviço de Autenticação Notarial Digital VeriSign" é um serviço que oferece uma declaração assinada digitalmente ("Recibo Digital") de que determinado documento ou conjunto de dados existiram em certo momento. A VeriSign age como uma terceira parte que oferece garantia da hora e a integridade do documento ou informações. Uma das principais finalidades do Serviço de Autenticação Notarial Digital VeriSign é a obtenção de um Recibo Digital de um documento que faz parte de uma transação comercial, mostrando que o documento transacional existiu em dado momento da transação. O Serviço de Autenticação Notarial Digital VeriSign atende aos requisitos de comércio eletrônico de Parte Confiante, protege o arquivamento de dados, confirmação de pagamento à prova de violação e auditoria de processo empresarial. Este serviço é uma oferta exclusiva para Clientes de PKI Gerenciada e seus Assinantes.

A VeriSign estabeleceu uma "Autoridade em Datação) e uma "Autoridade Certificadora em Datação". A CA de Datação emitiu um Certificado corporativo de Classe 3 à Autoridade de Datação, que lhe permite assinar digitalmente Recibos Digitais.

Ao usar o Serviço de Autenticação Notarial da VeriSign, o software cliente do usuário envia um hash assinado digitalmente do documento à Autoridade de Datação. A assinatura digital deve ser verificável referente a um Certificado de PKI Gerenciada durante o Período Operacio-

nal. Uma vez recebido, a Autoridade de Datação verifica a assinatura digital e assegura que o Cliente da PKI Gerenciada possui uma conta válida. Assim, a Autoridade de Datação cria uma datação eletrônica dos dados submetidos, consultando uma fonte segura de informações de datação. A Autoridade de Datação então combina a datação com um hash no documento, para formar um objeto de dados que possa ser assinado digitalmente pela Autoridade, criando assim um Recibo Digital. Os Recibos Digitais são armazenados pela VeriSign por um período específico com as informações sobre o documento fornecidas pelo usuário, que poderão ser posteriormente disponibilizadas às partes interessadas para fins de resolução de disputas e auditorias, se necessário. Um documento não precisa ser divulgado à VeriSign para que seja digitalmente notado; apenas o hash é enviado ao Serviço de Cartório Digital VeriSign.

A Autoridade de Datação obtém a informação cronológica a partir de um servidor de tempo da VeriSign sincronizado por meio de GPS com o Tempo Universal Coordenado (UTC). Enquanto a precisão do servidor de tempo de VeriSign é de precisa em um segundo, devido à natureza de tráfego da Internet, a hora mostrada em um Recibo Digital pode ser 30 segundos maior ou menor que o Tempo Universal Coordenado.

1.1.2.2.3. Plano de Proteção NetSureSM.

O Plano de proteção NetSure é uma programa de garantia extendida que se aplica ao Subdomínio VeriSign da VTN e Subdomínios das Afiliadas participantes. O Plano de Proteção NetSure oferece a Assinantes que recebem Certificados de Varejo, Certificados ASB Individuais de Classe 2 e Classe 3 proteção contra incidentes como roubo, corrupção, prejuízo ou revelação não-intencional da chave privada do Assinante (correspondendo à chave pública no Certificado), bem como falsidade ideológica e prejuízos decorrentes do uso do Certificado do Assinante. O Plano de Proteção NetSure também fornece proteção a Parte Confiante, quando estes necessitam de Certificados cobertos pelo Plano de Proteção NetSure. O NetSure é um programa fornecido pela VeriSign, que contam com um seguro obtido de corretores comerciais. Para informações gerais sobre o Plano de Proteção NetSure e a relação de Certificados cobertos pelo seguro, consulte http://www.verisign.com/netsure.

A proteções do Plano de Proteção NetSure também são oferecidas mediante uma taxa a Clientes de PKI Gerenciada da VeriSign. Eles podem obter proteção com o Plano de Proteção NetSure, sujeito aos termos deste contrato de serviço. Este serviço não só extende as proteções do Plano de Proteção NetSure a Assinantes cujas Solicitações de Certificado foram aprovadas pelo Cliente de PKI Gerenciada como também extende tais proteções ao próprio Cliente de PKI Gerenciada. Por exemplo, se o Cliente de PKI Gerenciada aprova uma Solicitação de Certificado de um funcionário do Cliente de PKI Gerenciada, que usa o Certificado para fins comerciais do Cliente da PKI Gerenciada, e se as ações do Assinante resultam em prejuízos, a parte a se responsabilizar pelos prejuízos causados pode vir a ser o Cliente da PKI Gerenciada, que exerce o papel de empregador do Assinante. Se houver a cobertura do Plano de Proteção NetSure, o Cliente de PKI Gerenciada pode solicitar uma indenização pelo prejuízo prolongado pelas ações do Assinante.

1.1.2.3. Tipos Especiais de Certificado

1.1.2.3.1. Serviços de Certificados Wireless

A VeriSign oferece certificados corporativos para aplicações sem fio. Os certificados VeriSign para servidores WAP permite estabelecer conexões seguras entre servidores e dispositivos sem fio como telefones celulares digitais e outros dispositivos móveis. A tecnologia “WAP” (Wireless Application Protocol) permite a autenticação entre servidores wireless Web e dispositivos móveis através do “WTLS” (Wireless Transport Layer Security). O WTLS é um parente próximo do SSL, o protocolo primário usado para proteger a Internet convencional.

Os Certificados WTLS são usados para autenticar um servidor WTLS a um cliente WTLS e fornecer uma base para estabelecer uma chave de criptografia em uma sessão cliente-servidor. Os Certificados WTLS são como Certificados de servidor SSL, exceto que os Certificados WTLS não estão no formato X.509. Eles são certificados menores e mais simples que os X.509, que facilitam seu processamento em aparelhos com poucos recursos.

1.1.2.3.2. Serviço de Gerenciamento de Chave PKI Gerenciada VeriSign

O Serviço de Gerenciamento de Chave é um sistema de aplicativos instalado nas instalações de uma empresa, formando parte da família de produtos PKI Gerenciada VeriSign. O serviço de gerenciamento de chave opera com um serviço de PKI Gerenciada VeriSign. Esta combinação permite ao gerente de uma empresa controla as operações de backup e recuperação de chaves privadas e certificados digitais.1

As chaves privadas são armazenadas nas instalações da empresa, de forma criptografada.. Cada chave privada de Assinante é individualmente criptografada, com sua própria chave simétrica de triplo DES. Um registro "Key Escrow Record" (KER) é gerado, e depois, a chave DES triplo é combinada com uma máscara de chave de sessão aleatória, gerada por hardware e depois destruída. Somente a chave de sessão resultante (MSK - masked session key) é enviada e armazenada na VeriSign. O KER (contendo a chave privada do usuário final) e a máscara aleatória da chave de sessão são armazenados no banco de dados do gerenciador de chaves, nas instalações da empresa.

A recuperação de uma chave privada e certificado digital requer que o administrador da PKI Gerenciada registre corretamente no Centro de Controle de PKI Gerenciada, selecionando o par de chaves adequado para recuperar e clicar em um link de "recuperação". Somente depois que um administrador aprovado clicar no link "recover" (recuperar), a MSK do par de chaves é devolvida, do banco de dados de PKI Gerenciada. O Administrador de Chave combina a MSK com uma máscara de chave de sessão aleatória, e gera novamente a chave DES tripla, que foi originalmente usada para criptografar a chave privada, permitindo a recuperação da chave privada do usuário final. E finalmente, um arquivo criptografado PKCS#12 é enviado de volta ao administrador e distribuído ao usuário final.

Uma empresa usando o KMS deve, pelo menos:

. • Notificar assinantes que suas chaves privadas foram escrituradas

. • Protege as chaves escrituradas dos assinantes contra a divulgação não autorizada,

. • Proteger todos os dados, incluindo a(s) chave(s) do próprio administrador, que podem ser utilizadas par recuperar chaves escrituradas de assinantes.

. • Liberar chaves escrituradas de assinantes somente para solicitações de recuperação devidamente autenticadas e autorizadas.

. • Revogar o par de chaves do Assinante antes da recuperação da chave de codificação.

1 A VeriSign pode, sob circunstâncias limitadas, hospedar KMSs em nome de um cliente corporativo. Em tal cenário, o KMS atuará conforme descrito na seção 1.1.2.3.2, exceto pela parte normalmente hospedada pela empresa, agora hospedada em uma instalação segura da VeriSign. A única pessoa autorizada a recuperar chaves de codificação escrituradas em nome da empresa são os administradores da empresa. O banco de dados de gerente de chave deverá ser guardado em um local físico separado do banco de dados que armazena o MSK. O acesso da VeriSign ao banco de dados do Administrador de Chave será restrito às Pessoas Autorizadas, pelo uso de controle de acesso por senha e nome de usuário duplo.

. • Não deverá fornecer qualquer informação sobre recuperação de chave ao assinante exceto quando o próprio tenha solicitado a recuperação.

. • Não tornar público ou permitir a divulgação de chaves escrituradas ou informações relacionadas a Parte Confiante, a menos que exigido por lei, determinação governamental ou regulamentação; pela política organizacional da empresa ou por meio de mandato judicial da jurisdição competente.

1.1.2.3.3. Serviço de Roaming VeriSign

O "Serviço de Roaming VeriSign," oferecido a Clientes de PKI Gerenciada, permite a um Assinante assinar digitalmente transações importantes, como compra e venda de ações e obter acesso a informações confidenciais, sem estar preso a um único terminal cliente que hospeda sua chave privada. O serviço de roaming tem se tornado comum em muitos

ambientes de trabalho, e tem prevalecido consideravelmente nos ambientes de consumo, como quiosques públicos. Desenvolvido pela equipe de pesquisa da VeriSign em parceria com o RSA Laboratories, a tecnologia de roaming da VeriSign permite que assinantes usem o serviço (Assinantes Roaming") para baixar suas chaves privadas e concluir as operações de chave privada em diferentes terminais clientes. O Cliente de PKI Gerenciada não precisa distribuir e oferece suporte à cartões inteligentes e outros dispositivos de sinal.

O Assinante Roaming pode usar sua chave privada em qualquer terminal cliente. O Serviço de Roaming VeriSign codifica as chaves públicas dos Assinantes com chaves simétricas que são divididas e armazenadas em um ou dois servidores, em dois locais distintos, para proteger contra ataques um único servidor de credenciais. A chave pública está armazenada em uma forma criptografada no Servidor de Roaming Corporativo. O assinante do serviço de roaming faz sua autenticação no(s) servidor(es) usando uma senha a chave criptografada e os componentes da chave simétrica necessários para decodificar a chave privada do Assinante são baixados no terminal cliente. No terminal cliente, a chave simétrica é reconstituída, a chave privada do Assinante é decodificada e então fica disponível para uso durante uma única sessão. Terminada a sessão, a chave privada no terminal cliente é excluída de forma irrecuperável.

1.2. Identificação

A VeriSign, na posição de autoridade determinadora das políticas, determina a política de certificado nesta PC para cada Classe de Certificado uma extensão de valor OID (object identifier) definida nesta seção. Os valores de OID usados para as três classes de Certificados do usuário final são:

. • A Política de Certificado Classe 1: VeriSign/pki/policies/vtn-cp/class1 (2.16.840.1.113733.1.7.23.1).

. • A Política de Certificado Classe 2: VeriSign/pki/policies/vtn-cp/class2 (2.16.840.1.113733.1.7.23.1).

. • A Política de Certificado Classe 3: VeriSign/pki/policies/vtn-cp/class3

(2.16.840.1.113733.1.7.23.1). Estes OIDs de Certificados de Assinantes correspondem à Classe apropriada.

1.3. Comunidade e Aplicabilidade

A comunidade regida por esta PC é a Rede de Confiança VeriSign (VTN - VeriSign Trusted Network). A Rede de Confiança da VeriSign (" VTN") é uma PKI que acomoda uma grande comunidade pública de usuários, com as mais variadas necessidades em comunicação e segurança da informação. A VTN é o domínio público regido por esta PC, que por sua vez é o documento que rege a VTN.

1.3.1. Autoridades Certificadoras

O termo Autoridade Certificadora é um termo guarda-chuva que se refere a todas as entidades que emitem certificados dentro da VTN. O termo AC é composto por uma subcategoria de emissores chamados Autoridades Primárias de Certificação. As APCs são as raízes de três domínios, um para cada classe de Certificado. Cada APC é uma entidade VeriSign. Subordinadas às APCs estão as Autoridades Certificadoras que emitem Certificados a Assinantes (usuário final) ou outras ACs. As ACs também possuem cinco categorias: (1) Centros de Processamento, (2) Centros de Atendimento ao Cliente, (3) Clientes de PKI Gerenciada, (4) Clientes Gateway e (5) Clientes ASB.

Os centros de processamento nas linhas de negócios voltada ao Consumidor e Web Site são as ACs que realizam as funções primárias e secundárias de AR, a menos que as funções primárias sejam delegadas a uma AR. Os Centros de processamento na linha de negócios Corporativa são terceirizadores das funções de CA para Clientes de PKI Gerenciada. As funções primárias da AR consistem em estabelecer procedimentos de registro, confirmação de identidade, aprovação ou reprovação de Solicitações de Certificado, iniciar revogações e aprovar ou reprovar solicitações de renovação de certificados. As funções secundárias incluem a emissão, gerenciamento , revogação e renovação de certificados de uma instalação segura protegendo chaves privadas da AC. A VeriSign é um Centro de Processamento que comporta todas as APCs da VTN e certas ACs em sua instalação segura de ACs. As Afiliadas também podem estabelecer um Centro de Processamento com a aprovação da VeriSign.

Os Centros de Atendimento ao Cliente, por sua vez, são Afiliadas atuando como ACs, que não possuem seus

próprios centros de processamento. Elas realizam funções primárias de AR, porém terceirizam a um centro de processamento, seja da VeriSign ou um Centro de Processamento Afiliado, suas funções secundárias. Clientes de PKI Gerenciada, como Centros de Serviço, passam a ser ACs dentro da VTN. Como Centros de Atendimento ao Cliente, os Clientes de PKI Gerenciada terceirizam as funções secundárias a um Centro de Processamento, enquanto mantém as funções de AR. Clientes Gateway que usam o software de servidor da Nestcape ou Microsoft para emitir Certificados de Classe 1 Os Clientes Gateway executam tanto as funções primárias como secundárias. Finalmente, o contrato de Clientes ASB com a VeriSign ou uma Afiliada se torna uma AC, que emite Certificados nomeando o Cliente ASB como a Autoridade Certificadora. Os Clientes ASB, por sua vez, terceirizam à VeriSign ou Provedora ASB Afiliada todas as funções primárias e secundárias, exceto pela obrigação de iniciar a revogação de Certificados permitido pela AC do Cliente ASB, conforme dita o parágrafo 4.4.1.1 da PC.

Uma AC da VTN tecnicamente fora das três hierarquias sob as quais cada uma das APCs é a Autoridade de Certificação de Servidor Seguro RSA, obtida pela VeriSign com a RSA Security Inc. A AC de Servidor Seguro RSA não possui uma AC superior, como uma raiz ou uma APC. Em vez disso, ela atua como sua própria raiz, emitindo seu próprio Certificado raiz com auto-assinatura. Ela também emite Certificados a Assinantes. Assim, a hierarquia de servidor seguro RSA consiste apenas na AC de Servidor Seguro RSA. A AC de Servidor Seguro RSA emite IDs de servidor seguro, que são avaliadas como Certificados corporativos de classe 3.

Embora A CA de Servidor Seguro RSA não seja certificada sob o APC de Classe 3, os certificados emitidos são funcionalmente equivalentes aos certificados emitidos por uma AC de classe 3. A AC de Servidor utiliza práticas de ciclo de vida de outras ACs de classe 3 dentro da VTN. Assim, a VeriSign aprovou e determinou a Autoridade Certificadora de Servidor Seguro RSA como uma AC de Classe 3 dentro da VTN. Os Certificados que emite, as IDs de Servidor Seguro são consideradas provas de confiança comparáveis a outros Certificados corporativos de Classe 3.

1.3.2. Autoridades de Registro

As ARs auxiliam a AC, realizando as funções secundárias de confirmação de identidade, aprovação ou reprovação de Solicitações de Certificado, solicitação de revogação de Certificados e aprovação ou reprovação das solicitações de renovação. As ARs das VTNs dividem-se em cinco categorias: (1) Centros de Serviço de Servidor, (2) PKI Gerenciada, (3) Clientes de PKI Gerenciada Lite, (4) PKI Gerenciada para Clientes SSL, (5)PKI Gerenciada para Clientes SSL Premium Edition e (6) Provedores ASB. Outros tipos de Ars são permitidos através de autorização por escrito da VeriSign, e se estas ARs atendem às obrigações definidas para Clientes de PKI Gerenciada, sujeitos a modificações necessárias por conta das diferenças entre a tecnologia de PKI Gerenciada e a tecnologia usada pelas ARs e os termos de um contrato adequado. Os Centros de Serviço de Servidor atuam como Centros de Serviço que aprovam Solicitações de Certificado para Certificados de servidor (IDs de Servidor Seguro e Servidor Global). Eles agem como um AR que auxilia a AC da VeriSign na emissão destes Certificados. Estas ACs da VeriSign incluem a AC de Servidor Seguro RSA, que emite IDs de Servidor Seguro, e a AC de Criptografia Concentrada Universal, que emite IDs de Servidor Global. Os Clientes de PKI Gerenciada Lite se tornam ARs que prestam auxiliam a uma AC da VeriSign ou Afiliada para a emissão de Certificados clientes para Assinantes. De forma similar, a PKI Gerenciada para Clientes SSL e Clientes SSL Premium Edition se tornam ARs usando a PKI Gerenciada que auxilia a AC de Servidor Seguro RSA, a AC de Criptografia Concentrada Universal de Classe 3 da VeriSign, ou AC VeriSign similar para a emissão de IDs de Servidor Global e IDs de Servidor Seguro. Provedores ASB (Clientes de PKI Gerenciada VeriSign) oferecem Serviços do Centro de Serviços de Autenticação aos Clientes ASB. Os Provedores ASB executam tanto as funções primárias como secundárias para ACs de Cliente ASB

1.3.3. Titulares do Certificado

Os Certificados de Classe 1 e 2 são certificados clientes emitidos somente a Assinantes (usuário final). Os Certificados de classe podem ser emitidos a indivíduos, e outros tipos de Certificados podem ser emitidos a organizações. Os Certificados de classe 1 e 2, e Certificados individuais de classe 2 podem ser Certificados de Varejo ou Certificados de PKI Gerenciada. Além disso, os certificados ASB individuais de classe 2 são oferecidos através do Centro de Serviços de Autenticação. Os Certificados de varejo podem ser emitidos para o público em geral. Exceto sob o Serviço de Autenticação de Nível Duplo descrito no parágrafo 1.1.2.1.1 desta PC, indivíduos que obtém Certificados de PKI Gerenciada, devem ser afiliados do Cliente da PKI Gerenciada que aprovou

suas Solicitações de Certificado ou o titular como "Indivíduo Afiliado". Os indivíduos afiliados são pessoas físicos relacionadas a uma pessoa jurídica Cliente de PKI Gerenciada ou Cliente de PKI Gerenciada Lite (i) como diretor, funcionário, parceiro, consultor, estagiário ou outra pessoa dentro da empresa, (ii) como membro de uma comunidade de interesses registrada VeriSign, (iii) ou como uma pessoa mantendo uma relação com a empresa, enquanto esta possui registros comerciais e outros registros que asseguram a identidade de tal pessoal (por exemplo, um cliente).

Clientes de PKI Gerenciada obtendo serviços através do Serviço de Autenticação de Nível Duplo delegam funções de AR à outra organização com a qual se relaciona. Indivíduos obtendo Certificados de PKI Gerenciada devem ser filiados como Indivíduo Afiliado da organização à qual as funções de AR foram delegadas.

Os certificados de administrador de classe 2 são certificados especiais e limitados, que um administrador autorizado da VeriSign, um Cliente de PKI Gerenciada ou Afiliada utiliza exclusivamente para executar funções de Administrador. Os administradores que utilizam estes Certificados são pessoas de confiança que executam funções de gerenciamento de certificados em nome de Centros de Processamento, Centros de Serviço ou Clientes de PKI Gerenciada.

Além de certificados cliente emitidos a indivíduos, os certificados de classe 3 também incluem certificados emitidos a assinantes corporativos. Os certificados ASB corporativos de classe 3 são emitidos para uma organização, cuja chave privada é controlada por um representante autorizado da organização. Os procedimentos de autenticação confirmam que o representante possui autonomia para agir em nome da organização. Além dos certificados ASB de classe 3, os certificados corporativos são emitidos para dispositivos, incluindo:

. • Servidores da Web (Secure Server IDs e Global Server IDs).

. • Servidores OFX e

• Dispositivos que assinam digitalmente códigos e outros tipos de conteúdo. Esta lista de assinantes dos certificados corporativos de classe 3 não é extensa.

As IDs de servidor seguro e servidor global podem ser Certificados de varejo ou de PKI gerenciada. As IDs de servidor seguro e servidor global de varejo serão diretamente emitidas à organização pela VeriSign, depois que esta ou sua Afiliada tenham aprovado a solicitação de Certificado do assinante. As IDs de servidor seguro e servidor global que são Certificados de PKI Gerenciada serão emitidas pela VeriSign após a aprovação da solicitação de Certificado por uma PKI Gerenciada de Cliente SSL ou PKI Gerenciada de Cliente SSL Premium Edition.

As próprias ACs são, do ponto de vista técnico, Assinantes de Certificados, sejam na condição de uma APC que emite seu próprio certificado, com sua assinatura, ou como uma AC que emitiu um Certificado por uma AC superior. A referências a "Assinantes" nesta PC aplicam-se somente aos Assinantes tidos como usuários final.

1.3.4. Aplicabilidade

Esta PC aplica-se a todos os participantes VTN, incluindo a VeriSign, Afiliadas, Clientes, Centros de Serviço Universal, Revendedores, Assinantes e Parte Confiante. Esta PC define as políticas que regem o uso de certificados em cada uma das Classes (1 a 3). Cada classe de certificado é adequada para o uso com as aplicações definidas no parágrafo § 1.3.4.1 da PC. Entretanto, por contrato ou dentro de ambientes específicos (tais como ambiente inter-empresarial), os participantes da rede VTN podem usar procedimentos de validação mais consistentes que aqueles fornecidos nos parágrafos 1.1.1, 1.3.4.1 da PC. Tal utilização estará limitada a tais entidades e sujeitas aos parágrafos 2.2.1.2, 2.2.2.2 da PC, e estas entidades responsabilizar-se-ão por qualquer dano ou prejuízo causado pela utilização.

1.3.4.1. Aplicações Adequadas

As subseções desta seção principal relacionam as aplicações adequadas para os Certificados VTN conforme a Classe. Esta relação, porém, não deve ser extensa

Certificados individuais e alguns certificados corporativos permitem a Parte Confiante verifica as assinaturas digitais. Os participantes da VTN reconhecem e concordam, conforme os limites aplicáveis da lei, que da necessidade de uma transação por escrito, uma mensagem ou outro registro contendo uma assinatura digital verificável, referente a um Certificado VTN é válida, efetiva e aplicável conforme

a mesma mensagem ou registro escrito e assinado em papel. Sujeitos às leis aplicáveis, uma assinatura digital ou transação realizada, referente a um Certificado VT deverá ser efetiva independente da localização geográfica onde o Certificado VTN foi emitido ou onde a assinatura digital foi criada ou utilizada, e independente da localização geográfica da sede da AC ou do Assinante.

A VeriSign periodicamente faz a renovação de chaves das ACs intermediárias. As aplicações ou plataformas de Parte Confiante que tenham uma AC intermediária incorporada como um certificado raiz não podem operar conforme determinado após a renovação de chaves da AC intermediária. A VeriSign, portanto, não garante o uso de ACs Intermediárias como certificados raiz e recomenda que estas não os incorpore a aplicativos e/ou plataformas como certificados raiz. A VeriSign recomenda o uso de Raízes de APCs como certificados raiz.

1.3.4.1.1. Certificados de Classe 1

Os certificados de classe 1 são adequados para uma melhoria modesta na segurança de e-mails através do uso de assinaturas digitais e criptografia de confidencialidade, onde o e-mail requerem um baixo nível de segurança, comparado às classes 2 e 3. Não oferecem uma segurança de identidade do Assinante. Assim, uma assinatura digital feita com uma chave privada correspondente à chave pública em um certificado de classe 1 usando o protocolo S/MIME não pode ser usada para fins de autenticação ou para suporte a NÃO-REPÚDIO. Em vez disso, a função da assinatura digital é adequada como forma de assegurar, quando os correspondentes de um e-mail estão realizando uma série de trocas de mensagens, que as comunicações são originadas da mesma pessoa, e que não foram modificadas sem detecção desde a colocação de sua assinatura digital. A assinatura digital também oferece garantias razoáveis de que o e-mail foi criado por um remetente com um determinado endereço de e-mail. O certificado não oferece qualquer prova de identidade do remetente usando aquele endereço de e-mail. A aplicação de criptografia permite a Parte Confiante usar o certificado do Assinante para criptografar mensagens destinadas ao Assinante, embora a 'terceira parte'-remetente não possa assegura que o destinatário é, de fato, a pessoa nomeada no Certificado.

Os certificados de classe 1 também podem ser usados para autenticação de clientes durante sessões online. O web site ou outro dispositivo pode usar o certificado para assegurar, através de inúmeras sessões, que as sessões estão sendo iniciadas com o mesmo Assinante, possuidor de determinado endereço de e-mail. Reiterando, o certificado não oferece qualquer prova de identidade do Assinante.

1.3.4.1.2. Certificados de Classe 2

Os certificados de classe 2 são adequados para proteger a troca de mensagens inter/intra-organizacional, comercial e pessoal, exigindo um nível médio de segurança em relação às classes 1 e 3. O uso de assinaturas digitais com o protocolo S/MIME permitem a autenticação de identidade dos correspondentes do e-mail, integridade da mensagem e suporte para a não-repúdio. Adicionalmente, o S/MIME permite o uso de certificados de classe 2 para a troca e/ou criptografia de chaves de sessões para codificar e-mails. Os certificados de classe 2 também são adequados para autenticação cliente, onde o web site ou outro dispositivo requer uma prova de identidade de nível médio de segurança com a Classe 1 e 3. A autenticação cliente pode, por exemplo, fornecer acesso ao controle de bancos de dados e web sites protegidos

1.3.4.1.3. Certificados de Classe 3

Certificados Individuais de Classe 3

Os certificados de classe 3 são adequados para proteger a troca de mensagens inter/intra-organizacional, comercial e pessoal, exigindo um nível médio de segurança em relação às classes 1 e 2.. O uso de assinaturas digitais com o protocolo S/MIME permitem a autenticação de identidade dos correspondentes do e-mail, integridade da mensagem e suporte para a não-repúdio. Adicionalmente, o S/MIME permite o uso de certificados de classe 3 para a troca e/ou criptografia de chaves de sessões para codificar e-mails. Os certificados de classe 3 também são adequados para autenticação cliente, para o controle de acesso, onde o web site ou outro

dispositivo requer uma prova de identidade de alto nível de segurança em comparação às classes 1 e 2.

A VeriSign emite certificados especiais de classe 3 aos Administradores ("Certificados de Administradores"), que aprovam solicitações de certificado em nome dos Centros de Processamento, Centros de Serviço e Clientes de PKI Gerenciada. Os Certificados de Administrador são utilizados para as funções de administrador. Isto é, os Administradores podem usar os certificados de administrador para executar funções como aprovação ou reprovação de solicitações de certificado, iniciar solicitações de revogação e aprovar ou reprovar a renovação de certificados de Assinantes ou de outro Administrador.

Certificados corporativos de Classe 3

A tabela 3 resume os tipos mais comuns de Certificados Corporativos de Classe 3 oferecidos na VTN, cada um deles é descrito abaixo. Note que esta tabela não é uma lista extensa dos Certificados corporativos de classe 3.

Tipos de Classe 3 Certificados Corporativos	Funções	Protocolos de Segurança Aplicáveis e Tecnologia
IDs de Servidor Seguro	Autenticação de servidor, criptografia de confidencialidade e, na comunicação com outros servidores servidores, autenticação cliente	SSL
IDs de Servidor Global	Autenticação de servidor, criptografia de confidencialidade e, na comunicação com outros servidores	SSL e SGC (Server Gated) Cryptography).
	servidores, autenticação cliente	
Certificados OFX	Autenticação de servidor e criptografia de confidencialidade	SSL e OFX (Open Financial Exchange) padrão
Certificados para código e outros assinatura de conteúdo	Autenticação de integridade	Várias tecnologias
Certificados ASB Corporativo de Classe 3 Certificado	Assinaturas digitais, mensagem integridade, criptografia de confidencialidade, autenticação cliente	Centro de Serviços de Autenticação tecnologia

Tabela 3 - Tipos de Certificados Corporativos de Classe 3

Uma ID de Servidor Seguro possibilita aos visitantes do site autenticar a identidade do servidor da Web do Assinante, e criar um canal criptografado entre o navegador e o servidor do Assinante, usando o protocolo SSL. As IDs de Servidor Global são uma espécie de certificado de servidor, que, além de realizar as seguintes funções, ajudam a estabelecer uma proteção criptográfica sólida nas sessões SSL deste servidor. As IDs de Servidor Global podem ainda tornar possível a proteção criptográfica para navegadores "de exportação" que, sem uma ID de Servidor Global, estão limitados ao uso de criptografia de 40 bits.

Um tipo adicional de certificado corporativo de classe 3 é o Certificado OFX (Open Financial Exchange). O OFX é um padrão para a troca de dados financeiros em formato eletrônico entre instituições financeiras, empresas e consumidores pela Internet. O padrão OFX facilita as

atividades bancárias de clientes e pequenos negócios, apresentação de contas e pagamentos, investimentos em ações, títulos e companhias de investimento.

Os negócios que usam o OFX preparam um servidor a comunicação com os clientes. Um certificado OFX permite criar conexões SSL entre o servidor e o cliente. Como nas IDs de Servidor Seguro e Servidor Global, o uso de SSL nos Certificados OFX autenticam o servidor para o cliente, garantem a integridade da mensagem, e criptografa as comunicações entre servidor e cliente.

A VTN oferece certificados de classe 3 para assinatura de códigos e outros tipos de conteúdo para organizações que desejam assinar digitalmente seus códigos e conteúdo digital. A finalidade destes certificados é autenticar a fonte do código ou conteúdo e fornecer provas de sua integridade. Isto é, estes certificados fornecem a garantia de que o código ou conteúdo realmente veio do desenvolvedor ou fonte apropriado, e que seu conteúdo não foi violado, por exemplo, uma tentativa de inserir vírus e/ou códigos maliciosos. Qualquer AC que emita tais certificados não endossa o uso do código ou conteúdo dos Assinantes destes Certificados. Nenhuma AC deve se envolver com a parte funcional do código ou conteúdo assinado, produtos ou serviços oferecidos ou funções de suporte ao cliente destes Assinantes.

Finalizando, os Certificados ASB corporativos de classe 3 permitem que um representante autorizado da empresa atuem em seu nome. Eles são adequados para a troca de mensagens inter/ intra-organizacional, comercial e pessoal usando assinaturas digitais e criptografia de confidencialidade, bem como autenticação cliente, onde o remetente ou usuário é considerado uma organização em vez de um indivíduo, com um alto nível de segurança com relação às classes 1 e 2.

1.3.4.2. Aplicações Restritas

Em geral, os Certificados VTN servem para finalidades gerais. Eles podem ser utilizados globalmente e na interação com Parte Confiante no mundo todo. O uso de certificados VTN não se restringem a um ambiente comercial específico, como sistema piloto de serviços financeiros, ambiente de mercado vertical ou mercado virtual. Entretanto, tal uso é permitido, sendo que os Clientes que utilizam Certificados dentro de seus próprios ambientes podem determinar restrições adicionais no uso de certificados em tais ambientes. A VeriSign e demais participantes da VTN não se responsabilizam pela monitoração ou aplicação destas restrições nestes ambientes.

Entretanto, alguns certificados VTN são limitados quanto à função. Por exemplo, os certificados de AC podem ser usados apenas em funções de AC.. Adicionalmente, os certificados clientes são voltados para aplicações clientes e não devem ser utilizados como certificados de servidor ou corporativos Certificados corporativos de classe 3 emitidos para dispositivos limitam-se às funções de servidores da web e proteção de sessões SSL/TLS (no caso de IDs de servidor seguro e global), sessões OFX (no caso de certificados OFX) e assinatura de objetos (no caso de Certificados de assinatura de objetos). Certificados de Administradores deverão ser utilizados apenas para executar funções de Administrador.

Com relação aos Certificados VTN X.509 Versão 3, a extensão de uso de chave dedica-se a limitar as finalidades técnicas para as quais a chave privada correspondente à chave pública em um Certificado possa ser utilizada dentro da VTN. Consulte o parágrafo 6.1.9. Adicionalmente, os Certificados de Assinantes não devem ser usados como Certificados de ACs. Esta restrição confirma-se pela ausência de uma extensão Basic Constraints. Consulte o parágrafo 7.1.2.4. A eficácia das limitações baseadas em extensão está sujeita à operação do software fabricado ou controlado por outras entidades que não a VeriSign.

De forma geral, os certificados deverão ser usados conforme o escopo de uso consistente com a legislação aplicável, particularmente, deverá ser usado somente para as finalidades permitidas pelas leis de importação e exportação.

1.3.4.3. Aplicações Proibidas

Os certificados VTN não foram criados, destinados ou autorizados para uso ou revenda como equipamento de controle sob circunstâncias de risco ou para uso que exijam desempenho à prova de falhas tais como a operação de instalações nucleares, navegação de aeronaves ou sistemas de comunicação, sistemas de controle de tráfego aéreo ou sistemas de controle de equipamento bélico,

onde a falha pode resultar diretamente em morte, lesões pessoais e sérios danos ambientais. Conforme rege o parágrafo 1.3.4 desta PC, os Certificados de Classe 1 não devem ser utilizados como prova de identidade ou como apoio à não-repúdio de identidade ou autoridade.

1.4. Dados de Contato

1.4.1. Organização de Administração de Especificações

A organização que administra esta PC é a Autoridade de Administração de Políticas da VeriSign (“PMA”); O endereço da PMA é:

VeriSign Trust Network Policy Management Authority c/o VeriSign, Inc. 487 E. Middlefield Road Mountain View, CA 94043 USA +1 (650) 961-7500 (voice) +1 (650) 426-7300 (fax) practices@verisign.com

1.4.2. Pessoa de Contato

Encaminhe dúvidas quanto à PC para cp@verisign.com ou no seguinte endereço:

VeriSign, Inc. 487 E. Middlefield Road Mountain View, CA 94043 USA A/C: Practices and External Affairs Ð CP +1 (650) 961-7500 (voice) +1 (650) 426-7300 (fax) practices@verisign.com

1.4.3. Pessoa que Determina a Adequabilidade do CPS para a Política

As pessoas que definem se o CPS de uma Afiliada é adequado para esta PC são os membros da PMA Veja o parágrafo § 1.4.2 desta PC.

2. DISPOSIÇÕES GERAIS

2.1. Obrigações (Classes 1-3)

2.1.1. Obrigações da AC

As ACs devem cumprir com obrigações específicas detalhadas nesta PC. As disposições das obrigações específicas da PC de cada categoria de AC : Centros de Processamento, Centros de Atendimento ao Cliente, Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB.

Além disso, a VeriSign e Afiliadas farão uso de todos os meios comerciais disponíveis para assegurar que os Contratos de Assinante e Contratos de Parte Confiante vinculem Assinantes e Parte Confiante a seus respectivos subdomínios. Alguns exemplos de tais medidas incluem, porém não se limitam a, solicitar concordância de um Contrato de Assinante com uma condição para registro ou solicitar concordância em um Contrato com Parte Confiante como condição para receber informações de status do Certificado. Os Contratos de Assinante e de Parte Confiante da VeriSign e Afiliadas devem atender aos requisitos do Guia de Requisitos Legais para Prática de Afiliadas (“Afilliate Practices Legal Requirements Guidebook”). De forma similar os Centros de Serviço Universal e Revendedoras (onde necessário por contato) deverão utilizar os Contratos de Assinante e Parte Confiante conforme as exigências impostas pela VeriSign ou Afiliada aplicável. Os contratos de Assinante e Parte Confiante utilizados pela VeriSign, Afiliadas, Centros de Serviço Universal e Revendedores devem incluir as disposições apresentadas nos parágrafos 2.2-2.4 desta PC.

Clientes de PKI Gerenciada e Clientes Gateway têm permissão para usar os Contratos de Assinante que lhes são específicos, embora não seja necessário. Os Clientes de PKI Gerenciada e Clientes Gateway utilizando Contratos de Assinante deverão incluir as disposições previstas nos parágrafos 2.2-2.4 desta PC. Se um cliente de Cliente de PKI Gerenciada, cliente Gateway ou revendedor não utilizar seu próprio Contrato de Assinante, aplicar-se-á o contrato de Assinante da VeriSign ou Afiliada aplicável. Se um revendedor não possui um Contrato de Parte Confiante, aplicar-se o contrato de Parte Confiante da VeriSign ou Afiliada aplicável.

2.1.1. Obrigações da AR

As ARs auxiliam um a AC- Centro de Serviço ou Processamento, realizando as funções de validação, aprovação ou reprovação de Solicitações de Certificado, solicitação de revogação de Certificados e aprovação das

solicitações de renovação. As disposições quanto às obrigações específicas da PC de cada categoria de ARs: Centros de Serviço de Servidor, Clientes de PKI Gerenciada Lite, PKI Gerenciada para Clientes SSL E SLL Premium Edition, e Provedores ASBs.

Além disso, os Centros de Serviço de Servidor e Provedores ASB deverão assegurar que os Contratos de Assinante e Parte Confiante vinculam Assinantes e Parte Confiante a seus respectivos subdomínios, conforme rege o parágrafo 2.1.1 desta PC. Este requisito não se aplica a outras ARs.

2.1.3. Obrigações do Titular (Assinante)

Os candidatos ao Certificado deverão fornecer informações completas e precisa sobre as solicitações de Certificado e deverão manifestar sua aquiescência quanto ao contrato de Assinante aplicável como condição para obtenção do Certificado.

Os Assinantes deverão realizar as funções de Assinantes conforme determina as obrigações específicas apresentadas nesta PC. Os Assinantes deverão usar seus Certificados conforme rege o parágrafo § 1.3.4 da PC. Os assinantes deverão proteger as chaves privadas conforme regem os parágrafos 6.1-6.2, 6.4 desta PC. Se um Assinante descobrir, ou tiver motivos para acreditar que houve um comprometimento da chave privada do Assinante ou dos dados de ativação que protegem tal chave privada, ou que as informações no Certificado estão incorretas ou foram alteradas, deverá o Assinante:

. • Notificar prontamente a entidade que forneceu a solicitação de Certificado, seja uma AC ou AR, conforme o parágrafo 4.4.1.1 da PC e solicitar a revogação do Certificado conforme os parágrafos 3.4, 4.4.3.1 desta PC, e

. • notificar qualquer pessoa que possa vir a ser esperada pelo Assinante para contar com ou na prestação de serviços de suporte do Certificado do Assinante ou uma assinatura digital verificável com relação ao Certificado de Assinante.

Os Assinantes deverão cessar o uso de suas chaves privadas findo o período de utilização disposto no parágrafo 6.3.2 desta PC.

Assinantes não deverão monitorar, interferir ou aplicar a técnica de engenharia reversa na implementação técnica da VTN, exceto mediante aprovação prévia por escrito da VeriSign, e tampouco deverão intencionalmente comprometer a segurança da VTN.

2.1.4. Obrigações de Parte Confiante (Relying Party)

Antes de qualquer ato de confiança, os Parte Confiante deverão avaliar de forma independente a adequabilidade de uso de um Certificado para qualquer finalidade e determina se o Certificado irá, de fato, ser utilizado para uma finalidade apropriada. A VeriSign, ACs e ARs não se responsabilizam pela avaliação de adequabilidade de uso de um Certificado. Parte Confiante não deverão utilizar os Certificados além dos limites definidos no parágrafo 1.3.4.2 e finalidades proibidas determinadas no parágrafo 1.3.4.3 desta PC.

Assumindo que o uso do Certificado é apropriado, os Parte Confiante deverão utilizar o software e/ou hardware apropriados para realizar a verificação de assinatura digital ou outras operações criptográficas que possam desejar realizar em cada operação. Tais operações incluem a identificação da Cadeia de Certificados e verificação de assinaturas digitais em todos os certificados na cadeia de certificados. Os Parte Confiante não deverão contar com um Certificado a menos que os procedimentos de verificação sejam executados com êxito.

Os Parte Confiante deverão também verificar o estado de um Certificado no qual desejam confiar, bem como todos os Certificados na cadeia de Certificados, conforme os parágrafos §§ 4.4.10, 4.4.12 da PC. Se um dos Certificados na Cadeia de Certificados tiver sido revogado, a Terceira Parte não deverá confiar no Certificado de assinante ou outro certificado revogado na cadeira de certificados.

Finalmente, os Parte Confiante deverão avaliar os termos do Contrato de Assinante e Contrato de Parte Confiante como condição de uso ou confiança nos Certificados Parte Confiante que também são Assinantes concordam com os termos aplicáveis a Parte Confiante, termos de exonerabilidade de garantia e limitações de responsabilidades ao concordar com um Contrato de Assinante.

Se todas as verificações supracitadas forem bem sucedidas a Terceira Parte poderá contar com o Certificado, com a condição de que a confiança no Certificado seja razoável mediante as circunstâncias. Caso as circunstâncias

indiquem a necessidade de garantias adicionais, a Terceira Parte deverá obter tais garantias para que a confiança seja considerada razoável.]

As Terceiras Partes não deverão monitorar, interferir ou aplicar a técnica de engenharia reversa na implementação técnica da VTN, exceto mediante aprovação prévia por escrito da VeriSign, e tampouco deverão comprometer intencionalmente a segurança da VTN.

2.1.5. Obrigações do Repositório

Na VTN, não há uma entidade distinta que fornece serviços de repositório. Em vez, a VeriSign e Afiliadas são responsáveis pelas funções do repositório, da seguinte maneira: Centros de Processamento possuem um repositório para suas próprias ACs, e as ACs de Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB. Os Centros de Serviço possuem um repositório para suas próprias ACs, e as ACs de Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB, mas como parte de seu contrato com um Centro de Processamento, o Centro de Processamento hospeda aquele repositório para o Centro de Serviços.

Clientes Gateway e Centros de Processamento que emitem Certificados a Assinantes deverão publicar os Certificados emitidos no repositório determinado na Tabela 4, conforme estabelece o parágrafo 2.6 desta PC.

AC	Entidade que emite o Certificado em nome da AC	Repositório Aplicável
Centro de Processamento	O Centro de Processamento	O próprio repositório do Centro de Processamento
Centro de Serviços Cliente	Centro de Processamento	O repositório do Centro de Serviços, acessível pelo seu site, hospedado por um Centro de Processamento
Cliente de Cliente de PKI Gerenciada ou Cliente ASB de um Centro de Processamento	Centro de Processamento	O repositório do Centro de Processamento
Cliente de Cliente de PKI Gerenciada ou Cliente ASB de um Centro de Serviços	Centro de Processamento	O repositório do Centro de Serviços, acessível pelo seu site, hospedado por um Centro de Processamento
Cliente Gateway de um Centro de Processamento	O Cliente Gateway	O repositório do Centro de Processamento
Cliente Gateway de um Centro de Serviços	O Cliente Gateway	O repositório do Centro de Serviços, acessível a partir de seu site, hospedado pelo Centro de Processamento do Centro de Serviços

Tabela 4 - Repositórios Aplicáveis por Tipo de AC

Mediante a revogação do Certificado do Assinante, o Centro de Processamento ou Cliente Gateway que emitiu o Certificado deverá notificar tal revogação no repositório indicado na Tabela 4. Além disso, os Centros de Processamento devem emitir LCRs e prestar serviços de OCSP (Online Certificate Status Protocol - protocolo de status de certificado on-line) (contanto que forneçam serviços OCSP) para suas próprias ACs e ACs de Centros de Serviço, Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB dentro de seus Subdomínios, conforme os parágrafos 4.4.9, 4.4.11 desta PC.

2.2. Responsabilidade (Classe 1-3)

2.2.1. Responsabilidade da Autoridade Certificadora

As garantias, termos de exoneração de garantia e limites de responsabilidade entre a VeriSign, Afiliadas, Centros de Serviço Universal, Revendedores, e seus respectivos Clientes são determinadas e regidas pelos

contratos existente entre as partes. O parágrafo 2.2.1 da PC relaciona apenas as garantias que certas ACs (Centros de Processamento, Centros de Atendimento ao Cliente, Clientes de PKI Gerenciada, Clientes Gateway) devem fazer ao Assinante que recebe seus Certificados e a Parte Confiante, a exoneração de garantia que deverão fazer para tais Assinantes e Parte Confiante e as limitações de confiabilidade aplicadas a tais Assinantes e Parte Confiante. Desde a terceirização das funções primárias e secundárias ao Provedor ASB, as exigências de garantia desta seção não se aplicam a Clientes ASB.

A VeriSign, Afiliadas, Centros de Serviço Universal e Revendedores (onde necessário) deverão utilizar os Contratos de Assinante e Contratos de Parte Confiante conforme o parágrafo 2.1.1 da PC. Clientes de PKI Gerenciada e Clientes Gateway têm a opção de usar um Contrato de Assinante. Estes contratos de Assinante e Parte Confiante devem atender às exigências do Guia de Práticas de Requisitos Legais da Afiliada (no caso da VeriSign e Afiliadas) e os requisitos impostos pela VeriSign ou Afiliada (no caso de Centros de Serviço Universal e Revendedores). Os requisitos dos Contratos de Assinantes contêm garantias, termos de exoneração e limitações de responsabilidade abaixo aplicam-se à VeriSign, Afiliadas, Centros de Serviço Universal e àqueles Clientes de PKI Gerenciada, Clientes Gateway e Revendedores que utilizam Contratos de Assinante. Os requisitos com relação a garantias, termos de exoneração e limitações nos Contratos de Parte Confiante aplicar-se-ão à VeriSign, Afiliadas, Centros de Serviço Universal e àqueles Revendedores que utilizam Contratos de Parte Confiante. Observe que os termos aplicáveis a Parte Confiante também deverão constar nos Contratos de Assinante, além dos Contratos de Parte Confiante, uma vez que Assinantes muitas vezes atuam como Parte Confiante.

2.2.1.1. Garantias da Autoridade Certificador a Titulares e Parte Confiante

Os Contratos de Assinante deverão incluir uma garantia aos Assinantes que:

. • Não há adulteração material encontrada no Certificado conhecido como originário das entidades que aprovam a Solicitação do Certificado ou responsáveis por sua emissão,

. • As informações contidas no Certificado não apresentam erros que foram introduzidos por entidades que aprovaram a Solicitação do Certificado ou responsáveis pela sua emissão, resultante de uma falha em exercer os devidos cuidados no gerenciamento da solicitação ou geração de certificado,

. • Seus Certificados atende a todos os requisitos materiais da CPS aplicável, e

. • Os serviços de revogação e uso de um repositório estão em conformidade com a CPS aplicável em todos os aspectos materiais.

Os Contratos de Parte Confiante deverão conter uma garantia a Parte Confiante que dependem de um Certificado que:

. • Todas as informações contidas ou incorporadas por referência em tal Certificado, exceto por Informações do Assinante Não-verificadas, estão corretas,

. • Em caso de Certificados que aparecem em um repositório, que o Certificado foi emitido para um indivíduo ou organização indicados no Certificado como o Assinante, e que o Assinante aceitou o Certificado, conforme o parágrafo 4.3, e

. • As entidades aprovação a Solicitação de Certificado e emitindo o Certificado cumpriram substancialmente com a CPS aplicável na emissão do Certificado.

Além dessas garantias, o Plano de Proteção NetSure VeriSign fornece garantias aos Assinantes que adquiriram Certificados sujeitos ao Plano de Proteção NetSure dentro do subdomínio da VeriSign ou em subdomínios das Afiliadas participantes. Estas garantias adicionais cobre as atividades do Assinante quando na posição de Parte Confiante. Para mais informações sobre o Plano de Proteção NetSure, veja o parágrafo 1.1.2.2.3 da PC.

2.2.1.2. Termos de Exoneração de Garantias Garantias das Autoridades Certificadoras

Na medida da legislação aplicável, os Contratos de Assinante e Parte Confiante deverão renunciar às possíveis garantias da VeriSign e Afiliadas aplicáveis, incluindo qualquer garantia de comerciabilidade ou adequação para determinado propósito, fora do contexto do Plano de Proteção NetSure.

2.2.1.3. Limites de Responsabilidade da Autoridade Certificadora

Na medida da legislação aplicável, os Contratos de Assinante e Parte Confiante deverão limitar a responsabilidade da VeriSign e Afiliadas aplicáveis, quando fora do contexto do Plano de Proteção NetSure. As limitações de responsabilidade deverão incluir uma exclusão de danos indiretos, especiais, acidentais e conseqüentes. Elas também deverão incluir os seguintes limites de responsabilidades, reduzindo os danos da VeriSign e Afiliada com relação a um Certificado específico:

Classe	Limites de responsabilidade
Classe 1	Cem dólares. dólares (US$ 100,00)
Classe 2	Cinco mil dólares (US$ 5.000,00)
Classe 3	Cem mil dólares (US$ 100.000,00)

Tabela 5 - Limites de Responsabilidade

Nota: Os limites de responsabilidade na Tabela 5 limitam os danos recuperáveis fora do contexto do Plano de Proteção NetSure. As quantias pagas no Plano de Proteção NetSure estão sujeitas a seus próprios limites de responsabilidade. Os limites de responsabilidade no Plano de Proteção NetSure dos diferentes tipos de Certificados variam de US$ 1.000,00 a US$ 1.000.000,00. Consulte o Plano de Proteção NetSure para mais detalhes em http://www.verisign.com/repository/netsure/.

2.2.1.4. Força Maior

Na medida da legislação aplicável, os Contratos de Assinante e Parte Confiante deverão incluir uma cláusula de força maior, protegendo a VeriSign e Afiliada aplicável.

2.2.2. Responsabilidade da Autoridade de Registro

Garantias, termos de exoneração de garantia e limites de responsabilidade entre uma AR e a AC a quem ajuda na emissão de Certificados, ou o Centro de Serviços Universal ou Revendedor aplicável, são definidos e regidos pelos contratos existente entre as partes. A VeriSign, Afiliadas e Provedores ASB deverão utilizar os Contratos de Assinante e Contratos de Parte Confiante conforme os parágrafos 2.1.1-2.1.2 da PC, que possuem suas próprias garantias, termos de exoneração e limites. O parágrafo 2.2.2 desta PC relata apenas as garantias, termos de exoneração de garantia e limitações de responsabilidade que as ARs de Centros de Serviço do Servidor e Provedor ASB aplicar-se-ão aos Assinantes cujas Solicitações de Certificados aprovadas e Parte Confiante que confiam em Certificados resultantes da aplicação de certificado por elas aprovadas.

Clientes de PKI Gerenciada Lite, PKI Gerenciada para Clientes SSL e Clientes SSL Premium Edition não utilizam Contratos de Assinante ou Parte Confiante. Portanto, as exigências desta seção não se aplicam a eles. Em vez disso, aplica-se o Contrato de Assinante da Entidade Superior do Cliente de PKI Gerenciada Lite, PKI Gerenciada para Cliente SSL e PKI Gerenciada para Cliente SSL Premium Edition (i.e., Clientes de PKI Gerenciada da VeriSign).

Os Centros de Serviço de Servidor e Provedores ASB, em nome de suas ACs de Cliente ASB, deverão incluir nos Contratos de Assinantes e Parte Confiante as garantias, termos de exoneração de garantia, limitações de responsabilidade e cláusulas de força maior determinadas nos parágrafos 2.2.1.1 a 2.2.1.4 desta PC.

2.2.3. Responsabilidade do Titular

2.2.3.1. Garantias do Titular

Os Contratos de Assinante deverão incluir uma garantia aos Assinantes que:

• Cada assinatura digital criada usando a chave privada correspondente à chave pública listada no Certificado é a assinatura digital do Assinante, e o Certificado foi aceito e está em funcionamento (não expirou, nem foi revogado) no momento de criação da assinatura digital.

• Nenhuma pessoa não autorizada teve acesso à chave privada do Assinante,

• Todas as representações feitas pelo Assinante na solicitação de certificado e por ele enviadas são verdadeiras,

• Todas as informações fornecidas pelo Assinantes e contidas no Certificado são verdadeiras,

• O Certificado está sendo usado exclusivamente para fins autorizados e legais, consistentes com a DPC aplicável, e

• O assinante é o Assinante (usuário final) e não um AC, e não está usando a chave privada correspondente à chave pública listada no Certificado para fins de assinatura digital de qualquer Certificados (ou qualquer outro formato de chave pública certificada) ou LCR, como uma AC ou similar.

Onde uma solicitação de certificado de Assinante foi aprovada pelo Cliente de PKI Gerenciada usando Administrador de Chaves de PKI Gerenciada, o Assinante garante apenas que nenhuma pessoa não-autorizada obteve acesso à cópia da chave privada do Assinante, na plataforma de hardware/software do Assinante. Estes assinantes não concedem garantias no que se refere às cópias de suas chaves privadas em posse de Clientes de PKI Gerenciada, usando o Administrador de Chaves para PKI Gerenciada.

2.2.3.2. Comprometimento da Chave Privada

Esta DPC define os Padrões da VTN para a proteção das chaves privadas dos Assinantes Consulte o parágrafo 6.2.7.1. Os contratos de Assinante deverão constar que o Assinante que atenda aos padrões da VTN é o único responsável por quaisquer perdas ou danos resultantes de tal falha.

2.2.4. Responsabilidade de Parte Confiante

Contratos de Assinantes e Parte Confiante deverão exigir que Parte Confiante reconheçam que têm informações suficientes para tomar uma decisão embasada sobre até que ponto devem confiar nas informações apresentadas em um Certificado, que eles são os únicos responsáveis pela decisão de confiar ou não em tais informações, e que deverão arcar com as conseqüências legais da falha para cumprir com as Obrigações a Parte Confiante definidas no parágrafo 2.1.4 desta PC

2.3. Responsabilidade Financeira (Classe 1-3)

2.3.1. Indenização devidas por Titulares e Parte Confiante

2.3.1.1. Indenização devidas por Titulares

Conforme determina a legislação aplicável, os contratos de Assinantes deverão exigir dele a indenização à VeriSign e qualquer ACs e ARs que não sejam da VeriSign a título de:

• Falsidade ou adulteração do fato por parte do Assinante em sua solicitação de Certificado,

• Falha por parte do Assinante em revelar um fato material na solicitação de certificado,se a adulteração ou omissão foi feita negligentemente ou com intenção de enganar qualquer uma das partes,

• A falha do Assinante em proteger sua chave privada, em usar um Sistema confiável ou na tomada de medidas preventivas necessárias contra o comprometimento, perda, revelação, modificação e uso não-autorizado da chave privada do Assinante, ou

• O uso de um nome (incluindo, porém não se limitam a um nome comum, nome de domínio ou endereço de e-mail) por parte do Assinante que infrinja sobre os direitos de propriedade intelectual de Parte Confiante.

2.3.2. Indenização devidas por Parte Confiante

Conforme determina a legislação aplicável, os contratos de Assinante e Parte Confiante deverão exigir que Parte Confiante indenizem a VeriSign e qualquer AC ou AR não sejam da VeriSign a título de:

• A falha por parte da Terceira parte em executar as suas obrigações previstas por contrato,

• A confiança de Parte Confiante em um Certificado que não está razoável dentro das circunstâncias, ou

• A falha por parte de Parte Confiante em verificar o estado de dado Certificado para determinar sua expiração ou revogação.

2.3.3. Relações Fiduciárias

No que se refere à legislação aplicável, os Contratos de Assinante e Parte Confiante deverão abrir mão de qualquer relação fiduciária entre a VeriSign e uma AC ou AR não que seja d VeriSign por um lado, e um Assinante ou Parte Confiante por outro.

2.3.4. Processos Administrativos

A VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão dispor de recursos financeiros suficientes para manter suas operações e executar suas tarefas, e deverão ser razoavelmente capazes de assumir o risco da responsabilidade de Assinantes e Parte Confiante. A VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway também devem manter um nível comercialmente razoável de cobertura de seguro por erros e omissões, seja através de um programa de seguro contra erros e omissões com uma corretora de seguros ou retenção assegurada. Este requisito de seguro não se aplica a entidades governamentais..

2.4. Interpretação e Execução (Classe 1-3)

2.4.1. Legislação

Sujeitas a quaisquer limites das leis aplicáveis, as leis do Estado da Califórnia, EUA, governarão a aplicabilidade, construção, interpretação e validade desta PC, independente do contrato ou outra opção de disposição legal e sem a necessidade de estabelecer um nexo comercial na Califórnia, EUA. Essa opção de legislação é feita para assegurar procedimentos e interpretações uniformes de todos os participantes da VTN, independente de sua localização.

Essa disposição de legislação em vigor aplica-se somente a esta PC. Os contratos que venham a incorporar esta PC por referência podem ter suas próprias disposições legais, uma vez que este parágrafo 2.4.1 da PC rege a aplicabilidade, construção, interpretação e validade dos termos individuais da PC e separado das demais disposições de tais contratos, sujeitos a quaisquer limitações aplicáveis pela lei.

Esta PC está sujeita às leis, regras, regulamentações, mandatos, decretos e ordens de âmbito nacional, estadual, local e internacional, incluindo sem limitar-se às restrições em importação e exportação de software, hardware ou informações técnicas.

2.4.2. Individualidade, Permanência em Vigor, Incorporação, Notificação

Na medida da legislação aplicável, os Contratos de Assinante e Parte Confiante deverão incluir cláusulas de individualidade, permanência em vigor, incorporação e notificação. Uma cláusula de individualidade em um contrato evita que qualquer determinação de invalidade ou inexigibilidade de uma cláusula no contrato prejudique o restante do contrato. Uma cláusula de sobrevivência especifica as disposições de um contrato que continuam em vigor, após sua cessão ou expiração. Uma cláusula de incorporação determina que todos os entendimentos referentes ao objeto do contrato estão nele incorporados. Uma cláusula de notificação determina que as partes devem notificar uma às outras.

2.4.3. Procedimentos na Solução de Disputas

2.4.3.1. Disputas entre a VeriSign, Afiliadas e Clientes

As disputas entre uma ou mais de qualquer entidade, incluindo a VeriSign, Afiliadas ou Clientes, deverão ser resolvidas conforme disposto nos contratos aplicáveis entre as partes.

2.4.3.2. Disputas com o Titular (Usuário Final) ou Parte Confiante

Na medida da legislação aplicável, os Contratos de Assinantes e Parte Confiante deverão incluir cláusulas de resolução de disputas. Os procedimentos dispostos no Guia de Práticas de Requisitos Legais da Afiliada para a resolução de disputas envolvendo a VeriSign requerem um período inicial de negociação de 60 (sessenta) dias, seguido por litigação em tribunal federal ou estadual do Condado de Santa Clara, Califórnia, no caso de autores residentes nos EUA. ou, no caso de outros autores, a arbitração administrada pela Câmara Internacional de Comércio (“ICC”) conforme as Regras ICC de Conciliação e Arbitragem.

2.5. Tarifas (Classe 1-3)

2.5.1. Tarifas de Emissão e Renovação de Certificado

A VeriSign, Afiliadas e Clientes estão intitulados a cobrar Assinantes pela emissão, administração e renovação de Certificados.

2.5.2. Tarifas de Acesso ao Certificado

A VeriSign, Afiliadas e Clientes não deverão cobrar taxas como condição para tornar um Certificado disponível em um repositório ou torná-lo disponível à Parte Confiante.

2.5.3. Tarifas de Revogação ou de Acesso à Informação de Status

VeriSign e Afiliadas não deverão cobrar taxas como condição para execução de LCRs exigidas conforme o parágrafo 4.4.9 da PC, disponível em um repositório ou Parte Confiante. Entretanto, poderão cobrar taxas para fornecer LCRs personalizadas, serviços de OCSP e outros serviços de revogação avançados e serviços de informação de estado. A VeriSign e Afiliadas não deverão permitir o acesso à informações de revogação, informações de estado de Certificado ou selo cronológico em seus repositórios a Parte Confiante que ofereçam produtos ou serviços que utilizam informações de estado de certificado sem a prévia autorização por escrito da VeriSign.

2.5.4. Tarifas para Outros Serviços, como Informação de Política

A VeriSign e Afiliadas não deverão cobrar tarifas pelo acesso a sua PC ou respectivas DPCs. Qualquer uso feito para fins que não de simples visualização do documento, tais como reprodução, redistribuição, modificação ou criação de obras derivadas estarão sujeitos a um contrato de licença com a entidade detentora dos direitos autorais do documento.

2.5.5. Política de Reembolso

Dentro dos limites da legislação aplicável, a VeriSign, Afiliadas, Centros de Serviço Universal e Revendedores utilizando Contratos de Assinante deverão implementar uma política de reembolso em conformidade com o Guia de Práticas de Requisitos Legais da Afiliada (no caso da VeriSign e Afiliadas) ou os requisitos da VeriSign ou Afiliada (em caso de Centros de Serviço Universal e Revendedores). Eles deverão definir suas políticas de reembolso em seus respectivos web sites (incluindo uma lista de seus repositórios), nos Contratos de Assinante e, no caso de da VeriSign e Afiliadas, em suas DPCs.

2.6. Publicação e Repositório (Classe 1-3)

2.6.1. Publicação das Informações das ACs

2.6.1.1. Publicação pela VeriSign e Afiliadas

A VeriSign e Afiliadas deverão se responsabilizar pelas funções de repositório. Os Centros de Processamento, como parte de seus contratos com os Centros de Serviço, deverão publicar os Certificados no repositório do Centro de Serviços baseados nas Solicitações de Certificado aprovadas pelos Centros de Serviço e seus Clientes de PKI Gerenciada, bem como informações de revogação referente estes Certificados. Clientes de PKI Gerenciada Lite PKI Gerenciada para Clientes SSL e PKI Gerenciada para Clientes SSL Premium Edition não precisam publicar tais Certificados ou informações de revogação em um repositório, uma vez que a VeriSign ou uma Afiliada se responsabilizaria pela execução de suas funções de repositório.

As DPCs da VeriSign e Afiliadas, Contratos de Assinantes e Parte Confiante e uma ligação a esta PC deverão constar em seus respectivos repositórios hospedados em seus web sites. A VeriSign e cada Afiliada deverão publicar a URL do Contrato de Parte Confiante aplicável dentro de cada Certificado que ela emitir, conforme rege os parágrafos 3.1.1, 7.1.6, 7.1.8 da PC.

Os Centros de Processamento deverão publicar os Certificados emitidos em nome de suas próprias ACs, e as ACs dos Centros de Serviços de Cliente, Clientes de PKI Gerenciada e Clientes ASB em seu

subdomínio. Mediante a revogação do Certificado do Assinante, o Centro de Processamento que emitiu o Certificado deverá publicar a notificação de tal revogação no repositório indicado no parágrafo 2.1.5 da PC. Além disso, os Centros de Processamento devem emitir LCRs e, se disponível, prestar serviços de OCSP para suas próprias ACs e ACs de Centros de Serviço, Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB dentro de seus respectivos Subdomínios, nos termos dos parágrafos 4.4.9 e 4.4.1.1 desta PC. Quando Clientes Gateway notificam a VeriSign ou Afiliada sobre uma revogação conforme o parágrafo 2.6.1.2, o Centro de Processamento aplicável deverá incluir a notificação de revogação no repositório adequado.

2.6.1.2. Publicação por Clientes Gateway

Os Clientes Gateway deverão publicar os Certificados por ele emitidos, conforme o parágrafo 2.1.5 da PC, e para fornecer informação de estado do Certificado. Mediante revogação de um Certificado de Assinante, os Clientes Gateway deverão notificar sua Entidade Superior (seja ela a VeriSign ou uma Afiliada) sobre a revogação para inclusão no repositório da Entidade Superior.

2.6.2. Freqüência da Publicação

As informações da AC deverão ser publicadas assim que disponibilizadas à AC. Os DPCs deverão conter disposições referentes a aditamentos realizados, e as alterações nas DPCs deverão ser publicadas conforme disposto. Os parágrafos 4.4.9, 4.4.11 da PC regerão a freqüência da publicação de informações de estado de Certificado..

2.6.3. Controles de Acesso

A VeriSign e Afiliadas não deverão usar de forma intencional, quaisquer meios técnicos de limite de acesso a esta PC, DPC, Certificados, informações de estado de certificados ou LCRs. A VeriSign e Afiliadas deverão, entretanto, solicitar que as pessoas concordem com um Contrato de Parte Confiante ou Contrato de Utilização de LCR como condição para o acesso a Certificados, informações de estado de certificados ou LCRs. A VeriSign e Afiliadas deverão implementar controles para impedir que pessoas não-autorizadas adicionem, excluam ou modifiquem as entradas do repositório.

2.6.4. Repositórios

Consulte o parágrafo 2.1.5

2.7. Auditoria de Conformidade

A VeriSign, Afiliadas e Cliente deverão se submeter a auditorias de conformidade periódicas (doravante, "Auditorias de Conformidade") para assegura a conformidade com os Padrões VTN após o início de suas operações. Os requisitos para a auditoria de conformidade são apresentados nas subseções do parágrafo 2.7 desta PC.

Além das auditorias de conformidade, a VeriSign e Afiliadas deverão ser capazes de realizar outras revisões e investigações que se façam necessárias para assegurar a confiabilidade da rede VTN, que incluem, porém não se limitam a:

• Uma "Revisão de Segurança e Práticas" de uma Afiliada antes que esta obtenha permissão para iniciar suas operações. Uma Revisão de Segurança e Práticas consistem na revisão as instalações seguras, documentação de segurança, CPS, contratos relativos à VTN, política de privacidade e planos de validação para assegurar que a Afiliada atende aos Padrões da VTN.

• A VeriSign deverá ter o direito, à seu critério exclusivo, realizar a qualquer momento uma "Auditoria/Investigação Severa" em si mesma, em uma Afiliada, Cliente no caso da VeriSign ou Entidade Superior àquela a ser submetida à auditoria tenha motivos para crer que a entidade sendo auditada falhou no cumprimento dos Padrões VTN, passou por um incidente ou Comprometimento, ou agiu ou falhou em tomar as medidas necessárias que resultaram na falha da entidade sob auditoria, o incidente ou Comprometimento, ou ato ou falha em agir configura um risco real ou potencial à segurança ou integridade da VTN. .

• A VeriSign terá o direito de realizar "Revisões Adicionais de Gerenciamento de Risco" em si mesma, em uma Afiliada ou Cliente, seguindo descobertas incompletas ou excepcionais em uma Auditoria de Conformidade ou como parte do processo geral de gerenciamento de risco no curso normal dos negócios.

A VeriSign terá o direito de delegar a realização de tais auditorias, revisões e investigações à Entidade Superior da entidade sob auditoria, revisão ou investigação ou por uma terceira firma de auditoria externa. As entidades que estão sujeitas a auditorias, revisões ou investigações deverão cooperar com a VeriSign e com a equipe realizando a auditoria, revisão ou investigação.

2.7.1. Freqüência da Auditoria de Conformidade (Classe 1-3)

As Auditorias de Conformidade deverão ser realizadas anualmente, com as despesas cobertas pela entidade sujeita à auditoria.

2.7.2. Identificação e Qualificações do Auditor

Uma firma de auditoria externa deverá realizar as Auditorias de Conformidade da VeriSign, Afiliadas, e Clientes de PKI Gerenciada aprovando 100 (cem) ou mais Solicitações de Certificado dentro de um período de 12 (doze) meses. As Auditorias de Conformidade de Clientes Gateway (Classe 1) ou outros Clientes de PKI Gerenciada que aprovam Solicitações de Certificado de Classe 1 ou 2 ou inferior a 100 (cem) Solicitações de Certificado de Classe 3 poderão realizar sua própria auditoria, sujeitas às limitações dispostas no parágrafo 2.7.2.1 da PC.

2.7.2.1. Equipe Realizando Auditorias Internas (Classe 1-3)

As Auditorias de Conformidade são auditorias internas de Clientes Gateway ou Clientes de PKI Gerenciadas que aprovam Solicitações de Certificado de Classe 1 ou 2, ou aprovam menos que 100 (cem) Solicitações de Certificado de Classe 3 deverão ser realizadas por uma pessoa dentro da entidade sendo auditada que seja organizacionalmente independente do Administrador Gateway, Administrador de PKI Gerenciada, Administrador de Gerenciador de Chave ou outros Administradores realizando funções de ACs e ARs. A VeriSign recomenda que a auditoria seja concluída pelo departamento de auditoria interna da entidade, se houver.

Caso a empresa sendo auditada não possa contratar uma pessoa organizacionalmente independente de tal Administrador com as habilidades necessárias para concluir uma auditoria, a entidade auditada deverá empresar um auditor independente qualificado, com as qualificações dispostas no parágrafos 2.7.2.2 para a realização da Auditoria de Conformidade da entidade, em vez de realizar uma auditoria interna. Alternativamente, a entidade auditada pode, com o prévio consentimento escrito da VeriSign ou Entidade Superior, utilizar uma pessoa para realizar a auditoria, que seja independente das funções de auditoria, caso a entidade auditada tenha emitido ou aprovado solicitações de certificado inferiores a 100 (cem) Certificados de qualquer Classe, dentro dos últimos 12 (doze) meses) e a Entidade Superior ou VeriSign não tiveram motivos para crer que houver qualquer irregularidade ou incidentes de segurança nos últimos 12 (doze) meses que poderiam representar um risco real ou potencial à segurança da VTN.

2.7.2.2. Qualificações de Empresas de Auditoria Externa (Classe 1-3)

Revisões e auditorias realizadas por uma auditora externa deverão ser realizadas por uma auditor contábil com experiência reconhecida em segurança computacional ou por profissionais de segurança computacional credenciados, empregados por uma consultoria de segurança competente. Tal firma também deverá mostrar provas de sua experiência na realização de auditorias de conformidade de segurança da tecnologia da informação e PKI.

2.7.3. Relação entre o Auditor e a Parte Auditada (Classe 1-3)

As Auditorias de Conformidade realizadas por auditoras externas deverão ser conduzidas por empresas independentes da entidade sendo auditada. Tais firmas não deverão ter conflitos de interesse que lhes impeçam de executar os serviços de auditoria. Com relação às auditorias internas, consulte o parágrafo 2.7.2.1.

2.7.4. Tópicos Cobertos pela Auditoria

Os tópicos de auditora para cada categoria de entidade são definidos abaixo. A entidade auditada pode realizar uma Auditoria de Conformidade um módulo que faz parte de uma auditoria geral anual dos sistemas de informação da entidade.

2.7.4.1. Auditorias Internas de Clientes Gateway (Classe 1)

Um guia de programa de auditora que descreve os procedimentos de auditoria de Clientes Gateway. Os Clientes Gateway deverão cumprir com sua auditoria de conformidade anual através de auditoria interna, que atestam o cumprimento dos objetivos de controle do guia de programa de auditoria e observação de quaisquer exceções ou irregularidades.

2.7.4.2. Auditorias Internas de Clientes de PKI (infra-estrutura de Chave Pública) Gerenciada (Classe 1-2)

Um guia de programa de auditoria descreve os procedimentos para auditoria de Clientes de PKI Gerenciada que aprova solicitações de certificado de Classe 1 e 2. Os Clientes de PKI Gerenciada deverão cumprir com sua auditoria de conformidade anual através de auditoria interna, atestando o cumprimento dos objetivos de controle do guia de programa de auditoria e observação de quaisquer exceções ou irregularidades.

2.7.4.3. Auditoria de um Cliente de PKI Gerenciada (Classe 3)

Um guia de programa de auditoria descreve os procedimentos para auditoria de Clientes de PKI Gerenciada que aprova solicitações de certificado de Classe 3 Se tais Clientes de PKI Gerenciada aprovaram 100 (cem) ou mais Solicitações de Certificado de Classe 3 em um período de 12 (doze) meses, tais Clientes de PKI Gerenciada deverão cumprir com sua obrigação de auditoria de conformidade anual, através de uma auditoria realizara por uma empresa de auditoria externa, atestando o cumprimento dos objetivos de controle no guia de programa de auditoria e a observância de exceções e irregularidades. Caso contrário, tais Clientes de PKI Gerenciada deverão atender à exigência de Auditoria de conformidade Anual através de auditoria interna, atestando o cumprimento dos objetivos de controle no guia de programa de auditoria e a observância de quaisquer exceções ou irregularidades.

2.7.4.4. Auditoria da VeriSign ou de uma Afiliada (Classe 1-3)

A VeriSign e cada Afiliada deverão ser auditadas conforme o Guia de Programa de Auditoria de Afiliadas, que incorpora diretrizes fornecidas no SAS (Statement on Auditing Standards) Nº 70, Reports on the Processing of Transactions by Service Organizations (Relatórios sobre o processamento de transações realizadas por organizações prestadoras de serviços) do American Institue of Certificate Public Accounts.. Suas Auditorias de Conformidade deverão ser SAS 70 Tipo II Revisão A: Relatório de Políticas e Procedimentos em Operação e Teste de Eficácia Operacional, ou padrão de auditoria equivalente, aprovado pela VeriSign.

2.7.5. Medidas Tomadas como Resultado de Deficiência (Classe 1-3)

Após receber um relatório baseado na Auditoria de Conformidade, determinada no parágrafo 2.7.6 da PC, a Entidade Superior deverá contatar a entidade auditada para discutir quaisquer exceções ou deficiências apresentadas pela auditoria. A VeriSign também terá o direito de discutir tais exceções ou deficiências com a parte auditada. A entidade auditada e sua Entidade Superior deverão, de boa fé, utilizar de recursos comercialmente razoáveis para acordar sobre um plano de ação corretiva para corrigir os problemas que causaram as exceções ou deficiência, e a implementação do plano. A falha por parte da entidade auditada em desenvolver o plano de ações corretivas, bem como sua implementação, ou o caso de identificação de exceções ou deficiências tidas pela VeriSign e Entidade Superior àquela sendo auditada para considerar uma ameaça imediata à segurança ou integridade da VTN, (a) A VeriSign e/ou Entidade Superior determinarão a necessidade de revogação e geração de relatório de Comprometimento, conforme os parágrafos 4.4.1.1, 4.4.15; (b) A VeriSign e a Entidade Superior reservar-se-ão o direito de suspender os serviços prestados à entidade auditada; e (c) se necessário, a VeriSign e a Entidade Superior podem determinar o encerramento da prestação de serviços sujeitos ao parágrafo 4.9 e aos termos do contrato da entidade auditada com a Entidade Superior.

2.7.6. Comunicação dos Resultados (Classe 1-3)

Seguinte à qualquer Auditoria de Conformidade, a entidade auditada deverá fornecer à VeriSign e sua Entidade Superior (se esta não for a própria VeriSign) com o relatório anual e certificações baseadas em sua auditoria ou auditoria interna dentro de 14 (catorze) dias após a conclusão da auditoria, e antes de 45 (quarenta e cinco) dias antes da data de aniversário do início das operações.

2.8. Sigilo (Classe 1-3)

A VeriSign e Afiliadas deverão implementar uma política de privacidade em conformidade com o Guia de Práticas de Requisitos Legais da Afiliada. Tais políticas de privacidade deverão estar em conformidade com as leis de privacidade locais aplicáveis. A VeriSign e Afiliadas não deverão revelar ou vender os nomes dos Solicitantes a Certificados ou informações que levem a sua identificação, sujeitos às disposições do parágrafo 2.8.2 da PC e com o direito à uma AC de encerramento para transferir tais informações a uma AC sucessora, conforme o parágrafo 4.9 da PC.

2.8.1. Tipos de informações sigilosas

Os seguintes registros de Assinantes deverão ser mantidos confidencial, conforme o parágrafo 2.8.2 da PC ("Confidential/Private Information"):

. • Registros de solicitação de AC, aprovados ou rejeitados,

. • Registros de Solicitação de Certificado (sujeitos ao parágrafo 2.8.2 da PC),

. • Chave privada mantidas por Clientes de PKI Gerenciada utilizando o Gerenciado de Chave para PKI Gerenciada e demais informações necessárias para recuperar tais Chaves Privadas.

. • Registros de transações (registros completos e pista de auditora das transações),

. • Registros VTN com pistas de auditoria criadas ou mantidas pela VeriSign, uma Afiliada ou um Cliente,

. • Relatórios de auditoria da VTN criados pela VeriSign, uma Afiliada ou um Cliente (na medida em que os relatórios sejam atualizado), ou seus respectivos auditores (internos ou públicos),

. • Planos de contingência e planos de recuperação de desastre, e

. • Medidas de segurança para controlar as operações do hardware e software da VeriSign ou Afiliada hardware e a administração dos serviços de Certificados e serviços de registros designados.

2.8.2. Tipo de informações não-sigilosas

Os Participantes da VTN reconhecem que Certificados, revogação de certificados, e outras informações de estado, repositórios de participantes da VTN, e informações contidas não são consideradas informações confidenciais/particulares. As informações que não são expressamente declaradas como Confidencial/Privada conforme a PC § 2.8.1 não serão consideradas nem confidenciais ou particulares. Esta seção está sujeita às leis de privacidade aplicáveis.

2.8.3. Divulgação de informação de revogação ou suspensão de certificado

Consulte PC § 2.8.2.

2.8.4. Quebra de sigilo por motivos legais

Os Participantes da VTN reconhecem que a VeriSign e a Afiliada reservar-se-ão o direito de divulgar informações confidenciais/particulares se, de boa-fé, a VeriSign ou Afiliada considerar que tal revelação se faça necessária em virtude de intimações e mandatos de busca e apreensão. Esta seção está sujeita às leis de privacidade aplicáveis.

2.8.5. Quebra de sigilo como parte de descoberta pública

Os Participantes da VTN reconhecem o direito da VeriSign Afiliada em revelar informações Confidenciais/Privadas se, em boa fé, a Afiliada ou a VeriSign acreditarem que tal quebra de sigilo se faça necessária, em virtude de processo judicial, administrativo durante o processo de descoberta em uma ação civil ou administrativa, tais como intimações, interrogatórios, solicitações para confissão e solicitações para produção de documentação. Esta seção está sujeita às leis de privacidade aplicáveis.

2.8.6. Divulgação por solicitação do Titular do Certificado

As políticas de privacidade estabelecidas conforme a PC § 2.8 deverão conter dispostos com relação à quebra de sigilo de informações confidenciais/privadas à pessoa revelando-as à VeriSign ou Afiliada. Esta seção está sujeita às leis de privacidade aplicáveis.

2.8.7. Outras circunstâncias de divulgação de informações

Sem estipulação

2.9. Direitos de Propriedade Intelectual (Classe 1-3)

A alocação dos Direitos de Propriedade Intelectual entre os Participantes da VTN que não Assinantes e Parte Confiante deverão ser regidos pelos contratos aplicáveis a estes Participantes VTN. As subseções seguintes ao parágrafo 2.9 desta PC aplicam-se aos Direitos de Propriedade Intelectual com relação a Assinantes e Parte Confiante.

2.9.1. Direitos de propriedade sob as informações de certificados e revogações

As ACs detêm todos os Direitos de Propriedade Intelectual dos Certificados e informações de revogação que venham a ser emitidas. VeriSign, Afiliadas e Cliente deverão conceder permissão para a reprodução e distribuição de Certificados de forma não-exclusiva, sem cobrança de royalties, contanto que sua reprodução seja integral e que o uso dos Certificados está sujeito ao Contrato de Parte Confiante citado no Certificado. A VeriSign, Afiliadas e Clientes deverão conceder permissão para uso das informações de revogação para a execução de funções de Parte Confiante sujeitos ao Contrato de Uso de LCR, Contrato de Parte Confiante e demais contratos aplicáveis.

2.2.9.2. Direitos de propriedade na PC

2.2.9.3. Direitos de propriedade sobre nomes

Os Participantes da VTN reconhecem os Direitos de Propriedade Intelecutal nesta PC.

Um Solicitante de Certificado detém todos os direitos que possui (se houver) sobre quaisquer marcas comerciais, marcas de serviço ou nome fantasia contido em qualquer Solicitação de Certificado e nome distinto dentro de um Certificado emitido ao referido Solicitante.

2.9.4. Direitos de propriedade sobre chaves e materiais de chaves

Os pares de chaves correspondentes aos Certificados das ACs e Assinantes são propriedade das ACs e Assinantes que são os respectivos Objetos destes Certificados, sujeitos aos direitos dos Clientes de PKI Gerenciada usando o Gerenciador de Chave de PKI Gerenciada, independente do meio físico onde estão armazenados e protegidos, e pessoas detentoras de todos os direitos de propriedade intelectual referentes a estes pares de chaves. Sem limitar-se à generalidade apresentada a seguir, as chaves publicas raiz da VeriSign e Certificados raiz que as contêm, incluindo todas as chaves públicas de APCs e Certificados com assinatura própria são de propriedade da VeriSign. A VeriSign licencia fabricantes de software e hardware reproduzirem tais Certificados de raiz, para guardar as cópias em dispositivos de hardware ou software seguros. Finalmente, sem limitar-se à generalidade do seguinte as partes secretas de uma chave privada de AC são de propriedade da AC, e esta por sua vez retém todos os Direitos de Propriedade Intelectual sobre tais partes secretas, mesmo que não detenham a posse física destas partes ou a AC da VeriSign.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Registro inicial

3.1.1. Tipos de nomes (Classe 1-3)

Os Certificados de Assinantes deverão conter um nome distinto X.501 no campo de nome Subject. O nome distinto de Objeto dos Certificados do Assinante incluem um componente de nome comum (CN=). O valor autenticado de componente de nome comum incluía os nomes distintos dos Objetos dos Certificados corporativos deverão ser um nome de domínio (no caso de IDs de Servidor Seguro e IDs de Servidor Global) ou a denominação da organização ou unidade de negócio. O valor autenticado de nome comum incluído no nome distinto de Objeto de um Certificado ASB Corporativo de Classe 3 deverá ser o nome pessoal comumente aceito do representante autorizado da empresa, para o uso da chave privada, sendo o componente

da organização (O=) a denominação da organização. O valor de nome comum incluído no nome distinto de Objeto de Certificados individuais representará o nome pessoal comumente aceito do indivíduo. Os nomes comuns deverão ser autenticados em caso de Certificados de Classe 2 ou 3. Os Certificados VTN deverão conter uma referência ao Contrato de Parte Confiante aplicável em seus nomes distintos, conforme esta PC, § 7.1.4.

3.1.2. Necessidade por nomes significativos (Classe 1-3)

Certificados de Assinantes de Classe 2 e 3 deverão incluir nomes significativos na seguinte maneira: Certificados de Assinantes Classe 2 e 3 deverão conter nomes com semânticas comumente inteligíveis, permitindo a determinação da identidade do indivíduo ou organização Objeto do Certificado. Para tais Certificados, os pseudônimos (nomes diferentes do nome verdadeiro do assinante ou denominação da empresa) não são permitidos.

3.1.3. Regras para interpretação de vários tipos de nomes (Classe 1-3)

Sem estipulação

3.1.4. Exclusividade de nomes (Classe 1-3)

Os nomes de Assinantes dentro da VTN deverão ser exclusivos dentro dos Subdomínios de uma Afiliada e Cliente para determinada classe de Certificado. É possível para um Assinante ter dois ou mais certificados com o mesmo nome distinto de Objeto.

3.1.5. Procedimento para resolver disputa de nomes (Classe 1-3)

Os Solicitantes ao Certificado não devem utilizar nomes em suas Solicitações de Certificado que infrinjam sobre os Direitos de Propriedade Intelectual de Parte Confiante. Não caberá à VeriSign nem a qualquer de suas Afiliadas a determinação de posse dos direitos de propriedade intelectual no nome que consta em uma Solicitação de Certificado ou para arbitrar, mediar, ou resolver quaisquer disputas referentes e propriedade de qualquer nome de domínio, denominação, marca registrada ou marca de serviço; a VeriSign e suas Afiliadas se reservam o direito, sem responsabilidades para com qualquer Solicitante de Certificado - rejeitar ou suspender qualquer solicitação de certificado geradora de tal disputa.

3.1.6. Reconhecimento, autenticação e papel das marcas registradas (Classe 1-3)

Consulte o parágrafo 3.1.5 da PC.

3.1.7. Método de comprovação de posse de chave privada (Classe 1-3)

O método para comprovação de posse de chave privada deverá ser o método PKCS #10, outra demonstração criptograficamente equivalente, ou outro método aprovado pela VeriSign. Esta exigência não se aplica aos pares de chaves gerados por uma AC, em nome de um Assinante, por exemplo, onde as chaves pré-geradas são armazenadas em cartões inteligentes.

3.1.8. Autenticação da identidade da organização

3.1.8.1. Autenticação da identidade de assinantes de uma organização (Classe 3)

A identidade dos assinantes corporativos e outras informações de registro fornecidas por Solicitantes a Certificados (exceto para Informações de Assinantes Não-verificadas), deverão ser confirmadas conforme os procedimentos definidos no documento da VeriSign, Procedimentos de Validação. Os procedimentos de avaliação das Afiliadas para a autenticação de identidade corporativa deverão ser submetidos à aprovação da VeriSign, e tal aprovação será uma condição para que uma Afiliada possa iniciar sua operações como uma AC ou AR, na aprovação de Solicitações de Certificados ou emissão de Certificados Corporativos de Classe 3.. Além dos procedimentos descritos abaixo, o Solicitante de Certificado deverá demonstrar que ele verdadeiramente possui a chave privada correspondente à chave pública a ser apresentada no Certificado, conforme determina esta PC, § 3.1.7.

3.1.8.1.1. Autenticação de Certificados Corporativos de Varejo

A confirmação da identidade de um Solicitante de Certificado para um Certificado Corporativo de Varejo deverá constar:

• A determinação de que a organização existe, usando pelo menos um serviço ou banco de dados de comprovação de identidade de Parte Confiante, ou documentação da empresa emitida ou arquivada com o órgão governamental aplicável que comprove a existência da empresa.

• Em caso de certificados servidor, a determinação que o Solicitante ao Certificado é o proprietário do registro do nome do domínio do servidor que é o Objeto do Certificado, ou autorizado a usar o domínio,

• Uma confirmação telefônica, carta postal confirmatória ou procedimento comparável para que o Solicitante de Certificado confirme certas informações sobre a organização, confirme que a organização autorizou a Solicitação de Certificado e confirmar que a pessoa submetendo a solicitação em nome do Solicitante de Certificado está autorizada a fazê-los.

• No caso de IDs de Servidor Global, as verificações adicionais necessárias para atender às regulamentações norte-americanas de exportação e licenças emitidas pelo U.S. Department of Commerce Bureau of Industry and Science (“BIS”) (antes conhecido como Bureau of Export Administration - “BXA”).

3.1.8.1.2. Autenticação para PKI’s gerenciadas para SSL ou PKIs Gerenciadas para SSL Premium Edition

Com relação às PKIs Gerenciadas para Clientes SSL e SSL Premium Edition, o processo de confirmação de identidade se inicia com a confirmação de identidade da VeriSign ou de uma Afiliada da PKI Gerenciada para o Cliente SSL ou PKI Gerenciada para o Cliente SSL Premium Edition, conforme esta PC, § 3.1.8.2. Seguindo a confirmação, a PKI Gerenciada para Cliente SSL ou a PKI Gerenciada para Cliente SSL Premium Edition é responsável pela aprovação da emissão de Certificados aos servidores dentro de sua organizações, através de:

• Confirmação de que o servidor designado como o Objeto da ID de Servidor Seguro ou ID de Servidor Global realmente existe, e

• Certificação de que a organização autorizou a emissão de uma ID de Servidor Seguro ou ID de Servidor Global para o servidor.

3.1.8.1.3. Autenticação para Certificados ASB Corporativos Classe 3

A confirmação da identidade de um Solicitante de Certificado para um Certificado ASB Corporativo de Classe 3 deverá incluir:

• A determinação de que a organização existe, usando pelo menos um serviço ou banco de dados de comprovação de identidade de Parte Confiante, ou documentação da empresa emitida ou arquivada com o órgão governamental aplicável que comprove a existência da empresa.

• Uma confirmação telefônica, carta postal confirmatória ou procedimento comparável para que o Solicitante de Certificado confirme certas informações sobre a organização, confirme que a organização autorizou a Solicitação de Certificado e confirme que o representante submetendo a solicitação de certificado em nome do Solicitante de Certificado está autorizada a fazê-lo, e

• Uma confirmação telefônica, carta postal confirmatória e/ou procedimento comparável para que o representante do Solicitante de Certificado possa confirmar que a pessoa nomeada como representante enviou a Solicitação de Certificado.

3.1.8.2. Autenticação da Identidade de ACs e ARs (Classe 1-3)

Afiliadas, Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB, antes de se tornarem ACs ou ARs, celebram um contrato com uma entidade acima dentro da hierarquia VTn de Classe 1, 2 ou 3 (a “Entidade Superior”) ou um Centro de Serviços Universal ou Revendedor, comercializando em nome da VeriSign ou uma Afiliada. A tabela abaixo mostra as possíveis Entidades Superiores correspondentes a cada Solicitante de Certificado de AC.

A Entidade Superior deverá autenticar a identidade da futura Afiliada, Cliente de PKI Gerenciada, Cliente Gateway ou Cliente ASB antes da aprovação final de seu status como AC ou AR, exceto onde a VeriSign ou uma Afiliada delegue tal responsabilidade a um Centro de Serviço Universal ou Revendedor. Onde ocorrer tal delegação, o Centro de Serviços Universal ou Revendedor deverá autentica a identidade do futuro Cliente de PKI Gerenciada. Para os fins desta PC, a VeriSign ou a Afiliada permanece sendo a Entidade Superior, em vez do Centro de Serviços Universal ou Revendedor. Os procedimentos de Afiliadas para a autenticação da identidade da organização de Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB deverão ser submetidas à VeriSign para aprovação, e tal aprovação é uma condição para que uma Afiliada possa iniciar suas operações como provedora de PKI Gerenciada, serviços Gateway ou ASB, conforme for o caso. Os procedimentos de Centros de Serviço Universal e Revendedores para a autenticação da identidade organizacional deverá será submetida à VeriSign para aprovação, sendo esta aprovação uma condição para que uma Afiliada possa iniciar suas operações como provedora de PKI Gerenciada, serviços Gateway ou ASB, conforme for o caso.

A identidade das Afiliadas, Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB confirmar-se-á por meio de:

• Aparição pessoal de um representante autorizado da organização ante pessoas autorizadas da Entidade Superior à organização, um Centro de Serviços Universal ou Revendedor, junto com procedimento de autenticação para assegurar a confirmação da organização e a autoridade de seu pessoal, ou

• No caso de a VeriSign ou uma Afiliada confirmarem a identidade de Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB, os procedimentos determinados no Guia de Práticas de Requisitos Legais de Afiladas ou, no caso de Centros de Serviço Universal ou Revendedores confirmando a identidade de Clientes de PKI Gerenciada ou Clientes ASB, as exigências impostas pela VeriSign ou Afiliadas aos Centros de Serviço Universal e Revendedores. Estes procedimentos incluem:

a. o As verificações necessárias para confirmação da identidade do Assinante corporativo, conforme a PC, § 3.1.8.1, com exceção de uma Solicitação de Certificado, as validações é de uma solicitação para se tornar um Cliente de PKI Gerenciada, Cliente Gateway ou Cliente ASB, e

b. o No caso de Clientes de PKI Gerenciada ou Clientes Gateway, a confirmação de que a pessoa identificada como Administrador de PKI Gerenciada ou Administrador Gateway está autorizada em atuar conforme sua capacidade.

3.1.9. Autenticação de Identidade Individual

Os procedimentos de autenticação deverão estar em conformidade com os requisitos específicos para cada Classe de Certificado, conforme determinado no Guia de Práticas de Requisitos Legais da Afiliada. Métodos sólidos de autenticação para cada Classe de Certificado definia nesta Seção

3.1.9. deve ser permitido para atender às necessidades do negócio.

Em geral, os procedimentos de autenticação de cada Classe de Certificados estão confirmando que o Solicitante de Certificado é a pessoa identificada na Solicitação de Certificado (exceto pelos Solicitantes a Certificados que detêm os direitos da chave privada correspondente à chave pública relacionada no Certificado, conforme rege o parágrafo 3.1.7 da PC, e que as informações a serem relacionadas no Certificados são precisar, exceto pelas Informações de Assinante Não-verificadas. Estes procedimentos, junto com procedimentos mais detalhados descritos abaixo para cada Classe de Certificado.

Os procedimentos das Afiliadas para a autenticação de identidade individual deverão ser aprovados pela VeriSign antes que a Afiliada inicie suas operações como AC ou AR, para emitir ou aprovar Solicitações de Certificado para Certificados de Classe 1-3 ou como prestador de serviços a Clientes, emitindo ou aprovando Solicitações de Certificados para Certificados de Classe 1-2.

3.1.9.1. Certificados de Classe 1

A Autenticação de indivíduos para Certificados de Classe 1 deverá consistir na verificação que assegura que o nome distinto do Titular é único e inequívoco dentro do Subdomínio da VeriSign, Afiliada ou Cliente Gateway Classe 1. A autenticação de classe 1 não oferece garantias de identidade, i.e., que o Assinante é quem ele/ela diz ser. O nome comum do Assinante é uma Informação de Assinante não-verificada. A autenticação de Classe 1 também inclui uma confirmação limitada do endereço de e-mail

do Solicitante de Certificado. Os Centros de Serviços que oferecem Certificados de Classe 1 delegam estas funções de autenticação a um Centro de Processamento.

A autenticação feita por Clientes de PKI Gerenciada e Clientes Gateway para Certificados de PKI Gerenciada Classe 1 incluem os procedimentos de autenticação supracitados, que também são delegados às Entidades Superiores, e finalmente a um Centro de Processamento. Entretanto, o Cliente de PKI Gerenciada ou Cliente Gateway deve determinar que o Solicitante de Certificado trata-se de um Indivíduo Afiliada em relação ao Cliente de PKI Gerenciada ou Cliente Gateway antes da aprovação da Solicitação de Certificado.

3.1.9.2. Certificados Classe 2

A autenticação de Solicitações de Certificado de Classe 2 ocorre de duas maneiras. Primeiro, para Certificados de PKI Gerenciada, Clientes de PKI Gerenciada e Clientes de PKI Gerenciada Lite usam os registros comerciais ou bancos de dados com informações comerciais para aprovar ou rejeitar Solicitações de Certificado conforme a PC, § 3.1.9.2.1. O segundo método de autenticação, que se aplica a Certificados de Classe 2 Varejo e Certificados ASB Individuais de Classe 2, requerem que a VeriSign ou uma Afiliada confirme a identidade das Solicitações e Certificado, utilizando as informações residentes em um banco de dados de um serviço de comprovação de identidade aprovado pela VeriSign, conforme a PC, § 3.1.9.2.2.

3.1.9.2.1. Certificados de PKI Gerenciada Classe 2

Os Clientes de PKI Gerenciada e Clientes de PKI Gerenciada Lite deverão confirmar a identidade de indivíduos por meio da comparação das informações de inscrição com os registros comerciais ou bancos de dados de informações comerciais. Por exemplo, eles podem confirmar as informações de inscrição com base nos registros de funcionário ou contratado autônomo em um banco de dados de recursos humanos. O Cliente de Cliente de PKI Gerenciada ou Cliente PKI Gerenciada Lite pode aprovar a Solicitação de Certificado manualmente, usando o Centro de Controle de PKI Gerenciada se as informações da inscrição coincidirem com os registros do banco de dados usado para a autenticação. Este processo é conhecido como "Autenticação Manual".

O Módulo de software de Administração Automatizada para PKIs Gerenciadas e outros software similares da VTN oferecem aos Clientes de PKI Gerenciada uma opção de aprovação e revogação automática de usuários ou dispositivos diretamente a partir de um sistema administrativo pré-existente ou bancos de dados, em vez de solicitar a Autenticação Manual de cada Solicitação de Certificado. Os Clientes de PKI Gerenciada que utilizam o Módulo de software de Administração Automatizada para PKIs Gerenciadas autenticam a identidade de Solicitações de Certificado potenciais antes de colocar as informações em um banco de dados. Quando um Solicitante de Certificado envia uma Solicitação de Certificado, o Módulo de Software de Administração Automatizada compara as informações na Solicitação de Certificado com aquelas no banco de dados, e caso as informações coincidam, ocorre a aprovação automática da Solicitação de Certificado pelo Centro de Processamento. Este processo é chamado de "Autenticação Automatizada". Clientes de PKI Gerenciada que não utilizam o software de Administração Automatizada ou software VTN similar devem usar o procedimento de Autenticação Manual.

3.1.9.2.2. Certificados de Varejo Classe 2

A VeriSign e Afiliadas deverão validar Solicitações de Certificado para Certificados de Varejo Classe 1 e Certificados ASS Individuais de Classe 2 através da determinação se as informações de identificação que constam na Solicitação de Certificado coincidem com as informações residentes no banco de dados de um serviço de comprovação de identidade aprovado pela VeriSign, como uma grande central de crédito ou outra fonte confiável de serviços de informação no país ou território da VeriSign ou Afiliada. Se as informações constantes na Solicitação de Certificado coincidem com as informações no banco de dados, a Afiliada poderá aprovar a Solicitação de Certificado.

3.1.9.3. Certificados Individuais de Classe 3

A autenticação de Certificados Individuais de Classe 3 baseia-se na presença física de um Solicitante de Certificado ante um agente de uma Afiliada ou Cliente de PKI Gerenciada ou ante um tabelião ou

outro oficial com autoridade comparável dentro da jurisdição do Solicitante de Certificado. O agente, tabelião ou oficial deverão verificar a identidade do Solicitante de Certificado comparando com um formulário reconhecido de identificação emitido pelo governo federal, como passaporte, carteira de habilitação e outras credenciais de identificação.

A autenticação de Administradores para Certificados de Administradores de Classe 3 deverá consistir na autenticação da existência do empregador do Administrador (uma Afiliada ou Cliente de PKI Gerenciada) e confirmação do emprego e autorização da pessoal nomeada como Administrador. A VeriSign e Afiliadas deverão autenticar Solicitações de Certificado, primeiro pela autenticação da identidade da entidade que empregador ou mantenedora do administrador, conforme rege o parágrafo 3.1.8.2 desta PC. Tal entidade deverá ser um Centro de Processamento, Centro de Serviço ou Cliente de PKI Gerenciada. A VeriSign e Afiliadas também deverão, no curso do processo de autenticação, confirmar a autorização do Solicitante de Certificado para agir como Administrador

A VeriSign e Afiliada também terão a oportunidade de aprovar Solicitações de Certificado para seus próprios Administradores. Administradores são "Pessoas Confiáveis" dentro de uma organização (veja a PC, § 5.2.1). Nesse caso, a autenticação de Solicitações de Certificado será com base na confirmação das identidades em relação a seu emprego ou retenção como contratado autônomo (veja PC § 5.2.3) e procedimentos secundários de verificação (veja PC § 5.3.2).

VeriSign e Afiliada podem aprovar Certificados de Administrador associados a um destinatário que não seja pessoa, como um dispositivo ou servidor. A Autenticação de Solicitações de Certificado de Administrador Classe 3 para destinatários não-humanos deverão incluir::

. • Autenticação de existência e identidade do serviço nomeado como o Administrador na Solicitação de Certificado

. • Autenticação de que o serviço foi implementado de forma consistente com a realização das funções administrativas.

. • Confirmação de emprego e autorizada da pessoa se inscrevendo para o Certificado de Administrador para o serviço nomeado como Administrador na Solicitação de Certificado.

3.2. Renovação Temporária de Chave (Renovação) (Classe 1-3)

3.2.1. Renovação de Certificados de Assinantes

A entidade que aprova a Solicitação de Certificado para o Assinante de um Certificado deverá ser responsável pela autenticação da solicitação de renovação. Os procedimentos de renovação deverão assegurar que a pessoal ou organização que pretendem renovar um Certificado de Assinante é, de fato, o Assinante do Certificado.

Um procedimento aceitável é o uso de uma Frase de Desfio (ou equivalente), ou prova de posse da chave privada. Os assinantes escolhe e enviam suas informações de registro com uma frase de identificação. Mediante a renovação de um Certificado, se um Assinante enviar corretamente a frase de identificação de Assinante (ou equivalente) junto com as informações de renovação de registro do Assinante e informações do registro original (incluindo informações de contato), contato que tais informações não tenham sido alteradas, a renovação do Certificado é emitida automaticamente. Após renovação de chave ou renovação completa dessa forma, e em circunstâncias alternativas de renovação ou nova emissão de chave, a AC ou AR deverão reconfirmar a identidade do Assinante, conforme os requisitos especificados na PC, §§ 3.1.8.1, 3.1.9 para a autenticação de uma Solicitação de Certificado original.

Outros procedimentos, bem como procedimentos aprovados pela VeriSign, os requisitos de autenticação de uma Solicitação de Certificado original, conforme a PC §§ 3.1.8.1, 3.1.9 deverá ser utilizado na renovação de Certificado de Assinante. A autenticação de uma solicitação de renovação de Certificado ASB Corporativo de Classe 3, entretanto, requer o uso de uma frase de identificação, bem como procedimentos para uma Solicitação original de Certificado, conforme a PC, § 3.1.8.1.3.

3.2.2. Renovação de Certificados da AC

Uma Entidade Superior da AC que aprova uma solicitação de Certificado de AC responsabilizar-se-á pela autenticação da solicitação de renovação. Os procedimentos de renovação deverão assegurar que uma

organização que pretende renovar um Certificado de AC de um Centro de Processamento, Centro de Serviços Cliente, Cliente de PKI Gerenciada, Cliente Gateway ou Cliente ASB é, de fato, o Assinante do Certificado da AC. Os procedimentos de autenticação deverão ser os mesmo que aqueles usados no registro original, conforme rege o parágrafo § 3.1.8.2 da PC.

3.3. Renovação de Chave Após Revogação (Classe 1-3)

A renovação após a revogação é regida pelo parágrafo § 3.3 desta PC. A renovação após revogação não será permitida, porém, se a revogação ocorrer devido à emissão do Certificado (outro certificado que não os de Classe 1) por outra pessoa que não aquela indicada como Objeto do Certificado, ou da emissão do Certificado (classe 2 ou 3) sem a autorização da pessoa indicada como Objeto do Certificado, ou a entidade que aprova a Solicitação de Certificado do Assinante descobre ou tem motivos para crer que um fato material na Solicitação do Certificado é falso.

Sujeitos ao parágrafo anterior, a renovação de um Certificado corporativo ou de AC, seguida da revogação do Certificado é permitida contanto que os procedimentos de renovação assegurem que a organização ou AC requerente da renovação é, de fato, o Assinante do Certificado. Certificados corporativos renovados deverão conter o mesmo nome distinto de Objeto que o Object que consta no Certificado sendo renovado.

A renovação de Certificado individual, seguida da revogação, deverá novamente assegurar que a pessoal que solicita a renovação é, de fato, o Assinante. Um procedimento aceitável é o uso de uma Frase de Desfio (ou equivalente), ou prova de posse da chave privada. Para outros procedimentos diferentes deste, bem como procedimentos aprovados pela VeriSign, os requisitos para validações de uma Solicitação de Certificado original, conforme a PC §§ 3.1.8.1, 3.1.9 deverá ser utilizado na renovação de Certificado seguido de revogação.

3.4. Solicitação de Revogação (Classe 1-3)

Os procedimentos de revogação deverão assegurar que antes de qualquer revogação de qualquer Certificado, que a revogação foi de fato solicitada pelo Assinante do Certificado, a entidade que aprovou a Solicitação de Certificado, o Centro de Processamento aplicável, ou no caso de Certificados emitidos por uma AC de Cliente ASB CA, o Cliente ASB aplicável. Os procedimentos aceitáveis para autenticação de solicitações de revogação de um Assinante são os seguintes:

. • O Assinante deverá possuir, para certos tipos de certificado a frase de identificação do Assinante (ou equivalente), resultando na revogação automática do Certificado ao fornecer a frase de identificação correta (ou equivalente) que consta no registro,2

. • Recebimento de uma mensagem que aparenta ser do Assinante, que solicita revogação e contém uma assinatura digital verificável, referente ao Certificado a ser revogado, e

. • Comunicação como Assinante, fornecendo garantias razoáveis conforme a Classe de Certificado de que a pessoa ou organização solicitação a revogação é, de fato, o Assinante. Esta comunicação, dependendo das circunstâncias, poderá incluir um ou mais meios de verificação: telefone, número de fax, e-mail, endereço postal ou serviço de mensageiros.

Os Administradores de AC/AR têm o direito de solicitar a revogação de Certificados de Assinantes dentro do subdomínio das ACs e ARs. A VeriSign e Afiliadas deverão autenticar a identidade de Administradores através do controle de acesso usando a autenticação SSL e cliente antes de permitir a execução das funções de revogação. No caso de Administradores de ACs de Clientes ASB fornecendo instruções de revogação, os Provedores ASB deverão autenticar a identidade de tais Administradores de ACs usando comunicação telefônica.

Os Clientes de PKI Gerenciada que utilizam o Módulo de Administração Automatizada podem enviar solicitações de revogação em lotes ao Centro de Processamento. Tais solicitações deverão ser autenticadas através de uma solicitação com assinatura digital, usando a chave privada no dispositivo de controle de acesso de hardware de Administração Automatizada do Cliente de PKI Gerenciada.

As solicitações de Centros de Processamento, Centros de Serviços Cliente, Clientes de PKI Gerenciada e Clientes Gateway para a revogação de um Certificado AC deverão ser autenticadas pelas Entidades Superiores, para assegurar que a revogação foi, de fato, solicitada pela AC. Os Centros de Processamento que recebem uma solicitação de revogação um Centro de Serviços, por iniciativa do próprio Centro de Serviços, o Certificado de AC de um dos Clientes de PKI Gerenciada ou Clientes Gateway deverão autenticar a solicitação para garantir que a revogação foi, de fato, solicitada pelo Centro de Serviços.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado (Classe 1-3)

4.1.1. Solicitações para Certificados de Assinante

Todos os Solicitantes ao Certificado deverão passar pelo processo de inscrição, que consiste em::

• completar uma Solicitação de Certificado, fornecendo as informações solicitadas,

• gerar ou tomar as medidas necessárias para a criação de um par de chaves, conforme a PC, § 6.1,

• fornecer sua chave pública ao Centro de Processamento ou Cliente Gateway conforme o parágrafo 6.1.3 da PC,

2- A Revogação Automática On-line usando uma frase de identificação não está disponível pra Certificados VeriSign Classe 3 para Assinatura de Código e Conteúdo. Estes certificados serão revogados e publicados na LCR adequada, mediante solicitação de revogação de certificado do assinante junto à VeriSign. A solicitação deve indicar claramente sob quais circunstâncias relacionadas no § 4.4.1.1 baseia-se a solicitação de revogação. Para solicitar a revogação, os Assinantes deverão contatar o centro de atendimento ao cliente VeriSign: E-mail: support@verisign.com, ou Telefone: 1-877-438-8776 ou 1-650-426-3400. A VeriSign verificará a solicitação de revogação e os motivos que levaram à revogação antes de revogar o certificado,

• demonstrando ao Centro de Processamento ou Cliente Gateway emissor, conforme o § 3.1.7 da PC, que o Solicitante de Certificado detém a posse da chave privada correspondente à chave pública fornecida o Centro de Processamento ou Cliente Gateway, e

• manifestar aquiescência ao Contrato de Assinante relevante. Os Web Hosts poderão submeter Solicitações de Certificado em nome de seus clientes, de acordo com o Programa Web Host (veja PC, § 1.1.2.6).

As Solicitações de Certificado são enviadas a um Centro de Processamento, Centro de Serviços, Cliente de PKI Gerenciada, ou Cliente Gateway para o processamento e aprovação ou rejeição final A entidade que processa a Solicitação de Certificado e a entidade emissora do Certificado, conforme a PC, § 4.2, podem ser duas entidades distintas, conforme mostrado na tabela a seguir

Classe de Certificado	Entidade Processadora de Solicitações de Certificado	Entidade Emissora de Certificado
Certificado Individual de Varejo Classe 1	Centro de Processamento ou Centro de Serviços	Centro de Processamento
Certificado Individual Classe 1 (Gateway)	Cliente Gateway	Cliente Gateway
Certificado de PKI Gerenciada Classe 1 Individual	Cliente de PKI Gerenciada Classe 1	Centro de Processamento
Certificado Individual de Varejo Classe 2	Centro de Processamento ou Centro de Serviços	Centro de Processamento
Certificado ASB Individual Classe 2	Provedor ASB (Centro de Processamento ou Centro de Serviço)	Centro de Processamento
Certificado de PKI Gerenciada individual Classe 2	Cliente de PKI Gerenciada Classe 2 ou Cliente Lite PKI Gerenciada	Centro de Processamento
Certificado de Varejo individual Classe 3	Centro de Processamento ou Centro de Serviço	Centro de Processamento
Certificado de Administrador Classe 3	Centro de Processamento ou Centro de Serviço	Centro de Processamento

Certificados de Varejo corporativos Classe 3	VeriSign ou Centro de Serviço	VeriSign
Certificados de PKI Gerenciada corporativa Classe 3 (PKI Gerenciada para SSL ou SSL Premium Edition)	PKI Gerenciada Classe 3 para Cliente SSL ou SSL Premium Edition	VeriSign
Certificado ASB corporativo Classe 3	Provedor ASB (Centro de Processamento ou Centro de Serviço)	Centro de Processamento

Tabela 7 - Entidades Recebedoras de Solicitações de Certificado.

4.1.2. Solicitação de Certificados de ACs e ARs

Esta PC não requer que Afiliadas ou Cliente, que são assinantes de Certificados AC ou AR, completem as Solicitações formais de Certificado. Em vez disso, eles devem assinar um contrato com suas Entidades Superiores ou Centros de Serviços Universais ou Revendedores de suas Entidades Superiores. Consulte o parágrafo § 3.1.8.2 da PC. Os candidatos a AC e AR deverão fornecer credenciais, conforme exige o parágrafo 3.1.8.2 da PC, para demonstrar sua identidade e fornecer informações de contato durante o processo de contratação. Durante este processo de contratação, antes da Cerimônia de Geração de Chave para criar o par de chaves de um Centro de Processamento, Centro de Serviços Cliente, Cliente de PKI Gerenciada, Clientes Gateway ou Clientes ASB, o candidato deverá cooperar com sua Entidade Superior na determinação de um nome distinto adequado e o conteúdo dos Certificados a serem emitidos pelo Solicitante..

4.2. Emissão de Certificado (Classe 1-3)

4.2.1. Emissão de Certificados de Assinantes

Após o Solicitante de Certificado enviar a Solicitação de Certificado, a entidade recebedora da Solicitação de Certificado (veja a PC, § 4.1.1) deverá confirmar ou não confi8rmar as informações constantes na Solicitação de Certificado (informações que não seja Informações não-verificáveis do Assinante) conforme a PC, §§ 3.1.8.1, 3.1.9. Mediante a realização bem-sucedida de todos os procedimentos necessários de autenticação, conforme o § 3.1 da PC, a entidade recebedoras da Solicitação de Certificado deverá aprová-la. No caso de falha na autenticação, a entidade recebedora da Solicitação de Certificado deverá rejeitar a Solicitação de Certificado.

Um Certificado será criado e emitido, seguindo a aprovação de uma Solicitação de Certificado, ou seguindo o recebimento de uma solicitação de AR para emissão de Certificado. Os Centros de Processamento e Clientes Gateway que recebem Solicitações de Certificado deverão criar e emitir ao Solicitante de Certificado um Certificado baseado nas informações contidas em uma Solicitação de Certificado seguido da aprovação de tal Solicitação de Certificado. Quando um Centro de Serviços, Cliente de PKI Gerenciada, ou Provedor ASB aprova uma Solicitação de Certificado e comunica essa aprovação ao Centro de Processamento, o Centro de Processamento deverá criar um Certificado e emiti-lo ao Solicitante de Certificado.

Os procedimentos desta seção também deverão ser utilizados para a emissão de Certificados em relação ao envio de uma solicitação de renovação do Certificado.

4.2.2. Emissão de Certificados de ACs e ARs

A identidade das entidades que desejam se tornar Afiliadas e Clientes deverá ser autenticada conforme o disposto no § 3.1.8.2 da PC, e no caso de aprovação, serão emitidos os Certificados necessários para a execução de suas funções de AC ou AR. Antes de celebrar um contrato com uma entidade candidata à Afiliada ou Cliente, conforme o § 4.1.2, a identidade da Afiliada ou Cliente potencial deverá ser confirmada com base nas credenciais apresentadas. A execução de tal contrato indica a conclusão e aprovação final da solicitação pela Entidade Superior. A decisão de aprovação ou reprovação de uma solicitação de Afiliação ou Cliente deverá ser feita conforme critério exclusivo da Entidade Superior (ou seu Centro de Serviços Universal ou Revendedor). Após tal aprovação, a própria Entidade Superior (no caso de um Centro de Processamento) ou o Centro de

Processamento acima dela na VTN (no caso de um Centro de Serviços) deverá emitir o Certificado à AC ou AR Afiliada ou Cliente, em conformidade com o Guia de Referência para Cerimônia de Chave, o Guia de Requisitos de Segurança e Auditoria, e o parágrafo § 6.1 da PC.

4.1. Aceitação de Certificado (Classe 1-3)

Centros de Processamento, Centros de Serviços Cliente, Clientes de PKI Gerenciada, Clientes Gateway e Provedores ASB emitindo Certificados a Assinantes deverão, seja de forma direta ou mediante de uma AR, notificar os Assinantes com acesso aos Certificados, notificando-os também de que seus Certificados estão disponíveis e sobre os meios de obtenção do Certificado. Se o Centro de Processamento não estabeleceu um procedimento para notificar os Assinantes de que um Certificado foi criado, e que o Certificado está pendente, e que os Assinantes podem recuperar o Certificado, então os Centros de Serviço Servidor ou Clientes de PKI Gerenciada aprovando Solicitações de Certificados de Assinantes deverão fazê-lo.

Mediante a emissão, os Certificados deverão ser disponibilizados aos Assinantes, seja permitindo seu download de um web site ou por uma mensagem enviada ao Assinante contendo o Certificado. Por exemplo, um Centro de Processamento pode enviar ao Assinante um número PIN, que deverá ser inserido em uma página de inscrição em um web site para a obtenção do Certificado. O Certificado também poderá ser enviado ao Assinante por e-mail. Fazer o download de um Certificado, ou instalá-lo a partir de uma mensagem de e-mail constitui na aceitação do Certificado por parte do Assinante.

4.4. Suspensão e Revogação de Certificado (Classe 1-3)

4.4.1. Circunstâncias para revogação

4.4.1.1.Circunstâncias para Revogação de Certificados e Assinantes

Somente quando das circunstâncias apresentadas abaixo, deverá o certificado do Assinante ser revogado pela VeriSign, por um Centro de Processamento ou Afiliada (ou pelo Assinante, conforme o disposto no § 3.4 da DPC) e publicado em uma LCR.

Um Certificado de Assinante será revogado se:

• A entidade que aprova a Solicitação de Certificado do Assinante ou um Cliente ASB descobre ou tem motivos para crer que há um Comprometimento da chave privada do Assinante,

• O Assinante não cumpriu com uma obrigação material, representação ou garantia disposta no Contrato de Assinante aplicável,

• O Contrato de Assinante com o Assinante foi encerrado,

• A afiliação entre um Cliente de PKI Gerenciada ou um Cliente ASB na emissão de Certificados ASB Corporativos Classe 3 com um Assinante é cancelado ou encerrado,

• A afiliação entre uma organização que é um Assinante de Certificado ASB Corporativo Classe 3 e o representante organizacional controlando as chaves privadas do Assinante é rescindida ou encerrada,

• A entidade que aprova a Solicitação de Certificado do Assinante ou Cliente ASB descobre, ou tem motivos para crer que o Certificado foi emitido sem cumprir com os procedimentos necessários pela DPC aplicável, o Certificado (certificados de classe 2 ou 3) foi emitido a uma pessoa que não aquela nomeada como Objeto do Certificado, ou o Certificado (certificados de classe 2 ou3) foi emitido sem a autorização da pessoa indicada como Objeto de tal Certificado,

• A entidade que aprova a Solicitação de Certificado do Assinante ou um Cliente ASB descobre ou tem motivos para crer que há um fato material na Solicitação de Certificado que é falso,

• A entidade que aprova a Solicitação de Certificado do Assinante ou um Cliente ASB determina que o pré-requisito material para a emissão do Certificado não foi atendido ou foi desconsiderado.

• No caso de Certificados Corporativos de Classe 3, o nome da organização do Assinante muda,

• As informações que constam no Certificado, exceto por informações não-verificáveis do Assinante, estão incorretas ou foram alteradas, ou

• O assinante solicita a revogação do Certificado, conforme disposto no § 3.4 da PC.

• O uso de tal certificado representa riscos à VTN

Um Certificado de Administrador também deverá ser revogado se a autoridade do Assinante-Administrador do Certificado que atua como Administradora tenha sido desligada ou encerrada..

Os Centros de Processamento e Clientes Gateway revogam os Certificados por eles emitidos com base nas Solicitações de Certificado por eles aprovadas.. Os Centros de Processamento também deverão revogar os Certificados em conformidade com as solicitações de revogação de seus Centro de Serviços e de Clientes de PKI Gerenciada e Clientes ASB dentro de seus subdomínios. A VeriSign, Afiliadas, Clientes de PKI Gerenciada, Gateway e Clientes ASB deverão iniciar a revogação de Certificado de Assinante quando exigido pelo disposto no parágrafo § 4.4.1.1 desta PC. Os Contratos de Assinante deverão exigir do Assinante sua notificação à entidade, seja uma AC ou AR, que aprovou sua Solicitação de Certificado, caso este Assinante saiba ou suspeite que ocorreu um Comprometimento da chave privada do Assinante, conforme os procedimentos determinados no § 4.4.3.1 da PC.

4.4.1.2. Circunstâncias para revogação de certificados de ACs e ARs

O Certificado emitidos a um Centro de Processamento, Centro de Serviços, Cliente de PKI Gerenciada, dispositivo de controle de acesso de hardware da Administração Automatizada ou Cliente Gateway deverá ser revogado nos seguintes casos:

• A Entidade Superior da AC ou AR descobre ou tem motivos para crer que há um Comprometimento da chave privada da AC ou da AR,

• O contrato entre a AC ou AR com sua Entidade Superior foi rescindido,

• A Entidade Superior das ACs ou ARs descobre, ou tem motivos para crer que o Certificado foi emitido sem cumprir com os procedimentos necessários pela DPC aplicável; o Certificado foi emitido a uma entidade que não aquela nomeada como Objeto do Certificado, ou o Certificado foi emitido sem a autorização da entidade indicada como Objeto de tal Certificado,

• A Entidade Superior das ACs ou ARs determina que o pré-requisito material para a emissão do Certificado não foi atendido ou foi desconsiderado, ou

• A AC solicita a revogação do Certificado.

• O uso de tal certificado representa riscos à VTN

Centros de Processamento deverão revogar Certificados de AC dentro de seus subdomínios quando esta seção exigir a revogação. Centros de Serviços cliente, Clientes de PKI Gerenciada, Gateway e Clientes ASB devem solicitar a revogação de um Centro de Processamento que emitiu o Certificado de AC, quando a revogação se faz necessária.

4.4.2. Quem pode solicitar a revogação

4.4.2.1. Quem pode solicitar a revogação de um certificado de assinante

Assinantes Individuais estão autorizados a solicitar a revogação de seus próprios Certificados individuais. No caso de Certificados corporativos, um representante devidamente autorizado pela organização poderá solicitar a revogação dos Certificados emitidos à esta organização. Um representante devidamente autorizado da VeriSign ou Afiliada, ou um Cliente de PKI Gerenciada cujo Administrador receba um Certificado de Administrador estará autorizado a solicitar de revogação do Certificado de Administrador. A entidade que aprova a Solicitação de Certificado de um Assinante também estará intitulada a revogar ou solicitar a revogação do Certificado do Assinante. Um Cliente ASB estará autorizado a iniciar a revogação de Certificados emitidos por sua AC.

4.4.2.2. Quem pode solicitar a revogação de um certificado de uma AC ou AR

Apenas a VeriSign tem autorização para solicitar ou iniciar a revogação de Certificados emitidos às suas ACs. Centros de Processamento que não são da VeriSign, Centros de Serviços, Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB estarão autorizados, por meio de seu representante devidamente autorizado, a solicitar a revogação de seus próprios Certificados, e suas Entidades Superiores estarão autorizadas a solicitar ou iniciar a revogação de seus Certificados.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. Procedimento para solicitação de revogação de um certificado de assinante

Um Assinante que solicita a revogação deverá comunicar sua solicitação à entidade que aprovação sua Solicitação de Certificado de Assinante (uma AC ou AR), sendo que tal entidade deverá revogar ela mesma o Certificado (em caso de Centros de Centros de Processamento ou Clientes Gateway) ou solicitar a revogação ao Centro de Processamento que emitiu o Certificado (no caso de Centro de Serviços ou Clientes de PKI Gerenciada). A comunicação de tais solicitações deverá ser feita conforme disposto no parágrafo 1.3.4 da PC. Um Centro de Processamento, Centro de Serviços, Cliente de PKI Gerenciada, Cliente Gateway ou Cliente ASB revogando um Certificado de Assinante por sua própria iniciativa, deverá revogar o Certificado (no caso de Centros de Processamento ou Clientes Gateway) ou solicitar a revogação junto ao Centro de Processamento que emitiu o Certificado (no caso de Centro de Serviços ou Clientes de PKI Gerenciada) ou junto ao Provedor ASB (no caso de Clientes ASB). Um Provedor ASB revogando um Certificado de Assinante deverá se incumbir da revogação (no caso de Provedores ASB que também são Centros de Processamento) ou solicitar a revogação ao Centro de Processamento que emitiu o Certificado (no caso de Provedores ASB que são Centros de Serviços).

4.4.3.2. Procedimento para solicitação de revogação de um certificado de uma AC ou AR

A AC ou AR solicitando a revogação deverá comunicá-la a sua Entidade Superior. Esta por sua vez deverá fazer a revogação do Certificado (no caso de Centros de Processamento) ou solicitar a revogação ao Centro de Processamento que emitiu o Certificado (no caso de Centros de Serviços). A Entidade Superior de uma AC ou AR revogando Certificados de ACs ou ARs por iniciativa própria deverão iniciar a revogação da mesma maneira.

4.4.4. Prazo para solicitação de revogação

As solicitações de revogação devem ser enviadas assim que possível, dentro do período comercial razoável.

4.4.5. Circunstâncias para suspensão

A VTN não oferece serviços de suspensão de Certificados de Assinantes.

4.4.2. Quem pode solicitar a suspensão

Não se aplica

4.4.7. Procedimento para solicitação de suspensão

Não se aplica

4.4.8. Limites no período de suspensão

Não se aplica

4.4.9. Freqüência de emissão de LCR (se aplicável)

A VTN oferece Listas de Certificados Revogados (“LCR”) mostrando a revogação de Certificados da VTN, e oferecendo serviços de verificação de status através do Repositório da VeriSign e Afiliadas. As LCRs de Certificados de Assinantes deverão ser emitidas ao menos uma vez ao dia. As LCRs de Certificados de AC deverão ser emitidas a cada quinzena, porém sempre que um Certificado de AC for revogado. As LCRs de ACs raiz de Assinatura Autenticada de Conteúdo (ACS - Authenticated Content Signing) são anualmente publicadas e sempre que um Certificado de AC for revogado. Caso um Certificado apresentado na LCR expire, ele pode ser removido a partir da próxima edição das LCRs, após sua expiração.

4.4.10. Requisitos para verificação de LCR

As terceiras partes (“Parte Confiante”) deverão verificar o status dos Certificados nos quais confiam. Um método pelo qual Parte Confiante poderão verificar o status de um Certificado é através da consulta da LCR

mais recente da AC que emitiu ou Certificado em que esta terceira parte deseja confiar. Alternativamente, Parte Confiante poderão atender a esta exigência, seja pela verificação de status do Certificado usando o repositório da Web aplicável ou usando o OCSP (se disponível). A VeriSign e Afiliadas deverão fornecer a Parte Confiante informações sobre como localizar a LCR adequada, repositório na Web ou OCSP responder (quando disponível) para verificar o andamento da revogação.

4.4.11. Disponibilidade para revogação ou verificação de status on-line

A revogação on-line e outras informações de status de Certificado deverão estar disponíveis mediante de um repositório na Internet e, onde oferecido, no OCSP. A VeriSign e Afiliadas deverão dispor de um repositório na Web que permita a Parte Confiante fazer consultar online com relação à revogação e outras informações de status de Certificado. Um Centro de Processamento, como parte de seu contrato com um Centro de Serviços, deverá hospedar o repositório para o Centro de Serviços. A VeriSign e Afiliadas deverão fornecer a Parte Confiante informações sobre como localizar o repositório adequado para verificar o estado do Certificado, e se o OCSP estiver disponível, como localizar o OCSP responder correto. Consulte o parágrafo .4.4.9

4.4.12. Requisitos para verificação de revogação on-line

Se uma terceira parte não verifica o estado de um Certificado em que deseja confiar, através da consulta da LCR mais recente, esta terceira parte deverá verificar o estado do Certificado através da consulta do repositório aplicável ou solicitando o estado do Certificado usando o OCSP responder (onde houver serviços OCSP disponíveis).

4.4.13. Outras formas disponíveis para divulgação de revogação

Sem estipulação

4.4.14. Requisitos para verificação de outras formas de divulgação de revogação

Sem estipulação

4.4.15. Requisitos especiais para o caso de comprometimento da chave

Os participantes da VTN deverão ser notificados sobre qualquer Comprometimento real ou potencial da chave privada da AC, usando dos recursos comercialmente viáveis. A VeriSign e Afiliadas deverão utilizar todos os recursos comercialmente viáveis para notificar Parte Confiante potenciais caso descubram, ou tenham motivos para crer que houve um Comprometimento da chave privada de uma de suas ACs ou uma das ACs dentro de seus subdomínios.

4.5. Procedimentos de auditoria de segurança

4.5.1. Tipos de eventos registrados

Os tipos de eventos de auditoria que devem ser registrados por cada entidade são definidos abaixo: Todos os registros (logs), em formato eletrônico ou manual, deverão conter a data e hora do evento, a identidade da entidade que causou o evento..

4.5.1.1. Eventos Registrados por Centros de Processamento

Os Centros de Processamento deverão registrar em arquivos de registro (log) os eventos relacionados à segurança do sistema da AC, tais como:

- Inicialização e desligamento do sistema,
- Inicialização e desligamento do aplicativo da AC,
- Tentativas de criação, remoção, geração de senhas ou alteração nos privilégios de sistema de usuários privilegiados (funções de confiança)
- Alterações nos detalhes e/ou chaves da AC,
- Alterações nas políticas de criação de Certificado, por exemplo, período de validade,

• Tentativas de acesso (login) e saída (logoff),

• Tentativas não autorizadas no acesso de rede ao sistema da AC,

• Tentativas não autorizadas de acesso a arquivos de sistema,

• Geração de chaves próprias de ACs e autoridades certificadores subordinadas,

• Falha nas operações de leitura e escrita de Certificado e repositório,

• Eventos relacionados à administração do ciclo de vida do Certificado, (por exemplo., solicitações, emissões, revogações e renovações de Certificados), e

• Eventos relacionados à administração do ciclo de vida do módulo criptográfico (por exemplo., recibo, uso, desinstalação e remoção).

Os Centros de Processamento deverão coletar e consolidar, seja de forma eletrônica ou manual, as informações de segurança não relacionadas ao sistema da AC, como:

• Cerimônia de Geração de Chave e bancos de dados de administração de chaves,

• Registros de acesso físico,

• Alterações na configuração do sistema e manutenção,

• Alterações no quadro de funcionários,

• Relatórios de discrepância e comprometimento,

• Registros de destruição de mídia contendo material de chave, dados de ativação ou informações pessoais do Assinante, e

• Posse dos dados de ativação para operações com chave privada da AC.

4.5.1.2. Eventos registrados por Centros de Serviço, Clientes de PKI Gerenciada (Classe 1-3)

Os Centros de Serviços e Clientes de PKI Gerenciada deverão registrar em arquivos de registro de auditoria os eventos relacionados à segurança do sistema, como:

• Inicialização e desligamento do sistema,

• Inicialização e desligamento do aplicativo da AR,

• Tentativas de criação, remoção, geração de senhas ou alteração nos privilégios de sistema de usuários privilegiados (funções de confiança)

• Alterações nos detalhes e/ou chaves da AR,

• Alterações nas políticas de criação do certificado, por exemplo, período de validade,

• Tentativas de acesso(login) e saída (logoff),

• Tentativas não autorizadas no acesso de rede ao sistema da AC/AR,

• Tentativas não autorizadas de acesso a arquivos de sistema,

• Falha nas operações de leitura e escrita de Certificado e repositório,

• Eventos relacionados à administração do ciclo de vida do Certificado (por exemplo, aprovação ou reprovação de solicitações de certificado) e

• no caso de Clientes de PKI Gerenciada usando o Gerenciador de Chave para PKI Gerenciada a cópia de segurança (backup) e recuperação das chaves privadas do Assinante.

4.5.1.3. Eventos registrados por Clientes Gateway (Classe 1)

Os Clientes Gateway deverão registrar em arquivos de registro de auditoria os eventos relacionados à segurança do sistema da AC, tais como:

• Tentativas de criação, remoção, geração de senhas ou alteração nos privilégios de sistema de usuários privilegiados (funções de confiança)

• Alterações nos detalhes e/ou chaves da AC,

• Tentativas não autorizadas no acesso de rede ao sistema da AC,

• Tentativas não autorizadas de acesso a arquivos de sistema,

• Geração de chaves de AC,

• Criação e revogação de certificados,

• Eventos relacionados à administração do ciclo de vida do Certificado, (por exemplo., solicitações, emissões, revogações e renovações de Certificados), e

• Eventos relacionados à administração do ciclo de vida do módulo criptográfico (por exemplo., recibo, uso, desinstalação e remoção), onde houver um módulo criptográfico em uso.

4.5.2. Freqüência de auditoria de registros (Classe 1-3)

Os Centros de Processamento, Centros de Serviços, Clientes de PKI Gerenciada, e Clientes Gateway deverão revisar seus registros de auditoria em resposta a alertas baseados em irregularidades e incidentes oriundos dos sistemas da AC/AR. Os Centros de Processamento deverão comparar seus registros de auditoria com os registros eletrônicos e manuais de apoio de seus Clientes de PKI Gerenciada e Centros de Serviços, sempre que qualquer ação for considerada suspeita.

O processamento do registro de auditoria consistirá na revisão dos registros de auditoria e na documentação do motivo para todos estes eventos significativos em um resumo dos registros de auditoria. As revisões dos registros de auditoria deverão incluir a verificação da inviolabilidade do registro, inspeção de todas as entradas de registro e investigação de alertas ou irregularidades registradas. As medidas a serem tomadas com base nas revisões do registro de auditoria deverão ser documentadas.

4.5.3. Período de retenção para registros de auditoria (Classe 1-3)

Os registros de auditoria deverão ser retidos por um período mínimo de 02 (dois) meses, após o processamento e posterior arquivamento, conforme disposto no § 4.6.2 da PC.

4.5.4. Proteção de registro de auditoria (Classe 1-3)

Os registros de auditoria deverão ser protegido por um sistema eletrônico de registros de auditoria que inclui mecanismos de proteção para os arquivos de registro, impedindo a visualização, modificação, exclusão ou outros tipos de violação não-autorizadas.

4.5.5. Procedimentos para cópias de segurança de registro de auditoria (Classe 1-3)

Cópias de segurança adicionais dos registros de auditoria deverão ser diariamente criadas, com a produção semanal completa de cópias de segurança.

4.5.6. Sistema de coleta de dados de auditoria (Classe 1-3)

Sem estipulação

4.5.7. Notificação de agentes causadores de eventos (Classe 1-3)

Quando um evento é registrado pelo sistema de coleta de dados de auditoria, não é preciso notificar o indivíduo, organização, dispositivo ou aplicativo que tenha causado o evento.

4.5.8. Avaliações de vulnerabilidade (Classe 1-3)

Os eventos no processo de auditoria são registrados, em parte, para monitorar as vulnerabilidades do sistema. As avaliações lógicas de vulnerabilidade de segurança (“LSVAs”) deverão ser realizadas, revistas e revisadas seguido de uma avaliação destes eventos monitorados. As LSVAs tomarão como base os dados de registro automático em tempo real e deverão ser executadas diariamente, mensalmente ou anualmente, conforme suas definições nos Requisitos de Segurança e Auditoria. Uma LSVA anual servirá como uma entrada para uma Auditoria de Conformidade anual de uma entidade.

4.6. Arquivamento de registros (Classe 1-3)

4.6.1. Tipos de eventos registrados

Os registros deverão ser mantidos e disponibilizados à VeriSign ou Entidade Superior mediante solicitações que incluam:

(i) documentação de registro de conformidade da própria entidade, com a CPS aplicável e demais obrigações conforme regem os contratos firmados com suas Entidades Superiores, e

(ii) documentação de medidas e informações que são pertinentes à cada Solicitação de Certificado e à criação, emissão, uso, revogação, expiração e renovação de cada Certificado emitido. Estes registros deverão conter todas as evidências relevantes no registro de posse da entidade referentes a:

• a identidade do Assinante nomeado em cada Certificado (exceto Certificados Classe 1, para os quais é mantido apenas um registro do nome inequívoco do Assinante),

• a identidade das pessoas que solicitam a revogação do Certificado (exceto para Certificados de Classe ,

.para os quais é mantido apenas um registro do nome inequívoco do Assinante), • outros fatos representados no Certificado,

• selos cronológicos, e

• certos fatos previsíveis relacionados à emissão de Certificados, incluindo sem limitar-se às informações relevantes para a conclusão bem sucedida de uma Auditoria de Conformidade, conforme o disposto no § 2.7 da PC.

Os registros podem ser mantidos em forma de mensagens eletrônicas ou documentos impressos, contanto que estejam indexados, armazenados, conservador e sua reprodução seja precisa e integral.

4.6.2. Período de retenção para arquivo

Os registros associados a um Certificado compilados no parágrafo § 4.6.1 da PC deverão ser mantidos por um período mínimo a ser definido abaixo, seguindo da data de expiração ou revogação do Certificado:

• 05 (cinco) anos para Certificados de Classe 1,

• 10 (dez) anos para Certificados de Classe 2,

• 30 (trinta) anos para Certificados de Classe 3. As DPCs podem conter períodos prolongados de retenção, conforme exige a legislação aplicável.

4.6.3. Proteção de arquivo

Uma entidade que mantém um arquivo de registros compilados conforme o § 4.6.1 da PC deverá proteger o arquivo, de forma que somente Pessoas de Confiança autorizadas pela entidade possam ter acesso ao arquivo. O arquivo deverá ser protegido contra a visualização, modificação, exclusão não-autorizadas ou outro tipo de violação pelo armazenamento dentro de um Sistema Confiável A mídia que contém os dados do arquivo e aplicativos necessários para o processamento dos dados de arquivo deverá ser mantida para assegurar que os dados do arquivo possam ser acessado pelo período estipulado no § 4.6.2.

4.6.4. Procedimentos para cópia de segurança de arquivo

As entidades que fazem a compilação eletrônica das informações ,conforme o § 4.6.1 da PC deverão fazer, de forma progressiva, cópias de segurança diárias dos arquivos de sistema, e realizar cópias de segurança completas a cada semana.. As cópias dos registros impressos, conforme disposto no § 4.6.1, deverão ser mantidas em uma instalação de recuperação de desastres distinta, conforme o § 4.8 da PC.

4.6.5. Requisitos para datação de registros

Certificados, LCRs e outras entradas no banco de dados de revogação deverão conter informações de data e hora. Tais informações cronológicas não requerem criptografia. Vale ressaltar que o uso de datação é separado do Serviço de Cartório Digital VeriSign (veja § 1.1.2.2.2 da PC).

4.6.6. Sistema de coleta de dados de arquivo

Os sistemas de coleta de dados de arquivo de entidades dentro da VTN deverá ser feito internamente, exceto pelos Clientes de PKI Gerenciada, para os quais a funcionalidade de PKI Gerenciada oferece um serviço externo de coleta de dados de arquivo. Os Centros de Processamento deverão auxiliar os Clientes de PKI Gerenciada na conservação da trilha de auditoria. Este sistema de coleta de dados de arquivo é, portanto, para aquele Cliente de PKI Gerenciada, externo. Caso contrário, as entidades dentro da VTN devem utilizar os sistemas interno para a coleta de dados de arquivos. As CPs da VeriSign e Afiliadas deverão exigir seus próprios sistemas de coleta de dados de auditoria interna, bem como para seus Clientes Gateway e Clientes de PKI Gerenciada.

4.6.7. Procedimentos para obtenção e verificação da informação do arquivo

Para informações sobre como obter acesso às informações do arquivo, consulte o parágrafo 4.6.3 da PC.

4.7. Troca de chave (Renovação) (Classe 1-3)

Um Certificado de AC pode ser renovado se a Entidade Superior desta AC reconfirmar sua identidade, conforme disposto nos parágrafos §§ 3.1.8.2, 3.2.3 da PC. Após a reconfirmação, a Entidade Superior deverá aprovar ou rejeitar a solicitação de renovação.

Depois de aprovar ou rejeitar, a própria Entidade Superior (no caso de um Centro de Processamento) ou através de um Centro de Processamento de nível superior ao seu na VTN (no caso de um Centro de Serviços), deverá realizar a Cerimônia de Geração de Chave para um novo par de chaves para a AC. Durante tal cerimônia, a Entidade Superior deverá assinar e emitir um novo Certificado à AC. Esta Cerimônia de Geração de Chave deverá atender aos requisitos do Guia de Referências da Cerimônia de Chave, o Guia de Requisitos de Segurança e Auditoria e o § 6.1 da PC. Os novos Certificados da AC contendo as chaves públicas geradas durante a Cerimônia de Geração de Chave deverão ser dispostos a Parte Confiante, conforme o § 6.1.4 da PC.

4.8. Comprometimento e recuperação de desastre (Classe 1-3)

As cópias de segurança das seguintes informações de AC deverão ser armazenadas fora do local, e disponibilizadas em caso de um Comprometimento ou desastre: os dados de Solicitação de Certificado, dados de auditoria (conforme § 4.5 da PC) e registros de bancos de dados de todos os Certificados emitidos. As cópias de segurança das chaves privadas da AC deverão ser criadas e mantidas conforme o disposto no § 6.2.4 da PC. Os Centros de Processamento deverão manter as cópias de segurança das seguintes informações de AC de suas próprias ACs, bem como ACs dos Centros de Serviços de Cliente, Clientes de PKI Gerenciada e Clientes ASB em seus subdomínios.

4.8.1. Recursos computacionais, software e/ou dados corrompidos

Quando da corrupção de recursos, software e/ou dados computacionais, um registro do evento destinado à VeriSign e demais, bem como uma resposta ao evento deverá ser prontamente feito pela AC ou AR afetada, em conformidade com os procedimentos para relatar e lidar com incidentes e Comprometimentos nas CPS aplicáveis e o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

4.8.2. Chave da AC é revogada.

Mediante a revogação do Certificado contendo a chave pública de uma AC:

• A revogação deverá ser relatada conforme disposto no § 4.4.9 da PC no Repositório VeriSign e (no caso de ACs não-VeriSign) no repositório da Entidade Superior da AC,

• Todos os esforços comercialmente possíveis deverão ser utilizados para a notificação adicional da revogação aos participantes da VTN,

• As ACs deverão realizar um troca de chaves conforme o disposto no parágrafo 4.7 da PC, exceto se seguido da revogação de um Certificado de AC em relação ao encerramento das operações da AC, conforme o § 4.9 da PC.

4.8.3. Chave da AC está comprometida

No caso de comprometimento de chave privada de uma AC da VeriSign, Centro de Serviços Cliente, Cliente de PKI Gerenciada, Cliente Gateway ou Cliente ASB, o certificado de AC daquela entidade deverá ser revogado,

conforme o § 4.4.3.2 da PC. Portanto, a notificação da revogação deve ser feita em conformidade com o § 4.8.2 da PC, sendo que a AC deverá interromper o uso da chave privada em questão.

4.8.4. Instalação segura após desastre natural ou outro tipo de desastre

As instalações seguras de operação das entidades da VTN para as operações de AC e AR (VeriSign, Afiliadas, Clientes de PKI Gerenciada, e Clientes Gateway) deverão desenvolver, testar, manter e se necessário, implementar um plano de recuperação de desastre criado para mitigar os efeitos de qualquer tipo de desastre natural ou causado pelo homem. Os planos de recuperação de desastres deverão abordar a restauração dos serviços de sistemas de informação e as principais funções comerciais. Os locais de recuperação de desastre deverão possuir proteção física especificada no Guia de Requisitos de Segurança e Auditoria..

Os Centros de Processamento deverão ser capazes de restaura ou recuperar suas operações dentro de 24 (vinte e quatro) horas após um desastre com, no mínimo, suporte às seguintes funções: emissão de Certificado, revogação de Certificado, publicação de informações de revogação e fornecimento de informações de recuperação de chave para Clientes de Clientes de PKI Gerenciada usando um Gerenciador de Chaves para PKI Gerenciada. O banco de dados de recuperação de desastre um Centro de Processamento deverá estar sincronizado com o banco de dados de produção dentro dos limites de tempo definidos no Guia de Requisitos de Segurança e Auditoria. O equipamento de recuperação de desastre de um Centro de Processamento deverá contar com proteções físicas de segurança especificadas no Guia de Requisitos de Segurança e Auditoria, que inclui a aplicação de camadas físicas de segurança, conforme o § 5.1.1 da PC.

Os Centro de Serviços deverão ser capazes de declarar um desastre em seus sites, no idioma local e em inglês, orientando Assinantes e Parte Confiante e demais interessados a recorrerem a um Centro de Processamento para a prestação de seus serviços de ciclo de vida.

Um plano de recuperação de desastre de um Centro de Serviços ou Centro de Processamento deverá tomar as medidas necessárias para a recuperação completa dentro de uma semana após a ocorrência do desastre no local primário do Centro de Serviços ou Centro de Processamento. Cada Centro de Serviços e Centro de Processamento deverá instalar e testar os equipamentos em seus locais primários para oferece apoio às funções de AC/AR, após um desastre de tal proporção que tornaria toda a instalação inoperante. Tais equipamentos deverão assegurar total tolerância a falhas e redundância.

4.9. Extinção da AC (Classe 1-3)

A extinção de uma AC não pertencente à VeriSign (Afiliada, Cliente de PKI Gerenciada, Cliente Gateway ou Cliente ASB) estará sujeita ao contrato entre a AC sendo extinta e sua Entidade Superior (ou o Centro de Serviços Universal/ Revendedor da Entidade Superior). Uma AC em extinção e sua Entidade Superior deverão, de boa fé, fazer uso de todos os recursos possíveis para acordar sobre um plano de extinção que minimize a interferência nos serviços prestados a Clientes, Assinantes e Parte Confiante. O plano de extinção pode cobrir questões como:

- Notificação das partes afetadas pela extinção, tais como Assinantes, Parte Confiante e Clientes
- Quem arcará com os custos de tal notificação , a AC sendo extinta ou a Entidade Superior,
- A revogação do Certificado emitido para a AC pela Entidade Superior,
- A conservação dos arquivos e registros da AC pelo período determinado pelo parágrafo § 4.6 da PC,
- A continuação dos serviços de suporte ao Assinante e cliente,
- A continuação dos serviços de revogação, como a emissão de LCRs ou a manutenção dos serviços online de verificação de status,
- A revogação de Certificados não-revogados e válidos de Assinantes e ACs subordinadas, se necessário,
- O pagamento compensatório (se necessário) aos Assinantes cujos Certificados não-revogados e válidos foram revogados por força do plano de extinção ou determinação, para a emissão de Certificados substitutos a serem emitidos pela AC sucessora.
- Disposição da chave pública da AC e o dispositivo de controle de acesso de hardware contendo tal chave privada,
- As provisões necessárias para a transição dos serviços da AC para sua sucessora.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAIS E DE PESSOAL

Todas as entidades executando funções de AC e AR (VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway) deverão preparar, implementar e aplicar uma política de segurança em conformidade com o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas). Cada política de segurança deverá discutir os controles de segurança física, procedimental, lógica e de pessoal.

5.1. Controles físicos

5.1.1. Construção e localização das instalações

Todas as operações de AC e AR (pela VeriSign, Afiliada, Cliente de PKI Gerenciada ou Cliente Gateway) deverão ser conduzidas dentro de um ambiente fisicamente protegido, que possa conter, prevenir e detectar o uso não-autorizado, acesso ou divulgação de informações e sistemas confidenciais. Para a VeriSign e Afiliadas, este ambiente deve cumprir com os requisitos do Guia de Requisitos de Segurança e Auditoria. Tais requisitos se baseiam parte nos estabelecimento de camadas de proteção física. Uma camada é uma barreira como uma porta trancada ou um portão fechado que fornece controle de acesso obrigatório aos indivíduos e requer uma resposta positiva (por exemplo, as portas destravam, ou o portão se abre) para que cada indivíduo processa à área seguinte. Cada camada sucessiva oferece acesso mais restrito e maior segurança física contra instruções e acesso não-autorizado. Além disso, cada camada física de segurança deve conter a próxima camada interna, de tal forma que a camada interna esteja completamente contida na camada externa e não possui uma parede externa em comum com a camada externa, sendo a camada mais externa a parede externa da instalação predial.

5.1.1.1. Requisitos para Clientes Gateway (Classe 1)

A instalação de um Cliente Gateway que aloja sua AC deverá possuir, no mínimo, duas camadas físicas de segurança, Camada 1 e Camada 2, onde os Clientes Gateway deverão realizar todas as operações de criptografia dentro da Camada 2 ou superior.

5.1.1.2. Requisitos para Clientes de PKI Gerenciada (Classe 1-3)

A instalação de um Cliente de PKI Gerenciada que comporta as funções de sua AR deverão ter no mínimo, duas camadas de proteção física, Camada 1 e Camada 2. Todas as operações de validação de AR deverão ser realizadas dentro da Camada 2 ou superior. Clientes de PKI Gerenciada utilizando o serviço de Administração Automatizada deverão colocar o servidor de Administração Automatizada na Camada 3 ou superior. Além disso, os Clientes de PKI Gerenciada cujos Assinantes estiverem usando o Serviço de Roaming VeriSign deverão possuir quatro camadas de proteção física, Camadas de 1 a 4. Os Serviços Corporativos de Roaming Servers deverão ser colocados na Camada 4 ou superior.

Todas as instalações de Clientes de PKI Gerenciada deverão ser construídas com material que obstruirá, impedirá detectará a penetração pública ou secreta.

5.1.1.3. Requisitos para Centros de Serviço (Classe 1-3)

Os Centro de Serviços deverão construir as instalações de alojamento para as funções de AR com pelo menos quatro camadas de proteção física, Camadas de 1 a 4. Os Centros de Serviço deverão realizar todas as funções de AR dentro da Camada 3 ou superior. Os Centro de Serviços deverão disponibilizar os sistemas de Serviços de Informações necessários ao apoio das funções de AC e AR na Camada 4 ou superior.

As instalações dos Centros de Serviço deverão ser construídas com material capaz de obstruir, prevenir e detectar a infiltração secreta ou pública. As instalações dos Centros de Serviços deverão atender aos requisitos mínimos de construção de Centros de Serviços, determinados no Guia de Requisitos de Segurança e Auditoria.

5.1.1.4. Requisitos para Centros de Processamento (Classe 1-3)

Os Centros de Processamento deverão construir as instalações de alojamento para suas funções de AC com pelo menos sete camadas de proteção, Camadas 1 a 7. Os Centros de Processamento deverão realizar todas as funções de AR dentro da Camada 3 ou superior. Os Centro de Processamento deverão disponibilizar os sistemas de Serviços de Informações necessários ao apoio das funções de AC e AR

na Camada 4 ou superior. Os Serviços de Roaming da VeriSign deverão ser colocados na Camada 4 ou superior. Os Centros de Processamento deverão colocar os módulos criptográficos de AC online e offline na Camada 5 ou superior. Os Centros de Processamento deverão ainda proteger os módulos criptográficos de AC online e offline, colocando-os na Camada 7 ou superior.

As instalações dos Centros de Processamento deverão ser construídas com material capaz de obstruir, prevenir e detectar a infiltração secreta ou pública. As instalações dos Centros de Processamento deverão atender aos requisitos mínimos de construção de Centros de Processamento determinados no Guia de Requisitos de Segurança e Auditoria.

5.1.2. Acesso físico

O acesso a cada camada de proteção física, construído de acordo com a PC, § 5.1.1, deverá ser controlado de forma que cada camada possa ser acessada somente por pessoas autorizadas, em conformidade com o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

5.1.2.1. Requisitos para Clientes Gateway (Classe 1) e Clientes de PKI

Clientes Gateway e Clientes de PKI Gerenciada deverão controlar o acesso às suas instalações de AC ou AR.. Os requisitos incluem:

• Minimizar a exposição de funções privilegiadas através da definição de perfis com função específica ou grupos de autorização,

• Aplicação do controle de acesso nestes perfis ou grupos,

• Uso de crachás de identificação de proximidade (por exemplo, ID Hugues),

• Registro automatizado de acesso de entrada e saída da instalação,

• O uso de sistemas de alarme (resistentes à violação) contra invasão física para a detecção de arrombamentos ou acesso não-autorizado às camadas de proteção física dentro da instalação, e

• Notificação automatizada enviada a uma agência externa de monitoração de alarme quanto à potencial violação de segurança quando não há seguranças instalados na instalação predial. Embora não seja obrigatório, recomenda-se o uso de leitores biométricos (por exemplo, geometria da mão ou varredura digital da íris) que oferecem autenticação de fator duplo.

5.1.2.2. Requisitos do Centro de Serviço (Classe 1-3)

Os Centro de Serviços deverão controlar o acesso às instalações de suas ACs e ARs e atender aos requisitos da PC, § 5.1.2.1 e aos Requisitos do Centro de Serviços definidos no Guia de Requisitos de Segurança e Auditoria.

5.1.2.3. Requisitos para Centros de Processamento (Classe 1-3)

Os Centro de Processamento deverão controlar o acesso às instalações de suas ACs e/ou ARs e atender aos requisitos da PC, § 5.1.2.1 e aos Requisitos do Centro de Processamento definidos no Guia de Requisitos de Segurança e Auditoria.

5.1.3. Energia e ar-condicionado (Classe 1-3)

As instalações seguras da VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão ser equipadas com sistemas de fornecimento de energia reserva para garantir o fornecimento contínuo de energia elétrica. Estas instalações de segurança também devem ser equipadas com sistemas principal e reserva de aquecimento/ventilação/refrigeração de ar para o controle de temperatura e umidade relativa. Tais sistemas deverão atender aos requisitos do Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

5.1.4. Exposição à água (Classe 1-3)

As instalações seguras da VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão ser construídas e equipadas; procedimentos deverão ser implementados para evitar inundações e outros danos causados pela exposição à água, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

5.1.5. Prevenção e proteção contra incêndio (Classe 1-3)

As instalações seguras da VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão ser construídas e equipadas, além da implementação de procedimentos para prevenir e extinguir incêndios ou outras exposições ao fogo ou fumaça, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas). Tais medidas devem atender às normas de segurança local aplicáveis.

5.1.6. Armazenamento de mídia (Classe 1-3)

A VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão proteger a mídia magnética, conservando cópias de segurança de dados importantes de sistema e outras informações confidenciais, longe de água, fogo ou outros riscos ambientais, e deverão aplicar medidas de proteção para impedir, detectar e evitar o uso não-autorizado de tais mídias, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

5.1.7. Destruição de lixo (Classe 1-3)

A VeriSign, Afiliadas, Clientes de PKI Gerenciada, e Clientes Gateway deverão implementar procedimentos para o descarte de lixo (papel, mídias ou qualquer outro tipo de lixo), a fim de evitar o uso não-autorizado, acesso ou revelação do lixo que possa contar informações Confidenciais/Particulares dentro do contexto especificado no § 2.8.1 da PC, em conformidade com o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

5.1.8. Cópias de segurança em local externo (Classe 1-3)

A VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão manter cópias de segurança de dados importantes do sistema ou qualquer outro tipo de informações importantes, incluindo dados de auditoria, em uma instalação segura e fora do local, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

Funcionários, contratados e consultores que são designados para gerenciar a confiabilidade estrutural deverão ser considerados como "Pessoas Qualificadas" prestando serviços em uma "Posição Qualificada". Pessoas com a pretensão de se tornarem Pessoas Qualificadas através da obtenção de uma Posição Qualificada deverão atender aos critérios de enquadramento dispostos na PC, § 5.3.

5.2.1.1. Perfis Qualificados de Cliente Gateway (Classe 1) e Centro de Processamento (Classe 1-3)

Os Centros de Processamento e Clientes Gateway deverão considerar as categorias de seus funcionários identificadas nesta Seção como Pessoas Qualificadas que têm uma Posição Qualificada As Pessoas Confiáveis são todos os funcionários, contratados e consultores que têm acesso ou controlam operações de autenticação e operações criptográficas que possam materialmente afetar:

• a validação das informações nas Solicitações de Certificado;

• a aceitação, rejeição ou outro processamento de Solicitações de Certificado, solicitações de revogação ou de renovação, ou informações de inscrição;

• a emissão ou revogação de Certificados, incluindo (no caso de Centros de Processamento) as pessoas que têm acesso a partes restritas de seus repositórios;

• ou que lidem com informações ou solicitações de Assinante. Pessoas Qualificadas incluem também qualquer pessoa identificada como tal no Guia de Requisitos de Segurança e Auditoria. As Pessoas Qualificadas incluem, porém não se limitam a: funcionários de serviço do cliente, pessoal de administração de sistema, pessoal de engenharia designado e executivos que possam ser designados para gerenciar a fiabilidade infra-estrutural.

5.2.1.2. Perfis Qualificados de Centro de Serviços e Cliente de PKI Gerenciada (Classe 1-3)

Os Centros de Serviço e Clientes de PKI Gerenciada deverão considerar as categorias de funcionários identificadas nesta Seção como Pessoas Qualificadas com uma Posição Qualificada. As Pessoas Qualificadas são todos os funcionários, contratados e consultores que têm acesso ou controlam operações que possam materialmente afetar:

• a validação das informações nas Solicitações de Certificado;

• a aceitação, rejeição ou outro processamento de Solicitações de Certificado, solicitações de revogação ou de renovação, ou informações de inscrição;

• o processamento de solicitações de revogação de Certificados; ou

• ou que lidem com o processamento de informações ou solicitações do Assinante. Pessoas Qualificadas incluem também qualquer pessoa identificada como tal no Guia de Requisitos de Segurança e Auditoria (no caso de Centros de Serviço). As Pessoas Qualificadas incluem, porém não se limitam a funcionários de serviço do cliente, pessoal de administração de sistema, pessoal de engenharia designado e executivos que possam ser designados para gerenciar a fiabilidade infra-estrutural.

5.2.1.3. Perfis Qualificados de Clientes ASB (Classe 2-3)

Os Clientes ASB deverão considerar seus Administradores de AC, que autenticam solicitações de revogação para seus Assinante, e comunicam tais solicitações aos Clientes ASB, como sendo Pessoas Qualificadas, em uma Posição Qualificada.

5.2.2. Número de pessoas necessárias por tarefa (Classe 1-3)

A VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão estabelecer, manter e aplicar procedimentos rígidos de controle, para assegura a segregação das tarefas baseada na responsabilidade do trabalho e para assegurar que várias Pessoas Qualificadas executem tarefas críticas em conformidade com o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

5.2.3. Identificação e Autenticação de cada perfil (Classe 1-3)

A VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão confirmar a identidade e autorização de todas as pessoas que procuram se tornar Pessoas Qualificadas, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas) antes que cada indivíduo:

• seja fornecido com seus dispositivos de acesso e tenha acesso concedido às instalações necessárias;

• recebam as credenciais eletrônicas para acessar funções específicas em Sistemas de Informação e sistemas de AC ou AR. Os Clientes ASB deverão confirmar a identidade e autorização das pessoas que desejam se tornar Administradores de AC.

A autenticação da identidade deverá incluir a presença física do indivíduo ante Pessoas Qualificadas realizando funções de RH ou segurança dentro de uma entidade e uma verificação de formas reconhecidas de identificação, como passaporte ou carteira de habilitação. (Esta autenticação de Administradores de ACs de Clientes ASB deve ser realizada por membros dos grupos de RH ou segurança do Cliente ASB, que não precisam ser membros e Pessoas Qualificadas.) A identidade deverá ser confirmada por meio de procedimentos de investigação de histórico, disposto no § 5.3.1 da PC.

5.3. Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade (Classe 1-3)

A VeriSign, Afiliadas e Clientes deverão exigir que funcionários que almejam se tornar Pessoas Qualificadas apresentem provas de antecedentes qualificações e experiência necessários para executar suas futuras responsabilidades de forma completa e satisfatória, bem como prova de qualquer autorização necessária para a realização dos serviços de certificação dispostos em contratos governamentais.

5.3.2. Procedimento de verificação de antecedentes

A VeriSign, Afiliadas e Clientes deverão realizar procedimentos de verificação de antecedentes para funcionários que desejam se tornar Pessoas Qualificadas, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas). As verificações de antecedentes serão constantes para indivíduos em Posições Qualificadas a cada 03 (três) anos, no caso de verificações de antecedentes realizadas por empresas privadas ou a cada 05 (cinco) anos, no caso de verificação de antecedentes realizada por entidades governamentais. Estes procedimentos estarão sujeitos às limitações em verificação de antecedentes impostas pela legislação local. Na medida em que uma das exigências impostas por esta seção não possa ser atendida devido a um proibição ou limitação na legislação local, a entidade encarregada pela investigação deverá utilizar uma técnica investigativa alternativa, permitida pela lei, que ofereça informações similares, que incluam, sem limitar-se à obtenção de uma verificação de antecedentes realizada por um órgão governamental competente.

Os fatores revelados em uma verificação de antecedentes que podem ser considerados fundamentos para a rejeição de candidatos a Posições Qualificadas, ou para a tomada de ação contra uma Pessoa Qualificada existente são explicados no Guia de Requisitos de Segurança e Auditoria geralmente incluem (mas não se limitam) aos seguintes fatos:

• Adulterações feitas pelo candidato ou Pessoa Qualificada,

• Referências profissionais altamente desfavoráveis ou não-confiáveis;

• Certas condenações criminais,

• Indicações de falta de responsabilidade financeira.

Os relatórios contendo tais informações serão avaliados por funcionários de recursos humanos e segurança, devendo estes tomarem as medidas cabíveis, sob a ótica do tipo, extensão e freqüência do comportamento revelado pela verificação de antecedentes. Tais ações podem incluir medidas como o cancelamento de ofertas de emprego feitas aos candidatos a Posições Qualificadas ou rescisão das Pessoas Qualificadas existentes O uso das informações relevadas na verificação de antecedentes para a tomada de ações estará sujeita à legislação aplicável.

5.3.2.1. Procedimentos de verificação de antecedentes para Clientes Gateway (Classe 1), Clientes ASB (Classe 2-3) e Clientes de PKI Gerenciada (Classe 1-3)

Os Clientes Gateway, Clientes ASB e Clientes de PKI Gerenciada deverão realizar uma investigação de antecedentes das pessoas que desejam se tornar Pessoas Qualificadas, que inclui:

. • confirmação de ocupação anterior,

. • verificação de referências profissionais,

. • confirmação do mais alto nível educacional obtido (diploma universitário) ou certificado educacional relevante,

. • uma pesquisa de fichas criminais (em nível local, estadual e federal),

. • verificação de registros de crédito/registros de contabilidade

5.3.2.2. Procedimentos de Verificação de antecedentes para Centros de Serviço e Centros de Processamento (Classe 1-3)

Os Centros de Serviço e Centros de Processamento deverão realizar investigações de antecedentes das pessoas que desejam se tornar Pessoas Qualificadas, que consistem em:

. • os assuntos incluídos em uma investigação, conforme os parágrafos §§ 5.3.2.1 da PC,

. • uma pesquisa nos registros de habilitação

. • pesquisa nos registros do seguro social federal (equivalente aos registros do “Social Security Administration” nos EUA, ou órgão competente equivalente nos demais países).

5.3.3. Requisitos de treinamento Classe 1-3)

A VeriSign, Afiliadas e Clientes deverão fornecer seus funcionários com o treinamento obrigatório necessário antes da contratação efetiva, e deverá fornecer ainda treinamento prático relacionado às operações de AC

ou AR de maneira competente e satisfatória. Eles deverão ainda fazer revisões periódicas dos programas de treinamento, sendo que este deve endereçar os elementos relevantes às funções realizadas pelos funcionários. Os funcionários do atendimento ao cliente da Afiliada deverão ser aprovados no treinamento da VeriSign, como condição da Afiliada para o início das operações.

Os programas de treinamento devem abordar os elementos relevantes ao ambiente particular de trabalho da pessoa em treinamento, incluindo:

• Princípios de segurança e mecanismos da VTN e do ambiente pessoal,

• Versão de hardware e software em uso,

• Todas as tarefas a serem executadas pela pessoa,

• Relato e procedimento a adotar em caso de Incidentes e Comprometimento

• Procedimentos de recuperação de desastre e continuidade do negócio.

5.3.4. Freqüência e requisitos para reciclagem técnica (Classe 1-3)

A VeriSign, Afiliadas e os Clientes deverão oferecer treinamentos e programas de reciclagem para seu pessoal, na medida e freqüência necessárias para assegurar que os funcionários serão capazes de manter o nível de proficiência para executar suas tarefas de forma competente e satisfatória.

5.3.5. Freqüência e seqüência de rodízio de cargos (Classe 1-3)

Sem estipulação

5.3.6. Sanções para ações não autorizadas (Classe 1-3)

A VeriSign, Afiliadas e Clientes deverão determinar, manter e aplicar políticas de trabalho para a disciplina de funcionários praticantes de ações não autorizadas. As ações disciplinares podem incluir medidas como a rescisão, e deverão ser avaliadas com freqüência e severidade das ações não-autorizadas.

5.3.7. Requisitos para contratação de pessoal (Classe 1-3)

A VeriSign, Afiliadas e Clientes deverão permitir que contratados autônomos ou consultores se tornem Pessoas Qualificadas apenas o necessário para acomodar relações de terceirização claramente definidas e somente sob as seguintes circunstâncias:

(1) a entidade usando os contratados autônomos ou consultores como Pessoas Qualificadas não conta com profissionais qualificados em seu quadro de funcionários para preencher os cargos de Pessoas Qualificadas;

(2) os contratados ou consultores são confiados pela entidade da mesma forma como se fossem seus funcionários. No caso de contratados autônomos e consultores tenham acesso às instalações de segurança da VeriSign, Afiliada ou Cliente somente se forem acompanhados e diretamente supervisionados por Pessoas Qualificadas.

5.3.8. Documentação fornecida ao pessoal (Classe 1-3)

A VeriSign, Afiliadas e Clientes deverá fornecer a seus funcionários (incluindo Pessoas Qualificadas) o treinamento obrigatório e outras documentações necessárias para a execução de suas tarefas de forma competente e satisfatória.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação de par de chaves

6.1.1. Geração de par de chaves (Classe 1-3)

A geração de par de chaves deverá ser feita em conformidade com o § 6.1 desta PC, usando sistemas Confiáveis e processos que oferecem a solidez criptográfica necessária para as chaves geradas e evita a perda, revelação,

modificação ou uso não autorizado das chaves privadas. Este requisito se aplica a Assinantes, Clientes de PKI Gerenciada utilizando o Administrador de Chave para PKI Gerenciada, ACs pré-gerando pares de chaves em dispositivos de controle de acesso por hardware de Assinantes, Centros de Processamento e Clientes Gateway. Os Centros de Processamento geram pares de chave da AC do Centros de Serviços Cliente, Clientes de PKI Gerenciada e Clientes ASB em seus Subdomínios.

As chave de AC deverão ser geradas em uma Cerimônia de Geração de Chave. Todas as Cerimônias de Geração de Chave deverão atender aos requisitos do Guia de Referências da Cerimônia de Chave, o Guia do Usuário da Ferramenta de Gerenciamento de Chave da AC e o Guia de Requisitos de Segurança e Auditoria.

6.1.2. Entrega de chave privada à entidade titular (Classe 1-3)

As chaves privadas de Assinantes geralmente são geradas pelos próprios Assinantes, sendo assim desnecessária a entrada da chave privada ao Assinante. As chaves privadas devem ser entregues ao Assinante somente quando:

• Suas Solicitações de Certificado foram aprovadas por um Cliente de PKI Gerenciada usando um Administrador de Chave de PKI Gerenciada,

• Eles são Assinantes Roaming, cujas chaves privadas são enviadas aos terminais clientes que estes assinantes usam, e decriptografas para uso em uma única sessão, conforme descrito no § 1.1.2.3.3 da PC, ou

• Seus pares de chave são pré-gerados em dispositivos de controle de acesso por hardware (tokens), que são distribuídos aos Solicitantes de Certificado relacionados ao processo de inscrição.

Os Clientes de PKI Gerenciada usando o Administrador de Chave de PKI Gerenciada (ou um serviço equivalente fornecido pela VeriSign) deverão usar o Software do Administrador de Chave de PKI Gerenciada (ou software equivalente aprovado pela VeriSign) e Sistemas Confiáveis para fornecer chaves privadas aos Assinantes e garantir que a entrega, feita por meio de um pacote PKCS#12 ou qualquer outro meio comparável (por exemplo, criptografia), para evitar a perda, divulgação, modificação ou uso não-autorizado de tais chaves privadas. Onde pares de chave são pré-gerados em dispositivos de controle de acesso por hardware, as entidades distribuidoras de tais dispositivos deverão tomar as providências necessárias para fornecer segurança e proteção física dos dispositivos, evitando perda, divulgação, modificação ou uso não-autorizado de chaves privadas nos dispositivos.

6.1.3. Entrega de chave pública para o emissor de certificado (Classe 1-3)

Quando uma chave pública é transferida para um Cliente Gateway ou Centro de Processamento para ser certificada, ela deverá ser entregue através de um mecanismo que assegure que a chave pública não foi alterada durante o trânsito e que o Solicitante do Certificado possui a chave privada correspondente à chave pública transferida. O mecanismo aceitável dentro da VTN para a entrega de chave pública é o pacote de solicitação de assinatura de Certificado, PKCS#10, ou um método equivalente que assegure que:

1. 1. A chave pública não foi alterada durante o trânsito, e

2. 2. O Solicitante do certificado possui a chave privada correspondente à chave pública transferida.

Os Centros de Processamento realizando Cerimônias de Geração de Chave para si, Clientes de PKI Gerenciada, Centros de Serviços e Clientes ASB dentro de seus respectivos Subdomínios deverão transferir a chave pública do módulo criptográfico onde foi criada para o módulo criptográfico da AC superior (mesmo módulo criptográfico se uma APC), envolvendo-o em uma solicitação de assinatura de Certificado PKCS#10.

6.1.4. Entrega de chave pública da AC para usuários (Classe 1-3)

A VeriSign e Afiliadas deverão disponibilizar as chaves públicas de suas ACs e as ACs de Clientes de PKI Gerenciada, Clientes Gateway e Clientes ASB a Parte Confiante e público em geral através de Certificados de AC, de forma segura. As chaves públicas das APCs estão incluídas nos Certificados raiz que já estão incorporados em muitos aplicativos de software populares, tornando desnecessários os mecanismos de distribuição especial de raiz. Também, em muitas instâncias, um Terceiro usando o protocolo S/MIME automaticamente receberá o Certificado do Assinante, os Certificados (e assim as chaves públicas) de todas as ACs subordinadas à APC relevante.

6.1.5. Tamanhos de chave (Classe 1-3)

Os pares de chave possuem comprimento suficiente para evitar que outros determinem a chave privada do par de chaves usando a análise criptográfica, durante o período esperado da utilização de tais pares de chaves. O Padrão VTN atual para o tamanho mínimo de chave é o uso de pares de chave equivalentes a RSA de 1024 bits para APCs, Acs e Assinantes de Classe 3, e pares de chaves equivalentes em potência a um RSA de 512 bit para Assinantes de Classe 1 e 2..

6.1.6. Geração de parâmetros de chave pública (Classe 1-3)

Os Participantes VTN usando o Padrão de Assinatura Digital deverão gerar os Parâmetros de Chave necessários, conforme o padrão FIPS 186-2 ou um padrão equivalente aprovado pela PMA.

6.1.7. Verificação da qualidade dos parâmetros (Classe 1-3)

Quando Participantes VTN utilizam o Padrão de Assinatura Digital, a quantidade de Parâmetros de Chave gerados será verificada conforme o padrão FIPS 186-2 ou um padrão equivalente aprovado pela PMA.

6.1.8. Geração de chave por hardware/software (Classe 1-3)

Centros de Processamento deverão gerar pares de chaves Classe 2 e 3 (para eles mesmos, para Centros de Atendimento ao Cliente, Clientes de PKI Gerenciada ou Clientes ASB), e os números aleatórios para tais pares de chaves, em hardware. A VeriSign recomenda que os pares de chaves de AC Classe 1, (AC de Centro de Processamento ou Cliente Gateway CA), Administração Automatizada (AR), Administrador e Assinantes sejam geradas por hardware, embora tais pares de chaves possam ser gerados por hardware ou software.

6.1.9. Finalidades de uso da chave (conforme o campo “key usage” na X.509 v3) (Classe 1-3)

Para Certificados X.509 Versão 3, Centros de Processamento e Clientes Gateway geralmente preenchem a extensão KeyUsage dos Certificados emitidos, conforme o RFC 3280: Internet X.509 Public Key Infrastructure Certificate (Certificado de Infra-estrutura de Chave Pública) e Perfil da LCR, abril de 2002. A extensão KeyUsage nos Certificados VTN X.509 Versão 3 deve ser configurada, de forma que permita configurar (“set”) ou apagar (“clear”) bits a definir e apagar bits e o campo de criticalidade, conforme apresentado na Tabela 8 abaixo, embora seja permitida a configuração para o bit nonRepudiation para Certificados com assinatura de par de chaves duplo através do Gerenciador de Chaves da PKI Gerenciada.

	CAs	Assinantes Classe 1 e Classe 2	Tokens de Administração Automatizada e Assinantes Classe 2-3	Assinatura com Par de Chaves Duplo (Administrador de Chave de PKI Gerenciada)	Ciframento de par de chaves duplo (Administrador de Chave de PKI Gerenciada)
Criticalidade	FALSE	FALSE	FALSE	FALSE	FALSE
0 digitalSignature	Clear	Set	Set	Set	Clear
1 nonRepudiation	Clear	Clear	Clear	Clear	Clear
2 keyEncipherment	Clear	Set	Set	Clear	Set
3 dataEncipherment	Clear	Clear	Clear	Clear	Clear
4 keyAgreement	Clear	Clear	Clear	Clear	Clear
5 keyCertSign	Set	Clear	Clear	Clear	Clear
6 CRLSign	Set	Clear	Clear	Clear	Clear
7 encipherOnly	Clear	Clear	Clear	Clear	Clear
8 decipherOnly	Clear	Clear	Clear	Clear	Clear

Tabela 8 - Configurações para a Extensão KeyUsage

Certificados WTLS e certos Certificados de AC não são Certificados X.509 Versão 3, logo, não contém uma extensão KeyUsage.

Note que embora o bit NonRepudiation não é definido nas extensões KeyUsage dos Certificados emitidos em dispositivos de controle de acesso para Administração Automatizada, os Assinantes de Classe 2-3 e o Certificado de assinatura para Assinantes que recebem Certificados por meio do Gerenciador de Chaves da PKI Gerenciada, a VTN suporta os serviços de não-repúdio destes certificados. O bit nonRepudiation não precisa ser definido nestes Certificados, pois a indústria de PKI ainda não atingiu um consenso quanto ao significado do bit nonRepudiation. Até que se chegue a um consenso, o bit nonRepudiation não será significativo para Parte Confiante. Além disso, os aplicativos usados mais frequentemente não reconhecem o bit nonRepudiation. Logo, definir o bit não ajudará Parte Confiante a tomar uma decisão de confiança. Conseqüentemente, esta PC exige que o bit nonRepudiation seja zerado, embora ele possa ser definido em caso de Certificados com assinatura de par de chaves duplo emitido pelo Gerenciador de Chaves da PKI Gerenciada

6.2. Proteção da Chave Privada

As chaves privadas deverão ser protegidas usando um Sistema Confiável, e portadores de chave privada deverão tomar as precauções necessárias para evitar a perda, divulgação, modificação ou uso não-autorizado de tais Chaves Privadas, conforme dita o parágrafo 6.2 da PC, o Guia de Requisitos de Segurança e Auditoria (no caso de VeriSign e Afiliadas). Este requisito aplica-se a Assinantes, Clientes de PKI Gerenciada usando o Gerenciador de Chaves de PKI Gerenciada, Clientes Gateway e Centros de Processamento, que protegem suas próprias chaves privadas e aqueles dos Centros de Atendimento ao Cliente, Clientes de PKI Gerenciada e Clientes ASB dentro de seus respectivos Subdomínios. Os Assinantes têm a opção de proteger suas chaves privadas em um cartão inteligente (smart card) ou dispositivo de controle de acesso por hardware (hardware token). As chaves privadas de Assinantes em Roaming residem em um servidor, Enterprise Roaming Server, em um formulário criptografado e chaves simétricas para criptografar e decriptografar a chave privada são divididas em duas, residindo no servidor Roaming da VeriSign e o servidor Roaming Enterprise. A VeriSign e os Clientes de PKI Gerenciada deverão proteger os segmentos de chave privada nestes servidores usando um Sistema Confiável.

6.2.1. Padrões para módulos criptográficos (Classe 1-3)

Os Centros de Processamento deverão realizar todas as operação criptográficas de AC com suas próprias chaves privadas e as chaves privadas dos Centros de Atendimento ao Cliente, Clientes de PKI Gerenciada, e Clientes ASB dentro de seus Subdomínios, em módulos criptográficos classificados com mínimo FIPS 1401 de nível 2. Os Centro de Serviços deverão realizar todas as operações criptográficas da AR em um módulo criptográfico classificado em FIPS 140-1 nível 2. A VeriSign recomenda que os Clientes de PKI Gerenciada realizem todas as operações criptográficas de Administração Automatizada em um módulo criptográfico classificado em FIPS 140-1 nível 2; os Clientes Gateway Classe 1 devem executar todas as operações criptográficas da AC em um módulo criptográfico classificado em FIPS 140-1 nível 1. Os requisitos de classificação nesta seção estão sujeitos às exigências locais aplicáveis por classificações mais altas.

6.2.2. Controle multipessoal (“n de m”) para chave privada (Classe 1-3)

O controle multipessoal deverá ser implementado para proteger os dados de ativação necessários para ativar chaves privadas de AC mantidas por Centros de Processamento, conforme o Guia de Referência da Cerimônia de Geração de Chave, e o Guia de Requisitos de Segurança e Auditoria. Centros de Processamento deverão usar o “Secret Sharing” para dividir a chave privada ou os dados de ativação necessários para a operação da chave privada em partes separadas chamadas “Secret Shares”, mantidas por indivíduos intitulados “Shareholders”. Um número limite de Secret Shares (m) de um número total de Secret Shares (n) será necessário para operar a chave privada.

Os Centros de Processamento deverão usar o Secret Sharing para proteger os dados de ativação necessários para ativar suas próprias chaves privas, e aquelas dos Centros de Serviço Cliente, Clientes de PKI Gerenciada e Clientes ASB dentro de seus respectivos Subdomínios, conforme o Guia de Referência da Cerimônia da Chave e o Guia de Requisitos de Segurança e Auditoria. Os Centros de Processamento também deverão usar o Secret Sharing para proteger os dados de ativação necessários para ativar as chaves privadas localizadas em seus respectivos locais de recuperação de desastre. Os Centros de Processamento deverão implementar o Secret Sharing.

O número limite de cotas necessárias para assinar um certificado de AC é 3. Deve-se observar que o número de cotas distribuídas para os tokens de recuperação de desastre pode ser inferiores ao número distribuído de tokens operacionais, enquanto o número limite das cotas necessárias permanece o mesmo. As "Secret Shares" são protegidas conforme o disposto no § 6.4.2 da PC.

6.2.3. Recuperação (escrow) da chave privada (Classe 1-3)

Clientes de PKI Gerenciada utilizando o serviço de Gerenciador de Chave de PKI Gerenciada (ou um serviço equivalente aprovado pela VeriSign) poderão recuperar chaves privadas de Assinantes conforme descrito na PC, §1.1.2.3.2.. As chaves privadas recuperadas deverão ser guardadas de forma codificada, usando o software do Gerenciador de Chave de PKI Gerenciada. Com exceção dos Clientes de PKI Gerenciada usando o serviço de Gerenciador de Chave de PKI Gerenciada (ou um serviço equivalente aprovado pela VeriSign), as chaves privadas das ACs ou Assinantes não devem ser recuperadas.

As chaves privadas dos Assinantes deverão ser recuperadas sob circunstâncias permitidas pelo Guia do Administrador de Serviços de Administração de Chaves de PKI Gerenciada, onde:

• Clientes de PKI Gerenciada usando o Gerenciador de Chaves de PKI Gerenciada deverão confirmar a identidade de qualquer pessoas dizendo ser o Assinante, para assegurar que uma solicitação falsa da chave privada do Assinante é, de fato, do Assinante e não um impostor.

Tais Clientes de PKI Gerenciada deverão recuperar a chave privada do Assinante sem sua solicitação somente para fins legítimos e legais, como o cumprimento de processo judicial ou administrativo, mandato de busca e não para fins ilegais, fraudulentos ou ofensivos;

Tais Clientes de PKI Gerenciada deverão contar com controles de pessoal no local, para evitar que Administradores do serviço de Gerenciamento de Chave e outras pessoas tenham acesso não-autorizado às chaves privadas.

6.2.4. Cópia de segurança da chave privada (Classe 1-3)

Os Centros de Processamento e Clientes Gateway deverão fazer as cópias de segurança de suas próprias chaves, para que possa recuperá-las em caso de desastre ou mau funcionamento do equipamento, conforme o Guia de Referência da Cerimônia da Chave e o Guia de Requisitos de Segurança e Auditoria. Centros de Processamento também deverão fazer as cópias de segurança das chave privadas de Centros de Serviços Cliente, Clientes de PKI Gerenciada e Clientes ASB, em conformidade com estes documentos. As cópias de segurança deverão ser feitas copiando as chaves privadas e inserindo-as nos módulos criptográficos de segurança, em conformidade com o § 6.2.6 desta PC.

As chaves privadas são copiadas e protegidas contra a modificação ou divulgação não-autorizadas por meios físicos e criptográficos. As cópias deverão ser protegidas com um nível físico e criptográfico de proteção igual ou superior àquele dos módulos criptográfico dentro das instalações da AC do Centro de Centro de Processamento ou Cliente Gateway, como em um local de recuperação de desastre ou outra instalação segura distinta, como o cofre de um banco.

A cópia de segurança das chaves privadas do Assinante sujeito ao serviço do Gerenciador de Chaves da PKI Gerenciada é regido pelo § 6.2.3 da PC. A VeriSign recomenda que os Clientes de PKI Gerenciada com tokens de Administração Automatizada, e Assinantes de Classe 3 que não estão sujeitos ao serviço do Gerenciador de Chaves da PKI Gerenciada que façam as cópias de suas chaves privadas, e protejam-nas contra modificação ou divulgação não autorizada, através de meios físico ou criptográficos. O banco de dados das chaves privadas criptografadas armazenado em um servidor Roaming Enterprise e os bancos de dados dos segmentos de chaves simétricas (usadas para codificar e decodificar estas chaves privadas) armazenados no Servidor Roaming VeriSign e Servidores Roaming Enterprise deverão ser copiadas para fins de recuperação de desastre e continuidade dos negócios.

6.2.5. Arquivamento da chave privada (Classe 1-3)

Sem estipulação

6.2.6. Inserção de chave privada no módulo criptográfico (Classe 1-3)

Os mecanismos de entrada de uma chave privada em um módulo criptográfico deverão impedir a perda, roubo, modificação, divulgação não autorizada ou uso não autorizado da chave privada.. As chaves privadas de ACs ou Ars mantidas em módulos criptográficos em hardware deverão ser armazenadas em formulário criptografado.

Os Centros de Processamento gerando chaves privadas de AC ou AR em um módulo criptográfico, e transferindo-as para outro módulo deverá transferir as chaves de forma segura para o segundo módulo criptográfico, na medida necessária para evitar a perda, roubo, modificação, divulgação não autorizada ou uso não autorizado das chaves privadas. Tais transferências limitam-se a realização das cópias das chaves privadas em tokens, em conformidade com o Guia de Requisitos de Segurança e Auditoria e o Guia de Referência da Cerimônia de Chave. As chaves privadas deverão ser criptografadas durante a transferência.

Os Participantes da VTN que pré-geram chaves privadas e as transfere para um dispositivo de controle de acesso por hardware (token), por exemplo,

transferindo as chaves privadas de um Assinante em um cartão inteligente. deverá transferir tais chaves de forma segura para o token, na medida necessária para evitar a perda, roubo, modificação, divulgação não autorizada ou uso não autorizado das chaves privadas

6.2.7. Método de ativação de chave privada

Todos os participantes da VTN deverão proteger os dados de ativação de suas chaves privadas contra perda, roubo, modificação, divulgação não-autorizada ou uso não-autorizado.

6.2.7.1. Chaves privadas de assinantes

Esta seção define os Padrões VTN para a proteção de dados de ativação das chaves privadas de Assinantes, embora os Assinantes tenham a opção de usar os mecanismos avançados de proteção de chave privada disponíveis atualmente, incluindo o uso de cartões inteligentes, dispositivos de acesso biométrico e outros dispositivos de controle de acesso por hardware para armazenar as chaves privadas.

6.2.7.1.1. Certificados de Classe 1

O Padrão VTN para a proteção de chave privada Classe 1 requer que o Assinante tome as medidas comercialmente disponíveis para a proteção física de sua estação de trabalho, e evitar o uso da mesma, e sua chave privada associada, sem a autorização do Assinante. Além disso, a VeriSign recomenda que os Assinantes utilizem uma senha, conforme o § 6.4.1.1 da PC, ou proteção adequada para autenticar o Assinante antes da ativação da chave privada que inclui, por exemplo, uma senha para operar a chave privada, uma senha de login no Windows, senha de protetor de telas ou senha de login de rede.

6.2.7.1.2. Certificados de Classe 2

O Padrão VTN para a proteção de chave privada Classe 2 é voltado aos Assinantes para que:

• Utilizem uma senha, conforme o § 6.4.1.1 da PC, ou proteção adequada para autenticar o Assinante antes da ativação da chave privada que inclui, por exemplo, uma senha para operar a chave privada, uma senha de login no Windows, senha de protetor de telas ou senha de login de rede.

Tomem as medidas comercialmente disponíveis para a proteção física de sua estação de trabalho, de forma a evitar o uso da mesma e de sua chave privada associada sem a autorização do Assinante.

Quando desativadas, as chaves privadas deverão ser mantidas apenas em formulário codificado.

6.2.7.1.3. Outros Certificados de Classe 3 , exceto Certificados do Administrador

O Padrão VTN para a proteção de chave privada Classe 3 (exceto Administradores) é voltado aos Assinantes para:

Uso de um cartão inteligente, dispositivo de acesso biométrico, senha em conjunto ao Serviço Roaming VeriSign, ou nível de segurança equivalente para autenticar o Assinante antes da ativação da chave;

Tomada de medidas comercialmente disponíveis para a proteção física de sua estação de trabalho, de forma a evitar o uso da mesma e de sua chave privada associada sem a autorização do Assinante.

Recomenda-se usar uma senha junto com um dispositivo de acesso biométrico, em conformidade com o § 6.4.1.1 da PC. Quando desativadas, as chaves privadas deverão ser mantidas apenas em formulário codificado.

6.2.7.2. Chaves Privadas de Administradores (Classe 3)

6.2.7.2.1. Administradores

Os Padrões VTN para a proteção de chave privada de Administrador exigem que eles:

o uso de um cartão inteligente, dispositivo de acesso biométrico, senha conforme o § 6.4.1.1 da PC, ou proteção adequada para autenticar o Administrador antes da ativação da chave privada que inclui, por exemplo, uma senha para operar a chave privada, uma senha de login no Windows, senha de protetor de telas ou senha de login de rede;

Medidas comercialmente disponíveis para a proteção física da estação de trabalho do Administrador, de forma a evitar o uso da mesma e de sua chave privada associada sem sua autorização.

VeriSign recomenda que os Administradores utilizam um cartão inteligente dispositivo de acesso biométrico ou segurança de nível equivalente, junto possivelmente o uso de uma senha, conforme disposto no § 6.4.1.2 da PC para autenticar o Administrador antes da ativação da chave privada.

Quando desativadas, as chaves privadas deverão ser mantidas apenas em formulário codificado.

6.2.7.2.2. Administradores de PKI Gerenciada usando um Módulo Criptográfico (com serviço de Administração Automatizada ou Gerenciador de Chave de PKI Gerenciada).

O Padrão VTN para a proteção de chave privadas de Administrador usando um módulo criptográfico, requer:

• uso do módulo criptográfico junto com uma senha, conforme disposto na PC, § 6.4.1.2 para autenticar o Administrador antes da ativação da chave privada.;

• medidas comercialmente disponíveis para a proteção física da estação de trabalho que aloja o leitor do módulo criptográfico, de forma a evitar o uso da estação de trabalho e da chave privada associada ao módulo criptográfico sem a autorização do Administrador.

6.2.7.3. Chaves Privadas de Clientes Gateway (Classe 1)

O Padrão VTN para a proteção de chave privada de Clientes Gateway exigem:

• uso de senha (ou medida de segurança equivalente), conforme a PC, § 6.4.1.3, para autenticar o Cliente Gateway antes da ativação da chave privada, que está associada a uma conta com privilégios de administrador no servidor Gateway;

• medidas comercialmente disponíveis para a proteção física do servidor Gateway, evitando o uso do servidor e da chave privada associada ao servidor sem a autorização do Cliente Gateway.

Uma vez ativada, ela fica ativada por um período indefinido, até sua desativação, quando o sistema de AC Gateway entra offline.

6.2.7.4. Chaves Privadas Mantidas por Centros de Processamento (Classe 1-3)

Esta seção se aplica à própria AC de um Centro de Processamento e das ACs dos Centros de Serviços Cliente, Clientes de PKI Gerenciada e Clientes ASB dentro de seu Subdomínio. Uma chave privada

online de AC deverá ser ativada por um número limite de Shareholders, conforme definido no § 6.2.2, fornecendo seus dados de ativação (armazenados em mídia protegida). Uma vez ativada, a chave privada pode ser ativada por um período indefinido, até que seja desativada quando a AC fica offline. De forma similar, um número limite de Shareholders será necessário para fornecer seus dados de ativação para ativar uma chave privada de AC offline. Uma vez ativada, a chave estará ativa por uma única vez.

6.2.8. Método de desativação de chave privada

6.2.8.1. Assinantes

6.2.8.1.1. Certificados de Classe 1

Sem estipulação

6.2.8.1.2. Certificados de Classe 2

Sem estipulação

6.2.8.1.3. Certificados de Classe 3

Assinantes têm a obrigação em proteger suas chaves privadas, conforme o § 6.2.7.1 da PC. Tais obrigações extendem-se à proteção das chaves privadas após o inicio da operação da chave privada.

6.2.8.2. Clientes Gateway (Classe 1)

Sem estipulação

6.2.8.3. Centros de Processamento (Classe 1-3)

Esta seção se aplica à própria AC de um Centro de Processamento e das ACs dos Centros de Serviços Cliente, Clientes de PKI Gerenciada e Clientes ASB dentro de seu Subdomínio. Quando uma AC é colocada offline, o pessoal do Centro de Processamento deverá remover o token contendo a chave privada da AC do leitor, para que a AC possa ser desativada. Com relação às chaves privadas da AC desativada (offline), após a conclusão da Cerimônia de Geração de Chave (veja o § 6.1.1da PC) na qual tais chaves privadas são usadas para operações com chaves privadas, o pessoal do Centro de Processamento deverá remover o token contendo tais chaves privadas da AC do leitor, para assim desativa-las. Após serem removidos dos leitores, os tokens deverão ser protegidos, conforme o Guia de Requisitos de Segurança e Auditoria.

6.2.9. Método de destruição de chave privada

As chaves privadas serão destruídas de forma que impeça sua perda, roubo, modificação, divulgação ou uso não-autorizado..

6.2.9.1. Clientes Gateway (Classe 1)

Todos Clientes Gateway deverão proteger os dados de ativação de suas chaves privadas contra perda, roubo, modificação, divulgação não-autorizada ou uso não-autorizado.

6.2.9.2. Centros de Processamento (Classe 1-3)

No encerramento das operações da AC de um Centro de Processamento, ou de um Centro de Serviços Cliente, Cliente de PKI Gerenciada ou Cliente ASB dentro de seu Subdomínio, o pessoal do Centro de Processamento deverá remover de serviço a chave privada da AC, excluindo-a usando a funcionalidade de um token contento tal chave privada da AC, de forma a impedir sua recuperação após a eliminação, ou perda, roubo modificação, divulgação não-autorizada ou uso não-autorizado de tais chaves privadas, enquanto não prejudicam as chaves privadas de outras ACs contidas no token. Este processo deve ser testemunhado, conforme disposto no Guia de Requisitos de Segurança e Auditoria e no Guia de Referência da Cerimônia de Chave.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves (Classe 1-3)

6.3.1. Arquivamento de chave pública

Os Centros de Processamento deverão arquivar suas próprias chaves públicas, bem como chaves públicas de todos os Centro de Serviços Clientes, Clientes de PKI Gerenciada e Clientes ASB em seus Subdomínios, conforme o § 4.6 da PC. Os Clientes Gateway deverão usar suas chaves públicas, conforme o parágrafo § 1.3.4 da PC.

6.3.2. Períodos de utilização de chaves públicas e privadas..... 81

O Período Operacional de Certificados deve ser definido conforme o limite de tempo estipulado na Tabela 9 abaixo. Para garantir a segurança da VTN, a VeriSign deverá encarregar novas APCs. Os períodos operacionais de certificados das novas APCs serão parcialmente definidos com base nas previsões de desenvolvimento de novas versões de navegadores.

O período de utilização dos pares de chave do Assinante corresponde ao período operacional de seus Certificados, exceto pelas chaves privadas, que continuam a ser utilizadas após o período operacional para decriptografar mensagens enviadas ao Assinante durante o período operacional. Observe que o período operacional de um certificado encerra mediante sua expiração ou revogação. Uma AC, entretanto, não poderá emitir Certificados se seus períodos operacionais extendem-se além do período de uso do par de chaves da AC. Assim, o período de utilização do par de chaves da AC é necessariamente inferior ao período operacional do Certificado da AC. De maneira específica, o período de utilização corresponde ao período operacional dos Certificados da AC menos o período operacional dos certificados emitidos pela AC. Findo o período de utilização de um par de chaves de Assinante ou AC, estes devem cessar imediatamente o uso do par de chaves, exceto quando uma AC precisa assinar informações de revogação até o final do período operacional do último certificado emitido.

Certificado emitido por:	Classe 1	Classe 2	Classe 3
APC auto-assinada	Até 30 anos	Até 30 anos	Até 30 anos
APC para AC	Até 10 anos	Até 10 anos	Até 10 anos
AC para AC subordinada	Até 5 anos	Até 5 anos s	Até 5 anos
AC para Assinante	Até 2 anos	Normalmente, em até 2 anos, porém, sob as condições descritas abaixo, até 5 ano	Normalmente, em até 2 anos, porém, sob as condições descritas abaixo, até 5 anos
Ac para Certificado corporativo de Administração Organizacional do usuário final	N/D	N/D	Até 5 anos

Tabela 9 - Períodos Operacionais de Certificado

Exceto pelo indicado abaixo, os participantes da VTN deverão cessar o uso dos pares de chaves após expirar o período de utilização.

Certificados emitidos pelas ACs para Assinantes podem ter períodos operacionais mais extensos que dois anos, até cinco anos, se as seguintes condições forem atendidas:

• Os certificados são Certificados individuais,

• Os pares de chave o Assinante residem em um dispositivo de controle de acesso por hardware (token), como um cartão inteligente,

• Anualmente, os Assinantes passam pelo pro0cesso de re-autenticação, conforme o § 3.1.9 da PC,

• Os Assinantes deverão fornecer anualmente provas de posse das chaves privadas correspondentes às chaves públicas contidas no Certificado

• Se um assinante for incapaz de completar o procedimento de reautenticação, a AC deverá revogar imediatamente o Certificado do Assinante

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de Ativação

Os participantes da VTN que geram e instalam dados de ativação para suas chaves privadas deverão usar métodos que protegem os dados de ativação na medida necessária para evitar a perda, roubo, modificação, divulgação e uso não-autorizado de tais chaves públicas..

6.4.1.1. Assinantes (Classe 1-3)

Considerando que senhas são usadas como dados de ativação (veja PC § 6.2.7.1), os Assinantes deverão gerar senhas que não sejam facilmente desvendadas. A VeriSign e Afiliadas deverão informar os Assinantes seu Subdomínio quanto aos métodos para a escolha de senhas seguras. Os Assinantes de Classe 3 não precisarão gerar os dados de ativação, por exemplo, caso utilizem dispositivos de acesso biométrico.

6.4.1.2. Administradores (Classe 3)

Os dados de ativação usados pelos Administradores deverão atender aos requisitos da PC § 6.4.1.1.

6.4.1.3. Clientes Gateway (Classe 1)

Os Clientes Gateway deverão gerar seus dados de ativação, conforme o parágrafo § 6.2.7.3 da PC. Os Clientes Gateway deverão usar senhas como dados de ativação que não sejam facilmente desvendadas ou exploradas por ataques de dicionários.

6.4.1.4. Centros de Processamento (Classe 1-3)

Os Centros de Processamento deverão gerar os dados de ativação das chaves privadas de suas ACs, bem como chaves privadas de Centros de Serviço Cliente, Clientes de PKI Gerenciada e Clientes ASB dentro de seus respectivos Subdomínios, conforme o Guia de Referência da Cerimônia da Chave e o Guia de Requisitos de Segurança e Auditoria.

6.4.2. Proteção dos dados de ativação

Os participantes da VTN deverão proteger os dados de ativação de suas chaves privadas usando métodos para a proteção contra perda, roubo, modificação, divulgação ou uso não-autorizado de tais chaves privadas.

6.4.2.1. Assinantes (Classe 1-3) e Clientes Gateway (Classe 1)

Os Assinantes e Clientes Gateway deverão proteger os dados de ativação de suas chaves privadas usando métodos para a proteção contra perda, roubo, modificação, divulgação ou uso não-autorizado de tais chaves privadas.

6.4.2.2. Centros de Processamento (Classe 1-3)

Centros de Processamento utilizarão Secret Sharing em conformidade com a PC, § 6.2.2 e o Guia de Requisitos de Segurança e Auditoria. Os Centros de Processamento deverão fornecer procedimentos e meios para que os Shareholders possam tomar as precauções necessárias para evitar a perda, roubo, modificação, divulgação ou uso não-autorizado das Secret Shares que possuem. Os Shareholders não deverão:

. • Copiar, divulgar ou disponibilizar o Secret Share a Parte Confiante, ou praticar o uso não autorizado do mesmo; ou

. • revelar o estado de Shareholder de qualquer pessoa, inclusive o seu a Parte Confiante. As Secret Shares e informações divulgadas ao Shareholder com relação a suas responsabilidades como Shareholder constituirá em Informações Sigilosas/Confidenciais, conforme a PC § 2.8.1.

Adicionalmente, os Centros de Processamento deverão incluir em seus planos de recuperação de desastre provisões para que os Shareholders disponibilizem suas Secret Shares em um local de recuperação de desastre após ocorrido o evento..

Cada Centro de Processamento manter uma pista de auditoria de todas as Secret Shares; os Shareholders deverão participar da manutenção de uma trilha de auditoria.

6.4.3. Outros aspectos dos dados de ativação (Classe 1-3)

6.4.3.1. Transmissão de dados de ativação (Classe 1-3)

No que se refere aos dados de ativação de chaves privadas, os Participantes da VTN deverão proteger a transmissão de tais dados de ativação de suas chaves privadas, usando métodos que protejam contra a perda, roubo, modificação, divulgação ou uso não-autorizado de tais chaves privadas. Por exemplo, os Centros de Processamento deverão assegurar a transferência das Secret Shares, realizada conforme a PC § 6.4.2. Ademais, no que se refere ao uso de nomes e senhas do Windows ou de usuário de rede como dados de ativação para Assinantes ou Cliente Gateway, as senhas transferidas pela rede deverão ser protegidas contra o acesso de usuários não-autorizados.

6.4.3.2. Destruição de dados de ativação (Classe 1-3)

Os dados de ativação das chaves privadas de AC deverão ser desativados usando métodos para a proteção contra perda, roubo, modificação, divulgação ou uso não-autorizado de tais dados de ativação. Findo os períodos de retenção determinado na CP § 4.6, os Centros de Processamento deverão descartar os dados, através da sobregravação ou destruição física.

6.5. Controles de segurança computacional

As funções de AC e AR deverão ocorrer em Sistemas Confiáveis, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas).

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. Controles para Centros de Processamento (Classe 1-3)

Os Centros de Processamento deverão assegurar que os sistemas mantendo o software da AC e arquivos de dados são Sistemas Confiáveis, protegidos contra o acesso não-autorizado, que pode ser demonstrado pela conformidade com os critérios de auditoria aplicáveis na PC § 2.7.4. Além disso, os Centros de Processamento deverão limitar o acesso aos servidores de produção àquelas pessoas com um motivo comercial válido para o acesso. Usuários em geral não devem ter contas em servidores de produção.

Os Centros de Processamento deverão contar com redes de produção logicamente separadas de outros componentes. Esta separação impede o acesso à rede, exceto através dos processos de aplicativos definidos. Os Centros de Processamento deverão usar firewalls para proteger a rede contra intrusões internas e externas, e limitar a natureza das atividades de rede que podem acessar os sistemas de produção. Os Centros de Processamento deverão impor o uso de senha com um comprimento mínimo de caracteres, e um combinação de caracteres alfanuméricos e especiais; tal senha deverá ser trocada periodicamente e sempre que se fizer necessário. O acesso direito ao banco de dados do Centro de Processamento mantenedor do repositório limitar-se-á às Pessoas Qualificadas no grupo operacional do Centro de Processamento, com motivos comerciais válidos para tal acesso.

6.5.1.2. Controles para Clientes Gateway (Classe 1)

Os servidores Gateway deverão incluir as seguintes funcionalidades:

- controle de acesso aos serviços de AC,
- identificação e autenticação para a inicialização de serviços de AC,
- reutilização objetiva da memória volátil de acesso da AC,

• uso de criptografia para comunicação de sessão e segurança de banco de dados,

• arquivamento do histórico e dados de auditoria da AC e Assinantes,

• auditoria de eventos relacionados à segurança,

• auto-teste para serviços de AC relacionados à segurança

• caminho confiável para identificação de perfis e PKI e identidades associadas.

6.5.1.3 Controles para Centros de Serviço e Clientes de PKIs Gerenciadas (Classe 1-3)

Os Centros de Processamento e Clientes de PKI Gerenciada deverão assegurar que os sistemas mantendo o software da AR e arquivos de dados são Sistemas Confiáveis, protegidos contra o acesso não-autorizado, que pode ser demonstrado pela conformidade com os critérios de auditoria aplicáveis na PC § 2.7.4.

Os Centros de Serviços e Clientes de PKI Gerenciada deverão separar logicamente o acesso a estes sistemas e informações a partir de outros componentes. Esta separação impede o acesso à rede, exceto através dos processos definidos. Os Centros de Serviço e Clientes de PKI Gerenciada deverão usar firewalls para proteger a rede contra invasões internas e externas e limitar a natureza das atividades de rede que podem acessar tais sistemas e informações. Os Centros de Serviço e Clientes de PKI Gerenciada deverão impor o uso de senha com um comprimento mínimo de caracteres, e um combinação de caracteres alfanuméricos e especiais; tal senha deverá ser trocada periodicamente e sempre que se fizer necessário. O acesso direito ao banco de dados da AR do Centro de Serviços ou do Cliente de PKI Gerenciada mantenedor das informações do Assinante limitar-se-á às Pessoas Qualificadas no grupo operacional do Centro de Serviço ou Cliente de PKI Gerenciada, com motivos comerciais válidos para tal acesso.

6.5.2. Classificação de segurança computacional (Classe 1-3)

As áreas críticas e específicas quanto à segurança de funcionalidades das ACs e ARs do software fornecido pela VeriSign deverão atender aos requisitos de segurança EAL 3 (Common Criteria for Information Technology Security Evaluation, v 2.1, agosto 1999).

6.6. Controles Técnicos do Ciclo de Vida (Classe 1-3)

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. Software Usado por Cliente Gateway

Sem estipulação

6.6.1.2. Software Usado por Clientes de PKI Gerenciada, Centros de Serviços e Centros de Processamento

A VeriSign oferece o software para as funções de AC e AR aos Centros de Processamento, Centros de Serviços e Clientes de PKI Gerenciada. Tal software, utilizado para gerenciar Certificados de Classe 2 ou 3, deverá ser desenvolvido dentro de ambientes de desenvolvimento de sistemas que atendam aos requisitos de garantia de desenvolvimento da VeriSign. VeriSign deverá usar um processo de design e desenvolvimento que reforça a garantia da qualidade e exatidão do processo.

O software fornecido pela VeriSign aos Clientes de PKI Gerenciada, Centros de Serviços e Centros de Processamento, quando na sua primeira inicialização, deverá fornecer um método para que a entidade verifique se o software no sistema: • foi originado pela VeriSign,

• não foi modificante antes da instalação,

• possui a versão correta para uso.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. Software Usado por Clientes Gateway Classe 1

Sem estipulação

6.6.2.2. Software Usado por Clientes de PKI Gerenciada, Centros de Serviço e Centros de Processamento

O software para funções de AC e AR criado para gerenciar Certificados de Classe 2 ou 3 estará sujeito a verificações de integridade. A VeriSign deverá fornecer um "hash" de todos os pacotes de software ou atualizações que sejam fornecidas aos Clientes de PKI Gerenciada, Centros de Serviços e Centros de Processamento. Este hash pode ser usado para verificar manualmente a integridade de tal software. Os Centros de Processamento deverão também contar com mecanismos e/ou políticas para o controle e monitoração da configuração de seus sistemas de AC. Na instalação, e pelo menos uma vez ao dia, os Centros de Processamento deverão validar a integridade do sistema da AC.

6.6.3. Classificações de Segurança de Ciclo de Vida

Sem estipulação

6.7. Controles de Segurança de Rede (Classe 1-3)

A VeriSign, Afiliadas, Clientes de PKI Gerenciada e Clientes Gateway deverão realizar as funções de AC e AR usando redes seguras, conforme o Guia de Requisitos de Segurança e Auditoria (no caso da VeriSign e Afiliadas) para evitar o acesso não autorizado, violação e ataques de DoS (negação de serviço). A VeriSign, Afiliadas e Clientes deverão proteger a comunicação de informações críticas, usando a tecnologia de criptografia de ponto a ponto para confidencialidade e assinaturas digitais para não-repúdio e autenticação.

6.8. Controles de Engenharia do Módulo Criptográfico (Classe 1-3)

Veja o parágrafo.6.2.1 da PC.

7. PERFIS DE CERTIFICADO E LCR (CLASSE 1-3)

7.1. Perfil do Certificado

Os Certificados VTN deverão possuir um perfil e conter os campos especificados na PC § 7.1. Exceto pelos Certificados WTLS, os Certificados VTN deverão atender à: (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate e CRL Profile, April 2002 ("RFC 3280").

Como condição básica, os Certificados VTN X.509 deverão contém os campos básico e valores prescritos ou valores limite indicados nas Tabela 10 abaixo:

Campo	Valor ou limite de valor
Serial Number	Valor exclusivo por DN Emissor
Signature	O OID (Object identifier) do algoritmo usado para assinar o certificado (Veja a PC § 7.1.3)
Algorithm	
Issuer DN	Consulte o parágrafo 7.1.4 da PC
Valid From	Base de Tempo Universal Coordenado (UCT). Sincronizado com o Master Clock of U.S. Naval
	Observatory. Codificado conforme o RFC 3280.
Valid To	Base de Tempo Universal Coordenado (UCT). Sincronizado com o Master Clock of U.S. Naval
	Observatory. Codificado conforme o RFC 3280.
Subject DN	Consulte o parágrafo 7.1.4 da PC
Subject Public	Codificado conforme o RFC 3280.
Key	
Signature	Gerado e codificado conforme o RFC 3280.

Tabela 10 - Campos Básicos de Perfil de Certificado

Os Certificados WTLS atenderam à versão mais atual do protocolo WAP (Wireless Application Protocol).

Os Centros de Processamento e Clientes Gateway deverão emitir Certificados conforme o perfil determinado nesta PC § 7.1. Além disso, os Centros de Processamento deverão emitir Certificados que possuam tal perfil para suas próprias ACs e Ars do Centros de Serviços Cliente, Clientes de PKI Gerenciada e Clientes ASB dentro de seus Subdomínios.

7.1.1. Número(s) de versão

Exceto pelos Certificados WTLS Certificados, que atenderam à versão mais atual do protocolo WAP, todos os Certificados VTN deverão constituir em Certificados X.509, embora certos Certificados Raiz possam ser Certificados X.509 versão 1 para suportar sistemas com tecnologias antigas.. Os Centros de Processamento deverão emitir Certificados de AC X.509 Versão 1 ou Versão 3. Adicionalmente, os Centros de Processamento deverão emitir Certificados de Assinante X.509 Versão 3 Os Centros de Processamento deverão emitir Certificados WTLS.

7.1.2. Extensões de Certificado

Os Centros de Processamento e Clientes Gateway deverão preencher os Certificados VTN com as extensões exigidas pela PC, §§ 7.1.2.1-7.1.2.8. Extensões privadas são permitidas, porém o uso de extensão(ões) privada(s) não é garantido por esta PC, e a CPS aplicável, a menos que especificamente incluído por referência.

7.1.2.1. Utilização da chave

Os Centros de Processamento e Clientes Gateway deverão preencher a extensão KeyUsage de Certificados de AC X.509 Versão 3, Certificados de Administração Automatizada e de Assinantes, definindo ou zerando o(s) bit(s) e o campo de criticalidade, conforme a PC § 6.1.9. O campo de criticalidade desta extensão normalmente é definido como FALSE (falso).

7.1.2.2. Extensão das políticas de certificado

Os Centros de Processamento e Clientes Gateway deverão preencher a extensão CertificatePolicies de Certificados de AC X.509 Versão 3, Certificados de Administração Automatizada e de Assinantes com o OID (object identifier) desta PC, conforme o parágrafo 7.1.6 e com os qualificadores de política definidos na PC, parágrafo 7.1.8. O campo de criticalidade desta extensão deve ser definido como FALSE (falso).

7.1.2.3. Nomes alternativos

Centros de Processamento e Clientes Gateway deverão preencher a extensão subjectAltName de Certificados de AC X.509 Versão 3, Certificados de Administração Automatizada e de Assinantes, conforme a RFC 3280. O campo de criticalidade desta extensão deve ser definido como FALSE (falso).

7.1.2.4. Restrições básicas

Os Centros de Processamento deverão preencher os Certificados de AC X.509 Versão 3 com uma extensão BasicConstraints e o campo da AC definido como TRUE (verdadeiro). Os Centros de Processamento e Clientes Gateway deverão preencher Certificados de Assinantes com uma extensão BasicConstraints, porém deverá atribuir a esta extensão um valor de seqüência vazia. O campo de criticalidade desta extensão deve ser definido como TRUE (verdadeiro) para os Certificados, e para os demais casos, como FALSE (falso).

Os Certificados de AC X.509 Versão 3 emitidos a APCs, Centros de Processamento e Centros de Serviços Cliente deverão ter um campo “pathLenConstraint” da extensão BasicConstraints definido conforme o número máximo de certificados de AC em um caminho de certificação. Certificados de AC emitidos para AC online de Clientes de PKI Gerenciada e Clientes Gateway emitindo Certificados de Assinante deverão ter um campo “pathLenConstraint” definido em “0”, indicado que somente um Certificado de Assinante pode seguir o caminho de certificação.

7.1.2.5. Utilização de chave prolongada

Os Centros de Processamento e Clientes Gateway deverão preencher os Certificados de Entidade Final VTN X.509 Versão 3 com uma extensão ExtendedKeyUsage configurada para incluir os OIDs

principais, mostrados na Tabela 11 abaixo. Exceto onde especificamente indicado abaixo, esta extensão normalmente não é incluída em certificados de entidade final. Por padrão , a extensão ExtendedKeyUsage é definida como uma extensão não-crítica. Os Certificados de AC VTN não incluem uma extensão ExtendedKeyUsage.

	Certificados de AR emitidos por tokens de Administração Automatizada, e Certificados ASB Corporativos Classe 3 Certificados Cliente Classe 1-3,	Certificados Corporativos de Classe 3 Assinatura de Objeto	Certificados Corporativos (por exemplo, IDs de Servidor Seguro, IDs de Servidor Global) Outro Classe 3
ServerAuth (1.3.6.1.5.5.7.3.1)	Não incluído	Não incluído	Incluído
ClientAuth (1.3.6.1.5.5.7.3.1)	Incluído	Não incluído	Incluído
CodeSigning (1.3.6.1.5.5.7.3.3)	Não incluído	Incluído	Não incluído
EmailProtection (1.3.6.1.5.5.7.3.1)	Incluído	Não incluído	Não incluído
TimeStamping (1.3.6.1.5.5.7.3.1)	Não incluído	Não incluído	Não incluído

Tabela 11 - Tipos de Finalidade de Chave incluídos na extensão ExtendedKeyUsage.

7.1.2.6. Pontos de distribuição de LCR

Os Centros de Processamento e Clientes Gateway deverão preencher Certificados VTN X.509 Versão 3 com uma extensão cRLDistributionPoints contendo a URL do local onde a terceira parte pode obter uma LCR e verificar o status do Certificado. O campo de criticalidade desta extensão deve ser definido como FALSE (falso).

7.1.2.7. Identificador de chave da autoridade

Os Centros de Processamento e Clientes Gateway, em geral, preenchem os Certificados VTN X.509 Versão 3 com uma extensão authorityKeyIdentifier e um método para gerar o keyIdentifier baseado na chave pública da AC que emite o Certificado deverá ser calculado conforme um dos métodos descritos na RFC 3280. O campo de criticalidade desta extensão deve ser definido como FALSE (falso).

7.1.2.7. Identificador de chave do titular do certificado

Se os Centros de Processamento ou Cliente Gateway preenchem os Certificados VTN X.509 Versão 3 com uma extensão subjectKeyIdentifier, o método para a geração do identificador de chave baseado na chave pública do Titular do Certificado deverá ser calculado conforme um dos métodos descritos na RFC 3280. O campo de criticalidade desta extensão, se houver, deverá ser definido como FALSE (falso).

7.1.3. Identificadores de algoritmo

Os Centros de Processamento e Clientes Gateway deverão assinar Certificados VTN usando um dos seguintes algoritmos.

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

md2WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}

Assinaturas de certificado produzidas usando estes algoritmos deverão atender ao RFC 3279. O uso do sha1WithRSAEncryption é preferível ao uso do md5WithRSAEncryption. O uso do md5WithRSAEncryption será

o preferido em vez do md2WithRSAEncryption (que era usado para assinar Certificados de AC e Assinantes legados (antigos))

7.1.4. Formatos de nome

Os Centros de Processamento e Clientes Gateway deverão preencher os Certificados VTN com o nome exigido conforme a PC § 3.1.1. Além disso, os Centros de Processamento e Clientes Gateway deverão incluir nos Certificados de Assinante um campo adicional de unidade organizacional ("Organizational Unit") que contém uma notificação, declarando os termos de uso do Certificado estão definidos em uma URL, e a URL deverá ser indicada no Contrato de Parte Confiante aplicável. As exceções aos requisitos supracitados limitar-se-ão somente quando houver restrições de espaço, formato ou interoperabilidade nos Certificados, impossibilitando o uso da Unidade Organizacional junto com a aplicação esperada do Certificado.

7.1.5. Restrições de nomes

Sem estipulação

7.1.6. OID (Object Identifier) de Política de Certificado

O identificador de uma política de Certificado correspondente a cada Classe de Certificado é definido na PC § 1.2. Os Centros de Processamento e Clientes Gateway deverão preencher a extensão CertificatePolicies em cada Certificado VTN X.509 Versão com o identificador correspondente à classe de Certificado definida na PC, § 1.2.

7.1.7. Uso da extensão "Policy Constraints"

Sem estipulação

7.1.8. Sintaxe e semântica dos qualificadores de política

Os Centros de Processamento e Clientes Gateway deverão preencher todos os Certificados VTN X.509 Versão 3 Certificados VTN com um qualificador de política nas extensões CertificatePolicies.. Tais Certificados deverão conter qualificador indicador CPS preenchido com uma URL, indicando o Contrato de Parte Confiante aplicável.

7.1.9. Semântica de processamento para extensões críticas de política de certificado

Sem estipulação

7.2. Perfil de LCR

Os Centros de Processamento e Clientes Gateway deverão emitir as LCRs em conformidade com o RFC 3280 e OCSP responders que atendam ao RFC2560.

7.2.1. Número(s) de versão

Sem estipulação

7.2.2. Extensões e entradas de LCR

Sem estipulação

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos para Mudança de Especificação

As alterações desta PC deverão ser feitas pela Autoridade de Gerenciamento de Política da Rede de Confiança VeriSign. As alterações deverão ser feitas na forma de um documento, contendo um formulário de aditamento da PC ou uma atualização. As versões alteradas ou atualizações deverão possuir um link de acesso às seções Practices Updates and Notices do Repositório VeriSign, localizado em: https://www.verisign.com/repository/updates. Atualizações substituem quaisquer dispositivos designados ou conflitantes de uma versão da PC. A PMA deverá determina se as alterações na PC requerem uma alteração nos identificadores OID das políticas de Certificado correspondentes a cada Classe de Certificado.

8.1.1. Itens passíveis de mudança sem aviso prévio

A VeriSign e a PMA se reservam o direito de alterar a PC sem qualquer aviso prévio, para alterações que não sejam materiais, incluindo porém sem limitar-se a erros tipográficos, alterações nas URLs e alterações nas informações de contato. Fica a critério da PMA a decisão em designar alterações como sendo materiais ou não-materiais.

8.1.2. Itens passíveis de mudança com aviso prévio

A PMA deverá fazer as alterações materiais na CP conforme dita a Seção 8.1.2.

8.1.2.1. Lista de itens

Alterações materiais são aquelas que, pela PMA e conforme a PC § 8.1.1, são consideradas materiais.

8.1.2.2. Mecanismo de notificação

A PMA deverá notificar as Afiliadas quanto às alterações materiais na PC proposta pela PMA. A notificação deverá conter o texto das alterações propostas e o período de comentários da Seção 8.1.2.3. As alterações propostas à PC deverão constar na seção Practices Updates and Notices do Repositório VeriSign, localizado em: https://www.verisign.com/repository/updates. As Afiliadas deverão publicar ou fornecer um link para as alterações propostas em seus próprios repositórios na Web, dentro de um período razoável, após receber a notificação de tais alterações.

A PMA solicita alterações propostas para PC de outros Participantes da VTN. Se a PMA considera uma alteração desejável, e propõe sua implementação, esta PMA deverá notificar a alteração conforme explicado nesta seção.

Se a PMA acredita que as alterações materiais na PC imediatamente necessárias, para parar ou evitar uma brecha de segurança da VTN ou pare da rede, a VeriSign e a PMA estarão autorizadas a fazer tais alterações, publicando-as no Repositório da VeriSign. Tais alterações deverão ser feitas imediatamente após sua publicação. Dentro de um período razoável após a publicação, a VeriSign deverá notificar as Afiliadas de tais alterações.

8.1.2.3. Período de comentário

Exceto pelo disposto na PC § 8.1.2.2, o período de comentário para qualquer alteração material na PC deve ser e 15 (quinze) dias a partir da data de publicação das alterações no repositório da VeriSign. Qualquer participante da VTN está autorizado a fazer comentários à PMA, até o final do período de comentários.

8.1.2.4. Mecanismo para processar comentários

A PMA deverá considerar quaisquer comentários feitos às alterações propostas. A PMA deverá (a) permitir a efetivação da alteração proposta sem alteração posterior, (b) alterar as alterações propostas e republicá-las como uma nova alteração, conforme a PC § 8.1.2.2, ou (c) retirar as alterações propostas.. A PMA está autorizada a retirar alterações propostas, notificando as Afiliadas e notificando também a seção Practices Updates and Notices no repositório VeriSign. A menos que as alterações propostas sejam alteradas ou removidas, elas tornar-se-ão efetivas a partir da expiração do período de comentário determinado na Seção 8.1.2.3.

8.1.3. Alterações que exigem mudanças adicionais nos OIDs da política de certificado ou Indicador da PC

Se a PMA difere quanto à necessidade de uma alteração no OID correspondente a uma política de Certificado, a alteração deverá conter novos OIDs para estas políticas. OID (Object Identifier) de Política de Certificado

8.2. Políticas de Publicação e Notificação

8.2.1. Itens não publicados na PC

Documentos e informações de segurança contidos na PC, considerados confidenciais pela VeriSign e Afiliadas não serão divulgados ao público em geral. Os documentos de segurança confidenciais incluem os documentos identificados na PC § 1.1(a) Tabela 1 como documentos que não são disponibilizados ao público.

8.2.2. Distribuição da PC

Esta PC está publicada em formato eletrônico no Repositório da VeriSign em https://www.verisign.com/CP. Esta PC está disponível em formato impresso na PMA, mediante solicitação enviada para: VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 EUA Attn: Practices Development.

8.3. Procedimentos de Aprovação da DPC

As Afiliadas da VTN deverão possuir suas próprias DPCs. Uma PC de uma Afiliada regerá o Subdomínio desta Afiliada dentro da VTN. As Entidades que desejam se tornar Afiliadas assinam um contrato com a VeriSign e enviam uma proposta de DPC ao Departamento de Práticas e Assuntos Externos da VeriSign. O Departamento de Práticas e Assuntos Externos deverá aprovar ou rejeitar as DPCs, a seu exclusivo critério. Veja a PC § 1.4.2 para informações de contato com o Departamento de Práticas e Assuntos Externos.

Acrônimos e Definições Tabela de Acrônimos

Acrônimo	Termo
ANSI	American National Standards Institute.
ASB	Authentication Service Bureau
B2B	Business-to-business (interempresarial)
BIS	United States Bureau of Industry and Science of the United States Department of Commerce.
BXA	United States Bureau of Export Administration of the United States Department of Commerce (which has been replaced by the BIS).
AC	Autoridade Certificadora.
PC	Política de Certificado.
DPC	Declaração de Práticas de Certificação.
LCR	Lista de Certificados Revogados
EAL	Nível de garantia da avaliação (conforme os Critérios Comuns).
EDI	Electronic Data Interchange (Troca eletrônica de dados)
EDIFACT	EDI para administração, comércio e transporte (padrões estabelecidos pela UNECE - Comissão Econômica para a Europa das Nações Unidas).
FIPS	United States Federal Information Processing Standards.
ICC	Câmara de Comércio Internacional.
KRB	Key Recovery Block - bloco para recuperação de chave.
LSVA	Logical security vulnerability assessment (Avaliação lógica de vulnerabilidade)
OCSP	Protocolo de Status de Certificado On-line.
OFX	Open Financial Exchange.
PCA (ACP)	Autoridade Certificadora de Políticas
PIN	PIN - número pessoal de identificação.
PKCS	Padrão de Criptografia de Chave Pública
PKI	(ICP) Infra-estrutura de Chave Pública.
PMA	Autoridade de Gerenciamento de Políticas.
AR	Autoridade de Registro.
RFC	Solicitação para comentário.
SAS	Declaração de Padrões de Auditoria (promulgado pelo American Institute of Certified Public Accountants).
S/MIME	Extensões seguras de correio eletrônico para múltiplas finalidades.
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network - Rede de Confiança da VeriSign.
WAP	Protocolo WAP - Wireless Application Protocol.
WTLS	Wireless Transport Layer Security.

Termo	Definição
Administrador	Uma Pessoa Qualificada dentro da organização de um Centro de Processamento, Centro de Serviços, Cliente de PKI Gerenciada, ou Cliente Gateway que executa a validação e outras funções de AC e AR.
Certificado do Administrador	Certificado emitido a um administrador, deve ser usado apenas para a execução das funções de AC ou AR.
Afiliada	Parte Confiante, líderes no ramo de tecnologia, telecomunicações ou serviços financeiros, que fizeram um contrato com a VeriSign para se tornar um canal de distribuição e serviços na VTN, em um território
Guia do Programa de Auditoria da Afiliada	Documento específico da VeriSign contendo os requisitos para Auditorias de Conformidade de Afiliadas, incluindo as Metas de Controle de Administração de Certificado contra as quais as Afiliadas são auditadas.
Guia de Requisitos de Práticas Legais da Afiliada	Documento da VeriSign contendo os requisitos DPCs de Afiliadas, bem como contratos, procedimentos de validação e políticas de privacidade e outros requisitos que as Afiliadas devem preencher.
Indivíduo Afiliado	Pessoa física relacionada a um Cliente de PKI Gerenciada,
	Cliente de PKI Gerenciada Lite ou Cliente Gateway (i) como um como um oficial, diretor, funcionário, contratado, estagiário ou qualquer outra pessoa dentro da entidade, (ii) como membro de uma comunidade de interesses registrada da VeriSign, ou (iii) uma pessoa que mantém uma relação com a entidade, onde a entidade possui negócios ou outros registros que forneçam provas adequadas da identidade da pessoa.
Cliente ASB	Uma entidade que contrata a VeriSign ou uma Afiliada para obter Serviços do ASB - Authentication Service Bureau (centro de serviços de autenticação) Um Cliente ASB Customer é uma Ac, e nomeado como tal nos Certificados emitidos por sua AC, porém terceiriza todas as funções de AC a um Provedor ASB.
Provedor ASB	Uma entidade (seja a VeriSign ou Afiliada) que oferece serviços ASB (Authentication Service Bureau) para clientes ASB. Um Provedor ASB age como um provedor terceirizador de funções secundárias para o Cliente ASB e como uma AR.
Authentication Service Bureau	Um serviço dentro da VTN, onde a VeriSign ou uma Afiliada realizam a maioria das funções secundárias de AC e funções primárias de AR em nome de uma organização
Módulo de Software	Um procedimento onde as Solicitações de Certificado são aprovadas automaticamente quando as informações de inscrição coincidem com asinformações contidas em um banco de dados.
Módulo de Software para Administração Automatizada	Software fornecido pela VeriSign que realiza a Administração Automatizada.
Certificado	Uma mensagem que, no mínimo, declara um nome ou identifica a AC, identifica o Assinante, contém a chave pública do assinante, identifica oPeríodo Operacional do Certificado, contém um número de série de certificado e é digitalmente assinado pela AC.
Solicitante de Certificado	Um indivíduo ou organização que solicita a emissão de um Certificado por uma AC.
Solicitação de Certificado	Uma solicitação feita pelo Solicitante ao Certificado (ou agente autorizado do Solicitante) para uma AC, requisitando a emissão de um Certificado.
Cadeia de certificado	Uma lista ordenada de Certificados contendo o Certificado do Assinante e Certificados da AC, que terminam em um Certificado raiz.
Objetivos de Controle de Gerenciamento	Os critérios aos quais uma entidade deve atender para satisfazer uma Auditoria de Conformidade.
Políticas de Certificados (PC)	Este documento, intitulado “Políticas de Certificado da Rede de Confiança da VeriSign” é a principal declaração de política que rege a VTN.
Lista de Certificados Revogados (LCR)	Uma lista emitida periodicamente, digitalmente assinada por uma AC, contendo os Certificados identificados como revogados antes da data de vencimento, conforme a PC § 3.4. Em geral, a lista o nome do emissor da LCR, a data de emissão, data prevista para a próxima edição da LCR, os números de série dos. e os horários específicos e motivos para a revogação.

Solicitação de Assinatura de Certificado	Uma mensagem informando que uma solicitação para Certificado foi emitida.
Autoridade Certificadora (AC)	Uma entidade autorizada a emitir, gerenciar, revogar e renovar Certificados na VTN.
Declaração de Práticas de Certificação. (DPC)	Uma declaração das práticas que a VeriSign ou uma Afiliada utilizam na provação ou rejeição de Solicitações de Certificado e emitindo, gerenciando, revogando Certificados para serem utilizados por seus Clientes de PKI Gerenciada e Clientes Gateway.
Frase de Identificação	Uma frase secreta escolhida pelo Solicitante durante a inscrição para o Certificado. Quando um certificado é emitido, o Solicitante se torna um Assinante, e a AC ou AR pode usar a Frase de Identificação para autenticar o Assinante, quanto este tenta revogar ou renovar o Certificado de Assinante.
Classe	Um nível especificado de garantias definidos na PC. Veja a PC § 1.1.1.
Certificados ASB Individual Classe 2	Um Certificado individual de Classe 2 emitido por um Provedor ASB em nome de uma AC de um Cliente ASB.
Certificados ASB Corporativo Classe 3	Um Certificado corporativo de Classe 3 emitido por um Provedor ASB em nome de uma AC de um Cliente ASB.
Client OnSite Lite Customer	Veja Cliente de PKI Gerenciada Lite.
Centro de Serviços Cliente	Um Centro de Serviços que é uma Afiliada fornecendo Certificados cliente para as linhas de negócio Consumer e Enterprise.
Auditoria de Conformidade	Auditoria periódica à qual são submetidos o Centro de Processamento, Centro de Serviços, Cliente de PKI Gerenciada, ou Cliente Gateway, para determinar sua conformidade com os Padrões VTN aplicáveis
Comprometimento	Uma violação (ou suspeita de violação) de uma política de segurança, onde a divulgação não-autorizada, perda de controle sobre informações críticas possa ter ocorrido. Com relação às chaves privadas, um Comprometimento representa uma perda roubo, modificação, divulgação ou uso não-autorizado da chave privada
Informações Sigilosas/ Confidenciais	Informação que deve ser mantida em sigilo, conforme a PC § 2.8.1.
Consumidor como em Centro de Atendimento ao Consumidor	Uma linha de negócio em que uma Afiliada atua para fornecer Certificados de Varejo cliente a Solicitantes de Certificado.
Contrato de Utilização de LCR	Um contrato que define os termos e condições sob as quais uma LCR ou informações podem ser utilizadas.
Cliente	Organização que é um Cliente de PKI Gerenciada, Cliente Gateway ou Cliente ASB
Recibo Digital	Um objeto de dados criado, referente ao Serviço de Notarização Digital VeriSign e digitalmente assinado pela Autoridade de datação, que inclui o hash de um documento ou conjunto de dados e um selo cronológico mostrando que o documento ou dado existiram em certo momento.
Electronic Data Interchange EDI - (Troca eletrônica de dados)	As trocas entre computadores de transações comerciais, tais como ordens de compra, faturas e notificações de pagamento, conforme os padrões aplicáveis
Electronic Data Interchange Interchange Certificate (Certificado EDI)	Um Certificado corporativo Classe 3 que permite a assinatura digital em mensagem EDI, e também para a codificação de me nsagens EDI.[3]
Enterprise, como em Centro de Atendimento à Empresa	Uma linha de negócio em que uma Afiliada que fornece serviços de PKI a Clientes de PKI gerenciada.
Enterprise Roaming Server	Um servidor que reside no local do Cliente de PKI Gerenciada, usado com o Serviço VeriSign Roaming para manter chaves privadas e partes de chaves simétricas dos Assinantes usadas para criptografar e decriptografar as chaves privadas de Assinantes Roaming.

Enterprise Security Guide	Um documento que define as recomendações de segurança para Clientes de PKI Gerenciada e Clientes Gateway.
Auditoria/Investigação Completa	Uma auditoria ou investigação feita pela VeriSign, onde esta tem motivos para crer que uma entidade falhou em atender aos Padrões VTN, um incidente ou Comprometimento relacionado à entidade, ou uma ameaça real ou potencial à segurança da VTN causada pela entidade.
Gateway	Um serviço pela VeriSign ou uma Afiliada que permite à uma organização usar um servidor independente de Certificado para se tornar uma AC dentro da VTN, delegando à uma AC da VeriSign a certificação da chave pública da organização.
Gateway Administrator	Um administrador que executa funções de validação e outras funções de AR para um cliente Gateway.
Certificado Gateway	Um certificado emitido a um Cliente Gateway, certificando sua chave pública.
Cliente Gateway	Uma organização que obteve serviços Gateway fornecidos pela VeriSign ou uma Afiliada, onde a organização se torna uma AC dentro da VTN para emitir Certificados de Classe 1.
ID de Servidor Global	Um certificado corporativo de classe 3 usado no suporte às sessões de SSL entre navegadores e servidores que estão criptografados, utilizando uma sólida proteção criptográfica consistente com as leis de exportação aplicáveis.
Global Server OnSite	Veja PKI Gerenciada para SSL Premium Edition.
Global Server OnSite Customer	Veja PKI Gerenciada para Cliente de SSL Premium Edition.
Go Secure!	Um conjunto de serviços plug-and-play estruturados pelos serviços de PKI Gerenciada e criados para acelerar os aplicativos de comércio eletrônico.
Direitos de Propriedade Intelectual	Direitos sobre um ou mais dos seguintes: direitos autorais, patente segredo industrial, marca comercial, e quaisquer outros tipos de direitos de
Intermediate Certification Authority (AC Intermediária)	Uma Autoridade Certificadora cujo Certificado está localizado dentro deuma Cadeia de Certificados entre o Certificado da AC raiz e o Certificado de uma Autoridade Certificadora que emitiu um certificado de Assinante.
Guia de Referência da Cerimônia da Chave	Um documento que descreve os requisitos e práticas para a Cerimônia de Geração de Chave.
Cerimônia de Geração de Chave	Um procedimento onde o par de chave de uma AC ou AR é gerado, sendo transferida sua chave privada para um módulo criptográfico; é feita a cópia de segurança da chave, e/ou a certificação da chave pública.
Administrador de Gerenciador de Chave	Um administrador que executa as funções de geração e recuperação d de chaves para um Cliente de PKI Gerenciada usando um Administrador de Chave de PKI Gerenciada.
Key Recovery Block (KRB)	Uma estrutura de dados contendo a chave privada do Assinante, que é criptografada usando uma chave criptográfica. Os KRBs são gerados usando os software Managed PKI Key Manager
Key Recovery Service	Um serviço oferecido pela A VeriSign que fornece chaves criptográficas necessárias para a recuperação de um Key Recovery Block como parte do uso do software Managed PKI Key Manager de um Cliente de PKI Gerenciada
PKI Gerenciada	Serviço de PKI gerenciada, totalmente integrado, fornecido pela VeriSign que permite que Clientes corporativos da VeriSign e suas Afiliadas distribuam Certificados a indivíduos, como funcionários, parceiros, fornecedores, e clientes, bem como dispositivos, como servidores, roteadores e firewalls. A PKI Gerenciada possibilita às empresa a troca segura de mensagens, intranet, extranet, VPN e aplicativos de comércio eletrônico
Administrador de PKI Gerenciada	Um administrador que executa funções de validação e outras funções de AR para um Cliente de PKI Gerenciada.
Guia do Administrador de PKI Gerenciada	Documento da VeriSign contendo os requisitos operacionais e práticas para Clientes de PKI gerenciada.
Contrato de PKI Gerenciada	Um contrato onde uma organização se torna um Cliente de PKI Gerenciada e concorda com os termos da DPC da VeriSign e Afiliadas.

Certificado de PKI Gerenciada	Um Certificado cuja Solicitação de Certificado foi aprovada por um Cliente de PKI Gerenciada.
Cliente de PKI Gerenciada.	Uma organização que obteve serviços de PKI Gerenciada fornecidos pela VeriSign ou uma Afiliada, onde a organização se torna uma AC dentro da VTN, para emitir Certificados cliente e/ou servidor. Os Clientes de PKIGerenciada terceirizam as funções secundárias de emissão, gerenciamento e revogação para a VeriSign ou Afiliada, porém mantêm consigo as funções de AR para a aprovação ou rejeição de Solicitações de Certificado, e iniciar as revogações e renovações de Certificados.
Cliente de PKI Gerenciada. Center (Centro de controle dePKI gerenciada)	Uma interface Web que permite a Administradores de PKI Gerenciada executar a Autenticação Manual de Solicitações de Certificado
Managed PKI Key Manager (Gerenciador de chave PKI Gerenciada)	Uma solução de recuperação de chave para Clientes de PKI Gerenciada que optam por implementar a recuperação da chave em um contrato especial de PKI Gerenciada.
Managed PKI Key Management Service Administrator's Guide	Documento da VeriSign contendo os requisitos operacionais e práticas para um Cliente de PKI Gerenciada usando um Administrador de Chave de PKIGerenciada.
PKI Gerenciada Lite	Um tipo de serviço de PKI Gerenciada que permite à organização se tornar uma Autoridade de Registro dentro da VTN, para auxiliar na emissão deCertificados Clientes para uma AC da VeriSign ou Afiliada.
PKI Gerenciada para SSL	Um tipo de serviço de PKI Gerenciada que permite à organização se tornar uma Autoridade de Registro dentro da VTN, para auxiliar na emissão de Ids de Servidor Seguro para uma AC da VeriSign ou Afiliada, dentro dos domínios designados. Esta AC delega aos Clientes de PKI Gerenciada Servidor as funções de AR de aprovação e rejeição de Solicitações de Certificado, revogações e renovações de IDs de Servidor Seguro.
PKI Gerenciada para Cliente SSL	Uma organização que obteve serviços de PKI Gerenciada para SSL da VeriSign ou Afiliada.
PKI Gerenciada para SSL Premium Edition	Um tipo de serviço de PKI Gerenciada que permite à organização se tornar uma Autoridade de Registro dentro da VTN, para auxiliar uma AC da VeriSign ou Afiliada na emissão de Ids de Servidor Seguro nos domínios designados. Esta AC delega às PKIs Gerenciadas para Clientes SSL Premium Edition Clientes de PKI Gerenciada as as funções de AR para a aprovação ou rejeição de Solicitações de Certificado e dar início a revogações e renovações de Ids de Servidor Global.
PKI Gerenciada para Cliente SSL Premium Edition	Uma organização que adquiriu serviços de PKI Gerenciada para SSL Edition da VeriSign ou uma Afiliada
Cliente Lite de PKI Gerenciada	Uma organização que adquiriu serviços de PKI Gerenciada Lite da VeriSign ou uma Afiliada, onde a organização se torna uma Autoridade de Registro dentro da VTN, para auxiliar na emissão de Certificados cliente para uma AC da VeriSign ou Afiliada. Esta AC delega aos Clientes de PKI Gerenciada Lite funções de AR para aprovação rejeição de Solicitações de Certificado e iniciar as revogações e renovações de Certificados.
Autenticação Manual	Um procedimento onde as Solicitações de Certificado são avaliadas e aprovadas manualmente, uma a uma, por um Administrador usando uma interface Web
Plano de Proteção NetSure	Um programa de garantia prolongada, descrito na PC § 1.1.2.2.3.
Informações não-verificáveis do Assinante	As informações submetidas por um Solicitante de Certificado a uma AC ouAR, inclusas em um Certificado, que não foram confirmadas pela AC ou AR, que por sua vez não fornecem garantias adicionais além daquelas apresentadas pelo Solicitante de Certificado

Não-repúdio (Non-repudiation)	Um atributo de uma comunicação que protege contra uma parte, para uma comunicação que deslealmente nega sua origem, negando que foi enviada ou entregue. Uma negação de origem consistem na negação de que uma comunicação originada da mesma fonte que uma seqüência de uma ou mais mensagens, mesmo que a identidade associada ao remetente seja desconhecida. Nota: apenas uma sentença judicial, comissão de arbitragem ou outro tribunal podem definitivamente evitar a repúdio. Por exemplo, uma assinatura digital verificada com referência a um Certificado VTN pode servir de prova na sustentação de uma determinação de não-repúdio por um tribunal, mas que não consistem em não-repúdio por si mesma.
Certificado OFX	Um certificado corporativo de classe 3 emitidos ao servidor de uma instituição financeira para uso com a especificação Open Financial Exchange (OFX).
OCSP - Online Certificate Status Protocol (Protocolo de Status de Certificado On-line)	Um protocolo que fornece a Parte Confiante informações de status de certificados em tempo real
OnSite	Consulte PKI Gerenciada.
OnSite Administrator	Consulte Administrador de PKI Gerenciada.
OnSite Administrator's Handbook	Veja o Guia do Administrador de PKI Gerenciada.
OnSite Agreement	Consulte o Contrato de PKI Gerenciada.
Certificado OnSite	Certificado de PKI Gerenciada.
OnSite Control Center (centro de controle OnSite)	Managed PKI Control Center (centro de controle de PKI Gerenciada).
Cliente OnSite	Veja Cliente de PKI Gerenciada Lite.
Administrador de Chave OnSite	Veja (software) Managed PKI Key Manager, Administrador de Chave de PKI Gerenciada.
OnSite Key Management Service Administrator's Guide	Veja o Guia do Administrador de Gerenciamento de Chave de PKI Gerenciada
OnSite Lite	Veja Cliente de PKI Gerenciada Lite.
Open Financial Exchange. (OFX)	Uma especificação padrão baseada na Web para a troca eletrônica de dados financeiros entre instituições financeiras, negócios e consumidores
Período Operacional	O período inicial, com a data e hora de emissão de um Certificado (ou posteriormente, se especificado no Certificado) e encerrando com a data e hora de expiração do Certificação ou de sua revogação
PKCS #10	Public-Key Cryptography Standard #10, desenvolvido pela RSA Security Inc., que define uma estrutura para uma Solicitação de Assinatura de Certificado.
PKCS #12	Public-Key Cryptography Standard #12, desenvolvido pela RSA Security Inc., que define meios seguros para a transferência de chaves privadas.
PMA - Policy Management Authority (Autoridade de Gerenciamento de Política)	Organização na VeriSign responsável pela promulgação desta política pela VTN.

PCA - Primary Certification Authority (Autoridade Certificadora de Políticas)	Uma AC que age como AC raiz para uma classe específica de certificados, eemite certificados às suas ACs subordinadas.
Centro de Processamento	Uma organização (VeriSign ou certas Afiliadas) que criam uma instalação segura, entre outras detalhes, os módulos criptográficos usados na emissão de Certificados. Na linha de negócios Consumidor e Web Site, os Centros de Processamento atuam como ACs na VTN, executando todos os serviços de ciclo de vida de emissão, administração, revogação e renovação de certificados. Na linhas de negócio Enterprise. os Centros de Processamento prestam serviços de ciclo de vida em nome dos Clientes de PKI Gerenciada ou clientes de PKI gerenciada de seus Centros de Serviço subordinados.
Public Key Infrastructure (ICP - Infra-estrutura de ChavePública)	A arquitetura, organização, técnicas, práticas e procedimentos que coletivamente suportam a implementação e operação de um sistema criptográfico de chave pública baseada em Certificado. A PKI da VeriSign consiste nos sistemas que colaboram para a implementação da VTN.
Autoridade de Registro. AR	Uma entidade aprovada por uma AC, a auxiliar Solicitantes de Certificado na inscrição para certificados, bem como funções de aprovação ou rejeição de Solicitações, revogação e renovação de Certificados.
Parte Confiante (‘terceira parte’)	Um indivíduo ou organização dá credibilidade a um certificado e/ou assinatura digital.
Contrato de Parte Confiante	Um contrato usado por uma AC que define os termos e condições sob as quais uma um indivíduo ou organização age como Terceiro.
Certificado de Varejo	Um certificado emitido pela VeriSign ou uma Afiliada, agindo como uma AC, para indivíduos ou organizações que fazem solicitações individuais à VeriSign ou uma Afiliada em seu site.
Assinante Roaming	Um assinante que usa o serviço de roaming, VeriSign Roaming Service, onde sua chave privada é criptografada e decriptografada com uma chave simétrica, que é dividida entre o Servidor VeriSign Roaming e um Servidor Roaming corporativo .
RSA	Sistema criptográfico de chave pública, inventando por Rivest, Shamir e Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	Autoridade Certificadora que emite IDs de Servidor Seguro.
Hierarquiea RSA Secure Server	A hierarquia de PKI composta pela Autoridade de Certificação RSA de Servidor Seguro .
Secret Share compartilhamento de segredo	Parte de uma chave privada de AC, ou parte dos dados de ativação necessários para operar uma chave privada de AC conforme disposto em um
Secret Sharing (compartilhamento de segredo)	Consistem em separar a chave privada de AC dados de ativação que operam uma chave privada de AC, para aplicar o controle multipessoal sobre as operações de chave privada de AC, conforme a PC § 6.2.2.
ID de Servidor Seguro	Um certificado corporativo de classe 3 usado no suporte às sessões de SSL entre navegadores e servidores.
Secure Sockets Layer. (SSL)	Método padrão da indústria para proteger as comunicações via Internet, foi desenvolvida pela Netscape Communications Corporation. O protocolo de segurança SSL oferece a criptografia de dados, autenticação de servidor, integridade de mensagem e autenticação cliente opcional para uma conexão TCP/IP.
Guia de Requisitos de Segurança e Auditoria	Documento da VeriSign que define os requisitos e práticas de segurança e auditoria para Centros de Processamento e Centros de Serviço.
Análise de Segurança e Práticas	Uma análise de uma Afiliada, realizada pela VeriSign, antes que esta Afiliada possa iniciar suas operações.

Server Gated Cryptography	Tecnologia que permite servidores Web que tenham emitido uma ID de Servidor Global para criar uma sessão SSL com um navegador criptografado com alta proteção criptográfica.
Server OnSite	Veja PKI Gerenciada para Servidor
Cliente SSL Server OnSite	Veja PKI Gerenciada para Cliente SSL.
Centro de Serviços para Servidores	Um Centro de Serviços que é uma Afiliada fornecendo IDs de Servidor Seguro e IDs de Servidor Global, seja na linha de negócios Web Site ou Enterprise.
Centro de Serviços	Uma Afiliada que não aloja unidades de assinatura de Certificado para a emissão de classe ou tipo especial; um Centro de Processamento realiza as funções de emissão, gerenciamento, revogação e renovação de tais Certificados.
Subdomínio	A parte da VTN controlada por uma entidade e entidades subordinadas, dentro da hierarquia da VTN.
Titular	O portador da chave privada correspondente à chave pública. O termo “Titular” pode ser referir também a uma Certificado corporativo, o equipamento ou dispositivo que contém uma chave privada.. Um Titular é atribuído a um nome exclusivo, vinculado a uma chave pública contida no Certificado do Titular.
Assinante	Para certificados individuais, a pessoa que é o Titular e para quem foi emitido o Certificado. No caso de um Certificado corporativo, uma organização que possui o equipamento ou dispositivo que é o Titular do certificado, para quem o Certificado foi emitido. Um Assinante é capaz de usar, e está autorizado a faze-lo, a chave privada que corresponde à chave pública listada no Certificado.
Contrato do Assinante	Um contrato usado por uma AC que define os termos e condições sob as quais uma um indivíduo ou organização age como Terceiro.
Entidade Superior da AC	Entidade acima de outra entidade dentro da hierarquia da VTN (a hierarquia das classes 1, 2 ou 3).
Supplemental Risk Management Review (Revisões Adicionais de Gerenciamento de Risco)	Uma análise de uma entidade realizada pela VeriSign, apresentando descobertas incompletas ou excepcionais em uma Auditoria de Conformidade ou como parte do processo geral de gerenciamento de risco no curso normal do negócio
Revendedor	Uma entidade disponibiliza serviços para a VeriSign ou uma Afiliada em mercados específicos.
Autoridade de Datação	Entidade VeriSign que assina Recibos Digitais como parte do Serviço de Cartório Digital VeriSign
AC da Autoridade de Datação -	A AC VeriSign que emitiu um certificado corporativo especial classe 3 para a Autoridade de Datação, usando na verificação das assinaturas digitais em Recibos Digitais.
Pessoa Qualificada	Um funcionário, contratado ou consultor de uma entidade dentro da VTN responsável pelo gerenciamento da confiança infra-estrutural da entidade, seus produtos, serviços, instalações, práticas conforme disposto na PC § 5.2.1.
Posição Qualificada	As posições dentro de uma entidade da VTN que devem ser ocupadas por uma Pessoa Qualificada
Sistema Confiável	Hardware e software de computador e procedimentos que são razoavelmente protegidos contra invasões e abuso, fornecem um nível razoável de disponibilidade, confiabilidade e operação correta; são adequados para executar as funções planejadas e reforçar a política de segurança aplicável. Um sistema confiável não é necessariamente um “sistema qualificado”, conforme reconhece a nomenclatura governamental classificada.
Centro de Serviços Universal	Uma entidade participante do Programa do Centro de Serviços Universal
Programa do Centro de Serviços Universal	Um programa onde as entidades comercializam serviços da VeriSign em mercados específicos, usando uma plataforma de software especializada para gerenciar a complexa implantação multinível de PKI.

VeriSign	Significa, com relação às partes pertinentes desta DPC, VeriSign, Inc. e/ou subsidiária VeriSign responsável por operações específicas de emissão.
Serviço de Notarização Digital VeriSign	Um serviço oferecido a Clientes de PKI Gerenciada, que fornece uma segurança/prova digitalmente assinada (um Recibo Digital) que certo documento ou conjunto de dados existiram em certo momento.
Repositório VeriSign	Banco de dados da VeriSign e outras informações relevantes da VTN acessíveis online.
Servidor Roaming VeriSign	Um servidor residente no Centro de Processamento da VeriSign, junto com o serviço Roaming, para manter parte das chaves simétricas usadas para criptografar e decriptografar as chaves privadas de Assinantes Roaming.
Serviço Roaming VeriSign	Serviço oferecido pela VeriSign que permite a um Assinante fazer o download da chave privada, e realizar operações em terminais lidif
Política de Segurança	O documento mais importante que descreve as políticas de segurança da VeriSign.
VTN - VeriSign Trust Network (Rede de Confiança da VeriSign)	A Infra-estrutura de Chave Pública baseada em Certificado, regida pelas Políticas de Certificado da VeriSign Trust Network, que permite a implementação e uso global dos Certificados pela VeriSign e suas Afiliadas e seus respectivos Clientes, Assinantes e Parte Confiante.
Participante VTN	Um indivíduo ou organização que tem um ou mais dos papéis descritos a seguir na rede VTN: VeriSign, Afiliada, Cliente, Centro de Serviços Universal Revendedor, Assinante ou Terceiro.
Padrões VTN	Os requisitos empresariais, legais e técnicos para a emissão, administração, revogação, renovação e uso de Certificados dentro da
Web Host	Uma entidade que hospeda um web site de outra, como um provedor de serviços na Internet, integrador de sistemas, Revendedor, consultor técnico e provedores de serviços em software, ou entidades
Programa Web Host	Um programa que permite a inscrição de Web Hosts a IDs de Servidor Seguro e IDs de Servidor Global, em nome de Assinantes, que por sua vez, são clientes dos Web Hosts.
Web Site, como em web site,site na Internet,	Uma linha de negócio em que uma Afiliada que fornece ID de Servidor Seguro e Certificados de ID de Servidor Global, um a um liidifid
Protocolo WAP - Wireless Application Protocol.	Padrão para apresentação e entrega de informações sem fio e serviços telefônicos em telefones celulares e outros terminais sem fio
Wireless Transport Layer Security. (WTLS)	Um protocolo que protege a comunicação dos aplicativos que operam usando o protocolo WAP, como as comunicações entre um fone sem fio e um servidor.
Wireless Transport Layer Security Certificate (Certificado WTLS)	Um certificado corporativo Classe 3 cujo formato é definido como parte do protocolo Wireless Application Protocol, que autentica um servidor Wireless Transport Layer Security para um cliente WTLS, facilitando a comunicação criptografada entre o servidor e cliente WLS.