

## GLOSSÁRIO DE CERTIFICAÇÃO DIGITAL

### ACEITAÇÃO

Demonstração da concordância quanto à correção e adequação do conteúdo e de todo o processo de emissão de um Certificado Digital, feita pelo indivíduo ou entidade que o solicitou. A aceitação ocorre através do recebimento e reconhecimento de uma notificação sobre o conteúdo do certificado, conforme os termos da Declaração de Práticas de Certificação – DPC.

O certificado é considerado aceito ao ser instalado no sistema do solicitante a partir de sua primeira utilização ou após haver decorrido o prazo pré-estipulado para sua rejeição.

### ACESSO

Estabelecimento de conexão entre um indivíduo ou entidade e um sistema de comunicação ou de informações. A partir do acesso podem ocorrer a transferência de dados e a ativação de processos computacionais.

### ADMINISTRADOR DE UMA MPKI (MANAGED PKI ADMINISTRATOR)

Indivíduo designado para controlar e administrar as funções de uma Infraestrutura de Chaves Públicas – PKI.

### ADVANCED ENCRYPTION STANDARD - AES

O Padrão de Cifração Avançada (AES) é uma cifra de bloco adotada como padrão de cifração pelo governo dos Estados Unidos. O AES é um dos algoritmos mais populares usados na criptografia de chave simétrica. AES tem um tamanho de bloco fixo de 128 bits e uma chave com tamanho de 128, 192 ou 256 bits.

### ADWARE

Software que exibe publicidade. O adware muitas vezes inclui spyware, de modo que os anúncios podem ser dirigidos segundo interesses e hábitos do usuário.

## AMERICAN INSTITUTE OF CERTIFIED PROFESSIONAL ACCOUNTANTS - AICPA

Instituto de profissionais de contabilidade norte-americano que estabeleceu os padrões de auditoria conhecidos como SAS-70 Statement of Audit Standards, utilizados como procedimento em auditorias sobre os controles físicos e de acesso das instalações de segurança de empresas e organizações. O site da AICPA funciona no endereço: <http://www.aicpa.org>.

## APPLICATION GATEWAY - AGATE

Componente do Internet Transaction Server (ITS) em aplicativos SAP. O Application Gateway é um processo servidor ativo que funciona independente de um servidor web em particular. Ele estabelece conexão com o servidor do aplicativo SAP, gerencia o processo de conexão e controla o contexto e o tempo de inatividade (time-out) da sessão. Além disso, gera páginas HTML e fornece conversões das páginas de códigos e suporte para o idioma local.

## AGENTE DE REGISTRO

Responsável pela execução das atividades inerentes à Autoridade de Registro. É a pessoa que realiza a autenticação da identidade de um indivíduo ou de uma organização e validação das solicitações de emissão e revogação de certificados nas Autoridades de Registro.

## ALGORITMO

### ALGORITHM

Série de etapas utilizadas para completar uma tarefa, procedimento ou fórmula na solução de um problema. Em criptografia, um algoritmo representa o processo matemático utilizado para “embaralhar” os dados.

## ALGORITMO CRIPTOGRÁFICO

### CRYPTOGRAPHIC ALGORITHM

Processo matemático especificamente definido para criptografar e decriptografar mensagens e informações, normalmente com a utilização de chaves.

## ALGORITMO ASSIMÉTRICO

É um algoritmo de criptografia que utiliza duas chaves: uma Chave Pública, que pode ser distribuída abertamente, e uma Chave Privada, que é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave.

## ALGORITMO SIMÉTRICO

Algoritmo de criptografia que usa somente uma chave, tanto para cifrar como para decifrar. Essa chave deve ser mantida secreta para garantir a confidencialidade da mensagem. Também conhecido como algoritmo de chave secreta.

## AMERICAN NATIONAL STANDARDS INSTITUTE - ANSI

Organização privada sem fins lucrativos, cujo objetivo é promover o uso internacional de padrões norte-americanos, a defesa de políticas e posições técnicas dos EUA em entidades de padronização locais e internacionais, e o estímulo à adoção nos EUA de padrões internacionais que atendam às necessidades da comunidade de usuários. O site do ANSI funciona no endereço: <http://www.ansi.org>.

## APPLICATION PROGRAMMING INTERFACE - API

Interface de programação de aplicativos que permite a comunicação entre programas ou entre um programa e o kernel (de um sistema operacional), estabelecendo as convenções e os parâmetros a serem seguidos.

## ARQUITETURA ARCHITECTURE

Modo de configuração de um sistema, incluindo o relacionamento entre suas partes. Arquitetura de Hardware é a configuração dos componentes físicos do sistema (servidores e firewalls). Arquitetura de Software é a configuração dos componentes (programas, sistemas operacionais ou scripts) dentro do sistema.

## ASSISTENTE DE AUTENTICAÇÃO AUTHENTICATION WIZARD

Componente do serviço de PKI Certisign disponível através do Centro de Processamento da Certisign. Permite ao administrador personalizar o modo como o usuário será autenticado para que se dê a aprovação ou rejeição de uma solicitação de Certificado Digital.

ASSINANTE  
SUBSCRIBER

Indivíduo ou organização para quem foi emitido um Certificado Digital dentro de uma hierarquia criptográfica. O assinante é o titular da Chave Privada correspondente à Chave Pública contida no certificado e possui a capacidade de utilizar tanto uma quanto a outra.

ASSINATURA DIGITAL  
DIGITAL SIGNATURE

Transformação de uma mensagem eletrônica através da aplicação de uma função matemática e da criptografia do seu resultado com a Chave Privada do remetente, de modo que o destinatário da mensagem possa verificar sua origem e integridade. A assinatura digital garante que um conjunto de dados (mensagem ou arquivo) realmente provém de determinado remetente e não foi adulterado após o envio.

AUDITORIA  
AUDIT

Procedimento realizado por agentes independentes e utilizado para verificar se todos os controles, equipamentos e dispositivos estão preparados e são adequados às suas funções. Inclui o registro e análise de todas as atividades importantes para detectar vulnerabilidades ou abusos em um sistema de informações.

AUTENTICAÇÃO  
AUTHENTICATION

Processo de confirmação da identidade de um indivíduo ou organização, e de comprovação da posse ou integridade de certas informações. Um administrador executa a autenticação das solicitações de certificados através da validação da identidade do solicitante e da confirmação dos dados da solicitação.

AUTENTICAÇÃO AUTOMÁTICA  
AUTOMATED AUTHENTICATION

Processo pelo qual uma solicitação de certificado é aprovada por comparação automática dos dados da solicitação com informações previamente disponíveis em um banco de dados. As opções de autenticação automática oferecidas pela MPKI Certisign são a Automated Administration e a Autenticação por Passcode.

## AUTENTICIDADE

Qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção.

## AUTORIDADE CERTIFICADORA – AC CERTIFICATE AUTHORITY - CA

Entidade autorizada a emitir, suspender, renovar ou revogar Certificados Digitais. Cabe também à Autoridade Certificadora emitir Listas de Certificados Revogados (LCR) e manter registros de suas operações. A principal competência de uma AC, no entanto, é emitir certificados que vinculem uma determinada Chave Pública ao seu titular. Na hierarquia dos Serviços de Certificação Pública Certisign, as ACs estão subordinadas à Autoridade Certificadora Primária (AC-Raiz) da VeriSign, enquanto as ACs abaixo da hierarquia da ICP-Brasil subordinam-se à AC-Raiz da ICP-Brasil. A AC é identificada por um nome distinto - distinguished name (DN) em todos os certificados que emite.

## AUTORIDADE DE CARIMBO DE TEMPO - ACT

A autoridade na qual os usuários de serviços de carimbo do tempo (isto é, os subscritores e as terceiras partes) confiam para emitir carimbos do tempo.

## AUTORIDADE EMISSORA – AE ISSUING AUTHORITY - IA

A Autoridade Emissora (AE) pode ser uma Autoridade de Certificação Primária (AC-Raiz), uma Autoridade Certificadora (AC) ou uma AC Subordinada, que somente pode emitir certificados válidos e confiáveis com a aprovação prévia da AC-Raiz da hierarquia. Uma AE pode delegar as responsabilidades de avaliar, aprovar e recusar solicitações de certificados a uma ou mais Autoridades de Registro Local (ARLs), que não pertençam nem sejam operadas por aquela AE. Quando isso ocorre, o termo "AE" deve incluir as ARLs para efeito de obrigações, garantias e exclusões.

AUTORIZAÇÃO  
AUTHORIZATION

Concessão de direito ou permissão que inclui a capacidade de acessar informações e recursos específicos em um sistema computacional.

BANCO DE DADOS  
DATABASE

Conjunto de informações relacionadas que são criadas, armazenadas e/ou manipuladas por um sistema de informações gerenciado por computador.

BACK DOOR

Uma vulnerabilidade na segurança instalada por vírus ou trojan para facilitar o acesso de um invasor – normalmente secreto – a um computador, driblando salvaguardas.

BASE64

É um método para codificação de dados para transferência na Internet (Content Transfer Encoding).

BASIC ENCODING RULES - BER

Regras para codificação de objetos ASN.1 em uma sequência de bytes.

BIOMETRIA  
BIOMETRICS

Ciência que utiliza propriedades físicas e biológicas para identificar indivíduos. São exemplos de identificação biométrica as impressões digitais, o escaneamento de retina e o reconhecimento de voz.

BIT  
BINARY DIGIT

Dígito binário (Binary digit), que pode ser 1 ou 0.

BLOCO  
BLOCK  
Seqüência de bits de comprimento fixo.

BROWSER  
NAVEGADOR

Vide Navegador de Internet / Web Browser.

CADEIA DE CERTIFICADOS  
CERTIFICATE CHAIN

Lista ordenada de certificados que contém um certificado de assinante (entidade final) e um ou mais certificados de nível superior até a Autoridade Emissora (AE). Permite a um destinatário verificar que o remetente e todas as AEs envolvidas são confiáveis.

CANAL SEGURO

Canal de comunicação criptograficamente seguro para transmissão de informações.

CARIMBO DE TEMPO

Documento eletrônico emitido pela Autoridade de Carimbo de Tempo (ACT). Serve como evidência de que uma informação digital existia numa determinada data e hora no passado.

CAPI  
CRYPTOGRAPHIC APPLICATION PROGRAMMING INTERFACE

É uma interface de programação para aplicações incluída com o sistema operacional *Microsoft Windows* que provê serviços para habilitar desenvolvedores para aplicações de segurança baseadas em *Windows* usando criptografia. É um conjunto de bibliotecas dinamicamente ligadas que provê um nível de abstração e isola programadores do código usado para cifrar dados.

CENTRO DE CONTROLE  
CONTROL CENTER

Conjunto de páginas web no serviço de MPKI Certisign/VeriSign. Permite aos Administradores visualizar, aprovar, recusar, suspender e revogar os certificados solicitados.

## CERTIFICAÇÃO CRUZADA CROSS-CERTIFICATION

Situação em que uma Autoridade Certificadora Primária emite um certificado cujo assunto (subject) é uma entidade emissora de certificados que representa outro domínio de certificação, ou vice-versa. A certificação cruzada permite compartilhar a confiança entre diferentes entidades e redes de PKI.

## CERTIFICAÇÃO DIGITAL DIGITAL CERTIFICATION

É a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.

## CERTIFICADO AUTOASSINADO

Certificado assinado com a Chave Privada da própria entidade que o gerou. O único certificado autoassinado da ICPBrasil é o da Autoridade Certificadora Raiz.

## CERTIFICADO DE AFILIAÇÃO

Certificado emitido para indivíduos ou entidades afiliadas. Um certificado de afiliação fornece uma comprovação de identidade adequada, sem necessariamente afirmar que o indivíduo ou entidade em questão possui autorização para agir em nome da entidade à qual é afiliado.

## CERTIFICADO DE ASSINATURA DE CÓDIGO CODE SIGNING CERTIFICATE

Certificado emitido para empresas que desenvolvem software, permitindo que assinem digitalmente o código-objeto de programas, o que garante a origem e a integridade absoluta para quem recebe o código pela Internet.

## CERTIFICADO DE ASSINATURA DIGITAL (A1, A2, A3 E A4)

São os certificados usados para confirmação da identidade na web, correio digital, transações online, redes privadas virtuais, informações eletrônicas,

cifração de chaves de sessão e assinatura de documentos com verificação da integridade.

#### CERTIFICADO DE ATRIBUTO

Estrutura de dados contendo um conjunto de atributos (características e informações) sobre a entidade final, que é assinada digitalmente com a Chave Privada do órgão que o emitiu. Pode possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos.

#### CERTIFICADO DE CALIBRAÇÃO

Documento emitido pelo Observatório Nacional atestando que o equipamento usado para emitir Carimbos de Tempo (SCT) está dentro dos padrões de sincronismo esperados e está apto a entrar em funcionamento.

#### CERTIFICADO DE CHAVE PÚBLICA PUBLIC KEY CERTIFICATE

Credencial eletrônica cujos requisitos mínimos são: declarar o nome ou identidade da respectiva Autoridade Certificadora; identificar o respectivo titular; conter a Chave Pública referente ao titular; identificar o período operacional; conter o número de série do certificado e a assinatura digital da Autoridade Certificadora. Os Certificados Digitais são utilizados para autenticar o remetente e confirmar a integridade dos dados enviados, podendo também fornecer elementos que impeçam ou dificultem o repúdio infundado a atos ou transações. Além disso, os certificados podem ser utilizados para criptografar dados e enviá-los ao seu titular. Os Certificados Públicos Certisign podem ser publicados através da VeriSign Trust Network (VTN) e estabelecer comunicação fora de seu domínio. Os Certificados Privados Certisign não fazem parte da VTN e não podem estabelecer comunicação fora do seu domínio.

#### CERTIFICADO DE SIGILO (S1, S2, S3 E S4)

São os certificados usados para cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.

#### CERTIFICADO DIGITAL

É um conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITUT X.509,

que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.

#### CERTIFICADO DE DEMONSTRAÇÃO (DEMO) DEMO CERTIFICATE

Certificado emitido por uma Autoridade Certificadora com a finalidade exclusiva de apresentação e demonstração, não podendo ser utilizado para comunicações seguras ou confidenciais. Os certificados demo só podem ser utilizados por pessoas autorizadas.

#### CERTIFICADO DO TIPO A1 E S1

É o certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha, cifrado por software. Sua validade máxima é de um ano, sendo a frequência de publicação da Lista de Certificados Revogados no máximo de 48 horas e o prazo máximo admitido para conclusão do processo de revogação de 72 horas.

#### CERTIFICADO DO TIPO A2 E S2

É o certificado em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em cartão inteligente ou *token*, ambos sem capacidade de geração de chave e protegidos por senha. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de dois anos, sendo a frequência de publicação da Lista de Certificados Revogados no máximo de 36 horas e o prazo máximo admitido para conclusão do processo de revogação de 54 horas.

#### CERTIFICADO DO TIPO A3 E S3

É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão inteligente ou *token*, ambos com capacidade de geração de chaves e protegidos por senha ou hardware criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da Lista de Certificados Revogados no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação de 36 horas.

## CERTIFICADO DO TIPO A4 E S4

É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão inteligente ou *token*, ambos com capacidade de geração de chaves e protegidos por senha ou hardware criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 2048 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da Lista de Certificados Revogados no máximo de 12 horas e o prazo máximo admitido para conclusão do processo de revogação de 18 horas.

## CERTIFICADO EXPIRADO

Certificado cuja data de validade foi ultrapassada.

## CERTIFICADO VÁLIDO

É um certificado que está dentro do prazo de validade, não tendo sido Revogado. É possível validar toda a cadeia do certificado até uma Autoridade Certificadora Raiz aceita pelo usuário que recebe e valida o certificado.

## CERTIFICADOS DIGITAIS DE CLASSE 1/2/3

Certificados com nível específico de segurança e confiança dentro da hierarquia VeriSign Trust Network:

- Classe 1: fornece o nível mais baixo de segurança e confiança. Os certificados de classe 1 validam apenas o endereço de e-mail do indivíduo para quem o certificado foi emitido.
- Classe 2: oferece nível médio de confiança. Os certificados de classe 2 validam a identidade do indivíduo com a utilização de um banco de dados de clientes online e verificação do e-mail, ou então através de uma partição secreta.
- Classe 3: fornece o mais alto nível de confiança. Os certificados de classe 3 validam indivíduos através do comparecimento pessoalmente dos mesmos perante um agente autorizado, além de outras comprovações específicas de identidade. Os certificados de classe 3 validam organizações através de bancos de dados de terceiros (como o Cadastro Nacional de Pessoas Jurídicas - CNPJ) e outros meios independentes.

CGI

COMMON GATEWAY INTERFACE

Protocolo que especifica como um servidor de Internet executa e troca dados com um programa.

#### CHAVE COMUM COMMON KEY

Partição física em um sistema de hardware criptográfico, armada através de um processo de partição secreta que exige que a partição física permaneça anexada ao hardware quando armada. Não se presume que seja secreta, já que não permanece continuamente sob o controle de um indivíduo.

#### CHAVE DE SESSÃO SESSION KEY

Chave utilizada em sistemas criptográficos de chave simétrica pela duração de uma mensagem ou sessão de comunicação. O protocolo SSL (Secure Sockets Layer) utiliza as chaves de sessão para manter a segurança das comunicações via Internet.

#### CHAVE DISTRIBUÍDA DISTRIBUTED KEY

Chave dividida em várias partes e compartilhada (distribuída) entre diferentes participantes.

#### CHAVE PRIVADA

Uma das chaves de um par de chaves criptográficas (a outra é uma Chave Pública) em um sistema de criptografia assimétrica. Mantida secreta pelo seu dono (detentor de um Certificado Digital), é usada para criar assinaturas digitais e para decifrar mensagens ou arquivos cifrados com a Chave Pública correspondente.

#### CHAVE PÚBLICA

Uma das chaves de um par de chaves criptográficas (a outra é uma Chave Privada) em um sistema de criptografia assimétrica. É divulgada pelo seu dono e usada para verificar a assinatura digital criada com a Chave Privada correspondente. Dependendo do algoritmo, a Chave Pública também é usada para cifrar mensagens ou arquivos que possam, então, ser decifrados com a Chave Privada correspondente.

## CHAVE SIMÉTRICA

Chave criptográfica gerada por um algoritmo simétrico (ver Algoritmo Simétrico).

## CHAVES ASSIMÉTRICAS

Chaves criptográficas geradas por um algoritmo assimétrico (ver Algoritmo Assimétrico).

## CICLO DE VIDA DO CERTIFICADO CERTIFICATE LIFECYCLE

Período de tempo que se inicia com a solicitação do certificado e termina com sua expiração, renovação ou revogação.

## CIFRA ASSIMÉTRICA ASYMMETRIC CIPHER

Algoritmo criptográfico que utiliza uma chave para criptografar e outra para descriptografar. A criptografia de Chaves Públicas é um exemplo de cifra assimétrica.

## CIFRA DE BLOCO BLOCK CIPHER

Cifra simétrica que criptografa um arquivo dividindo-o em blocos e criptografando cada bloco.

## CLIENTE CLIENT

Programa normalmente utilizado pelo usuário como interface para acessos a um conjunto de serviços tornados disponíveis por um servidor em relações cliente/servidor.

## COMITÊ GESTOR DA ICP-BRASIL

Autoridade gestora de políticas da ICP-Brasil que tem suas competências definidas na Medida Provisória 2.2002. É responsável, dentre outras coisas, por estabelecer a política e as normas de certificação e fiscalizar a atuação da Autoridade Certificadora Raiz - cuja atividade é exercida pelo Instituto Nacional de Tecnologia da Informação.

COMMON NAME – CN

Vide Nome Comum.

COMPONENTE DE RETAGUARDA  
BACK-END COMPONENT

Programa, dispositivo ou equipamento não diretamente visível para o usuário em sistemas, produtos ou serviços Certisign. Os componentes de apoio são geralmente protegidos por *firewall* para garantir sua segurança.

COMPONENTE DE INTERFACE  
FRONT END COMPONENT

Componente de um sistema, produto ou serviço Certisign diretamente visível para o usuário.

COMPROMETIMENTO  
COMPROMISE

Violação concreta ou suspeita de violação de uma política de segurança, onde possa ter ocorrido divulgação não autorizada ou perda do controle sobre informações sigilosas.

CONSULTA ONLINE DE SITUAÇÃO DO CERTIFICADO

Vide OCSP.

COOKIE

Uma espécie de arquivo que alguns websites põem nos computadores dos usuários para permitir a personalização do conteúdo da Internet. A maioria dos cookies é inofensiva, mas alguns registram hábitos de navegação na web e informação pessoal, além de serem considerados spyware.

## CONFIANÇA

Suposição de que uma entidade se comportará substancialmente como esperado no desempenho de uma função específica.

## CONFIDENCIALIDADE

### CONFIDENTIALITY

Propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. Assegurar a confidencialidade de documentos é assegurar que apenas pessoas autorizadas tenham acesso à informação.

## CONTROLE DE ACESSO

### ACCESS CONTROL

Conjunto de componentes dedicados a proteger a rede, aplicações web e instalações físicas de uma Autoridade Certificadora (AC) contra o acesso não autorizado, permitindo que somente organizações ou indivíduos previamente identificados possam acessar. Vide também Lista de Controle de Acesso / Access Control List.

## CONTROLE DISCRICIONÁRIO DE ACESSO

### DISCRETIONARY ACCESS CONTROL (DAC)

Conjunto de meios de restrição de acesso a objetos baseado na identidade dos titulares e/ou dos grupos a que pertencem. O controle é discricionário no sentido de que um titular com determinada permissão de acesso é capaz de transferir essa permissão (talvez até indiretamente) para qualquer outro titular a seu critério.

## CÓPIA DE SEGURANÇA

São as cópias feitas de um arquivo ou de um documento que deverão ser guardadas sob condições especiais para a preservação de sua integridade no que diz respeito tanto à forma quanto ao conteúdo. Permite o resgate de

programas ou informações importantes em caso de falha ou perda dos originais.

## COTEC

O Comitê Técnico COTEC presta suporte técnico e assistência ao Comitê Gestor da ICP-Brasil, sendo responsável por manifestar previamente sobre as matérias apreciadas e decididas pelo comitê Gestor.

## CPM

### CERTIFICATE PARSING MODULE

Módulo de análise de certificados, parte de produtos Certisign que extrai informações dos certificados de clientes apresentados a um servidor de Internet e as torna disponíveis para aplicativos que utilizem Certificados Digitais.

## CREENCIAMENTO

### ACCREDITATION

Declaração formal feita por uma autoridade competente para afirmar que um sistema de informações, organização ou profissional foi considerado apto a executar determinadas tarefas ou operar em um modo de segurança específico, após cumprir um conjunto de condições preestabelecido.

## CRIPTOGRAFIA

### CRYPTOGRAPHY

Processo de embaralhamento de dados para que não possam ser recuperados sem a utilização do processo inverso de decryptografia. A criptografia é uma ciência matemática usada para assegurar o sigilo e a autenticidade das informações, convertendo-as em uma versão ininteligível que só pode ser decifrada com a chave e o algoritmo criptográfico corretos.

## CRIPTOGRAFIA DE CHAVES PÚBLICAS

### PUBLIC KEY CRIPTOGRAPHY

Tipo de criptografia que usa um par de chaves criptográficas matematicamente relacionadas. A Chave Pública está disponível a todos que desejem criptografar informações e enviá-las ao dono da Chave Privada, ou verificar uma assinatura digital criada com aquela Chave Privada. A Chave

Privada é mantida em segredo por seu dono e pode decriptografar informações ou gerar assinaturas digitais.

#### CRYPTOAPI

Cryptographic Application Programming Interface (também conhecida como CryptoAPI, Microsoft Cryptography API, ou simplesmente CAPI) é uma interface de programação para aplicações incluída com o sistema operacional Microsoft Windows que provê serviços para habilitar desenvolvedores para aplicações de segurança baseadas em Windows usando criptografia. É um conjunto de bibliotecas dinamicamente ligadas, fornecendo um nível de abstração que isola programadores do código usado para cifrar dados.

#### CRYPTOGRAPHIC SERVICE PROVIDER - CSP

Vide Provedor de Serviços Criptográficos.

#### CPS

#### CERTIFICATION PRACTICE STATEMENT

Vide Declaração de Práticas de Certificação – DPC.

#### CSR

#### CERTIFICATE SIGNING REQUEST

Vide Solicitação de Assinatura de Certificado.

#### CSV – COMMA - SEPARATED VALUE

#### VALOR SEPARADO POR VÍRGULA

Formato de arquivo também conhecido como flat file (arquivo plano), que pode ser transferido entre aplicações baseadas em tabelas, como bancos de dados e planilhas. Este tipo de arquivo contém uma série de linhas de texto ASCII onde os valores das colunas são separados por uma vírgula, dando início a cada novo registro na linha imediatamente inferior.

#### DATA ENCRYPTION STANDARD - DES

#### PADRÃO DE CRIPTOGRAFIA DE DADOS

Sistema de cifragem em blocos desenvolvido pela IBM e pelo governo dos EUA nos anos 70 como padrão oficial. Está definido no documento de padronização FIPS 46-1.

#### DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO – DPC CPS – CERTIFICATION PRACTICE STATEMENT

Documento, periodicamente revisado e republicado, que contém as práticas e procedimentos implementados por uma Autoridade Certificadora para emitir certificados. É a declaração da entidade certificadora a respeito dos detalhes do seu sistema de credenciamento, das práticas e políticas que fundamentam a emissão de certificados e de outros serviços relacionados. É utilizado pelas Autoridades Emissoras para garantir a emissão correta dos certificados e pelos Solicitantes e Partes Confiantes para avaliar a adequação dos padrões de segurança empregados às necessidades de segurança de suas aplicações.

#### DECRIPTOGRAFIA DECRYPTION

Processo que transforma dados previamente criptografados e ininteligíveis (ciphertext) de volta à sua forma legível (plaintext).

#### DIFFIEHELLMAN

*DiffieHellman* é um método de criptografia desenvolvido por Whitfield Diffie e Martin Hellman e publicado em 1976. O algoritmo *DiffieHellman* permite que haja a troca de Chaves Públicas entre duas ou mais partes, permitindo que as pessoas que recebem a Chave Pública usem essa chave para cifrar o conteúdo de uma mensagem que será enviada à parte que forneceu a Chave Pública. Esse texto cifrado não poderá ser aberto por indivíduos que possuam a Chave Pública e, sim, apenas pela parte que enviou a Chave Pública, pois a mesma possui a Chave Privada que se encontra em seu poder. Tendo posse dessa chave, a mensagem cifrada poderá ser aberta.

#### DIGITAL ID

Nome comercial e marca registrada da VeriSign para um Certificado Digital. Vide Certificado Digital.

#### DIRECTORY ACCESS PROTOCOL - DAP PROTOCOLO DE ACESSO A DIRETÓRIOS

Protocolo que permite a um usuário de diretórios (um indivíduo ou outro aplicativo de software) acessar um diretório compatível com X.500.

#### DISPONIBILIDADE AVAILABILITY

Capacidade de utilizar informações e processos sob demanda, permitindo o acesso autorizado a recursos e a performance de operações críticas em tempo hábil.

#### DISTINGUISHED ENCODING RULES – DER

Regras para codificação de objetos ASN.1 em uma seqüência de *bytes*. Corresponde a um caso especial de BER.

#### DISTINGUISHED NAME - DN NOME DISTINTO

Conjunto de dados que identifica de modo inequívoco uma entidade ou indivíduo pertencente ao mundo físico no mundo digital (por exemplo: país=BR, estado=Rio de Janeiro, nome organizacional=Sua Empresa S.A., nome comum=José da Silva).

#### DOMAIN NAME SERVICE - DNS SERVIÇO DE NOMES DE DOMÍNIO

Processo que transforma endereços IP (1.2.3.4) em nomes hierárquicos, que podem ser lidos por seres humanos (www.companyname.com), e vice-versa.

#### DOCUMENTO

Registro que consiste em informações inscritas num meio tangível, como uma folha de papel, ao contrário das informações baseadas em sistemas de computação.

## EMISSÃO DE CERTIFICADO

Ação desempenhada por uma Autoridade Certificadora na criação de um certificado e subsequente notificação ao seu solicitante, ou seja, à pessoa ou organização listada no conteúdo do certificado, que se torna assinante a partir da aceitação.

## ENTIDADE AFILIADA

### AFFILIATED ENTITY

Entidade relacionada a outra: (i) como matriz, subsidiária, sócia, joint-venture, contratada ou agente; (ii) como membro de uma comunidade de interesses registrada; (iii) como entidade que mantém relacionamento com uma entidade principal ou negócios e registros capazes de fornecer comprovação adequada da identidade da afiliada.

## ENTIDADE DE AUDITORIA DE TEMPO – EAT

Entidade que realiza as atividades de autenticação e sincronismo de Servidores de Carimbo do Tempo (SCT), instalados nas ACT. Na estrutura de carimbo do tempo da ICP-Brasil, a EAT é o próprio Observatório Nacional.

## EULA

Abreviação de “End-User Licence Agreement”, ou acordo de licença do usuário final, os contratos que acompanham a maioria dos programas e governam os termos de uso. A maior parte dos usuários com computadores infectados por adware e spyware concorda em instalar os programas ao clicar em “Aceito” no pé dos EULAs que acompanham software shareware e outros programas gratuitos.

## EXTENSÃO .PFX

Extensão de arquivo associada a todos os Certificados Digitais exportados do navegador Microsoft Internet Explorer que incluem as Chaves Pública/Privada em formato PKCS #12.

## EXTENSÃO .P12

Extensão de arquivo associada a todos os Certificados Digitais exportados do navegador Mozilla Firefox ou Netscape que incluem as Chaves Pública/Privada em formato PKCS #12.

#### FERRAMENTA DE ADMINISTRAÇÃO DE CHAVES DA AUTORIDADE CERTIFICADORA CA KEY MANAGEMENT TOOL

Componente do Centro de Processamento utilizado para testar e inicializar os cartões Luna, gerar pares de chaves, certificados e solicitações de certificados.

#### FEDERAL INFORMATION PROCESSING STANDARDS – FIPS

Correspondem aos padrões e diretrizes desenvolvidos e publicados pelo NIST (National Institute of Standards and Technology) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST desenvolve os padrões e diretrizes FIPS quando há requisitos obrigatórios do governo federal, como segurança e interoperabilidade, e não há padrões ou soluções industriais aceitáveis.

#### FIPS 140

O Federal Information Processing Standards 140 é um padrão do governo dos Estados Unidos para implementações de módulos de criptografia, ou seja, hardware e software para cifrar e decifrar dados ou realizar outras operações criptográficas (como geração ou verificação de assinaturas digitais). Encontra-se atualmente na versão 2 – a versão 3 está sendo elaborada pelo NIST.

#### FRASE DE IDENTIFICAÇÃO CHALLENGE PHRASE

Sequência de números e/ou letras criada por um solicitante de certificado no momento da solicitação e utilizada mais tarde para renovar e revogar o Certificado Digital, conforme exigido pela DPC. A frase de identificação é também utilizada por um detentor de partição secreta para autenticar a si próprio perante o emissor das partições secretas.

#### FONTE CONFIÁVEL DE TEMPO – FCT

É a denominação dada ao Relógio Atômico localizado no Observatório Nacional.

## GERAÇÃO DE PAR DE CHAVES

Processo de criação de um par de chaves (Chave Privada e Chave Pública), sendo normalmente executado na solicitação de um Certificado Digital.

## GERENCIAMENTO DE CERTIFICADO

É a forma como uma Autoridade Certificadora, baseada em sua Declaração de Práticas de Certificação (DPC), Política de Certificados (PC) e Política de Segurança (PS), atua na emissão, renovação e revogação de certificados, bem como na emissão e publicação da sua Lista de Certificados Revogados.

## HASH

É o resultado da ação de algoritmos que fazem o mapeamento de uma sequência de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor conhecido como resultado hash, de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão). Faz com que o processo reverso também não seja realizável (dado um hash, não é possível recuperar a mensagem que o gerou).

## HIERARQUIA DE CERTIFICADOS

Estrutura de validade de certificados que permite verificar se o emissor de um Certificado Digital é confiável. Os certificados são emitidos e assinados por outros certificados, localizados em posição superior na hierarquia. A validade de um determinado certificado é estabelecida pela respectiva validade do certificado anterior.

## HARDWARE SECURE MODULE - HSM

É um dispositivo baseado em hardware que gera, guarda e protege chaves criptográficas, além de ter a capacidade de executar operações criptográficas - como assinatura digital.

## INFRAESTRUTURA DE CHAVES PÚBLICAS - ICP PKI (PUBLIC KEY INFRASTRUCTURE)

São as técnicas, arquitetura, organização, práticas e os procedimentos que suportam, em conjunto, a implementação e a operação de um sistema de certificação baseado em criptografia de Chave Pública.

## INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP-BRASIL

É um conjunto de técnicas, arquitetura, organização, práticas e procedimentos implementado pelas organizações governamentais e privadas brasileiras que suportam, em conjunto, a implementação e a operação de um sistema de certificação. Tem como objetivo estabelecer os fundamentos técnicos e metodológicos de um sistema de Certificação Digital baseado em criptografia de Chave Pública para garantir a autenticidade, integridade e validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem Certificados Digitais, bem como a realização de transações eletrônicas seguras.

A ICPBrasil foi criada pela Medida Provisória 22002, de 24.08.2001, e está regulamentada pelas Resoluções do Comitê Gestor da ICP-Brasil, disponíveis no site [www.iti.gov.br](http://www.iti.gov.br).

## INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI

É uma autarquia federal vinculada à Casa Civil da Presidência da República e uma Autoridade Certificadora Raiz da ICP-Brasil. É a primeira autoridade da Cadeia de Certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

## INTEGRIDADE

Garantia oferecida ao usuário de que um documento eletrônico, mensagem ou conjunto de dados não foi alterado intencionalmente ou acidentalmente por pessoas não autorizadas durante sua transferência entre sistemas ou computadores.

## INTEGRIDADE DE DADOS

### DATA INTEGRITY

Situação na qual é possível comprovar que um conjunto de dados não foi adulterado ou destruído sem autorização durante sua transferência entre sistemas ou computadores.

## IRRETRATABILIDADE

Consiste basicamente em um mecanismo para garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a autoria.

## KEY LOGGER

Uma forma de spyware que registra cada toque no teclado ou outra atividade no sistema. Esses programas podem coletar números de cartão de crédito, senhas ou outros dados delicados e transmiti-los a terceiros.

## LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL - LDAP

LDAP é o protocolo de serviço de diretório usado na Internet. É um padrão aberto, produzido pela IETF (Internet Engineering Task Force), que roda sobre o TCP/IP. O LDAP é baseado no modelo cliente/servidor - os clientes LDAP conectam-se com os servidores para obter dados contidos no diretório e os servidores respondem às requisições. Um ou mais servidores LDAP contêm as informações.

## LEITORA DE CARTÃO INTELIGENTE

Hardware instalado no computador: utiliza a interface serial ou USB e serve para efetuar leituras de cartões inteligentes (*smart cards*).

## LISTA DE CERTIFICADOS REVOGADOS – LCR CERTIFICATE REVOCATION LIST - CRL

Lista assinada digitalmente por uma Autoridade Certificadora (AC) e publicada periodicamente ou sob demanda, contendo certificados que foram suspensos ou revogados antes de suas respectivas datas de expiração. A lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.

## LISTA DE CONTROLE DE ACESSO ACCESS CONTROL LIST - ACL

Lista de indivíduos ou entidades com permissão de acesso a certas áreas específicas de um servidor, rede, aplicação de Internet ou instalações físicas.

## MÉTODO DE AUTENTICAÇÃO

Processo de verificação da identidade de um solicitante e da veracidade dos dados da solicitação como parte do processo de aprovação de uma solicitação de Certificado Digital. O serviço de MPKI Certisign oferece três métodos de autenticação: Autenticação Manual, Autenticação por Passcode e Autenticação Automatizada.

## MÓDULO CRIPTOGRÁFICO CRYPTOGRAPHIC MODULE (CRYPTOMODULE)

Software ou hardware (vide HSM) que fornece serviços criptográficos, como criptografia, decifração, geração de chaves, geração de números aleatórios ou suporte para cartões inteligentes (*smart cards*).

## MD5 MESSAGE-DIGEST ALGORITHM 5

É uma função de hash espalhamento unidirecional inventada por Ron Rivest. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sido descobertos contra a função hashing prévia: a MD4.

O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir um valor hash de somente 128 bits causa maior preocupação.

## NÃO-REPÚDIO

Não-repúdio ou não-recusa é a garantia de que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica não poderá posteriormente negar sua autoria, visto que somente aquela Chave Privada poderia ter gerado aquela assinatura digital. Deste modo, ao menos de um uso indevido do Certificado Digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação. Transações digitais estão sujeitas a fraude quando sistemas de computador são acessados indevidamente ou infectados por cavalos de tróia ou vírus. Assim, os participantes podem, potencialmente, alegar fraude para repudiar uma transação.

## NAVEGADOR DE INTERNET WEB BROWSER

Aplicativo utilizado para visualizar arquivos HTML, VRML, textos, arquivos de áudio, animação, vídeos e/ou correio eletrônico pela Internet. Entre os principais navegadores disponíveis no mercado estão: Microsoft Internet Explorer, Netscape Navigator e Opera.

## NOME COMUM COMMON NAME

Atributo especificado dentro do campo Assunto (Subject), que faz parte do Nome Distinto (Distinguished Name) de um certificado.

Para Certificados de Servidores Web, o Nome Comum é o FQDN (Fully Qualified Domain Name). O Nome Comum é composto por host + domínio. Um Nome Comum válido por exemplo seria [www.certisign.com.br](http://www.certisign.com.br), sendo www o host e o certisign.com.br o domínio.

Para um Certificado de Assinatura de Software, o Nome Comum é o nome da organização. Em certificados para pessoa física, o Nome Comum é composto pelo prenome e sobrenome do assinante. Já nos certificados para pessoa jurídica, o Nome Comum é composto pelo nome da organização.

## NÚMERO DE SÉRIE DO CERTIFICADO SERIAL NUMBER

Um valor que identifica de forma unívoca um certificado emitido por uma Autoridade Certificadora.

## OBJECT IDENTIFIER – OID

Um OID é um número único que identifica uma classe de objetos ou o atributo em um diretório ou combinação de diretórios. OIDs são definidos por entidades emissoras e formam uma hierarquia. Um OID é representado por um conjunto de números decimais separados por pontos (ex.: 1.2.3.4).

OIDs são usados extensivamente em certificados de formato X.509 como, por exemplo, para designar algoritmos criptográficos empregados, políticas de certificação e campos de extensão. Praticamente toda implementação de ICP usando este formato requer o registro de novos OIDs, em particular uma que designe a política de certificação que estabelece seu regime regulatório básico. É crucial que os OIDs sejam obtidos dos legítimos responsáveis pelos arcos, para se evitar incompatibilidades e colisões.

Nos certificados da ICP-Brasil, os OIDs utilizados para identificar as Políticas de Certificados e Declaração de Práticas de Certificação das Autoridades Certificadoras são atribuídos pelo ITI durante o processo de auditoria da Autoridade Certificadora e obedecem a seguinte lógica:

2.16.76.1.1.n – OID para Declarações de Práticas de Certificação;

2.16.76.1.2.n – OID para Políticas de Certificados;

2.16.76.1.3.n e 2.16.76.1.4.n – OID usados para permitir a inclusão no certificado de outros dados de pessoas físicas e jurídicas, como CNPJ, CPF, título de eleitor e categoria profissional.

## OBSERVATÓRIO NACIONAL – ON

Vinculado ao Ministério da Ciência e Tecnologia, integrante do Sistema Nacional de Metrologia – Sinmetro, o ON é o responsável legal pela geração, conservação e disseminação da Hora Legal Brasileira, com rastreabilidade metrológica ao BIPM (Bureau International des Poids et Mesures). Mantém e opera o Relógio Atômico, que é a Fonte Confiável do Tempo (FCT), a partir da qual se determina a Hora Legal Brasileira.

## ONLINE CERTIFICATE STATUS PROTOCOL - OCSP

O Protocolo Online para verificação de estado de certificados, OCSP é um dos dois esquemas comuns para verificar se um Certificado Digital não se encontra revogado. O outro método é a Lista de Certificados Revogados (ver LCR). Através do OCSP, qualquer aplicação pode fazer consultas a um serviço que checa, diretamente no Banco de Dados da Autoridade Certificadora, o status de um determinado certificado. As respostas emitidas por este serviço são individuais (uma para cada certificado) e são assinadas digitalmente, a fim de garantir sua confiabilidade. Dessa maneira, a lacuna entre o momento da revogação e a emissão da próxima LCR deixa de existir, já que, uma vez que seja marcado como revogado no banco de dados da Autoridade Certificadora, a próxima resposta OCSP já apresentará esse status, eliminando a possibilidade de um acesso não-autorizado desta natureza.

## ONSITE FOR MULTIPLE SERVER IDS

Solução de gerenciamento do ciclo de vida de Certificados para Servidores Web.

## ONSITE FULL

Solução de gerenciamento do ciclo de vida de certificados para usuário final. O Onsite Full é recomendado para ambientes que necessitem de mais de 1.000 Certificados Digitais.

#### ONSITE LITE

Solução de gerenciamento do ciclo de vida de certificados para usuário final. O Onsite Lite é recomendado para ambientes que necessitem de até 1.000 Certificados Digitais.

#### OPENSSL

É uma biblioteca de código aberto para implementação dos protocolos SSL e TLS. A biblioteca (escrita na linguagem C) implementa as funções básicas de criptografia e disponibiliza várias funções utilitárias. O OpenSSL está disponível para a maioria dos sistemas do tipo Unix, incluindo Linux, Mac OS X, para as quatro versões do BSD de código aberto e também para o Microsoft Windows.

#### PERSONAL IDENTIFICATION NUMBER – PIN

É uma seqüência de números e/ou letras (senha) usados para liberar o acesso ao conteúdo (Chave Privada) de um hardware criptográfico.

#### PERSONAL IDENTIFICATION NUMBER UNBLOCKING KEY - PUK

É uma seqüência de números e/ou letras (senha) usados para desbloquear o Número de Identificação Pessoal (PIN), o qual normalmente fica bloqueado após várias tentativas inválidas. Como o PIN, a senha PUK deve ser guardada de forma segura, pois ambas permitem, em dispositivos como *tokens*, o acesso à Chave Privada de um titular de certificado.

#### PKCS (PUBLIC KEY CRYPTOGRAPHIC STANDARD)

Padrões de criptografia de Chave Pública. São especificações produzidas pelos Laboratórios RSA em cooperação com desenvolvedores de sistemas seguros de todo o mundo com a finalidade de acelerar a distribuição da criptografia de Chave Pública.

#### PKCS#7 (CMS)

O padrão CMS descreve uma sintaxe genérica para dados que podem ser submetidos a funções criptográficas, como assinatura e envelopagem digital. Permite recursividade, com alinhamento de envelopes e *wrappers*, e associação de atributos arbitrários, como selo temporal ou contra-assinatura, à mensagem no processo de autenticação por assinatura. Casos particulares oferecem meios de disseminação de certificados e CRLs.

O padrão CMS pode dar suporte a uma variedade de arquiteturas de gerenciamento de chaves baseadas em ICP, como aquela proposta para o padrão PEM na RFC 1422. Entretanto, topologias, modelos de confiança e políticas de certificação para ICPs estão fora do seu escopo. Valores produzidos pelo padrão estão destinados à codificação DER, ou seja, para transmissão e armazenagem na forma de cadeias de octetos de comprimento não necessariamente conhecidos de antemão. Na ICP-Brasil, é largamente utilizado na assinatura digital.

#### PKCS#10

Descreve uma sintaxe padrão para requisição de um Certificado Digital.

#### PKCS#12

Descreve uma sintaxe para a transferência de informação de identificação pessoal, incluindo Chaves Privadas, certificados, chaves secretas e extensões. É uma norma muito útil, uma vez que é utilizada por diversas aplicações (ex: IE e Mozilla) para importar e exportar esse tipo de informação. Suporta a transferência de informação pessoal em diferentes condições de manutenção da privacidade e integridade. O grau de segurança mais elevado prevê a utilização de assinaturas digitais e cifras assimétricas para proteção da informação.

#### PUBLIC KEY INFRASTRUCTURE – PKI

Ver Infraestrutura de Chaves Públicas – ICP.

#### POLÍTICA DE CERTIFICADOS – PC

É um conjunto de regras que indica a aplicação de um certificado para uma comunidade particular e/ou classe de aplicação com requisitos de segurança. A Política de Certificado pode ser usada por um usuário certificado para ajudar a decidir se um certificado é confiável o suficiente para uma dada aplicação.

## POLÍTICA DE CARIMBO DE TEMPO - PCT

Conjunto de normas que indicam a aplicabilidade de um carimbo de tempo para uma determinada comunidade e/ou classe de aplicação com requisitos comuns de segurança.

## POLÍTICA DE SEGURANÇA – PS

É um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades.

## PROGRAMA CGI

### COMMON GATEWAY INTERFACE PROGRAM

É um padrão que determina a forma de comunicação entre o servidor Web e uma outra aplicação rodando neste servidor. Qualquer linguagem de programação que segue esse padrão pode ser utilizada para criar uma aplicação CGI.

Um programa CGI pode ser um programa executável ou um script que fica localizado dentro do servidor Web em uma pasta onde o servidor possa encontrá-lo. Várias linguagens podem escrever um programa CGI, desde que a linguagem escolhida seja capaz de fazer com que o servidor Web converse com o programa CGI - lendo em um input e escrevendo em um output.

## PROVEDOR DE SERVIÇOS CRIPTOGRÁFICOS - CSP

### CRYPTOGRAPHIC SERVICE PROVIDER

É uma biblioteca de software que implementa a Cryptographic Application Programming Interface (CAPI). CSPs implementam funções de codificação e decodificação que os programas de aplicação de computador podem usar para autenticação segura de usuário, geração de pares de chaves, encriptação ou assinaturas digitais. CSPs são executados basicamente como um tipo especial de DLL (Dynamic-Link Library), com limitações especiais no carregamento e no uso.

## PERSONAL TRUST AGENT - PTA

É um componente da MPKI VeriSign que permite controle de acesso, assinatura digital de formulários e a administração de chaves e certificados.

## REGISTRATION AUTHORITY - RA

Componente dos Serviços de MPKI (e MPKI Full) Certisign que substitui o processo de aprovação manual de solicitações de certificados por um software personalizado, mantendo todo o processo dentro das instalações da organização. Disponível somente com os serviços de MPKI (e MPKI Full), o RA aprova as solicitações de certificados sem a participação do administrador, comparando os dados da solicitação com informações previamente cadastradas pela organização assinante dos serviços de MPKI.

## RENOVAÇÃO DE CERTIFICADOS

É o processo para obter um certificado novo antes que o certificado existente tenha expirado. Na ICP-Brasil, é obrigatória a geração de novas chaves criptográficas para cada certificado emitido.

## REPOSITÓRIO

É um diretório confiável e acessível online, mantido por uma Autoridade Certificadora, para publicar sua Declaração de Práticas de Certificação (DPC), Políticas de Certificado (PC), Política de Segurança (PS), Lista de Certificados Revogados (LCR) e endereços das instalações técnicas das Autoridades de Registro vinculadas.

## RETIRADA

Processo pelo qual um solicitante de certificado acessa um endereço digital fornecido pela Autoridade Certificadora para retirar um Certificado Digital pendente, após o envio da solicitação e respectiva aprovação. Depois de retirado, o certificado passa a ser considerado emitido.

## REVOGAÇÃO DE CERTIFICADOS

Encerramento da validade de um Certificado Digital antes do prazo previsto. Pode ocorrer por iniciativa do usuário, da Autoridade de Registro, da Autoridade Certificadora ou da Autoridade Certificadora Raiz.

## REQUEST FOR COMMENTS - RFC

RFCs são documentos técnicos ou informativos que discutem os mais diversos aspectos relacionados à Internet. Os assuntos variam desde especificações, padrões e normas técnicas, até questões históricas acerca

da rede mundial de computadores. Os RFCs são documentos públicos e qualquer pessoa tem acesso a eles, podendo ler, comentar, enviar sugestões e relatar experiências sobre o assunto. Pode se pesquisar os RFCs no site:

<http://www.faqs.org/rfcs>.

## RSA

RSA é um algoritmo de criptografia de dados que deve o seu nome a três professores do Instituto MIT (fundadores da atual empresa RSA Data Security, Inc.): Ron Rivest, Adi Shamir e Len Adleman. Eles inventaram este algoritmo. Atualmente é a mais bem sucedida implementação de sistemas de chaves assimétricas, e fundamenta-se em teorias clássicas dos números. Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital, e uma das grandes inovações em criptografia de Chave Pública.

## SECURE HASH ALGORITHM – SHA1

O Secure Hash Algorithm, uma função de espalhamento unidirecional inventada pela NSA, gera um valor hash de 160 bits a partir de um tamanho arbitrário de mensagem. SHA-1 foi considerado o sucessor do algoritmo MD5 (Message-Digest algorithm 5).

## SHA2 FAMILY SECURE HASH ALGORITHM - SHA224, SHA256, SHA384 E SHA512

O NIST (National Institute of Standards and Technology) publicou quatro funções adicionais da família SHA, cada uma com valores hash maiores, conhecidos coletivamente como SHA2.

As variantes individuais são nomeadas através de seus comprimentos de hash (em bits): SHA224, SHA256, SHA384 e SHA512.

O SHA224 foi definido para combinar o comprimento da chave com duas chaves TripleDES. SHA256 e SHA512 são funções de hash computadas com palavras de 32 bits e 64 bits, respectivamente. Usam quantidades diferentes de deslocamento e constantes adicionais, mas suas estruturas são virtualmente idênticas, diferindo somente no número de voltas. SHA224 e SHA384 são simplesmente versões truncadas das duas primeiras, computadas com valores iniciais diferentes.

## SELO CRONOLÓGICO DIGITAL

## DIGITAL TIMESTAMP

Serviço que registra a data e a hora correta de um ato, além da identidade da pessoa ou equipamento que enviou ou recebeu o Selo Cronológico. O Selo Cronológico Digital cria uma confirmação assinada digitalmente e à prova de fraude sobre a existência de uma transação ou documento específico.

#### SELO DE SITE SEGURO SECURE SITE SEAL

Símbolo que indica um ambiente seguro para transações digitais. A presença do selo demonstra que um site possui um Certificado de Servidor de VeriSign ou ICP-Brasil. Além disso, o selo funciona como link para uma página segura que fornece detalhes sobre o Certificado Digital e o programa Certisign de Sites Seguros.

#### SENHA

Informações confidenciais de autenticação que, em geral, são compostas por uma série de caracteres conhecidos apenas pelo usuário – usados para dar acesso a um recurso computacional.

#### SERVIDOR DO BANCO DE DADOS DATABASE SERVER

Servidor da área interna do Centro de Processamento que armazena todas as informações relativas a solicitações de inscrição para certificados (como os certificados emitidos ou revogados).

#### SERVIDOR DE CARIMBO DE TEMPO – SCT

Dispositivo único constituído por hardware e software que gera os carimbos de tempo sob o gerenciamento da Autoridade de Carimbo de Tempo. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.

#### SIGILO

Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas. Os titulares de certificados de assinatura digital emitidos pela Autoridade Certificadora são responsáveis pela geração, manutenção e pela garantia do sigilo de suas respectivas Chaves

Privadas, bem como pela divulgação ou utilização indevidas dessas mesmas chaves.

## SIGNATÁRIO

É a pessoa/entidade que cria uma assinatura digital para uma mensagem com a intenção de autenticá-la.

## SOLICITAÇÃO DE ASSINATURA DE CERTIFICADO - CSR CERTIFICATE SIGNING REQUEST

É um arquivo, gerado por um software ou hardware, que contém as informações para a solicitação de um Certificado Digital junto a uma Autoridade Certificadora.

O CSR contém as informações do solicitante (nome, departamento, cidade, estado, país) e a Chave Pública.

## SMART CARD

É um tipo de cartão plástico (semelhante a um cartão de crédito) com um ou mais microchips embutidos, capaz de armazenar e processar dados. Um smart card pode ser programado para desempenhar inúmeras funções, inclusive pode ter capacidade de gerar Chaves Públicas e Privadas e de armazenar Certificados Digitais. Pode ser utilizado tanto para controle de acesso lógico como para controle de acesso físico.

## SISTEMA DE PAGAMENTOS BRASILEIRO - SPB

Sistema responsável pela interação entre o Banco Central, o governo, as instituições financeiras, as empresas e até mesmo as pessoas físicas. Gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, ligando as Instituições Financeiras credenciadas ao Banco Central do Brasil ([www.bcb.gov.br](http://www.bcb.gov.br)). Utiliza Certificados Digitais para autenticar e verificar a identidade dos participantes em todas as operações realizadas.

## SPYWARE

Software que monitora hábitos no computador, como padrões de navegação na web, e transmite a informação de terceiros, às vezes menciona autorização ou consentimento do usuário.

## SECURE SOCKETS LAYER - SSL

Protocolo de segurança que provê privacidade na comunicação através da Internet. O Protocolo permite que aplicativos cliente e servidor comuniquem-se utilizando mecanismos criados para proteger o sigilo e a integridade do conteúdo que trafega pela Internet. Desenvolvido pela Netscape para transmitir documentos privativos pela Internet.

## S/MIME

Especificação para segurança de e-mail que implementa uma sintaxe de mensagem criptografada num ambiente de Internet MIME (método seguro de envio de e-mails que utiliza o sistema de criptografia Rivest-Shamir-Adleman). Esse método foi sugerido pela RSA como padrão.

## TERCEIRO DE CONFIANÇA

Um terceiro de confiança, em geral independente e imparcial, que contribui para a máxima segurança e confiabilidade das informações permutadas entre os computadores. A Certisign é um exemplo.

## TERMOS DE ADESÃO

É o contrato executado entre o assinante e uma Autoridade Emissora para a provisão dos serviços de certificação de acordo com sua Declaração de Práticas de Certificação (DPC).

## TERMO DE RESPONSABILIDADE

Termo assinado por uma pessoa física, responsável pelo uso do certificado, quando o titular do certificado é uma organização. No termo, estão estabelecidas as condições de uso do certificado.

## TERMO DE TITULARIDADE

Termo assinado pelo titular do Certificado Digital emitido para pessoa física ou jurídica no qual são estabelecidas as condições de uso do mesmo.

## TEXTO CIFRADO CIPHERTEXT

Conjunto de dados criptografados e ininteligíveis.

## TITULAR DO CERTIFICADO

Uma pessoa, física ou jurídica, para a qual um certificado tenha sido emitido, que é capaz de usá-lo e que foi autorizada a usá-lo, possuindo a Chave Privada correspondente à Chave Pública incorporada ao certificado.

## TOKEN

Hardware para armazenamento do Certificado Digital de forma segura, sendo seu funcionamento parecido com o smart card - tem conexão com o computador via USB.

## TRIPLE DES (3DES)

O 3DES é uma variação do algoritmo DES (Data Encryption Standard), utilizado em três ciframentos sucessivos - pode empregar uma versão com duas ou com três chaves diferentes. Seu tamanho de chave é de 112 ou 168 bits.

## TROJAN ou TROJAN HORSE

O cavalo de tróia é um programa que parece ter uma função útil, como um game, mas inclui recursos escondidos e potencialmente maliciosos. Às vezes driblam mecanismos de segurança para tapear os usuários e fazê-los autorizar o acesso aos computadores.

## UNIFORM RESOURCE LOCATOR - URL

Um mecanismo padronizado para identificar e localizar certos cadastros e outros recursos disponíveis em uma rede, seja a Internet, uma rede corporativa ou uma Intranet. A maioria das URLs aparece na forma familiar de endereços de sites, como [www.certisign.com.br](http://www.certisign.com.br).

## VALIDADE DE LCR

Período de tempo em que a Lista de Certificados Revogados (LCR) está com sua data de validade operacional. As LCRs possuem prazo máximo de validade de acordo com o tipo de certificado previsto na ICP-Brasil.

## VALIDADE DO CERTIFICADO

Período de tempo em que o certificado está com sua data de validade operacional. Os certificados possuem prazo máximo de validade de acordo com o tipo de certificado previsto na ICP-Brasil.

## VeriSign Trust Network - VTN

Rede de Confiança da VeriSign.

## X.509

Recomendação ITUT, a especificação X.509 é um padrão que especifica o formato dos Certificados Digitais de tal maneira que se possa amarrar firmemente um nome a uma Chave Pública, permitindo autenticação forte. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseadas em nomes distintos para localização. Na ICP-Brasil utilizam-se certificados no padrão X509 V3.

## WORLD WIDE WEB (WWW)

Um sistema de informações distribuído com base em hipertexto no qual o usuário pode criar, editar ou procurar documentos; uma publicação gráfica de documento e de acesso médio; e uma coleção de documentos ligados residentes na Internet.