Segurança da Informação

Estudo Dirigido

Assinatura e Certificação Digital

1. Introdução

Este estudo tem como propósito oferecer a oportunidade para conhecer o processo de Assinatura Digital e os Certificados Digitais, tecnologias fundamentais para a segurança da informação em ambientes digitais. Através da criptografia de chave pública, essas ferramentas proporcionam autenticação, integridade e não-repúdio, elementos essenciais em transações eletrônicas. Este estudo aborda os aspectos técnicos dessas tecnologias, a infraestrutura legal e institucional no Brasil, e seu papel em diversos campos como mercado financeiro, comércio eletrônico e meio jurídico.

2. Contextualização

A era digital transformou a forma como interagimos, comunicamos e realizamos transações. Em meio a esse cenário, a segurança das informações se tornou crucial, exigindo soluções robustas para garantir a autenticidade, integridade e não repúdio de dados eletrônicos. Nesse contexto, a assinatura digital e os certificados digitais emergem como ferramentas essenciais para a segurança digital, possibilitando a realização de diversas atividades de forma segura e confiável no ambiente online.

Para entender e utilizar de forma adequada essas ferramentas, é necessário conhecer alguns termos e elementos. Mas, afinal, o que é a **Assinatura Digital**? É um mecanismo de autenticação que permite ao receptor de uma mensagem verificar a autenticidade da identidade do remetente e a integridade do conteúdo enviado. E o que é o **Certificado Digital**? É um documento eletrônico que contém dados de uma entidade (pessoa física, jurídica, máquina) associando uma chave pública à entidade portadora da chave privada correspondente.

2.1. Criptografia de Chave Pública

A criptografia de chave pública, também conhecida como criptografia assimétrica, utiliza um par de chaves, uma pública e uma privada. A chave pública pode ser divulgada, enquanto a chave privada deve ser mantida em segredo pelo proprietário. Esse mecanismo é a base para a assinatura digital, pois a mensagem assinada com a chave privada pode ser verificada por qualquer pessoa que tenha acesso à chave pública correspondente. Para assinar digitalmente um documento, o signatário utiliza sua chave privada para gerar uma assinatura criptográfica que é anexada ao documento. Ao receber o documento assinado, o destinatário utiliza a chave pública do signatário para verificar a autenticidade e integridade do documento.

Figura 1 - Criptografia de Chave Pública (ou Assimétrica).

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

3. ASSINATURA DIGITAL

As assinaturas digitais são as primitivas de chave pública da autenticação de mensagens. É comum usarmos assinaturas manuscritas em documentos e mensagens manuscritos ou digitados, usadas para vinculá-los ao signatário. Da mesma forma uma assinatura digital é uma técnica que vincula uma pessoa ou entidade aos dados digitais. Essa ligação pode ser verificada independentemente pelo destinatário, bem como por qualquer um interessado em fazê-lo.

3.1. O processo de Assinatura Digital

Assinatura digital é um valor criptográfico calculado a partir dos dados e uma chave secreta conhecida apenas pelo signatário. O receptor da mensagem precisa ter certeza de que a mensagem pertence ao remetente, sem poder negar a origem dessa mensagem. Esse requisito é crucial no mundo dos negócios para manter a confiança nas negociações. A Figura 2 apresenta o processo completo, cujos detalhes são descritos nos itens a seguir.

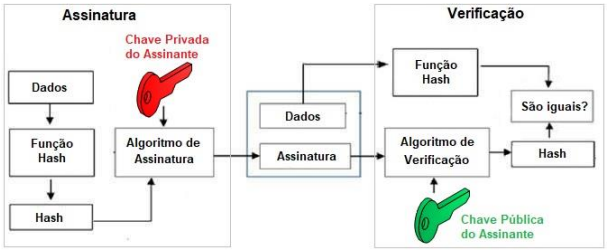

Figura 2 - O processo de Assinatura Digital

Remetentes e destinatários do processo têm seu par de chaves público-privado. Geralmente, os pares de chaves usados para criptografia / descriptografia e assinatura / verificação são diferentes. A chave privada usada para assinatura é referida como chave de assinatura e a chave pública como chave de verificação. O processo então é executado com essas etapas:

1. O signatário fornece os dados da mensagem para a função hash e gera hash de dados;
2. O hash e a chave de assinatura são então submetidos ao algoritmo de assinatura, que produz a assinatura digital em determinado hash;
3. A assinatura é anexada aos dados e ambos são enviados para o verificador;
4. O verificador fornece a assinatura digital e a chave de verificação ao algoritmo de verificação;
5. O algoritmo de verificação fornece um valor como saída;
6. O verificador também executa a mesma função de hash nos dados recebidos para gerar o valor de hash;
7. Para a verificação, esse valor de hash dos dados e a saída do algoritmo de verificação são comparados;
8. Com base no resultado da comparação, o verificador decide se a assinatura digital é válida;
9. Como a assinatura digital é criada pela chave privada do assinante e ninguém mais pode ter essa chave, o signatário não pode repudiar a assinatura dos dados no futuro.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

Deve-se notar que, em vez de assinar os dados diretamente com o algoritmo da assinatura, isso é feito com o hash dos dados. Como o hash de dados é uma representação única de dados, basta assinar o hash no lugar dos dados. A razão mais importante do uso de hash em vez de dados diretamente para assinatura é a eficiência do processo. Considerando que o RSA seja usado como o algoritmo de assinatura, e conforme tratado no tema sobre criptografia de chave pública, o processo de criptografia / assinatura usando RSA envolve exponenciação modular. Assinar grandes conjuntos de dados por meio de exponenciação modular é computacionalmente caro e demorado. O hash dos dados é um resumo relativamente pequeno dos dados, portanto, assinar um hash é mais eficiente do que assinar todos os dados.

3.2. Os objetivos da Assinatura Digital

A assinatura digital usando criptografia de chave pública é considerada uma ferramenta muito importante e útil para alcançar a segurança da informação. Além da capacidade de garantir o não repúdio à mensagem, a assinatura digital também fornece autenticação de mensagens e integridade de dados, como detalhado a seguir:

- **Autenticação da mensagem**: Quando o verificador valida a assinatura digital usando a chave pública de um remetente, ele tem a garantia de que a assinatura foi criada apenas pelo remetente que possui a chave privada secreta correspondente e mais ninguém.
- **Integridade de dados**: No caso de acesso indevido e modificação dos dados, a verificação da assinatura digital no final do receptor falhará. O hash de dados modificados e a saída fornecida pelo algoritmo de verificação não corresponderão. Portanto, o receptor pode negar com segurança a mensagem, assumindo que a integridade dos dados foi violada.
- **Não repúdio**: Como se presume que somente o signatário tem o conhecimento da chave de assinatura, somente ele poderá criar uma assinatura exclusiva em um determinado dado. Assim, o destinatário pode apresentar dados e a assinatura digital a terceiros como evidência, em caso de dúvida da autenticidade da origem.

Ao adicionar a criptografia de chave pública ao processo de assinatura digital, criamos um sistema criptográfico que pode fornecer quatro elementos essenciais à segurança: privacidade, autenticação, integridade e não repúdio.

4. INFRAESTRUTURA DE CHAVES PÚBLICAS

A principal característica da infraestrutura de chave pública – ICP, ou Public Key Infrastructure – PKI, é que ela usa um par de chaves para prover os serviços de segurança subjacente. Como já vimos, o par de chaves é composto por chave privada e chave pública. Como as chaves públicas estão em domínio aberto podem ser violadas, é necessário estabelecer e manter algum tipo de infraestrutura confiável para gerenciar essas chaves.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

4.1. Gerenciamento de chaves

Já repetimos diversas vezes que a segurança de qualquer sistema criptográfico depende de quão seguramente suas chaves são gerenciadas. Sem procedimentos seguros para o manuseio de chaves criptográficas, os benefícios do uso de esquemas criptográficos fortes são potencialmente perdidos. Observa-se que modelos criptográficos raramente são comprometidos através de pontos fracos em seu design. No entanto, eles geralmente são comprometidos por meio do gerenciamento inadequado de chaves. Os aspectos mais importantes da gestão de chaves são os seguintes:

1. Chaves criptográficas não são nada mais que dados especiais
2. Gerenciamento de chaves refere-se à administração segura de chaves criptográficas;
3. O gerenciamento de chaves lida com todo o ciclo de vida da chave, conforme mostrado na Figura 3;
4. Existem dois requisitos específicos de gerenciamento de chaves para criptografia de chave pública:
   4.1. O segredo das chaves privadas: durante todo o ciclo de vida da chave, as chaves secretas devem permanecer em segredo de todas as partes, exceto aquelas que são proprietárias e estão autorizadas a usá-las.
   4.2. A garantia das chaves públicas. Na criptografia de chave pública, as chaves públicas estão em ambiente aberto e são dados públicos. Por padrão, não há garantias que uma chave pública está correta, a quem ela pode ser associada ou para o que ela pode ser usada. Então o gerenciamento de chaves públicas deve visar a garantia do propósito das chaves públicas.

O requisito mais importante da garantia da chave pública pode ser alcançado por meio da infraestrutura de chave pública - PKI, um dos principais sistemas de gerenciamento para apoiar a criptografia de chave pública.

Figura 3 - O ciclo de vida das chaves

A PKI fornece garantia de chave pública. Ele fornece a identificação de chaves públicas e sua distribuição. Uma estrutura de PKI compreende os seguintes componentes:

- Certificado de chave pública, comumente chamado de "certificado digital";
- Tokens de chave privada;

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

- Autoridade Certificadora;
- Autoridade de Registro;
- Sistema de Gerenciamento de Certificados.

4.2. Autoridades Certificadoras (CA)

As Autoridades Certificadoras são entidades de confiança responsáveis por emitir, gerenciar, revogar e renovar certificados digitais. Algumas das CAs mais conhecidas:

- **Let's Encrypt (https://letsencrypt.org/pt-br/)**;
- **DigiCert (https://www.digicert.com/pt)**;
- **Comodo (https://comodosslstore.com/)**;
- **Symantec:** Anteriormente uma das líderes do mercado, muitos de seus serviços de certificação digital agora são administrados pela DigiCert;
- **Serasa Experian (https://serasa.certificadodigital.com.br/);**
- **ITI (https://www.gov.br/iti/pt-br);**
- **Certificado Digital Positivo (https://positivoon.com.br/);**
- **GeoTrust (https://www.geotrust.com/);**

Importante: Ao escolher uma AC, é importante considerar fatores como confiabilidade, preço, suporte ao cliente e recursos adicionais oferecidos, como validação de extended validation (EV) e wildcards. É fundamental manter o seu certificado SSL atualizado para garantir a segurança do seu site. Certifique-se de instalar o certificado SSL corretamente no seu servidor web. Em caso de dúvidas, consulte a documentação da sua AC ou entre em contato com o suporte técnico.

A CA emite o certificado para um cliente e ajuda outros usuários a verificar o certificado. A CA assume a responsabilidade de identificar corretamente a identidade do cliente que está solicitando a emissão de um certificado, e garante que as informações contidas no certificado estejam corretas e as assina digitalmente.

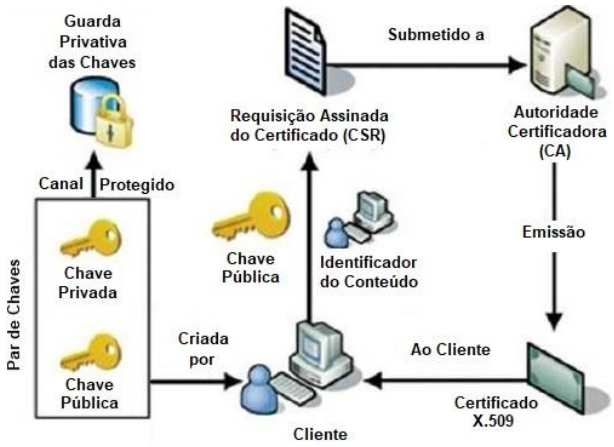

Figura 4 - Obtenção do Certificado Digital.

As principais funções de uma CA são:

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

- Geração dos pares de chaves: A CA pode gerar um par de chaves independentemente ou em conjunto com o cliente.
- Emissão de certificados digitais: A CA pode ser considerada o equivalente PKI de uma agência de passaportes: a CA emite um certificado depois que o cliente fornece as credenciais para confirmar sua identidade. Então a CA assina o certificado para impedir a modificação de suas informações.
- Publicação de certificados: A CA precisa publicar certificados para que os usuários possam encontrá-los. Existem duas maneiras de conseguir isso. Uma delas é publicar os certificados no equivalente de uma lista telefônica eletrônica. A outra é enviar seu certificado para as pessoas que você acha que podem precisar dele de uma forma ou de outra.
- Verificar certificados: A autoridade certificadora disponibiliza sua chave pública no ambiente para auxiliar na verificação de sua assinatura no certificado digital dos clientes.
- Revogação de certificados: Às vezes, a CA revoga o certificado emitido devido a algum motivo, como comprometimento da chave privada pelo usuário ou perda de confiança no cliente. Após a revogação, a CA mantém a lista de todos os certificados revogados disponíveis para o ambiente.

4.3. Classes de Certificados

Existem quatro classes típicas de certificados:

- Classe 1: Podem ser facilmente adquiridos através do fornecimento de um endereço de e-mail;
- Classe 2: Exigem informações pessoais adicionais a serem fornecidas;
- Classe 3: Só podem ser adquiridos após a verificação da identidade do solicitante;
- Classe 4: Usados por governos e organizações financeiras que precisam de níveis muito altos de confiança.

4.4. Autoridade de Registro (RA)

A CA pode usar uma Autoridade de Registro (Registration Authority - RA) terceirizada para executar as verificações necessárias da pessoa ou organização que solicita o certificado, para confirmar sua identidade. A RA pode parecer uma autoridade certificadora para o cliente, porém não assina o certificado emitido. O Sistema de Gerenciamento de Certificados (Certificate Management System - CMS) é o sistema de gestão pelo qual os certificados são publicados, temporariamente ou permanentemente suspensos, renovados ou revogados.

Os sistemas de gerenciamento de certificados normalmente não excluem certificados porque pode ser necessário provar seu status em um determinado momento, talvez por motivos legais. Uma CA juntamente com a RA associada executa sistemas de gerenciamento de certificados para poder controlar suas responsabilidades e obrigações.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

4.5. Token de chave privada

Enquanto a chave pública de um cliente é armazenada no certificado, a chave privada secreta associada pode ser armazenada no computador do proprietário da chave. Este método geralmente não é adotado. Se um invasor obtiver acesso ao computador, ele poderá obter acesso à chave privada com facilidade. Por esse motivo, uma chave privada é armazenada em um acesso seguro, vinculado ao token de armazenamento removível protegido por uma senha. Diferentes fornecedores costumam usar formatos de armazenamento diferentes e, por vezes, proprietários, para armazenar chaves. Por exemplo, o Entrust usa o formato proprietário .epf, enquanto a Verisign, GlobalSign e Baltimore usam o formato padrão .p12.

4.6. Hierarquia de CAs

Com as redes de comunicações globais da atualidade e a ampla gama de requisitos de segurança, não é viável ter apenas uma CA confiável, da qual todos os usuários obtêm seus certificados. E a disponibilidade de apenas uma CA pode causar dificuldades, tanto pelo desempenho quanto se a CA for comprometida por um ataque ou vazamento. Nesse caso, o modelo de certificação hierárquica é de interesse, pois permite que certificados de chave pública sejam usados em ambientes em que duas partes em comunicação não têm relações de confiança com a mesma CA.

A CA Raiz está no topo da hierarquia da CA e o certificado da CA raiz é um certificado auto assinado. As autoridades certificadoras secundárias, subordinadas diretamente à autoridade certificadora raiz, possuem certificados de autoridade certificadora assinados pela autoridade certificadora raiz. As autoridades certificadoras vinculadas às autoridades certificadoras subordinadas na hierarquia têm seus certificados de autoridade certificadora assinados pelas autoridades certificadoras subordinadas de nível superior, e assim sucessivamente.

As hierarquias da autoridade certificadora (CA) são refletidas nas cadeias de certificados. Uma cadeia de certificados rastreia um caminho de certificados de uma ramificação na hierarquia até a raiz da hierarquia. A verificação de uma cadeia de certificados é o processo de garantir que uma cadeia de certificados específica seja válida, corretamente assinada e confiável. O procedimento descrito a seguir verifica uma cadeia de certificados, começando com o certificado apresentado para autenticação:

1. Um cliente cuja autenticidade está sendo verificada fornece seu certificado, geralmente junto com a cadeia de certificados até a CA raiz.
2. O verificador recebe o certificado e o valida, usando a chave pública do emissor.
3. A chave pública do emissor é encontrada no certificado do emissor, que está na cadeia ao lado do certificado do cliente.
4. Se a autoridade certificadora mais alta que assinou o certificado do emissor tiver a confiança do verificador, a verificação será bem-sucedida e será interrompida.
5. Além disso, o certificado do emissor é verificado de maneira semelhante à do cliente nas etapas acima.
6. Esse processo continua até que uma CA confiável seja encontrada, ou continua até a CA.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

4.7. Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil)

No Brasil, a Infraestrutura de Chaves Públicas ICP-Brasil, vinculada ao Instituto Nacional de Tecnologia da Informação da Casa Civil da Presidência da República, é quem responde pela AC-Raiz. A ela estão vinculadas todas as Autoridades Certificadoras – ACs de 1º e 2º nível, e as Autoridades de Registro – ARs, da ICP-Brasil.

Criada pela Medida Provisória nº 2.200-2 de 24 de agosto de 2001, a ICP-Brasil é a infraestrutura que possibilita a emissão de certificados digitais para identificação digital em transações eletrônicas no Brasil. A ICP-Brasil é gerida pelo Instituto Nacional de Tecnologia da Informação (ITI) e assegura a validade jurídica dos documentos eletrônicos. A ICP-Brasil é um sistema hierárquico de entidades que garante a confiabilidade e autenticidade dos certificados digitais emitidos no país. No topo da hierarquia está a Autoridade Raiz da ICP-Brasil, responsável por emitir certificados para as Autoridades Certificadoras (ACs). As ACs, por sua vez, são responsáveis pela emissão de certificados digitais para pessoas físicas e jurídicas. Essa hierarquia pode ser verificada em https://estrutura.iti.gov.br/

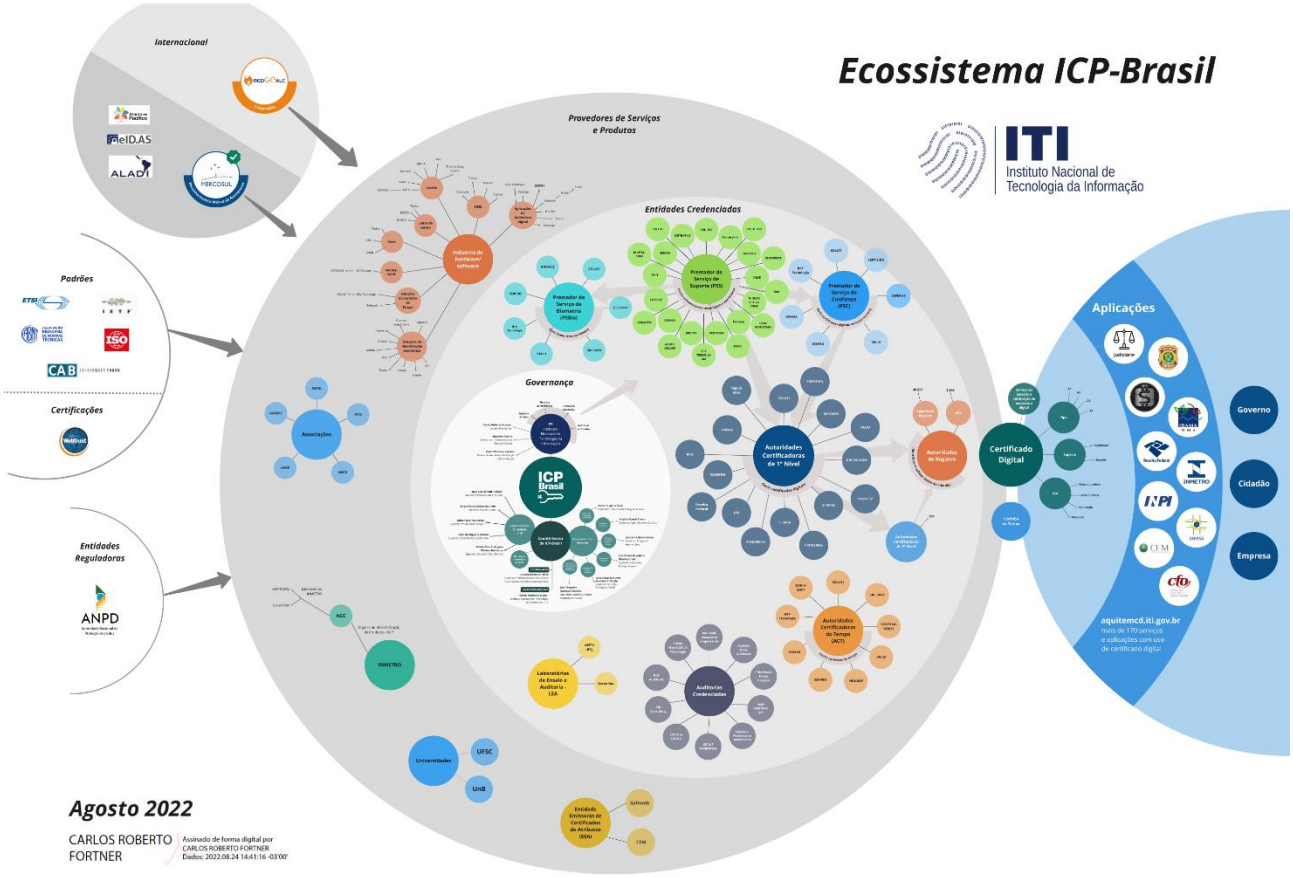

Figura 5 - Ecossistema ICP Brasil.
Fonte: https://www.gov.br/iti/pt-br/assuntos/icp-brasil/ecossistema-icp-brasil.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

4.8. Legislação Brasileira:

O uso da assinatura digital e dos certificados digitais no Brasil é regulado principalmente pela MP 2.200-2, que confere aos documentos eletrônicos assinados digitalmente a mesma validade jurídica dos assinados manualmente. Isso é crucial para aplicações no comércio eletrônico, no setor financeiro e no meio jurídico. A Lei nº Lei nº 14.063, de 23 de Setembro de 2020 regulamenta o uso da assinatura digital e dos certificados digitais. A legislação define os requisitos para a emissão e utilização de certificados digitais, bem como os casos em que a assinatura digital é legalmente válida.

4.9. Aplicações

No mercado financeiro, a assinatura digital é usada para garantir a segurança em transações como transferências eletrônicas, operações de crédito e investimentos online. As instituições financeiras adotam esses mecanismos para cumprir regulamentações rigorosas de proteção de dados e prevenção de fraudes. A assinatura digital é amplamente utilizada no mercado financeiro para diversas transações, como por exemplo:

- Abertura de contas bancárias;
- Realização de transferências bancárias;
- Negociação de investimentos;
- Acesso a serviços bancários online;

No comércio eletrônico, os certificados digitais garantem a segurança das transações online, autenticando as partes envolvidas. A assinatura digital garante a segurança de transações online, como:

- Compras em lojas virtuais;
- Contratação de serviços online;
- Assinatura de contratos eletrônicos;

No meio jurídico, são essenciais para a validação de contratos digitais, petições e outros documentos e processos oficiais, como por exemplo:

- Assinatura de petições e outros documentos processuais;
- Protocolo de processos eletrônicos;
- Realização de audiências virtuais;

5. Certificados Digitais

Os certificados digitais são componentes fundamentais para a segurança na Internet, servindo como uma forma de identificação digital para entidades (pessoas, empresas, servidores, etc.). Eles permitem a criptografia de dados e a autenticação de identidades, assegurando transações eletrônicas seguras. Um certificado digital é um documento eletrônico que contém dados sobre a pessoa física ou jurídica que o

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

utiliza, servindo como uma identidade virtual que confere validade jurídica e aspectos de segurança digital em transações digitais.

Este documento utiliza um sistema criptográfico conhecido como criptografia assimétrica, e geralmente inclui o nome do usuário, sua chave pública, a entidade emissora, a assinatura digital e o prazo de validade do certificado. A emissão, distribuição, renovação e revogação de um certificado digital é feito por uma autoridade certificadora, entidade encarregada da validação dos certificados e vinculada a uma hierarquia na infraestrutura de chaves públicas (ICP).

A certificação digital é uma tecnologia de identificação que permite que transações eletrônicas sejam realizadas considerando os aspectos de integridade, autenticidade, confidencialidade e irretratabilidade, de modo a evitar que adulterações, interceptações de informações privadas ou outros tipos de ações indevidas ocorram. Deste modo, o certificado digital faz a ligação entre a chave pública exclusiva do usuário e a Autoridade Certificadora que chancela a identidade do documento.

Por analogia, um certificado pode ser considerado como a carteira de identidade para a pessoa. As pessoas usam a carteira de identidade, a carteira de motorista e o passaporte para provar sua identidade. Um certificado digital faz a mesma coisa no mundo eletrônico, mas com uma diferença: os Certificados Digitais não são emitidos apenas para pessoas: podem ser emitidos para computadores, pacotes de software ou qualquer outra coisa que precise provar a identidade no mundo eletrônico.

Os certificados digitais são baseados no padrão X.509 da ITU, que define um formato de certificado padrão para certificados de chave pública e validação de certificação. Portanto, os certificados digitais às vezes também são chamados de certificados X.509. A chave pública referente ao cliente do usuário é armazenada em certificados digitais pela Autoridade Certificadora (CA – Certification Autority) juntamente com outras informações relevantes, como informações do cliente, data de validade, uso, emissor etc.

A CA assina digitalmente toda essa informação e inclui assinatura digital no certificado. Qualquer pessoa que precise da garantia sobre a chave pública e as informações associadas do cliente pode realizar o processo de validação de assinatura usando a chave pública da CA. A validação bem-sucedida assegura que a chave pública fornecida no certificado pertença à pessoa cujos detalhes são fornecidos no certificado. O processo de obtenção do Certificado Digital por uma pessoa / entidade é descrito na Fig. 12. Conforme mostrado, a CA aceita o aplicativo de um cliente para certificar sua chave pública. A CA, depois de verificar devidamente a identidade do cliente, emite um certificado digital para esse cliente.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

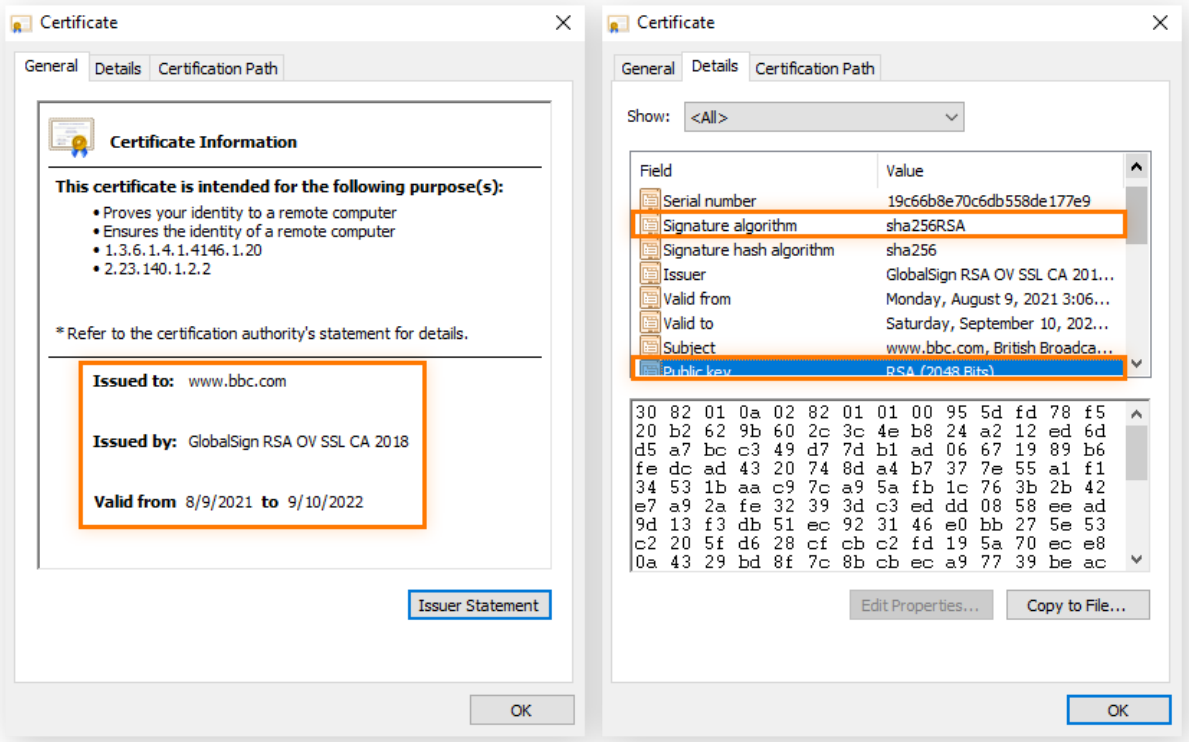

Figura 6 - Um certificado SSL.

O padrão mais utilizado de formato dos certificados, o X.509, apresenta os seguintes campos:

- **Versão** - Número da versão X.509 do certificado.
- **Número de série** - Identificador único do certificado e representado por um inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma AC.
- **Algoritmo de Assinatura da AC** - Identificador do algoritmo usado para assinatura do certificado pela AC.
- **Nome do Emissor** - Nome da AC que produziu e assinou o certificado.
- **Período de Validade** - Intervalo de tempo que determina até quando um certificado deve ser considerado válido
- **Nome do sujeito** - Identifica o dono do Certificado
- **Chave Pública do Sujeito** - Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada.
- **ID único do Emissor** - Campo para permitir o reuso de um emissor com o tempo.
- **ID único do Sujeito** - Campo para permitir o reuso de um sujeito com o tempo.
- **Extensões** - Campos complementares para personalizar um certificado.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

5.1. Algoritmos Criptográficos utilizados

A segurança dos certificados digitais é garantida por algoritmos de criptografia de chave pública. Os principais algoritmos utilizados incluem:

- **RSA (Rivest-Shamir-Adleman):** Um dos primeiros sistemas de criptografia de chave pública e ainda amplamente utilizado. Suporta chaves de 1024, 2048, ou 4096 bits, embora chaves de 2048 bits ou mais sejam recomendadas para segurança adequada.
- **ECDSA (Elliptic Curve Digital Signature Algorithm):** Baseado na teoria dos números em curvas elípticas, oferece segurança equivalente ao RSA com chaves significativamente menores. Isso resulta em processos mais rápidos e menor consumo de dados.
- **DSA (Digital Signature Algorithm):** Usado principalmente para assinaturas digitais e não para criptografia de dados.

5.2. Obtenção, Instalação e Atualização de Certificados SSL

Obtenção: Para adquirir um certificado SSL, a entidade solicitante deve gerar um par de chaves (pública e privada) e submeter uma Solicitação de Assinatura de Certificado (CSR) a uma Autoridade Certificadora (CA). O CSR contém detalhes como o nome da organização, o domínio, o país, entre outros, além da chave pública. Para isso é necessário:

- **Escolher uma Autoridade Certificadora (AC) confiável**: Diversas ACs oferecem certificados SSL, cada uma com suas próprias políticas e preços. É importante pesquisar e escolher uma AC confiável e que atenda às suas necessidades.
- **Solicitar o certificado SSL**: O processo de solicitação geralmente envolve o preenchimento de um formulário com informações sobre o seu site, organização e domínio.
- **Validar a propriedade do domínio**: A AC irá verificar se você é o proprietário do domínio para o qual deseja o certificado SSL. Isso pode ser feito por meio de métodos como DNS validation, email validation ou HTTP validation.
- **Instalar o certificado SSL**: Após a validação, a AC fornecerá os arquivos do certificado SSL. Você precisará instalá-los no servidor web que hospeda o seu site.

Instalação: Após a emissão do certificado pela CA, ele deve ser instalado no servidor da entidade solicitante. O processo específico de instalação pode variar dependendo do servidor web utilizado (Apache, Nginx, IIS, etc.). Geralmente, envolve configurar o servidor para utilizar o certificado digital e a chave privada associada para estabelecer conexões seguras.

Atualização: Certificados digitais têm um prazo de validade e devem ser renovados periodicamente. A renovação envolve a geração de um novo CSR e a repetição do processo de solicitação com uma CA. É importante manter o certificado atualizado para evitar interrupções nas operações e manter a conformidade com os padrões de segurança.

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

6. Para pesquisar, discutir e resumir

1. Como a criptografia de chave pública garante a segurança das transações eletrônicas?
2. Discuta o papel da ICP-Brasil no sistema de certificação digital nacional.
3. Quais são os impactos da legislação brasileira sobre os certificados digitais no comércio eletrônico?
4. Analise a importância da assinatura digital no contexto do mercado financeiro.
5. Explique o papel dos certificados digitais no meio jurídico brasileiro.

7. Referências Bibliográficas

Livros:
STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. São Paulo: Pearson Education do Brasil, 2015.
Sites:
Instituto Nacional de Tecnologia da Informação (ITI) (https://www.gov.br/iti/pt-br)
ITI. ICP-Brasil. Disponível em https://www.iti.gov.br/icp-brasil
ICP-Brasil (https://www.gov.br/iti/pt-br/assuntos/icp-brasil)
ICP-Brasil: https://www.gov.br/pt-br/servicos/obter-certificacao-digital
Let's Encrypt: https://letsencrypt.org/getting-started/
Mozilla SSL Observatory: https://observatory.mozilla.org/
https://www.kaspersky.com.br/resource-center/definitions/what-is-a-ssl-certificate
https://pt.wikipedia.org/wiki/Certificado_digital
https://support.microsoft.com/pt-br/office/obter-um-certificado-digital-e-criar-uma-assinatura-digital-e3d9d813-3305-4164-a820-2e063d86e512
https://support.microsoft.com/pt-br/office/assinaturas-e-certificados-digitais-8186cd15-e7ac-4a16-8597-22bd163e8e96
https://arquivar.com.br/blog/leis-que-regulamentam-a-assinatura-eletronica-e-digital/

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.

PROFESSOR-AUTOR

Luis Gonzaga de Paulo

luis.gonzaga@pucpr.br

PUCPR

GRUPO MARISTA

© PUCPR. Todos os direitos reservados. Nenhum texto pode ser reproduzido sem prévia autorização.