**O Que São Autoridades Certificadoras E Como Elas Certificam Um Determinado Site?**

**Autoridades Certificadoras (CAs – Certificate Authorities)** são **entidades confiáveis** responsáveis por **emitir, validar e revogar certificados digitais**. Elas são fundamentais na **infraestrutura de segurança da internet**, especialmente em conexões HTTPS.

**🔐 O que é uma Autoridade Certificadora (CA)?**

É uma organização responsável por **verificar a identidade de uma entidade (como um site, empresa ou pessoa)** e emitir um **certificado digital** que comprova essa identidade.

**📜 O que é um certificado digital?**

Um certificado digital é um arquivo que contém:

* A **chave pública** do titular (ex: de um site),
* Informações de identidade (ex: nome do domínio),
* A assinatura digital da **Autoridade Certificadora**.

**✅ Como a CA certifica um site? (Etapas)**

1. **Geração do par de chaves**
   * O dono do site (ex: exemplo.com) gera um par de chaves: **pública e privada**.
2. **Criação do CSR (Certificate Signing Request)**
   * O site gera um pedido de certificado que contém a chave pública e as informações do domínio.
3. **Envio para a CA**
   * O CSR é enviado à autoridade certificadora.
4. **Validação pela CA**
   * A CA realiza a **validação de identidade**, que pode variar conforme o tipo de certificado:
     + **DV (Domain Validation):** verifica que o solicitante controla o domínio.
     + **OV (Organization Validation):** verifica também dados da empresa.
     + **EV (Extended Validation):** verificação rigorosa com documentação legal.
5. **Emissão do certificado**
   * A CA **assina digitalmente** o certificado com sua chave privada, atestando a autenticidade.
6. **Instalação**
   * O certificado é instalado no servidor web.

**🔒 Como o navegador confia nisso?**

1. Navegadores possuem uma **lista de CAs confiáveis** embutida (como DigiCert, Let's Encrypt, GlobalSign).
2. Quando você acessa um site HTTPS:
   * O navegador verifica se o certificado foi assinado por uma CA confiável.
   * Verifica também a validade, o nome do domínio e se o certificado foi revogado.
3. Se tudo estiver certo, aparece o **cadeado verde**.

**🛡️ Por que as CAs são importantes?**

* Garantem que o site é quem diz ser.
* Protegem contra ataques como **man-in-the-middle**.
* Tornam possível o uso de **criptografia segura em escala global** (como no TLS/HTTPS).

**📌 Exemplo real:**

1. Você acessa https://meubanco.com.
2. O navegador recebe o certificado do site.
3. Verifica se foi assinado, por exemplo, pela **DigiCert**, e se está válido.
4. Se estiver tudo certo, estabelece conexão **TLS segura** com criptografia.

**O Que É Uma Cadeia De Certificados De CA Intermediárias?**

Uma **cadeia de certificados de CA intermediárias** (ou **cadeia de confiança**) é uma sequência ordenada de certificados digitais que **liga o certificado de um site (ou entidade final)** até uma **Autoridade Certificadora raiz (Root CA)** confiável.

**📚 Definição**

**Cadeia de certificados** é o conjunto de certificados que conecta o **certificado final (ex: de um site)** a uma **CA raiz confiável**, passando por uma ou mais **CAs intermediárias**.

**🔗 Como é formada a cadeia?**

1. **Certificado do site** – também chamado de **certificado de entidade final**.
2. **Certificado da CA intermediária** – emitido por outra autoridade superior.
3. **(Opcionalmente) outras CAs intermediárias**.
4. **Certificado da CA raiz (Root CA)** – autoassinado e já embutido nos sistemas operacionais e navegadores.

**🧭 Exemplo de cadeia (HTTPS):**

[meusite.com]

↓

[CA Intermediária – Let's Encrypt R3]

↓

[CA Raiz – ISRG Root X1]

**🔐 Por que usar CAs intermediárias?**

* **Segurança:** A **Root CA é mantida offline** para evitar comprometimento.
* **Escalabilidade:** CAs intermediárias podem ser criadas para diferentes propósitos ou clientes.
* **Revogação controlada:** Se uma intermediária for comprometida, pode ser revogada sem afetar toda a infraestrutura.

**📦 Como o navegador valida?**

Quando você acessa https://exemplo.com:

1. O servidor envia:
   * O **certificado do site**
   * E geralmente os **certificados das CAs intermediárias**
2. O navegador:
   * Verifica se pode **construir uma cadeia válida até uma Root CA confiável**.
   * Valida **assinaturas, datas e nomes de domínio**.
3. Se tudo estiver correto, a conexão segura é estabelecida.

**🔎 Como visualizar a cadeia (exemplo):**

**No navegador:**

1. Clique no **cadeado** ao lado da URL.
2. Vá em “**Certificado**” → “**Detalhes**”.
3. Verá a cadeia: **certificado do site → CA intermediária → Root CA**.

**Via terminal com openssl:**

openssl s\_client -connect exemplo.com:443 -showcerts

**✅ Resumo**

| **Elemento** | **Papel na cadeia** |
| --- | --- |
| Certificado do site | Identifica o domínio |
| CA intermediária | Assina certificados de sites |
| Root CA | Autoridade máxima, confiada pelo sistema |

**DigiCert É Uma Certificadora Intermediária?**

Sim, a DigiCert é uma Autoridade Certificadora (CA) que emite tanto certificados raiz quanto intermediários. Um certificado raiz é o certificado de nível mais alto, que estabelece a confiança em uma hierarquia de certificados. Certificados intermediários são usados para emitir certificados para clientes, como certificados SSL/TLS para sites, e eles são encadeados de volta ao certificado raiz. A DigiCert opera como uma CA raiz confiável e também oferece certificados intermediários para seus clientes.

Explicação:

* **Autoridade Certificadora (CA):**

Uma CA é uma entidade confiável que emite e gerencia certificados digitais.

* **Certificado Raiz:**

É o certificado de nível mais alto em uma hierarquia de certificados, utilizado para validar a confiança em outros certificados emitidos por essa CA.

* **Certificado Intermediário:**

É um certificado emitido pela CA raiz e usado para emitir certificados para clientes. Eles servem como um "intermediário" entre a CA raiz e os certificados do usuário final.

* **DigiCert:**

A DigiCert é uma das principais CAs do mercado, fornecendo tanto certificados raiz quanto certificados intermediários para empresas e organizações.

* **Hierarquia:**

A DigiCert, como CA raiz, emite certificados raiz e, a partir desses, certificados intermediários, que por sua vez são usados para emitir certificados para sites (SSL/TLS) e outros fins.

**A Chave Publica No Certificado É A Mesma Chave Usada Na Criptografia do TLS?**

Sim, a chave pública presente em um certificado digital é a mesma chave utilizada na criptografia TLS. Essa chave é usada para criptografar dados transmitidos entre o cliente e o servidor, garantindo a segurança da comunicação.

Explicação detalhada:

* **Certificados Digitais e PKI:**

Certificados digitais, como os usados no TLS/SSL, fazem parte da Infraestrutura de Chave Pública (PKI). Eles contêm informações sobre a identidade do proprietário (site, servidor, etc.) e uma chave pública.

* **Chave Pública:**

A chave pública é usada para criptografar dados. Qualquer pessoa pode ter acesso à chave pública, pois ela é usada para garantir que a mensagem criptografada com ela só possa ser descriptografada pela chave privada correspondente, que fica sob o controle do proprietário do certificado.

* **TLS/SSL e Criptografia:**

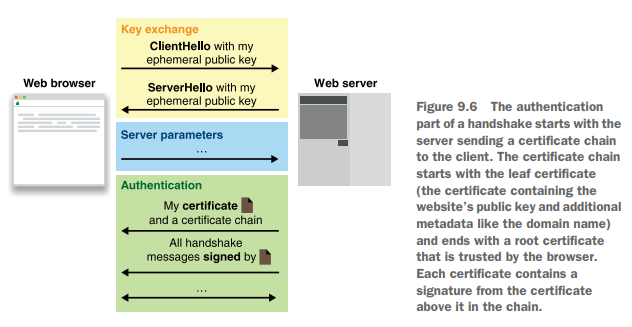
No TLS/SSL, a chave pública do certificado do servidor é usada pelo cliente para criptografar a chave de sessão (uma chave simétrica que será usada para a comunicação segura). Essa chave de sessão é então usada para criptografar o resto da comunicação.

* **Segurança:**

A chave pública no certificado garante que apenas o proprietário do certificado (com sua chave privada) possa descriptografar os dados enviados pelo cliente, protegendo a confidencialidade da comunicação.

A cadeia de certificados é enviada em uma mensagem TLS chamada *certificate*, tanto pelo servidor quanto pelo cliente (caso o cliente tenha sido solicitado a autenticar-se). Em seguida, o servidor pode usar seu par de chaves de longo prazo certificado para assinar todas as mensagens de *handshake* que foram recebidas e previamente enviadas, no que é chamado de mensagem *CertificateVerify*. A Figura 9.6 revisa esse fluxo, onde apenas o servidor se autentica.

A assinatura na mensagem *CertificateVerify* prova ao cliente o que o servidor viu até aquele momento. Sem essa assinatura, um atacante *MITM* poderia interceptar as mensagens de *handshake* do servidor e substituir a chave pública efêmera do servidor contida na mensagem *ServerHello*, permitindo que o atacante se passasse com sucesso pelo servidor.  
Reserve alguns momentos para entender por que um atacante não pode substituir a chave pública efêmera do servidor na presença da assinatura *CertificateVerify*.



*Figura 9.6: A parte de autenticação de um handshake começa com o servidor enviando uma cadeia de certificados ao cliente. A cadeia de certificados começa com o certificado folha (o certificado contendo a chave pública do website e metadados adicionais como o nome do domínio) e termina com um certificado raiz confiado pelo navegador. Cada certificado contém uma assinatura do certificado imediatamente acima na cadeia.*

Finalmente, para encerrar oficialmente o *handshake*, ambos os lados da conexão devem enviar uma mensagem *Finished* como parte da fase de autenticação.  
Uma mensagem *Finished* contém uma tag de autenticação produzida por HMAC, instanciada com a função hash negociada para a sessão.  
Isso permite que tanto o cliente quanto o servidor digam um ao outro:

"Estas são todas as mensagens que enviei e recebi em ordem durante este *handshake*."

Se o *handshake* for interceptado e adulterado por atacantes *MITM*, essa verificação de integridade permite que os participantes detectem e abortem a conexão.