**Certificados raiz e intermediários: Explicação das principais diferenças**

Atualizado em Abril 4th, 2025 por [Dionisie Gitlan](https://www.ssldragon.com/pt/blog/author/dinugtln/)

Compreender a **diferença entre certificados raiz e certificados intermediários** é essencial para proteger as comunicações on-line. Esses dois tipos de certificados digitais, juntamente com os certificados SSL, formam a espinha dorsal da navegação segura na Web, permitindo a transferência de dados criptografados e estabelecendo confiança entre servidores e usuários. Mas o que exatamente os diferencia?

**Os certificados raiz** servem como autoridade máxima, situando-se no topo da hierarquia de certificados, enquanto **os certificados intermediários** atuam como intermediários, criando uma **cadeia** segura **de confiança**. Neste artigo, detalharemos os papéis, as funções e as principais diferenças entre esses certificados para ajudar você a entender como eles trabalham juntos para proteger informações confidenciais on-line.

**Principais conclusões**

* **Os certificados raiz** são os certificados de nível mais alto na cadeia de confiança, autoassinados por uma autoridade de certificação (CA) confiável. Eles formam a base das comunicações seguras e são essenciais para estabelecer a confiança na Internet.
* **Os certificados intermediários** atuam como intermediários entre o certificado raiz e o certificado do usuário final. Eles são assinados por certificados raiz ou outros certificados intermediários e ajudam a criar uma cadeia de confiança, reduzindo o risco associado ao uso direto de certificados raiz.
* Os dois tipos de certificados trabalham juntos para garantir a criptografia, a autenticação e a integridade dos dados na Web, protegendo informações confidenciais contra ameaças cibernéticas.

1. **Índice**
2. [O que é um certificado raiz?](https://www.ssldragon.com/pt/blog/certificados-raiz-intermediarios/#What-is-a-Root-Certificate)
3. [O que é um certificado intermediário?](https://www.ssldragon.com/pt/blog/certificados-raiz-intermediarios/#What-is-an-Intermediate-Certificate)
4. [Explicação da hierarquia de certificados](https://www.ssldragon.com/pt/blog/certificados-raiz-intermediarios/#Certificate-Hierarchy-Explained)
5. [Importância das cadeias de certificados](https://www.ssldragon.com/pt/blog/certificados-raiz-intermediarios/#Importance-of-Certificate-Chains)
6. [Principais diferenças entre certificados raiz e intermediários](https://www.ssldragon.com/pt/blog/certificados-raiz-intermediarios/#Key-Differences-Between-Root-and-Intermediate-Certificates)
7. [Conceitos avançados relacionados a certificados raiz e intermediários](https://www.ssldragon.com/pt/blog/certificados-raiz-intermediarios/#Advanced-Concepts-Related-to-Root-and-Intermediate-Certificates)

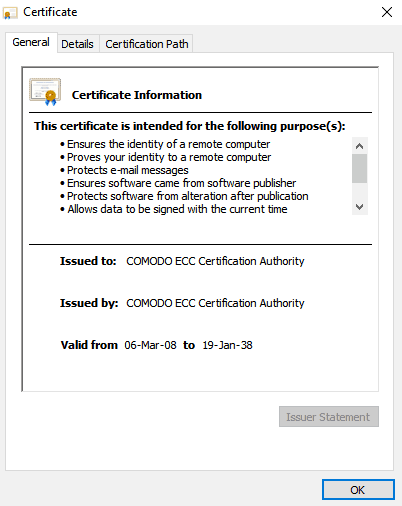
**Visão geral dos certificados raiz e intermediários**

**O que é um certificado raiz?**

[Um **certificado raiz**](https://www.ssldragon.com/pt/blog/o-que-e-certificado-raiz/), geralmente chamado de **certificado CA**, é um certificado digital que serve como base de um sistema [de infraestrutura de chave pública (PKI)](https://www.ssldragon.com/pt/blog/que-e-pki-infraestrutura-de-chave-publica/). Ele é emitido por uma [autoridade de certificação (CA)](https://www.ssldragon.com/pt/blog/que-e-autoridade-certificacao/) confiável e é autoassinado, o que significa que a CA autentica a si mesma. Os certificados raiz são armazenados em um repositório confiável conhecido como armazenamento raiz, que é mantido por navegadores e sistemas operacionais para autenticar conexões seguras.

Os certificados raiz são essenciais para estabelecer o nível mais alto de confiança em uma cadeia de certificados. Eles validam e assinam certificados intermediários, que, por sua vez, assinam certificados de usuários finais. Devido à sua importância, os certificados raiz normalmente são válidos por longos períodos, geralmente de 20 a 25 anos ou mais.

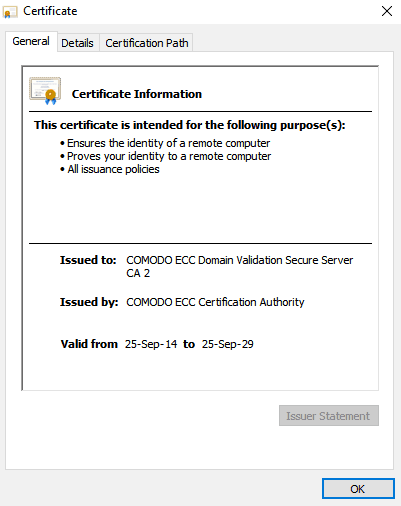
Ao contrário dos certificados comerciais, os certificados raiz têm uma vida útil muito mais longa. Aqui você encontra o período de validade do [Sectigo](https://www.ssldragon.com/sectigo-ssl-certificate/) ECC. Como você pode ver, ele expira no distante ano de 2038.



A segurança de toda a cadeia de certificados depende da integridade do certificado raiz.

O que é um certificado intermediário?

Um certificado intermediário atua como uma ponte entre o certificado raiz e os certificados de servidor, como os certificados SSL/TLS para sites. Ao contrário dos certificados raiz, os certificados intermediários não são autoassinados; eles são assinados por um certificado raiz ou por outro certificado intermediário. Essa estrutura cria uma hierarquia conhecida como “cadeia de confiança“.



Os certificados intermediários desempenham um papel fundamental na redução de riscos. Em vez de usar o certificado raiz para emitir certificados de usuário final diretamente, uma autoridade de certificação usa certificados intermediários. Essa abordagem limita a exposição do certificado raiz e facilita a revogação e a substituição de certificados comprometidos sem afetar toda a cadeia de confiança.

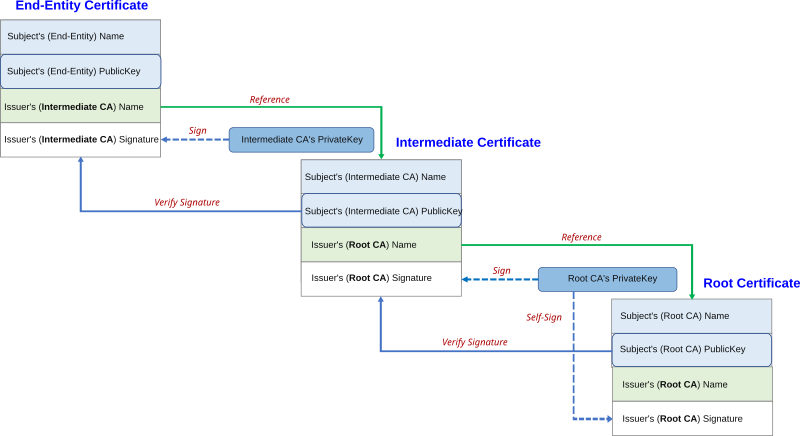
**Explicação da hierarquia de certificados**

Em uma hierarquia de certificados digitais, o **certificado raiz** fica na parte superior, seguido por um ou mais **certificados intermediários** e, por fim, **os certificados do servidor ou do usuário final** na parte inferior. Essa hierarquia é fundamental para estabelecer uma cadeia segura de confiança. Quando um usuário se conecta a um site, o navegador verifica a validade do certificado do servidor seguindo a cadeia até o certificado raiz confiável.

* **Certificado raiz**: A autoridade mais alta, autoassinada pela AC.
* **Certificado intermediário**: Assinado pela raiz ou por outro certificado intermediário, criando várias camadas de confiança.
* **Certificado de servidor/usuário final**: Emitido para o site ou entidade, fornecendo comunicação criptografada e verificação de identidade.

**Importância das cadeias de certificados**

Uma **cadeia** de certificados, também conhecida como caminho de certificação, é a sequência de certificados que remonta do certificado do usuário final a um certificado raiz confiável. Essa cadeia é fundamental para estabelecer conexões seguras pela Internet. Cada certificado na cadeia é validado pelo certificado acima dele, garantindo que a confiança seja transferida da raiz confiável para o usuário final.



Crédito da imagem: [Fanyangxi – CC BY-SA 4.0](https://commons.wikimedia.org/wiki/File:Chain_of_trust_v2.svg" \t "_blank)

As cadeias de certificados aumentam a segurança fornecendo várias camadas de verificação. Se um certificado intermediário for comprometido, ele poderá ser revogado sem afetar o certificado raiz ou outros certificados intermediários, preservando a integridade do sistema geral.

**Principais diferenças entre certificados raiz e intermediários**

Entender as diferenças entre os **certificados raiz** e **os certificados intermediários** é fundamental para qualquer pessoa envolvida em segurança digital. Embora ambos os tipos de certificados desempenhem funções essenciais na hierarquia de confiança, eles diferem significativamente em termos de emissão, armazenamento, vida útil e finalidade. Aqui você encontra um detalhamento das principais distinções:

1. **Hierarquia e nível de confiança**. Os certificados raiz estão posicionados no topo da hierarquia de confiança. Como autoridade final, eles são os certificados mais confiáveis e são autoassinados por uma autoridade de certificação (CA). Em contrapartida, os certificados intermediários estão abaixo na hierarquia, atuando como intermediários que vinculam o certificado raiz aos certificados do usuário final. Essa estrutura hierárquica garante que a confiança flua da raiz até o usuário final.
2. **Autoridade de emissão e assinatura**. Os certificados raiz são emitidos por uma autoridade de certificação confiável e são autoassinados, o que significa que a CA verifica sua própria identidade. Os certificados intermediários, no entanto, são assinados por um certificado raiz ou por outro certificado intermediário. Essa delegação de autoridade de assinatura permite que as CAs emitam certificados com mais segurança, pois o certificado raiz não é usado diretamente para assinar certificados de usuários finais.
3. **Práticas de armazenamento e segurança**. Os certificados raiz de autoridades de certificação raiz confiáveis são armazenados em locais confiáveis, como os armazenamentos confiáveis de navegadores da Web e sistemas operacionais. Esses armazenamentos confiáveis contêm uma lista de certificados raiz reconhecidos que são automaticamente confiáveis por todos os usuários. Os certificados intermediários, por outro lado, são armazenados nos servidores das organizações que precisam deles. Como eles não exigem o mesmo nível de confiança que os certificados raiz, seu armazenamento é menos crítico, mas ainda exige um manuseio seguro para evitar o acesso não autorizado. A maioria dos dispositivos e navegadores vem com um conjunto de **certificados raiz pré-carregados** que são armazenados em seus repositórios de confiança, fornecendo uma linha de base para comunicações seguras.
4. **Períodos de validade e vida útil**. O período de validade dos certificados raiz normalmente é muito maior do que o dos certificados intermediários. Os certificados-raiz podem ser válidos por 20 a 25 anos ou mais, enquanto os certificados intermediários costumam ter períodos de vida mais curtos, geralmente entre 1 e 5 anos. Esse período de validade mais curto ajuda a minimizar o risco no caso de um certificado intermediário ser comprometido, pois ele pode ser revogado ou substituído mais facilmente do que um certificado raiz.
5. **Gerenciamento e mitigação de riscos**. Os certificados raiz apresentam um nível mais alto de risco se forem comprometidos, pois representam a âncora de confiança final na cadeia de certificados. Para atenuar esse risco, os certificados intermediários são usados para emitir certificados de usuário final. Se um certificado intermediário for comprometido, ele poderá ser revogado sem comprometer o certificado raiz, mantendo assim a segurança geral do sistema de PKI.
6. **Aplicativos e exemplos do mundo real**. Na prática, os certificados raiz e intermediários são amplamente usados para proteger transações on-line, sites e comunicações. Por exemplo, um certificado raiz pode ser confiável para todos os navegadores, enquanto um certificado intermediário é usado para emitir um certificado SSL para um site, autenticando sua identidade e permitindo a comunicação segura. Ao criar essa abordagem em camadas, o sistema garante que, mesmo que uma parte da cadeia de certificados seja comprometida, o sistema inteiro não entrará em colapso.

**Conceitos avançados relacionados a certificados raiz e intermediários**

É importante que você entenda como os certificados raiz e intermediários interagem no contexto mais amplo da segurança digital, aprofundando-se em seus conceitos. Esses conceitos avançados ajudarão a esclarecer suas funções nos sistemas de infraestrutura de chave pública (PKI) e os mecanismos que mantêm nossas comunicações on-line seguras.

**O que é um programa raiz?**

Um **programa raiz** é uma estrutura de política que determina quais certificados raiz são confiáveis para navegadores da Web, sistemas operacionais e outras plataformas de software. Gerenciados por grandes organizações como Microsoft, Apple, Mozilla e Google, esses programas mantêm uma lista de certificados raiz confiáveis, conhecida como trust store.

Os programas raiz são essenciais para garantir que os certificados incluídos nos repositórios confiáveis sejam autênticos, seguros e sigam padrões de segurança rigorosos. Eles revisam e auditam periodicamente os certificados raiz, adicionando novas raízes confiáveis e removendo aquelas que não atendem mais aos requisitos de segurança.

**Assinaturas digitais e sua função**

**As assinaturas digitais** são assinaturas criptográficas que autenticam a integridade e a origem de um certificado. Os certificados raiz e intermediários dependem de assinaturas digitais para verificar se não foram adulterados e se foram emitidos por uma autoridade certificadora (CA) legítima.

* **Para certificados raiz:** A assinatura digital é autoassinada pela AC, estabelecendo sua autoridade e confiabilidade.
* **Para certificados intermediários:** A assinatura digital é criada usando a chave privada da raiz emissora ou do certificado intermediário, fornecendo um link para uma raiz confiável.

As assinaturas digitais garantem que cada certificado da cadeia possa ser rastreado até uma autoridade de certificação raiz confiável, mantendo a integridade das comunicações seguras.

**Diferenças entre sistemas de raiz única e em cadeia**

Há dois tipos principais de sistemas de certificados: **sistemas raiz encadeados** e **sistemas raiz únicos**.

* **Sistemas raiz encadeados:** Utilize vários certificados intermediários entre o certificado raiz e o certificado do usuário final. Isso adiciona camadas de segurança e flexibilidade, pois os intermediários podem ser revogados ou substituídos sem afetar o certificado raiz.
* **Sistemas de raiz única:** Use um único certificado raiz para emitir certificados diretamente para o usuário final. Embora seja mais simples, esse sistema é mais arriscado porque qualquer comprometimento do certificado raiz pode prejudicar a segurança de todo o sistema.

Os sistemas de raiz encadeados são mais comumente usados devido à sua capacidade de mitigar riscos e oferecer segurança mais robusta.

**Linha de fundo**

Compreender a diferença entre **certificados raiz** e **certificados intermediários** é fundamental para manter um ambiente digital seguro.

Enquanto os certificados raiz estabelecem a confiança máxima no topo da hierarquia de certificados, os certificados intermediários fornecem uma camada essencial de segurança que preenche a lacuna dos certificados de usuário final. Juntos, eles criam uma cadeia de confiança robusta que protege as comunicações on-line, garante a integridade dos dados e autentica as identidades em toda a Internet.

Ao reconhecer suas funções distintas e como elas funcionam em conjunto, você pode apreciar melhor os mecanismos que mantêm suas interações on-line seguras e protegidas.