UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM ARQUITETURA E GERENCIAMENTO DE INFRAESTRUTURA DE TI

JEFERSON LUIZ RODRIGUES MICHALSZESZEN

UM GUIA SOBRE GESTÃO E ADMINISTRAÇÃO DE CERTIFICADOS DIGITAIS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2021

JEFERSON LUIZ RODRIGUES MICHALSZESZEN

UM GUIA SOBRE GESTÃO E ADMINISTRAÇÃO DE CERTIFICADOS DIGITAIS

Monografia de Especialização, apresentada ao Curso de Especialização em Arquitetura e Gestão de Infraestrutura de TI, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Joilson Alves Junior

CURITIBA
2021

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Arquitetura e Gestão de Infraestrutura de TI

TERMO DE APROVAÇÃO

UM GUIA SOBRE GESTÃO E ADMINISTRAÇÃO DE CERTIFICADOS DIGITAIS

por

JEFERSON LUIZ RODRIGUES MICHALSZESZEN

Esta monografia foi apresentada em 20 de dezembro de 2021 como requisito parcial para a obtenção do título de Especialista em Arquitetura e Gestão de Infraestrutura de TI. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. D.r Joilson Alves Júnior
Orientador

Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

RESUMO

MICHALSZESZEN, Jeferson Luiz Rodrigues. **Um guia sobre gestão e administração de certificados digitais**. 2021. 3130 p. Monografia de Especialização em Arquitetura e Gestão de Infraestrutura de TI, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

Este guia descreve os elementos para gestão de certificados digitais, que incluem escolhas das entidades certificadoras e do tipo de certificado digital. São abordados os procedimentos de geração, solicitação, assinatura e instalação do certificado, bem como das informações que devem ser registradas em cada etapa do ciclo de vida, incluindo o detalhamento de informações para a correta rastreabilidade das etapas. São detalhados os funcionamentos dos softwares na perspectiva de utilização de certificados digitais e a relação com os respectivos repositórios de certificados e a indicação de procedimentos adicionais para a redução dos impactos e indisponibilidades de serviços durante os procedimentos de gestão dos componentes, relacionados com expiração de certificados e substituição de entidades certificadoras.

Palavras-chave: Certificados Digitais. Gestão. Administração.

ABSTRACT

MICHALSZESZEN, Jeferson Luiz Rodrigues. **A guide to managing and administering digital certificates**. 2021. 30 31p. Monografia de Especialização em Arquitetura e Gestão de Infraestrutura de TI, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

This guide describes the elements for managing digital certificates, which include choices of certificate authority and the type of digital certificate. The procedures for generating, requesting, signing and installing the certificate are addressed, as well as the information that must be recorded at each stage of the life cycle, including the detailing of information for the correct traceability of the stages. The functioning of the software is detailed from the perspective of using digital certificates and the relationship with the respective certificate repositories and the indication of additional procedures to reduce the impacts and unavailability of services during the component management procedures, related to the expiration of certificates and replacement of certificate authority.

Keywords: Digital Certificate. Management. Administration.

LISTA DE FIGURAS

Figura 1 - Arquitetura hierárquica do certificado digital e entidades certificadoras ... 10

LISTA DE TABELAS

Tabela 1 - Principais atributos dos certificados digitais 12
Tabela 2 - Lista de certificados digitais em um repositório 25

LISTA DE SIGLAS

CA	*Certificate Authority*
CA Root	*Certificate Authority Root*
CN	*Common Name*
CRL	*Certificate Revocation List* (ou lista de certificados revogados)
CSR	*Certificate Signing Request*
JKS	*Java KeyStore*
KDB	*Key Database*
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO 8
1.1 CONSIDERAÇÕES INICIAIS 8
1.2 OBJETIVOS 8
1.3 ESTRUTURA DO TRABALHO 8
2 ESTRUTURA E COMPONENTES 9
2.1 CERTIFICADO DIGITAL 9
2.2 ESTRUTURA DO CERTIFICADO DIGITAL 9
2.3 REQUISIÇÃO DE CERTIFICADO DIGITAL 11
2.4 ATRIBUTOS 11
2.5 CHAVE PRIVADA 12
2.6 CHAVE PÚBLICA 13
2.7 REPOSITÓRIO DE CERTIFICADOS DIGITAIS 14
2.8 LISTA DE CERTIFICADOS REVOGADOS 16
2.9 APLICAÇÕES E USUÁRIOS FINAIS 16
3 APRESENTAÇÃO DOS RESULTADOS 18
3.1 CICLO DE VIDA 18
3.2 OS ENVOLVIDOS 18
3.3 A ESCOLHA DA ENTIDADE CERTIFICADORA 20
3.4 REQUISIÇÃO DE CERTIFICADO DIGITAL 22
3.5 RENOVAÇÃO DO CERTIFICADO DIGITAL 23
3.6 ASSINATURA DO CERTIFICADO DIGITAL 24
3.7 RECEPÇÃO DO CERTIFICADO DIGITAL 25
3.8 PROTEÇÃO DO CERTIFICADO DIGITAL 26
3.9 INVENTÁRIO DE CERTIFICADO DIGITAL 26
3.10 DISTRIBUIÇÃO DA CHAVE PÚBLICA 27
3.11 INSTALAÇÃO DO CERTIFICADO DIGITAL 27
3.12 VALIDAÇÃO E ACOMPANHAMENTO 27
3.13 REVOGAÇÃO DO CERTIFICADO DIGITAL 28
4 CONCLUSÃO 29
REFERÊNCIAS 30

1 INTRODUÇÃO

1.1 CONSIDERAÇÕES INICIAIS

O certificado digital é utilizado no contexto de Tecnologia da Informação (TI) para assinatura digital de documentos e criptografia[1] de dados. O uso crescente de tecnologias que utilizam certificados digitais aumenta consideravelmente o trabalho das equipes responsáveis pela administração destes recursos dentro das empresas.

1.2 OBJETIVOS

O objetivo deste documento é listar os principais elementos e componentes envolvidos na utilização dos certificados digitais. Pretende-se também descrever os elementos e procedimentos mínimos para gestão e controle, além de buscar a justificativa e simplificação dos procedimentos e auxiliar as equipes de TI responsáveis pela gestão dos certificados digitais.

1.3 ESTRUTURA DO TRABALHO

Esta monografia de Trabalho de Conclusão de Curso de Especialização está dividida em 4 seções ou capítulos.

Na primeira seção foi introduzido o assunto do trabalho, com contextualização e objetivos e estrutura do trabalho.

Na segunda seção será abordado as estruturas e componentes do certificado digital.

Na terceira seção: Apresentação dos resultados, descrevendo o ciclo de vida de um certificado digital, além de etapas de administração e controle.

Na quarta e última seção, será apresentado a conclusão dos estudos.

[1]Criptografia: Arte ou processo de escrever em caracteres secretos ou em cifras; esteganografia.

2 ESTRUTURA E COMPONENTES

2.1 CERTIFICADO DIGITAL

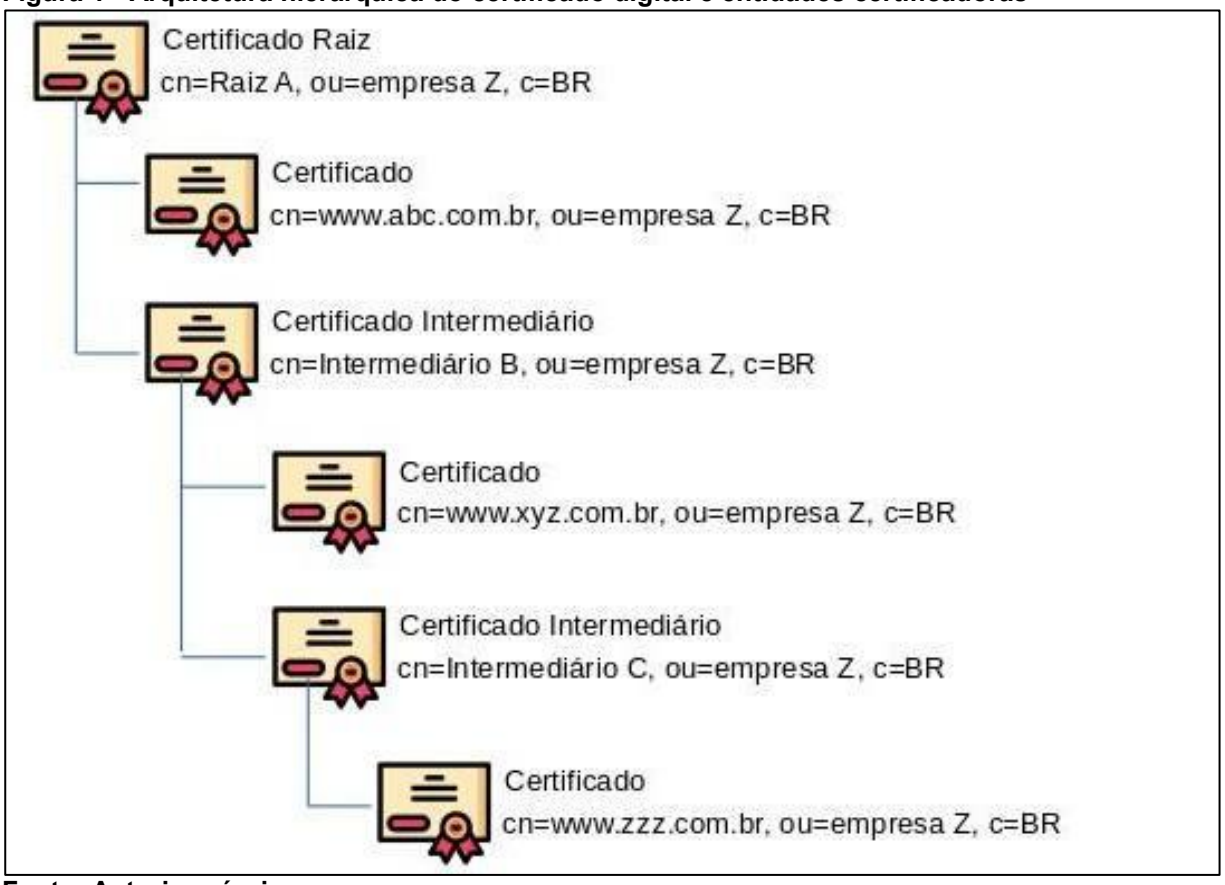
Um certificado digital é um conjunto de atributos e informações validados e assinados digitalmente por uma entidade certificadora ou *Certificate Authority* (CA) e são válidos dentro de um determinado período de tempo. O certificado digital possui dois componentes: a chave privada e a chave pública. A chave privada, utilizada exclusivamente pelo seu proprietário, deve ser protegida e utilizada para assinar digitalmente documentos e para criptografar informações. A chave pública, que pode ser distribuída livremente a todos os interessados, é utilizada para comprovar a veracidade das assinaturas digitais e para recuperar informações que foram criptografadas previamente pela chave privada. O certificado digital também é utilizado por pessoas físicas e jurídicas em atividades que envolvem a identificação pessoal e empresarial perante outras entidades e na assinatura de documentos digitais (SILVA, 2020).

Para que um programa de computador entenda que a assinatura digital atribuída a um documentos ou que uma informação digital criptografada são válidos e legítimos, é necessário que este programa entenda que os certificados digitais utilizados em tais processos sejam considerados confiáveis. Os programas de computadores possuem acesso às listas de certificados digitais, chamados de repositórios. Nestes repositórios as chaves públicas e privadas são inseridas e classificadas. Segundo Silva (2020), as chaves privadas são classificadas como Certificados Pessoais (ou *Personal Certificates*). As chaves públicas podem ser classificadas dentro do repositório de certificados como Entidades Certificadoras Confiáveis (ou *Trusted Certificate Authority*) e Entidades Certificadoras Intermediárias Confiáveis (ou *Trusted Intermediate Certificate Authority*).

2.2 ESTRUTURA DO CERTIFICADO DIGITAL

Os certificados digitais são estruturados em uma arquitetura hierárquica, representada na Figura 1. No primeiro nó desta hierarquia é atribuído o nome de Certificado Raiz, do inglês *Certificate Authority Root* (CA Root ou apenas CA).

Figura 1 - Arquitetura hierárquica do certificado digital e entidades certificadoras



Fonte: Autoria própria.

Uma entidade certificadora raiz poderá assinar a requisição de certificados de usuários finais, também chamados de *end user certificate* e requisições de certificados intermediários. Por sua vez, uma entidade certificadora intermediária poderá assinar requisições de certificados digitais de usuários finais e de outras entidades certificadoras intermediárias. Quando uma entidade certificadora, também chamada de *Certificate Authority* (CA) assina uma requisição que possui o atributo "Signatário de Certificados", significa que aquela CA estará emitindo um novo certificado digital com designação de certificado digital intermediário, também chamado de *Intermediate Certificate*, que, por sua vez, poderá assinar novos certificados digitais (SILVA, 2020).

Um Certificado Raiz é auto assinado, pois os atributos utilizados na requisição daquele certificado são validados e assinados digitalmente pelo próprio certificado digital. O conjunto composto pelos certificados digitais da CA Root e pelos certificados digitais das entidades Certificadoras Intermediárias dentro da mesma hierarquia é chamado de Cadeia de Certificados ou *Certificate Chain*.

2.3 REQUISIÇÃO DE CERTIFICADO DIGITAL

O primeiro passo para a emissão de um certificado digital é a criação da requisição de assinatura do certificado digital, chamada de *Certificate Signing Request* (CSR). As informações que compõem a requisição são chamadas de atributos. Durante o processo de emissão da requisição, são gerados dois novos componentes, o arquivo digital que possui a requisição e o arquivo digital com a chave privada.

O principal atributo para geração da requisição do certificado digital é o nome comum, também chamado de *Common Name* (CN). O arquivo digital com a requisição possui a extensão ".csr", é codificado em Base64[2] e apresenta duas linhas de texto características que o identificam (PUBLICO, 2021):

- A primeira linha contém o texto: -----BEGIN NEW CERTIFICATE REQUEST-
- A última linha contém o texto: -----END NEW CERTIFICATE REQUEST----

2.4 ATRIBUTOS

Os atributos são conjunto de informações presentes em um certificado digital, que podem ser obrigatórios e opcionais. Existem atributos que são fornecidos durante o processo de criação da requisição do certificado digital e outros atributos que são inseridos durante o processo de assinatura e emissão do certificado digital. O certificado digital de uma CA possui os atributos de "Signatário de Certificados" e "Signatário de lista de certificados revogados", que indicam que aquele certificado digital pode ser utilizado para assinar as informações que darão origem a outros certificados digitais intermediários e assinar listas de certificados digitais revogados (SILVA, 2020).

A lista dos principais atributos está demonstrada na Tabela 1.

[2] Base64: As informações em texto são codificadas como dados binários.

Tabela 1 - Principais atributos dos certificados digitais

Nome do Atributo	Abreviatura	Objetivo do Atributo
Common Name	CN	É definido durante a geração da requisição e é o principal atributo do certificado digital. Identifica o nome do site à qual está associado ou qualificação do requisitante e é definido durante a geração da requisição. Exemplo: *CN*=www.site.com.br
Country	C	É formado por duas letras, maiúscula, que identifica a abreviatura do país de emissão do certificado digital e é definido durante a geração da requisição. Exemplo: *C*=BR (BR de Brasil)
State	ST	Identifica o Estado de emissão do certificado digital e é definido durante a geração da requisição. Exemplo: *ST*=Paraná
Location	L	Identifica a cidade de emissão do certificado digital e é definido durante a geração da requisição. Exemplo: *L*=Curitiba
Organization	O	Identifica a organização que solicitou a emissão do certificado digital e é definido durante a geração da requisição. Exemplo: *O*=Empresa Site
Organization Unit	OU	Identifica a equipe/departamento ou área que emitiu o certificado digital. Procure definir um valor que não exponha informações sensíveis da área emissora. É definido durante a geração da requisição. Exemplo: *OU*=Departamento de Gestão de Certificados
Alternate Name		Contém o Common Name (*CN*) do certificado digital e, se houver, nomes alternativos (*CN* adicionais) que podem ser utilizados por aquele certificado digital e é definido durante a geração da requisição. Exemplo: www.site.com.br, www2.site.com.br
CRL Distribution Points		É o endereço digital que indica onde a lista de certificados revogados será publicada.

Fonte: Autoria própria.

2.5 CHAVE PRIVADA

A chave privada é gerada durante o processo de emissão da requisição do certificado digital. Ela pode ser armazenada em diretórios específicos no sistema operacional ou mantida dentro de repositórios de certificados digitais. Deve-se dar atenção especial quanto ao manuseio e permissões de segurança aos arquivos digitais que possuem chaves privadas (SILVA, 2020).

O arquivo digital gerado com a chave privada, na maioria das vezes possui a extensão ".key", é codificado em Base64 e possui duas linhas de textos característicos que o identificam (NOHE, 2018):

- A primeira linha contém o texto: -----BEGIN PRIVATE KEY-----
- A última linha contém o texto: -----END PRIVATE KEY-----

2.6 CHAVE PÚBLICA

A chave pública é gerada no processo de assinatura digital da requisição do certificado digital. A chave pública, em formato de arquivo digital, deverá ser instalada nos diretórios específicos ou em repositórios de certificados digitais do sistema operacional ou da aplicação. A chave pública poderá ser transmitida livremente para os interessados. O processo de transmissão da chave pública ocorre de diferentes destas formas (SILVA, 2020):

- Chave pública de certificado digital pertencentes às entidades certificadoras raiz (CA Root) deverá ser enviada previamente para os interessados e adicionada aos repositórios de certificados digitais e classificada como de entidade certificadora confiável. Algumas aplicações e sistemas operacionais implementam esta distribuição durante a instalação dos de correções ou na instalação de atualizações periódicas. Estão incluídos nestes processo automático de distribuição apenas as entidades certificadoras que possuem convênio com as empresas de software ou sistemas operacionais. A distribuição ocorre apenas para repositórios específicos e não atinge repositórios específicos utilizados por aplicações de terceiros ou desenvolvidas dentro da própria empresa, quando é necessário a distribuição e instalação manual da CA Root em cada um destes repositórios;
- Chave pública de certificado digital pertencentes às entidades certificadoras intermediárias, deverá ser instalada nos repositórios de certificados digitais com a classificação de entidade certificadora intermediária confiável (ou, na ausência desta classificação, como entidade certificadora confiável). Na maioria das vezes, a instalação da chave pública de certificados digitais de entidades certificadoras intermediárias só será requerida no repositório do software ou aplicação que irá criptografar as informações. Desta forma, durante o processo de estabelecimento de conexão segura (em inglês, *handshake*) entre o componente que irá enviar as informações criptografadas e o componente que irá receber as informações, ocorrerá também a transmissão dos certificados digitais intermediários utilizados para a criptografia dos dados;

- Chave pública de certificado digital de usuário final. A distribuição deste certificado digital para os interessados ocorre de forma automática. A chave pública é transmitida durante a fase de estabelecimento de conexões seguras ou como parte integrante das informações da assinatura digital em documentos.

O arquivo digital com a chave pública na maioria das vezes possui a extensão ".cer", é codificado em Base64 e apresenta duas linhas de texto característicos que o identificam (NOHE, 2018):

- A primeira linha contém o texto: -----BEGIN CERTIFICATE-----
- A última linha contém o texto: -----END CERTIFICATE-----

2.7 REPOSITÓRIO DE CERTIFICADOS DIGITAIS

Este componente é utilizado por vários softwares com o objetivo de organizar a administração dos certificados digitais. Estes são os repositórios mais comuns:

- Repositório *Windows Certificate Manager*: administrado pela ferramenta MMC no sistema operacional Microsoft Windows. Este repositório é utilizado por outros softwares e aplicativos que executam no mesmo computador. Os certificados administrados por estas ferramentas possuem visibilidade por usuário, computador ou conta de serviço. Assim, certificados adicionados na visão "usuários" não estarão visíveis para os demais usuários do computador. Certificados adicionados na visão "computador" (ou *local machine*) estarão visíveis para todos os usuários e serviços daquele computador (MICROSOFT, 2021).
- Repositório KDB: O repositório referenciado como *Key Database* (KDB) consiste de arquivos com extensão ".kdb" e que são gerenciados pela ferramenta keytool. Este arquivo é protegido por senha, que é cifrada em arquivo com extensão ".sth". A utilização em conjunto dos arquivos com extensão ".kdb" e ".sth" permite que estes softwares possam acessar os certificados digitais destes repositórios de forma segura.

- Repositório JKS: O repositório referenciado como *Java KeyStore* (JKS), utilizado em aplicações *Java* utiliza arquivos com extensão “.jks” (ou “.p12”) e é administrado pela ferramenta *ikeyman*. Também é possível administrar os certificados “CA Root” ou “CA Intermediate” na aba “*Root Authority Certificates*” do arquivo *cacerts* na instalação de programas Java, com visibilidade para todas as aplicações e softwares que utilizam aquela instalação do Java no computador, porém este arquivo não é preservado durante as operações de atualização do *Java* e o conteúdo pode ser perdido (SERVER_FAULT, 2013).
- Repositório OpenSSL ou GNUTLS: Algumas aplicações do sistema operacional Linux utilizam as bibliotecas *openssl* ou *gnults* para operações relacionadas com certificados digitais. Estas bibliotecas utilizam os arquivos de configuração para referenciar a localização dos arquivos com chaves públicas, privadas e de repositórios de certificados digitais utilizados (REDHAT, 2020).

Os certificados contidos em repositórios são organizados em pastas. As pastas mais comuns são: *Personal, Root Authority Certificates* e *Intermediate Authority Certificates*. Estes nomes podem variar em função da origem e idioma dos softwares. Na prática, a adição de arquivos “CA Root” ou “CA Intermediate” na pasta *Root Authority Certificates* (ou equivalente) em um determinado repositório, indica que aquela CA é confiável e todos os certificados digitais assinados por ela serão aceitos como confiáveis pelos software que fazem uso daquele repositório de certificados. Alguns produtos e softwares possuem ferramentas gráficas que permitem o gerenciamento destes repositórios de forma mais intuitiva. Na maioria das vezes a utilização de linhas de comandos utilizando as ferramentas de administração adequadas para cada repositório permite operações rápidas e seguras.

2.8 LISTA DE CERTIFICADOS REVOGADOS

A lista de certificados revogados, chamada de *Certificate Revocation List* (CRL, ou lista de certificados revogados), contém a relação de todos os certificados digitais emitidos por uma determinada CA e que foram revogados antes do prazo de expiração do certificado digital. A lista contém o número de série do certificado digital, a data e o motivo da revogação. Um certificado digital pode ser revogado por várias razões, entre elas (SILVA, 2020):

- O certificado digital deixou de ser utilizado, dentro do seu período de validade regular;
- Um funcionário da empresa, que possui certificado digital para acessar um determinado software ou equipamento teve o contrato de trabalho encerrado ou suspenso;
- Um equipamento ou software apresentou suspeita ou confirmação de invasão, com comprometimento das permissões e senhas atribuídas aos arquivos digitais com chaves privadas.

Para que o propósito do CRL seja atendido, será necessário que todos os equipamentos e softwares que façam uso de certificados digitais emitidos por aquela CA Root ou CA Intermediate, tenham acesso ao endereço digital publicado com a CRL. Algumas aplicações ou softwares não permitem acesso a um determinado site ou serviço se lhe for negado acesso ao endereço da CRL. Algumas operações envolvendo certificados digitais podem apresentar lentidão quando o endereço do CRL não estiver disponível, causando uma falha de comunicação com decurso de tempo (*timeout*) (DEACON; HURST, 2007).

2.9 APLICAÇÕES E USUÁRIOS FINAIS

As aplicações podem ser classificadas de acordo com os usos a que são submetidos. Algumas são desenvolvidas para operarem com o objetivo de fornecer serviços e informações e estão sempre preparadas para receber um pedido de comunicação de usuários finais. Elas são chamadas de aplicação servidor ou *application server* (INGALLS, 2021). Outras aplicações possuem a funcionalidade de originar chamadas e tentativas de conexões para uma aplicação servidor. Estas

aplicações são chamadas de aplicações cliente ou *application client* (INGALLS, 2021).

As aplicações *server* que se utilizam de canais de comunicação seguros para criptografar os dados trafegados, utilizam os certificados digitais para esta finalidade. Elas utilizam a chave privada para criptografar estas informações. Estas aplicações precisam ter acesso aos diretórios ou repositórios que contêm a CA Root e a cadeia de certificados intermediários utilizados. Durante a fase de estabelecimento da comunicação entre os pares, a aplicação *server* pode enviar os certificados intermediários para a aplicação *client*. Por este motivo, na maioria das vezes, não é necessário instalar a chave pública de certificados intermediários nos repositórios da aplicação cliente (SILVA, 2020).

A aplicação cliente que utiliza canais de comunicação seguros para estabelecer conexão com aplicação server, utilizam a chave pública para recuperar as informações criptografadas. Durante este processo, a aplicação cliente irá validar todos os certificados digitais utilizados, desde a CA Root e certificados intermediários até os certificados finais. A validação inclui a análise da data de validade do certificado digital, os atributos de finalidade e uso do certificado digital e a lista de certificados revogados (CRL). Se a validação não tiver sucesso em alguns dos requisitos, a tentativa de conexão será cancelada. As aplicações cliente também podem utilizar certificados digitais como credenciais de acesso com o objetivo de se identificar perante a aplicação server.

Algumas aplicações efetuam a criptografia dos dados que envia e recebe de outras aplicações. Nestes casos, ela irá utilizar simultaneamente funções de criptografia de modo server e client descritas anteriormente.

Aplicações que auxiliam no processo de assinatura digital de documentos possuem funcionamento similar ao descrito para aplicações server e quando é necessário validar a assinatura digital estampada em um documento, utiliza-se de aplicações com funcionamento similar ao descrito anteriormente para aplicação client.

3 APRESENTAÇÃO DOS RESULTADOS

Considerando os assuntos e aspectos apresentados, a gestão e administração dos certificados digitais resume-se: a) ciclo de vida; b) os envolvidos; c) a escolha da entidade certificadora; d) requisição de certificado digital; e) renovação do certificado digital; f) assinatura do certificado digital; g) recepção do certificado digital; h) proteção do certificado digital; i) inventário de certificado digital; j) distribuição da chave pública; k) instalação do certificado digital; l) validação e acompanhamento; e m) revogação do certificado digital.

3.1 CICLO DE VIDA

O ciclo de vida de um certificado digital envolve diversas fases (SILVA, 2020). Cada fase deve ser executada por pessoas ou equipes treinadas ou com conhecimento técnico suficiente para executar as atividades com segurança. Deve-se definir atribuições e responsabilidade para cada envolvido e as fases devem ser registradas para que se tenha o controle efetivo do processo, com rastreabilidade, para facilitar auditorias e relatórios atualizados dos certificados digitais.

3.2 OS ENVOLVIDOS

Considerando as pessoas e equipes envolvidas com todos os processos, estes são as atribuições e conhecimentos e atividades desempenhadas por cada um dos agentes (SILVA, 2020):

1. Responsável pelo software ou aplicação (*server*):
    - Iniciar o pedido de emissão do certificado digital, gerando o CSR;
    - Assegurar a integridade e segurança da chave privada;
    - Recepcionar o certificado digital assinado, com extensão .cer, e providenciar a sua instalação;
    - Garantir que o certificado digital foi instalado em todas as instâncias da aplicação e servidores envolvidos com o CN específico;

- Solicitar que as informações abaixo sejam adicionadas ao inventário:
  - data do evento;
  - CN e número de série do certificado digital;
  - nome da aplicação;
  - locais de instalação e repositórios e tipo do repositório;
  - nome dos equipamentos de hardware envolvidos;
  - Situação da aplicação: Ativa ou inativa;
  - Situação: Certificado digital instalado.

2. Responsável pela emissão do certificado digital:
   - Recepcionar os pedidos CSR de emissão e renovação de certificados digitais;
   - Analisar os pedidos de certificados digitais;
   - Operar as ferramentas de gerenciamento de entidades certificadoras, promovendo a emissão e revogação dos certificados digitais;
   - Assinar os pedidos de emissão de certificados digitais;
   - Enviar para o emissor do pedido CSR o certificado digital assinado;
   - Solicitar que as informações abaixo sejam adicionadas ao inventário:
     - data de emissão do certificado digital;
     - data e hora de validade (inicial e final) do certificado digital;
     - *CN* do certificado digital;
     - Situação: Certificado digital emitido, Certificado digital Revogado ou Descontinuado.
3. Responsável pelo inventário dos itens relacionados com o certificado digital:
   - Anotar em base de dados apropriada as informações relativas ao certificado digital;
   - Emitir relatórios com certificados digitais que irão expirar dentro de um número específico de dias;
   - Emitir relatórios com planejamento de certificados digitais com expiração nos próximos anos e meses;
   - Emitir relatórios com relação de digitais que foram emitidos;
   - Emitir relatórios de localização de cada certificado digital.

4. Responsável pela manutenção dos repositórios de Certificados digitais compartilhados ou do sistema operacional:
    - Efetuar a distribuição da CA utilizada para assinatura dos certificados digitais
    - Solicitar que as informações abaixo sejam adicionadas ao inventário:
        - data de emissão do certificado digital;
        - data e hora de validade (inicial e final) do certificado digital;
        - CN do certificado digital;
        - Situação: Certificado digital emitido, Certificado digital Revogado ou Descontinuado.
5. Responsável pela manutenção dos repositórios de Certificados digitais:
    - Efetuar a distribuição da *CA* utilizada para assinatura dos certificados digitais quando houver necessidade, motivada pela renovação de *CA* ou mudança do fornecedor de serviços de emissão de certificados digitais externos;
    - Fornecer subsídios técnicos ou listar o conteúdo dos repositórios de certificados digitais, quando for necessário;
    - Guardar em locais seguros a senha utilizadas para administração dos repositórios;
    - Solicitar que as informações abaixo sejam adicionadas ao inventário:
        - CN do certificado digital da CA ou CA Intermediate*;*
        - data e hora de validade (inicial e final);
        - locais de instalação e repositórios;
        - Situação: Certificado CA Instalado.

3.3 A ESCOLHA DA ENTIDADE CERTIFICADORA

Diversos fatores influenciam a escolha da entidade certificadora utilizada por uma empresa ou conglomerado de empresas. Pode-se optar pela duas modalidades de gestão de certificados digitais considerando o tipo de entidade certificadora (SILVA, 2020):

1. Entidade certificadora própria:
    - Os custos envolvidos estão relacionados com a aquisição e manutenção dos aplicativos e ferramentas utilizadas para a gestão dos certificados digitais;
    - Procedimentos de distribuição da chave pública da CA Root utilizada pela empresa (durante a fase de implementação ou durante a renovação do certificado digital da CA Root) que deve distribuir o certificado digital para todos os repositórios de certificados em uso na empresa, considerando estações e servidores. Considerar também que a distribuição destes arquivos podem ser necessários para empresas parceiras ou subcontratadas, que acessam sites internos ou serviços que utilizam certificados emitidos por aquelas CA Root ou CA intermediate.
    - Manutenção de equipes treinadas e disciplinadas para a gestão das emissão dos certificados digitais da Entidade Certificadora e seus certificados intermediários;
    - Administração e configuração dos softwares utilizados para a gestão dos certificados digitais;
    - Definição do prazo de validade dos certificados digitais emitidos internamente, para atender os requisitos de negócios. Esta periodicidade deve ser definida com critérios técnicos e em conformidade com os padrões de segurança adotados pela empresa. Na maioria das vezes esta periodicidade não ultrapassa os 2 anos;
    - Definição dos procedimentos que serão adotados pelas equipes que irão emitir e manipular os certificados digitais.
2. Entidade certificadora de terceiros:
    - Os custos envolvidos estão relacionados com o pagamento de valores relativos à emissão ou renovação dos certificados digitais emitidos. Pode-se pagar por certificado digital emitido individualmente ou por lotes de certificados digitais emitidos. Os valores cobrados estão relacionados com a quantidade de equipamentos que atendem determinado CN. Por exemplo, se o “CN=www.site.com.br” estiver distribuído em vários servidores, serão necessárias requisições de certificados (CSR) em número suficiente para distribuir um certificado digital para cada servidor

que atende aquele endereço. Cada certificado digital emitido será contabilizado para questões de faturamento e cobrança;

- Administração e configuração dos softwares utilizados para a gestão dos certificados digitais, executadas em ferramentas providas pela entidade certificadora;
- Definição dos procedimentos que serão adotados pelas equipes que irão emitir e manipular os certificados digitais.

Independente da modalidade utilizada, será necessário a definição dos prazos máximos para que uma atividade de emissão de certificados digitais seja concluída. Este prazo deve ser levado em consideração quando um determinado projeto demanda novos certificados digitais ou com qual antecedência as operações de renovações de certificados digitais devem ser iniciadas para que o certificado digital vencendo possa ser substituído antecipadamente pelo novo certificado sem interrupção das operações e serviços.

3.4 REQUISIÇÃO DE CERTIFICADO DIGITAL

Algumas atividades de TI envolvem atividades relacionadas com a criação de novos certificados digitais e a renovação periódica de certificados digitais. A criação de novos certificados digitais ocorre quando há demanda em novos projetos, criação de novos sites, admissão de novos funcionários ou utilização de novos produtos ou softwares, entre outros. A renovação de certificados digitais irá ocorrer de forma frequente e recorrente justamente pela presença de data de validade (início e fim de validade).

Nas situações mencionadas acima, as pessoas ou equipes envolvidas com a operação dos certificados digitais, previamente autorizadas para esta atividade, deverão iniciar o procedimento de emissão da requisição do certificado digital, gerando uma requisção CSR correspondente. Como mencionado anteriormente, deve-se manter a posse do arquivo que contém a chave privada de forma segura, preferencialmente dentro de repositórios protegidos com senha. O processo de geração do CSR deverá ser executado com todos os atributos considerados necessários, e as informações dos atributos devem seguir a padronização indicada (SILVA, 2020).

Por exemplo:

CN=www.site.com.br, *OU*=Depto de Informatica, *O*=Empresa Site,*L*=Curitiba, *ST*=Parana, *C*=BR
Alternate Name: www.site.com.br

Após a geração da requisição CSR, o arquivo digital resultante (apenas o arquivo com extensão .csr) deve ser encaminhado para as pessoas ou equipe responsável pela operação efetiva das ferramentas de gestão de certificados digitais. Este é o momento para indicar o inventário dos certificados digitais de que uma atividade de emissão ou renovação de certificados digitais para aquele CN está em andamento. Desta forma, será possível acompanhar o progresso desta atividade.

3.5 RENOVAÇÃO DO CERTIFICADO DIGITAL

Os certificados digitais são emitidos com períodos de validades variáveis, sendo 1 ano para certificados digitais emitidos por entidades certificadoras externas e a cada 2 anos para certificados digitais emitidos por entidades certificadoras internas (SILVA, 2020). Estes prazos podem variar de acordo com as definições atribuídas pelo gestor da entidade certificadora ou da modalidade de certificado digital emitido por entidades certificadoras comerciais ou por critérios técnicos adotados pela empresa. A renovação de certificados digitais deve ocorrer preferencialmente com alguns dias de antecedência antes da data de expiração, evitando a interrupção do serviço que utiliza o certificado digital.

Este é o momento para iniciar uma investigação para determinar se o site, serviço ou software ainda está em operação. Se constatado que não é mais necessário, pode-se optar pela revogação do certificado digital associado ou aguardar até a data de expiração, se próxima. Registrar no inventário de certificados digitais a condição do serviço (ativo ou inativo) e a situação do certificado digital (renovar, revogar, aguardar expiração).

Recomenda-se que a cada renovação de certificado digital ocorra também a substituição da chave privada utilizada para aquele certificado digital e consequentemente a geração de uma nova requisição (CSR). Esta recomendação tem o intuito anular a possibilidade de comprometimento da segurança em caso de exposição indevida da chave privada utilizada anteriormente.

As datas de expiração para certificados digitais emitidos e em uso devem ser levadas em consideração para evitar ultrapassar a data/hora da expiração, preferencialmente ocorrendo com antecedência de alguns dias. Vários fatores podem influenciar na conclusão da atividade de renovação do certificados digital (ausências não previstas de funcionários, falha no processo de geração do certificado digital, falha no processo de renovação, entre outros) assim é recomendado adiantar o processo de renovação para que haja tempo hábil para uma nova tentativa de renovação.

3.6 ASSINATURA DO CERTIFICADO DIGITAL

Considerando as recomendações de segurança aplicáveis ao processo de renovação, a emissão de novos certificados digitais e renovação de certificados digitais podem ser tratados com os mesmos procedimentos, que deverão iniciar com a posse do pedido de emissão de certificado digital (CSR), que deverá ser executado por equipes ou pessoas autorizadas e treinadas para tais procedimentos, utilizando a entidade certificadora preferencial para a emissão do certificado digital.

O processo de assinatura ou emissão do certificado digital ocorre quando os atributos definidos no arquivo digital que possui a requisição são validados e assinados digitalmente utilizando a chave privada da entidade certificadora que foi designada para esta operação. O resultado desta operação será a emissão do arquivo digital que contém a chave pública do certificado digital, com validade estipulada pelo gestor da entidade certificadora. Este arquivo deverá ser encaminhado para a pessoa ou equipe que iniciou o pedido de emissão do certificado digital e que detém a posse da chave privada.

Nesta etapa é designado um número de série para cada certificado digital assinado e este é o momento para incluir no inventário dos certificados digitais o apontamento de que uma atividade de emissão de certificados digitais para aquele CN foi iniciada.

Indicar no inventário as informações do requerente, CN do certificado digital, número de série, CN da entidade certificadora e data de vencimento do certificado digital.

3.7 RECEPÇÃO DO CERTIFICADO DIGITAL

As pessoas ou equipes responsáveis pela recepção deverão adotar as políticas da empresa e agendar a instalação dos certificados seguindo os critérios técnicos. Para cada certificado digital instalado, efetuar a monitoração da situação anterior e situação após a efetivação da instalação e ativação do certificado digital na aplicação e validar se houve mudanças na data de vencimento, CN do certificado digital e CA Root. Mudanças inesperadas no novo certificado digital em CN, CA Root ou datas de vencimentos inválidas podem ocasionar interrupção dos serviços e impactos para as aplicações.

Algumas ferramentas de administração de repositórios de certificados digitais podem atribuir uma etiqueta (em inglês, *label*) à chave privada que foi gerada durante a geração do CSR. Desta forma é possível a convivência de vários certificados digitais relativos ao mesmo CN dentro do mesmo repositório porém com label distintos. O processo de geração do arquivo CSR e importação do certificado digital assinado pode ser realizado de forma antecipada controlada sem interrupção dos serviços associados ao certificado digital atual. Na data agendada para a efetiva substituição do certificado digital, será necessário configurar o software que irá agora apontar para o novo label. A Tabela 2 demonstra vários certificados digitais presentes dentro do mesmo repositório, com labels diferentes. Considerando os dados presentes na tabela abaixo, a mudança aplicada ao software será o apontamento de “www.site.com.br-2020” para “www.site.com.br-2021”.

Tabela 2 - Lista de certificados digitais em um repositório

CN	Label	Tipo	Validade
www.site.com.br	www.site.com.br-2019	Certificado	00:00 de 01/jan/2019 até 23:59 de 01/dez/2020
www.site.com.br	www.site.com.br-2020	Certificado	00:00 de 01/nov/2020 até 23:59 de 01/nov/2021
www.site.com.br	www.site.com.br-2021	Certificado	00:00 de 01/out/2021 até 23:59 de 01/out/2022

Fonte: Autoria própria.

Registrar no inventário de certificados digitais nova a situação do certificado digital (renovado), bem como a nova data de expiração, número de série e o nome da *CA* que foi utilizada para a emissão do certificado digital.

3.8 PROTEÇÃO DO CERTIFICADO DIGITAL

O acesso indevido, praticado por terceiros, ao arquivo digital que contém a chave privada do certificado digital de um determinado site poderá permitir que pessoas não autorizadas possam criar sites falsos e apresentá-los como se fossem legítimos (SCHMIED *et al.*, 2003). Assim independentemente dos usos que se passam para os certificados digitais, alguns itens constituem elementos básicos de segurança:

- A correta configuração de permissão de acesso ao arquivo digital onde a chave privada está inserida, seja ela, arquivos digitais ou repositórios de certificados digitais. Recomenda-se atribuir ao arquivo apenas permissão de leitura atribuída ao usuário que irá manipular o certificado digital durante o funcionamento da aplicação ou software;
- Os arquivos digitais onde está inserida a chave privada ou arquivos digitais utilizados por repositórios de certificados digitais devem possuir senhas fortes e devem ser considerados como de acesso restrito (SCHMIED *et al.*, 2003);
- Não transmitir os arquivos de chaves privadas digitais para locais externos e não permitir manipulação destes arquivos por pessoas não autorizadas ou sem treinamento técnico adequado (SILVA, 2020). Caso seja necessário transmitir o arquivo digital de chave privada para locais externos, registrar este evento indicando o motivo, datas, horários, nome da pessoa que efetuou o envio, nome da pessoa que irá receber o arquivo e descrição dos elementos de software e hardware que irão acessar e manipular os arquivos. Estes registros devem ser consultados sempre que se fizer necessário à análises forenses, auditorias internas ou quando houver suspeitas de comprometimento dos componentes que utilizam as chaves privadas.

3.9 INVENTÁRIO DE CERTIFICADO DIGITAL

Definir procedimentos para cadastramento adequado das informações de um certificado digital, permitindo a rastreabilidade dos componentes, locais de instalação, período de validade, entidades certificadoras e elementos que possam ser utilizados durante procedimentos de auditoria e análises forenses.

3.10 DISTRIBUIÇÃO DA CHAVE PÚBLICA

Uma vez definidas as Entidades Certificadoras que irão emitir determinados certificados digitais, será necessário assegurar que os elementos que irão utilizar os certificados digitais, sejam eles *Server* ou *Client*, estão preparados para utilizar aquela CA, tanto para a assinatura digital das informações que serão enviadas para o requisitante, quanto para o elemento que irá receber as informações assinadas pelo certificado digital. Para isso é necessário a prévia distribuição dos certificados digitais envolvidos na emissão.

3.11 INSTALAÇÃO DO CERTIFICADO DIGITAL

O processo de instalação do certificado digital em repositórios envolve arquivo assinado (.cer) que será combinado com o arquivo privado (.key) e instalado no repositório de Certificados da aplicação *server* que irá assinar digitalmente as informações.

3.12 VALIDAÇÃO E ACOMPANHAMENTO

Para garantir que o certificado digital foi instalado corretamente em todos os pontos de utilização definidos será necessário executar imediatamente após o processo de instalação rotinas de validação. O processo de validação deverá assegurar que as informações de datas de validade inicial e final, número de série (ou impressão digital) e entidade certificadora são apresentados corretamente e com as informações esperadas.

O processo de validação também deverá ser executado de forma regular, podendo ser de periodicidade mensal ou de diária, conforme a importância dada a aquele conjunto de certificados digitais monitorados. A periodicidade do processo de monitoração definido deverá estar adequada para fornecer com antecedência necessária as informações de validade, de forma que todas as atividades de um processo de renovação do certificado digital possam ser agendadas com antecedência e adequado aos processos burocráticos definidos na organização.

3.13 REVOGAÇÃO DO CERTIFICADO DIGITAL

Em determinadas situações pode ser necessário garantir que um determinado certificado digital não possa mais ser utilizado, seja pela desativação da aplicação, desativação do site, encerramento ou suspensão do contrato de trabalho de funcionários ou desativação de servidores onde o certificado digital estava instalado, ou em caso de comprometimento da segurança dos arquivos ou servidores. Nestes casos faz-se necessário a revogação do certificado digital.

Durante o processo de revogação do certificado digital, será necessário obter o número de série e o nome da CA utilizada para a emissão do certificado digital em questão. Esta informação poderá ser recuperada através da análise do próprio certificado digital ou em caso de extravio deste, poderá ser recuperado do inventário dos certificados mantidos pela empresa.

Quando um processo de revogação é realizado, uma nova lista de certificados digitais revogados (CRL) será gerada e nela constará o número de série do certificado digital revogado, bem como a data e hora em que a revogação teve efeito. É obrigatório a publicação desta lista em endereço eletrônico acessível a todos os componentes envolvidos na utilização do certificado digital revogado.

4 CONCLUSÃO

O entendimento do funcionamento dos softwares e a relação com os respectivos repositórios de certificados devem ser levados em conta para o correto funcionamento das aplicações e visibilidade dos certificados administrados. A solução dos principais problemas de administração de certificados digitais estão relacionados com:

1. A utilização de uma nova CA Root ou CA Intermediate ou a substituição de CA em utilização;
2. A correta identificação dos repositórios associados com as aplicações e a execução de procedimentos de inclusão de novos certificados nas pastas corretas dentro destes repositórios;
3. O gerenciamento da expiração da data de vencimento do certificado digital.

O correto entendimento do funcionamento, das nomenclaturas, da estrutura e componentes que compõem os certificados digitais são essenciais para a sua administração segura, evitando interrupção de serviços e atividades.

REFERÊNCIAS

DEACON, Alexand; HURST, Ryan. **The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments**. Copyright© The IETF Trust, publicado em: set. 2007. Disponível em: <https://www.rfc-editor.org/rfc/pdfrfc/rfc5019.txt.pdf>. Acesso em: 29 out. 2021.

INGALLS, Sam. **What Is a Client-Server Model? A Guide to Client-Server Architecture**. Copyright© TechnologyAdvice, publicado em: 17 nov. 2021. Disponível em: <https://www.serverwatch.com/guides/client-server-model/ https://en.wikipedia.org/wiki/Client%E2%80%93server_model>. Acesso em: 21 nov. 2021.

MICROSOFT. **Local Machine and Current User Certificate Stores**. Copyright© Microsoft, publicado em: 14 dez. 2021. Disponível em: <https://docs.microsoft.com/en-us/windows-hardware/drivers/install/local-machine-and-current-user-certificate-stores>. Acesso em: 27 nov. 2021.

NOHE, Patrick. **How to convert a certificate to the correct format**: Instructions on how to convert digital certificates from one file format to another. Copyright© The SSL Store™, publicado em; 18 out. 2018. Disponível em: <https://www.thesslstore.com/blog/how-to-convert-a-certificate-to-the-correct-format/>. Acesso em: 29 out. 2021.

PUBLICO, Ricky Jay. **Noções Básicas de SSL: O que é Solicitação de Assinatura de Certificado (CSR)?** Copyright© GlobalSign, publicado em: 19 fev. 2021. Disponível em: <https://www.globalsign.com/pt-br/blog/what-is-a-certificate-signing-request-csr>. Acesso em: 3 nov. 2021.

REDHAT. **Using Shared System Certificates**. Copyright© Red Hat, Inc., publicado em: 26 jan. 2020. Disponível em: <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-shared-system-certificates>. Acesso em: 27 nov. 2021.

SERVER_FAULT. **Preserve imported CA Certificates through Java upgrades**. Copyright© Stack Exchange Inc, publicado em: 13 out. 2013. Disponível em: <https://serverfault.com/questions/636612/preserve-imported-ca-certificates-through-java-upgrades>. Acesso em: 27 nov. 2021.

SCHMIED, Will; *et al*. **Building DMZs for Enterprise Networks**, Syngress Publishing, Rockland, 2003, 744p.

SILVA, Hebert de Oliveira, **Criptografia (Série Universitária)**. Editora Senac São Paulo. 2020. 146p.