CAFA

Para Certificados Digitais

Versão 1.0

Equipe de Desenvolvimento

|  |
| --- |
| **Integrantes** |
| Arthur Barbato da Silva |
| Daniel Souza da Cruz |
| Eduardo Gabriel Zacarias Pereira |
| Fernando Scolari Camargo |
| Michel Da Silva Galvão |

Tabela de Conteúdo

**1.** **Introdução** 4

1.1 Finalidade 4

1.2 Escopo 4

1.3 Definições, Acrônimos, e Abreviações 4

**2**. **Descrição** **Geral** 4

2.1 Funções do Software 4

2.2 Restrições 4

2.3 Suposições e Dependências 4

2.4 Subconjuntos de Requisitos 5

**3. Requisitos Específicos** 5

3.1 Requisitos Funcionais 5

3.1.1 Conversão de .pfx para .crt e .key 5

3.1.2 Conversão de .crt e .key para .pfx 6

3.1.3 Local de Destino 6

3.1.4 Mensagens 6

3.2 Requisitos Não Funcionais 6

3.2.1 Requisitos de Usabilidade 6

3.2.2 Requisitos de Confiabilidade 7

3.2.3 Requisitos de Suportabilidade 7

Especificação de Requisitos de Software

# Introdução

Gerenciar certificados digitais pode ser complicado, especialmente quando precisamos converter entre os formatos .pfx, .crt e .key. Esses formatos são comuns para armazenar e usar certificados em várias aplicações. A conversão manual pode ser tediosa e propensa a erros, exigindo conhecimento técnico e ferramentas específicas.

O Cafa é uma solução intuitiva que simplifica essa conversão. Com uma interface amigável e recursos automatizados, ele permite que usuários de todos os níveis convertam arquivos .pfx para .crt e .key (e vice-versa) de maneira rápida e segura

## Finalidade

Este documento serve como Especificação de Requisitos de Software (SRS) para o Cafa, uma ferramenta desenvolvida para facilitar a conversão de arquivos de certificado digital entre os formatos .pfx, .crt e .key. Este documento servirá como um guia para o desenvolvimento, garantindo que todas as necessidades e expectativas dos stakeholders sejam atendidas de maneira precisa e compreensível.

## Escopo

O software de conversão de certificados digitais será uma ferramenta desktop que permitirá aos usuários converter arquivos de certificado .pfx para os formatos .crt e .key, e vice-versa. O sistema atenderá principalmente a usuários de forma geral, podendo ser tanto usuario leigos até os mais experientes. Ele oferecerá uma interface intuitiva, suporte a múltiplos formatos de entrada e saída, e garantirá a segurança dos dados durante o processo de conversão.

## Definições, Acrônimos e Abreviações

* **Certificado Digital**: Um arquivo que autentica a identidade de uma entidade (pessoa, organização, dispositivo) na internet.
* **Formato** **PFX/PKCS#12**: Personal Information Exchange, um formato de arquivo que contém o certificado público e a chave privada.
* **Formato** **CRT**: Certificate, um arquivo que contém apenas o certificado público.
* **Formato** **KEY**: Key, um arquivo que contém apenas a chave privada de um certificado digital.
* **Conversão**: Processo de transformar um arquivo de certificado de um formato para outro.

# Descrição Geral

O Cafa é uma ferramenta de desktop autônoma que visa facilitar a conversão de arquivos de certificado digital entre os formatos .pfx, .crt e .key. Ele será projetado para operar em ambientes desktop, oferecendo uma interface gráfica amigável. O sistema será integrado com bibliotecas de criptografia reconhecidas, como OpenSSL, para garantir a precisão e a segurança das conversões.

## Funções do Software

As principais funções do Cafa incluem:

* **Conversão de .pfx para .crt e .key**: Permitir que os usuários convertam arquivos .pfx em arquivos .crt e .key separados.
* **Conversão de .crt e .key para .pfx**: Facilitar a combinação de arquivos .crt e .key em um único arquivo .pfx.
* **Suporte para senhas**: Proteger seus certificados com senha durante a conversão.
* **Segurança e Criptografia**: Garantir que as operações de conversão mantenham a segurança dos dados, implementando boas práticas de criptografia.
* **Suporte Multiplataforma**: Funcionar em diferentes sistemas operacionais, incluindo Windows, macOS e Linux.

## Restrições

O desenvolvimento do Cafa depende das seguintes suposições e dependências:

* Substituir ferramentas de criptografia avançadas ou soluções de gerenciamento de certificados corporativos.
* Ser usado para fins ilegais ou maliciosos.
* Armazenar ou gerenciar certificados digitais em nuvem.
* O sistema depende de bibliotecas como OpenSSL para realizar operações de criptografia e conversão de certificados, o que implica em um monitoramento contínuo para atualizações e patches de segurança.

## Suposições e Dependências

O desenvolvimento do Cafa depende das seguintes suposições e dependências:

* Compatibilidade com os principais sistemas operacionais desktop, como Windows, macOS e Linux.
* O sistema dependerá de bibliotecas como OpenSSL para realizar operações de criptografia e conversão de certificados.
* O software deve ser atualizado regularmente para incorporar as últimas práticas de segurança e corrigir vulnerabilidades.

## Subconjuntos de Requisitos

O Cafa pode ser dividido em subconjuntos de requisitos com base em diferentes critérios, como:

* **Requisitos Funcionais**: Descrevem as funcionalidades específicas que o sistema deve oferecer, como conversão de arquivos, visualização de detalhes de certificados, etc.
* **Requisitos Não Funcionais**: Incluem aspectos como performance, usabilidade, segurança e compatibilidade.
  + **Compatibilidade**: O software deve ser compatível com os principais sistemas operacionais (Windows, macOS, Linux)
  + **Segurança**: Deve implementar mecanismos robustos de segurança para proteger as chaves privadas e outros dados sensíveis durante a conversão.
  + **Performance**: A conversão de certificados deve ser rápida e eficiente, mesmo para arquivos de grande tamanho.
  + **Usabilidade**: A interface deve ser intuitiva e fácil de usar, minimizando a necessidade de treinamento ou conhecimento técnico avançado.

# Requisitos Específicos

Esta seção detalha todos os requisitos de software de forma que os projetistas possam criar um sistema que atenda a esses requisitos e os testadores possam verificar sua conformidade. Á organização está feita por recurso, abordando aspectos funcionais, capacidades e segurança.

## Requisitos Funcionais

Esta seção descreve os requisitos funcionais do Cafa, detalhando as funcionalidades que o software deve oferecer aos usuários.

### **Conversão de .pfx para .crt e .key**

O sistema deve permitir a conversão de arquivos .pfx em arquivos .crt e .key separados.

* **Entrada**: Arquivo .pfx, senha opcional para o arquivo.
* **Processamento:** Extração do certificado e da chave privada do arquivo .pfx.
* **Saída**: Arquivos .crt e .key

### **Conversão de .crt e .key para .pfx**

O sistema deve permitir a combinação de arquivos .crt e .key em um único arquivo .pfx.

* **Entrada**: Arquivos .crt e .key, senha opcional para o arquivo .pfx gerado.
* **Processamento:** Combinação dos arquivos .crt e .key em um arquivo .pfx.
* **Saída**: Arquivo .pfx.

### **Local de destino**

O software deve permitir aos usuários especificar o local de destino para os arquivos convertidos.

### **Mensagens**

O software deve mandar mensagens informativas informando o sucesso ou o erro na conversão.

## Requisitos Não Funcionais

Esta seção descreve os requisitos não funcionais do Cafa, detalhando as características e padrões de qualidade que o software deve atender para garantir uma experiência satisfatória aos usuários

### **Requisitos de Usabilidade**

Esta seção define os requisitos de usabilidade para um software de conversão de certificados, com foco em garantir que o software seja fácil de usar, intuitivo e eficiente para usuários de todos os níveis de conhecimento.

* **3.2.1.1 Tempo de Treinamento**

1. Software deve ser intuitivo e fácil de usar, permitindo que usuários normais realizem conversões básicas de certificados sem a necessidade de treinamento formal.
2. Tempo médio para um usuário normal se familiarizar com as funcionalidades básicas do software e realizar conversões simples deve ser inferior a 15 minutos.

* **3.2.1.2 Navegação intuitiva**

1. O sistema deve permitir a navegação intuitiva, com menus e opções claramente identificados e acessíveis.

### **Requisitos de Confiabilidade**

Esta seção define os requisitos de usabilidade para um software de conversão de certificados, com foco em garantir que o software seja fácil de usar, intuitivo e eficiente para usuários de todos os níveis de conhecimento.

* **3.2.1.1 Tempo de Treinamento**

1. Software deve ser intuitivo e fácil de usar, permitindo que usuários normais realizem conversões básicas de certificados sem a necessidade de treinamento formal.
2. Tempo médio para um usuário normal se familiarizar com as funcionalidades básicas do software e realizar conversões simples deve ser inferior a 15 minutos.

* **3.2.1.2 Navegação intuitiva**

1. O sistema deve permitir a navegação intuitiva, com menus e opções claramente identificados e acessíveis.

### **Requisitos de Suportabilidade**

Esta seção define os requisitos de suportabilidade para um software de conversão de certificados, garantindo que seja fácil de manter, atualizar e reparar

* **3.2.3.1 Padrões de Codificação**

1. Todos os componentes do sistema devem aderir aos padrões de codificação definidos pela comunidade de desenvolvimento, como o estilo de codificação JavaScript padrão.
2. Variáveis, funções e classes devem ser nomeadas de forma descritiva e seguir uma convenção de camelCase para JavaScript e CSS.

* **3.2.3.2 Bibliotecas e Frameworks**

1. Utilizar **Electron** para criar uma aplicação desktop multiplataforma que integra nativamente com o sistema operacional do usuário.
2. Implementar bibliotecas confiáveis para manipulação de certificados, como **forge** para manipulação de certificados