

# Guia para Emissão e Configuração de Certificados SSL no Portal Ema

O objetivo deste documento é orientar clientes da Ema Sistemas na emissão e configuração de certificados SSL para uso em domínios próprios no Portal Ema.

A utilização do **HTTPS** (HTTP sobre SSL/TLS) garante uma camada adicional de segurança na comunicação entre o navegador e o servidor, protegendo os dados transmitidos por meio de criptografia.

## □ Etapas para emissão e configuração do certificado SSL

### 1. Registrar um domínio próprio

O primeiro passo é garantir que o cliente possua um **domínio registrado em seu nome**, como `suaempresa.com.br`. Esse domínio servirá de base para criação do endereço de acesso ao Portal Ema, por exemplo: `dox.suaempresa.com.br`

Se o cliente ainda não possui um domínio, é necessário registrar um através de sites como o [Registro.br](#) ou provedores de hospedagem (KingHost, GoDaddy, HostGator, etc.). Nós da Ema não realizamos o registro para o cliente, mas podemos instruí-lo a como fazer.

“□ registro de domínio é um serviço pago.

---

### 2. Hospedar o domínio

Após o registro, o domínio deve estar vinculado a um serviço de **hospedagem com suporte à emissão de certificados SSL**. Indicamos serviços como **KingHost** ou similares, que já oferecem emissão de certificados SSL do tipo que o sistema exige.

“ hospedagem do domínio também é um serviço pago.

### 3. Criar o subdomínio e emitir o certificado SSL

Com o domínio hospedado:

- Crie o subdomínio que será utilizado no acesso ao Portal Ema (ex: `dox.suaempresa.com.br`).
- Solicite no serviço de hospedagem a emissão do **certificado SSL para este subdomínio**, garantindo que o formato gerado seja compatível com o sistema da Ema: `.PEM` ou `.CRT`.
- **Caso a hospedagem não ofereça a emissão do certificado SSL**, será necessário buscar uma **certificadora terceirizada** especializada nesse serviço. Essa alternativa exige atenção redobrada, pois envolve um processo mais técnico e pode demandar etapas adicionais de validação e configuração.

A emissão pode levar até **1 dia útil**, a depender do provedor de hospedagem.

### 4. Configurar o certificado no Ema Configurador

Com o certificado em mãos, siga os passos abaixo com apoio do Suporte da Ema para integrá-lo ao sistema:

- Abra o **Ema Configurador** e edite o registro da conexão.
- Defina a **porta principal como 443** (HTTPS padrão). Portas alternativas também são permitidas, desde que especificadas corretamente no endereço de conexão.
- Marque a opção **Utiliza HTTPS**.
- Nos campos **Certificado e Arq. Senha** procure e informe o certificado no formato **.PEM** ou **.CRT**.
- Caso o cliente esteja executando o sistema anteriormente com uma conexão HTTP, altere o caminho de conexão no arquivo:  
`C:\Ema Software\Contas ERP\Ema_Conexao_Servidor.ini`, substituindo o protocolo de `http` para `https` e ajustando a porta.

### 5. Testar a inicialização do sistema com SSL

Caso os micros serviços do sistema não iniciem, execute o seguinte teste manual:

- Abra o terminal do Windows (Prompt de Comando).
- Execute: `C:\Ema_Software\Contas_ERP\fabio.exe" -cfg fabio.properties`

Esse comando tenta inicializar o serviço com o certificado SSL configurado e mostrará mensagens de erro úteis para diagnóstico.

“ Se o sistema estiver online, pare os serviços pelo `Ema_Start` antes de testar.

## i Informações importantes

- **Clientes que contratam o Cloud Server da Ema:** o domínio fornecido para acesso ao cloud **não pode** ser usado para emissão de certificados SSL. O cliente deve possuir um domínio próprio.
- **Opção gratuita com Let's Encrypt:** também é possível emitir certificados gratuitamente com o [Let's Encrypt](#). Essa opção exige conhecimento técnico em **Linux**, que o cliente renove o certificado a cada 90 dias e nos envie os arquivos atualizados antes do vencimento para garantir a continuidade do acesso seguro.

## FAQ — Perguntas frequentes

### Quem é responsável por emitir o certificado SSL?

“ O cliente da Ema é o responsável por emitir o certificado SSL.

### Quais formatos de certificados são compatíveis com o Portal Ema?

“ `.PEM`, `.CRT` e, quando necessário, `.KEY` (arquivo de senha).

### Como emitir o certificado SSL?

“

Recomendamos verificar se o serviço de hospedagem do domínio já oferece essa funcionalidade. Caso contrário, o cliente pode utilizar uma certificadora externa ou o Let's Encrypt. [Siga os passos citados anteriormente.](#)

## Qual porta devo informar no Ema Configurador?

“ A porta padrão é **443**, mas é possível utilizar portas alternativas. Nesse caso, informe a porta que deseja utilizar no Ema Configurator e adicione a porta ao final do endereço de conexão.

## O sistema redireciona HTTP para HTTPS automaticamente?


“ Não. Para isso, recomendamos utilizar o **serviço de redirecionamento HTTP do IIS** (Windows Server). Basta instalar a função IIS, adicionar o recurso de redirecionamento e configurar a URL de destino em HTTPS.

- Exemplo: <https://www.contoso.com/sales>
- Caso o certificado no formato **.PEM** esteja corrompido ou com estrutura inválida, o Microsoft Edge não será responsável pela comunicação segura, o **Fabio, não será iniciado**.
- É essencial garantir que o arquivo contenha a **chave privada correta**, seja embutida no **.PEM** ou fornecida separadamente como arquivo **.KEY**. A seguir um exemplo de como a chave privada deve estar configurada no arquivo:

arquivo Bloco de Notas

Arquivo Editar Formatar Exibir Ajuda

# Estrutura esperada dos arquivos de certificado

A utilização de um certificado no formato .PEM, o conteúdo do arquivo deve seguir o padrão esperado, não sendo aceito o conteúdo público e a chave privada. Caso opte por usar arquivos separados (.CRT e .KEY), configure-os da seguinte forma no Ema Configurator: 

Abaixo um exemplo de

srH87gGdbXB4cP3bR7E8THjwmFFPbfuBFfueD7z5XB06yEC4eypldg3R90schp17

L0PKpcUbvXE/K23btATp9tZoyunWRmrtmTI4Pz/2IECgYEA57YDkIx1b7YMOCTS  
C7MMvsAh1DbVb4++Sn9VETeATIIssP9HmKDznGcy5Wedps+EzqVbP2k11cFApbKo

# Configuração da chave RSA para compatibilidade com o Node.js

Em determinadas situações, especialmente ao atualizar o certificado, pode ser necessário configurar a chave RSA para que os serviços desenvolvidos em Node.js funcionem corretamente.

“ **Recomendamos executar este procedimento sempre que um novo certificado for gerado.**

Com o arquivo `.KEY` em mãos, execute o comando abaixo no **Terminal do Windows**, utilizando o **OpenSSL**: `openssl pkey -in arquivo-key.pem -out arquivo-rsa-key.pem -traditional`

Esse comando converte a chave privada para o formato tradicional RSA exigido por alguns serviços internos.

-----BEGIN RSA PRIVATE KEY-----  
MIIGAwIBAgCNEAQCZ1G5XXM4VnVhflC4p220R6QANDE3Q0VhO0VkbBAn  
qThXa10dLkCsP708/z8393yK099E8+3cn6qaJnXelpng02TJmms00Kqzu2t2K6  
aeOMBWJt7RkJaDbTWfW+Ubc6Yb0jzE0+vaSGcoFnMWm9xnf5NZ0KmV9vMACPfw8  
h7QzNg3vcKFdQsf1mkP3HeKtiQKb4AMy5644Z7ptGQ2Ov4xcVCS03fw/CPZIr0gS  
uX3w2XkuaBfR45BzygrmPyogSNaKSNFg3Mf8gca100dEPFe49B572uJpWg  
ie5e27ka3x1Unde0fnpYhGti03Bi8yB6/PZE+QELdXfwm06ZFE3fU2zn6oYqRcj  
cskCGj1pg9+UJXTmLgGRivR62Ag4DyMGB08n37j717rnbvY49NYphCqW+KmXuIj1  
Pxbatw+xxGKiH5dps4eg4gWtsh2UFm7/LK440g5V2sL8dP8Y+Tnk7gXG+iY5+  
yknGfs1QYFkJ+zuRagMBAAECggGACIj3fW+mA3NHauIgMoJ9aPJu4EQmnxwiPQgK  
2hvatc6G8vYDH3HMEFw/903MR4UXcUokZjzbsHb9EBz3q3RI126jds0FV2uwhVI  
++ogxe5q7xxSgSAeiw/vkV+X/yiPOZoulyWx92UktlCMLjoUGDldQjeNhTdtueCg  
7P1X/KV4Coo2imdOWIzpw752vJhFK6ggO/V+SdAK6Z+Q2valKc1XTepPvPrOgK/w  
o/8NvX5kckVzT9IzoH4ZwaMsn0m1VupaQItqBQiHvCJYRZuc87gssXGkpPP1X1F+  
2EtIy28bZUgBqfT3w/hdL79ANedDnElH6o3VUV/F/2RPjcPF1Gy5OsxiryMOCUCt  
UoTkWLTsA+XIiJFWX1fttGnA23dZrn18mHa8wYfsqdFEoZHBdhD0ix+snw4Y5S6p  
M/H8y9jXtWgV700RgvJm7PcuP60H3276vPC0Rc54UH0cL43iTxp7u/zPc7pq  
DVatpZ8kR30ApqK2020M14E07B4HAPF0i10GuaBPR6drYjesXxSFoAw18  
-----END RSA PRIVATE KEY-----

**Importante sobre acesso externo**

Se a porta padrão (443) for alterada para uma porta alternativa, é fundamental garantir que essa nova porta esteja liberada para acesso externo.

Para mais detalhes, consulte nossa documentação específica: [Como configurar o acesso externo ao Portal DOX](#).

Revisão #34  
Criado 3 December 2021 08:51:40 por Nicolly Andrielly