

MEMORIAL DESCRITIVO – CERTIFICADOS DIGITAIS SSL (SECURE SOCKETS LAYER)

1. Certificados Digitais SSL (Secure Sockets Layer)

O serviço de certificação digital prestado pelo Site Blindado tem por finalidade criptografar as informações transmitidas por meio da internet, garantindo a segurança no tráfego entre, por exemplo, o servidor web e o navegador do usuário.

Os certificados digitais têm modalidades diferentes com particularidades inerentes a cada tipo.

2. Tipos de Certificados Digitais SSL

SSL DV (Domain Validation): Solução mais rápida, simples e econômica para empresas online que desejam criar um ambiente seguro em seus sites.

SSL OV (Organization Validation): Oferece um nível extra de confiança online ao autenticar a identidade da empresa. A organização deve provar que possui o nome de domínio que deseja proteger e confirmar que é uma empresa legalmente registrada. O processo de verificação inclui uma autoridade certificadora confirmando detalhes como o nome e a localização da empresa antes de emitir o certificado.

SSL EV (Extended Validation): Oferece o mais alto nível de confiança e é o padrão da indústria para sites comerciais. Certificados EV são recomendados para todos os sites empresariais, especialmente para sites com grande volume de dados e de comércio eletrônico.

SSL SD (Single-Domain): Assegura a proteção de apenas um endereço de uma URL, conferindo e validando somente o endereço do seu site.

SSL MDC (Multi-Domain Certificate): Assegura a proteção de múltiplos endereços online através da inserção de domínios alternativos em único certificado.

SSL Wildcard: Protege um domínio principal e todos os subdomínios de primeiro nível abaixo dele.

SSL SAN (Subject Alternative Name) ou UCC (Unified Communications Certification): Focado em serviços de comunicação real-time unificados, tais como mensagens instantâneas (chat), telefonia (incluindo telefonia IP), videoconferência, controle de chamadas, reconhecimento de fala e mensagens (integrados de voz, e-mail, SMS e fax).

Os Certificados Digitais SSL SAN e SSL MDC permitem até 200 endereços de domínios e subdomínios FQDNs (Fully Qualified Domain Name - em Português, Nome de Domínio Completamente Qualificado).

Pode-se inserir o SSL Wildcard como parte dos FQDNs nos casos de SSL MDC (DV).

Podem ser contratados créditos de endereços adicionais para os Certificados junto a Equipe Comercial do Site Blindado.

3. Compra de Certificados Digitais SSL

Para compras no site do Site Blindado, serão solicitados os seguintes dados para cobrança:

- Nome completo da pessoa física.
- Telefone - contato secundário para comunicação entre as partes.
- E-mail - contato principal para comunicação entre as partes.
- CPF - número de Cadastro Nacional de Pessoa Física.
- Endereço de cobrança - rua, número, complemento, CEP, cidade, estado e país.

Caso a compra seja feita em nome de uma entidade ou empresa, os dados abaixo também serão solicitados:

- Razão Social - identificação legal da entidade ou empresa.
- CNPJ - número de Cadastro Nacional de Pessoa Jurídica.

Para fins de segurança, é armazenado também o IP (Internet Protocol Address) utilizado pelo Contratante durante o ato da compra.

4. Emissão de Certificados Digitais SSL

Em todas as modalidades de Certificados Digitais SSL é imprescindível e de responsabilidade do contratante a execução dos passos necessários para a efetiva emissão de certificados. Quando aplicável conforme seção Comunicação e Suporte do Contrato Padrão de Cessão de Uso de Software, a Equipe de Suporte do Site Blindado, poderá orientar os procedimentos necessários conforme o caso.

Para garantir a segurança e autenticidade do Certificado Digital SSL, é necessário o fornecimento das seguintes informações:

Certificado para pessoa física:

- Nome completo da pessoa física.
- CPF - número de Cadastro Nacional de Pessoa Física.
- Telefone - contato secundário para comunicação entre as partes.
- E-mail - contato principal para comunicação entre as partes.
- Endereço - localização física da pessoa.
- URL - endereço da web para o qual o certificado será emitido.

Certificado para pessoa jurídica:

- Razão Social - identificação legal da entidade ou empresa.
- CNPJ - número de Cadastro Nacional de Pessoa Jurídica.
- Telefone - contato secundário para comunicação entre as partes.
- E-mail - contato principal para comunicação entre as partes.
- URL - endereço da web para o qual o certificado será emitido.

Para a emissão de certificados SSL OV e SSL EV dados adicionais serão solicitados, tais como:

- Nome completo do representante do Contratante.
- Pronome Social - pronome utilizado durante comunicação com o representante do Contratante.

Estes dados serão enviados ao fornecedor de serviços do Site Blindado para emissão do certificado, e, para emissão de certificados SSL OV e SSL EV, será necessário a assinatura de um termo de serviços junto ao referido fornecedor e aceite dos seus termos de uso e política de privacidade.

O Contratante concorda com o armazenamento e uso destes dados para os propósitos específicos da emissão e gerenciamento do Certificado Digital SSL, conforme as políticas de privacidade e segurança do Site Blindado.

Para alguns certificados, há a necessidade de realizar o procedimento de Callback (descrito no item 6 abaixo), e, para a sua correta execução, os contatos do Contratante devem estar atualizados junto aos órgãos/empresas de registro nacionais e internacionais, sendo que, prioritariamente, as consultas são realizadas junto à Receita Federal de Brasil e/ou a empresa Dun&Bradstreet, que possui uma base privada internacional com dados sobre a situação fiscal de empresas. A atualização dos seus dados é de responsabilidade do Contratante.

Em alguns casos, quando uma empresa tenha sido criada recentemente, pode ser necessária a disponibilização pelo Contratante de documentos comprobatórios de sua existência.

Orienta-se prioritariamente a utilização do Portal Site Blindado para a emissão dos certificados contratados, e se, e somente se, ocorrerem problemas técnicos ou operacionais durante a realização dos procedimentos, entrar em contato com a Equipe de Suporte conforme estabelecido no Contrato Padrão de Cessão de Uso de Software.

Após a emissão do certificado, o próximo passo é o processo de validação do domínio, quando se verifica se o responsável pela solicitação do certificado possui acesso administrativo às contas de e-mail do seu domínio, ou a outras configurações que somente um administrador deveria ter acesso. Após a escolha do método de validação e consequente efetivação, o fornecedor de serviços do Site Blindado para emissão do certificado, irá checar todas as informações e, caso estejam corretas, o certificado estará disponível para instalação.

Para a emissão de quaisquer tipos de Certificados Digitais SSL, é premissa padrão e responsabilidade do Contratante manter seus dados e contatos atualizados, bem como, acionar, caso necessário e quando aplicável conforme seção Comunicação e Suporte do Contrato Padrão de Cessão de Uso de Software, a Equipe de Suporte do Site Blindado.

5. Instalação de Certificados Digitais SSL

Para finalizar o processo, o Certificado Digital SSL deve ser instalado e configurado corretamente. Quando aplicável, conforme seção Comunicação e Suporte do Contrato Padrão de Cessão de Uso de Software, pode-se contar com a Equipe de Suporte do Site Blindado para auxiliar a execução desses passos.

Apenas após a finalização do processo de instalação, o certificado poderá ser exibido junto à URL para a qual foi contratado.

Para aquisição de Certificados Digitais SSL, é necessário realizar a aquisição de créditos junto à Equipe Comercial do Site Blindado, ou através da loja virtual do Portal Site Blindado.

Todos certificados têm validade de 1 (um) ano. Para aquisição de mais créditos, deve-se entrar em contato com a Equipe Comercial do Site Blindado, ou através da loja virtual do Portal Site Blindado.

A depender do Certificado Digital SSL e das condições comerciais contratadas, pode ser disponibilizada certa quantidade de URLs adicionais.

6. Callback

O Contratante é acionado pelo fornecedor do Site Blindado, e deve verificar e disponibilizar dados solicitados para a devida emissão dos certificados.

No caso de Certificados Digitais SSL EV e SSL OV, o Contratante precisa confirmar seu registro junto à Receita Federal do Brasil através de seu CNPJ. Também é feita uma validação externa, via telefone ou e-mail, acionando o representante técnico do Contratante. O objetivo é verificar a existência legal, física e operacional do Contratante, e se sua identidade corresponde aos registros oficiais.

7. Renovação dos Certificados Digitais SSL

Para facilitar o controle dos certificados contratados, o Site Blindado disponibiliza no Portal Site Blindado o gerenciamento de todos os certificados emitidos para o Contratante.

Para os domínios cadastrados no Portal Site Blindado que estejam monitorados pelo Scan de Certificado Digital SSL, o Contratante receberá e-mails informando a validade do Certificado Digital SSL emitido.

A periodicidade dos e-mails tem início com 90 dias antes do vencimento, sendo que, com 60, 30, 15, 7 e 1 dias de antecedência serão enviados alertas sobre a situação da não renovação/vencimento.

Os contatos endereçados à renovação devem ser direcionados diretamente à Equipe Comercial do Site Blindado. No caso de compras online, a renovação poderá ser realizada através da loja virtual do Portal Site Blindado.

8. Scan de Certificado Digital SSL

Oferecemos também o serviço de Scan de Certificado Digital SSL, que possibilita verificar vulnerabilidades relacionadas às configurações do Certificado Digital SSL e do servidor web. O resultado do scan fica disponível no Portal Site Blindado, e é possível visualizar o resultado semanalmente ou mesmo solicitar um novo scan sob demanda.

O scan utiliza alguns critérios tais como inspeção do certificado, validade e confiabilidade do certificado, suporte de protocolos, key exchange, cifras utilizadas. Por meio desses critérios são avaliados: o nível de proteção do certificado e a forma com que ele foi instalado. Caso o certificado apresente nível que não seja reconhecido como ideal, é recomendado realizar a correção das vulnerabilidades.

9. Selo de Certificado Digital SSL

Os Certificados Digitais SSL contratados junto ao Site Blindado, permitem a exibição do Selo de Certificado SSL Site Blindado, observado o disposto no presente documento.

O Contratante deve realizar os procedimentos de scan com sucesso, e possuir o script SSL relativo à exibição do selo devidamente inserido no código-fonte do site.

O Contratante deve instalar o Certificado Digital SSL e então copiar o script SSL no código-fonte do site. Quando aplicável, conforme seção Comunicação e Suporte do Contrato Padrão de Cessão de Uso de Software, a Equipe de Suporte do Site Blindado poderá orientar este processo.

Sem o certificado devidamente instalado, o selo não será exibido.

10. Reemissão de Certificado Digital SSL

As reemissões de Certificados Digitais SSL são ilimitadas desde que a solicitação seja realizada no período de validade do certificado. Para solicitar a reemissão basta entrar em contato com a Equipe de Suporte do Site Blindado.

11. Cancelamento de Certificado Digital SSL

Durante o processo de emissão de Certificado Digital SSL, caso haja desistência por parte do Contratante, deve ser verificado junto a Equipe de Suporte do Site Blindado, a possibilidade de revogar o certificado. Após a emissão de Certificados Digitais SSL, não é mais possível realizar o cancelamento. O disposto nesta cláusula sobrepõe-se ao disposto no Contrato Padrão de Cessão de Uso de Software.