



ATIVIDADE DE LABORATÓRIO IV - CONFIGURAÇÃO SSL

Victor Dallagnol Bento
Universidade Federal de Santa Maria
Santa Maria - RS, Brasil
victor.bento@ecomp.ufsm.br

I. INTRODUÇÃO

Na quarta atividade de laboratório o professor nos apresentou conceitos sobre o protocolo SSL. Posteriormente foram incumbidas tarefas como solicitar um certificado digital para ser usado na configuração do protocolo SSL do servidor web, emitir o certificado e importá-lo para uso no servidor da web, verificar a confidencialidade e autenticação da conexão depois que o protocolo SSL estiver configurado. Também nos foi exigido explicar a partir dos procedimentos realizados como a segurança na web é garantida discutindo seus pontos fortes e fracos.

II. DESENVOLVIMENTO TEÓRICO

O protocolo SSL (Secure Sockets Layer) é um tipo de segurança digital que permite a comunicação criptografada entre um site e um navegador. Atualmente a tecnologia está sendo substituída pelo TLS que é uma sigla que representa Transport Layer Security e certifica a proteção de dados de maneira semelhante ao SSL já que o SSL está caindo em desuso.

O objetivo do SSL/TLS é tornar segura a transmissão de informações sensíveis como dados pessoais, de pagamento ou de login por exemplo. É uma alternativa à transferência de dados em texto simples na qual a conexão ao servidor não é criptografada e torna mais difícil para que hackers possam interceptar a conexão e roubar dados. A maioria das pessoas já estão familiarizadas com SSL/TLS que são utilizadas por webmasters para assegurar seus sites e oferecer uma opção segura para efetuar transferências.

Certificados SSL/TLS funcionam por unir digitalmente uma chave criptográfica à informação de identificação de uma companhia. Isso permite que dados possam ser transferidos de maneira que não podem ser descobertos por terceiros.

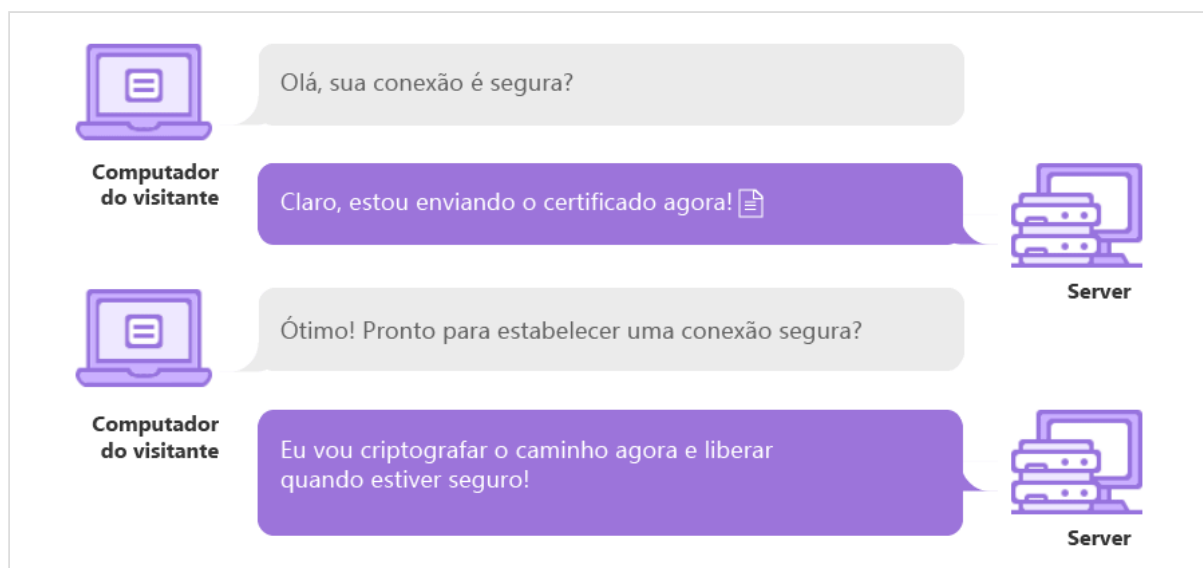


Figura 1: Exemplo SSL/TLS.

O SSL/TLS funciona através de chaves públicas e privadas, além de chaves de sessão para cada conexão segura. Quando o visitante coloca uma URL com SSL no navegador e navega pela página segura, o navegador e o servidor fazem uma conexão.

Durante a conexão inicial as chaves públicas e privadas são utilizadas para criar uma chave de sessão, que então é utilizada para criptografar e descriptografar os dados sendo transferidos. Essa chave de sessão vai se manter válida por tempo limitado e só vai ser utilizada para essa sessão específica.

O HTTPS é uma extensão segura do HTTP. Os sites que configurarem um certificado SSL/TLS podem utilizar o protocolo HTTPS para estabelecer uma comunicação segura com o servidor.

III. DESENVOLVIMENTO EXPERIMENTAL

Em um primeiro momento foi necessário ir até o diretório *Inetpub* no qual o conteúdo é um conjunto especial de servidores da Internet, criado pela Microsoft, para o qual o serviço IIS (Internet Information Server) é responsável pelo uso do sistema. Posteriormente acessamos então o diretório *wwwroot* que é um caminho compartilhado comum que pode ser acessado por todos os usuários em uma rede LAN. Se criarmos um novo aplicativo da web, um diretório virtual será criado em *c:\inetpub\wwwroot*. Editamos o arquivo *Iisstart.htm* do servidor web, colocando nosso nome e algumas particularidades para diferenciar dos demais colegas, feito isso, executamos o arquivo.

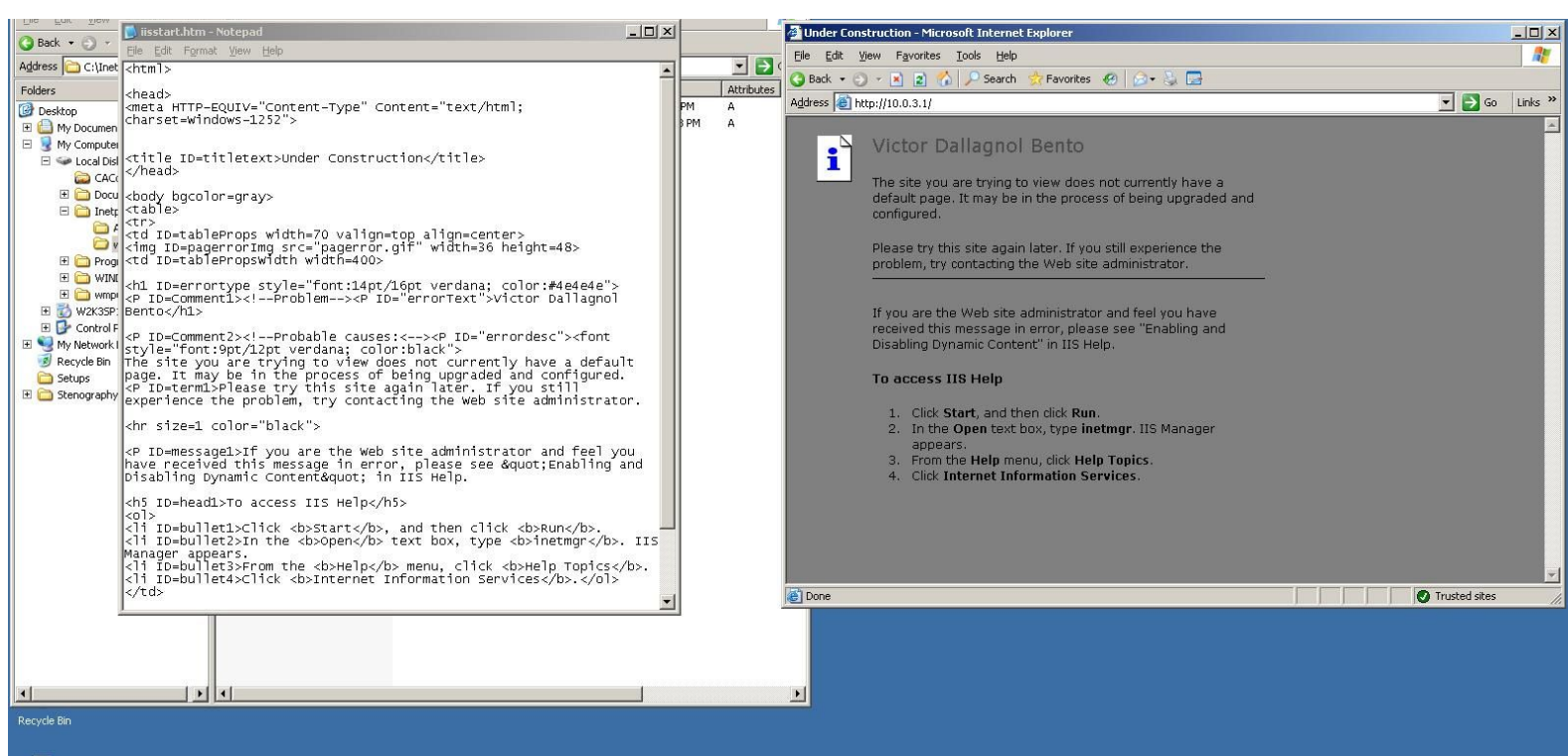


Figura 2: Caminho e abertura do nosso site.

Depois efetuamos uma mudança no arquivo *host*, localizado em `\system32\drivers\etc\`. Este arquivo faz parte da implementação do protocolo de internet, e serve na tradução de um nome compreensível para os seres humanos em um endereço IP, que identifica um integrante ou destino da rede. Adicionamos no arquivo uma nova linha, contendo o nosso IP e o nome da nossa página (10.0.3.1 *www.lab.com*).

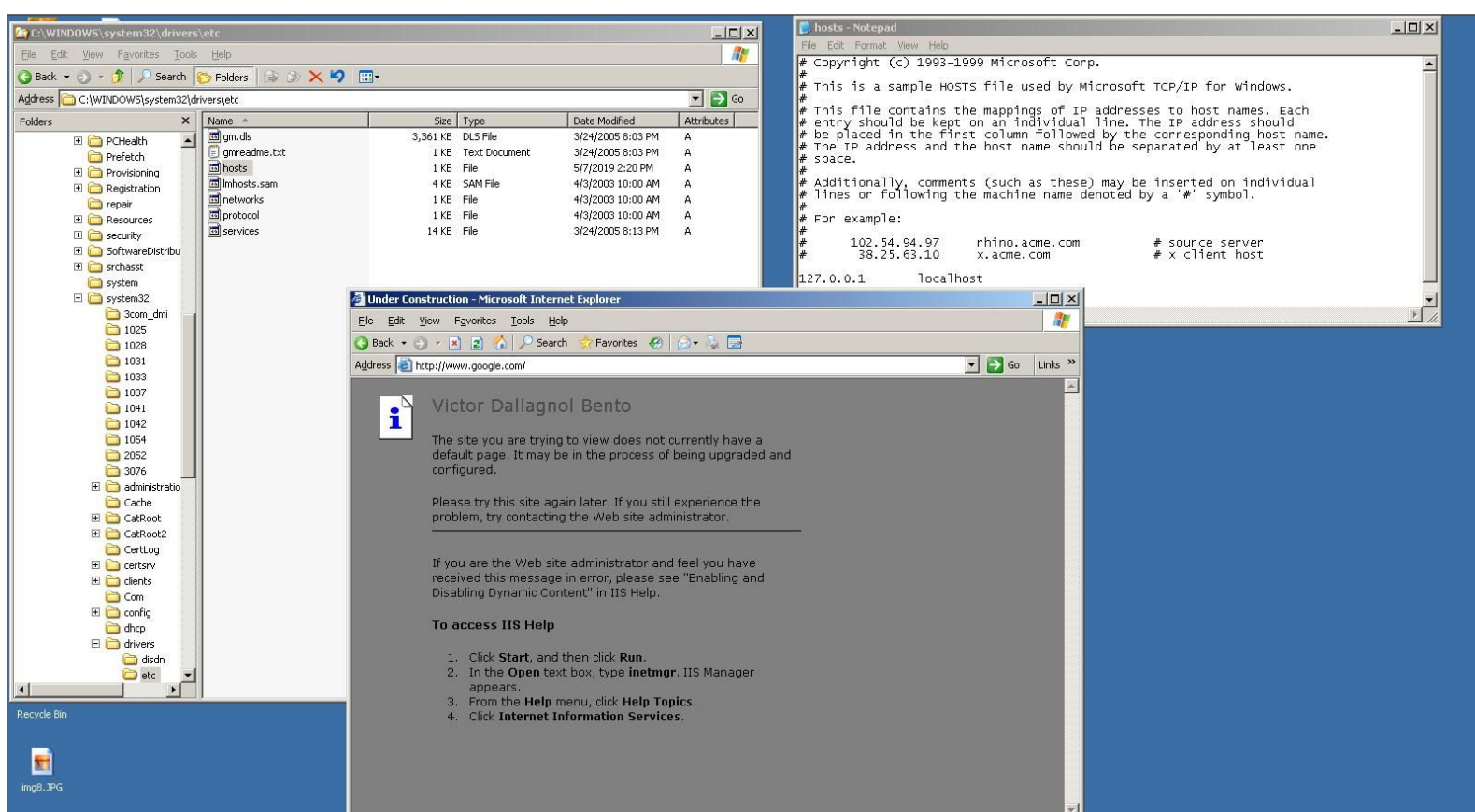


Figura 3: Edição do arquivo host.

Partimos então para a instalação do certificado SSL, usando o *IIS Manager*, *Web Site*, e clicando com o botão direito do mouse sobre *Default Web Site*, e em *Properties*. Conforme a Imagem abaixo.

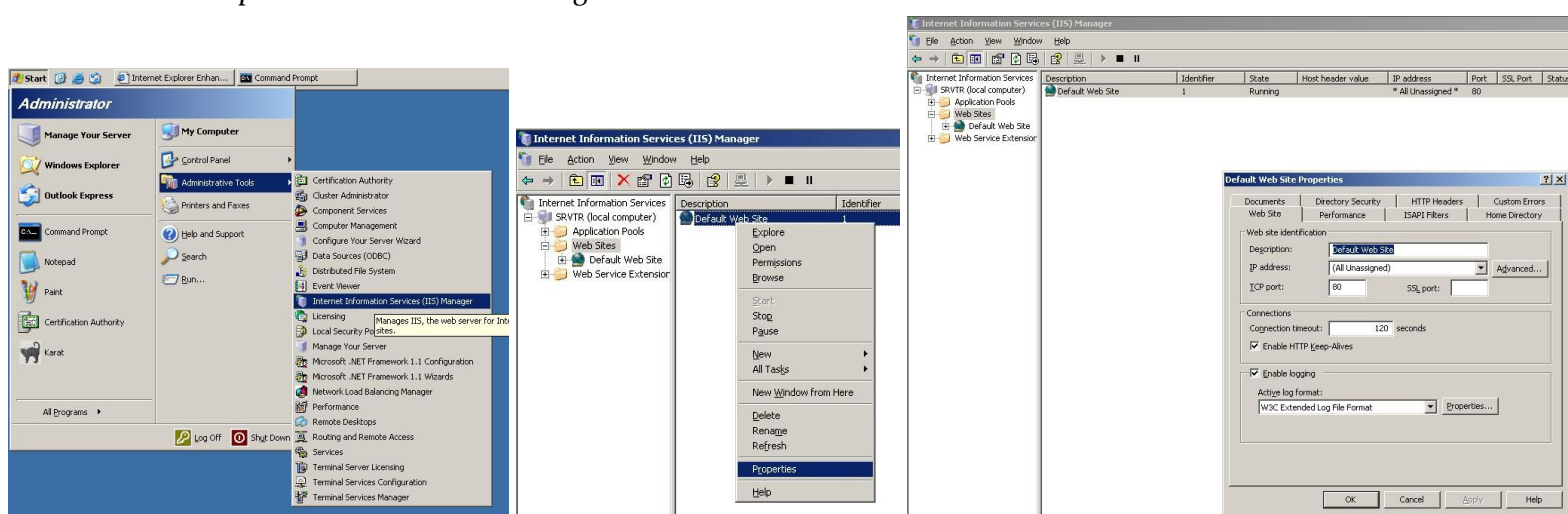


Figura 4: Configurações do servidor web.

Na aba *Directory Security* deve-se clicar em *Server Certificate*, para criação do certificado SSL da nossa página/site.

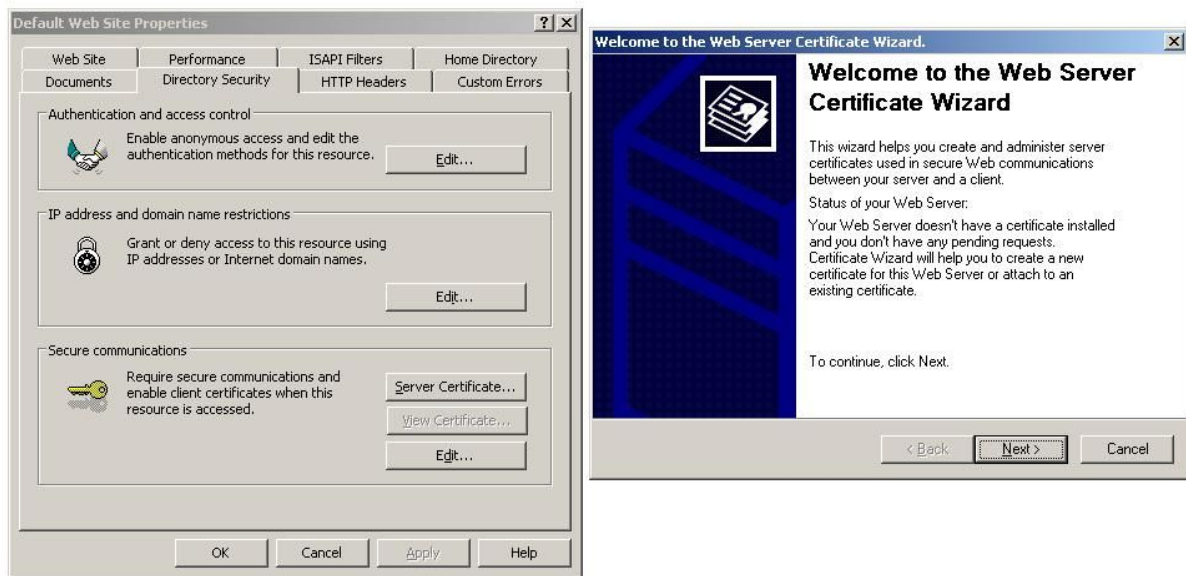


Figura 5: Criação do certificado web.

As imagens a seguir refletem o passo a passo para a criação do certificado SSL. Na **Figura 6** selecionou-se *Create a new certificate*, seguido pela primeira opção *Prepare the request now, but send it later*.

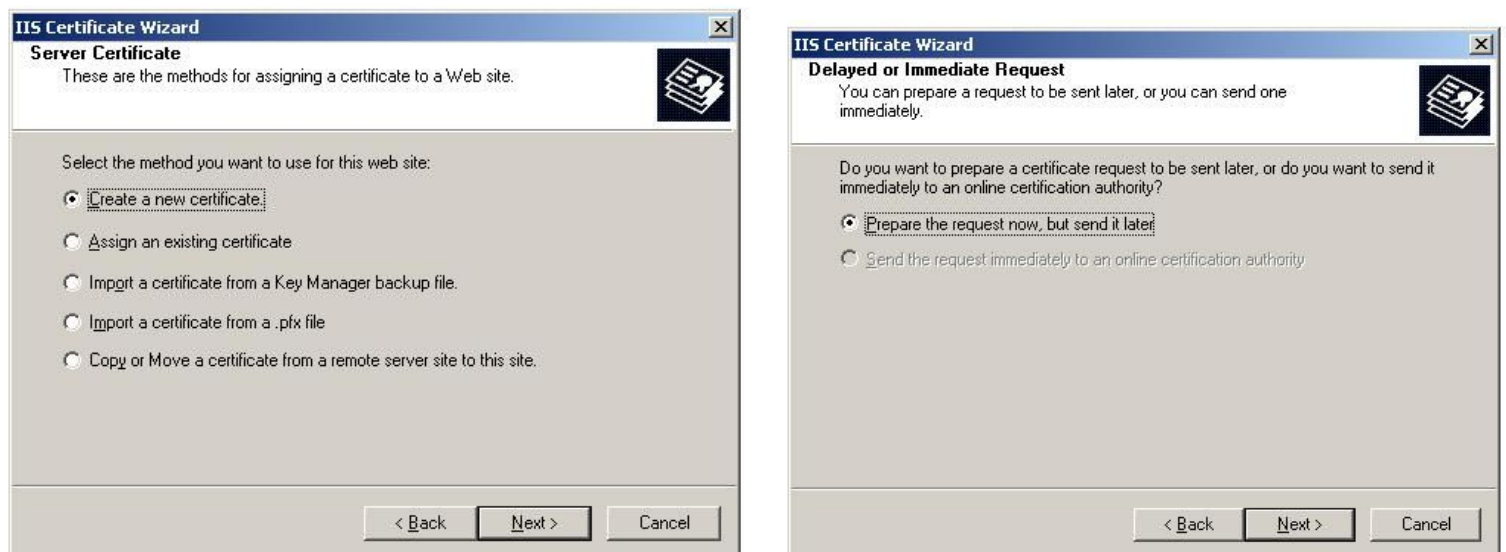
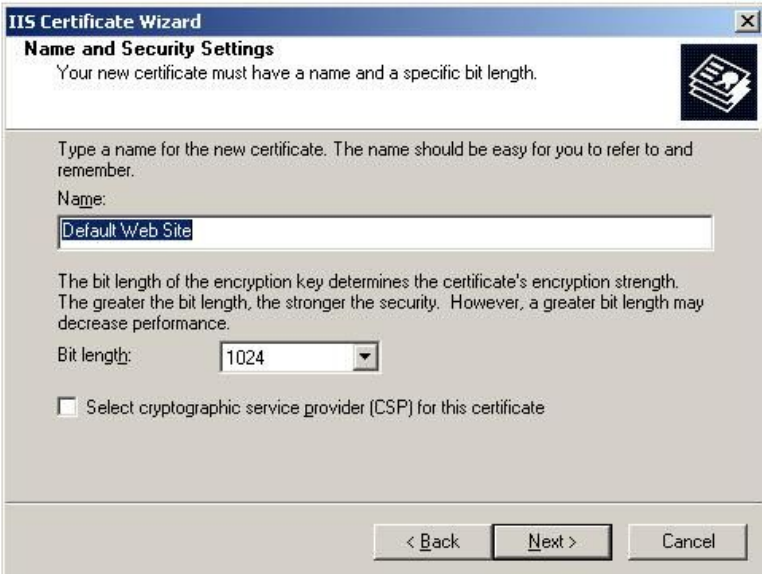


Figura 6: Criação do certificado SSL.

A **Figura 7** deve ser preenchida com o nome do certificado e com o tamanho da chave de encriptação. Também é necessário preencher a Organização e a Unidade Organizacional referentes a próxima tela.



IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

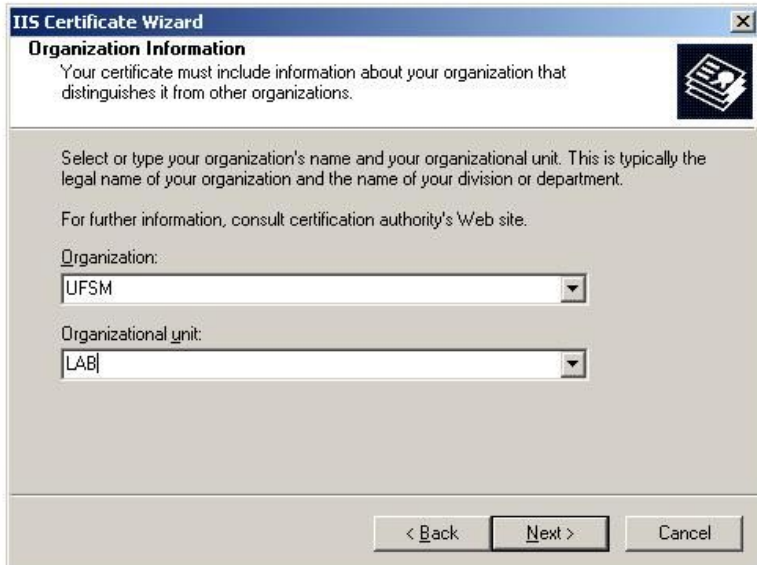
Name:

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length:

☐ Select cryptographic service provider (CSP) for this certificate

< Back Next > Cancel



IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:

Organizational unit:

< Back Next > Cancel

Figura 7: Nome do certificado, tamanho da chave, organização e unidade organizacional.

A **Figura 8** é necessário o preenchimento do nome do domínio que será utilizado no site, este nome, deve ser o mesmo que editamos no arquivo *host* localizado no caminho `\system32\drivers\etc\` que o servidor foi instalado. No caso o nome será *www.lab.com*.



IIS Certificate Wizard

Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:

< Back Next > Cancel

Figura 8: Nome do domínio da página/site.

Efetuada este processo de criação do certificado SSL, foi gerado um arquivo *.txt* contendo a chave pública criptografada (**Figura 9**).

Acessamos a primeira opção para requisição de um certificado “*Request a certificate*” e posteriormente selecionamos a opção de certificado web “*Web Browser Certificate*”. Selecionamos então a segunda opção para submeter o pedido “*Submite a certificate request...*”.

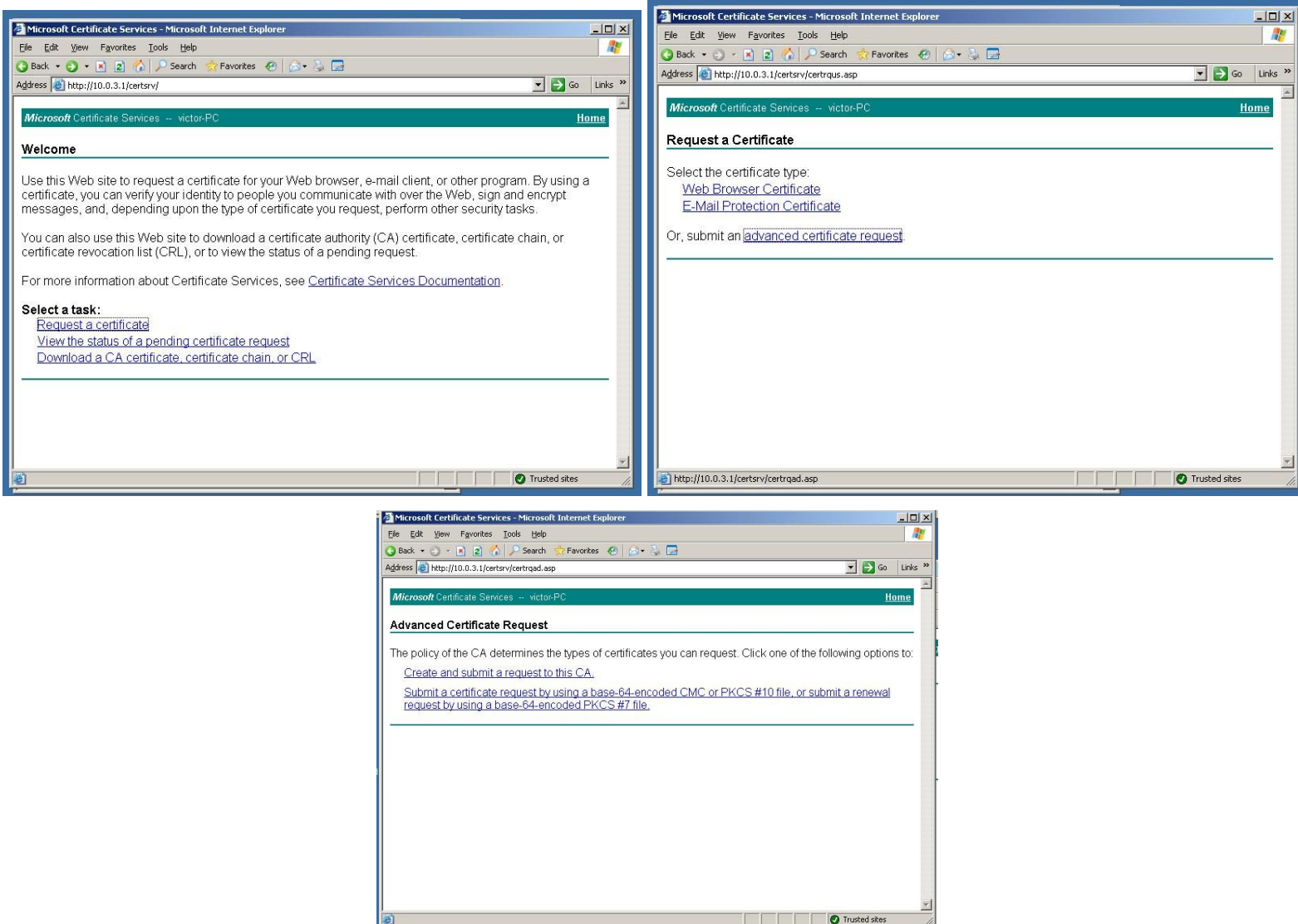


Figura 11: Requisição do certificado SSL para a entidade autenticadora.

Na **Figura 12** representa a chave pública cifrada gerada anteriormente e a submissão pela entidade certificado. Foi necessário colar a chave no campo de requisição da entidade, seguido de *Submit*.

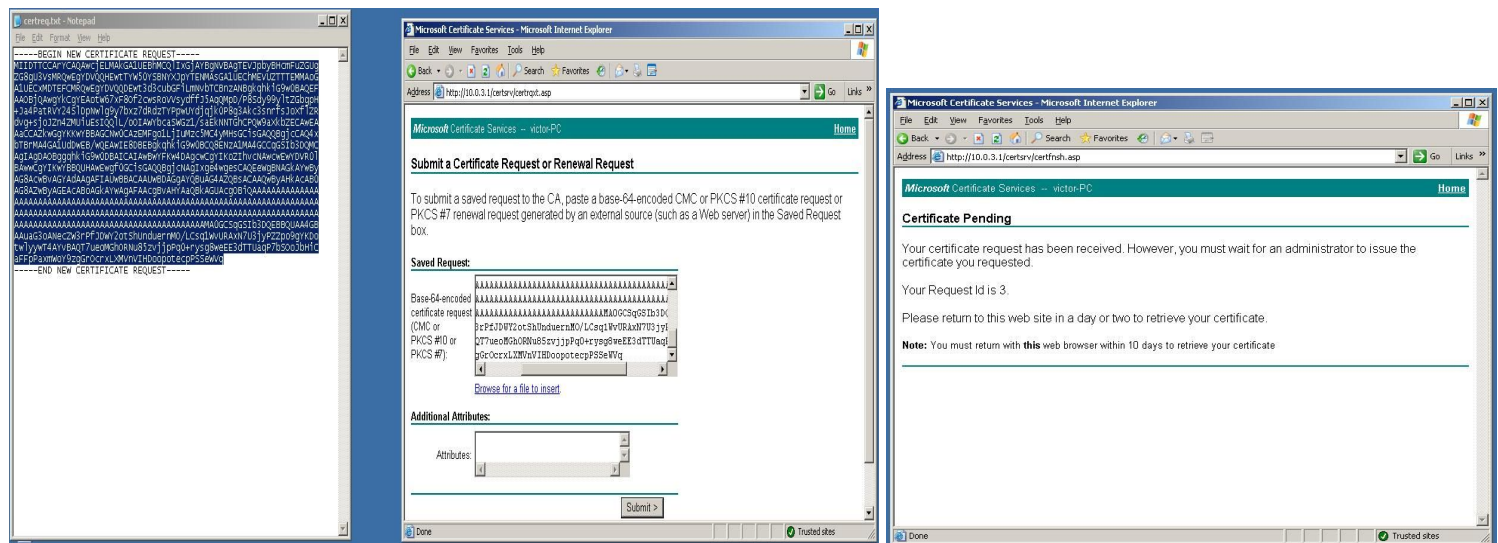


Figura 12: Requisição do certificado SSL.

Efetuada a requisição, precisamos acessar a aplicação da Autoridade de Certificação do computador. Ao acessar a Aplicação, podemos perceber que o certificado SSL requisitado anteriormente encontra-se na pasta *Pending Request*. Precisamos então aceitar o pedido do certificado, como mostra a **Figura 13**.

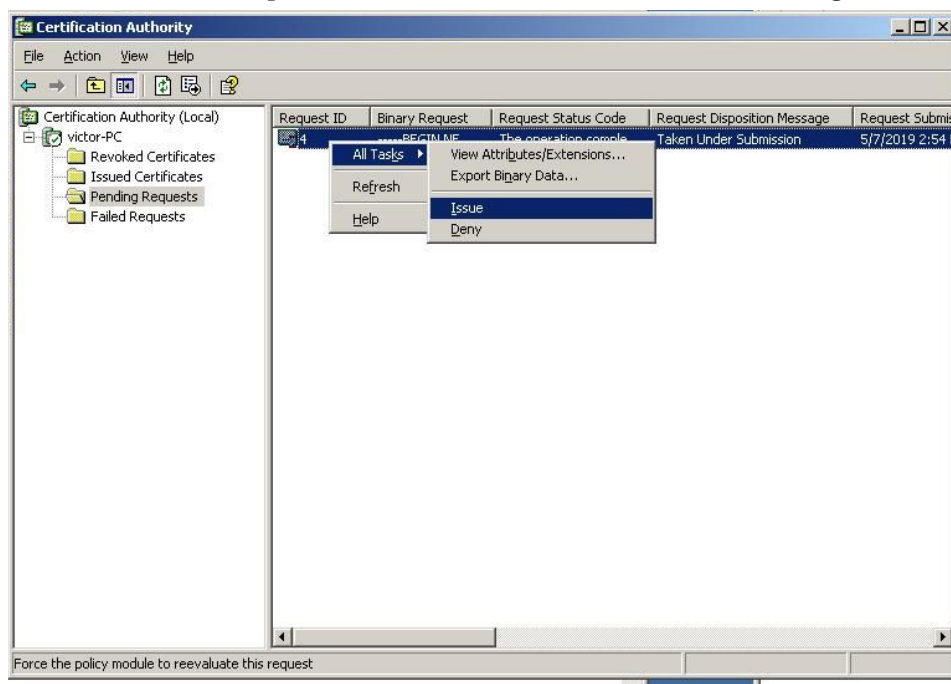


Figura 13: Aceitando o pedido do certificado.

Após aceitar o pedido de requisição do certificado SSL, se faz necessário voltar a Entidade Autenticadora para poder efetuar o download do mesmo (**Figura 14**).

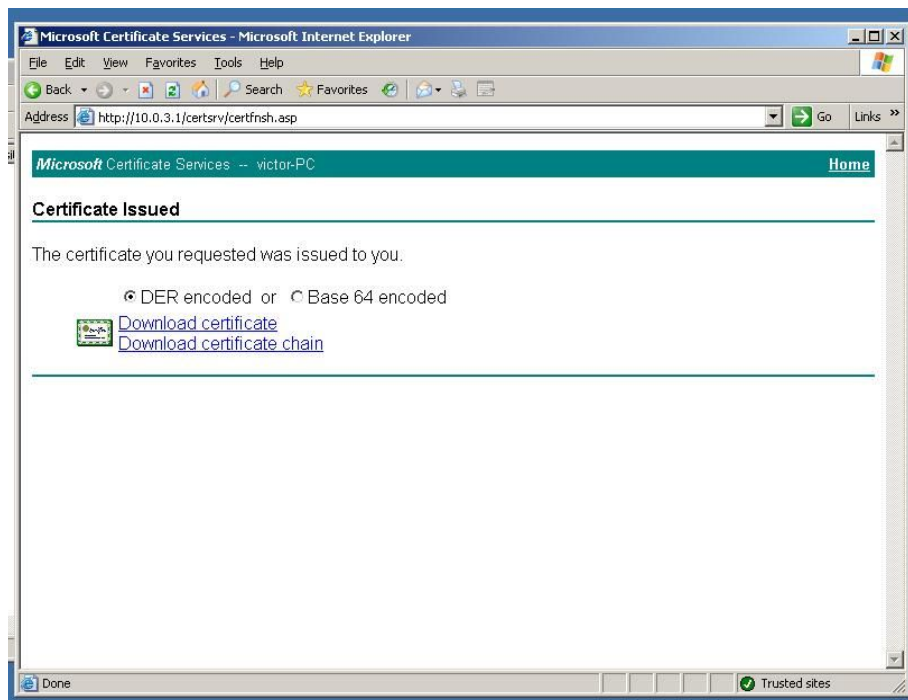


Figura 14: Download do certificado SSL.

Com o download do certificado, executou-se novamente a aplicação de *IIS Manager*, seguindo os mesmos passos citados anteriormente para a criação do certificado, porém no lugar de criar um certificado (**Figura 6**) selecionou-se a opção de importar o certificado, e assim, selecionou-se o certificado SSL baixado anteriormente.

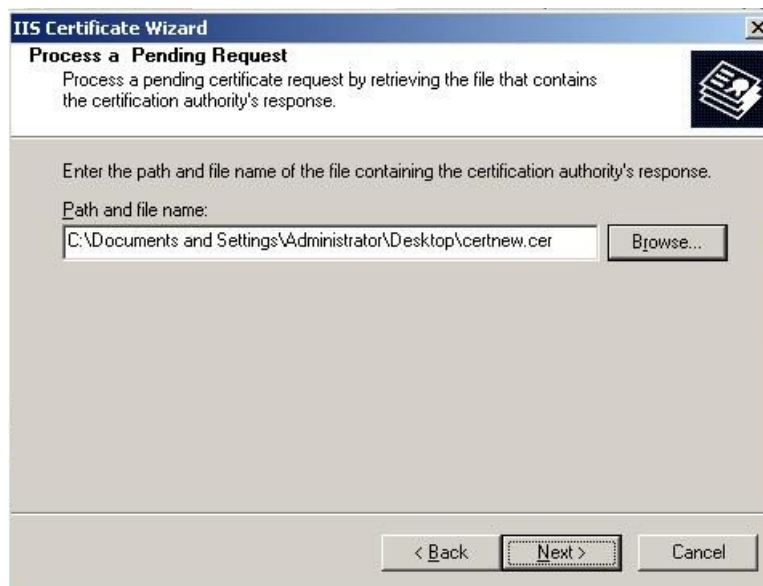


Figura 15: Importação do certificado SSL.

O próximo passo foi clicar em *Next* em todas as opções futuras sem efetuar nenhuma alteração. Por último, acessou-se o site utilizando *https://* e pode-se verificar

o funcionamento correto, provando que os procedimentos foram executados corretamente.

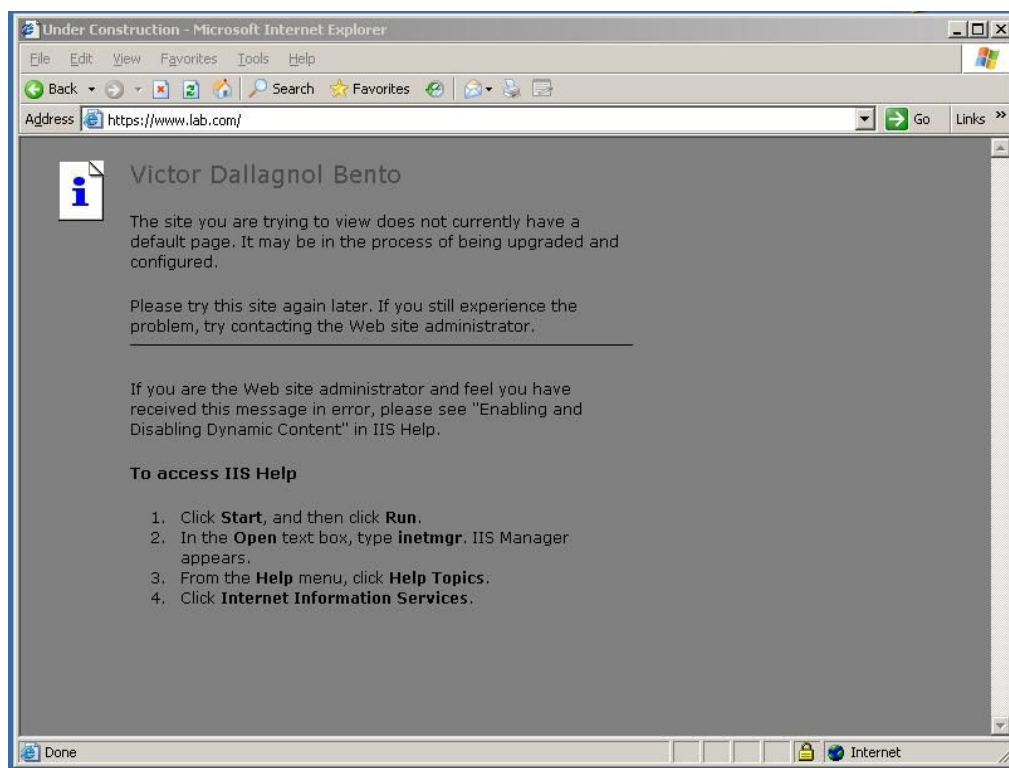


Figura 16: Acesso ao site utilizando *https*.

IV. CONCLUSÃO

Com este laboratório podemos concluir que a forma que foi criado o certificado assim como a requisição para o certificado SSL foi muito mais segura, pelo fato de não trocarmos a chave privada com a Entidade Certificadora.

Ademais, concluiu-se que uma conexão é segura se seu endereço está iniciando com *https* ou basta procurar por um ícone de cadeado ao lado da URL, no navegador. Ao clicar no cadeado você deve encontrar informações sobre o certificado em questão e realizar configurações. O SSL/TLS é essencial sempre que houver informações sensíveis sendo transmitidas, como nomes de usuário, senhas e informações de pagamento.

REFERÊNCIAS

[1] **O que é SSL/TLS e HTTPS?**, no site:

<https://www.hostinger.com.br/tutoriais/o-que-e-ssl-tls-https/> acessado em 12.05.2019.

[2] Material disponibilizado em aula.