ATIVIDADE DE LABORATÓRIO - CERTIFICAÇÃO (X.509)

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

I. INTRODUÇÃO

Na segunda atividade de laboratório o professor nos apresentou conceitos básicos sobre a certificação X.509. Posteriormente foram incumbidas tarefas como instalar uma autoridade de certificação, solicitar certificados pessoais, emitir certificados utilizando a ferramenta de gerenciamento da autoridade de certificação e importar e exportar certificados digitais.

II. DESENVOLVIMENTO TEÓRICO

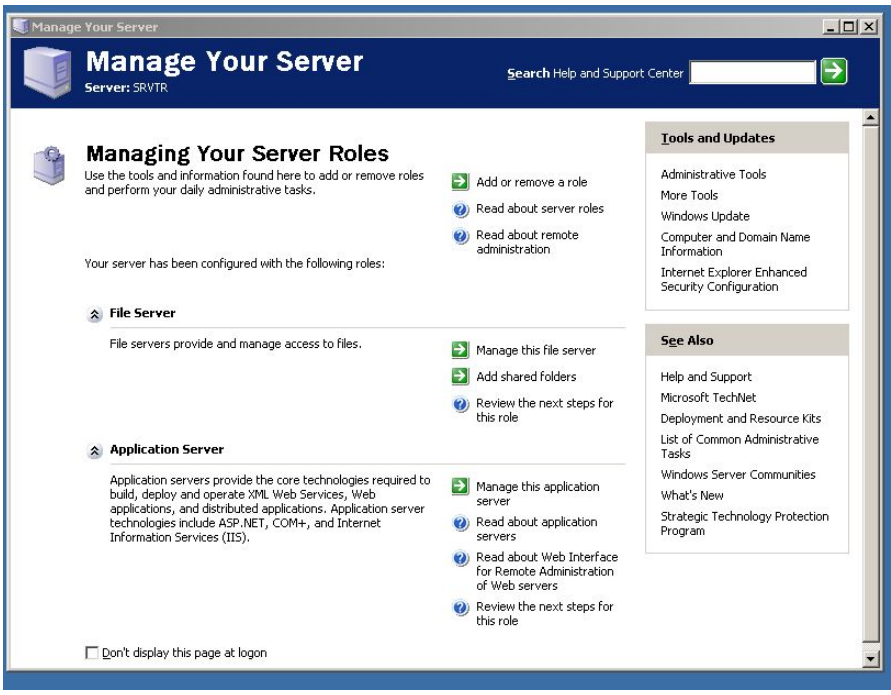
Os certificados X.509 são certificados digitais que usam a infraestrutura de chave pública X.509 padrão para associar uma chave pública a uma identidade contida em um certificado. Os certificados X.509 são emitidos por uma entidade confiável chamada CA (autoridade de certificação). A CA mantém um ou mais certificados especiais chamados certificados CA que são usados para emitir certificados X.509. Somente a autoridade de certificação tem acesso aos certificados CA.

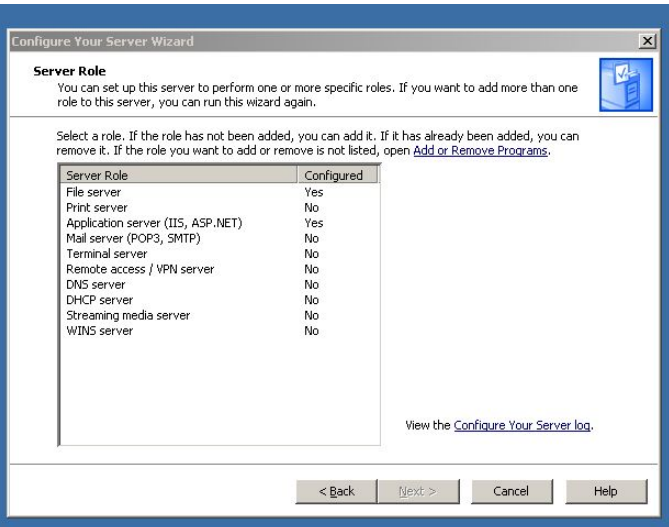
Os certificados oferecem vários benefícios em relação a outros mecanismos de identificação e autenticação. Os certificados permitem que as chaves assimétricas sejam usadas com os dispositivos. Isso significa que você pode gravar chaves privadas em armazenamento seguro em um dispositivo. Dessa forma, o material confidencial de criptografia nunca deixa o dispositivo. Os certificados fornecem opções mais fortes de autenticação de cliente em outros esquemas, como nome de usuário e senha ou tokens do portador, porque a chave secreta nunca deixa o dispositivo.

III. DESENVOLVIMENTO EXPERIMENTAL

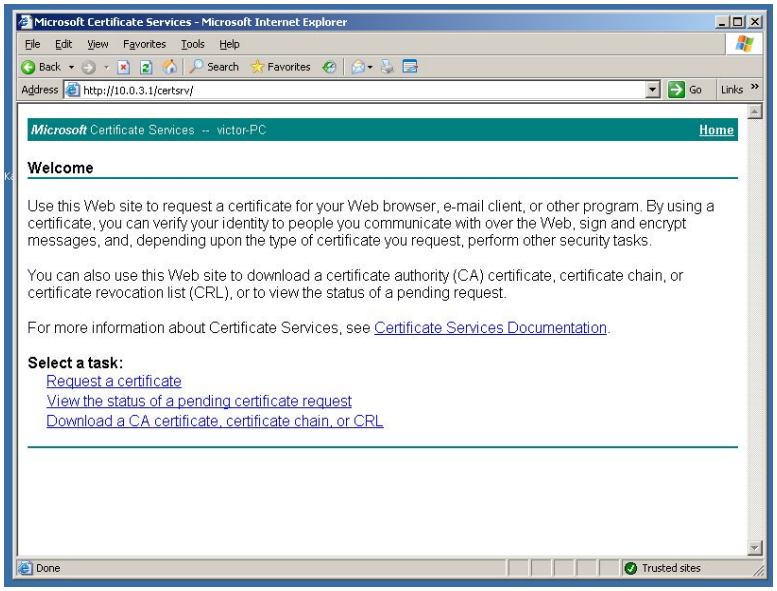
Por conta de problema de saúde, o aluno Victor Dallagnol Bento não pode comparecer a aula prática que originou este relatório. Os testes foram feitos posteriormente com a ajuda e informações dos colegas que estavam presentes na aula, do professor, e no material disponibilizado pelo professor.

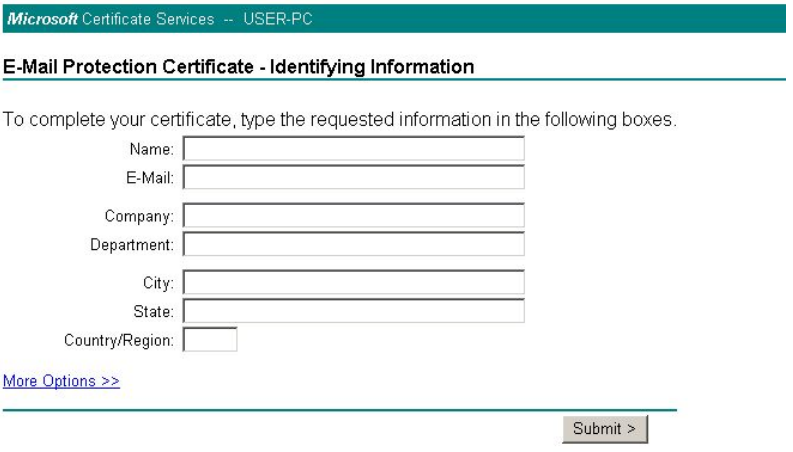
Em um primeiro momento efetuou-se a configuração do *Outlook*, colocando como servido *mail.lab.com* (*IP* do professor), e configurando a nossa conta de email seguida por *nome@lab.com*. Feito isso configurou-se a Autoridade Certificadora (CA) utilizando o assistente do *Service Manager*, indo em "*adicionar nova função*" e selecionando "*servidor de aplicações*".



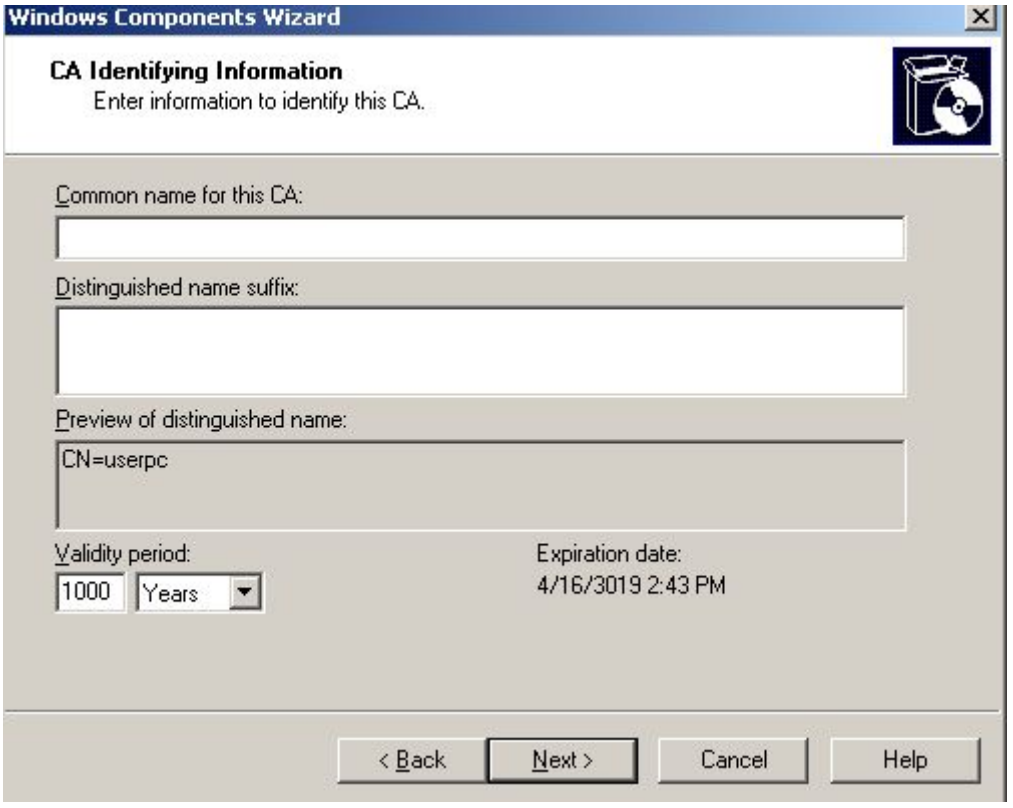


Após configurar a autoridade certificadora executou-se o navegador com o seguinte link *IP_LOCAL/certsrv* (10.0.3.1/certsrv) onde foi feita a requisição de um certificado, através do primeiro link. Foi selecionado "*Email Protection*" e então os dados que antes foram usados para configurar o *Outlook* agora foram utilizados para fazer o preenchimento e então obter o certificado.

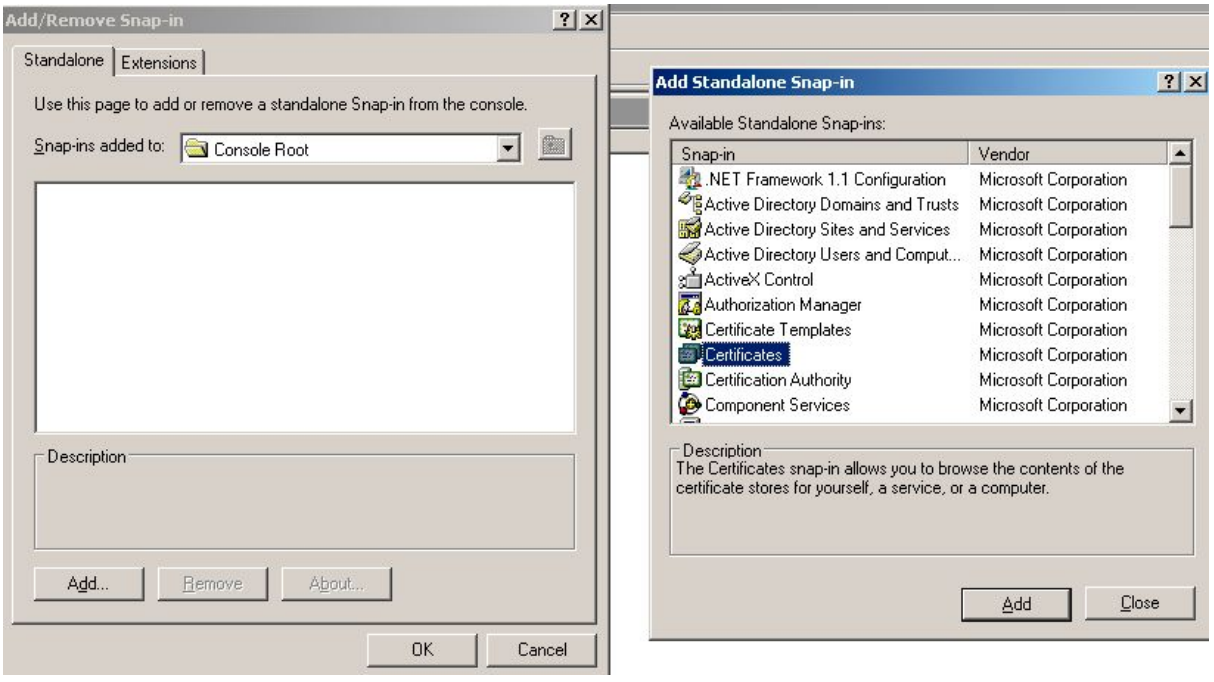




Em seguida no painel de controle, especificamente em "*Adicionar componentes do Windows*", selecionamos "*Serviços de Certificados*". Feita a instalação do certificado CA, foi necessário configurá-lo com um nome.

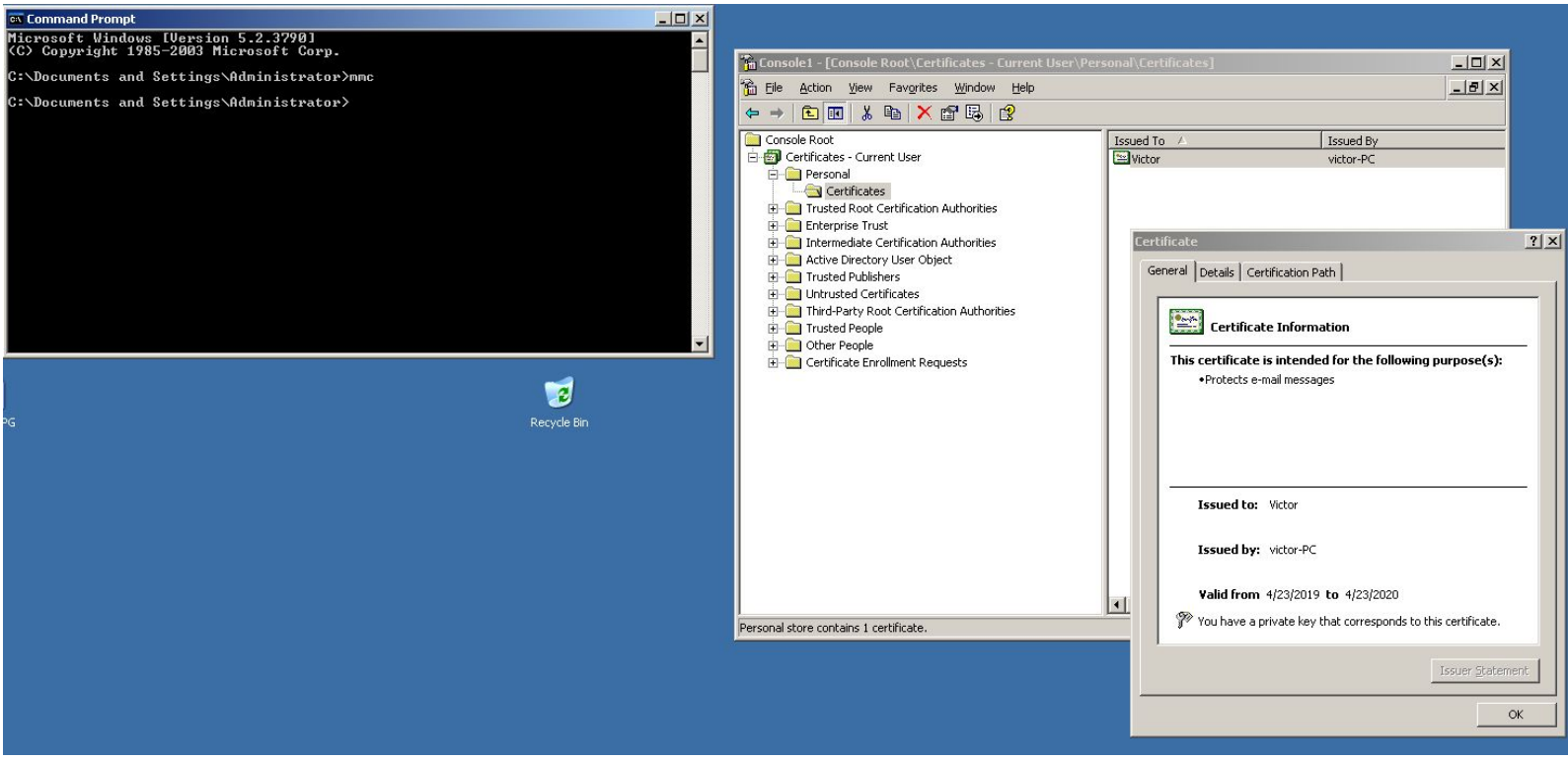


Executou-se então o prompt com o comando *mmc*, posteriormente indo em *Add, Adicionar/Remover Snap*, *certificados.*



Olhando nos certificados adicionados anteriormente, podemos verificar se a instalação do certificado ocorreu com êxito, indo em *Trusted Root Certification*

Authorities e em *Certificates*, devemos encontrar, o nome escolhido na configuração da *Autoridade Certificadora*.



IV. CONCLUSÃO

Com este relatório pode-se ter uma ideia real de como funciona uma autoridade certificadora, assim como os passo necessários para configurá-la e instalá-la, os passos necessários para a solicitação de certificados, como emitir, exportar e importar certificados utilizando as ferramentas do windows.

Ademais, foi possível ver a veracidade dos conceitos vistos em aula sobre a autoridade certificadora, certificados digitais e autenticação.

REFERÊNCIAS

[1] https://docs.aws.amazon.com/pt_br/iot/latest/developerguide/x509-certs.html
[2] Material disponibilizado em aula.