ATIVIDADE DE LABORATÓRIO III - E-MAIL SEGURO

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

I. INTRODUÇÃO

Na terceira atividade de laboratório o professor nos apresentou conceitos sobre autenticação e criptografia de e-mails. Posteriormente foram incumbidas tarefas como enviar email assinado digitalmente, enviar email criptografado, enviar e-mail assinado e criptografado ao mesmo tempo. Também foi exigido explicar a configuração para executar as operações de envio dos e-mails e o uso do gerenciamento de certificados digitais.

II. DESENVOLVIMENTO TEÓRICO

O S/MIME (Secure/Multipurpose Internet Mail Extensions) é um protocolo para enviar mensagens assinadas digitalmente e criptografadas. Ele permite a criptografia e assinatura digital de e-mails. Ao utilizar o S/MIME com uma mensagem de email, o destinatário que receber essa mensagem terá certeza de que o que veem em sua caixa de entrada é a mensagem exata que partiu do remetente. Isso também ajudará as pessoas que receberem mensagens a terem certeza de que a mensagem veio do remetente específico e não de alguém fingindo ser o remetente.

Para fazer isso, S/MIME presta serviços de segurança criptográfica como autenticação (**Signed Data**), integridade da mensagem e não recusa da origem (usando assinaturas digitais). Isso também ajuda a melhorar a privacidade e segurança (**Enveloped Data**) dos dados (usando criptografia) para mensagens eletrônicas.

As codificaçẽos utilizadas pelo S/MIME são pelo método **base64.** É um método de codificação de dados para transferência de conteúdo, utilizado frequentemente para transmitir dados binários por meios de transmissão que lidam apenas com texto, como por exemplo, o envio de anexos por e-mail. Ele é constituído por 64 caracteres (A-Z, a-z, 0-9 , “/” e “+”) que deram origem ao seu nome (64).

Os algoritmos utilizados para chave pública podem ser DSS, Diffie-Hellman, RSA. Para a função HASH os algoritmos podem ser SHA-1 e MD5. E os algoritmos para a chave privada são TDES e RC2. O S/MIME usa certificados de chave pública de acordo com a versão 3 do X.509.

III. DESENVOLVIMENTO EXPERIMENTAL

Para efetuar o experimento, é crucial completar as atividades propostas no relatório 2 pois utilizaremos certificação digital e o gerenciador de e-mail *Outlook*. Em um primeiro momento abrimos o *Outlook* e encaminhamos três e-mails para nós mesmo. O primeiro consistia em um email assinado digitalmente, o segundo um e-mail criptografado, e o terceiro criptografado e assinado. A **Figura 1** demonstra o primeiro passo da atividade.

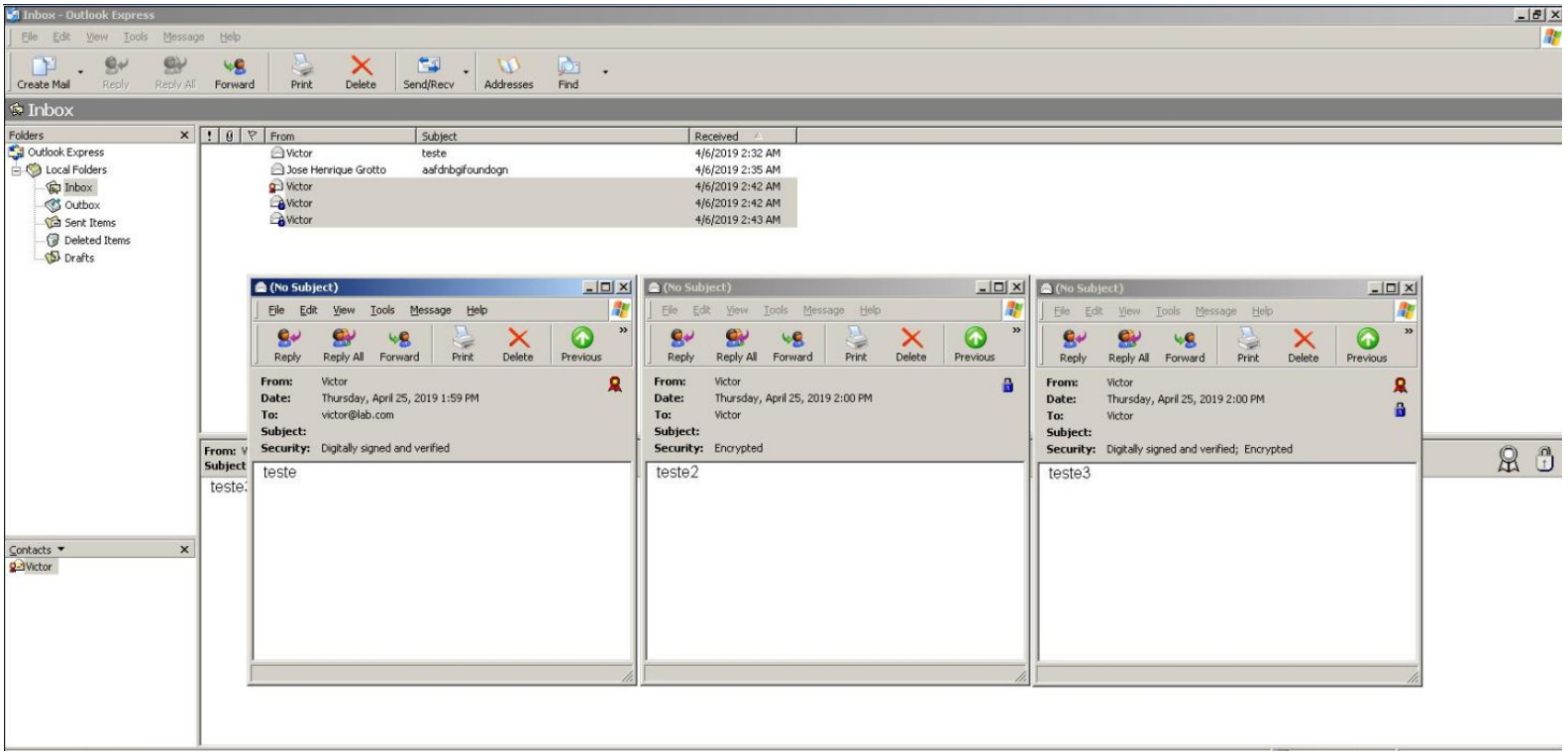

Figura 1: Envio de e-mail assinados, criptografados e assinados e criptografados para si.

Os três e-mails foram enviados com êxito, isso se deve pelo fato de já possuirmos nosso próprio certificado.

Feito isso, a próxima atividade era enviar os mesmo três tipos de e-mails para os colegas. Os colegas que participaram do experimento foram o Tobias e o José, que possuem respectivamente os e-mails tobias@lab.com e jose@loba.com. O e-mail autenticado pode ser enviado corretamente, entretanto, o e-mail criptografado ou autenticado e criptografado apresentou falhas, apresentando erro na autenticação do certificado. A **Figura 2** amostra o e-mail autenticado enviado para Jose.

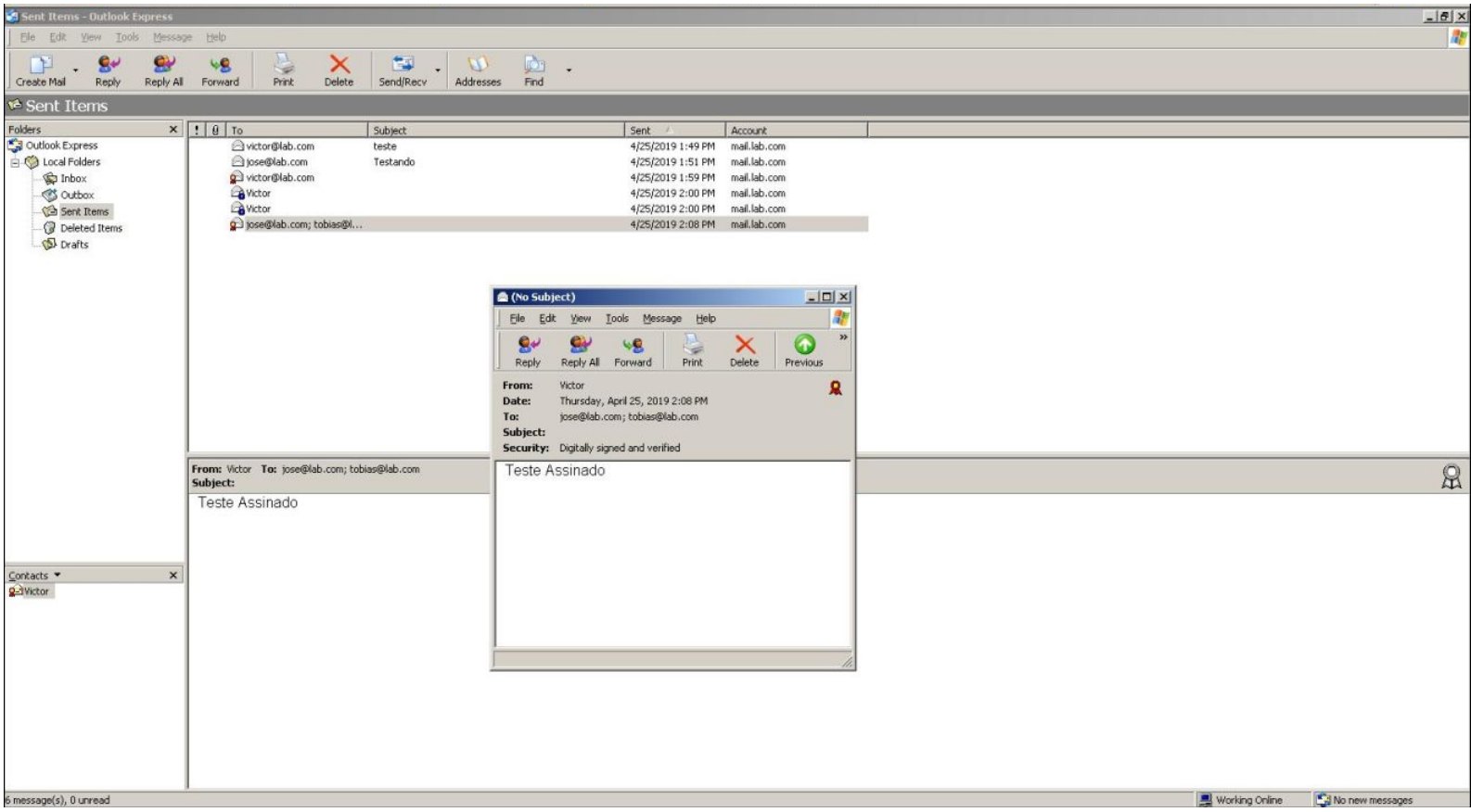

Figura 2: E-mail autenticado encaminhado para jose@lab.com.

Percebeu-se então que o problema no encaminhamento de e-mails criptografados para os demais colegas se dava pelo fato se não possuir os certificados dos mesmos, e que cada aluno utilizou uma Autoridade de Certificação diferente para a validação dos certificados, para isso, seria necessário obter os certificados da Autoridade Certificadora de cada aluno para que a comunicação ocorresse corretamente.

Uma das alternativas seria acessar a página da autoridade certificadora de cada um. Para isso seria necessário ter o conhecimento do *IP* dos envolvidos. Como por exemplo, o *IP* do José, colocaríamos no endereço *10.0.5.1/certsrv*, após isso seria necessário ir na terceira opção "*Download a CA certificate, certificate chain, or CTRL*" para efetuar o download do certificado da Autoridade Autenticadora desejado, depois disso seria necessário abrir o certificado e instalar (apenas dar *Next*). A **Figura 3** é uma imagem demonstrativa da página de *Download* do certificado.

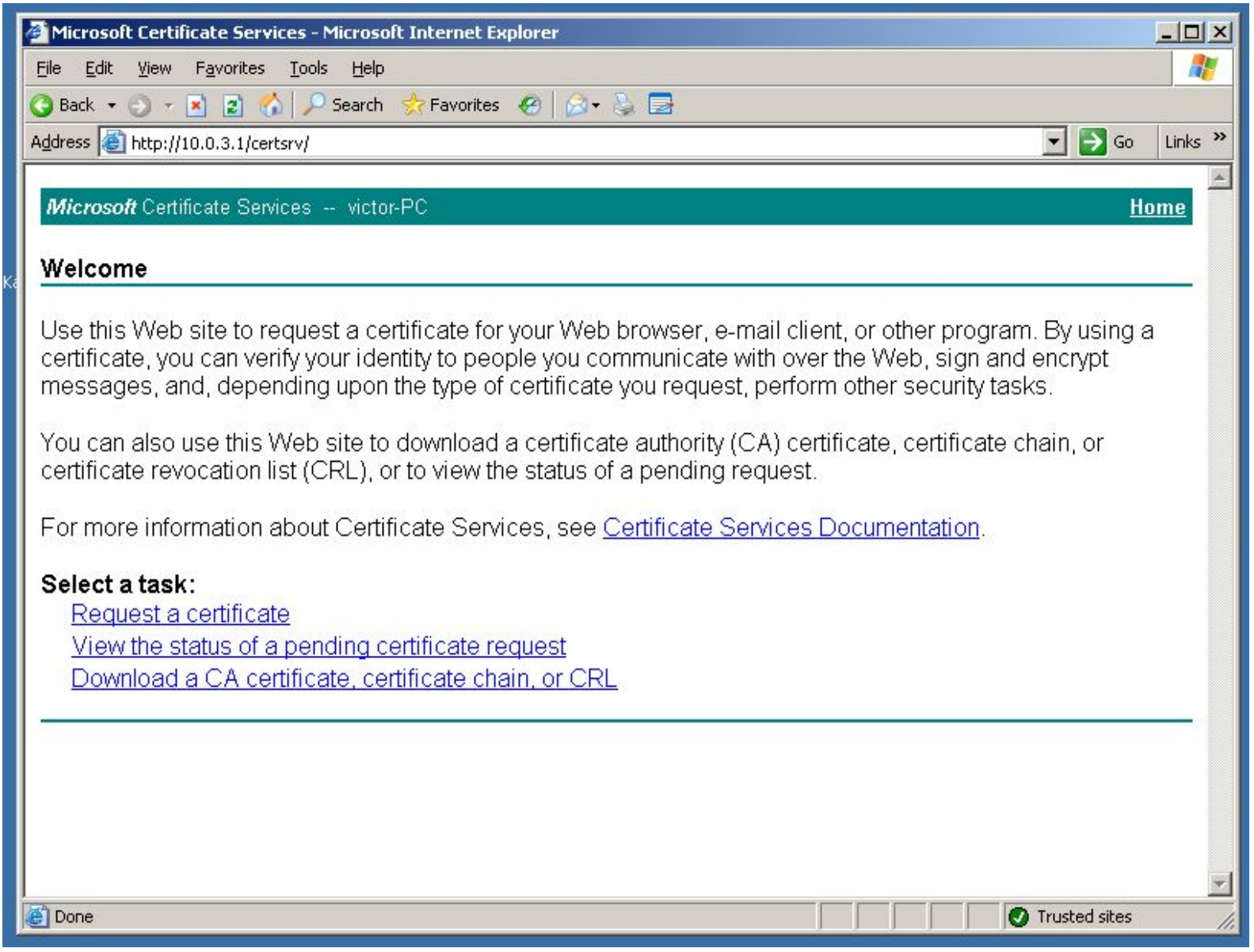

Figura 3: Imagem demonstrativa do site para download dos certificados desejados.

Em conjunto com os colegas, pensamos ter chegado em uma outra forma para obter os certificado de cada um: Enviar os certificados em anexo por e-mail. Para isso foi necessário mudarmos uma configuração do *Outlook* que bloqueia o recebimento de anexos, e em seguida (através do *Prompt de Comando*) executamos o comando *mmc* para que fosse possível exportar o certificado.

Para exportar o certificado basta ir em *Add, Adicionar/Remover Snap*, *certificados*, encontrar o nosso certificado, clicar com o botão direito do mouse (ou abrir o certificado e ir em *Detalhes*) e em seguida clicar em *Exportar*. As **Figuras 4, 5, 6, 7, 8, e 9** são imagens demonstrativas referentes a exportação do certificado.

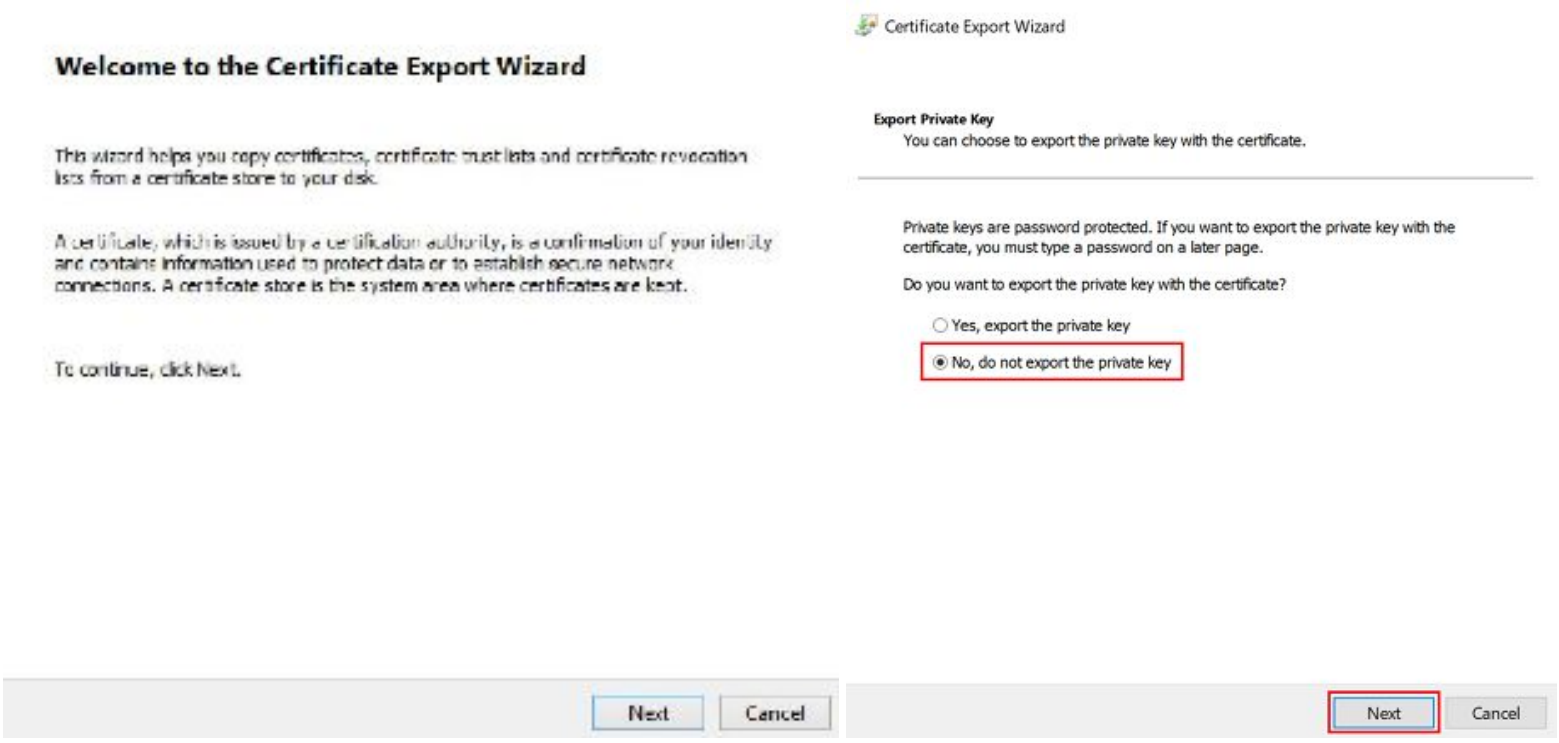

Figura 4 e 5: Exportação do certificado.

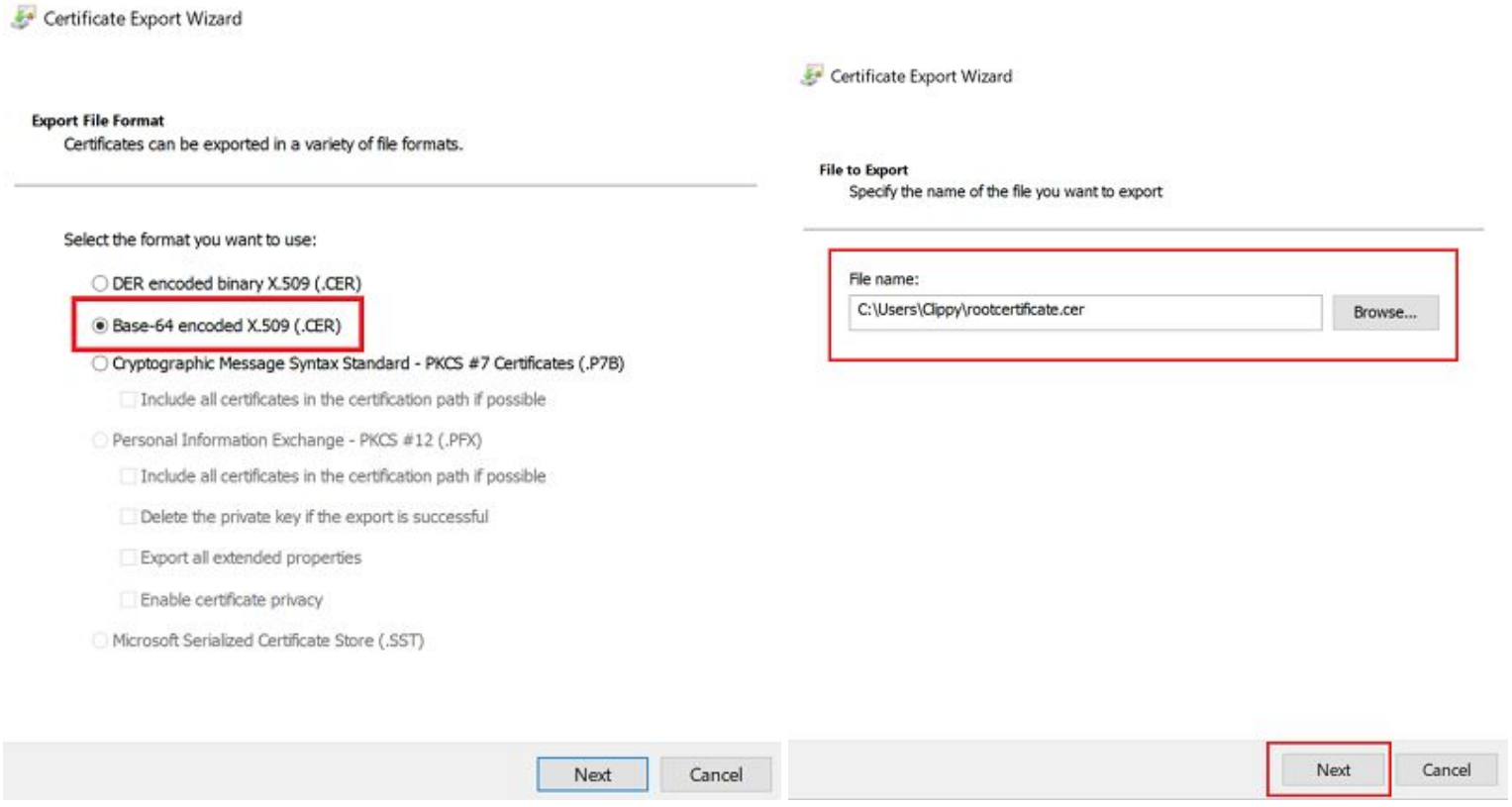

Figura 6 e 7: Exportação do certificado.

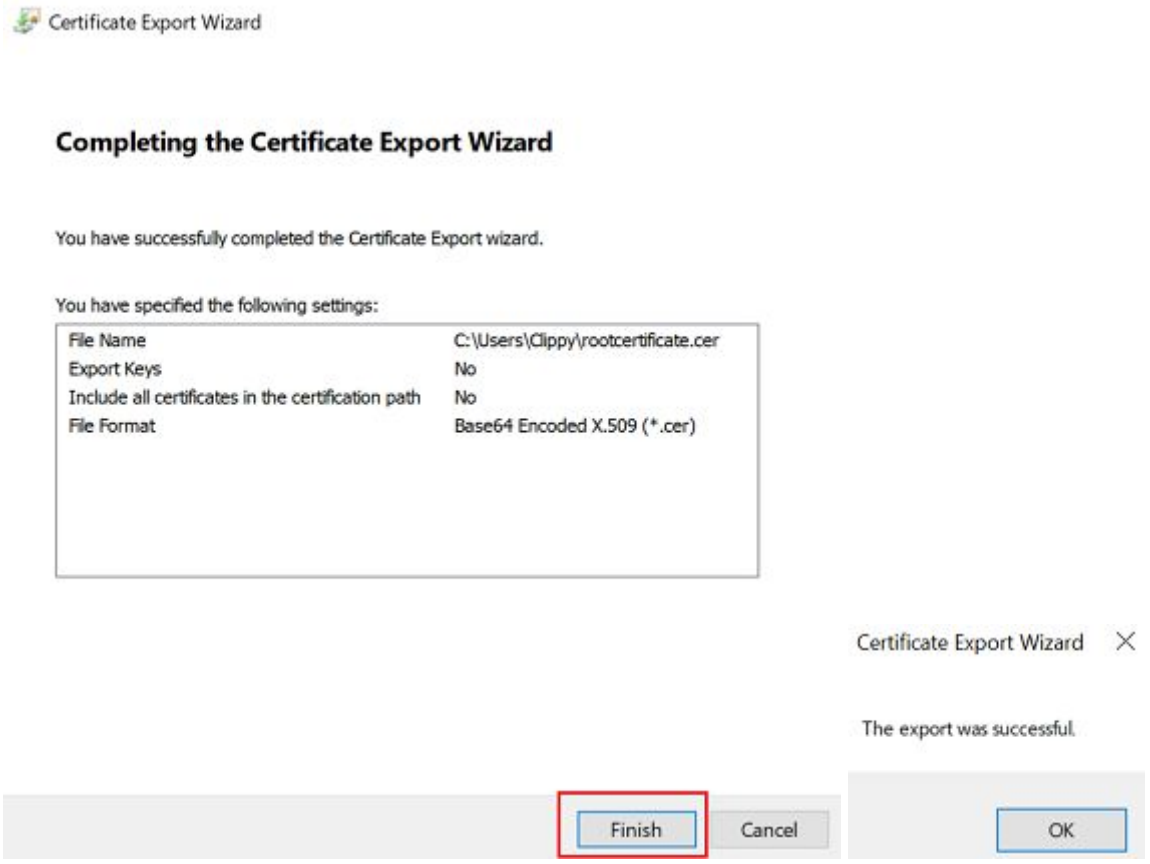

Figura 8 e 9: Exportação do certificado.

Após exportados, os certificados estarão no formato *.cer*, e cada aluno anexou seu certificado no e-mail e enviou o mesmo para os demais colegas (**Figura 10**).

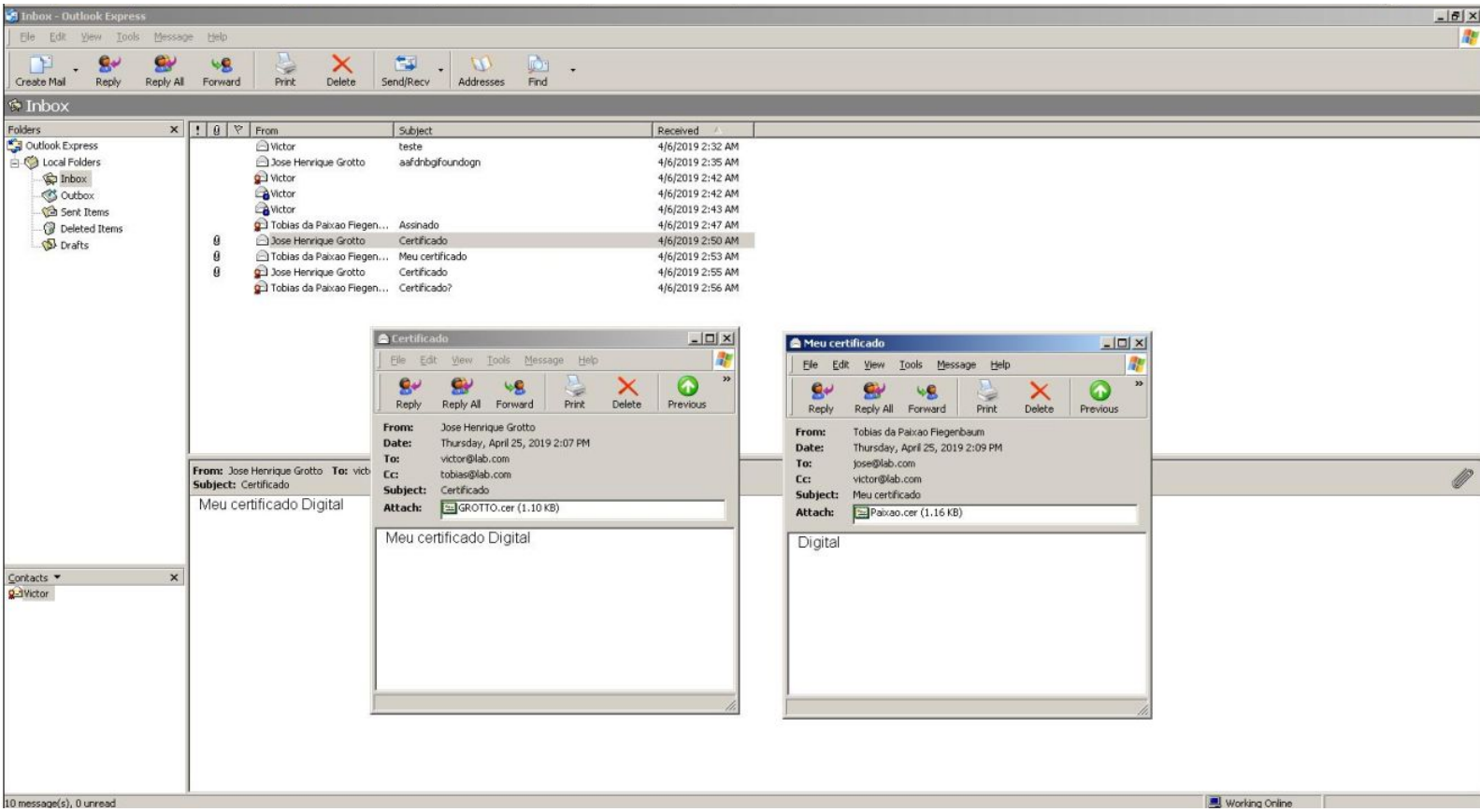

Figura 10: Envio de e-mail com os certificados anexados.

Após o recebimento do certificado efetuou-se o download do mesmo e posteriormente a instalação (dois cliques no certificado seguidos de *Next* até o final). Depois de instalados os certificados, os alunos tentaram enviar e-mails criptografados e a mensagem de erro continuou a ser exibida, chegou-se então a conclusão de que a segunda forma que havíamos pensado estar correta, exporta somente o certificado de cada usuário, e não o certificado da sua Autoridade Certificadora, como é feito do primeiro modo (**Figura 3**).

Essa diferença pode ser vista através da **Figura 11** e da **Figura 12**, onde vemos os certificados na aba de outros (certificados pessoais) e os certificados na aba de Trusted Root Certification Authorities (certificados da Autoridade de Certificação de cada aluno) respectivamente.

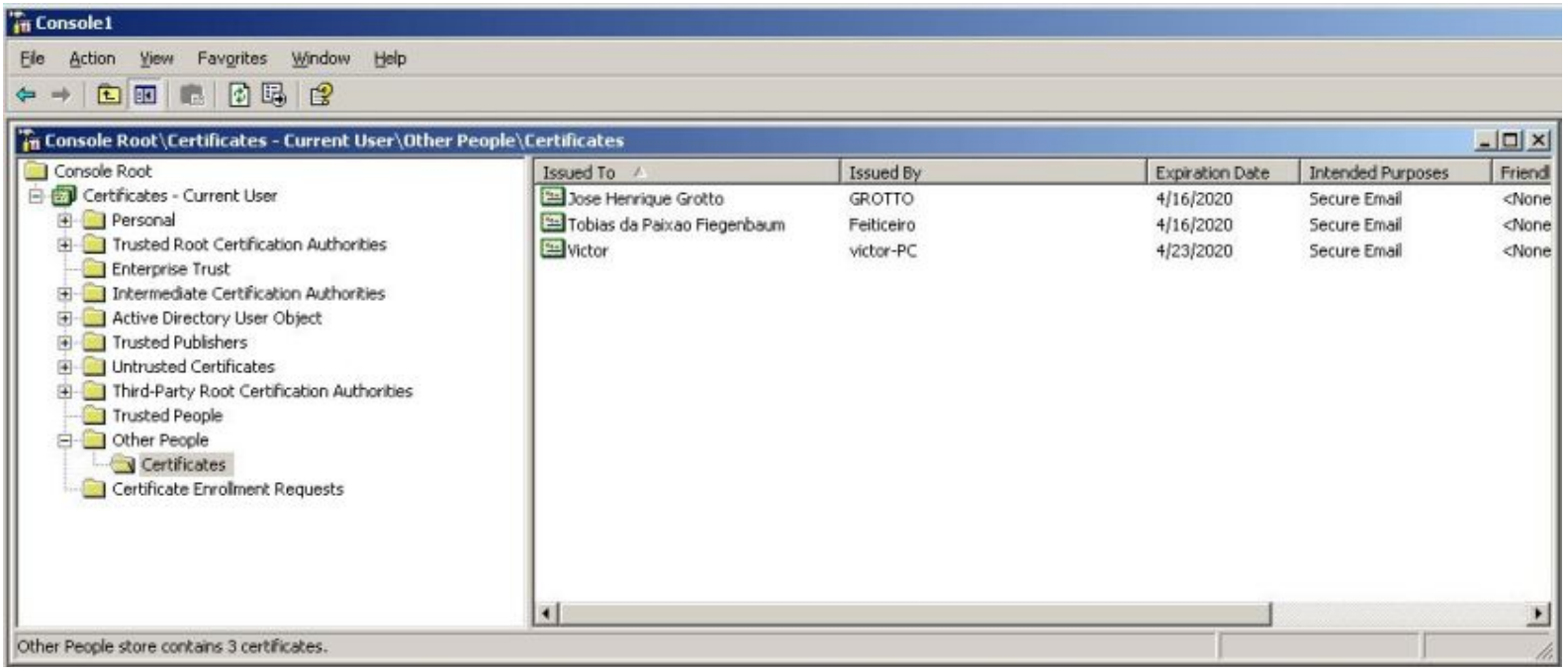

Figura 11: Certificados (user) instalados com sucesso.

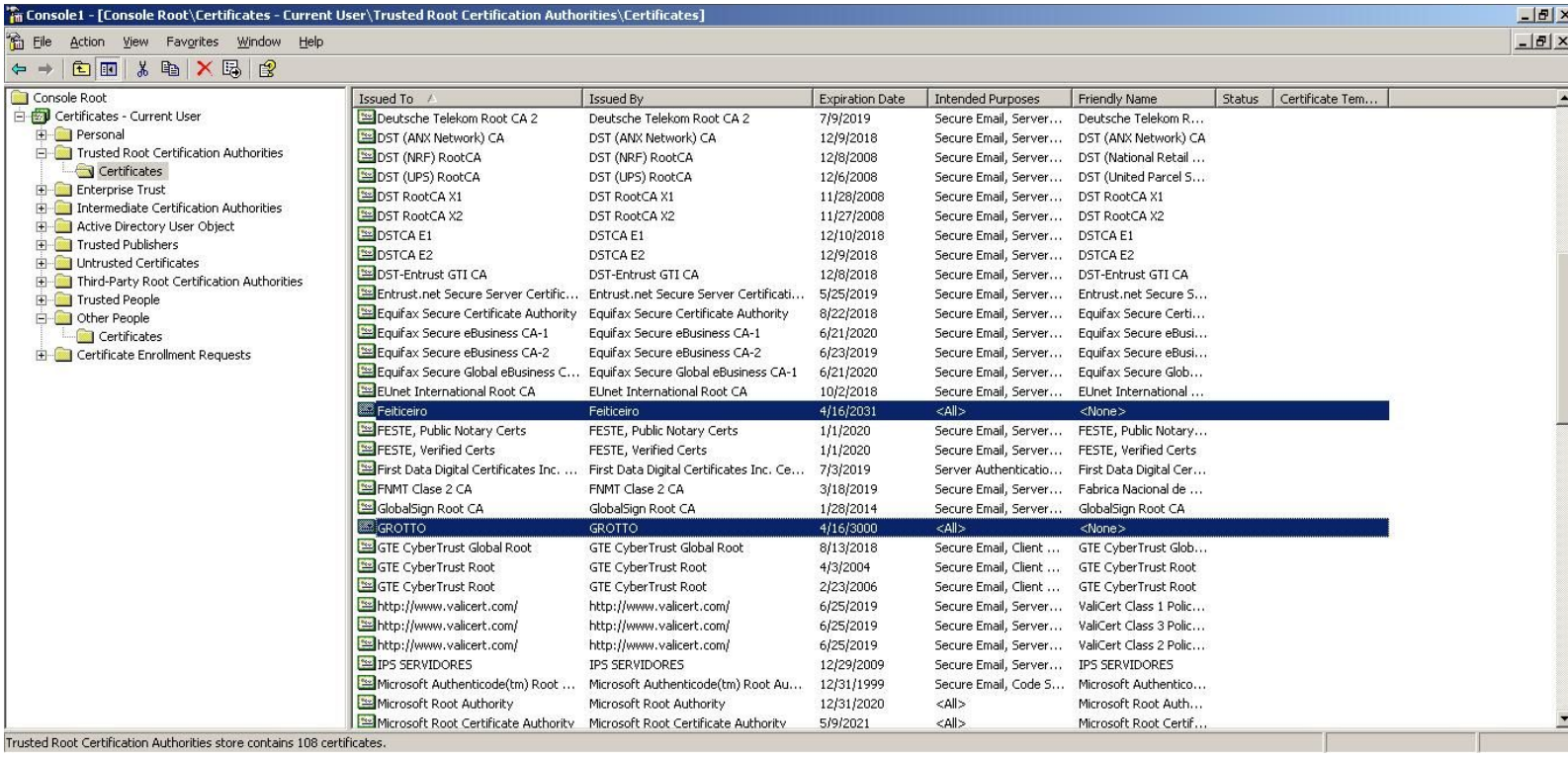

Figura 12: Certificados (CA) instalados com sucesso.

Feita a instalação correta dos certificados CA de cada aluno (seguindo o primeiro método, **Figura 3**), foi possível o envio de e-mails criptografados e assinados para os mesmo. Podemos ver através da **Figura 13** a diferença entre um e-mail normal e um e-mail criptografado e assinado digitalmente.

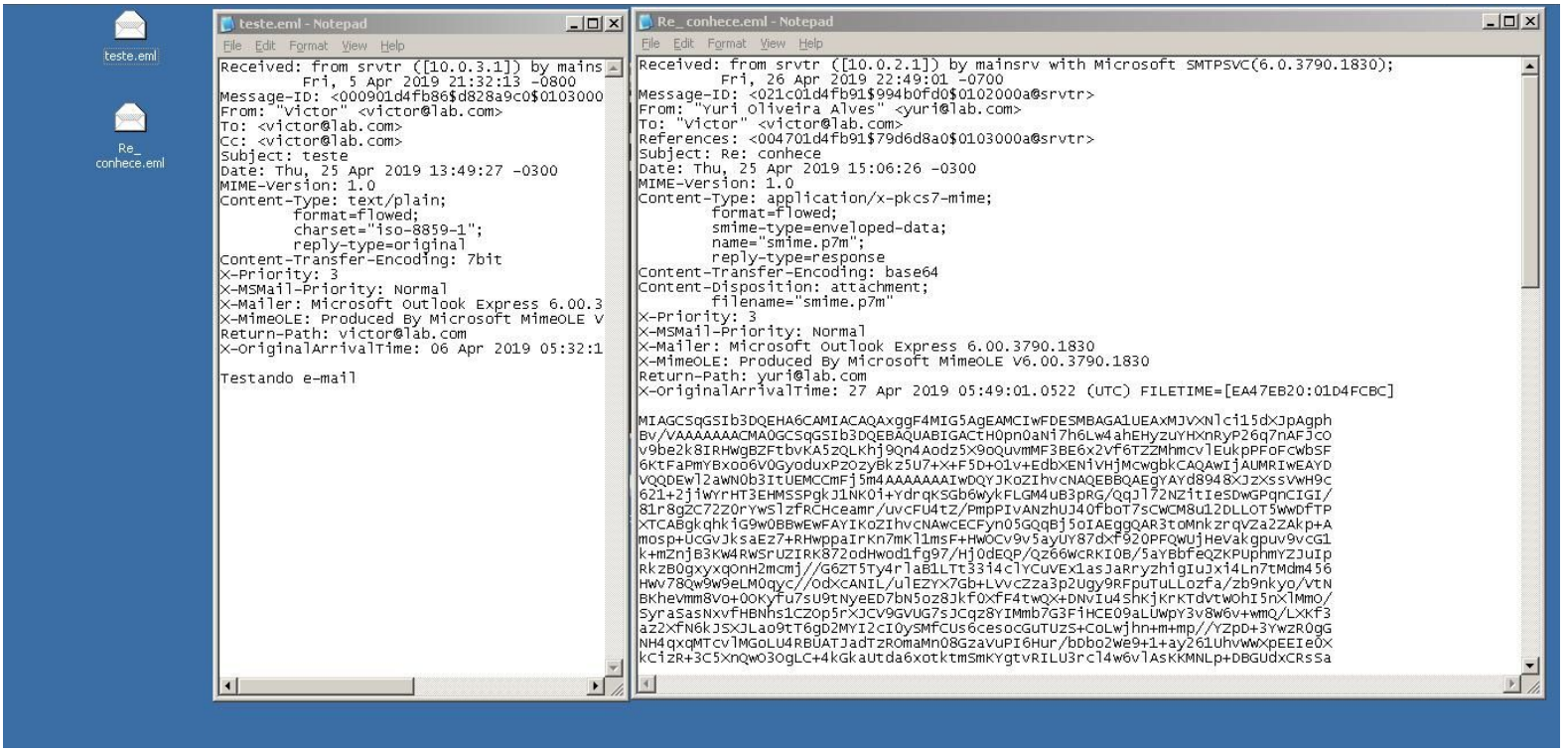

Figura 13: E-mail normal e e-mail criptografado e assinado respectivamente.

Podemos notar uma nítida diferença entre um e-mail normal (esquerda) e um e-mail assinado e criptografado (direita). Como já explicado na parte teórica, a criptografia utilizada foi do tipo TDES, uma criptografia de blocos que utiliza 3 chaves de 64 bits cada, fazendo com que a segurança e integridade da mensagem aumente.

IV. CONCLUSÃO

Por fim, este foi mais um laboratório muito importante, que nos proporcionou colocar em prática teorias estudadas anteriormente nas aulas teóricas, assim como verificar a veracidade dos conceitos sobre certificado digitais, autoridades certificadoras, e-mails assinados e criptografados estudados anteriormente.

REFERÊNCIAS

[1] **S/MIME For Message Signing And Encryption**
https://docs.microsoft.com/pt-br/office365/securitycompliance/s-mime-for-message-signing-and-encryption acessado em 28.04.2019.
[2] **VPN Gateway Certificates Point to Site**
https://docs.microsoft.com/pt-br/azure/vpn-gateway/vpn-gateway-certificates-point-to-site acessado em 30.04.2019.
[3] Material disponibilizado em aula.