SEGURANÇA EM CONEXÕES WEB

POR LÚCIA OLIVEIRA

Com o aumento das transações realizadas pela Internet e com grande parte dessas ações realizadas por intermédio de navegadores web, é fundamental saber reconhecer os tipos de conexões existentes e verificar a confiabilidade dos certificados digitais.

Existem dois tipos de protocolos de comunicação usados para acessar websites: o http (Hypertext Transfer Protocol) e o https (HyperText Transfer Protocol Secure). A diferença entre os protocolos é que o https utiliza uma camada adicional que permite a transmissão dos dados através de uma conexão criptografada, além de verificar a autenticidade do servidor de aplicação por meio de certificados digitais.

A criptografia impede que terceiros visualize a informação transmitida entre o navegador web e o servidor de aplicação, provendo integridade e confidencialidade. O uso de certificados digitais provê autenticidade, ou seja, garante que você está se comunicando exatamente com o website desejado.

Os certificados digitais são emitidos por entidades chamadas Autoridade Certificadora (AC). Uma AC é normalmente reconhecida por todos como confiável, fazendo o papel de "Cartório Eletrônico". Um certificado emitido por uma AC oficial – credenciada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) – é reconhecido automaticamente pelos navegadores Web.

Geralmente, o certificado emitido por uma AC oficial envolve custo financeiro para emissão e renovação anual do mesmo. Então, muitas instituições, governos e corporações adotam a emissão de seus próprios certificados digitais (autoassinados).

A DINFO adota o uso do protocolo https em suas aplicações web em que o acesso só é permitido com o fornecimento de login e senha ou algum outro dado pessoal. Utilizamos, também, certificados digitais emitidos, sem custo, pela AC StartCom e com validade de um ano. Entre a data de solicitação de renovação do certificado e emissão do novo certificado, utilizamos o tipo autoassinado.

A fim de evitar o "roubo" de informações, principalmente de login e de senha de acesso da aplicação web, solicitamos que o usuário:

1. mantenha o seu navegador web com a versão mais recente e com todas as atualizações aplicadas;
2. mantenha seu computador seguro com as atualizações do sistema operacional e antivírus aplicadas;
3. Digite a URL (Uniform Resource Locator), ou seja, o endereço de rede da aplicação, diretamente no navegador. Tenha cuidado ao acessar aplicações por meios de links recebidos por mensagens eletrônicas. Nesse caso, posicione o mouse no link e verifique no rodapé da página para que endereço eletrônico o link está apontando, ou seja, se corresponde ao link desejado;
4. Identifique o tipo de conexão em uso. Se a conexão não for segura, não forneça seu login e sua senha de acesso. Entre em contato imediatamente com a DINFO e relate o problema.

Para identificar uma conexão como segura, verifique:

1. Se o endereço do website/aplicação começa com "https://";
2. Se o desenho de um "cadeado fechado" é mostrado na barra de endereços.
3. Se desejar saber mais detalhes sobre o tipo de conexão e sobre o certificado digital utilizado, clique sobre o "cadeado fechado" na barra de endereço.

EXEMPLO 1:

Cenário: Sistema Operacional Windows e navegador web Google Chrome

Ao acessar o site www.id-unico.uerj.br, o navegador apresenta a tela "Primeiro Acesso", que solicita alguns dados pessoais do usuário.

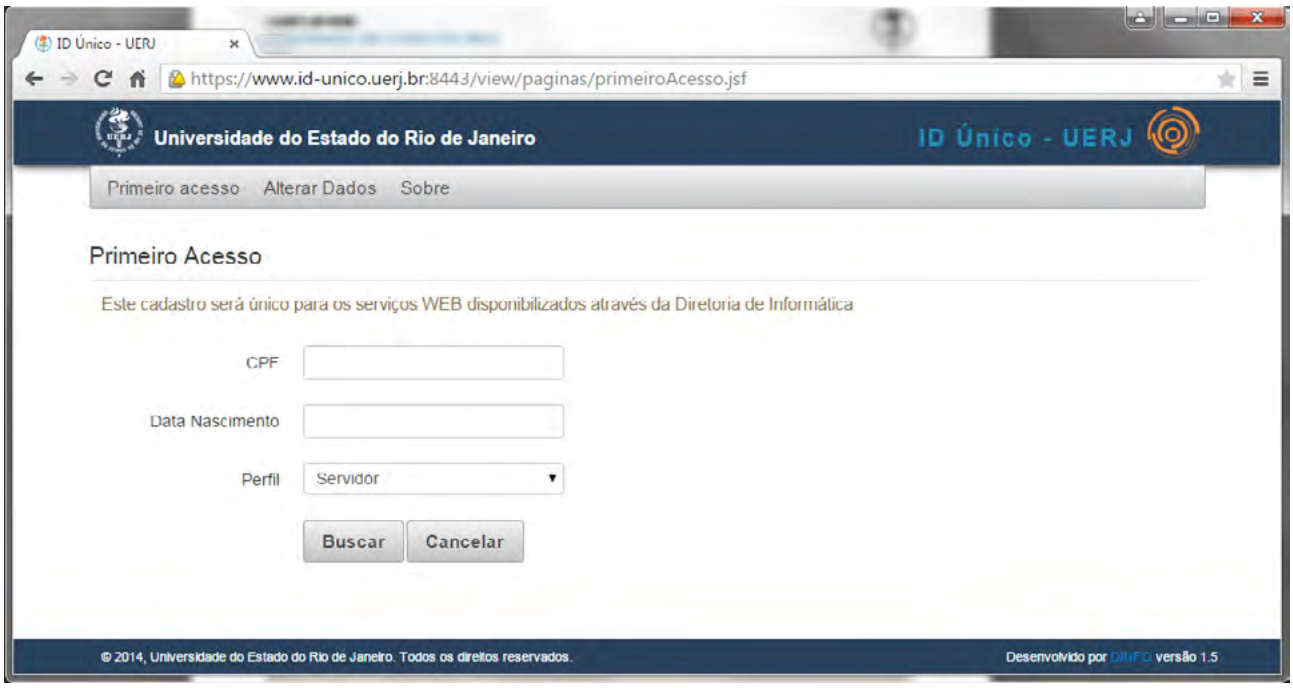

Figura 1: Tela Primeiro Acesso da aplicação ID Único

Na Figura 1, observe, na barra de endereço, que o protocolo utilizado é o https e o "cadeado está fechado e sem alertas". Logo, a conexão é segura, provendo integridade, confidencialidade e autenticidade.

Para saber mais detalhes sobre a conexão e o certificado digital utilizado, clique sobre o "cadeado fechado".

A figura 2 mostra os detalhes de uma conexão segura utilizando certificado digital emitido pela StartCom.

EXEMPLO 2:

Cenário: Sistema Operacional Windows e navegador web Google Chrome

Ao acessar o site www.helpdesk.dinfo.uerj.br, o navegar exibe um alerta "**Sua conexão não é particular**" (ver figura 3) e solicita a confirmação do usuário no "Ir para www.helpdesk.dinfo.uerj.br (não seguro)" para acessar o website/aplicação.

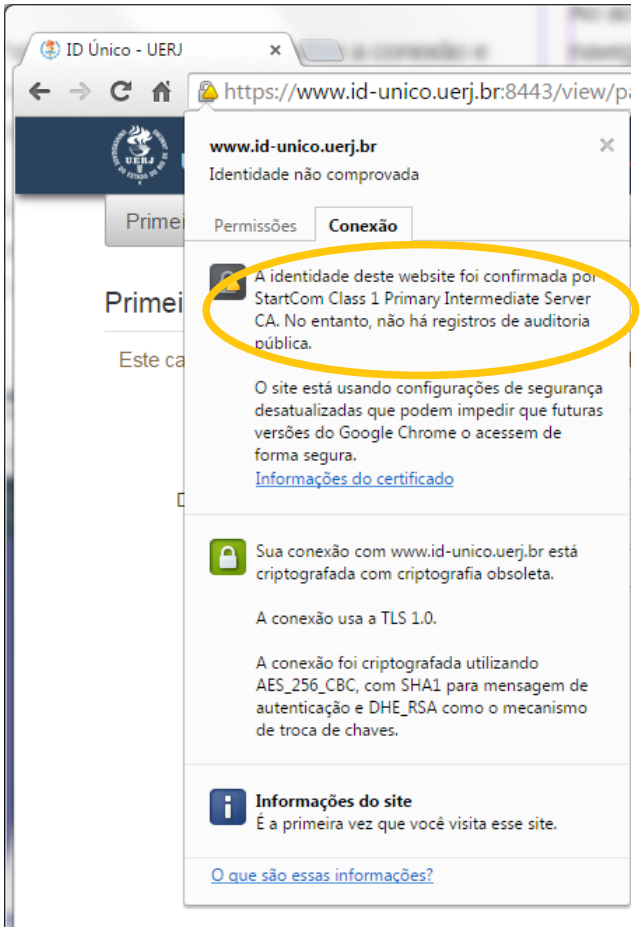

Figura 2 – Detalhes de uma conexão segura com certificado digital emitido pela AC StartCom.

Figura 3 – Mensagem de alerta para website com certificado digital autoassinado.

Observe, na barra de endereço, que o protocolo utilizado é o https e o "cadeado está fechado". Esse tipo de conexão garante a integridade e confidencialidade dos dados. Contudo, como o navegador web não reconheceu a AC que emitiu o certificado digital (certificado autoassinado) ou a validade do mesmo expirou, não pode garantir a autenticação.

Clique sobre o "cadeado fechado" para visualizar os detalhes da conexão (ver figura 4).

O primeiro "cadeado", mostrado na guia Conexão (ver figura 4), indica que o certificado digital não foi emitido por uma AC "oficial".

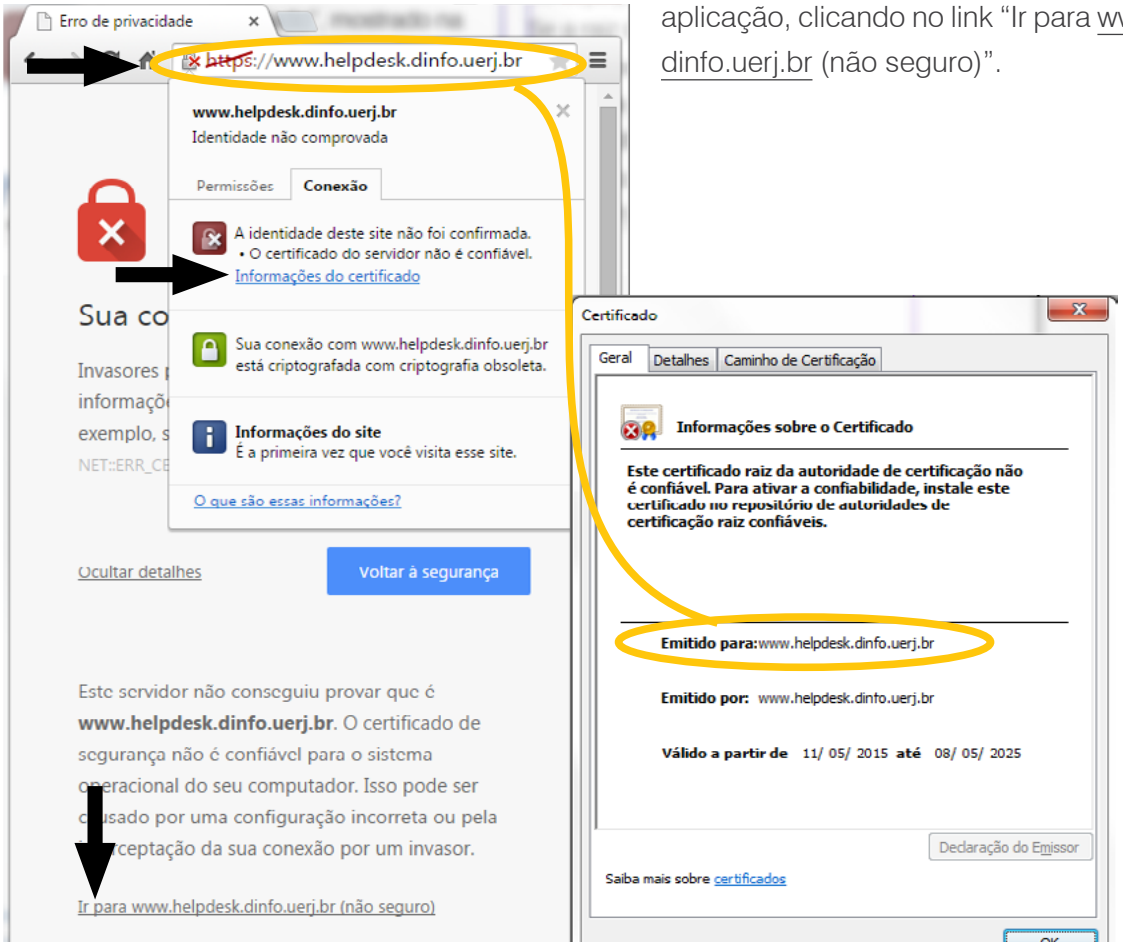

Figura 4 – Detalhes da conexão com certificado digital autoassinado.

O segundo "cadeado", mostrado na guia Conexão (ver figura 4), indica que o navegador web estabeleceu com êxito uma ligação segura com o website.

Clique em "**Informações do certificado**" (ver figura 4) e verifique se o mesmo foi emitido para o website/aplicação comparando o endereço eletrônico com a informação "**Emitido para**" do certificado digital. Um certificado digital (autoassinado) é emitido para uma e somente uma URL, ou seja, para um endereço eletrônico específico. Se a raiz da URL (a parte principal da URL), que está na barra de endereço, for igual ao campo "**Emitido para**" do certificado digital, o certificado é válido e o usuário pode confiar no website/aplicação, clicando no link "Ir para www.helpdesk.dinfo.uerj.br (não seguro)".