Parte 1: Configurando um servidor para utilizar certificados do cliente na autenticação

<https://msdn.microsoft.com/pt-br/library/ee923720.aspx?tduid=(0b73d400892f79a9e452483357ae3ee1)(256380)(2459594)(TnL5HPStwNw-Yqbx1uUyDsu6mM1ML6DlPw)()>

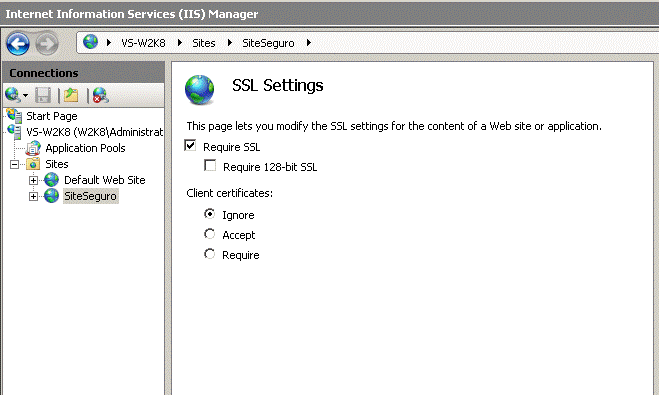
Agora que já temos um bom panorama do porque os certificados são importantes e como sua infraestrutura foi planejada vamos configurar o IIS para utilizar os certificados. Utilizaremos uma certificadora baseada no Windows 2008 para a emissão, já que para podermos fazer o processo de autenticação por certificados precisamos que o servidor IIS esteja com SSL habilitado. O meu servidor já está certificado e abordaremos como este processo foi feito adiante. Utilizarei neste exemplo um certificado próprio emitido pelo Windows 2008, mas o processo é o mesmo para o e-CPF/e-CNPF, apenas ao invés de utilizar um servidor próprio utilizaria um do ICP Brasil.

Talvez você se pergunte porque utilizar uma certificadora própria se o ICP-Brasil já existe para isso, mas lembre-se de que no inicio do artigo foi comentado que os certificados e-CPF/e-CNPJ são pagos, e com preços bastante elevados por sinal.

Nota  
Lembre-se que Autoridade Certificadora (CA) é quem emite o certificado, arquiva e mantêm a lista de revogação (CRL). Se o CA é interna ou da internet como as mais conhecidas e do ICP-Brasil não faz diferença no uso de PKI e certificados digitais.

Outra questão é como fazer o mesmo processo em servidores, como o Apache, por exemplo. Qualquer servidor web permite o uso de certificados para SSL, mas obviamente não é tão simples quanto no IIS. Quanto a emissão de certificados, tocamos no calcanhar de aquiles, já que emissão de certificados no Linux é bem mais complexo do que no Windows Server, mas também pode ser feito. Contudo, não vamos abordar esse tema nesse artigo.

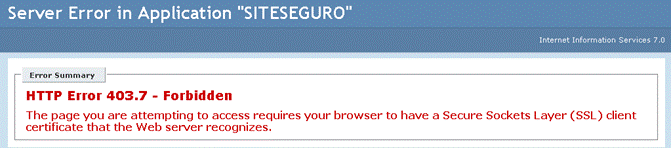
Voltando ao IIS, veja na Figura 5 que para utilizar a opção “Require client certificate” é necessário também ter o servidor certificado. Caso não possua o seu servidor com SSL poderá utilizar a opção “Accept client certificate” que não exige, apenas permite o uso de certificados pelo cliente, não garantindo assim um bom método de autenticação.



**Figura 5** **- Habilitando o uso de certificados no IIS**

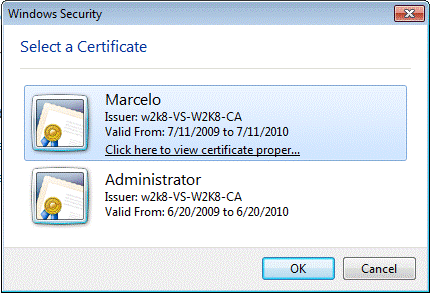
A Figura 6 demonstra o que acontece ao tentar acessar um servidor certificado e com obrigatoriedade de certificado pelo cliente. O erro “403.7” obviamente pode ser redirecionado para uma página de erro customizada que informe ao usuário que ele precisa comprar um certificado e a lista de onde isto pode ser feito, por exemplo.

Nota  
Não tente tratar este erro por try-catch pois a aceitação e leitura do certificado é feita diretamente pelo IIS, e neste caso a aplicação nem é inicializada.



**Figura 6** **- Acesso proibido por falta de um certificado**

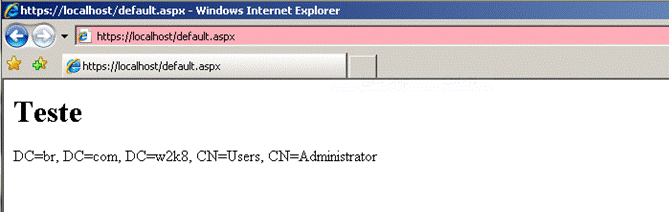
Após instalar o certificado para o meu usuário, Figura 7, uma lista dos certificados que eu possuo na maquina é mostrada, permitindo que eu escolha qual utilizar. Esta lista só aparece caso o usuário solicite ou se existirem múltiplos certificados.



**Figura 7** **- Certificado sendo solicitado ao usuário**

Parte 1.1: Utilizando os dados do certificado

O próximo passo é ler os dados do certificado para validar o usuário, e isto é mostrado na Figura 8, onde está listado o conteúdo do “subject” com os dados utilizados quando comprei o certificado. Para extrair estes dados foi utilizado o código da Listagem 1, que é extremamente simples.



**Figura 8** **- Acesso permitido e os dados do certificado exibidos**

HTML

  <HTML>

       <BODY>

             <H1>Bem-vindo </H1>

             <%=Request.ClientCertificate.Subject%>

       </BODY>

</HTML>

Listagem 1. Código ASP para ler os dados do certificado

Vale lembrar que neste certificado o subject é o email do cliente, mas isto é configurável, portanto o subject de um e-CPF será o numero do documento.