

Cartão de Cidadão

Autenticação com o Cartão de Cidadão

20 de Novembro de 2007

Versão 1.6

AMA

ÍNDICE

1. INTRODUÇÃO	3
<i>Modelo base de Autenticação</i>	<i>3</i>
<i>Modelo de Autenticação Federado</i>	<i>4</i>
2. AUTENTICAÇÃO COM O CARTÃO DE CIDADÃO	5
2.1. ARQUITECTURA DE AUTENTICAÇÃO	5
2.2. USABILIDADE	7
3. CONFIGURAÇÕES SERVIDOR.....	9
3.1. EXEMPLO DE CONFIGURAÇÃO COM IIS.....	9
3.2. INSTALAÇÃO DA ROOT DOS CERTIFICADOS	11
4. REFERÊNCIAS.....	13

1. Introdução

Com o Cartão de Cidadão, torna-se possível a realização de autenticação em *web sites* usando o certificado digital existente no *chip* do Cartão, tendo o cidadão de possuir um PC com um leitor de *SmartCard*.

Modelo base de Autenticação

Este documento identifica genericamente as tarefas preparatórias que devem ser cumpridas no servidor de suporte ao *web site* que pretenda oferecer a autenticação do “visitante” através do Cartão de Cidadão, demonstrando, a título exemplificativo, as configurações a realizar e o código para leitura do certificado. É ainda apontada a regra de boa prática de usabilidade, na qual se sublinha a obrigatoriedade dos interfaces indicarem com a máxima clareza, o serviço de autenticação com o Cartão de Cidadão.

De uma forma genérica, de modo ao servidor efectuar o pedido do certificado existente no Cartão de Cidadão, são necessários efectuar os seguintes passos:

- **Configurar o servidor para ligações SSL** – será necessário obter um certificado para o site em questão e proceder à sua instalação no servidor *web*, de modo a ser possível estabelecer comunicações seguras entre o servidor e as aplicações clientes;
- **Configurar o servidor para aceitar certificados de clientes** – neste passo configura-se o servidor de modo a este efectuar o pedido ao cliente de um certificado digital;
- **Configurar o servidor para pedir e aceitar o certificado do Cartão de Cidadão** – os servidores estão normalmente configurados para pedir e aceitar certificados clientes que sejam emitidos pelo seu *LDAP*, neste passo configura-se o servidor de modo a ele aceitar igualmente certificados emitidos pela *Certification Authority* emissora dos certificados presentes no Cartão de Cidadão (*GTE CyberTrust*);
- **Validação aplicacional do certificado** – Uma vez que existem diversos certificados clientes emitidos pela *GTE CyberTrust*, e de forma a garantir que só são aceites certificados presentes nos Cartões de Cidadão, o código desenvolvido para autenticação, deve validar um conjunto de parâmetros presentes no certificado, de forma a garantir a origem do certificado;

- **Validação de validade do certificado** - A última validação é efectuada pela entidade emissora do certificado, de modo a garantir que o certificado não foi revogado.

As configurações apresentadas no capítulo 3 têm como exemplo a utilização de um servidor com sistema operativo *Windows* 2003 com IIS 6.0.

Modelo de Autenticação Federado

No âmbito do projecto da Plataforma de Interoperabilidade da Administração Pública - *Framework* de Serviços Comuns é disponibilizado um modelo de autenticação federado. Este modelo de autenticação, prevê a existência de Fornecedores de autenticação, que são peças de software que permitem a autenticação de uma forma standard e independente das tecnologias de credencial utilizadas. Para o caso específico do cartão de cidadão está também em desenvolvimento um fornecedor de autenticação específico. Este fornecedor de autenticação implementa a autenticação com base no cartão de cidadão de acordo com as recomendações descritas neste documento.

A utilização do fornecedor de autenticação do cartão de cidadão, em alternativa a uma implementação específica de autenticação tal como é descrito neste documento, tem como vantagens para além de evitar que se repitam as implementações específicas de autenticação com o cartão, a possibilidade de Single Sign On bem como o reconhecimento automático do cartão de cidadão na execução dos serviços electrónicos existentes na plataforma de interoperabilidade.

Este modelo de autenticação é apresentado noutro documento específico, com uma descrição detalhada do Fornecedor de Autenticação do Cartão de Cidadão, bem como com os detalhes técnicos da sua utilização.

2. Autenticação com o Cartão de Cidadão

2.1. Arquitectura de Autenticação

O Cartão de Cidadão tem, no seu chip, dois certificados digitais:

- **Certificado digital de autenticação** – certificado digital que identifica univocamente um Cidadão e permite o acesso a serviços electrónicos de forma segura;
- **Certificado digital para assinatura digital qualificada** – certificado digital com enquadramento legal que permite assinatura digital de documentos de forma idêntica à assinatura manual reconhecida.

As Entidades (públicas ou privadas) que disponham de serviços electrónicos e que necessitem da autenticação do Cidadão, poderão adaptá-los de forma a permitir uma autenticação forte através do certificado digital de autenticação presente no cartão.

Note-se que este processo pressupõe que o Cidadão já se registou na Entidade, possuindo por isso uma credencial de identificação interna ao mesmo (dados de identificação do Cidadão existentes na Entidade).

A Entidade que disponibiliza o serviço electrónico, deverá pedir a validação do certificado de autenticação a uma entidade externa, designada por CA (Certificate Authority), que é responsável pela emissão e gestão dos certificados do Cartão. Esta validação obtém-se por consulta da lista de certificados activos e revogados, disponibilizada pela CA.

Caso o resultado da validação indique que o certificado do Cidadão se encontra activo, o sistema da Entidade poderá associar o certificado recebido à credencial interna do Cidadão.

Esta associação poderá ser efectuada, por exemplo, entre a credencial e os dados de identificação contidos no certificado digital, como sejam o nome e a data de nascimento do Cidadão e, caso legalmente autorizado, o respectivo número de identificação civil. Outro dado de possível associação para reconhecimento do Cidadão no Sistema do Organismo, através do Cartão de Cidadão, é o próprio identificador do certificado digital. No entanto, para que esta se possa verificar, a Entidade deverá ter associado previamente o identificador do certificado do Cartão de Cidadão à credencial interna do Cidadão. O Identificador do certificado digital é cancelado sempre que o respectivo Cartão de Cidadão seja revogado, mantendo-se enquanto o mesmo for válido.

Após a associação, o sistema da Entidade poderá validar e permitir ao Cidadão o acesso aos serviços electrónicos disponíveis ao seu perfil.

Resumindo:

1. O processo de validação da identidade do Cidadão baseado no Cartão de Cidadão garante a associação entre os dados do Cartão, incluindo o certificado digital produzido, e o seu titular;
2. A verificação do certificado digital de autenticação na CA permite verificar se este se encontra válido;
3. No entanto, é a Entidade que, após verificação no seu Sistema de Informação, autentica o Cidadão e lhe concede os privilégios de acesso aos serviços electrónicos disponíveis.

Este tipo de autenticação tem como principal vantagem a segurança, visto que só poderá ser utilizado por um cidadão que tenha Cartão de Cidadão, que conheça o PIN de acesso ao certificado e que possua um certificado válido; por outro lado, a entidade que fornece o serviço electrónico, deverá pedir a validação do mesmo a uma entidade externa, responsável pela emissão e gestão dos certificados do Cartão de Cidadão, de modo a garantir que o certificado que o cidadão apresentou ainda se encontra válido. Só a partir desse momento o cidadão é autenticado pela Entidade, estabelecendo-se uma comunicação segura entre ambos (ver Figura seguinte).

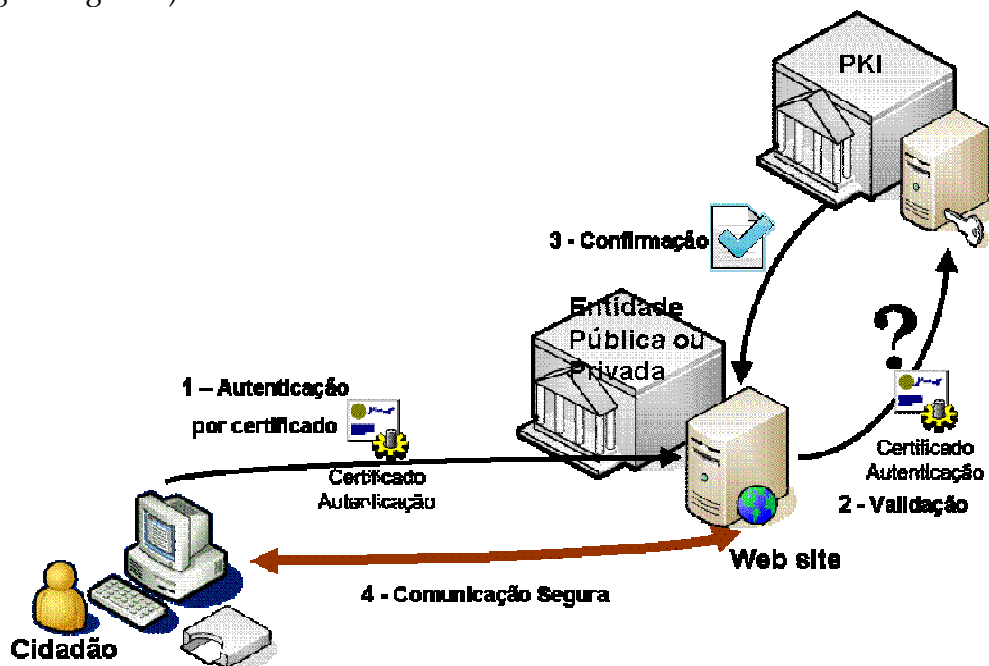


Figura - Utilização de certificado de autorização

Este canal de autenticação poderá ser utilizado desde o primeiro momento com vantagens para cidadãos e entidades:

- Possibilitar uma experiência de utilização semelhante na interação com diferentes Entidades Públicas e/ou Privadas;
- Disponibilizar níveis de segurança superiores aos actuais mecanismos de utilizador/palavra-chave, normalmente utilizados.

De forma semelhante à agregação de vários cartões físicos num só, os mecanismos de autenticação do Cartão de Cidadão permitem simplificar e potenciar o uso de serviços electrónicos da Administração Pública e envolver os cidadãos na utilização de serviços de *e-government*.

Como principal vantagem na utilização do certificado de autenticação existente no Cartão de Cidadão, temos a simplificação no acesso a serviços online para o Cidadão, uma vez que deixa de ser necessário ter um utilizador e uma password para cada entidade, passando a usar somente o seu Cartão de Cidadão, e o respectivo pin.

2.2. Usabilidade

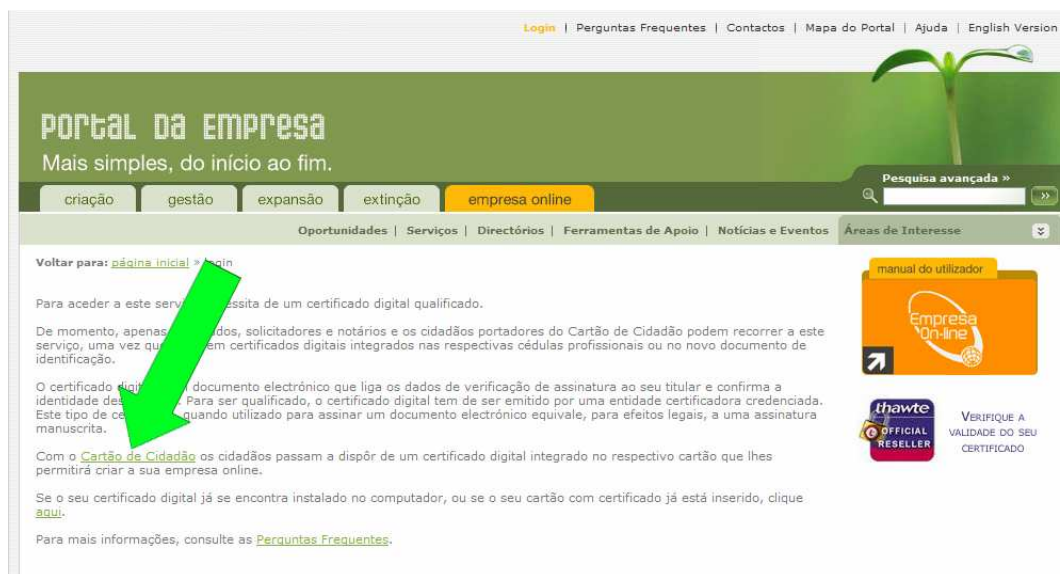
Nos sistemas cuja autenticação ou a execução de serviços seja realizada através do Cartão de Cidadão, as referidas acções devem estar devidamente assinaladas e referenciadas através de imagens ou textos que identifiquem claramente o acesso ou a execução de um serviço via Cartão de Cidadão.

Como exemplo desta prática, ilustram-se duas imagens referentes a dois portais que se encontram disponíveis:

- **Portal do Cidadão**



- **Portal de Empresa**



Os referidos acessos ou execução de serviços não devem ser realizados automaticamente de modo a que o cidadão não se aperceba de tal facto. Deve ser o cidadão a fornecer o estímulo para se autenticar ou utilizar um dado serviço, através do seu Cartão de Cidadão.

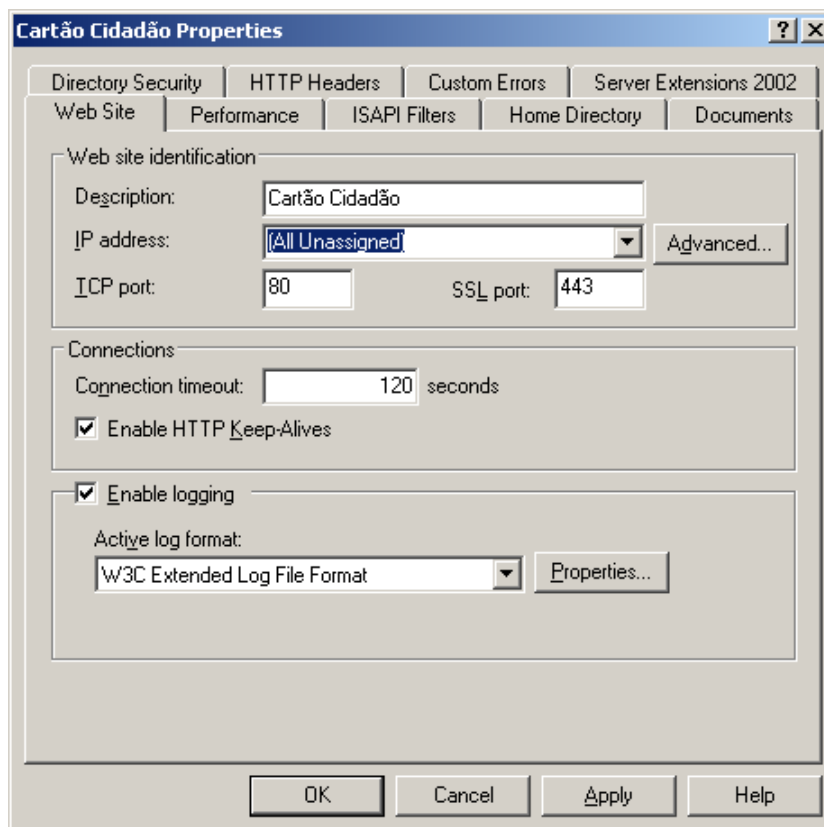
Como complemento dos serviços a implementar, sugere-se a promoção da criação de “áreas reservadas” com acesso a diversos serviços orientados ao “cliente”, seja ele “aluno”, “encarregado de educação”, “contribuinte”, “beneficiário”, “segurado”, entre outros.

3. Configurações Servidor

3.1. Exemplo de Configuração com IIS

Para se poder efectuar autenticação com o Cartão de Cidadão e uma vez que os certificados clientes só se encontram disponíveis em comunicações por **SSL**, é necessário ter um certificado instalado no servidor para o *web site* e definir um porto para **SSL** (valor *default* 443). Esta configuração é genérica para todos os sites que queiram usar ligações seguras.

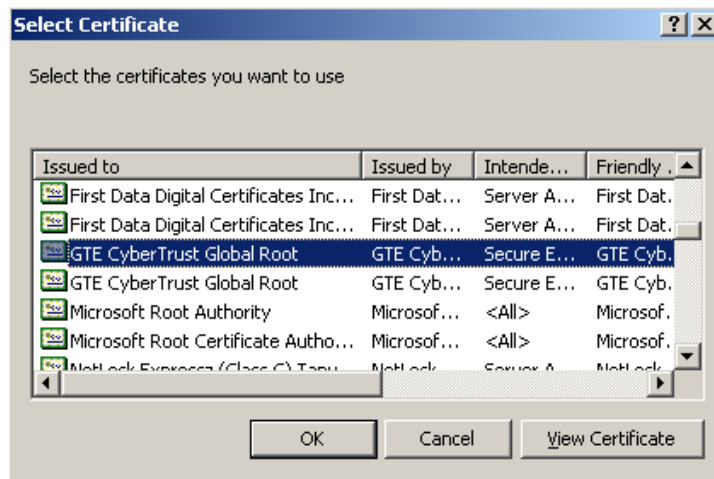
Para a autenticação, deve ser configurado o *IIS* de modo a aceitar os certificados clientes específicos.



Para tal aceder às propriedades do *web site* onde queremos efectuar a autenticação:

1. Seleccionar a *Tab Directory Security*;
2. Seleccionar *Secure Communications* → *Edit*;
3. Seleccionar a opção *Enable Certificate Trust List* → *New*;
4. Seguir as instruções do *Wizard* até chegar à página ilustrada na figura seguinte;
5. Seleccionar a opção *Add From Store*;

- Escolher o certificado *GTE CyberTrust Global Root* presente na *Location Trusted Root Certification Authorities*;

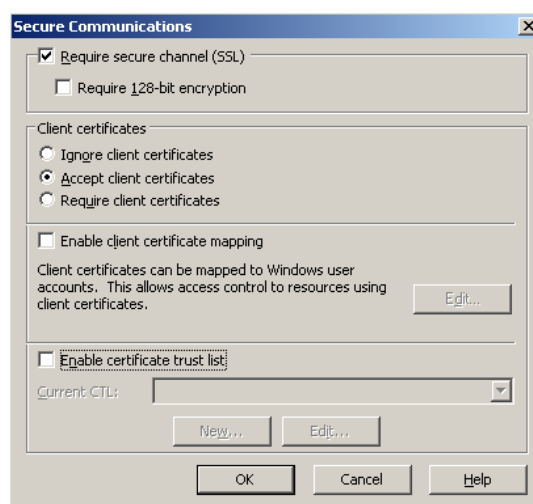


- Prosseguir o *Wizard* até ao final.

Com esta configuração, o *IIS* passará a aceitar os certificados clientes presentes no Cartão de Cidadão. Esta configuração tem de ser efectuada ao nível do *web site*.

De modo a requerer que o cidadão use o seu certificado em determinada página, pasta ou *web site*, terá de se fazer a seguinte configuração:

- Aceder às propriedades da **página, pasta ou web site** onde queremos efectuar a autenticação;
- Seleccionar a *Tab Directory Security*;
- Seleccionar *Secure Communications* → *Edit*;
- Seleccionar as opções *Require Secure Channel* e *Accept Client Certificates*.



3.2. Instalação da root dos certificados

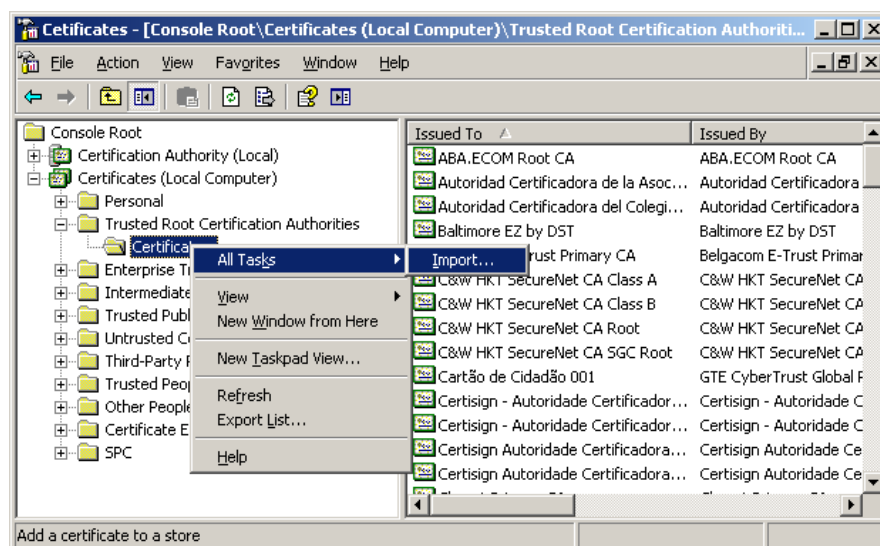
De modo a ser validada a totalidade da *path* do certificado presente no Cartão de Cidadão, é necessário adicionar à *Trusted Root Certification Authorities* os dois certificados seguintes.



(Os certificados estão disponíveis on-line em www.cartaodecidadao.pt junto a este Manual)

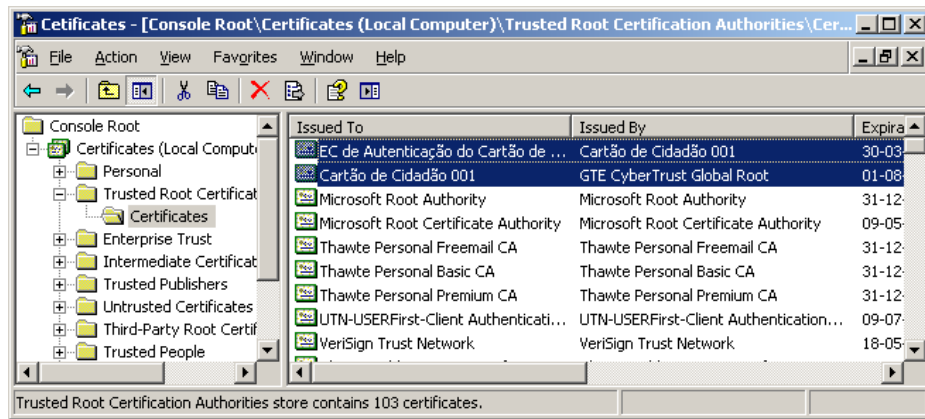
Para efectuar a adição dos certificados:

1. Abrir a consola de certificados (*Local Computer*);
2. Navegar pela árvore até *Trusted Root Certification Authorities* → *Certificates*;



3. Seleccionar com o botão do lado direito do rato e escolher a opção *All Tasks* → *Import*;
4. Seguir as instruções do *Wizard*, seleccionando o certificado **CCROOT_0001_CERT.cer**;
5. Continuar o *Wizard* até ao final deixando as opções *default* seleccionadas;
6. Repetir os passos 3 a 5 com o certificado **AUC_0001_CERT.cer**.

No final serão visíveis os dois certificados importados.



4. Referências

Neste capítulo apresentam-se algumas referências sobre o tema em análise:

- IIS and client certificates - <http://support.microsoft.com/kb/907274>
- Building Secure ASP.NET Applications Authentication, Authorization, and Secure Communication - <http://msdn2.microsoft.com/en-us/library/aa302412.aspx>
- CertCheckMode Metabase Property (IIS 6.0) - <http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/ISS/0c08d268-1634-4486-8382-b735e295b3aa.mspx?mfr=true>
- HttpRequest.ClientCertificate Property (System.Web) - <http://msdn2.microsoft.com/en-us/library/system.web.httprequest.clientcertificate.aspx>
- You receive a "403.13 client certificate revoked" error message when you connect to a computer that is running Windows Server 2003 and Internet Information Services 6.0 - <http://support.microsoft.com/kb/884115>
- AKAAS ASP.NET Tutorial - Security - <http://www.akaas.net/asp-net-tutorial/Chap-19.htm>
- HOW TO Secure an ASP.NET Application Using Client-Side Certificates - <http://support.microsoft.com/kb/315588>