

Projecto Cartão de Cidadão

Configuração Windows Logon

Versão 1.0

Fevereiro de 2011

ÍNDICE

1	INTRODUÇÃO	3
2	CERTIFICADOS	4
3	SERVIDOR - WINDOWS SERVER 2008	5
3.1	ALTERAÇÃO DO REGISTER.....	5
3.2	ALTERAÇÃO MANAGES CERTIFICATES IN SECURITY.....	5
3.3	ALTERAÇÃO NA PKI TOOL.....	6
3.4	ALTERAÇÃO NA ACTIVE DIRECTORY USERS.....	7
4	CLIENTE - WINDOWS 7	8
4.1	ALTERAÇÃO DO REGISTER.....	8
4.2	ALTERAÇÃO MANAGES CERTIFICATES IN SECURITY.....	8

1 Introdução

Este presente documento tem como objectivo descrever a configuração do 'Windows Logon' no servidor e no cliente.

Os sistemas operativos utilizados, no servidor e no cliente foram o Windows server 2008 e o Windows 7, respectivamente.

2 Certificados

Ao longo da configuração serão necessários os seguintes certificados:

- GTE CyberTrust Global Root;
- Certificado da entidade de certificação - ECRaizEstado
(https://pki.cartaodecidadao.pt/publico/certificado/cc_ec_cidadao/);
- Certificado da entidade de certificação de assinatura digital qualificada
(https://pki.cartaodecidadao.pt/publico/certificado/cc_ec_cidadao_assinatura/);
- Certificado de autenticação do utilizador.

3 Servidor –Windows Server 2008

3.1 Alteração do Register

Criar as seguintes *keys* e os respectivos *DWORD Value*:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider

AllowCertificatesWithNoEKU = dword:1

AllowSignatureOnlyKeys = dword:1

ForceReadingAllCertificates = dword:1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

UseCachedCRLOnlyAndIgnoreRevocationUnknowErrors = dword:1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kdc

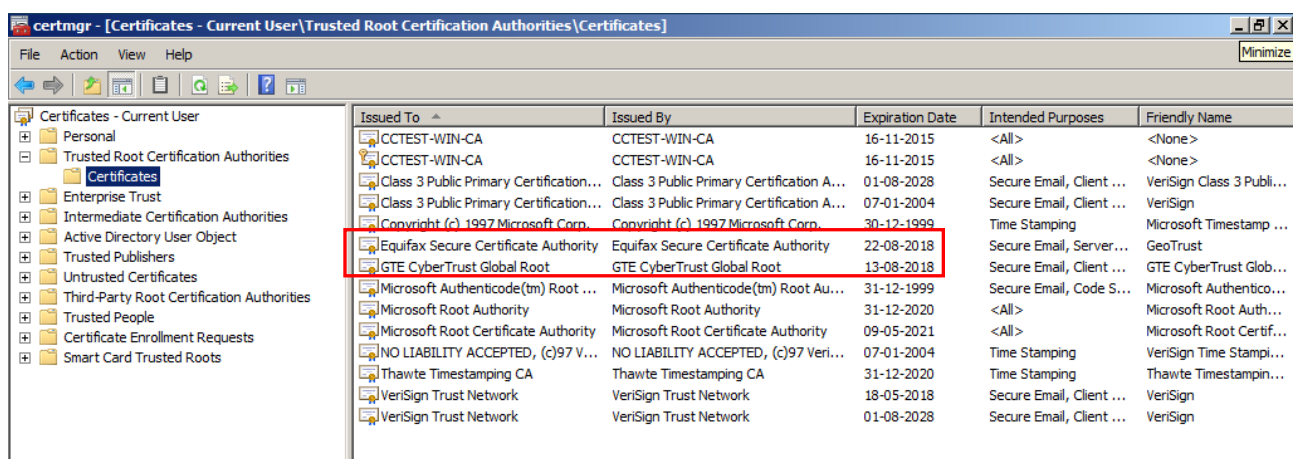
UseCachedCRLOnlyAndIgnoreRevocationUnknowErrors = dword:1

SCLogonEKUNotRequired = dword:1

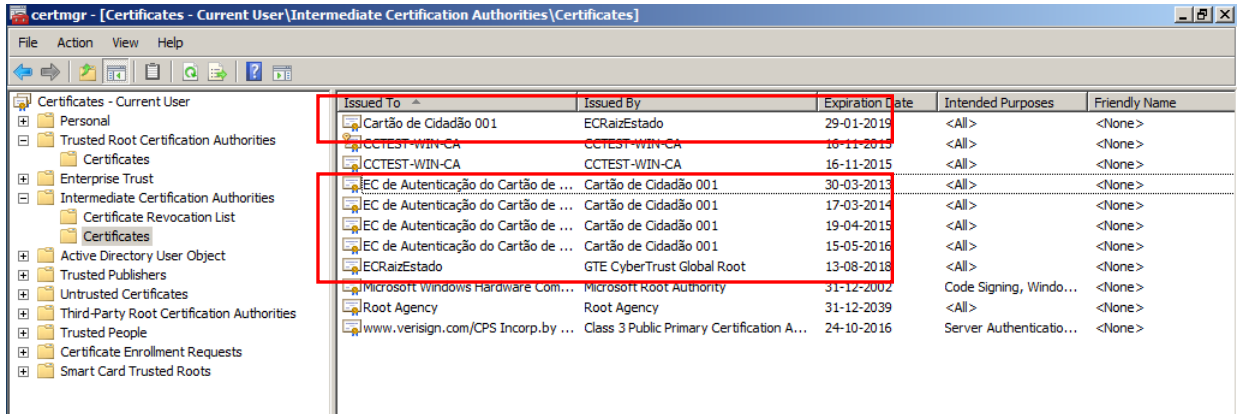
3.2 Alteração Manages certificates in security

→ Abrir a consola **certmgr.msc**;

→ Verificar a existência do certificado GTE CyberTrust Global Root em **'Trusted Root Certification Authorities\Certificates'**, como ilustra a imagem seguinte:

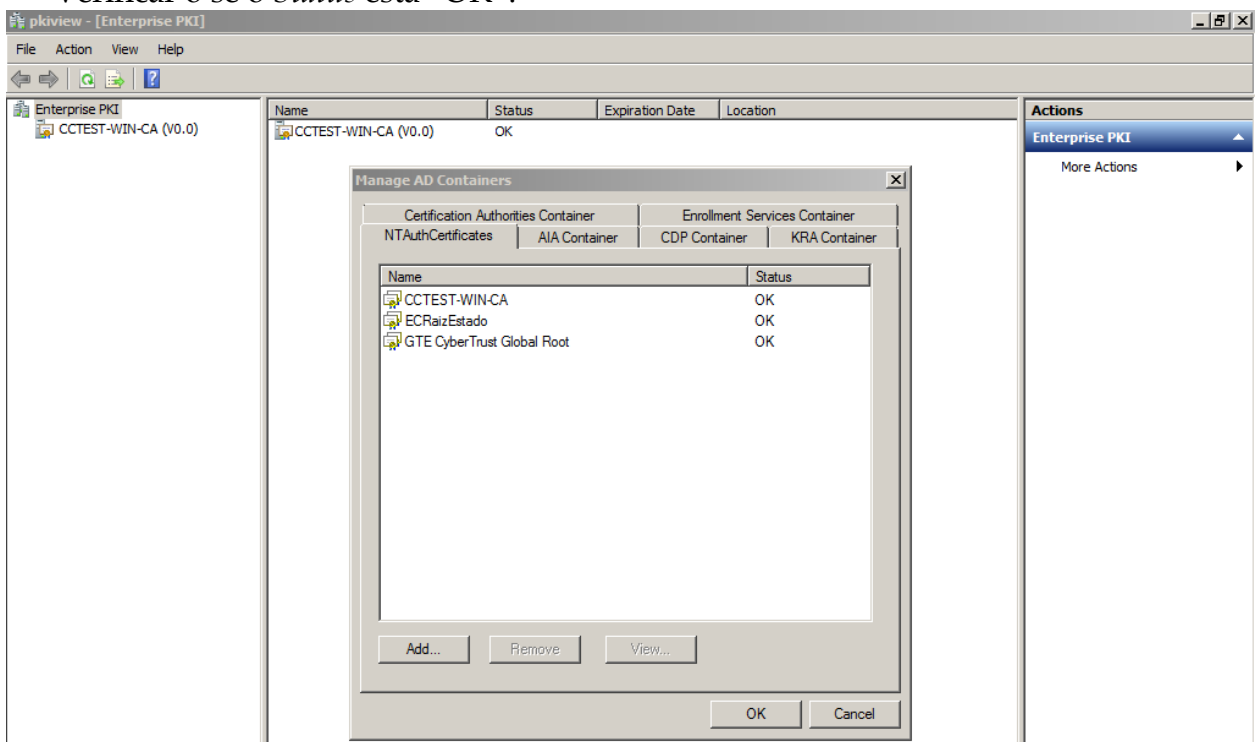


- ➔ Colocar o certificado ECRaizEstado e os certificados de EC de autenticação em 'Intermediate Certification Authorities\Certificates':



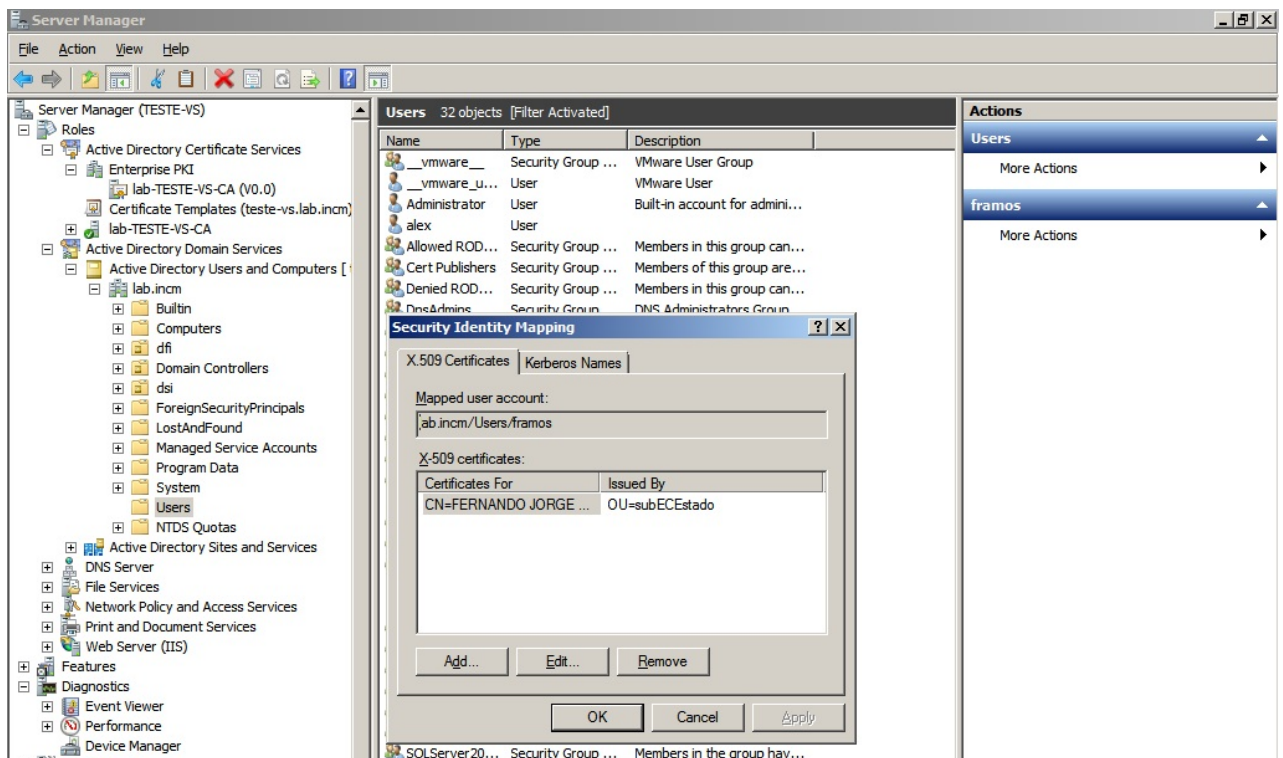
3.3 Alteração na PKI Tool

- ➔ Abrir a consola `pkiview.msc`;
- ➔ Utilizar **Manage AD Containers** (clicar com o botão direito do rato);
- ➔ Colocar os certificados GTE e o ECRaizEstado em 'NTAuthCertificates'.
Verificar o se o *Status* está "OK":



3.4 Alteração na Active Directory Users

- ➔ Exportar o certificado de autenticação através do MW;
- ➔ Adicionar o certificado de autenticação (ponto anterior) associado ao utilizador criado na *Active Directory\Users*, clicando do lado direito do rato e em 'Name Mappings':



4 Cliente -Windows 7

4.1 Alteração do Register

Criar as seguintes *keys* e os respectivos *DWORD Value*:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider

AllowCertificatesWithNoEKU = dword:1

AllowSignatureOnlyKeys = dword:1

ForceReadingAllCertificates = dword:1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

UseCachedCRLOnlyAndIgnoreRevocationUnknowErrors = dword:1

CRLTimeoutPeriod = dword:1

4.2 Alteração Manages certificates in security

Executar no cliente, os mesmos passos do [capítulo 3.2](#).