

RE: Problems enabling smart card login on windows 2000

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-07/1089.html>

From: Kenny Wood (Kenwood_at_online.microsoft.com)

Date: 07/26/04

Date: Mon, 26 Jul 2004 01:55:33 GMT

Hello Matthias,

From: <http://www.microsoft.com/technet/itsolutions/migration/unix/usecdirw/appwsdsu.msp>

KDC_ERR_CLIENT_NOT_TRUSTED translates to "the client trust failed or is not implemented"

Unfortunately this could be many things;

Bad Certificate;

Invalid Schannel;

Something wrong with computer domain membership;

OID – Smart Card Logon (1.3.6.1.4.1.311.20.2.2) – not in certificate as valid policy or key usage;

Here is some more information that might help.

TechNet Information on Smart Cards

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smrtcard/default.asp>

Smart Card Logon Whitepaper

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/sclogon.asp>

Troubleshooting Windows 2000 PKI Deployment and Smart Card Logon

<http://www.microsoft.com/windows2000/techinfo/administration/security/smrtcrdtr.asp>

The SmartCard Deployment Cookbook

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smrtcard/default.asp>

Q281245 Enabling Smart Card Logon with Third-Party CAs

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q281245>

Thank you for your post.

Kenny Wood
CISSP, MCSE (+S, +M)
PSS Security
Microsoft Corporation

--
This posting is provided "AS IS" with no warranties, and confers no rights. Use of included script samples are subject to the terms specified at <http://www.microsoft.com/info/copyright.htm>
Note: For the benefit of the community-at-large, all responses to this message are best directed to the newsgroup/thread from which they originated.

| Thread-Topic: Problems enabling smart card login on windows 2000
| thread-index: AcRucGEcCMgpgRs6R8aQQIGASrhYUA==
| X-WBNR-Posting-Host: 212.19.59.234
| From: "=?Utf-8?B?TWF0dGhpYXM=?" <Matthias@discussions.microsoft.com>
| Subject: Problems enabling smart card login on windows 2000
| Date: Tue, 20 Jul 2004 08:44:01 -0700
| Lines: 60
| Message-ID: <43893C8B-CD26-4A01-A9BE-B9783B76E36F@microsoft.com>
| MIME-Version: 1.0
| Content-Type: text/plain;
| charset="Utf-8"
| Content-Transfer-Encoding: 7bit
| X-Newsreader: Microsoft CDO for Windows 2000
| Content-Class: urn:content-classes:message
| Importance: normal
| Priority: normal
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.0
| Newsgroups: microsoft.public.win2000.security
| NNTP-Posting-Host: TK2MSFTNGXA03.phx.gbl 127.0.0.1
| Path: cpmsftngxa06.phx.gbl!TK2MSFTNGXA01.phx.gbl!TK2MSFTNGXA03.phx.gbl
| Xref: cpmsftngxa06.phx.gbl microsoft.public.win2000.security:29818
| X-Tomcat-NG: microsoft.public.win2000.security

| After installing a windows 2000 server and a windows 2000 professional system from scratch following the numerous step-by-step guides and How Tos - such as
| - Installing a Windows 2000 Server as a Domain Controller
| - Installing a Windows 2000 Professional Workstation and Connecting It to a Domain
| - Managing the Active Directory
| - Setting up a Certificate Authority
| - Advanced Certificate Management
| - End User Certificate Management
| - Setting Up Certification Authority Trust for a Domain
| - Installing and Using a Smart Card Reader
| - Publish a Certificate Revocation List in Windows 2000
| - ...

| ...we still have problems with smart card login!

| Among others the server is running the following services
| - Active Directory
| - Certificate Services (with enterprise root CA)
| - DNS server
| - IIS with certificate service web pages
| - Kerberos Key Distribution
| - Smart Card

| We initialized our smart card for a test user.
| The smart card contains the key pair and the corresponding certificate issued by the enterprise CA installed on the server.

microsoft.public.win2000.security: RE: Problems enabling smart card login on windows 2000

| Trying to login with inserting the card and entering the PIN (the card reader's LED indicates activity) we finally get this message:

| "The system could not log you on. Your credentials could not be verified."

| as described in

| <http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/smrtcard.mspx>

| The causes noted there ("domain controller unavailable" or "invalid CRL") seems not to be the answer, since we get the same error trying to log in into the server (=domain controller =CA, =Active Directory)!

| Enabling kerberos auditing there is the following error in the system log:

| The function LogonUser received a Kerberos Error Message:

| on logon session huber@unknown.local

| Client Time:

| Server Time: 14:12:38.0000 7/20/2004 (null)

| Error Code: 0x3e KDC_ERR_CLIENT_NOT_TRUSTED

| Client Realm:

| Client Name:

| Server Realm: UNKNOWN.LOCAL

| Server Name: krbtgt/UNKNOWN.LOCAL

| Target Name: krbtgt/UNKNOWN.LOCAL@UNKNOWN.LOCAL

| Error Text:

| File:

| Line:

| Error Data is in record data.

| 0000: 03a10530 010202

| Searching for "KDC_ERR_CLIENT_NOT_TRUSTED" (google, msdn,...) provides no results.

| Any help?!

| Thanks!

| Matthias