6.3.1

Issued To   Issued By   Expiration Date Intended Purposes   Friendly Name   Status
        Certificate Template

AddTrust External CA Root   AddTrust External CA Root   5/30/2020   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user   USERTrust

America Online Root Certification Authority 1   America Online Root Certification Authority 1
        11/19/2037   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user, IP security IKE intermediate   America Online Root Certification Authority 1

Baltimore CyberTrust Root   Baltimore CyberTrust Root   5/12/2025   Server Authentication, Secure Email, Client Authentication, Code Signing   Baltimore CyberTrust Root

Certum CA   Certum CA   6/11/2027   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, OCSP Signing   Certum

Class 2 Primary CA   Class 2 Primary CA   7/6/2019   Secure Email, Server Authentication, Client Authentication   CertPlus Class 2 Primary CA

Class 3 Public Primary Certification Authority   Class 3 Public Primary Certification Authority
        8/1/2028   Secure Email, Client Authentication, Code Signing, Server Authentication   VeriSign Class 3 Public Primary CA

Copyright (c) 1997 Microsoft Corp.   Copyright (c) 1997 Microsoft Corp.   12/30/1999   Time Stamping   Microsoft Timestamp Root

Deutsche Telekom Root CA 2   Deutsche Telekom Root CA 2   7/9/2019   Secure Email, Server Authentication, Client Authentication   Deutsche Telekom Root CA 2

DigiCert Assured ID Root CA   DigiCert Assured ID Root CA   11/9/2031   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping   DigiCert

DigiCert Global Root CA DigiCert Global Root CA 11/9/2031   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping   DigiCert

DigiCert High Assurance EV Root CA   DigiCert High Assurance EV Root CA   11/9/2031   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping   DigiCert

DT Soft Ltd   VeriSign Class 3 Code Signing 2009-2 CA 11/3/2012   Code Signing   <None>

Entrust Root Certification Authority   Entrust Root Certification Authority   11/27/2026   Server Authentication, Client Authentication, Code Signing, Secure Email, IP security tunnel termination, IP security user, IP security IKE intermediate, Time Stamping, Encrypting File System   Entrust

Entrust.net Certification Authority (2048)   Entrust.net Certification Authority (2048)
        7/24/2029   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security userEntrust (2048)

Entrust.net Secure Server Certification Authority	Entrust.net Secure Server Certification Authority	5/25/2019	Server Authentication, Client Authentication, Code Signing, Secure Email, IP security tunnel termination, IP security user, IP security IKE intermediate, Time Stamping, Encrypting File System	Entrust

Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Server Authentication, Code Signing	GeoTrust

GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping	GeoTrust Global CA

GlobalSign	GlobalSign	12/15/2021	Server Authentication, Client Authentication, Code Signing, Secure Email, Time Stamping, OCSP Signing, Encrypting File System, IP security tunnel termination, IP security user, IP security IKE intermediate	GlobalSign

GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authentication, Client Authentication, Code Signing, Secure Email, Time Stamping, OCSP Signing, Encrypting File System, IP security tunnel termination, IP security user, IP security IKE intermediate	GlobalSign

Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Authority	6/29/2034	Server Authentication, Client Authentication, Secure Email, Code Signing	Go Daddy Class 2 Certification Authority

Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	12/31/2037	Server Authentication, Client Authentication, Code Signing, Secure Email, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user	Go Daddy Root Certificate Authority – G2

GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client Authentication, Server Authentication, Code Signing	GTE CyberTrust Global Root

http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, Server Authentication	Starfield Technologies

Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Authority	12/31/1999	Secure Email, Code Signing	Microsoft Authenticode(tm) Root

Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Authority

Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certificate Authority

Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Authority 2010	6/23/2035	<All>	Microsoft Root Certificate Authority 2010

Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Authority 2010	6/23/2035	<All>	Microsoft Root Certificate Authority 2010

Microsoft Root Certificate Authority 2011	Microsoft Root Certificate Authority 2011	3/22/2036	<All>	Microsoft Root Certificate Authority 2011

Microsoft Root Certificate Authority 2011   Microsoft Root Certificate Authority 2011
        3/22/2036   <All>   Microsoft Root Certificate Authority 2011

NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.   NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
        1/7/2004   Time Stamping VeriSign Time Stamping CA

SecureTrust CA SecureTrust CA 12/31/2029   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping   Trustwave   CA

Starfield Class 2 Certification Authority Starfield Class 2 Certification Authority 6/29/2034   Server Authentication, Client Authentication, Secure Email, Code Signing   Starfield Class 2 Certification Authority

Starfield Root Certificate Authority - G2 Starfield Root Certificate Authority - G2 12/31/2037   Server Authentication, Client Authentication, Code Signing, Secure Email, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user   Starfield Root Certificate Authority – G2

Starfield Services Root Certificate Authority   Starfield Services Root Certificate Authority
        12/31/2029   Server Authentication, Client Authentication, Code Signing, Secure Email, Time Stamping, OCSP Signing, Encrypting File System, IP security tunnel termination, IP security user, IP security IKE intermediate   Starfield Technologies Inc.

StartCom Certification Authority   StartCom Certification Authority   9/17/2036   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user   StartCom Certification Authority

StartCom Certification Authority G2   StartCom Certification Authority G2   12/31/2039   Server Authentication, Client Authentication, Secure Email, Code Signing   StartCom Certification Authority G2

Thawte Premium Server CA   Thawte Premium Server CA   12/31/2020   Server Authentication, Code Signing   thawte

thawte Primary Root CAthawte Primary Root CA7/16/2036   Server Authentication, Client Authentication, Secure Email, Code Signing   thawte

Thawte Server CA   Thawte Server CA   12/31/2020   Server Authentication, Code Signing   thawte

Thawte Timestamping CA   Thawte Timestamping CA   12/31/2020   Time Stamping Thawte Timestamping CA

UTN - DATACorp SGC   UTN - DATACorp SGC   6/24/2019   Server Authentication   USERTrust

UTN-USERFirst-Hardware   UTN-USERFirst-Hardware   7/9/2019   IP security user, IP security tunnel termination, Server Authentication   USERTrust

UTN-USERFirst-Object   UTN-USERFirst-Object 7/9/2019   Encrypting File System, Time Stamping, Code Signing   USERTrust

VeriSign Class 3 Public Primary Certification Authority - G3   VeriSign Class 3 Public Primary Certification Authority - G3   7/16/2036   Code Signing, Server Authentication, Client Authentication, Secure Email   VeriSign

VeriSign Class 3 Public Primary Certification Authority - G4   VeriSign Class 3 Public Primary Certification Authority - G4   1/18/2038   Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping   VeriSign Class 3 Public Primary Certification Authority - G4

VeriSign Class 3 Public Primary Certification Authority - G5   VeriSign Class 3 Public Primary Certification Authority - G5   7/16/2036   Server Authentication, Client Authentication, Secure Email, Code Signing   VeriSign

VeriSign Commercial Software Publishers CA   VeriSign Commercial Software Publishers CA   1/7/2004   Secure Email, Code Signing   VeriSign

VeriSign Trust Network   VeriSign Trust Network   8/1/2028   Secure Email, Client Authentication, Code Signing, Server Authentication   VeriSign

6.3.2

Removing Digital Certificates

When a digital certificate is removed, any e-mail that is encrypted with the associated digital ID is no longer readable. This includes e-mail that you received before you removed the digital certificate, as well as e-mail you receive after you remove the digital certificate. The e-mail is encrypted using your public key, and because the digital certificate has been removed, you no longer have the private key needed to decrypt it. To read this e-mail again, you must import the digital certificate back into Internet Explorer, and then enabled it in Outlook Express. There is no method of exporting encrypted e-mail to an unencrypted format. If you receive any encrypted mail that you must be able to access, make sure you have successfully exported the digital certificate before you remove it. You may also be unable to view any Web sites that require client authentication based on that digital certificate until you either import it again, or generate another digital certificate to use for that Web site.

For these reasons, Microsoft does not recommend removing digital certificates. You should keep the current digital certificate and obtain a new one for a new e-mail account or Web site that requires one. However, if this is not possible, and a digital certificate must be removed due to incorrect operation or for troubleshooting purposes, follow these steps:

WARNING: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe. Note that you should back up the registry before you edit it.

Delete all the folders under the following registry key, and then restart your computer:
`HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\My\Certificates`

When you remove the digital certificate from Internet Explorer, the associated digital ID is removed from Outlook Express.

Importing Digital Certificates

To import digital certificates that you previously exported, follow these steps:

1. Click Start, point to Settings, click Control Panel, and then double- click Internet.
2. On the Content tab, click Personal, and then click Import.
3. In the Password box, type your password.

   NOTE: You may be prompted multiple times for your password.
4. In the Certificate File To Import box, type the filename of the certificate you want to import, and then click OK.
5. Click Close, and then click OK.

Source: http://support.microsoft.com/en-us/kb/179380