MasterCard Internet Gateway Service (MiGS) Notification of Changed SSL Certificates – Additional Information

Issued: March 2015

Introduction

On 25th February 2015 a notification was sent to MiGS customers advising of an upcoming hardware upgrade, and an associated change to the SSL Certificates which will be installed in the MiGS Production and Disaster Recovery (DR) sites.

The purpose of this notification is to provide customers with additional information as a guideline to assist with updating their systems.

Customers are advised that the new certificates are currently in place in the MiGS MTF (test) environment.

Date of Change

Production: The change is effective **Tuesday, 28th April 2015**

Microsoft Browser Certificate Trust Store Update

Although Windows XP, Windows Server 2003, and Windows Vista browsers automatically check the list of trusted CAs on the Windows Update Web site, some user browsers may not update

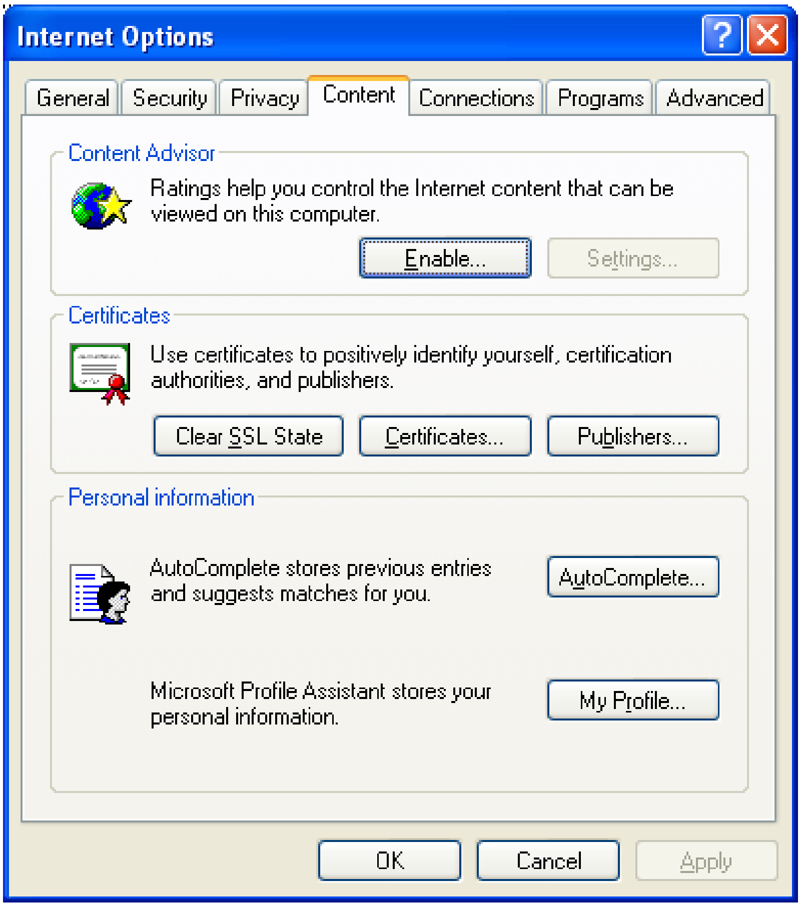
If your Internet Explorer displays a SSL warning when you try to connect to MiGS URL, please read the following and perform the steps as indicated:

MasterCard has supplied the following files for certificate upgrades/imports:

- Entrust_Chain.zip containing
  - Entrust_root.cer
  - Entrust_G2.cer
  - Entrust_L1K.cer
- Entrust_Full_Chain.p7b
- MTFTrustChain.pem

The certificates in each file are identical, but encoded in different formats. You will only need one of the files to complete your upgrade. You will need to unzip the archive to access the individual certificates.

1. Open the IE browser, select Tools\Internet Options and click on **Certificates** within the Content tab:



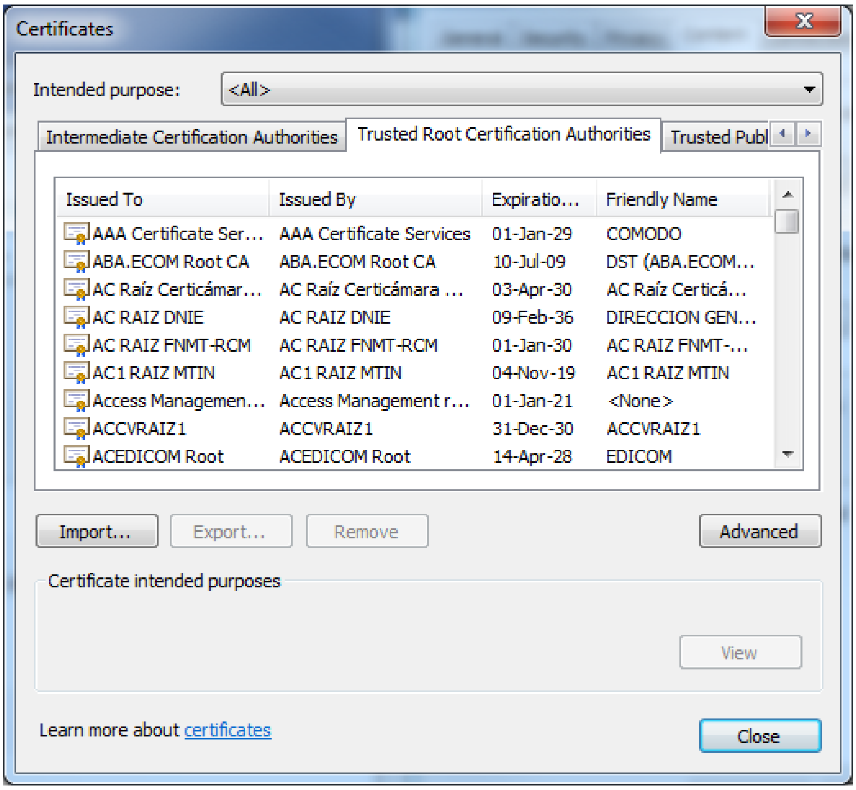
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

2. Click on the '**Trusted Root Certification Authorities**' tab to see the list of trusted certificates from a variety of certificate authorities that Microsoft trusts.

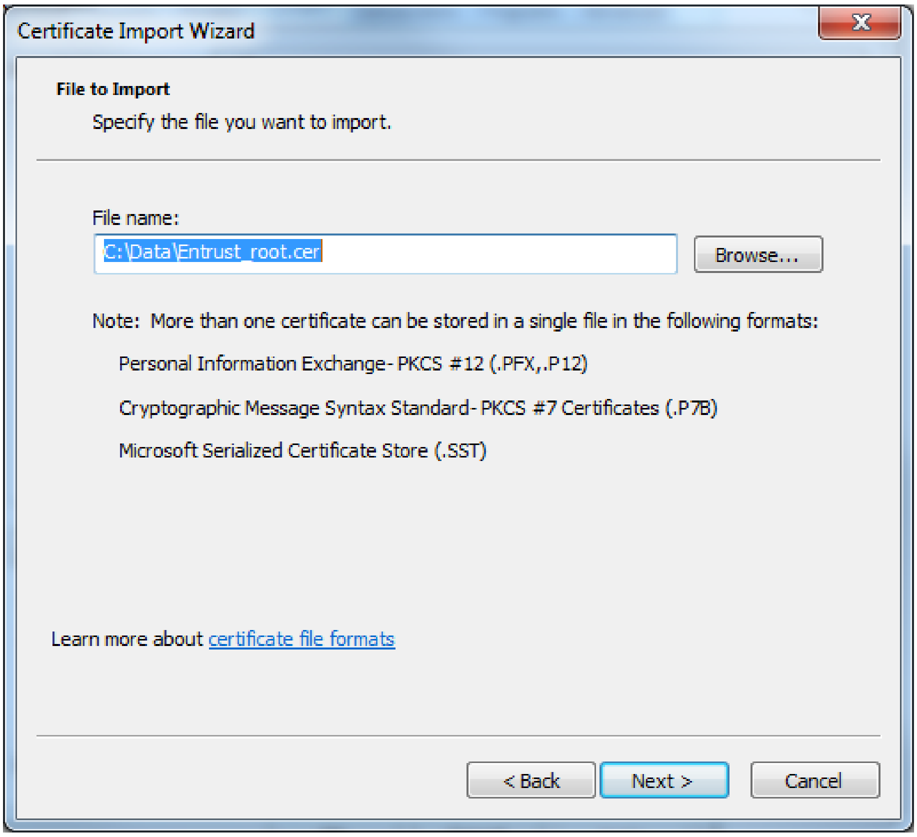

Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	01-Jan-29	COMODO
ABA.ECOM Root CA	ABA.ECOM Root CA	10-Jul-09	DST (ABA.ECOM...
AC Raíz Certicámar...	AC Raíz Certicámara ...	03-Apr-30	AC Raíz Certicá...
AC RAIZ DNIE	AC RAIZ DNIE	09-Feb-36	DIRECCION GEN...
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01-Jan-30	AC RAIZ FNMT-...
AC1 RAIZ MTIN	AC1 RAIZ MTIN	04-Nov-19	AC1 RAIZ MTIN
Access Managemen...	Access Management r...	01-Jan-21	<None>
ACCVRAIZ1	ACCVRAIZ1	31-Dec-30	ACCVRAIZ1
ACEDICOM Root	ACEDICOM Root	14-Apr-28	EDICOM

Learn more about certificates

3. Click ‘Import’, then select the new certificate or .pem file. MasterCard has supplied both individual certificate files (in a zip archive), and .pem and .r7b (trust chain) files. You can also retrieve your own Entrust root certificates from their website.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Data\Entrust_root.cer

Note: More than one certificate can be stored in a single file in the following formats:

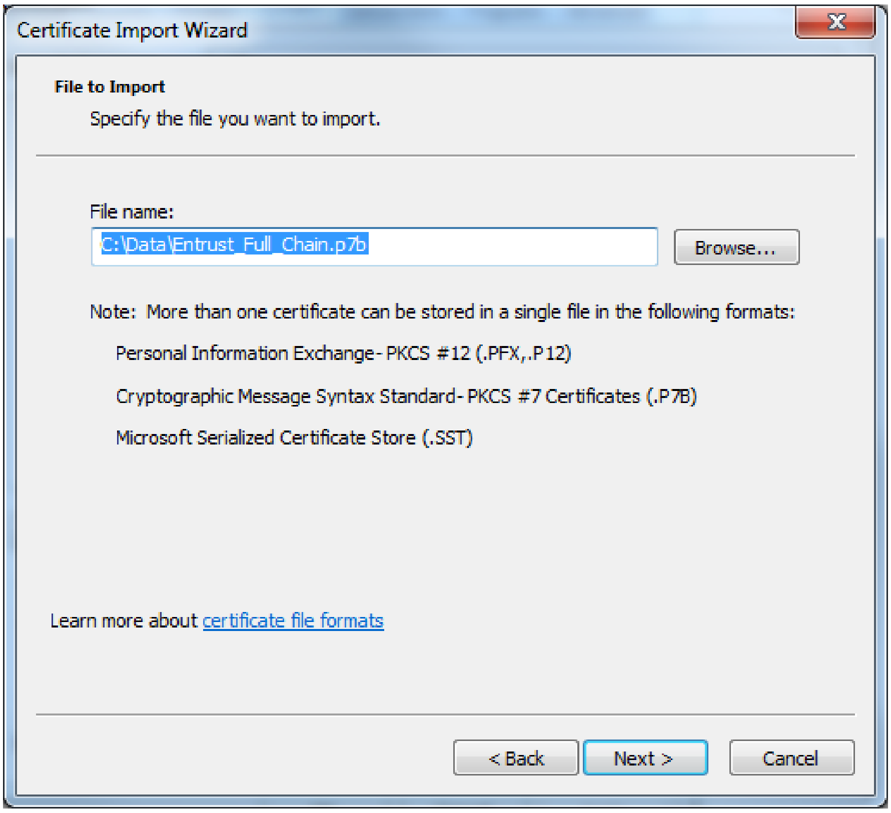
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Alternatively, importing in a single file format:



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Data\Entrust_Full_Chain.p7b

Note: More than one certificate can be stored in a single file in the following formats:

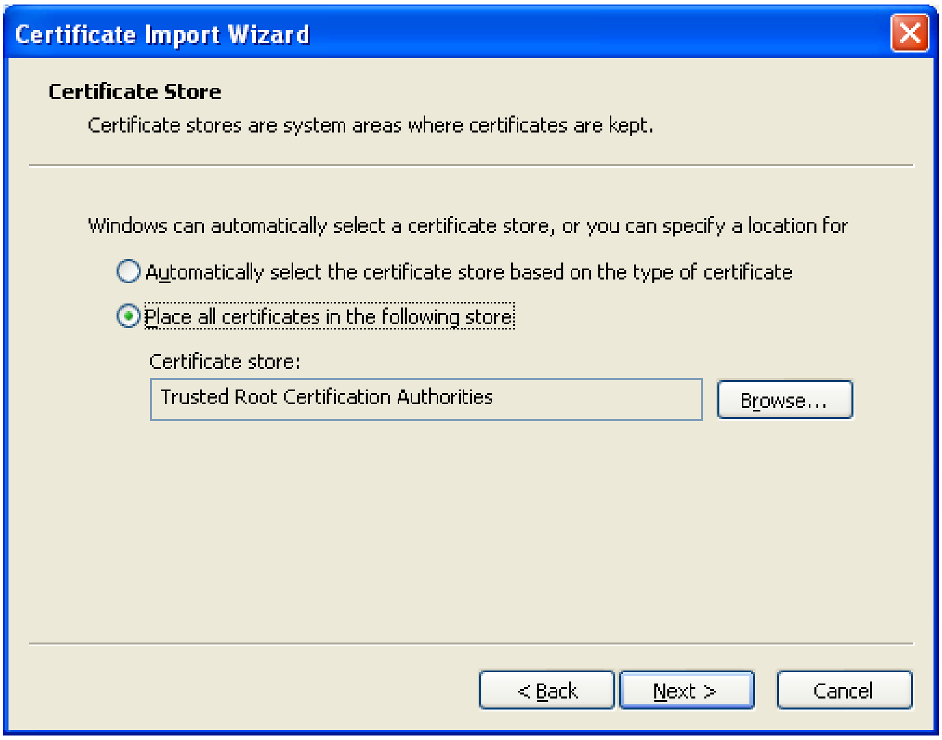
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

4. Then select ‘Place all certificates in the following store’ as Trusted Root Cert.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

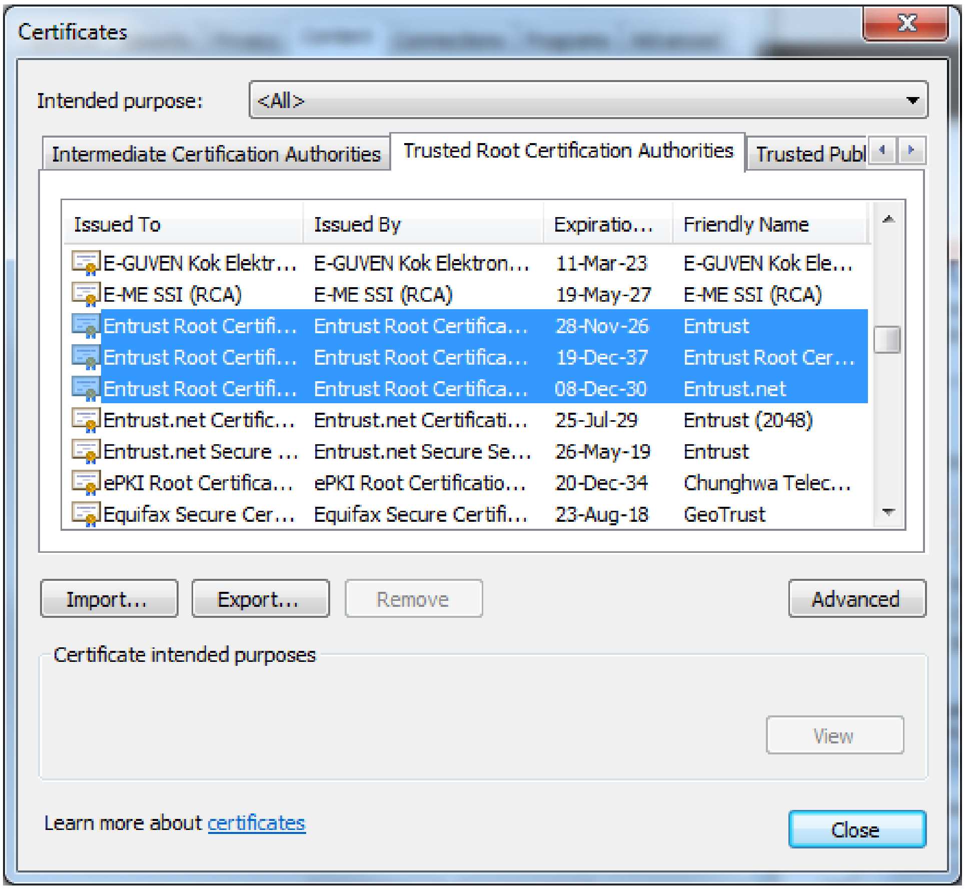
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

5. Then click through all the ‘next’ to complete the import.

After above steps are successfully completed for the full chain file, or individual files, you should be able to see the ‘**Entrust Root Certification Authority**’ is in the Trusted Root Certification Authorities list, along with the rest of the chain. Individual certificates can be inspected with the **View** button:



Certificates

Intended purpose: <All>

Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ

Issued To	Issued By	Expiratio...	Friendly Name
E-GUVEN Kok Elektr...	E-GUVEN Kok Elektron...	11-Mar-23	E-GUVEN Kok Ele...
E-ME SSI (RCA)	E-ME SSI (RCA)	19-May-27	E-ME SSI (RCA)
Entrust Root Certifi...	Entrust Root Certifica...	28-Nov-26	Entrust
Entrust Root Certifi...	Entrust Root Certifica...	19-Dec-37	Entrust Root Cer...
Entrust Root Certifi...	Entrust Root Certifica...	08-Dec-30	Entrust.net
Entrust.net Certific...	Entrust.net Certificati...	25-Jul-29	Entrust (2048)
Entrust.net Secure ...	Entrust.net Secure Se...	26-May-19	Entrust
ePKI Root Certifica...	ePKI Root Certificatio...	20-Dec-34	Chunghwa Telec...
Equifax Secure Cer...	Equifax Secure Certifi...	23-Aug-18	GeoTrust

Certificate intended purposes

Learn more about certificates