New Certificate Authority (CA) Certificates

Updated on Thursday, March 1, 2018.

Action may be required before mid-April 2018. IBM recommends you obtain and install both the DigiCert root CA certificates listed below before April, if you have not already done so.

What to do

To obtain and add the DigiCert CA certificates to your z/OS security manager database, perform the following steps:

1. Download the DigiCert CA certificate files to your workstation. Depending on which servers you use, two might be required. IBM recommends you obtain and install both:

    a. The first one, the "DigiCert Global Root CA" certificate, which will be needed for the testcase server, is available from https://www.digicert.com/CACerts/DigiCertGlobalRootCA.crt. For your reference, the certificate has this serial number: 083BE056904246B1A1756AC95991C74A.
    b. The second, "DigiCert Global Root G2" certificate, which will be needed for the Blue Diamond and ecurep servers, is available at https://www.digicert.com/CACerts/DigiCertGlobalRootG2.crt, and its serial number is: 033AF1E6A711A9A0BB2864B11D09FAE5.

    If you have trouble downloading the files directly using the links above, depending on how you are viewing this document, you may be able to right-click each link above, then use "Save Link As…" to download the file to your workstation. Or, go to https://www.digicert.com/digicert-root-certificates.htm, find the certificates in the list of Root Certificates, right-click on the "Download" link for each one, and then use "Save Link As…" to download each file to your workstation.

2. Upload the certificate files to your z/OS system. You can use FTP or another method, but be sure the files are uploaded in binary format and stored in sequential data sets with RECFM=VB and LRECL>=256.

3. After you have stored the certificates in sequential data sets, add each to your security manager database. If you are using RACF, then you can use the following commands:

    ```
    RACDCERT CERTAUTH ADD('ca-cert.dataset.name.CA') +
    WITHLABEL('DigiCert Global Root CA') TRUST

    RACDCERT CERTAUTH ADD('ca-cert.dataset.name.G2') +
    WITHLABEL('DigiCert Global Root G2') TRUST
    ```

© Copyright 2018, IBM Corporation

Where ca-cert.dataset.name.CA and ca-cert.dataset.name.G2 are the names of the sequential data sets you uploaded.

4. To use the CA certificates, you must add them to the keyrings used by client programs that will require these certificates for server authentication. (For example, you can add them to the keyring in RACF used by SMP/E for RECEIVE ORDER.)

Important Note: Do NOT delete the current GeoTrust Global CA certificate from your z/OS security management data base, or from the keyrings you use for accessing these servers, until after all the IBM servers have been updated to use new server and CA certificates, and all other servers you rely on have replaced their GeoTrust authenticated certificates.

Why do I need to do this?

There are several IBM servers which provide support for a number of functions, including ordering and downloading z/OS software products and service. These servers use Secure Sockets Layer (SSL) technology to encrypt communications between client and server applications. To enable SSL to be used, servers identify themselves using x.509 certificates, and trusted certificate authority (CA) certificates are used to authenticate the servers.

The server certificates and some of the certificate authority (CA) certificates used by the IBM servers are expiring and must be replaced. The current and expiring certificates are authenticated using the GeoTrust Global CA certificate. Those that expired in January 2018 have been replaced by certificates that also are authenticated using the same GeoTrust Global CA certificate.

Google and Mozilla have announced plans to stop trusting servers using a GeoTrust CA certificate in the Chrome and Firefox browsers later in 2018.

More details

Server	Use	Certificate expiration date	Planned replacement date	More information
eccgw02.rochester.ibm.com	Used by SMP/E RECEIVE ORDER to submit requests for PTFs and HOLDDATA.	March 12, 2019	TBD	
eccgw01.boulder.ibm.com		March 12, 2019	TBD	
www.secure.ecurep.ibm.com	Upload diagnostic data to IBM.	May 1, 2018	Mid-April 2018	See the eucrep home page, which will be updated as needed.

testcase.boulder.ibm.com	Upload diagnostic data to IBM, and download test fixes from IBM.	May 29, 2018	TBD	
msciftpgw.im-ies.ibm.com (Blue Diamond FTPS server)	Upload diagnostic data to IBM.	After 2018	March 2018	See the planned e-mail from the Blue Diamond team. Also, you can test browser-based access using: https://msciftptest.im-ies.ibm.com/
deliverycb-bld.dhe.ibm.com	Download z/OS software products, PTFs, and HOLDDATA requested by SMP/E RECEIVE ORDER and by Shopz.	After 2018	August 2018	
deliverycb-mul.dhe.ibm.com		After 2018	August 2018	