Certification Authority (CA) GT50 2020.07

Root Certificate Authority download and utilization

author	Umberto Rustichelli
date	21/07/2020 Version 1.0
addressees	GT50 web site Users; Lambda Service Integrators
filename	[GT50-20-iCA] T REL CA Root Certificate GT50 notes [1.0]

INTRODUCTION

This is the public key of our Certification Authority (CA).

A Certification Authority is an entity that issues digital certificates to people or other servers. Digital certificates allow to keep communications secure (not interceptable by third parties) and to grant identity of the other part you're exchanging information with.

In a client-server scenario, you're sure to "talk" to the legit system and the information you exchange with it are protected by a cryptographic tunnel with a high level of data protection.

To allow everything to work correctly, your Internet browsers have to know the Certification Authority which has issued the certificate to the server, likewise a police officer has to know the authority which has issued an identity document.

GT50 has its own Certification Authority which is, generally, unknown to Internet browsers because it's not available in their "trust list".

This only means it isn't an "enterprise level" of Authority and can be added to this trust list manually.

Likewise you give a foreign document to a police officer, he has to check the identity of the issuer, taking information (querying their data banks).

Add Root Certificate Authority

GT50 has issued its Root Certificate Authority with this Common Name (CN):
GT50 CA 2020.07

Length of private key is 2048 bit; its validity is from 21 July 2020 to 19 July 2030.

The certificate is valid from issue date.

Now we explain how to manually add the public key of our Certification Authority to your browser.

First of all you've to download our certificate, clicking here:
http://www.gt50.org/CA/CA.GT50-202007.crt

Regardless of your browser and/or Operating System, during or after the installation process, remember to check the SHA fingerprints of this digital certificate:

SHA1=   8C FC 64 D3 69 C7 D5 DA 5F 26 23 3F 4F E1 BA 8B 72 2A BE 59

SHA256= **4C E8 26 10 82 C7 CE CB 82 A4 F3 1E CA 49 79 F7**
67 77 C3 8D DA CA 08 E9 20 4A 25 07 C7 F0 02 4F

Then, according to you Operating System, you've to follow these steps.

Microsoft OS (browser Internet Explorer / Google Chrome):

1.   double click on the certificate file you've downloaded
2.   click on button "install certificate"
3.   on next wizard windows click "Next" (go ahead)
4.   click on "browse" button to choose "Root Trusted Authority" and confirm with "OK"
5.   it appears a new window showing an alert information with "SHA1 fingerprint" of this digital certificate: trust it with "OK"
6.   the import is now completed

Microsoft OS (browser Mozilla Firefox):

1.   select "Options" in your browser toolbar
2.   select "Advanced" from the left menu
3.   select "Certificates" from the main page
4.   select "Show Certificates"
5.   select "Authorities" tab then "Import"
6.   browse to directory where you already stored the file .crt of GT50 Certification Authority then click "Open"
7.   select option "Give trust to this CA to identify web sites" and confirm with "OK"
8.   the import is now completed

Mac OSX (browser Mozilla Firefox):

1.   select "Preferences" from the Firefox menu (by default on top left of your desktop)
2.   select "Advanced" from the left menu
3.   select "Certificates" from the main page
4.   select "Show Certificates"
5.   select "Authorities" tab then "Import"
6.   browse to directory where you already stored the file .crt of GT50 Certification Authority then click "Open"
7.   select option "Give trust to this CA to identify web sites" and confirm with "OK"
8.   the import is now completed

Mac OSX (Safari):

1. double click on the certificate file you've downloaded
2. in the keystore window, double click on "GT50 CA 2020.07"
3. in "Authorize" section, choose "Always Trust" from pulldown window
4. close the window
5. confirm the operation, entering your account password
6. the import is now completed

❖❖❖