How to make new Lets Encrypt CA certificates trusted

Root cause

Old Let's Encrypt CA certificates became invalid on 30.09.2021:

https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/

All TDS certificates are already signed by new Let's Encrypt authority for 6 months approximately. Thanks to cross signing it worked until expiry 30.09.2021.

Therefore you have to make sure that all your tools trust that new CA certificates which were created in 2015 but still is not distributed everywhere.

Solutions

Issues are usually caused by outdated tools installed or Let's Encrypt certificate missing in trusted CA stores.

Windows

Importing CA certificate into Windows certificates store

1. Open your favourite Browser
2. Download new Lets's Encrypt ISRG root certificate https://letsencrypt.org/certs/isrgrootx1.pem
3. Double click on downloaded CA certificates and follow import wizard. It can look like this: http://blog.didierstevens.com/2010/10/31/quickpost-adding-certificates-to-the-certificate-store/

Updating particular tools that might use own certificates store

- Git Bash aka Git SCM
  - install the latest version https://git-scm.com/download/win
  - this usually resolves issues for Visual Studio, TortoiseGit and other tools that utilise Git Bash/SCM
- TortoiseGit
  - install latest version https://tortoisegit.org/download/
  - in case of Git Bash/SCM presence, you must update it
- SourceTree
  - install latest version https://sourcetreeapp.com/?v=win
- Visual Studio
  - install latest version https://visualstudio.microsoft.com/downloads/
  - in case of Git Bash/SCM presence, you must update it
- Java
  - simply upgrade java to latest version
  - if upgrade is not possible, you must manually import new CA certificate https://letsencrypt.org/certs/isrgrootx1.pem into java cacerts Like in this example assuming C:\Program Files\Java\jdk-11.0.4\ Java path:

    ```
    C:\Program Files\Java\jdk-11.0.4\bin\keytool -import -trustcacerts -alias certAlias -file
    isrgrootx1.pem -keystore C:\Program Files\Java\jdk-11.0.4\lib\security\cacerts
    ```

    Inspired by: https://docs.oracle.com/javase/tutorial/security/toolfilex/rstep1.html

Linux

Following resolutions help to make CA certs trusted for curl, wget and other system tools, also updates openjdk cacerts store.

Remember to restart Java based applications to take new certificates in use.

Importing CA certificate into Ubuntu certificates store

```
apt-get install ca-certificates ca-certificates-java -y
wget https://letsencrypt.org/certs/isrgrootx1.pem -O /usr/local/share/ca-certificates/isrgrootx1.crt
update-ca-certificates
update-ca-certificates --fresh
```

Importing CA certificate into CentOS certificates store

```
yum install ca-certificates
wget https://letsencrypt.org/certs/isrgrootx1.pem -O /etc/pki/ca-trust/source/anchors/isrgrootx1.crt
update-ca-trust enable
update-ca-trust extract
update-ca-trust
```

Related articles

https://letsencrypt.org/docs/dst-root-ca-x3-expiration-september-2021/

https://www-root-cz.translate.goog/zpravicky/vyprsel-korenovy-certifikat-dst-root-ca-pouzivany-autoritou-let-s-encrypt/?_x_tr_sl=cs&_x_tr_tl=en&_x_tr_hl=fi&_x_tr_pto=nui

https://www.openssl.org/blog/blog/2021/09/13/LetsEncryptRootCertExpire/

- Jenkins cleanup
- Jira Project Admin guide for beginners
- How to make new Lets Encrypt CA certificates trusted
- How convert SSH Keys to PPK Format?
- How to generate a SSH Key in a Windows