Change of the maximum validity for new TLS/SSL certificates to 1 year

Due to new global browser requirements, the validity period for public TLS/SSL certificates issued after 27 August 2020 will be limited to a maximum of 397 days.

- The 397 days correspond to one year of validity plus transitional period for extensions
- This change affects **all CAs (Certificate Authorities) industry-wide and globally**. It applies to Business SSL (OV), EV and qualified Web authentication certificates
- **Two-year certificates issued before the changeover on 27 August remain fully valid until the end of their regular term**
- This change does not affect other certificate types such as code signing, document signing, S/MIME or private TLS/SSL certificates

Shorter validity periods generally increase security by encouraging more frequent key pair changes and faster expiration of older certificates. Furthermore, new encryption requirements can be introduced more quickly.

What are DigiCert QuoVadis customers required to do?

You don't have to do anything. DigiCert QuoVadis will automatically adjust the maximum validity period for new TLS/SSL certificates in its certificate management tool Trust/Link from 27 August 2020. After this change, new TLS/SSL certificate issuance can only be selected with a maximum validity period of 397 days. All TLS/SSL certificates issued before August 27 are not affected and retain their maximum validity.

QuoVadis Trustlink Schweiz AG
Poststrasse 17, Postfach, 9001 St. Gallen, Schweiz
+41 71 228 98 00, register@quovadisglobal.com
www.quovadis.ch