

## **Laufzeiten von SSL-/TLS-Zertifikaten werden immer kürzer**

**Die Laufzeit von SSL-/TLS-Zertifikaten darf künftig maximal ein Jahr betragen**

Digitale Zertifikate und die zugehörigen digitalen Signaturen dienen der Bestätigung der Identität und der sicheren Übermittlung sensibler Daten im Internet oder im Unternehmensnetzwerk. Sie werden für sichere E-Mail, Web-Security, Windows SmartCard-Logon, VPN, Verschlüsselung von Dateien, digitale Dokumentsignaturen und viele weitere Anwendungen genutzt.

Ein digitales Zertifikat ist eine unveränderbare "elektronische Identitätskarte", vergleichbar mit einem elektronischen Personalausweis, bestätigt von der Zertifizierungsstelle. Genau wie ein Personalausweis, verfügt auch ein digitales Zertifikat über eine begrenzte Gültigkeitsdauer. Nachdem bereits 2018 die zulässige Laufzeit von SSL-/TLS-Zertifikaten auf maximal 825 Tage (ca. 27 Monate) reduziert wurde, werden die Richtlinien für die Ausstellung von SSL-Zertifikaten nun weiter verschärft: Nach dem 1. September 2020 dürfen sie nur noch mit einer Laufzeit von maximal einem Jahr ausgestellt werden.

Apple hat bereits beim CA/Browser Forum in Bratislava im Mai 2020 angekündigt, ab dem 01. September 2020 im Safari-Browser und auf seinen Geräten nur noch SSL-Zertifikate mit einjähriger Gültigkeit zu akzeptieren. Google und Mozilla folgen der Ankündigung von Apple und wollen zukünftig keine mehrjährigen Zertifikate mehr akzeptieren. Die Verkürzung der Gültigkeitsdauer von Zertifikaten ist nicht überraschend und passt in den Kontext der permanenten Verbesserung der Sicherheit des Internets, denn sie erleichtert es Serverbetreibern, auf Sicherheitsvorfälle zu reagieren. Die häufigere Generierung eines neuen Schlüsselpaares reduziert das Risiko eines Schlüsselverlusts oder einer Kompromittierung deutlich. Laufzeiten von E-Mail-Zertifikaten sind nicht von der Reduzierung der Laufzeit betroffen und bleiben unverändert.

Beständig kürzere Gültigkeit von Zertifikaten erhöhen zwangsläufig den Verwaltungsaufwand. Es ist abzusehen, dass Laufzeiten noch weiter reduziert werden und demnächst bei nur noch drei Monaten liegen werden. Exponentiell wachsende Zertifikatsbestände in fortwährend komplexeren IT-Umgebungen sind mit herkömmlichen Mitteln kaum mehr zu bewältigen. Sie erhöhen die Prozesskosten für die Administration sowie das Risiko von Fehlern im Umgang mit Zertifikaten. Zudem steigt die Gefahr von Betriebsstörungen in der IT durch ungeplant abgelaufene Zertifikate. Die Folgen: Mögliche rechtliche Konsequenzen und nachhaltige Schädigung des Unternehmensimages.

Auch neue, sichere Verschlüsselungsalgorithmen wie elliptic Curve sowie die Einhaltung von strengeren Compliance-Vorgaben erhöhen die Anforderungen an die „**Krypto-Agilität**“ von Unternehmen.

Zu einem vollumfänglichen Management von Zertifikaten gehören Monitoring, automatisiertes Beantragen und das Verteilen von Zertifikaten in die Zielsysteme sowie erneuern oder revozieren.

**essendi xc – die Antwort auf mehr Krypto-Agilität.** Zur Lösung dieser Herausforderungen hat die essendi it GmbH mit Sitz in Schwäbisch Hall eine Anwendung für das professionelle und effiziente Management von digitalen Zertifikaten (X.509) entwickelt. essendi xc vereinfacht, automatisiert und optimiert das Management von Zertifikaten end-to-end. Die Software unterstützt dabei entlang aller Prozesse - von der Beantragung, über die Verlängerung bis zur Installation der Zertifikate. essendi xc hilft Unternehmen, den Überblick über ihre Zertifikatsbestände und

**Bulletin: Kürzere Zertifikatslaufzeiten**

deren Gültigkeiten zu behalten und reduziert somit die bekannten Risiken. Dabei lässt sich die Anwendung hervorragend in die vorhandene Infrastruktur integrieren und individuelle Ansprüche anpassen: So ist beispielsweise die Anbindung namhafter HSM sowie der Import vorhandener Zertifikate in das zentrale Inventar problemlos möglich.

Inhaber von Zertifikaten sollten sich bei Ihrer/n Zertifizierungsstelle/n informieren, bis zu welchem Datum noch SSL-/TLS-Zertifikate mit zweijähriger Laufzeit erworben werden oder bis wann bereits erworbene zweijährige Lizenzen noch eingelöst werden können. Diese Fristen gelten auch für die Bestellung von Zertifikaten via essendi xc.

Während z.B. Betreiber von Webseiten oder Webshops berücksichtigen müssen, dass Zertifizierungsstellen keine Verlängerung unterstützen und stattdessen jeweils neue Zertifikate geordert und an die jeweiligen Zielsysteme verteilt werden müssen, sind essendi xc-Nutzer fein raus: essendi xc unterstützt bei der Erneuerung und dem Enrollment von Zertifikaten oder übernimmt beides sogar ganz automatisch.

Weitere Informationen unter <https://xc-essendi.de>