

SW-Zertifikate & Ende Verwendung von SHA1 Algorithmen

Betrifft alle SS12 Nutzer, die Softwarezertifikate als Admin-Karten-Ersatz einsetzen

- Krankenanstalten
- Eigene Einrichtungen
- Weitere Gesundheitsdiensteanbieter
- und deren Softwarehersteller

Zum Signieren von Requests werden teilweise noch Algorithmen mit SHA1 verwendet. Diese sind stark veraltet, gelten als nicht mehr sicher und sind seit 2015 nicht mehr erlaubt. Wir haben dies bereits 2014 angekündigt. Mit 01.08.2024 können keine Request mehr mit SHA1 signiert werden. Es kommt zu einer Fehlermeldung (ZS-10012). Es ist daher dringend erforderlich, dass bis zum 31.07.2024 die Algorithmen zum Signieren von Requests auf mind. SHA256 umgestellt werden.



ENDE ÜBERGANGSFRIST

Die Übergangsfrist für die Umstellung von SHA1 endet am **31.07.2024**

Informationen zu SW-Zertifikaten finden Sie hier [www.chipkarte.at/sw-zertifikate]

Betroffen sind im Request

- SignatureMethod Algorithm
- DigestMethod Algorithm

ERLAUBT:

- z.B. <http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>

NICHT ERLAUBT

- z.B. <http://www.w3.org/2000/09/xmldsig#sha1>
-

Ihr Partnersupport und KA-Support

Sozialversicherungs-Chipkarten Betriebs- und Errichtungsges.m.b.H. – SVC

Ernst-Melchior-Gasse 22, A-1020 Wien

support@svc.co.at krankenanstalten@svc.co.at www.svc.co.at www.chipkarte.at	FN: 206187t, Handelsgericht Wien UID: ATU52613104c
--	---