PRESSEMITTEILUNG

Kein Widerspruch: Nationale Kryptografie-Souveränität im Rahmen europäischer Harmonisierung

Berlin, 23.10.2015 - Das Thema "Digitale Souveränität" betrifft in Bezug auf Kryptografie nicht nur die Schlüsselerzeugung, sondern auch die Algorithmenwahl, einschließlich Schlüssellängen. Nicht umsonst werden sogenannte Krypto-Kataloge unabhängig vom Einsatz in Qualifizierten Signaturen/eIDAS üblicherweise national festgelegt, z.B. FIPS (US), BSI TR-02102 und BNetzA-AlgoKat (DE). Andererseits sind für den Bereich "eIDAS" EU-einheitliche Festlegungen sinnvoll. TeleTrusT unterstützt die Forderung nach einer EU-weiten Regelung.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) weist darauf hin, dass die Querwirkungen von nationaler Krypto-Souveränität, Harmonisierung im eIDAS-Kontext und auch Zertifizierungsdetails für QSCDs beachtet werden müssen, da zertifizierte Produkte z.T. sowohl als QSCDs, aber gleichzeitig auch in anderen Anwendungen eingesetzt werden. Die Algorithmen bilden die sicherheitstechnische Basis für die darauf aufsetzenden und unter eIDAS (teil-)geregelten Services.

Ohne ein einheitliches Verständnis zur Gültigkeit der Algorithmen ist eine rechtlich und technisch harmonisierte Umsetzung in Europa nur schwer vorstellbar. Die Vorgaben aus dem ETSI-Bereich helfen hier jedenfalls teilweise weiter. Zum einen wird der entsprechende ETSI-Katalog 119 312 zutreffenderweise nur informativ referenziert, d.h. nicht verbindlich. Zum anderen ist auch EN 319 411-1 (AES und PTC) unabhängig von der Referenzierung in einem "Implementing Act" nicht notwendigerweise verbindlich, da der Implementing Act nur die Vermutung der Einhaltung der Verordnung bei Einhaltung eines referenzierten Standards beinhaltet, aber in keiner Weise alternative Methoden zur Einhaltung der Anforderungen der VO einschränkt.

Diese fehlende verbindliche Festlegung von Krypto-Algorithmen kann in Verbindung mit der verpflichtenden Anerkennung von Qualifizierten Signaturen und Qualifizierten Siegeln im öffentlichen Sektor zu dem interessanten Ergebnis führen, dass jede Signaturvalidierungssoftware, die im öffentlichen Sektor eingesetzt wird, zwingend alle in der EU für Qualifizierte Signaturen und Qualifizierte Siegel eingesetzten Algorithmen unterstützen muss.

Um in der EU möglichst gleiche Voraussetzungen im digitalen Binnenmarkt zu ermöglichen, empfiehlt TeleTrusT die Erarbeitung von Durchführungsrechtsakten, die den entsprechenden technischen Normen, die bereits erarbeitet wurden, Geltung verschaffen.

Ohne Netzwerkeffekt findet souveräne Kryptografie keine Anwendung, desweiteren wird zukünftige Kryptografie stets auch auf Tablets und Smartphones funktionieren, d.h. in den marktbestimmenden Betriebssystemen bzw. "AppStores" akzeptiert sein müssen.

TeleTrusT - Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
www.teletrust.de