Empfohlene Algorithmen und Parameter für elektronische Signaturen

Nach § 3 Abs. 2 SigV, BGBl. II Nr. 30/2000, geändert durch BGBl. II Nr. 527/2004, dürfen für sichere elektronische Signaturen nur solche Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs der Verordnung erfüllen. Diese nennt keinen Ablauf der Sicherheitsperiode. Nach § 3 Abs. 2 SigV sind jedoch die für die technische Sicherheit der Algorithmen und Parameter geltenden Randbedingungen so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen. In den Fällen, wo dazu eine Rechts- oder eine Vertragbasis besteht, werden diese Grundlagen auch zur Beurteilung der Erfüllung der Anforderungen des § 2 Z 3 lit. a bis d SigG herangezogen[1].

Das vorliegende Dokument enthält Empfehlungen der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) und des Zentrums für sichere Informationstechnologie – Austria (A-SIT) für Algorithmen und Parameter, die nach dem gegenwärtigen Stand der Technik voraussichtlich bis zum Ende des Jahres 2011 den Erfordernissen für sichere (also auch für fortgeschrittene) elektronische Signaturen entsprechen. Die Empfehlungen beruhen u. a. auf publizierten Prognosen und auf Vorschriften in anderen Mitgliedstaaten der Europäischen Union.

Die RTR-GmbH und A-SIT werden sich im Rahmen ihrer Tätigkeiten nach dem Signaturgesetz, soweit nicht Änderungen des Wissensstandes, der Rechtsvorschriften oder internationale Entwicklungen anderes erfordern, am vorliegenden Dokument orientieren. Das Dokument wird zumindest jährlich überarbeitet, an den aktuellen Stand der Technik angepasst und veröffentlicht.

Die in diesem Dokument verwendeten Bezeichnungen für Algorithmen und Parameter entsprechen, soweit nicht anders angegeben, dem Anhang der Signaturverordnung (BGBl. II Nr. 527/2004) bzw. dem vom European Telecommunication Standards Institute veröffentlichten Bericht ETSI SR 002 176[2].

Signaturalgorithmen und Parameter

Bis 31.12.2011 erscheinen die Signaturalgorithmen rsa, dsa, ecdsa-Fp, ecdsa-F2m, ecgdsa-Fp und ecgdsa-F2m geeignet.

Bezüglich der Parameter von rsa wird

bis 31.12.2007	MinModLen = 1024,
bis 31.12.2008	MinModLen = 1280 und
bis 31.12.2011	MinModLen = 1536

als Mindestwert empfohlen.

Bezüglich der Parameter von dsa wird

bis 31.12.2007	pMinLen = 1024,	qMinLen = 160,
bis 31.12.2008	pMinLen = 1280,	qMinLen = 160 und
bis 31.12.2011	pMinLen = 1536,	qMinLen = 160

als Mindestwert empfohlen[3].

---

[1] Das betrifft auch die in Österreich zur Zeit gesetzlich noch nicht umgesetzte „fortgeschrittene Signatur“.

[2] ETSI SR 002 176 V1.1.1 (2003-03): Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

[3] Der Standard FIPS 186-2 (Change Notice 1) für dsa sieht für p genau 1024 vor, die hier empfohlenen Schlüssellängen weichen davon ab.

Bezüglich der Parameter von ecdsa-Fp, ecdsa-F2m, ecgdsa-Fp bzw. ecgdsa-F2m wird

bis 31.12.2006	qMinLen = 160,	r0Min = 10^4,	MinClass = 200 und
bis 31.12.2011	qMinLen = 192,	r0Min = 10^4,	MinClass = 200

empfohlen.

Algorithmen zur Schlüsselerzeugung

Bis 31.12.2011 wird der Einsatz von Schlüsseln empfohlen, die mit den Verfahren rsagen1, dsagen1, ecgen1 bzw. ecgen2 für die jeweils entsprechenden Signaturalgorithmen erzeugt worden sind.

Padding-Verfahren

Bis 31.12.2011 erscheinen die Padding-Verfahren emsa-pkcs1-v1_5 und emsa-pss für den Signaturalgorithmus rsa geeignet.

Kryptographische Hashfunktionen

Die Hashfunktion sha1 erscheint in Kombination mit den Signaturalgorithmen rsa, dsa, ecdsa-Fp, ecdsa-F2m, ecgdsa-Fp bzw. ecgdsa-F2m bis 31.12.2009 geeignet[4].

Die Hashfunktion ripemd160 erscheint in Kombination mit den Signaturalgorithmen rsa, ecgdsa-Fp bzw. ecgdsa-F2m bis 31.12.2009 geeignet.

Bis 31.12.2011 erscheinen die vom National Institute of Standards and Technology in FIPS 180-2[5] definierten Hashfunktionen sha256, sha384 und sha512 geeignet.

Wien, am 1. März 2005

Dr. Georg Serentschy
Geschäftsführer, Fachbereich Telekommunikation
RTR-GmbH

Univ.-Prof. Dr. Reinhard Posch
Wissenschaftlicher Gesamtleiter
A-SIT

Manfred Holzbach
Geschäftsführer
A-SIT

[4] Da die Hashfunktion in der Regel durch die Software der Arbeitsstation und nicht auf einer Karte umgesetzt wird, wird das Anpassen an notwendige Veränderungen aufgrund des aktuellen Wissensstandes rascher erfolgen können.
[5] FIPS 180-2: Secure Hash Standard