Empfohlene Algorithmen und Parameter für elektronische Signaturen

Nach § 3 Abs. 2 SigV [1] 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, können diese Grundlagen auch zur Beurteilung der Erfüllung der Anforderungen des § 2 Z 3 lit. a bis d SigG [2] herangezogen werden.

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 2013 den Erfordernissen für sichere 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. Da es sich jedoch nicht um eine Rechtsnorm handelt, ist die Telekom-Control-Kommission als Aufsichtsstelle nach dem Signaturgesetz in ihrer Rechtsauslegung nicht an das Dokument gebunden. 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 SigV [1]. Bei jenen Algorithmen, die im Anhang der SigV [1] nicht ausdrücklich genannt werden, handelt es sich um Weiterentwicklungen, durch die dem aktuellen Stand der Technik Rechnung getragen wird.

Signaturalgorithmen und Parameter

Bis 31.12.2013 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,
bis 31.12.2011	MinModLen = 1536 und
bis 31.12.2013	MinModLen = 2048

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,
bis 31.12.2011	pMinLen = 1536,	qMinLen = 160 und
bis 31.12.2013	pMinLen = 2048,	qMinLen = 224

als Mindestwert empfohlen[1].

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

bis 31.12.2011	qMinLen = 192,	r0Min = 10^4,	MinClass = 200 und
bis 31.12.2013	qMinLen = 224	r0Min = 10^4,	MinClass = 200

empfohlen. Für diese Signaturalgorithmen wird die Verwendung elliptischer Kurven empfohlen, die entweder in FIPS 186-2 [3] definiert oder nach dem in ANS X9.62–2005 [6] spezifizierten Zufallsverfahren erzeugt worden sind.

Algorithmen zur Schlüsselerzeugung

Bis 31.12.2013 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 31.12.2013 erscheinen die in DIN V 66291-1, Ausgabe: 2000-04 [7], bzw. RFC 3447 [8] spezifizierten Padding-Verfahren emsa-pkcs1-v1_5, emsa-pkcs1-v2_1, emsa-pss, iso9796ds2, iso9796-din-rn und iso9796ds3 für den Signaturalgorithmus rsa geeignet.

Kryptographische Hashfunktionen

Zur Eignung der Hashfunktion sha1 in Kombination mit den Signaturalgorithmen rsa, dsa, ecdsa-Fp, ecdsa-F2m, ecgdsa-Fp bzw. ecgdsa-F2m kann auf Grund neuer Methoden zur Kollisionssuche keine Prognose bezüglich des uneingeschränkten Einsatzes bei der Erstellung von sicheren elektronischen Signaturen gegeben werden. Nach einem im Auftrag der Telekom-Control-Kommission von Prof. Vincent Rijmen erstellten Gutachten [9] sind bereits innerhalb eines Zeitraums von weniger als zwei Jahren Kollisionsberechnungen für sha1 zu erwarten. Die Hashfunktion sha1 kann deshalb nur mehr als vorläufig geeignet betrachtet werden und zwar so lange, bis praktische Kollisionsberechnungen möglich sind. Es wird daher empfohlen, jene technischen Komponenten und Verfahren, die sha1 im Zusammenhang mit der Erstellung von sicheren elektronischen Signaturen verwenden, sobald wie möglich auf andere – in der Folge genannte – Hashfunktionen, die für einen längeren Zeitraum als geeignet betrachtet werden können, umzustellen. Diese Umstellung sollte bis 31.12.2007 vorgenommen werden. Für die elektronische Signatur eines Zertifizierungsdiensteanbieters in einem qualifizierten Zertifikat erscheint sha1 noch für einen längeren Zeitraum geeignet, wenn durch geeignete Maßnahmen beim Zertifizierungsdienste-anbieter Kollisionsangriffe vermieden werden können und die Wirksamkeit dieser Maßnahmen im Wege der Aufsicht sichergestellt werden kann. Es wird jedoch auch hier empfohlen, bald auf Hashfunktionen, die für einen längeren Zeitraum als geeignet betrachtet werden können, umzustellen, da für qualifizierte Zertifikate eine Resistenz der Hashfunktion

[1] FIPS 186-2 [3] sieht als Länge von p genau 1024 und als Länge von q genau 160 vor. Nach FIPS 186-3 (Draft) [4] und ISO/IEC 14888-3:2006 [5] sind jedoch auch längere Parameter zulässig.

gegenüber Second-Preimage-Angriffen über die gesamte Gültigkeitsdauer des Zertifikats erforderlich ist.

Die Hashfunktion ripemd160 erscheint in Kombination mit den Signaturalgorithmen rsa, ecdsa-Fp, ecdsa-F2m, ecgdsa-Fp bzw. ecgdsa-F2m bis 31.12.2010 geeignet.

Bis 31.12.2013 erscheinen die vom National Institute of Standards and Technology in FIPS 180-2 [10] definierten Hashfunktionen sha224, sha256, sha384 und sha512 in Kombination mit den Signaturalgorithmen rsa, dsa, ecdsa-Fp, ecdsa-F2m, ecgdsa-Fp bzw. ecgdsa-F2m geeignet.

Referenzen

[1] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000 idF BGBl. II Nr. 527/2004

[2] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl. I Nr. 190/1999 idF BGBl. I Nr. 164/2005

[3] FIPS 186-2 with Change Notice 1 dated October 5, 2001, Digital Signature Standard (DSS)

[4] FIPS 186-3 (Draft), Digital Signature Standard (DSS)

[5] ISO/IEC 14888-3:2006, Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms

[6] ANS X9.62–2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signatures Algorithm

[7] DIN V 66291-1, Ausgabe: 2000-04, Chipkarten mit Digitaler Signatur-Anwendung/ Funktion nach SigG und SigV – Teil 1: Anwendungsschnittstelle

[8] RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

[9] Vincent Rijmen, Florian Mendel, Norbert Pramstaller, Christian Rechberger: Current Status of SHA-1. February 21, 2007

[10] FIPS 180-2 with Change Notice 1 dated February 25, 2004, Secure Hash Standard

Wien, am 1. Juni 2007

Dr. Georg Serentschy
Geschäftsführer, Fachbereich Telekommunikation
RTR-GmbH

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

Manfred Holzbach
Geschäftsführer
A-SIT