Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Empfänger lt. E-Mail-Verteilerliste

Aron Gohr

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-5969
FAX +49 (0) 228 9910 9582-5969

aron.gohr@bsi.bund.de
https://www.bsi.bund.de

Betreff: Angaben des BSI zur Eignung von Signaturalgorithmen gemäß §17 Abs. 1 bis 3 SigG

Aktenzeichen: KT23-360-01-02
Datum: 15.11.2016

Anlage: -1-

Sehr geehrte Damen und Herren,

gemäß Signaturverordnung (SigV) macht das BSI in jedem Jahr Angaben über die Eignung von Kryptoalgorithmen, mit denen elektronische Signaturen erzeugt werden können, die den Vorgaben des deutschen Signaturgesetzes genügen.
In der Anlage finden Sie den Entwurf des BSI für das Jahr 2017 mit der Bitte um Kommentierung.

Diesen Entwurf finden Sie auch auf der BSI-Homepage unter

https://www.bsi.bund.de/Algorithmenkatalog

Bitte senden Sie Kommentare, Hinweise und Korrekturen per E-Mail oder auch per Post bis zum 6.12.2016 an die folgenden zwei Adressen:

Bundesamt für Sicherheit in der Informationstechnik
Dr. Aron Gohr
Postfach 200363
D-53133 Bonn
E-Mail: algokat@bsi.bund.de

sowie

Bundesnetzagentur
Dr. Axel Schmidt
Postfach 8001
D-55003 Mainz
E-Mail: qes@bnetza.de

Der Termin zur Expertenanhörung steht derzeit noch nicht endgültig fest. Eine Einladung hierzu wird Ihnen in Kürze separat zugehen.

Zu den Angaben im vorliegenden Entwurf:

- Der Entwurf macht Eignungsaussagen bis Ende 2023, also wie in den Vorjahren über 7 Jahre anstatt über den in der SigV vorgeschriebenen Mindestzeitraum von 6 Jahren. Das erscheint beim gegenwärtigen kryptographischen Kenntnisstand vertretbar.
- Die Eignungsfristen für RSA und DSA mit Schlüssellängen unterhalb von 3000 Bit werden, wie im Algorithmenkatalog 2016 bereits angekündigt, im vorliegenden Entwurf nicht verlängert. Diese Schlüssellängen bleiben damit bis Ende 2022 geeignet.
- Entsprechend werden auch die Anforderungen an deterministische Zufallsgeneratoren für den Einsatzzeitraum bis 2023 auf ein Sicherheitsniveau von 120 Bit angehoben. Für eine Nutzung bis 2022 ändert sich an den bisher bestehenden Vorgaben nichts.
- Die Eignung des PKCS#1-v1_5-Paddingformats wird letztmalig bis Ende 2017 verlängert. Für spezielle Anwendungen, für die bisher eine Nutzung dieses Paddingformats bis Ende 2017 möglich war, wird die Eignungsfrist bis Ende 2018 ausgedehnt.
- Die Eignung von Nyberg-Rueppel-Signaturen wird nicht über das Jahr 2020 hinaus verlängert. Der Grund für die Streichung von Nyberg-Rueppel-Signaturen besteht darin, dass nicht davon ausgegangen wird, dass eine Nutzung dieses Verfahrens in durch das Signaturgesetz betroffenen Anwendungen stattfindet und dass die Streichung von Nyberg-Rueppel-Signaturen die Pflege des Algorithmenkatalogs erleichtert.

Im Auftrag

Dr. Gohr