Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung

(Übersicht über geeignete Algorithmen)

Vom 9.12. 2015

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Behörde gemäß § 3 Signaturgesetz (SigG) vom 16. Mai 2001 (BGBl. I S. 876), das durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, veröffentlicht gemäß Anlage 1 Abschnitt 1 Nr. 2 Signaturverordnung (SigV) vom 16. November 2001 (BGBl. I S. 3074), die durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt.

Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001

Vorbemerkung: Wie in den Vorjahren werden im Folgenden geeignete Algorithmen und Schlüssellängen für den Zeitraum der kommenden sieben Jahre anstatt des in der SigV vorgesehenen Mindestzeitraums von sechs Jahren aufgeführt. Das heißt konkret, dass geeignete Algorithmen und Schlüssellängen bis Ende 2022 statt bis Ende 2021 aufgeführt sind. Im Allgemeinen sind solche längerfristigen Prognosen schwer möglich. Die vorliegende Übersicht über geeignete Algorithmen unterscheidet sich von der zuletzt veröffentlichten Übersicht vom15. Dezember 2014 (BAnz AT 30.01.2015 B3) im Wesentlichen in folgenden Punkten:

1. Die Planungen zur vorgesehenen Anhebung des Sicherheitsniveaus für qualifizierte elektronische Signaturen auf 120 Bit wurden konkretisiert. Es ist vorgesehen, ab dem Algorithmenkatalog 2017 entsprechende Regelungen wirksam zu machen. Insbesondere ist keine Verlängerung von RSA-Signaturen und DSA-Signaturen mit Schlüssellängen unter 3000 Bit über das Jahr 2022 hinaus vorgesehen. Aus dem gleichen Grund ist vorgesehen, die Eignung von Zufallsgeneratoren mit einer Seed-Entropie unter 120 Bit nicht über das Jahr 2022 hinaus zu verlängern.

2. Da DSA-Signaturen potentiell anfällig für Angriffe unter Verwendung von Vorberechnungen sind, die nur von dem verwendeten Restklassenkörper abhängen, wird empfohlen, in DSA-Signaturverfahren schon jetzt Schlüssellängen ab 3000 Bit zu nutzen, falls eine große Anzahl von Nutzern den gleichen DSA-Modul verwendet.

3. Die Liste der geeigneten Hashfunktionen wurde um SHA3-256, SHA3-384 und SHA3-512 erweitert. Umgekehrt wird, wie bereits in der letzten Ausgabe des vorliegenden Dokuments angekündigt, die Hashfunktion SHA-224 nicht mehr als geeignet eingestuft.

4. Die Eignung von RSA-Signaturen nach PKCS#1v1.5 wird nicht über Ende 2016 hinaus verlängert.

5. Die Anforderungen an die RSA-Schlüsselerzeugung wurden etwas präziser formuliert. Dies hat keine Auswirkungen auf bestehende Systeme.

6. Es wurden verschiedene Verfahren, deren Eignung 2015 ausgelaufen ist, aus der vorliegenden Übersicht gestrichen. Beispiele hierfür sind DSA/ECDSA-Verfahren mit weniger als 250 Bit Gruppengröße und die Hashfunktion SHA-224.

Die Sicherheit einer qualifizierten elektronischen Signatur hängt entscheidend von der Stärke der zugrunde liegenden Algorithmen ab. Im Folgenden werden Algorithmen genannt, die für qualifizierte elektronische Signaturen mindestens für die kommenden sieben Jahre (d.h. bis Ende 2022) als geeignet anzusehen sind.

Darüber hinaus werden Empfehlungen aufgeführt, die dazu dienen, zukünftigen Entwicklungen im Bereich der kryptographischen Algorithmen und zugehörigen Parameter, die sich heute schon abzeichnen und in Zukunft an Bedeutung zunehmen könnten, zu begegnen. Diese als Empfehlung formulierten Angaben dienen dazu, dem "Interesse der Planungssicherheit der interessierten Hersteller, Dienstleister und Anwender" Rechnung zu tragen (vgl. Roßnagel/ Pordesch: Kommentierung des Signaturgesetzes [33]). Es besteht zum jetzigen Zeitpunkt jedoch keine Pflicht, diese Empfehlungen umzusetzen. Neben Empfehlungen beinhaltet der Algorithmenkatalog Bemerkungen, die seinem besseren Verständnis dienen und einen rein informativen Charakter haben.

Die bitgenauen Spezifikationen findet man in den entsprechenden Standards verschiedener Organisationen (ISO, IEC, NIST, IEEE usw.). Ebenso wie patentrechtliche Fragen und Definitionen der mathematischen Begriffe sind diese Spezifikationen nicht Gegenstand der vorliegenden Veröffentlichung. Informationen hierzu findet man in der einschlägigen Literatur (Lehrbücher, Tagungsbände von Konferenzen etc.) und im Internet.

In dieser Veröffentlichung werden die wichtigsten praxisrelevanten Algorithmen betrachtet, deren kryptographische Eigenschaften aufgrund der heute vorliegenden Ergebnisse langjähriger Diskussionen und Analysen am besten eingeschätzt werden können. Die Liste dieser Algorithmen wird gemäß der weiteren Entwicklung der kryptologischen Forschung und den Erfahrungen mit praktischen Realisierungen von Signaturverfahren aktualisiert und bei Bedarf ergänzt werden.

Auf die Sicherheit einer konkreten Implementierung in Hard- und Software wird hier nicht eingegangen. Diese wird im Rahmen der Untersuchung nach § 15 Abs. 7 und § 17 Abs. 4 SigG festgestellt.

Inhalt

1. Kryptographische Anforderungen

Nach Anlage 1 Abschnitt I Nr. 2 SigV sind folgende Algorithmen festzulegen:

- Ein Algorithmus zum Hashen von Daten (eine Hashfunktion), der die zu signierenden Daten (und in manchen Signaturverfahren noch gewisse zusätzliche Daten) auf einen Hashwert, d.h. eine Bitfolge vorgegebener Länge, reduziert. Signiert werden dann nicht die Daten selbst, sondern stattdessen jeweils ihr Hashwert.
- Ein asymmetrisches Signaturverfahren, das aus einem Signieralgorithmus und einem Verifizieralgorithmus besteht. Das Signaturverfahren hängt ab von einem Schlüsselpaar, bestehend aus einem privaten (d.h. geheimen) Schlüssel zum Signieren (gemäß § 2 Nr. 4 SigG als Signaturschlüssel zum Erzeugen einer Signatur bezeichnet) und dem dazugehörigen öffentlichen Schlüssel zum Verifizieren der Signatur (gemäß § 2 Nr. 5 SigG als Signaturprüfschlüssel zur Überprüfung einer Signatur bezeichnet).
- Ein Verfahren zur Erzeugung von Schlüsselpaaren für Signaturverfahren.

1.1. Hashfunktionen

Beim Signieren und Verifizieren wird der Hashwert der zu signierenden Daten gewissermaßen wie ein 'digitaler Fingerabdruck' benutzt. Damit hierbei keine Sicherheitslücke entsteht, muss die Hashfunktion *H* folgenden Kriterien genügen:

- *H* muss *kollisionsresistent* sein; d.h., es ist praktisch unmöglich, Kollisionen zu finden. Hierbei bilden zwei unterschiedliche Eingabewerte, die durch *H* auf denselben Hashwert abgebildet werden, eine Kollision.
- *H* muss eine *Einwegfunktion* sein; d.h., es ist praktisch unmöglich, zu einem gegebenen Bitstring aus dem Wertebereich ein Urbild bzgl. *H* zu finden.

Die Existenz von Kollisionen ist unvermeidbar. Bei der praktischen Anwendung kommt es jedoch nur darauf an, dass es, wie oben verlangt, praktisch unmöglich ist, Kollisionen (bzw. Urbilder) zu *finden*.

1.2. Signaturverfahren

Niemand anders als der Besitzer des Signaturschlüssels darf in der Lage sein, Signaturen zu erzeugen, die bei einer Prüfung mit dem zugehörigen Signaturprüfschlüssel als gültig bewertet werden. Insbesondere bedeutet dies, dass es praktisch unmöglich sein muss, den Signaturschlüssel aus dem (öffentlichen) Signaturprüfschlüssel zu berechnen. Allgemeiner darf es praktisch nicht möglich sein, mit Kenntnis des Signaturprüfschlüssels und Beispielen von Signaturen gültige Signaturen zu neuen Dokumenten zu erzeugen, ohne den Signaturschlüssel zu nutzen.

1.3. Schlüsselerzeugung

Die verschiedenen Signaturverfahren benötigen Schlüssel mit gewissen Eigenschaften, die sich aus dem jeweiligen konkreten Verfahren ergeben. Im Folgenden werden weitere einschränkende Bedingungen festgelegt, deren Nichtbeachtung zu Schwächen führen könnte. Zusätzlich wird generell verlangt, dass Schlüssel nach den unter „4. Erzeugung von Zufallszahlen“ genannten Maßnahmen zufällig erzeugt werden.

2. Geeignete Hashfunktionen

Die beiden Hashfunktionen SHA-1 und RIPEMD-160 sind bis Ende 2015 nur noch für die Prüfung qualifizierter Zertifikate geeignet.

Die folgenden Hashfunktionen sind geeignet, ein langfristiges Sicherheitsniveau zu gewährleisten:

- SHA-256, SHA-512/256, SHA-384, SHA-512 [2].
- SHA3-256, SHA3-384, SHA3-512 [38].

Dabei sind SHA-256 und SHA-512/256 Hashfunktionen mit einer Hashwertlänge von 256 Bit, während SHA-384 und SHA-512 jeweils 384 respektive 512 Bit lange Hashwerte erzeugen. SHA-512/256 entspricht SHA-512 mit einem auf 256 Bit abgeschnittenen Hashwert und einem anders als bei SHA-512 definierten Initialisierungsvektor. Insgesamt sind SHA-512/256, SHA-384 und SHA-512 hinsichtlich ihrer Implementierung und damit auch hinsichtlich aller Implementierungsaspekte (z.B. Performanz auf verschiedenen Plattformen) fast identisch.

Für SHA-512/256 wird eine gleiche Widerstandsfähigkeit gegen klassische generische Angriffe auf Kollisionsresistenz und Einwegeigenschaften erwartet wie für SHA-256. Aufgrund des größeren inneren Zustandes und der erhöhten Rundenanzahl von SHA-512/256 verglichen mit SHA-256 ist ein etwas verbesserter Sicherheitsspielraum gegen künftige kryptoanalytische Fortschritte zu erwarten. Ein weiterer theoretischer Vorteil ist eine gegenüber SHA-256 verbesserte Widerstandsfähigkeit gegen Multikollisions-Angriffe wie in [36].

Von einem praktischen Standpunkt aus betrachtet sind die Hashfunktionen der SHA-2-Familie und die der SHA-3-Familie nach heutigem Kenntnisstand als gleichermaßen sicher einzuschätzen. In manchen Anwendungen ergeben sich für die Funktionen der einen oder der anderen Familie besondere Implementierungsanforderungen: zum Beispiel muss der Endzustand der Hashfunktion vor Einsichtnahme durch einen Angreifer geschützt werden, wenn die Preimage-Sicherheit von SHA-3 für eine Anwendung wichtig ist; andererseits sind die Hashfunktionen der SHA-3-Familie etwa gegen Length Extension-Attacken grundsätzlich geschützt. Für die Anwendung der in der vorliegenden Bekanntmachung aufgelisteten Signaturverfahren ergeben sich allerdings dem jetzigen Kenntnisstand nach keine solchen Unterschiede. Zum Beispiel ist die Preisgabe des inneren Zustands der genutzten Hashfunktion bei der Berechnung des Hashwertes einer zu signierenden Nachricht unkritisch, wenn die Nachricht selbst nicht vertraulich gehalten werden soll.

Diese sieben Hashfunktionen sind (mindestens) in den **kommenden sieben Jahren**, d.h. **bis Ende 2022**, für die Anwendung bei qualifizierten elektronischen Signaturen geeignet. Die Hashfunktion SHA-224 [2] war bis **Ende 2015** für die Anwendung bei qualifizierten elektronischen Signaturen geeignet.
Die Hashfunktion SHA-1 war bis Ende 2010 zur Erzeugung qualifizierter Zertifikate zugelassen, sofern in die Erzeugung der Seriennummer Zufall mit mindestens 20 Bit Entropie eingeflossen ist. Auch wenn bei der SHA-2-Familie oder der SHA-3-Familie nach gegenwärtigem Kenntnisstand hierfür keine Notwendigkeit besteht, wird dennoch empfohlen, dies auch dort als eine zusätzliche Sicherheitsmaßnahme zu verwenden.

Bemerkung:

- Ob in die Erzeugung eines qualifizierten Zertifikats tatsächlich mindestens 20 Bit Entropie eingeflossen sind, kann im Rahmen der Prüfung des qualifizierten Zertifikats mittels einer Signaturanwendungskomponente gemäß § 2 Nr. 11 b) SigG nicht festge-

stellt werden. Die Anforderung ist vielmehr vom Zertifizierungsdiensteanbieter in seinem Betrieb zu erfüllen.

3. Geeignete Signaturverfahren

Im Jahr 1977 haben Rivest, Shamir und Adleman das nach ihnen benannte RSA-Verfahren [9] zum Erzeugen und Verifizieren digitaler Signaturen explizit beschrieben. Im Jahr 1984 hat ElGamal [8] ein weiteres Signaturverfahren vorgeschlagen. Eine Variante dieses ElGamal-Verfahrens ist der vom National Institute of Standards and Technology (NIST) publizierte Digital Signature Standard (DSS) [1], der den Digital Signature Algorithm (DSA) spezifiziert. Daneben gibt es Varianten des DSA, die auf Punktegruppen *E(K)* elliptischer Kurven über endlichen Körpern *K* basieren, wobei *K* entweder der Restklassenkörper modulo einer Primzahl *p* ist oder ein endlicher Körper der Charakteristik 2.

Folgende Signaturverfahren sind zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG geeignet:

1. RSA-Verfahren [21],
2. DSA [1], [4],
3. DSA-Varianten basierend auf elliptischen Kurven:
   - EC-DSA [1], [4], [5], [10],
   - EC-KCDSA, EC-GDSA [4],
   - Bis 2020: Nyberg-Rueppel-Signaturen [6].

Für weitere (nicht normative) Informationen zu EC-DSA und EC-GDSA siehe auch die Abschnitte 4.2.1 und 4.2.2 von [37].

Die Sicherheit der oben genannten Verfahren beruht dabei entsprechend auf:

1. dem RSA-Problem (im Hinblick auf bekannte Angriffe bei geeigneter Schlüsselerzeugung äquivalent dem Faktorisierungsproblem für ganze Zahlen),
2. dem Problem der Berechnung diskreter Logarithmen in der multiplikativen Gruppe von F_p oder
3. dem Diskreten-Logarithmus-Problem in einer elliptischen Kurve über einem Restklassenkörper modulo einer Primzahl *p* oder einem Körper der Charakteristik 2.

Um festzulegen, wie groß die Systemparameter bei diesen Verfahren zu wählen sind, um deren Sicherheit zu gewährleisten, müssen zum einen die besten heute bekannten Algorithmen zum Faktorisieren ganzer Zahlen bzw. zum Berechnen diskreter Logarithmen (in den oben genannten Gruppen) betrachtet und zum anderen die Leistungsfähigkeit der heutigen Rechnertechnik berücksichtigt werden. Um eine Aussage über die Sicherheit für einen bestimmten zukünftigen Zeitraum zu machen, muss außerdem eine Prognose für die künftige Entwicklung der beiden genannten Aspekte zugrunde gelegt werden, vgl. [12], [26], [35]. Solche Prognosen sind nur für relativ kurze Zeiträume sinnvoll (und können sich natürlich jederzeit aufgrund unvorhersehbarer Entwicklungen als falsch erweisen).

Im Folgenden bezeichnen wir mit der Bitlänge *r* einer positiven ganzen Zahl *x* diejenige ganze Zahl *r* mit der Eigenschaft $2^{r-1} \leq x < 2^r$.

Die Sicherheit der einzelnen Verfahren ist (mindestens) für die **kommenden sieben Jahre**, d.h. bis **Ende 2022**, bei der im Folgenden festgelegten Wahl der Parameter gewährleistet. Hierbei gibt es die folgenden Ausnahmen:

- Nyberg-Rueppel-Signaturen werden nur noch bis Ende 2020 als geeignet angesehen.
- RSA-Signaturen entsprechend RSASSA-PKCS1-v1_5 gemäß [14] können noch bis Ende 2016 erstellt werden. Ihr Beweiswert bleibt bis 2020 erhalten. Für RSA-Signaturschlüssel, die ab 2021 erzeugt werden, muss ein öffentlicher Exponent gewählt werden, der sich zwischen $2^{16}+1$ und 2^{256} bewegt.

3.1. RSA-Verfahren

Der Parameter *n* muss eine Länge von mindestens 1976 Bit haben. Empfohlen werden 2048 Bit. Für nach 2020 erzeugte Schlüsselpaare muss zudem der öffentliche Exponent *e* die Ungleichung $2^{16}+1 \leq e < 2^{256}$ erfüllen. Mittelfristig ist es empfehlenswert, eine RSA-Schlüssellänge von mindestens 3000 Bit anzustreben. Es ist geplant, ab 2017 diese Empfehlung in eine verbindliche Regelung zu überführen. Konkret ist vorgesehen, ab 2017 die Eignung von Schlüssellängen unter 3000 Bit nicht weiter zu verlängern. Die Eignung dieser Schlüssel wird damit voraussichtlich Ende 2022 auslaufen.

Die folgende Tabelle fasst die minimalen Bitlängen zusammen.

Tabelle 1: Geeignete Schlüssellängen für RSA-Verfahren

Parameter \ Zeitraum	bis Ende **2022**
n	1976 (Mindestwert) 2048 (Empfehlung)

Die Primfaktoren *p* und *q* von *n* sollten die gleiche Größenordnung haben, aber nicht zu dicht beieinander liegen:

$$\varepsilon_1 < | \log_2(p) - \log_2(q) | < \varepsilon_2.$$

Als Anhaltspunkte für die Werte ε_1 und ε_2 werden hier $\varepsilon_1 \approx 0{,}1$ und $\varepsilon_2 \approx 30$ vorgeschlagen. Die Primfaktoren *p* und *q* sind zufällig und annähernd gleichverteilt aus der Menge der Faktorpaare zu wählen, die diese Nebenbedingungen erfüllen.

Der öffentliche Exponent *e* wird unter der Nebenbedingung $\mathrm{ggT}(e,(p-1)(q-1)) = 1$ unabhängig von *n* gewählt. Der zugehörige geheime Exponent *d* wird dann in Abhängigkeit von dem vorher festgelegten *e* berechnet, so dass $ed \equiv 1 \mod \mathrm{kgV}(p-1,q-1)$ gilt. Es wird empfohlen, $2^{16}+1 \leq e < 2^{256}$ zu wählen. Ab 2021 wird eine Wahl von *e* entsprechend dieser Vorgabe verpflichtend werden.

Bemerkungen:

- Die Forderung, dass *p* und *q starke* Primzahlen sein müssen (d. h. $p-1$ und $q-1$ haben große Primfaktoren etc.), erscheint im Hinblick auf die besten heute bekannten Faktorisierungsalgorithmen nicht mehr ausreichend begründet und daher verzichtbar. Bei einer zufälligen Wahl von p und q, die die sonstigen Anforderungen der vorliegenden Bekanntmachung erfüllt, ist die Wahrscheinlichkeit vernachlässigbar, dass bekannte

Faktorisierungsverfahren, die die Existenz kleiner Faktoren von *p-1* und *q-1* ausnutzen können, effizienter sind als die besten bekannten Angriffe auf Basis des Zahlkörpersiebs.

- Im Sinne einer zufälligen Wahl von *p* und *q* sind geringe Abweichungen von der Gleichverteilung unter allen in Frage kommenden Primzahlpaaren zulässig, solange keine Eigenschaften induziert werden, die das Faktorisierungsproblem wesentlich erleichtern könnten. Zum Beispiel ist es zulässig, in *p* und *q* die führenden zwei Bits zu setzen.
- Der öffentliche Exponent *e* kann zufällig gewählt werden. Auf der anderen Seite haben kleine öffentliche Exponenten den Vorteil, dass die Verifikation einer Signatur sehr schnell durchgeführt werden kann. Das hier verlangte Verfahren (zuerst Wahl von *e*, danach Wahl von *d*) soll gewährleisten, dass kleine geheime Exponenten ausgeschlossen werden können, siehe z.B. [18].
- In [3], Table 3-2 werden für 2048-Bit RSA eine Unter- und eine Obergrenze für *e* spezifiziert ($2^{16} + 1 \leq e < 2^{256}$). Diese Bekanntmachung schließt sich dem an. Die Einhaltung dieser Grenzen wird daher ab 2021 für qualifizierte RSA-Signaturen nach dieser Bekanntmachung verpflichtend.

Der Hashwert muss vor der Anwendung des geheimen Exponenten *d* auf die Bitlänge des Moduls formatiert werden. Das Formatierungsverfahren ist dabei sorgfältig zu wählen, siehe [13]. Bis 2022 geeignete Verfahren sind:

- RSA: „Signature Schemes with Appendix“ PSS aus [14] Abschn. 8.1 und 9.1,
- „DSI according to ISO/IEC 9796-2 with random number“ [15],
- „digital signature scheme 2“ und „digital signature scheme 3“ aus [19].

Das Formatierungsverfahren RSA: „Signature Schemes with Appendix“ PKCS1-v1_5 aus [14] Abschn. 8.2 und 9.2 ist noch bis Ende 2016 geeignet. Für Zertifikatssignaturen ist das PKCS1-v1_5-Format darüber hinaus bis Ende 2017 geeignet. Gleiche verlängerte Fristen (bis 2017) gelten für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen.

Es wird aber empfohlen, dieses Verfahren nicht mehr zu verwenden. Der Beweiswert der erstellten Signaturen ist bis Ende 2020 gegeben.

Bemerkung:

- Die Realisierung eines Formatierungsverfahrens – z.B. die Form der Arbeitsteilung zwischen einer Chipkarte, auf der die Potenzierung mit dem geheimen Schlüssel durchgeführt wird, und dem Hintergrundsystem – ist für die Sicherheit durchaus relevant und muss im Rahmen der Prüfung technischer Komponenten nach § 15 Abs. 7 und § 17 Abs. 4 SigG untersucht werden.
- Bei Verwendung von Verfahren, die einen zufälligen Salt-Wert von variabler Länge benötigen, wird empfohlen, die Länge des Salt-Wertes entsprechend der Länge der Hashfunktion zu wählen.

Zur Erzeugung der Primfaktoren siehe näher z.B. [1] und [5]. Insbesondere muss bei Nutzung eines probabilistischen Primzahltests mit hinreichender Wahrscheinlichkeit ausgeschlossen sein, dass p oder q in Wirklichkeit zusammengesetzte Zahlen sind. Als obere Schranke für diese Wahrscheinlichkeit wird der Wert 2^{-100} (siehe [1]; vergleiche aber auch [5] und [16]) empfohlen.

3.2. DSA

Die Bitlänge von p beträgt mindestens 2048 Bit. Bis **Ende 2015** muss die Bitlänge des Parameters q mindestens 224 Bit betragen. **Ab Anfang 2016** sind für q mindestens 256 Bit notwendig. Mittelfristig wird empfohlen, für DSA-Schlüssel eine Länge von mindestens 3000 Bit anzustreben. Es ist vorgesehen, die Eignung von DSA-Schlüsseln mit unter 3000 Bit Schlüssellänge nicht über das Jahr 2022 hinaus zu verlängern.

Da die Berechnung diskreter Logarithmen in endlichen Körpern erheblich beschleunigt werden kann durch Vorberechnungen, die nur von dem verwendeten endlichen Körper abhängig sind, wird darüber hinaus empfohlen, Schlüssellängen unter 3000 Bit nicht mehr einzusetzen in Fällen, in denen eine große Anzahl von Nutzern mit einem gemeinsamen Grundkörper arbeitet.

Die folgende Tabelle fasst die Bitlängen für den DSA zusammen.

Tabelle 2: Geeignete Schlüssellängen für DSA

Parameter \ Zeitraum	bis Ende **2022**
p	2048
q	256

Bemerkungen:

- Zur Erzeugung von p und der weiteren Parameter siehe [1]; die Wahrscheinlichkeit, dass p oder q zusammengesetzt sind, soll kleiner als 2^{-100} sein.
- In FIPS-186 [1] werden konkrete Werte für die Bitlängen von p und q vorgegeben.
- Relativ kurze Bitlängen des Parameters q erlauben die Konstruktion von „Kollisionen“ im Sinne von Vaudenay [11] bei der Parametergenerierung. Diese Kollisionen haben jedoch in der Praxis der qualifizierten Signaturen keine Bedeutung. Soll dessen ungeachtet die Möglichkeit, diese Kollisionen konstruieren zu können, grundsätzlich ausgeschlossen werden, muss q größer als der maximal mögliche Hashwert sein.

3.2.a) DSA-Varianten basierend auf Gruppen $E(F_p)$

Um die Systemparameter festzulegen, werden eine elliptische Kurve E und ein Punkt P auf $E(F_p)$ erzeugt, so dass folgende Bedingungen gelten:

- Es ist $ord(P) = q$ mit einer von p verschiedenen Primzahl q.
- Für $r_0 := \min(r : q \text{ teilt } p^r - 1)$ gilt $r_0 > 10^4$.
- Die Klassenzahl der Hauptordnung, die zum Endomorphismenring von E gehört, ist mindestens 200.

Für den Parameter p gibt es keine Einschränkungen. Die Länge von q muss mindestens 224 Bit betragen, und **ab Anfang 2016** sind für q mindestens 250 Bit erforderlich.

Die folgende Tabelle fasst die Bitlängen für DSA-Varianten basierend auf Gruppen $E(F_p)$ zusammen.

Tabelle 3: Geeignete Schlüssellängen für DSA-Varianten in $E(F_p)$

Parameter \ Zeitraum	bis Ende **2015**	bis Ende **2022**
p	keine Einschränkung	keine Einschränkung
q	224	250

Bemerkung:

- Die untere Abschätzung für r_0 hat den Sinn, Attacken auszuschließen, die auf einer Einbettung der von P erzeugten Untergruppe in die multiplikative Gruppe eines Körpers F_{p^r} beruhen. In der Regel (bei zufälliger Wahl der elliptischen Kurve) ist diese Abschätzung erfüllt, denn r_0 ist die Ordnung von p (mod q) in F_q^* und hat deshalb im Allgemeinen sogar dieselbe Größenordnung wie q. Im Idealfall sollte r_0 explizit bestimmt werden, was allerdings die etwas aufwändige Faktorisierung von $q-1$ voraussetzt. Demgegenüber ist $r_0 > 10^4$ wesentlich schneller zu verifizieren und wird in diesem Zusammenhang als ausreichend angesehen. Für weitere Erläuterungen zu den Bedingungen und Beispielkurven siehe [20] und [23].
- Die Hashwerte müssen, falls ihre Bitlänge die von q übersteigt, auf die Bitlänge von q gekürzt werden. Dazu wird [10] eine geeignete Anzahl niederwertiger Bits abgeschnitten. Vergleiche auch die entsprechende Bemerkung im nächsten Abschnitt. Im Hinblick auf „Kollisionen“ im Sinne von [11] gelten die in Abschnitt 3.2 für DSA formulierten Bemerkungen hier ebenso. Die Verifikation der am Beginn dieses Abschnitts angegebenen Bedingungen an die Systemparameter bedeutet einen gewissen Aufwand. Es liegt daher nahe, Kurven zu verwenden, die bereits auf ihre Eignung hin untersucht wurden. Die in [23] angegebenen Kurven brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 und brainpoolP512t1 sind geeignet bis Ende 2022.
- Der Leitfaden [28] (Anlage zu [29]) definiert Minimalanforderungen zur Resistenz von Implementierungen elliptischer Kurven über F_p gegenüber Seitenkanalangriffen.

3.2.b) DSA-Varianten basierend auf Gruppen $E(F_{2^m})$

Um die Systemparameter festzulegen, werden eine elliptische Kurve E und ein Punkt P auf $E(F_{2^m})$ erzeugt, so dass folgende Bedingungen gelten:

- m ist prim.
- $E(F_{2^m})$ ist nicht über F_2 definierbar (d. h. die j-Invariante der Kurve liegt nicht in F_2).
- Es ist $ord(P) = q$ mit q prim.
- Für $r_0 := \min(r : q \text{ teilt } 2^{mr}-1)$ gilt $r_0 > 10^4$.
- Die Klassenzahl der Hauptordnung, die zum Endomorphismenring von E gehört, ist mindestens 200.

An den Parameter *m* werden keine Bedingungen gestellt. **Ab Anfang 2016** sind für *q* mindestens 250 Bit erforderlich. Bis Ende 2015 ist ein *q* von mindestens 224 Bit Länge noch ausreichend.

Die folgende Tabelle fasst die Bitlängen für DSA-Varianten basierend auf Gruppen $E(F_{2^m})$ zusammen.

Tabelle 4: Geeignete Schlüssellängen für DSA-Varianten in elliptischen Kurven über Körpern der Charakteristik 2

Parameter \ Zeitraum	bis Ende **2022**
m	keine Einschränkung
q	250

Bemerkungen:

- In Bezug auf die oben erwähnten 'Kollisionen' im Sinne von [11] gilt für die auf elliptischen Kurven basierenden Verfahren dasselbe wie für DSA.
- Ist bei der Berechnung der zweiten Signaturkomponente *s* die Bitlänge des Hashwerts größer als die Bitlänge des Moduls *q*, werden in [10] die überzähligen niederwertigen (rechten) Bits des Hashwerts abgeschnitten. Dies betrifft DSA und DSA-Varianten, die auf Gruppen $E(F_p)$ oder $E(F_{2^m})$ basieren.
- Bei DSA und bei elliptischen Kurven könnte die Wahl bestimmter, ganz spezieller Parameter möglicherweise dazu führen, dass das Verfahren schwächer ist als bei einer zufälligen Wahl der Parameter. Unabhängig davon, wie gravierend man diese Bedrohung einschätzt, kann man dem „Unterschieben“ schwacher Parameter vorbeugend dadurch begegnen, dass bei der Konstruktion der Parameter eine geeignete Einwegfunktion, d.h. eine der oben genannten Hashfunktionen, angewandt wird und die Parameter zusammen mit einer nachvollziehbaren entsprechenden Berechnung übergeben werden. Konkrete Vorschläge sind in [1], [10], [20] und [23] zu finden.

4. Erzeugung von Zufallszahlen

Zur Erzeugung von Systemparametern für Signaturverfahren und zur Schlüsselgenerierung werden Zufallszahlen benötigt. Bei DSA-ähnlichen Signaturverfahren wird bei der Generierung jeder Signatur eine neue Zufallszahl benötigt. Für diese Zwecke müssen geeignete Zufallszahlengeneratoren eingesetzt werden.

Die ehemaligen mathematisch-technischen Anlagen [30] und [31] zur AIS 20 [7] bzw. AIS 31 [17] wurden im September 2011 durch die mathematisch-technische Anlage [32] ersetzt. Die für den Algorithmenkatalog relevanten Funktionalitätsklassen wurden (unter neuem Namen) im Wesentlichen beibehalten, und es sind neue Funktionalitätsklassen hinzugekommen, u.a. hybride deterministische Zufallszahlengeneratoren (Funktionalitätsklasse DRG.4) und hybride physikalische Zufallszahlengeneratoren (Funktionalitätsklasse PTG.3). Insbesondere für die Erzeugung der in (EC)DSA und Varianten dieses Verfahrens benötigten Ephemeralschlüssel wird die Verwendung von Zufallsgeneratoren der Klassen DRG.4 und PTG.3 empfohlen.

Neben Zufallszahlengeneratoren, die nach den neuen Evaluierungskriterien [32] evaluiert werden, können **bis 2020** auch weiterhin Zufallszahlengeneratoren eingesetzt werden, die nach den alten Evaluierungskriterien evaluiert wurden. Soweit für den Algorithmenkatalog

relevant, stellt die nachfolgende Tabelle den neuen Funktionalitätsklassen die entsprechenden alten Funktionalitätsklassen gegenüber. Dies sind keine exakten 1-1-Beziehungen, da die Anforderungen der Funktionalitätsklassen zwar sehr ähnlich, aber nicht identisch sind. Die Anforderungen an die neuen Funktionalitätsklassen sind in einzelnen Aspekten weitergehend.

Tabelle 5: Gegenüberstellung der alten und neuen Funktionalitätsklassen für Zufallsgeneratoren nach AIS20/31

neue Funktionalitätsklasse [32]	alte Funktionalitätsklasse [30] bzw. [31]
PTG.2	P2
PTG.3	kein Pendant
DRG.2	K3
DRG.3	K4
DRG.4	kein Pendant

Bemerkungen:

- Hybride Zufallszahlengeneratoren vereinen Sicherheitseigenschaften von deterministischen und physikalischen Zufallszahlengeneratoren.
- Die Sicherheit eines hybriden deterministischen Zufallszahlengenerators der Klasse DRG.4 beruht in erster Linie auf der Komplexität des deterministischen Anteils, welcher der Klasse DRG.3 angehört. Während der Nutzung des Zufallszahlengenerators wird zusätzlich immer wieder neuer Zufall hinzugefügt. Dies kann (z.B.) in regelmäßigen Abständen oder auf die Anforderung einer Applikation hin erfolgen.
- Hybride physikalische Zufallszahlengeneratoren der Klasse PTG.3 besitzen neben einer starken Rauschquelle eine starke kryptographische Nachbearbeitung mit Gedächtnis.
- PTG.3 stellt die stärkste Funktionalitätsklasse in [32] dar.
- Die Konformität zur Funktionalitätsklasse PTG.3 kann mit einem PTG.2-konformen Zufallsgenerator mit geeigneter kryptographischer Nachbearbeitung mit Gedächtnis erreicht werden (vgl. [32], Abschnitt 4.5, Paragraph 304 und Punkt PTG 3.6 in FCS_RNG 1.1, Paragraph 305).

4.1. Anforderungen an die Eignung von Zufallsgeneratoren

Allgemeine Anforderungen

Grundsätzlich werden Zufallszahlengeneratoren als geeignet angesehen, die einer der folgenden Klassen angehören:

- Physikalische Zufallszahlengeneratoren: P2 (mit Resistenz gegen hohes Angriffspotential), PTG.2, PTG.3. P2-Zufallsgeneratoren sind dabei nur geeignet bis zum Jahr 2020. Ausnahmen hiervon werden in Abschnitt 4.3. definiert.
- Deterministische Zufallszahlengeneratoren: DRG.3, DRG.4 mit mindestens 100 Bit Seed-Entropie (siehe [32], Absatz 248 und auch [32], Absatz 332, insbesondere die letzte Zeile

von Tabelle 12). Daneben bis 2020 K4 (Resistenz gegen hohes Angriffspotential) mit mindestens 100 Bit Seed-Entropie.

Neben diesen allgemeinen Anforderungen sind die im Rest dieses Abschnitts enthaltenen Hinweise zu Randbedingungen und Spezialfällen sowie die Übergangsregelungen aus Abschnitt 4.3 zu beachten.

Es ist geplant, die Eignung von Zufallsgeneratoren mit weniger als 120 Bit Seed-Entropie Ende 2022 auslaufen zu lassen. Näheres hierzu findet sich in Abschnitt 7.3 der vorliegenden Bekanntmachung.

Randbedingungen und Spezialfälle

Für deterministische Zufallsgeneratoren der Klassen DRG.3 und DRG.4 bezieht sich die Forderung nach mindestens 100 Bit Seed-Entropie auf die Min-Entropie des Seeds, siehe auch [32], Absatz 332, Tabelle 12. Wird der deterministische Zufallsgenerator durch eine PTG.2-konforme physikalische Zufallsquelle initialisiert, dann kann zur Abschätzung der Min-Entropie auf die in Absatz 332 von [32] wiedergegebenen Kriterien zurückgegriffen werden.

Zur Erzeugung qualifizierter elektronischer Signaturen (keine Zertifikatssignaturen) kann ein deterministischer Zufallszahlengenerator der Klasse DRG.2 oder (bis 2020) K3 hoch verwendet werden, sofern der Antragssteller nachvollziehbar begründen kann, dass das Fehlen der DRG.3-spezifischen bzw. der K4-spezifischen Eigenschaft (enhanced backward secrecy) in den vorgesehenen Einsatzszenarien keine zusätzlichen Sicherheitsrisiken impliziert. Auch in diesem Fall ist eine Seed-Entropie von mindestens 100 Bit sicherzustellen (siehe [32], Absatz 248 und 332 wie oben).

Sind die Anforderungen an die Zufallszahlengeneratoren nicht erfüllt, muss das entsprechende Verfahren zur qualifizierten elektronischen Signatur als potenziell unsicher angesehen werden.

Eine aussagekräftige Bewertung eines Zufallszahlengenerators setzt umfassende Erfahrungen voraus. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügt über solche Erfahrungen. Bei Bedarf kann in diesem Zusammenhang auf das Know-how des BSI zurückgegriffen werden.

Bemerkungen:

- Die Ableitung von Signaturschlüsseln, Ephemeralschlüsseln und Primzahlen (für RSA) aus den erzeugten Zufallszahlen soll mit geeigneten Algorithmen erfolgen (zu elliptischen Kurven vgl. [28], Abschnitte 5.2 und 5.5.1). Vereinfacht gesagt, sollte einem potentiellen Angreifer so wenig Information über die abgeleiteten (geheim zu haltenden) Werte zur Verfügung stehen wie möglich. Im Idealfall treten alle Werte innerhalb des jeweilig zulässigen Wertebereichs mit derselben Wahrscheinlichkeit auf, und zu verschiedenen Zeitpunkten oder durch unabhängige Instanzen des Generierungsprozesses erzeugte Zufallszahlen sollten zumindest keine praktisch ausnutzbaren Zusammenhänge aufweisen.
- Ebenso wie die Signaturalgorithmen kann auch die Erzeugung geheim zu haltender Signaturschlüssel, Ephemeralschlüssel und Primzahlen Ziel von Seitenkanalangriffen werden ([27], [28] etc.). Dieser Aspekt wird in [32] explizit angesprochen.
- Auch im Hinblick auf Implementierungsangriffe vereinen hybride Zufallszahlengeneratoren Sicherheitseigenschaften von deterministischen und physikalischen Zufallszahlengeneratoren.

4.2 Empfehlungen zur Verwendung von Zufallsgeneratoren

Im Gegensatz zu den in Abschnitt 4.1 wiedergegebenen Anforderungen sind die im vorliegenden Abschnitt aufgeführten Empfehlungen zur Verwendung von Zufallsgeneratoren in Signaturerstellungseinheiten nicht bindend. Ihre Befolgung wird aber im Sinne des Zieles, ein hohes Sicherheitsniveau für alle Anwender qualifizierter elektronischer Signaturen zu erreichen, als sinnvoll erachtet.

Unabhängig von den Inhalten in Abschnitt 4.3, insbesondere also unabhängig von den dort wiedergegebenen Übergangsregelungen, wird Zertifizierungsdiensteanbietern empfohlen, für die Erzeugung ihrer Langzeitschlüssel und für die Erzeugung von Ephemeralschlüsseln in DSA-ähnlichen Verfahren einen Zufallsgenerator zu verwenden, der der Klasse PTG.3 oder DRG.4 angehört (PTG.3 dabei auf Grund des höheren Sicherheitsniveaus dieser Klasse prinzipiell bevorzugt).

Zur Erzeugung von Ephemeralschlüsseln (DSA, EC-DSA, EC-GDSA, ECKDSA) wird empfohlen, einen Zufallszahlengenerator zu wählen, der einer der folgenden Klassen angehört: PTG.3, DRG.3, DRG.4 oder K4 hoch (vgl. auch [28]). Hintergrund ist, dass Zufallszahlen, die von PTG.2- oder P2-konformen Zufallszahlengeneratoren erzeugt wurden, z.B. gewisse Schiefen aufweisen können. Es sind gegenwärtig keine Angriffe bekannt, die dies ausnutzen könnten. Vielmehr ist dies eine grundsätzliche Sicherheitsmaßnahme. Bei Verwendung eines deterministischen Zufallsgenerators wird eine Seed-Entropie von 120 Bit oder mehr empfohlen.

Soweit für die Erzeugung von Padding-Werten in den als geeignet eingestuften RSA-Signaturverfahren Zufallszahlen benötigt werden, wird die Verwendung von Zufallsgeneratoren der Funktionalitätsklassen NTG.1, PTG.2, PTG.3, DRG.2, DRG.3, DRG.4, P2, K3 oder K4 nach [32] empfohlen.

Es wird allen Betroffenen empfohlen, die in Abschnitt 7.3 beschriebenen Planungen hinsichtlich der Weiterentwicklung der vorliegenden Bekanntmachung frühzeitig zu berücksichtigen.

4.3 Übergangsregelungen und besondere Fälle

Anforderungen für EC-DSA-Signaturen

Mit Bezug auf die Erzeugung von Ephemeralschlüsseln bei der Erstellung von Signaturen in DSA-ähnlichen Verfahren (DSA, EC-DSA, EC-GDSA, EKCDSA) läuft die Eignung von Zufallsgeneratoren der Klasse PTG.2 mit dem Jahr 2020 aus. Ab dem Jahr 2021 sind somit bei der Erstellung von (EC)DSA-Signaturen nur noch Zufallsgeneratoren der Funktionalitätsklassen DRG.3, DRG.4 und PTG.3 geeignet.

Besondere Anforderungen für Zertifizierungsdiensteanbieter

Zertifizierungsdiensteanbieter müssen im Grundsatz seit 2015 Zufallsgeneratoren der Klasse PTG.3 oder DRG.4 für die Erstellung ihrer Langzeitschlüssel und für die Erstellung von Signaturen mit DSA-ähnlichen Verfahren nutzen. Davon ausgenommen sind in *bestehenden* Systemen von Zertifizierungsdiensteanbietern zur Erzeugung von Zufallszahlen bereits eingesetzte Produkte und Systemkomponenten: diese können weiterbetrieben werden, bis ihre Eignung nach Maßgabe der allgemeinen Anforderungen an die Erstellung qualifizierter elektronischer Signaturen ausläuft oder eine Erneuerung der Bestätigung dieser Produkte und Systemkomponenten notwendig wird. Sobald also eines der beiden vorgenannten Kriterien erfüllt ist, muss auf eine Zufallszahlenerzeugung unter Verwendung eines PTG.3-RNG oder eines DRG.4-RNG umgestellt werden.

Hoheitliche Dokumente

In hoheitlichen Dokumenten, die gleichzeitig eine Signaturkartenfunktion besitzen, können Zufallsgeneratoren, die nach [31] zertifiziert wurden, weiter genutzt werden, bis das hoheitliche Dokument seine Gültigkeit verliert oder bis die Eignung des verwendeten Signaturverfahrens aus anderen Gründen erlischt. Selbstverständlich gilt diese Bestandsschutzregelung nur vorbehaltlich der Möglichkeit, dass konkrete Schwächen in den Zufallsgeneratoren dieser Karten erkannt werden, für die eine Auswirkung auf die Sicherheit der Signaturkartenfunktion angenommen werden muss.

Sonstige Ausnahmeregelungen

Ähnliche Ausnahmeregelungen, wie sie im vorigen Absatz für hoheitliche Dokumente definiert wurden, können unter Umständen auch für andere Typen von weit verbreiteten Dokumenten erwogen werden. Gegenwärtig ist die Einführung weiterer entsprechender Regelungen aber nicht geplant. Entsprechende Kommentare können für den Algorithmenkatalog 2017 an die in Abschnitt 7.1 benannten Adressen gerichtet werden. Hierbei sind für eine Berücksichtigung mindestens folgende Punkte darzulegen:

1. Die entsprechenden Signaturkarten wurden vor dem Jahr 2015 bereits ausgegeben und befinden sich in großer Anzahl im Einsatz.
2. Die Karten besitzen, ähnlich wie es bei hoheitlichen Dokumenten der Fall ist, eine wesentliche andere Funktion außer der Funktion als Signaturkarte, und aus diesem Grund wäre ein Austausch mit unverhältnismäßigem Aufwand verbunden.
3. Die andere Funktion muss über das Jahr 2020 hinausreichen. Speziell ein Austausch der ausgegebenen Karten vor dem Jahr 2020 muss mit großem Aufwand verbunden sein.

5. Zeitraum und Verfahren zur langfristigen Datensicherung

Damit eine qualifizierte elektronische Signatur auch nach Überschreiten der Eignungsfrist eines Algorithmus, auf dessen Sicherheit die Signatur beruht, ihren Beweiswert erhält und sicher verifiziert werden kann, müssen vor Überschreiten dieser Frist geeignete Maßnahmen nach § 17 SigV getroffen werden. Dazu gehören qualifizierte Zeitstempel, die rechtzeitig vor Überschreiten der Frist erzeugt werden und deren Sicherheit auf längerfristig geeigneten Algorithmen beruht. Vor Überschreiten der Eignungsfrist eines Algorithmus, auf dessen Sicherheit ein solcher qualifizierter Zeitstempel beruht, muss dann dieser wiederum mit einem qualifizierten Zeitstempel längerfristiger Sicherheit versehen werden und so weiter. Die Technische Richtlinie [34] befasst sich mit der langfristigen Beweiswerterhaltung kryptographisch signierter Dokumente.

Statt für jedes einzelne qualifiziert signierte elektronische Datum einen Zeitstempel zu erzeugen, bietet es sich aus Effizienzgründen an, einen einzigen qualifizierten Zeitstempel jeweils für mehrere qualifiziert signierte elektronische Daten zugleich zu erzeugen. Ein geeignetes Verfahren dieser Art ist die Erzeugung so genannter Evidence Records für die qualifizierten elektronischen Signaturen gemäß [22]. Bei der Erzeugung eines solchen Evidence Records wird unter anderem ein Hashbaum erstellt. Für die dafür verwendete Hashfunktion wird hier sowohl die Kollisionsresistenz als auch die Einwegeigenschaft verlangt. Es sind dieselben Algorithmen hierfür geeignet wie für die Erzeugung qualifizierter elektronischer Signaturen. Auch die Eignungsfristen sind identisch.

In Anwendungen, in denen etwa aufgrund sehr langfristig ausgelegter Sicherheitsziele die Integrität der zu sichernden Daten über mehrere voneinander unabhängige Mechanismen sichergestellt werden soll, liegt es nahe, hierfür strukturell verschiedene Mechanismen zu verwenden. Zum Beispiel wäre es daher bei der Implementierung zweier voneinander unabhängiger Hashbäume für die gleichen zu schützenden Daten sinnvoller, einen der beiden Hashbäume auf SHA-2 basieren zu lassen und den anderen auf SHA-3, als für beide unterschiedliche Vertreter der SHA-2-Familie zu nutzen.

6. Nicht mehr geeignete kryptographische Algorithmen

In diesem Abschnitt sind alle kryptographischen Algorithmen mit Schlüssellängen und Parametergrößen aufgeführt, die jemals zur Erstellung von qualifizierten elektronischen Signaturen und qualifizierten Zertifikaten geeignet waren und diese Eignung inzwischen aber verloren haben. Diese Algorithmen werden auch weiterhin zur Prüfung von Signaturen oder Zertifikaten benötigt. Dazu müssen diese Algorithmen von den Signaturanwendungskomponenten unterstützt werden.

Die nachfolgenden Tabellen enthalten den letzten Zeitpunkt, an dem der jeweilige Algorithmus mit der angegebenen Schlüssellänge bzw. Parametergröße zur *Erzeugung* qualifizierter elektronischer Signaturen und qualifizierter Zertifikate geeignet war bzw. eine Übergangsfrist endete. (Bei RSA 1024 und SHA-1 wurden Übergangsfristen von 3 bzw. 6 Monaten eingeräumt.) Bei den Hashfunktionen werden zusätzlich die Zeitpunkte angegeben, an denen die Eignung zur *Prüfung* qualifizierter elektronischer Zertifikate erlischt, d.h., bis kurz vor diesem Zeitpunkt ist zur Erhaltung des Beweiswertes für qualifizierte Zertifikate keine Maßnahme nach Kap. 5 notwendig. Andere Daten besitzen dagegen keine gültige qualifizierte elektronische Signatur mehr, falls nicht vor Ablauf der angegebenen Eignungsfristen geeignete Maßnahmen zur Erhaltung des Beweiswertes der Signaturen ergriffen wurden.

Hashfunktionen

Tabelle 6: Nicht mehr geeignete Hashfunktionen

Hashfunktion	geeignet bis
SHA-1	Ende Juni 2008* Ende 2010** Ende 2015***
RIPEMD-160	Ende 2010 Ende 2015***
SHA-224	Ende 2015

* Januar – Juni 2008: Übergangsfrist

** nur noch zur Erzeugung qualifizierter Zertifikate (im Jahr 2010 zusätzlich unter der Auflage von einer Entropie ≥ 20 Bit in der Seriennummer)

*** nur noch zur *Prüfung* qualifizierter Zertifikate

RSA

Tabelle 7: Nicht mehr geeignete RSA-Schlüssellängen

Modullänge *n*	geeignet bis
768	Ende 2000
1024	Ende März 2008*
1280	Ende 2008
1536	Ende 2009
1728	Ende 2010

* Januar – März 2008: Übergangsfrist

DSA

Tabelle 8: Nicht mehr geeignete DSA-Parameter

Parameter *p*	Parameter *q*	geeignet bis
1024	160	Ende 2007
1280	160	Ende 2008
1536	160	Ende 2009
2048	160	Ende 2009
2048	224	Ende 2015

DSA-Varianten basierend auf Gruppen $E(F_p)$

Tabelle 9: Nicht mehr geeignete EC-Parameter über F_p

Parameter *p*	Parameter *q*	geeignet bis
keine Einschränkung	160	Ende 2006
192	180	Ende 2009
keine Einschränkung	224	Ende 2015

DSA-Varianten basierend auf Gruppen $E(F_{2^m})$

Tabelle 10: Nicht mehr geeignete EC-Parameter über binären Körpern

Parameter *m*	Parameter *q*	geeignet bis
Keine Einschränkung	160	Ende 2006
191	180	Ende 2009
Keine Einschränkung	224	Ende 2015

7. Ausblick auf künftige Entwicklungen

In diesem Kapitel soll kurz eingegangen werden auf die künftige Weiterentwicklung der vorliegenden Bekanntmachung. Ziel dieses Abschnittes ist es damit einerseits, die Planungssicherheit für Anwender, Zertifizierungsdiensteanbieter und Hersteller von Hard- und Software für die Erstellung und Prüfung qualifizierter elektronischer Signaturen zu erhöhen, und andererseits, den genannten Gruppen eine frühzeitige Rückmeldung zu geplanten Änderungen in der vorliegenden Bekanntmachung zu ermöglichen.

7.1. Langfristige Streichung wenig genutzter Algorithmen aus dem Algorithmenkatalog

Es ist vorgesehen, künftig Algorithmen die Eignung zur Erstellung qualifizierter elektronischer Signaturen auch ohne Vorliegen bekannter Sicherheitsschwächen zu entziehen, wenn davon ausgegangen wird, dass die Verfahren keine oder fast keine praktische Bedeutung haben. Dieser Schritt beruht auf der allgemeinen Überlegung, dass diese Algorithmen im Allgemeinen wesentlich weniger intensiv kryptoanalytisch untersucht wurden bzw. werden, als es für Algorithmen der Fall ist, die tatsächlich breite Anwendung finden.

Dieses Verfahren wird in keinem Fall zu einer Streichung eines Algorithmus vor Ablauf der in dieser Bekanntmachung angegebenen Eignungsfristen führen. Außerdem wird die Streichung eines Algorithmus aus solchen Gründen an dieser Stelle mit einem Vorlauf von etwa

18 Monaten angekündigt werden, um der Öffentlichkeit Gelegenheit zur Kommentierung zu geben. Algorithmen, deren Abkündigung auf diesem Wege beschlossen wurde, werden zukünftig in Abschnitt 8 dieser Bekanntmachung aufgelistet.

Es wurde beschlossen, folgendes Verfahren auf diese Weise auslaufen zu lassen:

- Nyberg-Rueppel-Signaturen [6], [19] (nur noch geeignet bis Ende 2020).

Das Auslaufen der Eignung von Nyberg-Rueppel-Signaturen ist für Ende 2020 vorgesehen. Ehemalige, gegenwärtige und (potentielle) zukünftige Anwender von Nyberg-Rueppel-Signaturen werden weiterhin um Rückmeldung hierzu an die Bundesnetzagentur und an das Bundesamt für Sicherheit in der Informationstechnik gebeten, genauer an die folgenden beiden Adressen:

Bundesnetzagentur **Referat IS 15** **Postfach 8001** **D-55003 Mainz** **E-Mail: qes@bnetza.de**	**Bundesamt für Sicherheit in der Informationstechnik** **Referat KT23** **Postfach 200363** **D-53133 Bonn** **E-Mail: algokat@bsi.bund.de**

7.2. Weiterentwicklung der Anforderungen an RSA-Signaturen

Es ist vorgesehen, beim Einsatz von RSA-Signaturen die Verwendung von öffentlichen Exponenten, die kleiner als $2^{16}+1$ oder größer als 2^{256} sind, ab dem Jahr 2021 nicht mehr zu gestatten. Die Eignung von RSASSA-PKCS-1v1_5 läuft Ende 2016 aus.

7.3. Mittelfristige Anhebung des generellen Sicherheitsniveaus der Verfahren zur Erstellung qualifizierter elektronischer Signaturen

Es ist geplant, in Verfahren zur Erzeugung qualifizierter elektronischer Signaturen beginnend mit dem Algorithmenkatalog 2017 und unter Wahrung der Restlaufzeiten der bislang als geeignet eingestuften Verfahren global ein Sicherheitsniveau von 120 Bit zu etablieren. Dies hat insbesondere folgende Konsequenzen:

- Für Signaturverfahren, für die die besten bekannten Angriffe auf dem Problem der Faktorisierung großer Zahlen oder auf dem Problem der Berechnung diskreter Logarithmen in endlichen Körpern beruhen (RSA und DSA) werden Schlüssellängen von mindestens 3000 Bit verpflichtend werden.
- Für deterministische Zufallsgeneratoren werden eine Min-Entropie des Seeds von 120 Bit verpflichtend werden. Es wird eine Größe des inneren Zustands von 240 Bit empfohlen werden. Es ist vorgesehen, entsprechende Regelungen im Algorithmenkatalog 2017 zu verankern. Die Eignung von RSA- und DSA-Verfahren mit einer Schlüssellänge unterhalb von 3000 Bit sowie von Zufallsgeneratoren mit weniger als 120 Bit Seed-Entropie wird damit voraussichtlich Ende 2022 auslaufen.

8. Ohne Sicherheitsgründe abgekündigte Algorithmen

Es wurde beschlossen, die Eignung von Nyberg-Rueppel-Signaturen nur noch bis zum Jahr 2020 zu verlängern. Hierzu werden wie in Abschnitt 7.1 beschrieben weiterhin Rückmeldun-

gen durch alle hiervon betroffenen Parteien erbeten. Andere ohne Sicherheitsgründe abgekündigte Algorithmen gibt es derzeit nicht.

Literatur

[1] NIST: *FIPS Publication 186-4: Digital Signature Standard (DSS),* Juli 2013

[2] NIST: *FIPS Publication 180-4: Secure Hash Standard (SHS),* März 2012

[3] NIST: W. Polk, D. Dodson, W. Burr, H. Ferraiolo, D. Cooper, *Special Publication 800-78-3: Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* Dezember 2010

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

[5] IEEE P1363: *Standard specification for public key cryptography,* 2000

[6] ISO/IEC 9796-3:2006 *Information technology – Security techniques – Digital Signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms,* 2006

[7] AIS 20: *Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren,* Version 2.0, 19.09.2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf

[8] T. ElGamal: *A public key cryptosystem and a signature scheme based on discrete logarithms,* Crypto ’84, LNCS 196, S. 10-18, 1985

[9] R. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public key cryptosystems,* Communications of the ACM, vol. 21 no. 2, 1978

[10] ANSI X9.62:2005 *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (EC-DSA),* 2005.

[11] S. Vaudenay: *Hidden collisions in DSS,* Crypto’96, LNCS 1109, S. 83-88, 1996

[12] A. K. Lenstra, E. R. Verheul: *Selecting Cryptographic Key Sizes,* J. Cryptology 39, 2001

[13] J. S. Coron, D. Naccache, J. Stern: *On the Security of RSA padding*. Crypto 99, LNCS 1666, 1999

[14] PKCS #1 v2.2: *RSA Cryptography Standard*, 27.10.2012, http://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf

[15] DIN V66291: *Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV,* Annex A, 2.1.1, 2002

[16] ANSI X9.31:1998 *Digital signatures using reversible public key cryptography for the financial services industry (rDSA),* 1998

[17] AIS 31: *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren,* Version 2.0, 19.09.2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.pdf

[18] D. Boneh, G. Durfee: *Cryptanalysis of RSA with private key d less than* $N^{0.292}$. Eurocrypt '99, LNCS 1592, 1999

[19] ISO/IEC 9796-2:2010 *Information technology – Security techniques – Digital Signature schemes giving message recovery – Part 2: Integer Factorization based mechanisms*, 2010

[20] ECC Brainpool (M. Lochter Hrsg.): *ECC Brainpool Standard Curves and Curve Generation*, v. 1.0 (19.10.05), http://www.ecc-brainpool.org/download/BP-Kurven-aktuell.pdf; Kurvenparameter als Binärdateien unter http://www.ecc-brainpool.org/ecc-standard.htm

[21] ISO/IEC 14888-2:2008 *Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms*, 2008

[22] IETF: RFC 4998, *Evidence Record Syntax (ERS)*, August 2007, http://www.ietf.org/rfc/rfc4998.txt

[23] IETF: RFC 5639, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*, März 2010, http://www.ietf.org/rfc/rfc5639.txt

[24] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG), Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) geändert worden ist. Siehe auch http://www.nrca-ds.de

[25] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), die zuletzt durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) geändert worden ist. Siehe auch http://www.nrca-ds.de

[26] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, P.L. Montgomery: *On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography* (version 2.1, 01.09.2009), http://eprint.iacr.org/2009/389

[27] T. Finke, M. Gebhardt, W. Schindler: *A New Side-Channel Attack on RSA Prime Generation*. CHES 2009, LNCS 5747, 2009

[28] W. Killmann, T. Lange, M. Lochter, W. Thumser, G. Wicke: *Minimum Requirements for Evaluating Side-Channel-Attack Resistance of Elliptic Curve Implementations*. Leitfaden, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_ECCGuide_e_pdf.pdf

[29] AIS 46: *Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren.* Version 2 (6.2.2013), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_pdf.pdf

[30] W. Schindler: *Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators*. Version 2.0, 02.12.1999, ehemalige mathematisch-technische Anlage zur AIS20, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_Functionality_Classes_Evaluation_Methodology_DRNG_e.pdf

[31] W. Killmann, W. Schindler: *A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators*. Version 3.1, 25.09.2001, ehemalige mathematisch-technische Anlage zur AIS 31, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_evaluation_methodology_for_true_RNG_e.pdf

[32] W. Killmann, W. Schindler: *A proposal for: Functionality classes for random number generators*. Version 2.0, 18.09.2011, mathematisch-technische Anlage zur AIS 20 und AIS 31, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf

[33] A. Roßnagel (Hrsg.): *Recht der Multimedia-Dienste*, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag, Beck Verlag, München 1999

[34] BSI Technische Richtlinie 03125: *TR-ESOR – Beweiswerterhaltung kryptographisch signierter Dokumente*, Version 1.2, 19.12.2014, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

[35] A. K. Lenstra: *Key Lengths*, in: H. Bigdoli (Hrsg.): *Handbook of Information Security*, John Wiley & Sons, 2006

[36] A. Joux: *Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions*, Crypto 2004, LNCS 3152, S. 306-316

[37] BSI, Technical Guideline TR 03111: Elliptic Curve Cryptography, Version 2.0, 28.6.2012, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.pdf

[38] NIST, FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, 2015, http://nvlpubs.nist.gov/nistpubs/fips/NIST.FIPS.202.pdf

Mainz, den 9.12.2015

IS 15

Bundesnetzagentur
für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Im Auftrag

Schwemmer