

# **Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen**

## **Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)**

**Vom 22. Dezember 2010**

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Behörde gemäß § 3 Signaturgesetz (SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091), veröffentlicht gemäß Anlage 1 Abschnitt 1 Nr. 2 Signaturverordnung (SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542), 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 2017 statt bis Ende 2016 aufgeführt sind. Normalerweise sind solche längerfristigen Prognosen schwer möglich. Neu hinzu gekommen ist der Abschnitt „Nicht mehr geeignete kryptographische Algorithmen“. Dort sind alle kryptographischen Algorithmen mit Schlüssellängen und Parametergrößen aufgeführt, die jemals zur Erstellung qualifizierter elektronischer Signaturen und qualifizierter Zertifikate geeignet waren.

Die Sicherheit einer qualifizierten elektronischen Signatur hängt primär von der Stärke der zugrunde liegenden Algorithmen ab. Im Folgenden werden Algorithmen genannt, die für qualifizierte elektronische Signaturen mindestens für die **kommenden sieben Jahre**<sup>1</sup> (d.h. bis Ende 2017<sup>1</sup>) als geeignet anzusehen sind. 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 Spe-

---

<sup>1</sup> Siehe Vorbemerkung

zifikationen 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.

## Inhaltsverzeichnis

1. KRYPTOGRAPHISCHE ANFORDERUNGEN .....	2
1.1. Hashfunktionen.....	3
1.2. Signaturverfahren.....	3
1.3. Schlüsselerzeugung .....	3
2. GEEIGNETE HASHFUNKTIONEN .....	3
3. GEEIGNETE SIGNATURVERFAHREN .....	4
3.1. RSA-Verfahren.....	5
3.2. DSA.....	6
3.2.a) DSA-Varianten basierend auf Gruppen $E(F_p)$ .....	7
3.2.b) DSA-Varianten basierend auf Gruppen $E(F_{2^m})$ .....	7
4. ERZEUGUNG VON ZUFALLSZAHLEN.....	8
5. ZEITRAUM UND VERFAHREN ZUR LANGFRISTIGEN DATENSICHERUNG .....	10
6. NICHT MEHR GEEIGNETE KRYPTOGRAPHISCHE ALGORITHMEN .....	11
LITERATUR.....	12

## 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 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. (Zwei unterschiedliche digitale Dokumente, die auf denselben Hashwert abgebildet werden, bilden 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. Dies ist aber nur eine Existenzaussage. Bei der praktischen Anwendung kommt es nur darauf an, dass es, wie oben verlangt, 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. Insbesondere bedeutet dies, dass es praktisch unmöglich ist, den Signaturschlüssel aus dem (öffentlichen) Signaturprüfschlüssel zu berechnen.

### 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.

Folgende Hashfunktionen mit verschiedenen Hashwert-Längen (SHA-224 ist eine 224-Bit Hashfunktion etc.) sind geeignet, ein langfristiges Sicherheitsniveau zu gewährleisten:

- SHA-256, SHA-384, SHA-512 [2].

Diese drei Hashfunktionen sind (mindestens) in den **kommenden sieben Jahren**, d.h. **bis Ende 2017**<sup>1</sup>, für die Anwendung bei qualifizierten elektronischen Signaturen geeignet. Die Hashfunktion SHA-224 [2] ist bis **Ende 2015** für die Anwendung bei qualifizierten elektronischen Signaturen geeignet.

Die folgende Tabelle fasst die Eignung der Hashfunktionen zusammen.

Erzeugung qualifizierter Zertifikate*: geeignet bis Ende <b>2010</b>	geeignet bis Ende <b>2010</b>	geeignet bis Ende <b>2015</b>	geeignet bis Ende <b>2017</b>
SHA-1	RIPEMD-160	SHA-224 (SHA-1, RIPEMD-160)**	SHA-256, SHA-384, SHA-512

\* d.h. zur Erzeugung qualifizierter Zertifikate mit mindestens 20 Bit Entropie der Seriennummer, nicht aber zur Erzeugung und Prüfung anderer qualifiziert signierter Daten.

\*\*ausschließlich zur Prüfung qualifizierter Zertifikate, aber nicht zu deren Erstellung oder zur Erzeugung und Prüfung anderer qualifiziert signierter Daten.

#### Bemerkungen:

- Der SHA-1 ist 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 nach gegenwärtigem Kenntnisstand hierfür keine Notwendigkeit besteht, wird dennoch empfohlen, dies auch dort als eine zusätzliche Sicherheitsmaßnahme einzuführen.
- 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 festgestellt werden. Die Anforderung ist vielmehr vom Zertifizierungsdiensteanbieter in seinem Betrieb zu erfüllen.

### 3. Geeignete Signaturverfahren

Im Jahr 1977 haben Rivest, Shamir und Adleman ein Verfahren zum Erzeugen und Verifizieren digitaler Signaturen explizit beschrieben. Es handelt sich um das nach seinen Erfindern benannte RSA-Verfahren [9]. 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 Punktgruppen  $E(K)$  elliptischer Kurven über endlichen Körpern  $K$  basieren, wobei  $K$  entweder ein endlicher Primkörper  $F_p$  oder ein endlicher Körper  $F_{2^m}$  der Charakteristik 2 ist.

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

1. RSA-Verfahren [23],
2. DSA [1], [4],
3. DSA-Varianten, basierend auf elliptischen Kurven. Insbesondere die Verfahren:
  - EC-DSA [1], [4], [5], [10], [11],
  - EC-KDSA, EC-GDSA [4], [11],
  - Nyberg-Rueppel-Signaturen [6], [19].

Die Sicherheit der oben genannten Verfahren beruht dabei entsprechend auf:

1. dem Faktorisierungsproblem für ganze Zahlen,
2. dem Diskreten-Logarithmus-Problem in der multiplikativen Gruppe eines Primkörpers  $F_p$ ,
3. dem Diskreten-Logarithmus-Problem in den Gruppen  $E(F_p)$  bzw.  $E(F_{2^m})$ .

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 beiden genannten Aspekte zugrunde gelegt werden, vgl. [13], [28]. Solche Prognosen sind nur für relativ kurze Zeiträume sinnvoll (und können sich natürlich jederzeit aufgrund unvorhersehbarer dramatischer Entwicklungen als falsch erweisen).

Im Folgenden bezeichnen wir mit der Bitlänge  $r$  einer Zahl  $x > 0$  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 2017**<sup>1</sup>, bei der im Folgenden festgelegten Wahl der Parameter gewährleistet.

### 3.1. RSA-Verfahren

Für den Zeitraum **bis Ende 2010** muss der Parameter  $n$  mindestens 1728 Bit lang sein. Ab **Anfang 2011** muss der Parameter  $n$  eine Länge von mindestens 1976 Bit haben. Empfohlen werden 2048 Bit.

Die folgende Tabelle fasst die minimalen Bitlängen zusammen.

Zeitraum	bis Ende <b>2010</b>	bis Ende <b>2017</b>
Parameter		
$n$	1728 (Mindestw.) 2048 (Empf.)	1976 (Mindestw.) 2048 (Empf.)

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  $\varepsilon_1$  und  $\varepsilon_2$  werden hier  $\varepsilon_1 \approx 0,1$  und  $\varepsilon_2 \approx 30$  vorgeschlagen. Die Primfaktoren  $p$  und  $q$  müssen unter Beachtung der genannten Nebenbedingungen zufällig und unabhängig voneinander erzeugt werden.

Der öffentliche Exponent  $e$  wird unabhängig von  $n$  unter der Nebenbedingung  $\text{ggT}(e, (p-1)(q-1)) = 1$  gewählt. Der zugehörige geheime Exponent  $d$  wird dann in Abhängigkeit von dem vorher festgelegten  $e$  berechnet, so dass  $ed \equiv 1 \pmod{\text{kgV}(p-1, q-1)}$  gilt. Es wird empfohlen,  $e \geq 2^{16} + 1$  zu wählen.

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 heute bekannten besten Faktorisierungsalgorithmen nicht mehr ausreichend begründet und daher verzichtbar.
- 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. [20].
- In [3], Table 3-2, sind Obergrenzen für  $e$  in Abhängigkeit von  $n$  spezifiziert.
- 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 [14]. Geeignete Verfahren sind zum Beispiel:
  - RSA: „Signature Schemes with Appendix“ PSS aus [15] Abschn. 8.1 und 9.1,
  - „DSI according to ISO/IEC 9796-2 with random number“ [16],
  - „digital signature scheme 2“ und „digital signature scheme 3“ aus [21].
  - Das Formatierungsverfahren RSA: „Signature Schemes with Appendix“ PKCS#1-v1\_5 aus [15] Abschn. 8.2 und 9.2 ist noch bis Ende 2014 geeignet. Zum Erzeugen von Zertifikatssignaturen ist das PKCS#1-v1\_5-Format darüber hinaus bis Ende 2016 geeignet. Es wird aber empfohlen, dieses Verfahren nicht über Ende 2013 hinaus zu verwenden.
- 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.
- Zur Erzeugung der Primfaktoren siehe z.B. [5] und [17]. Insbesondere muss bei Nutzung eines probabilistischen Primzahltests mit hinreichender Wahrscheinlichkeit ausgeschlossen sein, dass  $p$  oder  $q$  in Wirklichkeit zusammengesetzte Zahlen sind. Als Anhaltspunkt für eine obere Schranke für diese Wahrscheinlichkeit wird ab Anfang 2010 der Wert  $2^{-100}$  (siehe [1]; vergleiche aber auch [5] und [17]) vorgeschlagen.

**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. Die folgende Tabelle fasst die Bitlängen für den DSA zusammen.

Zeitraum	bis Ende <b>2015</b>	bis Ende <b>2017</b>
Parameter		
$p$	2048	2048
$q$	224	256

Bemerkungen:

- Zur Erzeugung von  $p$  und der weiteren Parameter siehe [1]; ab Anfang 2010 soll die Wahrscheinlichkeit, dass  $p$  oder  $q$  zusammengesetzt sind, 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 [12] bei der Parametergenerierung. Diese Kollisionen haben jedoch in der Praxis keine Bedeutung. Soll dessen ungeachtet die Möglichkeit, diese Kollisionen konstruieren zu können, ausgeschlossen werden, sind größere Bitlängen zu wählen.

**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:

- $ord(P) = q$  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.

Parameter \ Zeitraum	bis Ende <b>2015</b>	bis Ende <b>2017</b>
$p$	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  $p \pmod q$  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 [22] und [25].

**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  $F_2$ )
- $\text{ord}(P) = q$  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.

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

Parameter \ Zeitraum	bis Ende <b>2015</b>	bis Ende <b>2017</b>
$m$	keine Einschränkung	keine Einschränkung
$q$	224	250

#### Bemerkungen:

- In Bezug auf die oben erwähnten 'Kollisionen' im Sinne von [12] gilt für die auf elliptischen Kurven basierenden Verfahren dasselbe wie für DSA. Ist bei der Berechnung der zweiten Signaturkomponente  $s$  die Länge des Hashwerts größer als die Bitbreite des Moduls, 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.
- Beim 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], [22] und [25] zu finden.
- Referenz [30] adressiert Minimalanforderungen zur Resistenz von Implementierungen elliptischer Kurven gegenüber Seitenkanalangriffen.

## 4. Erzeugung von Zufallszahlen

Bei der Erzeugung von Systemparametern für Signaturverfahren und für die Schlüsselgenerierung werden Zufallszahlen gebraucht. Bei DSA-ähnlichen Signaturverfahren wird bei jeder Generierung einer Signatur eine neue Zufallszahl benötigt.

Für diese Zwecke bieten sich als Zufallszahlengeneratoren solche Systeme an, die

- eine physikalische Rauschquelle, die beispielsweise auf elektromagnetischen, elektro-mechanischen oder quantenmechanischen Effekten beruht, und
- ggf. eine algorithmische Nachbehandlung der digitalisierten Rauschsignale

besitzen. Die Eigenschaften der digitalisierten Rauschsignalfolge sollten sich hinreichend gut durch ein stochastisches Modell beschreiben lassen. Der physikalische Zufallszahlengenerator sollte ein P2-Generator (Stärke der Mechanismen bzw. Funktionen: hoch) im Sinne der AIS 31 [18] sein; ab Anfang 2011 ist diese Bedingung verbindlich, d. h. der Zufallszahlengenerator *muss* dann ein P2-Generator sein. Qualitativ bedeutet dies: Der durchschnittliche Entropiezuwachs pro Zufallsbit liegt oberhalb einer Mindestschranke. Die Zufallszahlen müssen im laufenden Betrieb statistischen Tests unterzogen werden („Onlinetests“). Der bzw. die Onlinetests sollten dem mathematischen Modell der Rauschquelle angepasst sein. Der bzw. die Onlinetests selbst und das Aufrufschema müssen geeignet sein, nicht akzeptable statistische Defekte oder Verschlechterungen der statistischen Eigenschaften der digitalisierte Rauschsignalfolge in angemessener Zeit zu erkennen. Auf einen Rauschalarm muss angemessen reagiert werden (z. B. weitere Tests, Stilllegen der Rauschquelle). Insbesondere muss ein etwaiger Totalausfall der Rauschquelle umgehend erkannt 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.

Als Alternative zu einem physikalischen Zufallszahlengenerator kommt ein Pseudozufallszahlengenerator in Frage. Der innere Zustand des Pseudozufallszahlengenerators wird durch den so genannten Seed initialisiert. In jedem Schritt wird der innere Zustand erneuert und hieraus eine Zufallszahl abgeleitet. Der innere Zustand des Pseudozufallszahlengenerators muss gegen Auslesen und Manipulation (physikalisch, durch Seitenkanalangriffe, über Schnittstelle etc.) ebenso sicher geschützt sein wie die geheimen Signaturschlüssel. Denn mit Kenntnis des inneren Zustands könnte ein potentieller Angreifer zumindest alle zukünftig erzeugten Zufallszahlen mühelos bestimmen.

Für Zertifizierungsdiensteanbieter wird die Verwendung eines physikalischen Zufallszahlengenerators empfohlen.

Jeder Pseudozufallszahlengenerator, der im Zusammenhang mit qualifizierten elektronischen Signaturen genutzt wird, muss grundsätzlich ein K4-DRNG mit Stärke der Mechanismen bzw. Funktionen „Hoch“ im Sinne der AIS 20 [7] sein (Ausnahme: vgl. unten), wobei die geforderte Mindest-Seedentropie über die AIS 20 hinaus geht (dort: 80 Bit). Qualitativ bedeutet dies:

- Es ist einem Angreifer nicht praktisch möglich, zu einer ihm bekannten Zufallszahlenteilfolge Vorgänger oder Nachfolger dieser Teilfolge oder gar einen inneren Zustand zu errechnen, oder diese mit einer Wahrscheinlichkeit zu erraten, die nichtvernachlässigbar über der Ratewahrscheinlichkeit ohne Kenntnis der Teilfolge liegt.
- Die Entropie des Seed beträgt mindestens 100 Bit; empfohlen wird eine Entropie von mindestens 120 Bit.
- (K4-spezifische Eigenschaft) Es ist einem Angreifer praktisch unmöglich, aus Kenntnis des inneren Zustands Vorgängerzufallszahlen oder innere Vorgängerzustände zu errechnen oder diese mit einer Wahrscheinlichkeit zu erraten, die nichtvernachlässigbar über der Ratewahrscheinlichkeit ohne Kenntnis des inneren Zustands liegt.

Ausnahme: Alternativ zur K4-spezifischen Eigenschaft genügt eine nachvollziehbare Begründung des Antragstellers, dass das Fehlen der K4-spezifischen Eigenschaft in den vorgesehenen Einsatzszenarien keine zusätzlichen Sicherheitsrisiken impliziert. Dann reicht

es aus, wenn der DRNG der Klasse K3, Stärke der Mechanismen bzw. Funktionen „hoch“, angehört.

Anderenfalls muss das entsprechende Verfahren zur qualifizierten elektronischen Signatur als potenziell unsicher angesehen werden.

Bemerkungen:

- Die Ableitung von Signaturschlüsseln, Ephemeralschlüsseln und Primzahlen (für RSA) aus den erzeugten Zufallszahlen soll mit geeigneten Algorithmen erfolgen. Vereinfacht gesagt, sollte einem potentiellen Angreifer so wenig Information über die abgeleiteten (geheim zu haltenden) Werte zur Verfügung stehen wie möglich. Im Idealfall sind alle Werte innerhalb der jeweilig zulässigen Wertebereiche gleich wahrscheinlich.
- Es ist vorgesehen, die AIS 20 und die AIS 31 im Jahr 2011 durch Neufassungen zu ersetzen. Die für den Algorithmenkatalog relevanten Klassen bleiben (unter neuem Namen) im Wesentlichen erhalten, und es kommen neue Klassen hinzu, u.a. hybride deterministische RNGs und hybride physikalische RNGs. Vereinfacht gesagt, wird hybriden deterministischen RNGs während der Nutzung immer wieder echter Zufall zugeführt, und hybride physikalische RNGs besitzen neben einer sicheren physikalischen RNG-Komponente eine starke deterministische (kryptographische) Nachbearbeitung mit Gedächtnis. Hybride RNGs vereinen (Sicherheits-)Eigenschaften von deterministischen und physikalischen RNGs. Wird zur Schlüsselerzeugung (einschließlich Ephemeralschlüssel) ein physikalischer RNG verwendet, wird empfohlen, zukünftig einen hybriden physikalischen RNG einzusetzen.
- Ebenso wie die Signaturalgorithmen kann auch die Erzeugung geheim zu haltender Signaturschlüssel, Ephemeralschlüssel und Primzahlen Ziel von Seitenkanalangriffen werden ([29] etc.).

## **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.

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 [24]. 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. Für die hier einzusetzenden Algorithmen gelten dieselben Eignungsfristen wie zur Erzeugung qualifizierter elektronischer Signaturen.

## 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 bzw. in Kürze mit Ende des Jahres 2010 verlieren werden. 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 endet. (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. Für alle anderen qualifiziert signierten Daten sind, falls ihr Beweiswert erhalten bleiben soll, dagegen Maßnahmen durchzuführen.

### Hashfunktionen

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

\* Januar – Juni 2008: Übergangsfrist

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

\*\*\* nur noch zur *Prüfung* qualifizierter Zertifikate

### RSA

Modullänge $n$	geeignet bis
756	Ende 2000
1024	Ende März 2008*
1280	Ende 2008
1536	Ende 2009
1736	Ende 2010

\* Januar – März 2008: Übergangsfrist

## DSA

Parameter $p$	Parameter $q$	geeignet bis
1024	160	Ende 2007
1280	160	Ende 2008
1536	160	Ende 2009
2048	160	Ende 2009

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

Parameter $p$	Parameter $q$	geeignet bis
keine Einschränkung	160	Ende 2006
192	160	Ende 2005
192	180	Ende 2009

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

Parameter $m$	Parameter $q$	geeignet bis
Keine Einschränkung	160	Ende 2006
191	160	Ende 2005
191	180	Ende 2009

## **Literatur**

- [1] NIST: *FIPS Publication 186-3: Digital Signature Standard (DSS)*, Juni 2009
- [2] NIST: *FIPS Publication 180-3: Secure Hash Standard (SHS)*, Oktober 2008
- [3] NIST: *Special Publication 800-78-2: Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, Februar 2010

- [4] ISO/IEC 14888-3: *Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*, 2006 (ersetzt entsprechende Inhalte von ISO/IEC-14888-3-1998)
- [5] IEEE P1363: *Standard specification for public key cryptography*, 2000
- [6] ISO/IEC 9796-3: *Information technology – Security techniques – Digital Signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*, 2006 (ersetzt ISO/IEC 9796-3-2000)
- [7] AIS 20: *Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*, Version 1, 2.12.99, samt mathematisch-technischem Anhang (Version 2.0, 2.12.99),  
[https://www.bsi.bund.de/cae/servlet/contentblob/478150/publicationFile/30276/ais20\\_pdf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/478150/publicationFile/30276/ais20_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 Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 2005. (ersetzt ANSI X9.62-1998)
- [11] ISO/IEC 15946-2: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*, 2002. (Zurückgezogen 7.11.2007; ersetzt durch [4] ISO/IEC 14888-3-2006.)
- [12] S. Vaudenay: *Hidden collisions in DSS*, Crypto'96, LNCS 1109, S. 83-88, 1996
- [13] A.K. Lenstra, E.R. Verheul: *Selecting Cryptographic Key Sizes*, J. Cryptology 39, 2001
- [14] J.-S. Coron, D. Naccache, J. Stern: *On the Security of RSA padding*. Crypto 99, LNCS 1666, 1999
- [15] PKCS #1 v2.1: *RSA Cryptographic Standard*, 14.6.2002
- [16] DIN V66291: *Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, Annex A*, 2.1.1, 1999
- [17] ANSI X9.31-1998: *Digital signatures using reversible public key cryptography for the financial services industry (rDSA)*, 1998
- [18] AIS 31: *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*, Version 1, 25.9.2001, samt mathematisch-technischem Anhang, (Version 3.1, 25.09.2001),  
[https://www.bsi.bund.de/cae/servlet/contentblob/478128/publicationFile/30271/ais31\\_pdf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/478128/publicationFile/30271/ais31_pdf.pdf) und  
[https://www.bsi.bund.de/cae/servlet/contentblob/478132/publicationFile/30239/trngkr31\\_pdf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/478132/publicationFile/30239/trngkr31_pdf.pdf)
- [19] ISO/IEC 15946-4: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery*, 2004 (zurückgezogen 7.11.2007; ersetzt durch [6] ISO/IEC 9796-3-2006)

- [20] D. Boneh, G. Durfee: *Cryptanalysis of RSA with private key  $d$  less than  $N^{0.292}$* . Eurocrypt '99, LNCS 1592, 1999
- [21] ISO/IEC 9796-2: *Information technology – Security techniques – Digital Signature schemes giving message recovery – Part 2: Integer Factorization based mechanisms*, 2002
- [22] ECC Brainpool: *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>
- [23] ISO/IEC 14888-2: *Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms*, 2008 (ersetzt entsprechende Inhalte von ISO/IEC-14888-3-1998)
- [24] IETF: *RFC 4998, Evidence Record Syntax (ERS) Standards Track*, August 2007, <http://www.ietf.org/rfc/rfc4998.txt>
- [25] IETF: *RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*, March 2010, <http://www.ietf.org/rfc/rfc5639.txt>
- [26] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG), <http://www.nrca-ds.de>
- [27] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), <http://www.nrca-ds.de>
- [28] 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>
- [29] T. Finke, M. Gebhardt, W. Schindler: *A New Side-Channel Attack on RSA Prime Generation*. CHES 2009, LNCS 5747, 2009
- [30] *Minimal Requirements for Evaluating Side-Channel-Attack Resistance of Elliptic Curve Implementations*. Leitfaden (Draft), erscheint in Kürze als Anhang zur AIS 46.
- [31] AIS 46: *Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren*. Version 1 (22.10.2010), [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretation/en/AIS\\_46\\_1\\_pdf.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretation/en/AIS_46_1_pdf.pdf?__blob=publicationFile)

Mainz, den 22.12.2010

IS 18

Bundesnetzagentur  
für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen  
Im Auftrag  
D r . W o h l m a c h e r