Empfehlung „Geeignete Kryptoalgorithmen gemäß §16 (5) SigV“ (Update 2000)
Stellungnahme

Dr. Holger Petersen, Dirk Fox
Secorvo Security Consulting GmbH

Version 1.1
Stand 17. Mai 2000

Inhaltsübersicht

Abkürzungen

ANSI	American National Standards Institute
DSA	Digital Signature Standard
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PDA	Personal Digital Assistant
RSA	Asymmetrisches Kryptosystem von Rivest, Shamir und Adleman, 1978
SigV	Signaturverordnung zum Deutschen Signaturgesetz

1 Zusammenfassung

Der folgende Text nimmt Stellung zum Entwurf eines „Update 2000“ der Empfehlung geeigneter Kryptoalgorithmen gemäß § 16 (5) der Signaturverordnung (SigV) zur Veröffentlichung im Bundesanzeiger vom 18.04.2000 (Version 4).

2 Anmerkungen zum Empfehlungsentwurf vom 18.04.2000

2.1 Kryptographische Anforderungen (Abschnitt 1)

Das Paddingschema (in der Empfehlung „Formatisierungsverfahren“ genannt) sollte expliziter Bestandteil des Dokuments sein, da die Sicherheit des Signaturalgorithmus von der Wahl eines geeigneten Paddingverfahrens maßgeblich abhängt, wie z. B. die in [14] diskutierten Angriffe zeigen.

Hilfreich für Hersteller wäre es, wenn zumindest erwiesen unsichere Paddingschemata, wie beispielsweise die in dem nun zurückgezogenen Standard ISO/IEC 9796, in der Empfehlung explizit ausgeschlossen würden.

2.2 Vorschläge für geeignete Signaturalgorithmen (Abschnitt 3)

In Abschnitt 3 werden zwei Kriterien für die Festlegung der Systemparameter angeführt: Die besten heute bekannten Algorithmen zum Faktorisieren resp. Bestimmen des Diskreten Logarithmus und die Leistungsfähigkeit heutiger Rechnertechnik.

Tatsächlich ist ein drittes wichtiges Kriterium zu berücksichtigen: Die bei einem Angriff einer bestimmten Qualität dem Angreifer entstehenden Kosten, sofern die Kosten nicht implizit bei der Bewertung der Leistungsfähigkeit berücksichtigt werden (z.B. Mips/US$ statt Mips/mm² Silizium o.ä.). Zudem können die Kosten von Speicher einen wichtigen Einfluß haben, da bei vielen Algorithmen fehlende Rechenleistung durch den Einsatz von (schnellem) Speicher kompensiert werden kann.

Anmerkung: Prognosen sind natürlich auch für sehr lange Zeiträume möglich, allerdings in der Regel weniger verläßlich. Wesentlich an einer Prognose ist in diesem Zusammenhang, daß sie „konservativ“ ist, d.h. eine Entwicklung annimmt, die sich an „negativen“ Erfahrungswerten orientiert.

2.3 RSA (Abschnitt 3.1)

Die Verdoppelung der Bitlänge des RSA-Modulus zwischen Ende 2004 und Ende 2005 ist (aus kryptographischer Sicht) nicht begründbar, da der Aufwand für einen Angriff subexponentiell wächst und damit nach heutiger Kenntnis erwartet werden kann, daß auch kürzere Bitlängen bis Ende 2005 als hinreichend sicher angesehen werden können. Die Abschätzungen von Lenstra/Verheul ermitteln unter bestimmten, vernünftigen Annahmen für den Zeitraum von 2004 auf 2005 eine Modulusverlängerung von lediglich etwa 40 bit (siehe [13]).

Insbesondere in Hinblick auf die Effizienz der Algorithmen und ihren Einsatz in Umgebungen mit beschränkten Ressourcen (Mobilfunkgerät, Smartcards, PDA) hat eine Verdoppelung der Bitlänge erhebliche Konsequenzen, da die Ausführungszeit für die Exponentiation in $O(n^2)$

liegt und bei 2n mindestens $O((2n)^2)=O(4n^2)=4O(n^2)$ beträgt, d.h. sich mindestens vervierfacht.

Wir empfehlen daher eine vorgeschriebene Mindest-Bitlänge von 1280 bit (= 160 byte). Damit würde die Verwendung längerer Moduluslängen bei Softwareimplementierungen durch Hersteller nicht ausgeschlossen. (Diese Bitlänge liegt um 130 bit über der Empfehlung von Lenstra/Verheul für das Jahr 2005, siehe [13].)

Hingegen sollten an die Länge des öffentlichen Exponenten Mindestanforderungen formuliert werden. Auch wenn bislang keine Angriffe auf das RSA-*Signatur*schema mit kurzem Exponenten bekannt sind, erscheint eine Mindestlänge von 32 bit sinnvoll. Dadurch wird die Rechengeschwindigkeit einer Implementierung nicht meßbar beeinträchtigt; für den Fall des Bekanntwerdens eines Fälschungsangriffs auf Signaturen mit sehr kurzen öffentlichen Schlüsseln (wie z.B. 3 oder 2^4+1) wären existierende Implementierungen nicht betroffen.

2.4 Formatisierungsverfahren (Abschnitt 3.1, Bemerkung 2)

Wie oben angeführt erscheint es uns erforderlich, für die Formatisierungsverfahren eine Empfehlung auszusprechen, um Herstellern und Anwendern einen Anhaltspunkt für geeignete Verfahren zu geben. Insbesondere in Hinblick auf Veröffentlichungen wie [14], die zu Verunsicherung bei den Anwendern führen, wird dies dringend angeraten.

2.5 DSA (Abschnitt 3.2)

Für den Sprung hinsichtlich der Bitlänge von p gilt die gleiche Bemerkung wie unter 3.1 für das RSA Verfahren. Für die Sicherheit der Verfahren erscheint eine Bitlänge von 1280 bit (= 160 byte) ausreichend, die auch effizientere Implementierungen zulassen würde.

2.6 DSA Varianten auf Gruppen (Abschnitt 3.3)

Es erscheint sinnvoll, Beispielkurven aus den Standards FIPS 186-2 [1], ANSI X9.62 [10] oder IEEE P1363 [5] zu referenzieren, möglicherweise sogar zu zitieren, bei denen alle geforderten Bedingungen eingehalten wurden, denn die Sicherheit der Verfahren wird durch die Wahl einer festen Kurve nicht beeinträchtigt.

Zur Erhöhung der Verständlichkeit empfehlen wir außerdem, die Bedingung vier in Abschnitt 3.3a (zugleich Bedingung sechs in 3.3b),

„*Die Klassenzahl der Hauptordnung, die zum Endomorphismenring von E gehört, ist mindestens 200*“,

so zu formulieren, daß sie auch einem Nicht-Mathematiker verständlich wird. Im gesamten Dokument sind an keiner Stelle die nur in diesem Satz verwendeten Betriffe „Klassenzahl“, „Hauptordnung“ und „Endomorphismenring“ definiert oder erläutert. Hilfreich wäre eine Formulierung dieser Bedingung, die deutlich macht, was dies in der Praxis für eine Implementierung bedeutet.

2.7 Zufallszahlen (Abschnitt 4)

Die formulierten Empfehlungen zu Zufallsgeneratoren, deren Wahl in einer konkreten Realisierung maßgeblichen Einfluß auf die Unvorhersagbarkeit der erzeugten Schlüssel hat, bleiben in einigen Punkten zu vage.

Wir empfehlen daher, einige der üblicherweise verwendeten statistischen Tests für physikalische Rauschquellen zu zitieren, oder zumindest auf FIPS 140-1 [NIST_94] zu verweisen. Eine deutlich umfassendere Liste empfehlenswerter Tests findet sich z. B. in [MeOV_96].

Außerdem sollte zumindest der Blum-Blum-Shub-Generator als guter Pseudozufallszahlengenerator erwähnt werden [BlBS_86], der bewiesene Sicherheitseigenschaften (Unvorhersagbarkeit ist äquivalent dem Faktorisierungsproblem) besitzt.

3 Literatur

BlBS_86 Blum, L.; Blum, M.; Schub, M.: *A Simple Unpredictable Pseudo-Random Number Generator*. SIAM J. Computing, 15/2, 1986, S. 364-383.

MeOV_96 Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A.: *Handbook of Applied Cryptography*. CRC Press, 1996.

NIST_94 National Institute of Standards and Technology (NIST): *Security Requirements for Cryptographic Modules*. Federal Information Processing Standards Publication 140-1 (FIPS-PUB), 11.01.1994.

SigV_97 *Verordnung zur digitalen Signatur (Signaturverordnung – SigV)*. Beschluß der Bundesregierung vom 8. Oktober 1997; in Kraft seit 1. November 1997.