DuD
Datenschutz und Datensicherheit

Digital Signature Standard (DSS)

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem "Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Hintergrund

Der Entwurf des Digital Signature Standard (DSS), des weltweit ersten Standards für einen Algorithmus zur Erzeugung digitaler Signaturen, jährt sich in diesem Jahr zum zehnten Mal. Im August 1991 hatte das amerikanische National Institute of Standards and Technology (NIST) in damals ungewohnter Offenheit die Standardisierung eines Kryptoverfahrens mit der öffentlichen Publikation eines Entwurfs gestartet.

Ziel der Standardisierung war es, die Abhängigkeit von dem einzigen bis dahin verbreiteten digitalen Signaturverfahren, dem in den USA patentierten RSA-Algorithmus, zu verringern. Unterstellt wurde dem NIST eine weitere Hauptzielsetzung: Die Durchsetzung eines Verfahrens, das sich – anders als RSA – nur zum Signieren, nicht aber zum Verschlüsseln von Daten nutzen lässt. Anders als der RSA-Algorithmus arbeitet der im DSS standardisierte Digital Signature Algorithm (DSA) nicht "selbstinvers" – bei Signieren und Verifizieren kommen unterschiedliche Operationen zur Anwendung.

Der DSA – FIPS PUB 186

Der Digital Signature Algorithm basiert auf dem Mitte der 80er Jahre publizierten ElGamal-Verfahren [ElGa_84]. Dessen Sicherheit beruht nicht – wie die von RSA – auf der Schwierigkeit der Faktorisierung großer Zahlen, sondern der Berechnung sogenannter "diskreter Logarithmen". Der DSA ähnelt einer 1991 von dem deutschen Mathematiker Schnorr vorgeschlagenen besonders effizienten Variante des ElGamal-Verfahrens [Schn_91].

Grob beschrieben funktioniert der DSA wie folgt [NIST_94]: Zu öffentlich bekannten, festen Primzahl-Moduln p und q sowie einem Generator g wird für die Berechnung einer digitalen Signatur zu einer Nachricht N vom Signierer eine nur einmal verwendbare Zufallszahl k gewählt. Mit dem geheimen Signierschlüssel G berechnet er dann:

$$\boldsymbol{r} := (g^k \bmod p) \bmod q \text{ und}$$

$$\boldsymbol{s} := (k^{-1} \times (\text{SHA-1}(N) + G \times r)) \bmod q.$$

Das Paar (r, s) bildet die Signatur zu SHA-1(N), dem Hashwert der Nachricht N. Die kryptographische Hashfunktion SHA-1 bildet dabei die zu signierende Nachricht auf einen 160 bit langen Wert ab.[1]

Die Prüfung einer Signatur (r, s) mit dem zugehörigen öffentlichen Prüfschlüssel $\ddot{O}$ umfasst drei Schritte:

$$w := s^{-1} \bmod q$$

$$u_1 := \text{SHA-1}(N) \times w \bmod q,\ u_2 := r \times w \bmod q$$

Prüfung: $r = (g^{u1} \times \ddot{O}^{u2} \bmod p) \bmod q$?

Die öffentlichen Moduln p und q sind Primzahlen der Länge 160 bit (q) bzw. 512 bis 1024 bit (p). Die Signatur besteht damit aus zwei je maximal 160 bit langen Werten (r und s).[2]

Große Verbreitung fand der DSA vor allem durch die Aufnahme des Verfahrens in "Pretty Good Privacy" (PGP) Version 5.0 als Standard-Signaturalgorithmus im Jahr 1997. Heute sind die bei weitem meisten erzeugten PGP-Schlüssel DSS-Schlüsselpaare, da DSS die Voreinstellung in PGP ist.

Ende Januar 2000 wurde eine Neufassung des Standards vom NIST publiziert (FIPS-PUB 186-2), die sich von der ursprünglichen in zwei wesentlichen Punkten unterscheidet [NIST_00]:

- Neben dem DSA wurde – nach Auslaufen des US-amerikanischen Patents – auch RSA als digitales Signaturverfahren aufgenommen (wie in der ANSI-Norm X9.31 beschrieben).
- Vor dem Hintergrund der ANSI-Standardisierung von digitalen Signaturverfahren auf elliptischen Kurven wurde die DSA-Variante auf elliptischen Kurven (ECDSA) in den Standard aufgenommen (ANSI X.9.62).

Sicherheit

Die kryptographische Sicherheit des DSA ist vergleichbar der des RSA-Verfahrens.[3] Das ECDSA-Verfahren erreicht hingegen dieselbe Sicherheit bislang mit deutlich geringeren Schlüssellängen, da – anders als beim DSA – bei geeigneter Wahl der zugrundeliegenden elliptischen Kurve bis heute keine Verfahren zur Berechnung diskreter Logarithmen mit subexponentiellem Aufwand bekannt sind.

Mit der Aufnahme des ECDSA in den NIST-Standard soll nun eine weitere Abhängigkeit verringert werden: Die fast aller heutiger kryptographischen Systeme mit asymmetrischen Verfahren von der Sicherheit der (verwandten) zahlentheoretischen Probleme der Faktorisierung und der Berechnung diskreter Logarithmen.

Literatur

[ElGa_84] ElGamal, Taher: *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. In: Blakley, G.R.; Chaum, D. (Hrsg.): Proceedings of Crypto '84, LNCS 196, Springer, Berlin 1995, S. 10-18.

[NIST_94] NIST: *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication 186, 19.05.1994.

[NIST_95] NIST: *Secure Hash Standard (SHS-1)*. FIPS-PUB 180-1, 17.04.1995.

[NIST_00] NIST: *Digital Signature Standard (DSS)*. FIPS-PUB 186-2, 27.01.2000.

[Schn_91] Schnorr, Claus P.: *Efficient Signature Generation by Smart Cards*. Journal of Cryptology, Vol. 4, No. 3, 1991, S. 161-174.

[1] Der Secure Hash Algorithm (SHA) wurde ebenfalls vom NIST standardisiert [NIST_95]. Zu kryptographischen Hashfunktionen siehe ausführlich Dobbertin, DuD 2/1997, S. 82-87.

[2] Zur effizienten Implementierung des DSA siehe Fox, *Der 'Digital Signature Standard': Aufwand, Implementierung und Sicherheit*, in: Verläßliche Informationssysteme VIS '93, DuD-Fachbeiträge 16, Vieweg 1993, S. 333-352.

[3] Genauer siehe Fox, *Fälschungssicherheit digitaler Signaturen*, DuD, 2/1997, S. 69-74.