

How to find the *socially accepted* minimal Key length for Digital Signature Algorithms

Dr. Gerhard Schabhüser

BSI

Essen, 23rd September 2002

Outline

- Introduction
- A review of the current procedure
 - The players
 - The Roles and Motivation of the Players
 - The current Algorithms
 - The current Procedure
- Conclusion 1
- A more conservative security paradigm
- Conclusion 2

Introduction



The BSI has to maintain a list of algorithms including parameter sizes, which are suitable for *qualified electronic signatures*.

This list must be updated once a year.

The algorithms must be secure at least for the next 6 years.

A review of the current procedure

The game:

*“Update the List of suitable
Digital Signature Algorithms”*

- The Players
- The Roles
- The Procedure

A review of the current procedure

The Players:

- The RegTP:
 - German Telecommunication Regulatory Authority
 - Root-CA
- The BSI:
 - Editor of the List
 - Responsible for security

A review of the current procedure

The Players (cont.):

- The Scientists:
 - Scientific Improvements
- The Hardware manufactures:
 - Secure Signature Creation Devices
- The OS-Providers:
 - Secure Signature Creation Devices

A review of the current procedure

The Players (cont.):

- The Application Providers:
 - System integrators
- The Certification Authorities:
 - Operate a CA
- The Accreditation-Authorities:
 - Evaluation of Components
- The Vendors:
 - Sell Products/ Systems

A review of the current procedure

The Roles and Motivation:

- RegTP:
 - overall security of *qualified electronic signatures*
 - operate a CA
- BSI:
 - guarantee the security of algorithms
 - watch for balance

A review of the current procedure

The Roles and Motivation (cont.):

- **Scientists:**
 - introduce new algorithms
 - promote new algorithms
 - provide info about new attacks
- **Hardware manufactures:**
 - provide hardware for SCD
 - promote everything they support
 - block everything which causes trouble on their platform

A review of the current procedure

The Roles and Motivation (cont.):

- OS-Providers:
 - provide secure SCDs
 - motivation similar to HM
- Application Providers:
 - watch for competitive advantage
 - watch for operating costs
- Certification Authorities:
 - operate CA
 - watch for availability of products

A review of the current procedure

The Roles and Motivation (cont.):

- The Accreditation-Authorities:
 - Evaluation of Components
 - watch for detailed criteria to enhance the evaluation
- The Vendors:
 - accept everything their product supports
 - object the rest
 - get information for future developments

A review of the current procedure

Current Algorithms:

- The Hash Functions:
 - RIPEMD160
 - SHA-1
- The Signature Algorithms:
 - RSA
 - the others:
 - DSA
 - ECDSA and variants

A review of the current procedure

The Procedure:

- BSI:
 - compiles a draft
 - take into account new results
 - publish for comment
- Public Hearing:
 - discuss comments
 - accept/reject
 - agree on modifications

A review of the current procedure

The Procedure (cont.):

- BSI:
 - edit the final document
 - send to RegTP
- RegTP:
 - publish the official document

A review of the current procedure

Highlights:

- 2000:
 - increase the minimal key size for RSA from 1024 to 2048 in the mid of 2005
- 2001:
 - decrease the minimal key size for RSA from 2048 to 1024 for the period mid of 2005 to the end of 2005.
 - set the minimal key size for RSA to 1024 in the year 2006
 - add a recommendation to use 2048 bit

A review of the current procedure

Highlights (cont.):

- 2002 (April):
 - withdraw the decision of last year
 - increase the minimal key size for RSA from 1024 to 2048 for 2006 and 2007
 - analyse the Bernstein paper
- 2002 (September):
 - revised draft for 2002: published for comment
 - minimal key size for RSA to 1024 in 2006
 - minimal key size for RSA to 1536 in 2007
 - recommend to use 2048 bit

Conclusion 1

The discussion on minimal key length for digital signature algorithms is in fact a discussion on the minimal key length for RSA.

The current key size is determined by the capability of SmartCards to run RSA of the specified size.

A more conservative security paradigm

Approach:

- Use the analysis of Lenstra and Verheul.
- The operation count of attacks against symmetric and asymmetric algorithms should be equivalent.
- **Fact:** The current symmetric key length is 128.
- Compute the key length for RSA/DSA/ECDSA with respect to the current best known algorithm, which breaks RSA/DSA/ECDSA, in such a way, that the operation count for a successful attack is equivalent to exhaustive key search of a symmetric 128 bit key algorithm.

A more conservative security paradigm

Define the
equivalent number of mips years

as:

$$EMY(k) := 2^{(k-56)} * 5 * 10^5 * \mathbf{n},$$

with $k := 128$ and $\mathbf{n} := 2$

Results:

- RSA/DSA: The current best algorithm to factor a modulus n of size l has the expected running time of:

A more conservative security paradigm

$$L(n) := e^{(a+o(1)) \cdot \ln(n)^u \cdot \ln(\ln(n))^{(1-u)}}$$

$$\text{with } a := \sqrt[3]{\left(\frac{64}{9}\right)} \quad \text{and} \quad u := \frac{1}{3}$$

Choose l , such that :

$$\frac{L(2^l)}{EMY(128)} \geq \frac{L(2^{512})}{10^4}$$

that is :

$$l \approx 3400$$

A more conservative security paradigm

- EC-DSA: The current best algorithm to compute discrete logs on an elliptic curve over a prime field of size l has expected running time of $0.88 \cdot \sqrt{q}$ group operations, where q is approximately of size p .

Choose l , such that :

$$\frac{2^{l/2} \cdot l^2}{EMY(128)} \geq \frac{2^{109/2} \cdot 109^2}{2.2 \cdot 10^6}$$

that is :

$$l \approx 250$$

Conclusion 2

If you accept this approach, then

- the starting point for selecting key sizes for RSA/DSA resp. ECDSA are parameter sizes of 3400 resp. 250 bit.
- You have to add a lot of rows to the table of the Lenstra-Verheul-paper to see the entries for the appropriate key sizes.