

NESSIE

Project Number	IST-1999-12324
Project Title	NESSIE
Deliverable Type	Report
Security Class	Public
Deliverable Number	D02
Title of Deliverable	Report on the NESSIE Call

Nature of the Deliverable

Document reference	NES/DOC/KUL/WP1/D02/1
Contributing WPs	WP1
Contractual Date of Delivery	Y1 M5
Actual Date of Delivery	Y1 M10
Editor	Bart Van Rompay

Abstract In this deliverable we detail the project's call for cryptographic primitives, together with the details of how it has been publicised.

Keywords

Disclaimer The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Report on the NESSIE Call

1 Introduction

The main objective of the NESSIE project is to put forward a portfolio of strong cryptographic primitives that has been obtained after an open call and been evaluated using a transparent and open process. Therefore, in the first phase of the project, an open call for the submission of cryptographic primitives, as well as for evaluation methodologies for these primitives has been launched. The scope of this call has been defined together with the project industry board, and it was published in March 2000. In the remainder of this report we first discuss the contents of the call, and next discuss how it has been publicised. The call itself is given in Appendix A.

2 Contents of the NESSIE Call

The NESSIE call includes a request for a broad set of primitives providing confidentiality, data integrity, and authentication. These primitives include block ciphers, stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption schemes. In addition, it asks for evaluation methodologies for these primitives. The scope of this call has been determined together with the project industry board during the PIB meeting of February 24. The PIB gave several important suggestions with regards to market requirements.

The text of the call begins with a presentation of the NESSIE project, its goals and the partners involved in it, as well as some background explaining the need for cryptographic primitives and the procedure of an open call (this is also compared with the NIST call for the Advanced Encryption Standard).

It has been stressed that not only block ciphers are needed, but also several other primitives such as stream ciphers, MAC's, etc. (since there are many block ciphers around but far fewer other primitives even though they are required in many applications). Thus the scope of this call is much wider than that of the AES call. In addition this call also asks for evaluation methodologies that can be used during the open evaluation process of the project.

Under the heading *General Requirements* a list is given of the types of primitives requested by the project and the main selection criteria which will be used to evaluate the proposals. These criteria are long-term security, market requirements, efficiency and flexibility. Primitives can be targeted towards a specific environment (such as 8-bit smart cards or high-end 64-bit processors), but it is clearly an advantage to offer a wide flexibility of use.

Next the *Security Requirements* for each type of primitive are listed. It has been chosen to specify two main security levels for symmetric primitives, named *normal* and *high*. The level depends on the key length, internal memory or output length of the primitive.

For block ciphers a third security level, *normal-legacy*, has been specified, which means a block size of 64 bits instead of 128 (the AES specifies only a 128-bit block size).

This was suggested by the project industry board, because the market will still need this block size for compatibility with present applications (e.g., payments with 8-byte personal identification numbers) and is interested in 64-bit block ciphers which are more secure and efficient than the ones presently used.

For the asymmetric primitives the security level is specified in terms of the computational effort of the most efficient attack.

The detailed *Evaluation Criteria* are then discussed. This includes security criteria, implementation criteria and others. Licensing is also discussed. The evaluation process is explained: it is an open process, which consists of two phases, and three workshops will be organised to facilitate this. A timetable is given. Since an open evaluation process is used, the NESSIE call also invites suggestions for other evaluation criteria such as testing methodologies.

Finally the formal *Submission Requirements* are listed. This is a specification of the contents that have to be provided with any submission. The main parts are: a cover sheet with general information; the primitive specification and supporting documentation (such as a statement of the claimed security properties, a design rationale etc.); implementation and test values (a reference implementation in portable C is required, the definition of portable C is given on the NESSIE web site, as well as an API which has to be used for symmetric primitives); an intellectual property statement. Proposals should arrive before September 29 2000.

The call then concludes with a request for suggestions for evaluation criteria (in addition to the criteria discussed above), such as testing methodologies (e.g., statistical testing).

3 Publication of the NESSIE Call

The NESSIE call was published in March 2000, and has been given a high visibility by several means. The call is available on the NESSIE web site (<http://www.cryptoneessie.org>). Announcements have been made in the February 2000 and May 2000 newsletters of the IACR (International Association for Cryptologic Research), which has an audience of over 1000 cryptographers. Moreover, oral presentations have been made at the rump sessions of two of the most important conferences in the area of cryptology: Fast Software Encryption Workshop (10-12 April 2000 in New York, USA), and Eurocrypt 2000 (14-18 May 2000 in Bruges, Belgium). The first conference had an audience of over 200 participants, most of which are particularly interested in efficient symmetric cryptographic primitives. Eurocrypt 2000 is a more general conference with about 500 participants.

Submissions to NESSIE have also been solicited through private conversations (both in person and by email). People who have been contacted include Johannes

Buchmann, Don Coppersmith, Bert den Boer, Hans Dobbertin, Burt Kaliski, Ron Rivest, Philip Rogaway, Bruce Schneier, Richard Schroepel, Victor Shoup, and Ramarathnam Venkatesan.

Appendix A

The NESSIE Call for Cryptographic Primitives

Version 2.2 8th March 2000

Introduction

NESSIE (New European Schemes for Signature, Integrity, and Encryption) is a project within the Information Societies Technology (IST) Programme of the European Commission. The participants of the project are:

Participant name	Country
Katholieke Universiteit Leuven	Belgium
École Normale Supérieure	France
Fondazione Ugo Bordon	Italy
Royal Holloway, University of London	U.K.
Siemens Aktiengesellschaft	Germany
Technion – Israel Institute of Technology	Israel
Université Catholique de Louvain	Belgium
Universitetet i Bergen	Norway

NESSIE is a 3-year project, which started on 1st January 2000. Further information about NESSIE is available at <http://cryptonessie.org>.

The main objective of the project is to put forward a portfolio of strong cryptographic primitives for a number of different platforms. These primitives will be obtained after an open call and evaluated using a transparent and open process. They should be the building blocks of the future standard protocols for the information society.

The deadline for the submission of primitives will be 29th September 2000. A workshop will be organised for submitters to present their primitives.

Background

In the information society, cryptology has become a key enabling technology to provide secure electronic commerce and electronic business, secure communications, secure payments, and the protection of the privacy of the citizen. Cryptology is a field that evolves quickly, and society needs robust primitives that provide long term security (15 to 20 years or more), rather than ad hoc solutions that need to be frequently replaced. With the current state of the art in cryptology, it is not possible to have provably secure solutions, although there is a trend to prove more and more security properties of primitives. However, for use in real applications, sufficient confidence in a primitive can only be achieved when primitives have been subjected to an open and independent evaluation for a sufficient amount of time.

The procedure of an open call followed by an evaluation process has been previously used in the selection process for the DES, the RIPE project, and the AES. The scope of this call for primitives is wider than the NIST call for AES. The information society needs other cryptographic primitives than just block ciphers. Thus the NESSIE call seeks cryptographic primitives in many areas, such as:

- Stream ciphers: for applications with high throughput requirements or tight performance constraints etc.
- MACs: for high-speed authentication of packets etc.
- Families of Pseudo-random functions: for key derivation, entity authentication, and encryption etc.
- Digital signatures and hash functions: for electronic commerce, business, and payment etc.
- Asymmetric encryption schemes.
- Asymmetric identification schemes.

Furthermore, there is a wide range of environments in which cryptographic primitives are used. Thus the NESSIE project will consider primitives designed for use in specific environments (though flexibility is clearly desirable). The NESSIE call also asks for testing methodologies of these primitives (such as statistical tests).

The results of this call will then be subjected to a thorough and open evaluation process. In addition to the responses to the call, the project will also consider a selection from existing standards containing such primitives. The main selection criteria will be long-term security, market requirements, efficiency (performance), and flexibility.

It is also a goal of the project to disseminate widely the results of the project, and to build a consensus based on these results. In order to achieve this, an Industry Group has been established. The Industry Group consists of about twenty leading European companies in this area and will be consulted on a regular basis throughout the project. It is expected that the Industry Group will provide input concerning the nature of the final call (requirements and definitions for primitives), the relevance of the selection criteria, and the standardisation strategy. An important part of the dissemination will be the introduction of these primitives into standardisation bodies (ISO, ISO/IEC,

CEN, IEEE, IETF), based in part on the consensus achieved within the project. It is anticipated that the results of the project will also be published in scientific publications.

General Requirements

This section discusses the general selection criteria, the type of primitives required, and the security requirements for each primitive.

Selection Criteria

The main selection criteria will be long-term security, market requirements, efficiency (performance) and flexibility.

- Security is the most important criterion, because security of a cryptographic primitive is essential to achieve confidence and to build consensus. It is anticipated that this evaluation process will be influenced by developments outside the project (such as new attacks or analysis techniques).
- A second criterion relates to market requirements. Market requirements are related to the need for a primitive, its usability, and the possibility for world-wide use.
- A third criterion is the performance of the primitive in the specified environment. For software, the range of environments considered include 8-bit processors (as found in inexpensive smart cards), 32-bit processors (e.g., the Pentium family) to the modern 64-bit processors. For hardware, both FPGAs and ASICs will be considered.
- A fourth criterion is the flexibility of the primitive. It is clearly desirable for a primitive to be suitable for use in a wide-range of environments.

Type of Primitives

The NESSIE project is seeking submissions of strong cryptographic primitives in the categories given below. The NESSIE project is particularly interested in receiving submissions in categories that have not received much standardisation effort.

1. Block ciphers
2. Synchronous stream ciphers
3. Self-synchronising stream ciphers
4. Message Authentication Codes (MACs)
5. Collision-resistant hash functions
6. One-way hash functions
7. Families of pseudo-random functions
8. Asymmetric encryption schemes
9. Asymmetric digital signature schemes
10. Asymmetric identification schemes

Definitions are broadly as given in the Handbook of Applied Cryptography (ISBN: 0-8493-8523-7).

Security Requirements for Each Primitive

Symmetric Primitives (Primitives 1-7)

There are two main security levels for symmetric primitives. These are named *normal* and *high*. For block ciphers, *normal-legacy* is also provided. The minimal requirements for a symmetric primitive to attain a security level are given below.

1) Block ciphers.

- a) *High*. Key length of at least 256 bits. Block length at least 128 bits
- b) *Normal*. Key length of at least 128 bits. Block length at least 128 bits.
- c) *Normal-Legacy*. Key length of at least 128 bits. Block length 64 bits

2) Synchronous stream ciphers.

- a) *High*. Key length of at least 256 bits. Internal memory of at least 256 bits.
- b) *Normal*. Key length of at least 128 bits. Internal memory of at least 128 bits.

3) Self-synchronising stream ciphers.

- a) *High*. Key length of at least 256 bits. Internal memory of at least 256 bits.
- b) *Normal*. Key length of at least 128 bits. Internal memory of at least 128 bits.

4) Message Authentication Codes (MACs).

The primitive should support all output lengths (in multiples of 32 bits) up to the key length (inclusive).

- a) *High*. Key length of at least 256 bits.

b) *Normal*. Key length of at least 128 bits.

5) Collision-Resistant Hash functions.

- a) *High*. Output length of at least 512 bits.
- b) *Normal*. Output length of at least 256 bits.

6) One-Way Hash Functions.

These hash functions shall be preimage resistant and second preimage resistant.

- a) *High*. Output length of at least 256 bits.
- b) *Normal*. Output length of at least 128 bits.

7) Families of pseudo-random functions.

Fixed block length of at least 128 bits.

- a) *High*. Key length of at least 256 bits.
- b) *Normal*. Key length of at least 128 bits.

Asymmetric Primitives (Primitives 8-10)

The security parameters should be chosen such that the most efficient attack on the primitive requires a computational effort of the order of 2^{80} 3-DES encryptions. Furthermore, a table giving the security levels in terms of the security parameters should be provided.

8) Asymmetric encryption schemes (deterministic or randomised).

The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.

9) Asymmetric digital signature schemes.

The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.

10) Asymmetric identification schemes.

The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions. The probability of impersonation should be smaller than 2^{-32} .

Evaluation of Proposals

Detailed Evaluation Criteria

Security Criteria

- An attack should be at least as difficult as the generic attacks against the type of primitive (exhaustive search, birthday attack etc.).
- Primitives will be evaluated against the security claims of the submitter. An attack requiring lower computing resources than claimed would usually disqualify the submission.
- Primitives will be evaluated within the stated environment. Thus, consideration of vulnerability to side channel attacks (e.g., timing attacks, power analysis) may be appropriate.

Implementation Criteria

- Software and hardware efficiency will be compared with similar submissions and existing primitives.
- Execution code and memory sizes will be assessed according to their relevance in different contexts. Special attention will be paid to smart cards.
- Submitted primitives will be assessed against claimed performance, though it is clearly preferable for primitives to offer wide flexibility of use.

Other Criteria

- Simplicity and clarity of design are important considerations. Variable parameter sizes are less important.

Licensing Requirements

- Submitted primitives should, if selected by NESSIE, be available royalty-free. If this is not possible, then access is non-discriminatory.
- The submitter should state the position concerning intellectual property. This statement should be updated when necessary.

The Evaluation Process

The NESSIE project reserves the right to reject submitted primitives that are not clearly specified and easily comprehensible or that fail to meet the NESSIE requirements in some way.

The NESSIE evaluation process is an open process. Thus as part of the evaluation process, the NESSIE project welcomes comments about both submitted primitives and the evaluation process, including evaluation methodologies. To facilitate this process, three NESSIE workshops will be organised; the first will be in October 2000, shortly after the deadline for submission of primitives. As part of the evaluation process, the NESSIE partners will give security and performance assessments of the submitted primitives. At the end of the evaluation process, the NESSIE project may recommend certain submissions for standardisation. The NESSIE project is to have two phases. A timetable for the NESSIE project is given below.

- 2000 January Beginning of first phase of NESSIE
- 2000 January Creation of Industry Board
- 2000 March Call for Cryptographic Primitives
- 2000 September Submission deadline
- 2000 October First NESSIE workshop
- 2001 June Preliminary assessment of submissions
- 2001 June Second NESSIE workshop
- 2001 June End of first phase of NESSIE

- 2001 July Beginning of second phase of NESSIE
- 2002 February Preliminary selection of submissions
- 2002 February Standardisation Plan
- 2002 October Third NESSIE workshop
- 2002 December Final selection of submissions
- 2002 December Final report of NESSIE project
- 2002 December End of second phase of NESSIE

Formal Submission Requirements

The following are to be provided with any submission:

A. Cover sheet with the following information:

- A.1 Name of submitted algorithm
- A.2 Type of submitted algorithm, proposed security level, and proposed environment.
- A.3 Principal submitter's name, telephone, fax, organization, postal address, e-mail address
- A.4 Name(s) of auxiliary submitter(s)
- A.5 Name of algorithm inventor(s)/developer(s)
- A.6 Name of owner, if any, of the algorithm (normally expected to be the same as the submitter)
- A.7 Signature of submitter
- A.8 (optional) Backup point of contact (telephone, fax, postal address, e-mail)

B. Primitive specification and supporting documentation

- B.1 A complete and unambiguous description of the primitive in the most suitable forms, such as a mathematical description, a textual description with diagrams, or pseudo-code. The specification of a primitive using code is not permitted. Input and output should be in the form of binary strings. For asymmetric algorithms, a method for key generation and parameter selection needs to be specified.
- B.2 A statement that there are no hidden weaknesses inserted by the designers.
- B.3 A statement of the claimed security properties and expected security level, together with an analysis of the primitive with respect to standard cryptanalytic attacks. Weak keys should also be considered.
- B.4 A statement giving the strengths and advantages of the primitive.
- B.5 A design rationale explaining design choices.
- B.6 A statement of the estimated computational efficiency in software. Estimates are required for different sub-operations like key setup, primitive setup, and encryption/decryption (as far as applicable). The efficiency should be estimated both in cycles per byte and cycles per block, indicating the processor type and memory. If performance varies with the size of the inputs, then values for some typical sizes should be provided. Optionally the designers may provide estimates for performance in hardware (area, speed, gate count, a description in VHDL).
- B.7 A description of the basic techniques for implementers to avoid implementation weaknesses.

C. Implementations and test values

- C.1 A reference implementation, in ANSI C. For symmetric primitives, NESSIE will specify an API, which will be published on the NESSIE web site by 1st

- June 2000. For asymmetric primitives, it is allowed to use a 'standard' library for mathematical functions, such as multi-precision arithmetic (e.g., Lydia).
- C.2 A sufficient number of test vectors. The NESSIE project will supply software to generate test vectors for symmetric primitives.
- C.3 Optionally, an optimized implementation for some architectures, a JAVA implementation, an assembly language implementation.

D. Intellectual property statement

A statement that gives the position concerning intellectual property position and the royalty policy for the primitive (if selected). This statement should include an undertaking to update the NESSIE project when necessary.

Requirements:

- Items A, B, and D shall be supplied in paper form and in electronic form (Adobe PDF or PostScript on one or more diskettes).
- Item C shall be supplied in electronic form only (diskette).
- Item A, B, C and D shall be supplied on separate 3,5" 1.44 MB floppy diskettes, formatted for use on an IBM-compatible PC. Every diskette shall be labeled with the submitter's name, the name of the primitive, the number, and the date. Every diskette shall contain an ASCII file labeled "README", that lists all files included on the diskette and provides a brief description of the content of each file.
- All submissions must be in English.
- Classified and/or proprietary submissions shall not be considered.
- Paper submissions and diskettes shall be sent to the following address:
Prof. Bart Preneel
NESSIE Project Coordinator
Katholieke Universiteit Leuven
Dept. Electrical Engineering-ESAT/COSIC
Kard. Mercierlaan 94,
B-3001 Heverlee
BELGIUM
They should arrive on or before 29th September 2000.
- Optionally, an electronic version may be sent to submissions@cryptonessie.org.

An acknowledgment will be sent by email and by regular mail within 5 working days.

General questions for clarification of the formal submission requirements and of the evaluation criteria can be sent to info@cryptonessie.org. Answers to questions that are relevant to other submissions will be made available at www.cryptonessie.org. The NESSIE project will endeavour to answer all relevant questions in a timely manner.

Call for Evaluation Criteria

In addition to the criteria given above, the NESSIE project also invites suggestions for Evaluation Criteria, such as testing methodologies (e.g., statistical testing).

Further Information

Email: info@cryptonessie.org. Website: <http://cryptonessie.org>.