

# NESSIE

<b>Project Number</b>	IST-1999-12324
<b>Project Title</b>	NESSIE
<b>Deliverable Type</b>	Report
<b>Security Class</b>	Public
<b>Deliverable Number</b>	D07
<b>Title of Deliverable</b>	<b>Response to the NESSIE Call</b>
<b>Nature of the Deliverable</b>	
<b>Document reference</b>	NES/DOC/KUL/WP1/D07/1
<b>Contributing WPs</b>	WP1
<b>Contractual Date of Delivery</b>	Y1M10
<b>Actual Date of Delivery</b>	Y2M1
<b>Editor</b>	Bart Van Rompay
<b>Abstract</b>	In this deliverable we discuss the response to the project's call for cryptographic primitives, and present a first classification of the different submissions.
<b>Keywords</b>	call, cryptographic primitives
<b>Disclaimer</b>	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.

# Response to 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 (March 2000), an open call for the submission of cryptographic primitives, as well as for evaluation methodologies for these primitives, was launched.

In response to the call (the deadline for the submission of proposals was 29th September 2000) 40 submissions were received: 39 primitives in 7 categories and 1 evaluation methodology. An interaction process of about a month with the submitters resulted in all the submissions meeting the formal submission requirements and entering the evaluation phase of NESSIE.

In the remainder of this report we first briefly summarize the contents of the call, and next discuss the response to this call by the cryptographic community. A classification of the different submissions is presented in Appendix A.

## 2 Contents of the NESSIE Call

The NESSIE call (see deliverable D02 [1]) included 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, public-key encryption schemes, digital signature schemes and identification schemes. In addition, the call asked for evaluation methodologies for these primitives.

A list was given of the types of primitives requested by the project, together with the security requirements for each type of primitive. The main selection criteria, which will be used to evaluate the proposals, are long-term security, market requirements, efficiency and flexibility. Security was put forward as the most important selection criterion, as security of a cryptographic primitive is essential to achieve confidence and to build consensus.

## 3 Response to the NESSIE Call

The cryptographic community has responded very enthusiastically to the call. Thirty nine primitives have been received, as well as one proposal for

a testing methodology. After an interaction process, which took about one month, all submissions comply with the requirements of the call. The results of the call seem promising, and will lead to a very interesting and challenging evaluation process.

- Seventeen block ciphers have been submitted, which is probably not a surprise given the increased attention to block cipher design and evaluation as a consequence of the AES competition organised by NIST. They are divided as follows: six 64-bit block ciphers, seven 128-bit block ciphers (none of these seven come from the AES process), one 160-bit block cipher, and three block ciphers with a variable block length (including one AES finalist, and an improved version of an AES contender).
- Six synchronous stream ciphers were submitted, two MAC algorithms and one collision-resistant hash function, which brings the total number of symmetric primitives to twenty six.
- The remaining thirteen algorithms are asymmetric primitives; there are five asymmetric encryption schemes, seven digital signature algorithms and one identification scheme.

A detailed list of submissions can be found in Appendix A.

Approximately<sup>1</sup> seventeen submissions originated within Europe (6 from France, 4 from Belgium, 2 from Sweden and Switzerland), nine in North America (7 USA, 2 from Canada), nine in Asia (8 from Japan), three in Australia and three in South America (Brazil). The majority of submissions originated within industry (27); seven came from academia, and six are the result of a joint effort between industry and academia. Note however that the submitter of the algorithm may not be the inventor, so the share of academic research is probably underestimated by these numbers.

On 13–14 November 2000 the first NESSIE workshop was organised in Leuven (Belgium), where 35 submissions were presented [2]. All submissions are available on the NESSIE web site <http://www.cryptoneessie.org/>.

---

<sup>1</sup>Fractional numbers have been used to take into account primitives with submitters over several continents/countries – the totals here are approximations by integers, hence they don't add up to 40.

## References

- [1] NESSIE, *D2: Report on the NESSIE Call*, NESSIE Deliverable 2, October 2000.
- [2] \_\_\_\_\_, *D8: Workshop on results of call*, NESSIE Deliverable 8, <http://www.cryptoneessie.org/workshop/>, November 2000.

## Appendix A: List of NESSIE Submissions

Thirty nine cryptographic primitives have been submitted. Below we make a classification by type of primitive, listing the name of the primitive and of the submitters.

- Block ciphers
  - 64-bit block ciphers
    - \* CS-Cipher (Pierre-Alain Fouque, *CS Communication & Systèmes*)
    - \* Hierocrypt-L1 (Kenji Ohkuma, Fumihiko Sano, Hirofumi Muratani, Masahiko Motoyama, Shinichi Kawamura, *Toshiba Corporation*)
    - \* IDEA (Richard Straub, *MediaCrypt AG*)
    - \* Khazad (Paulo Barreto, *Scopus Tecnologia*, and Vincent Rijmen, *K.U.Leuven*)
    - \* MISTY1 (Eisaku Takeda, *Mitsubishi Electric Corporation*)
    - \* Nimbus (Alexis Machado, *Gauss Informatica*)
  - 128-bit block ciphers
    - \* Anubis (Paulo Barreto, *Scopus Tecnologia*, and Vincent Rijmen, *K.U.Leuven*)
    - \* Camellia (Shiho Moriao, *NTT*, and Mitsuru Matsui, *Mitsubishi Electric Corporation*)
    - \* Grand Cru (Johan Borst, *K.U.Leuven*)
    - \* Hierocrypt-3 (Kenji Ohkuma, Fumihiko Sano, Hirofumi Muratani, Masahiko Motoyama, Shinichi Kawamura, *Toshiba Corporation*)
    - \* Noekeon (Joan Daemen, Michael Peeters, Gilles Van Assche, *Proton World*, and Vincent Rijmen, *K.U.Leuven*)
    - \* Q (Leslie McBride)
    - \* SC2000 (Naoya Torii, *Fujitsu Laboratories*)
  - 160-bit block ciphers
    - \* SHACAL (Helena Handschuh, David Naccache, *Gemplus*)
  - variable length block ciphers
    - \* NUSH: 64, 128, and 256-bit (including submissions in every other category) (Anatoly Lebedev, *LAN Crypto, Int.*)
    - \* RC6: at least 128-bit (Jakob Jonsson, *RSA Labs Europe*, and Burt Kaliski, *RSA Labs*)

\* SAFER++: 64 and 128-bit (Gurgen Khachatryan, *Cylink Corporation*, James Massey, *ETH Zürich*, Melsik Kuregian, *National Academy of Sciences, Armenia*)

- Synchronous stream ciphers
  - BMGL (Johan Håstad, *Royal Institute of Technology, Sweden*, and Mats Näslund, *Ericsson Research*)
  - Leviathan (David McGrew, *Cisco Systems, Inc.*)
  - LILI-128 (E. Dawson, A. Clark, W. Millan, L. Penna, L. Simpson, *Queensland University of Technology*, and J. Golić, *University of Belgrade*)
  - SNOW (Thomas Johansson and Patrik Ekdahl, *Lund University*)
  - SOBER-t16 (Philip Hawkes and Greg Rose, *Qualcomm*)
  - SOBER-t32 (Philip Hawkes and Greg Rose, *Qualcomm*)
- Message authentication codes
  - Two-Track-MAC (Bart Van Rompay, *K.U.Leuven*, and Bert den Boer, *debis Information Security Services GmbH*)
  - UMAC (Ted Krovetz, *Intel*, John Black, *U.C. Davis*, Shai Halevi, *IBM*, Hugo Krawczyk, *Technion*, Phillip Rogaway, *U.C. Davis*)
- Collision-resistant and one-way hash functions
  - Whirlpool (Paulo Barreto, *Scopus Tecnologia*, and Vincent Rijmen, *K.U.Leuven*)
- Asymmetric encryption schemes
  - ACE Encrypt (Victor Shoup, *IBM Zürich Research Lab*)
  - ECIES (Don Johnson and Simon Blake-Wilson, *Certicom*)
  - EPOC (Tatsuaki Okamoto, *NTT*)
  - PSEC (Tatsuaki Okamoto, *NTT*)
  - RSA-OAEP (Jakob Jonsson, *RSA Labs Europe*, and Burt Kaliski, *RSA Labs*)
- Asymmetric digital signature schemes
  - ACE Sign (Victor Shoup, *IBM Zürich Research Lab*)

- ECDSA (Don Johnson and Simon Blake-Wilson, *Certicom*)
- ESIGN (Tatsuaki Okamoto, *NTT*)
- FLASH (Jacques Patarin, *BULL CP8*)
- QUARTZ (Jacques Patarin, *BULL CP8*)
- RSA-PSS (Jakob Jonsson, *RSA Labs Europe*, and Burt Kaliski, *RSA Labs*)
- SFLASH (Jacques Patarin, *BULL CP8*)
- Asymmetric identification schemes
  - GPS (Guillaume Poupard, *Ecole Normale Supérieure*)

One testing methodology has been submitted:

- “Using the general next bit predictor like an evaluation criteria”, (J.C. Hernandez, J.M. Sierra, J.C. Mex-Perera, S. Shepherd, A. Ribagorda, B. Ramos)