



FOR IMMEDIATE RELEASE
September 24, 2001

Bart Preneel
Bart.Preneel@esat.kuleuven.ac.be
+32 (0)16 32 10 50

NESSIE PROJECT ANNOUNCES SELECTION OF CRYPTO ALGORITHMS

An open competition for the crypto algorithms for the 21st century.

The NESSIE project (New European Schemes for Signatures, Integrity and Encryption) (2000-2002) evaluates crypto algorithms that are essential to support e-commerce, e-government and electronic signatures. Today, the project announces its selection of the algorithms for the 2nd phase of the project. NESSIE plans to develop by the end of 2002 a strong portfolio of crypto algorithms that will protect the electronic society.

About one year ago, cryptographers from more than 10 different countries all over the globe submitted 42 crypto algorithms. Since then, researchers inside and outside the NESSIE project have tried to attack these algorithms, attempting to find weaknesses that would compromise their security. In addition, the efficiency of these algorithms (how fast are they?) has been assessed. As a consequence of this evaluation, the set of 42 contenders has been reduced to 24 candidates.

Crypto algorithms are mathematical formulas that are essential to protect electronic information. They come in different flavors. Encryption algorithms are essential to protect sensitive information such as medical data, financial information and Personal Identification Numbers (PINs) from prying eyes. The project distinguishes between three types of encryption algorithms: block ciphers, stream ciphers and public-key encryption algorithms. Digital signature algorithms (in combination with hash functions) replace manual signatures in electronic transactions. A similar role can be played by MAC algorithms. Identification protocols allow to securely establish the identity of the party at the other end of the line.

Fourteen months from now, the NESSIE project will publish a final set of recommendations with the best crypto algorithms of each type. The project also intends to input these algorithms to standardization bodies such as ISO, IETF and IEEE.

NESSIE has selected the following contenders for the 2nd phase:

Block ciphers:

- **IDEA**: MediaCrypt AG, Switzerland;
- **Khazad**: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium;
- **MISTY1**: Mitsubishi Electric Corp., Japan;
- **SAFER++₆₄**, **SAFER++₁₂₈**: Cylink Corp., USA, ETH Zürich, Switzerland, National Academy of Sciences, Armenia;
- **Camellia**: Nippon Telegraph and Telephone Corp., Japan and Mitsubishi Electric, Japan;
- **RC6**: RSA Laboratories Europe, Sweden and RSA Laboratories, USA;
- **SHACAL**: Gemplus, France.

Stream ciphers:

- **SOBER-t16**, **SOBER-t32**: Qualcomm International, Australia;
- **SNOW**: Lund Univ., Sweden;
- **BMGL**: Royal Institute of Technology, Stockholm and Ericsson Research, Sweden.

Public-key encryption:

- **ACE Encrypt**: IBM Zurich Research Laboratory, Switzerland;
- **EPOC-2**: Nippon Telegraph and Telephone Corp., Japan;
- **PSEC-2**: Nippon Telegraph and Telephone Corp., Japan;
- **ECIES**: Certicom Corp., USA and Certicom Corp., Canada
- **RSA-OAEP**: RSA Laboratories Europe, Sweden and RSA Laboratories, USA.

MAC algorithms and hash functions:

- **Two-Track-MAC**: K.U.Leuven, Belgium and debis AG, Germany;
- **UMAC**: Intel Corp., USA, Univ. of Nevada at Reno, USA, IBM Research Laboratory, USA, Technion, Israel, and Univ. of California at Davis, USA;
- **Whirlpool**: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium.

Digital signature algorithms:

- **ECDSA**: Certicom Corp., USA and Certicom Corp., Canada;
- **ESIGN**: Nippon Telegraph and Telephone Corp., Japan;
- **RSA-PSS**: RSA Laboratories Europe, Sweden and RSA Laboratories, USA;
- **SFLASH**: BULL CP8, France;
- **QUARTZ**: BULL CP8, France.

Identification schemes

- **GPS**: Ecole Normale Supérieure, Paris, BULL CP8, France Télécom and La Poste, France.

At this stage, no substantial weaknesses have been identified in any of the finalists. However, designers have been invited to make minor alterations to the algorithm to address any security concerns identified during the first phase. It is believed that each of these candidates has the potential to offer a very high security for the next decades.

The evaluation has been a fully *open* process based on published evaluation criteria. A significant effort has been spent by the project team. In addition, feedback has been received from the global

cryptographic community; all comments have been made public. The project has interacted with a project industry board, which consists of representatives from the key European security vendors and users. Two open workshops have been held to discuss the candidates: the first in November 2000 in Leuven, Belgium, and a second workshop in mid September 2001 in Egham, England. Detailed evaluation reports on security and performance, as well as a document motivating the selection for the 2nd phase are available at <http://www.cryptonessie.org>.

NESSIE is inviting the community at large to further analyse the candidates for the 2nd phase, and to offer comments on their security, performance and intellectual property status. All the candidates of the 2nd phase will be discussed at a workshop in November 2002. The project is accepting comments until mid November 2002. The final selection will be announced by December 2002.

NESSIE is a research project within the Information Societies Technology (IST) Programme of the European Commission (IST-1999-12324). The project partners are:

- Katholieke Universiteit Leuven (Belgium), coordinator;
- Ecole Normale Supérieure (France);
- 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).

For more information about NESSIE, see our web site <http://www.cryptonessie.org>.