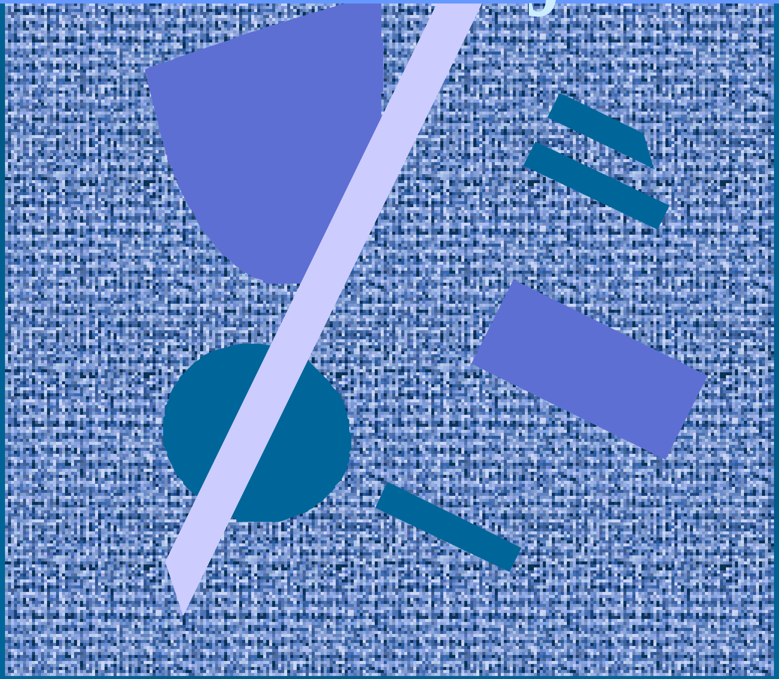
# NESSIE

## Project Overview



# NESSIE

# NESSIE

## New European Schemes for Signature, Integrity and Encryption

- Fifth Framework Program
- 2 300 000 Euro funding
- 8 Partners from 7 countries

- www.cryptonessie.org

# NESSIE: 5th Framework R&D Project (2000-2002)

- put forward a portfolio of strong cryptographic primitives that have been obtained based on an OPEN call and an OPEN evaluation process
- deliver input to AES
- develop evaluation methodology and software toolbox
- consensus building and dissemination
- strengthen European research and industry

# NESSIE partners

- Katholieke Univ. Leuven (Belgium)
- Ecole Normale Supérieure (France)
- Fondazione Ugo Bordoni (Italy)
- Royal Holloway, Univ. of London (UK)
- Siemens AG (Germany)
- Technion (Israel)
- Univ. Catholique de Louvain (Belgium)
- Univ. i Bergen (Norway)

# Some history: the 80s - RIPE

- RACE 1040 RIPE (Race Integrity Primitives Evaluation) (1989-1992)
- Open call for integrity primitives (hash functions, digital signature schemes, entity authentication protocols)
- Many of these schemes have since then surfaced in standards (RIPEMD, ISO 9796, ISO/IEC 11770-3)
- Several important attacks: MD4, MD5, ...

# NESSIE versus AES

- NESSIE will contribute European viewpoint to AES
- there are technical issues (smart cards)
- not a “me too”
  - broader scope (RIPE+AES)
  - legitimate concerns over lack of evaluation effort
  - some concerns over objectivity
  - “if we could start all over again”

# NESSIE Primitives

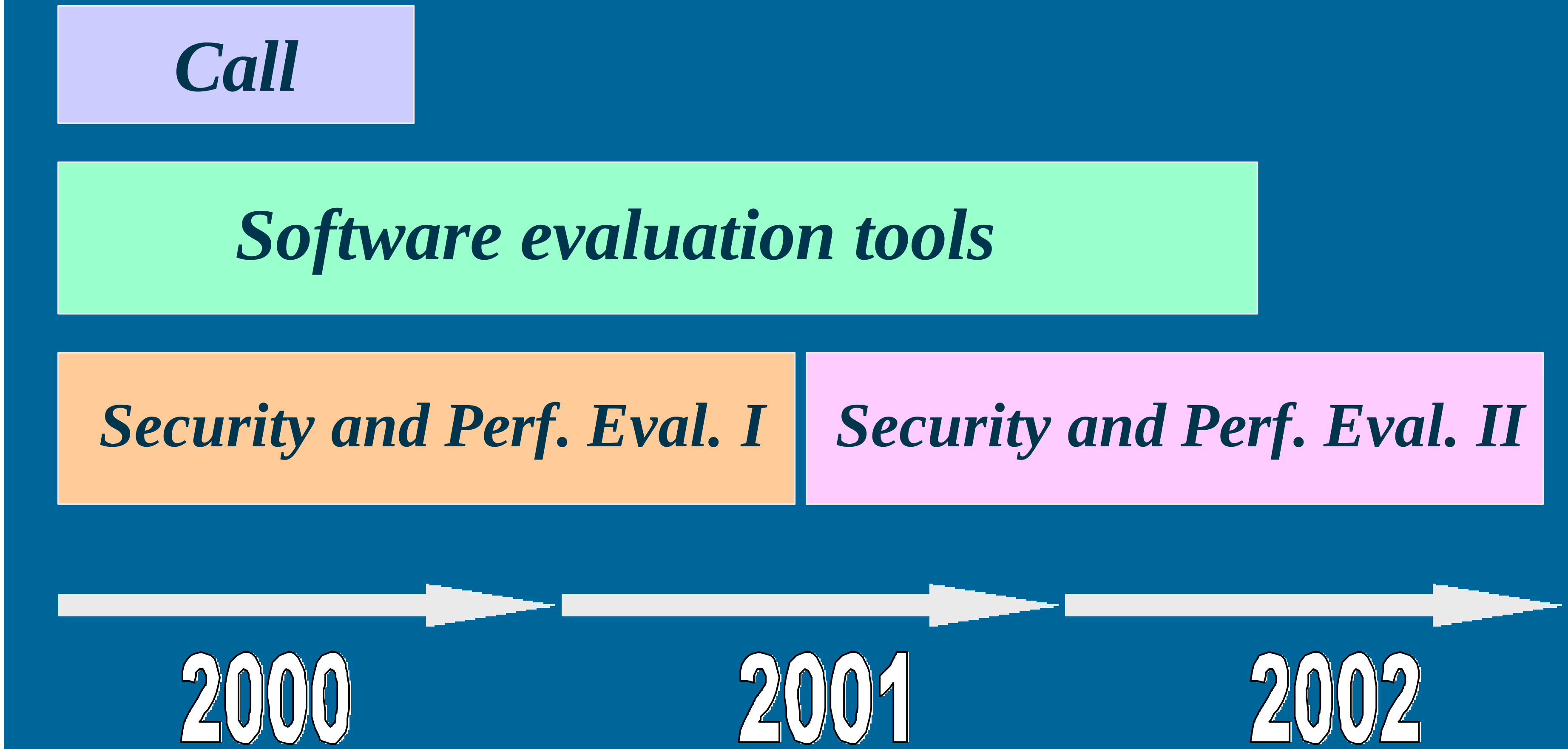
NESSIE is broader than DES or AES Calls

- Block Ciphers
- Stream Ciphers
- Hash Functions and MACs
- Pseudo-random Functions
- Asymmetric Encryption, Signature, and Identification Schemes

# NESSIE: technical approach

- open call (includes evaluation methodologies and criteria)
- development of software for evaluation toolbox
- security and performance evaluation in two rounds
- consensus building and standardisation activity

# NESSIE timing



*Call*

*Software evaluation tools*

*Security and Perf. Eval. I*

*Security and Perf. Eval. II*

2000

2001

2002

# NESSIE Submissions

- 16 Block Ciphers, including
  - Hierocrypt-3 and Hierocrypt-L1
  - Khazad
  - MISTY1
  - RC6
  - SAFER++
  - SC2000

- 5 Stream Ciphers
- 4 Hash Functions and MACs
- 5 Asymmetric Encryption Schemes
- 7 Digital Signature Schemes
- 1 Asymmetric Identification Scheme

# NESSIE Project Industry Board

- provide guidance on: type of primitives, evaluation criteria, intellectual property,…
- technical input: performance evaluation,…
- standardisation strategy (CEN, ETSI, IETF, ISO/IEC, …) and consensus building
- meeting: twice per year

# Project Industry Board: current members

- Algorithmic Research (Israel)
- Amtec SpA (I)
- Cryptomathic (DK)
- De La Rue Card Systems (F)
- Europay Intern. (B)
- Gemplus (F)
- Hewlett-Packard Laboratories (UK)
- Isabel (B)
- KPN Research (NL)
- Nokia (Finland)
- NDS (Israel)
- Racal Security and Payments (UK)
- S.W.I.F.T. (B)
- Telenor Research (N)
- Telsy Elettronica (I)
- Thomson-CSF (F)
- Utimaco (D)
- Vodafone (UK)

# Thank You