

# 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>	D11
<b>Title of Deliverable</b>	Internal evaluation report - Year 1
<b>Nature of the Deliverable</b>	
<b>Document reference</b>	NES/DOC/KUL/WP8/D11/1
<b>Contributing WPs</b>	WP8
<b>Contractual Date of Delivery</b>	Y1M12
<b>Actual Date of Delivery</b>	Y1M12
<b>Authors</b>	Eli Biham      Technion Lars Knudsen    UiB Keith Howker    KUL
<b>Abstract</b>	An assessment of the progress of the project during its first year, prepared by an internal evaluation team.
<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.

## **Document control**

### **Document History**

Previous drafts have been distributed for comment within the project team.

This is the first formal issue of the internal evaluation.

### **Changes forecast**

Any recommendations or corrections arising from the annual review will be incorporated.

## **NESSIE Internal evaluation report**

### **Summary**

This report is prepared by the internal evaluators appointed by the Project for Year 1, JAN/DEC-2000.

The purpose is to provide an objective assessment from the project's point of view of the progress and achievements of the project during this period and, in particular, to identify any improvements and adjustments that should be considered for the subsequent periods.

The achievements of the project and results to date are clearly identifiable, but the scope for improvement requires considerable introspection and reflection on the part of the participants.

Technically the project has performed well, meeting its planned goals and milestones during the year, with no accumulation of petty deficiencies at the end of the period.

Administratively, the project team could have performed better, being late in delivering its standard reports and cost claims throughout the period. This perhaps reflects the technical orientation of the participants, and a natural reluctance to sacrifice time to lowly form-filling. However the performance of late has improved, a situation to be maintained for the future.

The following sections of the report address each of the active workpackages in turn.

The final section gives the evaluators' conclusions and recommendations.

### **WP1 Call for Primitives and Testing Methodologies**

The call was made properly and on time (M1.1; M1.2). The report detailing the call (D2) was produced on time (M1.3), but only delivered after some administrative delay.

Response to the call was very enthusiastic: 39 primitives and 1 testing methodology were received. Interaction with submitters was good (M1.4). No submissions were rejected (M3.2).

The workshop was held as planned (M1.5). The report on the results of the call (deliverable D07) has recently been made available, again after some internal delay (M1.6). Most of the information in this report may be found in the status (review) report for Year 1.

### **WP2 Toolbox**

The purpose of WP2 is to provide tools for the analysis of the NESSIE submissions. This workpackage is making good progress.

Part of the RIPE tools developed by the RACE 1 project have been examined; a software interface layer has been proposed to improve the usability of the tools.

Several new tools have been developed, such as Dyadic Complexity Test, Percolation Test and Constant Runs Test, and supporting software for these tools.

A new set of tools has been developed that assists in the analysis of some block ciphers.

Work to date has been concentrated on the requirements for tools for block ciphers and stream ciphers. Tools for some of the other types of primitive have not yet been developed. This is the main outstanding item of this workpackage. Further research will be directed to developing tools for other classes of primitives.

The work will continue in three parallel streams:

- examination and possible adaptation of the other RIPE tools;
- design and implementation of the new tools;
- enhancement of the existing tools.

## **WP3 Security evaluation I**

There has been much activity within this workpackage, and the Security Evaluation is judged to be proceeding well. Many papers and reports on the submitted protocols are already available, well ahead of the end of WP3 and its final deliverable (D13, Y2M06).

As a result of good communication with those responding to the NESSIE call, all submissions were brought into conformance with the published requirements and criteria, and no rejections (M3.2) were required.

In the first phase of the workpackage a considerable number of NESSIE documents were input to the AES process. Most notable was a joint effort by all partners containing comments about the five final block ciphers that was submitted to NIST (D04, M3.1). As NESSIE partners had connections with three of five AES finalists, the security evaluation section of this joint report concentrated on the two remaining candidates. However NESSIE partners made individual comments on all five finalists. Most of the results on AES from NESSIE were presented at the third NIST workshop on the Advanced Encryption Standard in New York April 2000. In addition, NESSIE partners also contributed to the NIST workshop on modes of operation for AES, held in Baltimore USA, October 2000.

In the brief duration of the second phase so far, results on certain NESSIE submissions have already been achieved. The technical quality of these results is in general high and several documents have been submitted for presentation at the Fast Software Encryption Workshop in Japan in April 2001. Moreover, some of the work has already broken, or pinpointed a severe weakness in submitted primitives. These results indicate that several of the NESSIE submissions are unlikely to be recommended by the NESSIE project.

The report on methodology for security evaluation is recently available on the web page, following distribution of the draft within the project for comment (M3.3; D10). Formal delivery is expected to take place imminently.

It is felt that this workpackage has performed extremely well and produced many results. It is anticipated that this development will continue in the second year of NESSIE. However, it is also felt that the collaboration between the partners could be improved. This can be attributed partially to the fact that some partners have never worked in a European collaborative research project before, and that 6 new researchers have joined during the first year. One change which has been made is to assign pairs of evaluators at different partners to the same primitives, which will lead to a natural collaboration between partners.

## **WP4 Performance Evaluation - I**

This workpackage was started late, due to recruitment delays, but is now working according to plan. In November (two months later than plan) the report on methodology for comparing the performance of the primitives on a fair and equal basis was distributed.

As the work done in the month between the submission close date and the workshop was completed earlier than expected, an interim report on the submitted block ciphers could be given at the NESSIE workshop in November. An initial performance comparison was presented showing absolute and relative speeds of the block ciphers, demonstrating that performance claims of some submitters were not accurate.

## **WP7 Dissemination**

The Project Industry Board (PIB) was set up (M7.1) successfully and two productive meetings held. The project web site was created (M7.2) carrying the Project Presentation (M7.3, D1) and call information, and this contributed to good visibility of NESSIE, and good response to the call.

The first workshop (M7.5, D8) was very successful with good attendance and high quality presentations by submitters.

Dissemination and Use plan has been neglected schedule and was not available (M7.4, D5) at the time of writing. The project has to be better aware of the need to attend to these possibly less exciting tasks.

## **WP9 Project Management**

The Project Co-ordinator organized all the PCC/PMC, Forum and PIB meetings according to plan, and draft minutes were made available shortly after the meeting; however, the distribution of final reports on the earlier meetings was often delayed.

Project reports to the Commission have also suffered from delays in the final delivery. The Periodic Management Report (PMR) for the first and third quarters have been provided. The PMR for the second quarter is part of the Periodic Progress Report (PPR) for the first half, which has been provided.

The report for the fourth quarter is not available at the time of writing. It is recommended that PMRs will be provided separately from the PPR (and can then be attached as an appendix to the PPR).

The draft yearly report (second draft) is available within the project for final approval, but is not yet on the web page at this time. It does not contain the missing PMRs and PPR.

The quality plan (M9.1) was written after some delay.

Again the project as a whole needs to pay appropriate attention to the need for timely reports which provide a fuller understanding between the Co-ordinator and Project Officer about the progress of the project.

### Progress against project objectives

1. to publish an open call for cryptographic primitives, and to solicit submissions;	achieved
2. to develop generic and specific tools to support the evaluation;	achieved
3. to provide joint comments on the AES finalists;	achieved
4. to select from the submitted primitives a recommended subset; the main criterion for the selection process will be based on security and requirements of applications; other criteria will include performance, and flexibility; it will consist of two phases: <ul style="list-style-type: none"> <li>• preliminary screening and first evaluation;</li> <li>• thorough evaluation;</li> </ul>	<p>phase 1 of the evaluation process is progressing according to plan</p> <p>not planned in Year 1</p>
5. to develop a methodology for security and performance evaluation of primitives;	a NESSIE methodology is developing based on a standard approach to each class of primitive, and a recommended application of the tools
6. to disseminate results through three open workshops (one near the end of the first year, one half-way the project, and one near the end of the project) and scientific publications;	successful first workshop; two meetings of the Project Industry Board
7. to build consensus within a project industry board, that will be consulted on a regular basis;	two meetings of the Project Industry Board held
8. to input results to standardisation bodies;	project partners are active in relevant standards making bodies and will be able to propagate and support NESSIE results
9. to meet emerging generic security requirements of global networks and ubiquitous embedded systems, taking into account scalability requirements	the requirements of industry sectors are a major concern of the PIB

## **Conclusions and recommendations**

### **General**

There was a delay in the final approval of the NESSIE project by the Commission. This led to a serious delay in the planned recruitment of academic research workers, who are scarce commodities in a field offering high rewards in the commercial sector. Compensation for the shortfall in manpower in the early part of the project was provided by the increased involvement from its senior (unfunded) academic experts.

The withdrawal of FUB has further increased the load on the other participants, but this has again been accommodated. The lack of any specific expertise from that partner does not appear to have had a significant impact.

A new workplan will be proposed that re-allocates the FUB budget to the existing participants, rather than seeking to replace FUB.

### **Technical**

The technical performance of the project is well up to its commitments and expectations. The technical goals for Year 1 have been met successfully.

There was some disappointment with the overall spectrum of the submissions in response to the call, even though it was anticipated that the emphasis would inevitably be on block ciphers – possibly in the aftermath of AES. The project could possibly consider re-opening the call for certain specific categories.

It has been observed that communication between partners has occasionally been faulty. Many of the project participants have a long history of working together in informal research efforts; but they should not make undue assumptions about the operation of this project, and may need to make extra effort to work more as a team

### **Administrative**

The project should ensure no further instances of delays in making its formal reports and deliverables to the Commission. This has been mainly attributable to slowness and some miscommunication in the final delivery process rather than lateness in achieving results.

Project partners appeared to have been somewhat reluctant to claim their costs, resulting in annoying delays to the submission of the Integrated Claim for Period 1. The project team also needs to address this.

Both an internal and an external website have been established; these web pages have been maintained in a timely way, and have resulted in an effective internal communication.