Appendix 4

Part 2

Comments of Physikalisch-Technische Bundesanstalt (PTB)

Comments on the Draft Report of the Commission on Electronic Voting
Version 6.0, 18 June 2004

PTB wishes to comment on selected aspects of the draft report. The comments are restricted to testing activities performed at PTB and may contribute to understand and evaluate the tests. They cover basic working principles, explanations of unresolved findings, a comment on audit information generated by the system, and information to clear apparent misunderstandings.

Aspect 1: Working principles (Reference: Appendix 2B, section 2.2 "Software Assurance", pp.132/133)

Comment:
Software tests at PTB have been performed by the Software Testing Laboratory, which is accredited according to ISO/IEC 17025. The accreditation commits the laboratory to carry out software tests in accordance with recognised international standards as, e.g. ISO/IEC 9126, ISO/IEC 12119, ISO 9241, ISO 9899, ISO 12207 and ISO/IEC 6592.

All testing results presented are based on well-defined and documented testing procedures. The testing procedures have been derived from the international standards mentioned above and from state-of-the-art testing methods.

Owing to the documentation of each individual test scenario in test protocols, which are archived at PTB, each of the tests performed in the Software Testing Laboratory is repeatable. The testing method used and the testing procedure applied belong to the information laid down in protocols.

Aspect 2: Explanation of findings (Reference: Appendix 2A "Evaluation of previous testing, part 1", pp. 98-104)

- Issue 5 (Reference Statement: "Download of election information from IES to ballot module can be checked using manual procedures. It has not been verified that there is no possibility to transfer 'extra' data from IES to ESI2 via the ballot module")

Comment:
PTB tests have confirmed that there is no possibility to transfer "extra" data via the ballot module. The complete extent of read and write accesses to the ballot module has been inspected. Type and extent of data, which are transferred from the ballot module to the voting machine, are well-defined and accepted. However, because this issue did not belong to the requirements given, these test results were not stated in the test report.

- Issue 15 (Reference Statement: "The test documentation does not, however, explain what happens if power fails while a vote is being stored in the ballot module, e.g. 2 of 4 write operations have been completed, and the 3rd is underway. It needs to be clarified whether this is possible, and whether it might corrupt the module's vote memory."

Comment:
The storage process in case of a power failure and the corresponding reconstruction of votes have been tested by means of code inspection. The implementation of voting machine functions allows the interruption of the vote storage process at any point in time, even in the midst of the four vote copies.

- Issue 18 (Reference Statement: "It has not been tested that the backup is an exact copy

of the primary ballot module")

Comment;
Code inspections of certain functions have provided test results that also concern issue 18. However, the results are not part of the test report because this issue was not included in the requirements given. After creating the backup module, check sums of both the whole primary ballot module and the whole backup module are generated and compared. In case of deviations, the vote counting at close of poll is not started. The ballot module is not set on the status "analysed" and the voting results are not issued. The corresponding failure is indicated and recorded, and the execution of the voting machine program is stopped.

Aspect 3: Comment on audit information generated by the system
(Reference: Appendix 2B "Review of Hardware, Software Security and Testing", Section 2.1 (Security Policies), Item 3.a., p.131)

Reference statement:

"In general, only the external operations of the systems appear to be audited. For example, users are required to complete paper documents and attach printouts from the VM and IES software. There does not appear any audit information generated and stored automatically as the system is being used."

Comment:
The system generates 4 types of audit information:

(1) "Open Poll Statement" ,
(2) "Close Poll Statement",
(3) Information on so-called "Settings",
(4) Information on "Security Checks".

The different types of audit information consist of various identifications of modules, numbers of votes, checksums, and other dates and characteristics.

The audit information of the types (1) and (2) must be checked by the election authorities before and after the polling process, respectively. The types (3) and (4) are not prescribed, but may be easily found and made visible.

Aspect 4: Clearing of misunderstandings (Reference: Appendix 2C, section 2.1 "Test on the Design of a Voting Machine, Physikalisch-Technische Bundesanstalt, 1998, 2003, p. 159))

The following items of the presentation in the draft report are based on misinterpretations:

- Bullet 3: **Reference: "The voting machine ID can be changed. This could allow undocumented exchange of machines…."**
Comment: Changing of voting machine ID is only possible in the "service mode". Usually, only PTB and the manufacturer Nedap are able to switch on the "service mode".

- Bullet 5: Reference: "The voting machine backup module is cleared when a new ballot module is inserted. This seems to create the possibility of inadvertently destroying backup data."
Comment: There are only two possibilities to clear the backup module:
(1) At the beginning of the vote counting at close of poll, immediately before creating the new backup. This backup is automatically done.
(2) Driven by an explicit command (poll staff).

There is no automatic backup when a primary ballot module is inserted.

- Bullet 6: Reference: "In certain cases the voting machine may be used to a reduced extent. (Any variation in the behaviour of the machine is a source of potential complications and errors)

Comment: In case of faulty voting machine components, those functions cannot be used which are associated with the faulty components. So the poll can be closed and the votes counted, if, e.g., the printer is out of service.