# Final Report
# P270 DRDC Ottawa V&A Device System

Labcal.Group
Labcal.Group, 400 boul. Jean-Lesage, hall Ouest, bureau 30, Québec, Canada

Labcal.Group
Labcal.Group, 400 boul. Jean-Lesage, hall Ouest, bureau 30, Québec, Canada

Project Manager: S. Dahel 613-993-9949

Contract Number: W7714-010573/001/SV

Contract Scientific Authority: J. Savoie 613-993-5132

**DEFENCE R&D CANADA - OTTAWA**

Contractor Report

DRDC Ottawa CR 2003-039

March 2003


# Final Report

## P270 - DRDC-Ottawa V&A Device System

by Labcal.Group

Version 001
2003-03-30 16:03

Labcal.Group
400 boul. Jean-Lesage, hall Ouest,
bureau 30
Québec (Québec)
G1k 8W1
T (418) 692-3137
F (418) 692-1488
www.labcal.com

# DOCUMENT DISTRIBUTION LIST

| Name | Date |
|---|---|
| Carl Boudreau | 2003-03-11 |
| Martin Bilodeau | 2003-03-11 |
| François Boutet | 2003-03-11 |
| Frédéric Chabot | 2003-03-11 |
| Guy Dufour | 2003-03-11 |
| Daniel Martel | 2003-03-11 |
| Martin Ouellet | 2003-03-11 |
| Michel Roux | 2003-03-11 |
| Jean Savoie | 2003-03-31 |

# RECORD OF CHANGES

| Version | Rev. | Date | Author | Modifications |
|---|---|---|---|---|
| 001 | 000 | 2003-01-29 | Labcal.Group | Document creation |
| 001 | 001 | 2003-03-11 | Labcal.Group | Initial distribution |
| 001 | 002 | 2003-03-28 | Labcal.Group | Adjustments |

# TABLE OF CONTENTS

# ACRONYMS

| Term | Meaning |
|---|---|
| API | Application Program (Programming) Interface |
| CBIS | Content Based Information Security |
| CC | Common Criteria |
| CCD | Compatible Connected Device |
| CIDD | CBIS Integrated Design Document |
| CSP | Critical Security Parameter |
| DAVE | Verification and Authentication Data Entry and Display Device (or Trusted DAVE) |
| DRDC | Defence Research and Development Canada |
| EAL | Evaluation Assurance Level |
| LCD | Liquid Crystal Display |
| NA | Not Applicable |
| OS | Operating System |
| PC | Personal Computer |
| PIN | Personal Identification Number |
| TEMPEST | Telecommunications Electronics Material Protected from Emanating Spurious Transmissions |
| V&A | Verification and Authentication |

# DEFINITIONS

| Term | Meaning |
|---|---|
| Challenge-response | A common authentication technique whereby an entity is prompted (the challenge) to provide some information that only it can deliver (the response). |
| Trusted Path | Use of a challenge-response authentication protocol to establish an encrypted communication over what would otherwise be an unsafe channel. |
| Validation phrase | Word or group of words entered by the user during enrollment, securely stored in the authentication server and appearing on Trusted DAVE's display when the user inserts the token. It allows the user to make sure the device is a legitimate one, before typing his PIN. (In the demo version, if the 'Validation Phrase' field is left blank during enrollment, the feature will not be used and the phrase will simply not appear on the LCD during logon.) |

# REFERENCES

1. DRDC-Ottawa "Development of a Trusted Device for Authentication and Verification" RFP Document, 02-01-2002

2. System Requirements Specification, Three Factor Verification and Authentication Data Entry and Display Device, DRDC-Ottawa, Version 1.0, July 2001

3. Trusted DAVE SOW – Evaluation Plan – and System Requirement Specification

4. Technical and Management Proposal, Version 001, Labcal.Group, 11-03-2001

5. Standard Labcal, Processus de développement de projet

6. FIPS 140-2 Security Requirements for Cryptographic Modules, NIST, 05-25-2001

7. FIPS PUB 196 Entity Authentication Using Public Key Cryptography, 02-18-1997

8. CBIS Integrated Design Document (CIDD), Version 1.12, 06-12-2000

9. Low Cost Attacks on Tamper Resistant Devices, Ross Anderson1, Markus Kuhn21 Computer Laboratory, Pembroke Street, Cambridge UK, www.cl.cam.ac.uk/~mgk25/tamper2.pdf, 10-03-2002

10. Body Check: Biometrics Defeated, Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, 06-03-2002

11. Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication, 1994 January 11, http://csrc.nist.gov/publications/fips/fips1401.htm, 19-nov-2002

12. Building a High-Performance, Programmable Secure Coprocessor, Sean W. Smith Steve Weingart, IBM, October 16, 1998

13. Differential Power Analysis, Paul Kocher, Joshua Jae, and Benjamin Jun, Cryptography Research, Inc., http://www.cryptography.com/resources/whitepapers/DPA.pdf

14. Evaluating Differential Fault Analysis of Unknown Cryptosystems, [Published in H. Imai and Y. Zheng, Eds., Public-Key Cryptography, vol. 1560 of Lecture Notes in Computer Science, pp. 235-244, Springer-Verlag, 1999.], http://www.gemplus.com/smart/r_d/publi_crypto/pdf/Pai99dfa.pdf

15. Statistics and Secret Leakage [Published in Y. Frankel, Ed., Financial Cryptography (FC2000), vol. 1962 of Lecture Notes in Computer Science, pp. 157-173, Springer-Verlag, 2001.], Jean-Sébastien Coron, Paul Kocher, and David Naccache, http://www.gemplus.com/smart/r_d/publi_crypto/pdf/CKN01lea.pdf

16. Optical Fault Induction Attacks, Sergei Skorobogatov, Ross Anderson, University of Cambridge, Computer Laboratory, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/faultpap3.pdf

17. Comparative Biometric Testing, Version 2.11, International Biometric Group, 31-10-2002, http://www.ibgweb.com/reports/public/comparative_biometric_testing.html, 15-11-2002.

18. Best Practices in Testing and Reporting Performance of Biometric Devices, Version 1.0, Biometrics Working Group, 12-01-2000, http://www.cesg.gov.uk/assurance/iacs/itsec/documents/protection-profiles/media/BBP.pdf.

19. Biometric Technology Testing, Evaluation, Results, James L. Wayman, U.S. National Biometric Test Center, http://www.engr.sjsu.edu/biometrics/publications_technology.html

20. System Requirements Specification, P270 - DRDC-Ottawa V&A Device System, Labcal.Group, Version 001, Revision 004, 2002-10-14

21. Trust Analysis Comparison CBIS I&A / DREO V&A, , P270 - DRDC-Ottawa V&A Device System, Version 001, Revision 005, Labcal.Group, 2003-02-25

22. Two Design Concepts, P270 - DRDC-Ottawa V&A Device System, Labcal.Group, Version 001, Revision 005, Labcal.Group, 2002-10-29

23. Definition of sub-component options, P270 - DRDC-Ottawa V&A Device System, Version 001, Revision 005, Labcal.Group, 2002-11-01

24. DRDC - Trusted DAVE Project, Preliminary Design, Michel Roux, Labcal, 2002-10-23

25. Detailed Design, P270 - DRDC-Ottawa V&A Device System, Version 004, Revision 003, Labcal.Group, 2003-01-08

26. Security Target, P270 - DRDC-Ottawa V&A Device System, Version 004, Revision 001, Labcal.Group, 2002-12-12

27. Test Plan, P270 - DRDC-Ottawa V&A Device System, Version 003, Revision 002, Labcal.Group, 2003-03-

28. User Guide, P270 - DRDC-Ottawa V&A Device System, Version 002, Revision 000, Labcal.Group, 2003-03-

29. Monthly Report – Jan. 2003 Development of a Trusted Device for Authentication and Verification, Version 1.0, M. Roux, Labcal Technologies, 2003-02-20

**Table 1 – Deliverable Documents**

| Title | File name |
|---|---|
| System Requirements Specification | P270-P0-02A 001-004.pdf |
| Trust Analysis Comparison<br>CBIS I&A / DREO V&A | P270 Trust Analysis Comparison 001-005.pdf |
| Two Design Concepts | P270-P0-03A 001-005.pdf |
| Definition of Sub-component Options | P270-P0-03B 001-005.pdf |
| Preliminary Design | P270-P0-03C-001.ppt |
| Detailed Design | P270-P0-04A 004-003.pdf |
| Security Target | P270 Security Target 004-001.pdf |
| Test Plan | P270-P0-04B 003-002.pdf |
| Test Program | |
| User Guide | P270-P0-05B 002-000.pdf |
| Final Report | P270-Final Report 001-001.doc |
| Test Results Report | |

# PRELIMINARY NOTE

- In this text, use of the masculine is generic and applies to both the masculine and the feminine genders.

# ABSTRACT

Trusted DAVE project's main purpose was the development of a trusted device for authentication and verification. Analysis involved in this R&D project determined the following choices of technologies: contact smart card, capacitive fingerprint sensor, Intel StrongARM SA-1110 CPU, Intel Flash memory, Neutrino™ real-time operating system from QNX, use of the Five-Pass Authentication Protocol, etc. And, more specifically for tamper protection: multi-layer flexible printed circuit, metal case, special stacking of the printed circuit, use of double access memory, Shamir power supply, etc.

A prototype and a demonstration system were developed. Although different to some extent from the designed device, this proof of concept helped evaluate performance and feasibility. It will also be useful in demonstrating the concept to other parties involved.

# 1. PROJECT OBJECTIVES

The DRDC-Ottawa Trusted DAVE[1] research and development project involved the "analysis, design, development and testing of a three factor Verification and Authentication Data Entry and Display device"[2] designed to enhance security for computer systems used to process classified or sensitive information. "The system concept for the V&A was derived from the US project conducting R&D into Content Based Information Security (CBIS)".[2] DRDC "decided to explore the development of a more flexible three factor V&A device that could have applications to other secure systems".[2] The V&A device first role is to interact with the user to collect three factors of authentication: biometrics, a secure token and a PIN.

The device's main responsibilities, within the *overall system*, are the following[3]:

1) Scan user fingerprints and extract minutiae.
2) Read data from user's secure token, including the user's cryptographic key material, protect that data, read the user passwords.
3) Interrupt active operations on the V&A system after the electronic secure token has been removed or replaced and provide an indication of the interruption to the overall system.
4) Interact with the user by means of a LCD, audio feedback and an integrated keying device.
5) Accept and use secure authentication (including the V&A System's cryptographic key(s)) of the overall system.
6) Provide at least one physical connection interface with the overall system using an Industry Standard.
7) Provide one or more trusted paths that terminate at a trusted point on the overall system.
8) Securely communicate correctly formatted data over trusted paths to and from the overall system.
9) Receive and retain authorization data from the overall system resulting from the user authentication process initiated by the V&A System.
10) Provide tamper resistance through integrated tamper proof technology within the device.
11) Securely send event information over a trusted path to the overall system.

Subjacent to the fingerprint reading, an other main objective was to include liveness detection to ascertain that the biometric information acquired by the system is directly related to a living subject.

[1] Trusted Device for Authentication and Verification
[2] Trusted DAVE SOW – Evaluation Plan – and System Requirement Specification
[3] See: System Requirements Specification, Labcal.Group, Version 001, Revision 004, 2002-10-14

# 2. PROJECT CHARACTERISTICS

## 2.1. HYPOTHESIS

Here is the list of assumptions and hypothesis that were used:

- A secure endpoint is available to connect the V&A device to the workstation. One possible purpose of this endpoint is to control all information flow between the V&A device and a centralized server.
- It is assumed that system administrators and maintenance personnel are non-hostile and trusted to perform all their duties in a competent manner.
- The system is used along with a coherent and well adapted security policy.
- All users are aware of the security policy and apply it thoroughly.
- In case of interruption, no substitute system will be used.
- The rest of the overall system is assumed to be secure.

## 2.2. CONSTRAINTS

Constraints that were imposed on the device are listed here:

- Use an electronic key distribution system.
- Use a centralized maintenance approach.
- Be mountable on a wall or sit on a desktop.
- Communication between the V&A device and the secure endpoint shall use an industry standard.
- Use industry standard interfaces for keyboards, displays, etc.
- Use an open source operating system.
- Operate in a normal office environment.
- Be able to interact with the US CBIS system.

## 2.3. RISKS

### 2.3.1. US CBIS Project

Since the device had to be able to interact with the US CBIS system, the lack of reliability of information available about the US CBIS project represented a major risk. As an administrative reorganization of the US CBIS project made its technical orientations uncertain, it was impossible to make our development perfectly compatible to the US system. Use of industry standard interfaces in our design partly mitigates that risk.

### 2.3.2. Intended Use

Although a Windows 2000 logon is the only application that was specified, we designed the system with adaptability in mind. This is less of a risk for a demonstration or proof-of-concept system.

### 2.3.3. Liveness Detection

An effective liveness detection component is part of the requirements for the device. Many companies in the industry are working on that problem; their solutions are proprietary and not scientifically tested. This is clearly a very difficult requirement to meet.

### 2.3.4. Experimentation

Because the project's budget and time span are very narrow, some validations based on experiments could not be conducted. This is especially true about liveness detection and tamper protection.

### 2.3.5. Overall System

The V&A device is only one part of the security system. The level of security assurance would be jeopardized if one element in the rest of the system was poorly designed. In that regard, many questions regarding the overall system's security and interoperability had to be addressed.

### 2.3.6. Evolution

Is it possible to allow the system to improve in the future and keep up with cryptography's advances. Modularity and reusability in the design is a good first step in pursuing this objective.

### 2.3.7. Cost

"What if the equation between the cost of the V&A Device and the security level desired cannot be achieved?"[4] Components were carefully chosen considering the cost factor (along with other aspects) versus every associated security level.

[4] Monthly Report – January 2003, Labcal.Group

# 3. DEVELOPMENT RESULTS

## 3.1. EFFORTS OVERVIEW

First, a review of background information on the CBIS and the DRDC project documentation and of the Common Criteria related material[5] was performed.

It allowed production of a non-formal Threat and Risk Assessment and comparison between CBIS I&A and DRDC V&A. We "gave arguments to why the Trusted DAVE authentication subsystem is more secure than the CBIS authentication subsystem."[6] The comparison work could have been more precise, had it not been of risks described in section 2.3.1 and 2.3.2. Nonetheless, the results of this assessment were used during Trusted DAVE's design.

Conducted concurrently, the review of System Requirement Specifications established a consensus on the list of requirements that a production level device should meet.

The next task was to list and describe the system sub-components, define the specifications for the interfaces and protocols allowing these components to interact with each other, identify strong and weak points for off-the-shelf items, compare state of the art technologies for subcomponents and make recommendations on which technology should be used in a production level unit. All these points were covered in the 'Definition of sub-component options' document[7]

This phase also dealt with presenting two alternative design approaches for the implementation of the V&A device. However, as many questions regarding the overall system's security and interoperability had to be addressed, the 'Two Design Concepts'[8] document was used to that purpose.

Labcal.Group then presented DRDC with the Preliminary Design. This was done in person by means of a presentation and conference where major issues were discussed.

[5] Including Protection Profiles listed in the Reference section, page 8.
[6] Trust Analysis Comparison CBIS I&A / DREO V&A, Version 001, Revision 005, Labcal.Group, 2003-02-25
[7] Definition of sub-component options, Version 001, Revision 005, Labcal.Group, 2002-11-01
[8] Two Design Concepts, Version 001, Revision 005, Labcal.Group, 2002-10-29

Task number four included the Security Target and Detailed Design documents. The Security Target document, although informal, is helpful as a global security and assurance level evaluation. The Detailed Design Document is a low-level explanation of the V&A device's design. It describes and explains all important design decisions and subcomponents choices. It also analyses these decisions and choices in view of the requirements a production level device would satisfy.

Concurrently to the development of the demonstration system, a Test Plan and a User Guide were produced. The Test Plan is applicable to a production level device as well as to the demonstration level device being developed. Conversely, the User Guide describes only the demonstration system.

## 3.2. TECHNOLOGIC CHOICES

The following technologies were chosen for the device[9]:

- Contact smart card technology was chosen for its flexibility and built-in cryptographic features
- Capacitive sensor technology was selected for its availability, low cost solidity, small size and design flexibility.
- We picked the Neutrino real-time operating system from QNX and the Momentics development environment mainly for the following reasons: good OS-development tools integration, driver availability, technical support, reliability, serviceability and real-time performance.
- Intel StrongARM SA-1110 main CPU was chosen because it is well supported, offers sufficient computing power and is promised an interesting future.
- Intel Flash memory is used because it is very widespread and not very expensive.
- We selected an authentication protocol based on the Five-Pass Authentication Protocol described in section 6.2 of ISO/IEC 9798-2:1999.
- Multi-layer flexible printed circuit is used as an intrusion detection envelope. Arrangement: TGVTTVGT (T= trace layer, V=Vcc et G=GND)
- A metal case acts as a Faraday cage against electromagnetic emissions, is low cost and fast to produce.
- We strongly suggest stacking of the printed circuit in a pattern that reduces electromagnetic wave emission.
- Use of double access memory makes it possible to read and write memory in the same operation and thus decreases emitted noise.
- A Shamir power-supply uncouples the components containing secrets from the external power-supply.

[9] See Definition of sub-component options, Version 001, Revision 004, 2002-11-01 and Detailed Design, Version 004, Revision 003, Labcal.Group, 2003-01-08

- Removal detector for: keyboard, smart card, LCD, fingerprint sensor and casing.
- Wall-plug powered Electronic Tamper Detection.
- Microprocessor supervisory circuits, to allow powering of the low power section, generate the board RESET when sector power is out, etc.
- Use of bus switch. This component is used to isolate the electric signals from the USB port, fingerprint sensor and LCD display, which are connected to the CPLD.
- Use of a switch debouncer to simplify the keypad control software.
- Altera's MAX 3000A Family CMOS EEPROM Base CPLD, to control peripherals and memory.
- Permanent RAM memory used for secrets conservation in case of power outage.

## 3.3. DEMONSTRATION SYSTEM

### 3.3.1. Description

The purpose of the Trusted DAVE demonstration system is to test and demonstrate the main capabilities of the V&A device, without implementing all the feature that would normally be present in a production system.[10]

In short, the demonstration system is materially composed of the authentication server, a SmartPrint™ enroller, a workstation and a Trusted DAVE device. The server includes the authentication database, enrollment software, Trusted DAVE configuration and enroller testing software, a real-time event viewer and login manager, and the Trusted Dave Authentication Service, program and libraries.

The workstation includes a software secure endpoint, i.e. a software that participates as one of the Trusted paths' components, to allow secure intercommunication between itself, the V&A device and the authentication server. The workstation also contains a custom made Windows logon application and a status viewer.

A SmartPrint™ Enroller is used to perform enrollments and, since our comparison libraries were never ported to the PC, the demonstration system also uses it to make comparison between the template received and the user's template stored in the database.

Apart from this characteristic, the demonstration system is essentially composed of the same basic elements as the overall system referred to in the projects documentation.

[10] User Guide, Version 002, Revision 000, Labcal.Group, 2003-03-06

### 3.3.2. Limitations

Liveness detection and tamper protection are the main discarded device features. It was unthinkable to include them in the demo because the time and budget we had were too limited. However, these subjects were carefully analysed during the high level design phase. The detailed design plans include well defined tamper protection mechanisms. In contrast, as the field of life detection in biometric devices could be the scope of a research project in itself, no liveness detection device is included in the low level diagrams.

Other features mentioned earlier in the project were excluded from the demonstration device:

- The token does not offer access to several Windows user accounts;
- Corollary: username and domain cannot be selected from a menu.
- The V&A device does not use an operating system.
- Split knowledge secret insertion.
- Key erasure is implicit as the configuration software replaces secret keys instead of just erasing them.
- Remote re-flashing and associated secure boot loader .
- A contactless card reader was implemented instead of a contact card reader.
- Random number generation is done by software and not by a hardware component.
- Double access memory.
- Crypto-controller (Dallas DS5240).
- Smart card writing: the demo device does not write on the card.
- The fingerprint template is not time stamped.
- The keypad does not have backlighting capability.

# 4. ACCEPTANCE TESTS RESULTS

This section details how Trusted DAVE demonstration system performed with regards to its acceptance tests. Due to the project's short time span and limited resources, requirements that are not covered by this section are dealt with by analysis and reporting, particularly in the Detailed Design document[11] and the Test Plan[12]. See section 3.3.2 for an overview of the demonstration system limitations.

## 4.1. SRT0017 DEVICE INITIALIZATION

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | Software installation has been performed on the authentication server. | |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Using the configuration cable, connect Trusted DAVE's configuration port to one of the authentication server's serial ports. | NA | |
| 2 | Connect or re-connect Trusted DAVE's power supply, let it boot and when "WAITING FOR WORKSTATION" appears on its LCD, press DAVE's F4 key. | "SETUP DEVICE TO EXIT RESTART" will be displayed on the LCD. | |
| 3 | Launch the authentication server's 'TrustedDave & Enroller Configuration' software. | The V&A Initialization tab is displayed. | |
| 4 | Use the 'Options' menu to designate the COM port to which the unit's configuration cable is connected. | NA | |
| 5 | Enter and re-enter the Administrator password that will thereafter be used to authorize execution of the commands sent on the configuration port. | NA | |
| 6 | Click the 'Initialize' button. | If the unit has previously been initialized, you will be prompted to confirm the initialization.<br>The initialization function of 'TrustedDave & Enroller Configuration' software generates a random secret key, loads the Trusted DAVE with it and saves a copy in the database. | |
| 7 | Click on the 'V&A Commands' tab. Click on the 'Set Date and Time' button. | The Result displayed is 'Success!'. | |

[11] Detailed Design, Version 004, Revision 003, Labcal.Group, 2003-01-08
[12] Test Plan, Version 003, Revision 002, Labcal.Group, 2003-03-

| | | | |
|---|---|---|---|
| 8 | To further check that the initialization was performed successfully, you can perform tests SRT0002. | NA | |

**Special Considerations**

None.

**Notes**

## 4.2. SRT0008 ENROLLMENT

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | The enrollment officer is logged[13] on to enrollment station and the enrollment software is launched (use the appropriate start-menu shortcut to launch it). | |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Enrollment officer starts a chronometer and clicks on the 'Add User' button. | PIN entry window appears. | |
| 2 | Let the enrollee enter his PIN and validation phrase[14]. Click 'OK' | *User Selection* window appears. | |
| 3 | Select the appropriate Windows user, security role and security clearance.<br>Let the enrollee enter his current Windows user password and, if necessary, a new password. | Finger enrollment window number 1 appears. | |
| 4 | Let the user choose and enroll one finger. | Finger enrollment window number 2 appears. | |
| 5 | Let the user choose and enroll another finger. | Verification window appears. | |
| 6 | Perform verification: enrollee's scanned fingers and PIN are asked for and provided for token verification. | Verification is positive.<br>Confirmation message appears. | |
| 7 | Enrollment officer stops the chronometer. | Enrollment session is over. It took less than five minutes (SRQ0901). | |
| 8 | Alter template data in the server database.<br>Let the user try to authenticate to the system. | User fingerprints recognition fails. (SRQ1107) | NA |
| 9 | Restore the data.<br>Alter template timestamp in the server database<br>Let the user try to authenticate to the system. | User fingerprints recognition fails. (SRQ1107) | NA |
| 10 | Restore the data.<br>Alter template signature in the server database<br>Let the user try to authenticate to the system. | User fingerprints recognition fails. (SRQ1107) | NA |
| 11 | Restore the data.<br>Let the user try to authenticate to the system. | User fingerprints recognition succeeds. | NA |

**Special Considerations**

1. Verify testing conditions.
2. Execute steps 1 to 7. Verify number of trials: 1 or 2 trials for the whole cycle.
3. Steps 8 to 11 do not apply to the demonstration devices.
4. T.ILLENROL is prevented if FAR = 1/100 000

[13] If two enrollment officers are required by the security policy, the witness is authenticated before enrollments can take place. Also, please note that this will not be implemented in the demonstration system.

[14] Optional. See 'Validation phrase' in Definitions section.

**Notes**

Steps 1 thru 7: total enrollment time was 2,5 minutes, well within the five minutes limit required by SRQ0901.

## 4.3. SRT0012 POWER ON / SRT0013 POWER OFF

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | Initialized V&A device is required (connected to his endpoint and authentication server via network). | |
| 3 | The PC is already started. | |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Perform normal authentication and logon. Unplug the V&A device. | The device shuts down. The CCD and Windows lock the computer. An alert is sounded on the server, the event is logged and/or actions prescribed by the security policy are taken. | |
| 2 | Power on. Evaluate elapsed time between the device power cord is plugged and the device displays an invitation to insert token. | Power on including self-test and device authentication is no more than 6 seconds. | |
| 3 | Alter firmware and restart. | Device authentication fails. A message similar to "Device authentication failed" appears on the LCD. | NA |

**Special Considerations**

Step 3 does not apply to demonstration devices.

**Notes**

## 4.4. SRT0002 LOGON IN NORMAL OFFICE ENVIRONMENT

**Testing Conditions**

| # | Conditions | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | Initialized V&A device is required. | |
| 3 | Initialized token is required | |
| 4 | User is enrolled | |
| 5 | Normal office environment (+20° C to +25° C and 30 to 65 % of relative humidity) | |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Power on Trusted DAVE. | Upon power up, Trusted DAVE carries out its auto-diagnostic tests. A message is displayed to inform the user about self-tests' results. | |
| | | An event is recorded on the server. | |
| | | The device displays a prompt asking the user to insert his token in the reader. | |
| 2 | Insert secure token in token reader. | The user's validation phrase appears[15] and the user is asked for his PIN. | |
| 3 | Enter valid PIN. | Another prompt asks the user to put a specific enrolled finger on the fingerprint scanner. | |
| 4 | Put particular finger on fingerprint reader. | An other enrolled finger is specifically asked for. This prevents T.RESIDUAL. | |
| 5 | Put appropriate finger on fingerprint reader. | A prompt is displayed indicating that the authentication request in being processed. | |
| | | On successful authentication, the buzzer produces a sound and a generic message is displayed indicating that the authentication was successful. | |
| | | Upon successful session establishment, the date and time of the last successful and unsuccessful sessions establishment are displayed for 20 seconds. | |
| 6 | Continue on to the login application on the PC to choose which account to be logged in.♦<br>Choose one and presses '*OK*'. | The login application on the PC, in cooperation with the Server and Trusted DAVE, automatically logs the user into the account. | |
| | | An event is recorded on the server. | |
| 7 | Double click on the system tray application 'Trusted | The user's name, security role and security | |

[15] Optional. See 'Validation phrase' in Definitions section.

| | | | |
|---|---|---|---|
| | Dave status viewer' which is installed on the host workstation. | clearance are displayed on the PC screen. | |
| 8 | Wait *x* minutes, where *x* is the predefined inactivity period after which the workstation is locked by Windows. | The CCD and Windows lock the workstation. The user is prompted for his fingerprints and PIN. This is not an inactivity timeout. It should not be mistaken with the OS timeout.[16] | |
| 9 | Repeat step 3 to 5 and double click on the system tray application installed on the host workstation. | The user's name, security role and security clearance are displayed on the PC screen. | |
| 10 | Wait *x* minutes, where *x* is the predefined inactivity period after which the workstation is locked by Windows. | The CCD and Windows lock the workstation. The user is prompted to re-insert his token. | |
| 11 | Remove and insert the token. | The user's validation phrase appears and the user is asked for his PIN. | |
| 12 | Enter invalid PIN. | The PC stays locked. | |
| 13 | Remove token from device | The server registers the event (check event log) the workstation stays locked. | |

**Special Considerations**

1. Verify testing conditions
2. Execute step 1 to 8. Repeat the test but without authenticating again, the workstation should stay locked.
3. Check the desktop option, wall-mounted option, multi-line display, .

(♦): The multi-account feature will not be implemented in the demonstration system.

**Notes**

[16] Replaced by Windows Timeout

## 4.5. SRT0010 VERIFY FINGER SCANNING ORDER

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | Initialized V&A device is required (connected to his endpoint and authentication server via network). | |
| 3 | User is enrolled and has his or her token. | |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Power on Trusted DAVE | Upon power up, Trusted DAVE carries out its auto-diagnostic tests. A message is displayed to inform the user about self-tests' progress. | |
| | | The device displays a prompt asking the user to insert his token in the reader. | |
| 2 | Insert secure token in token reader. | The user's validation phrase[17] appears and the user is asked for his PIN. | |
| 3 | Enter PIN | Another prompt asks the user to put a specific finger on the fingerprint scanner. | |
| 4 | Try to logon using second finger when display asks for first. | Message similar to "Invalid fingerprint" is displayed.<br>V&A buzzer beeps. | |

**Special Considerations**

None

**Notes**

[17] Optional. See 'Validation phrase' in Definitions section.

## 4.6. SRT0006 CHANGE PIN

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | User is already authenticated by server and logged on. | |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Press V&A device F2 key to use the "Change PIN" function. | A message similar to "Enter old PIN" is displayed on the LCD. | |
| 2 | Enter the valid PIN. | A message similar to "Enter new PIN" is displayed. | |
| 3 | Enter a new (different and security policy compliant) PIN. | A message similar to "Confirm new PIN" is displayed.<br>If not verified, a message similar to "Invalid new PIN" is displayed. (Return to step 3). | |
| 4 | Re-enter new PIN (the PIN entered must be the same as the previous one). | A message similar to "PIN succesfuly changed" is displayed.<br>If not confirmed, a message similar to "Invalid new PIN" is displayed. (Return to step 3 or cancel). | |
| 5 | Remove token from device to logoff | The CCD and Windows lock the workstation. | |
| 6 | Insert token and perform normal authentication and logon. | The new PIN works as expected. | |
| 7 | Remove and insert token. Try to use the old PIN to perform authentication. | The old PIN no longer works. | |
| 8 | Perform normal authentication and logon. Press V&A device F2 key to use the "Change PIN" function. | A message similar to "Enter old PIN" is displayed on the LCD. | |
| 9 | Repeatedly enter wrong PIN. | A message similar to "Invalid PIN, try again" is displayed after the first trials. When the number of trials prescribed by the security policy is attained, actions prescribed by it are taken (the device locks itself, an alert is sounded, etc.). | |
| 10 | Make the V&A device operational again, insert token and perform normal authentication and logon. Perform step 8 and 9 but keep one short of the number of trial prescribed by the security policy. Then enter the valid PIN. | Invalid PIN counter is cleared. If verified, a message similar to "Enter new PIN" is displayed. | NA |
| 11 | Repeatedly enter non-compliant new PIN. | When the number of trial prescribed by the security policy is attained, actions prescribed by it are taken. | NA |
| 12 | Make the V&A device operational again, reboot both DAVE and the PC, insert token and try perform normal authentication and logon with the old PIN. | The old PIN no longer works. | |
| 13 | Perform normal authentication and logon with the new PIN. | The new PIN works as expected. | |

**Special Considerations**

1. Verify testing conditions
2. Check application log on server for all password related events.
3. Steps 10 and 11 should not be performed on the demonstration system.

**Notes**

## 4.7. SRT0007 TOKEN SUBSTITUTION

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | V&A device is initialized. | |
| 3 | 2 initialized tokens (A and B) are required. | |
| 4 | User is logged on with token A | |

**Testing Steps and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Remove token A from device | The CCD and Windows lock the workstation. | |
| 2 | Immediately insert token A in device | User's token A validation phrase[18] and PIN prompt appear on the LCD. | |
| 3 | Remove token A from device | The CCD and Windows lock the workstation. | |
| 4 | Immediately insert token B in device | User's token B validation phrase and PIN prompt appear on the LCD.[19] | |
| 5 | While you use device functionalities normally,<br>use an arbitrary function generator to grab data packets from the device and then replay them. Also it is recommended to use a logic analyzer or other logging tool to trace the signal and try to make correlations with several packets to see if packet structure may be identified and altered. Repeat the test on all device ports (Smartcard, serial, etc.)<br>Use computer generated random data and insert it in packet frame to find a random packet that passes signature verification and causes an error or even an unexpected security status. | The unit remains stable. It does not enter any maintenance or administrative mode.<br>If the proportion of fake packets exceeds the security policy prescribed threshold for noise:<br>• the CCD and Windows lock the workstation,<br>• the unit locks itself,<br>• the authentication server sound an alarm<br>• the event is logged<br>• other action prescribed by the security policy can be taken. | NA |

**Special Considerations**

1. Verify testing conditions
2. Execute steps 1 to 4
3. Verify conditions again
4. Perform step 5.

(*): Step 5 shall not be performed on demonstration devices.

[18] Optional. See 'Validation phrase' in Definitions section.
[19] Replaced by Windows Station locked comportment.

**Notes**

## 4.8. SRT0016 USER LOCKOUT

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | Initialized V&A device is required (connected to his endpoint and authentication server via network) | |
| 3 | Initialized token is required | |
| 4 | User is enrolled | |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Power on Trusted DAVE. | Upon power up, Trusted DAVE carries out its auto-diagnostic tests. A message is displayed to inform the user about self-tests' progress. | |
| | | An event is recorded on the server | |
| | | The device displays a prompt asking the user to insert his token in the reader. | |
| 2 | Insert secure token in token reader. | The user's validation phrase[20] appears and the user is asked for his PIN. | |
| 3 | Purposely enter invalid PIN. | A prompt is displayed inviting the user to try again. | |
| 4 | Repeat step 3 as many times as necessary to exceed the number of trials allowed by the security policy. | A prompt informs the user that he is locked out. | |
| | | Use the authentication server control console to unlock the user. | |
| 5 | Perform normal authentication and logon. | The user can log on normally. | |
| 6 | Re-insert secure token in token reader and enter valid PIN. | A prompt ask the user to put a specific finger on the fingerprint scanner. | |
| 7 | Put any other finger than the appropriate one on the fingerprint reader. | A prompt asks the user to try again. | |
| 8 | Repeat step 7 as many times as necessary to exceed the number of trials allowed by the security policy. | A prompt informs the user that he is locked out Use the authentication server control console to unlock the user. | |
| 9 | Perform normal authentication and logon. | The user can log on normally. | |
| 10 | If the security policy requires more than one finger, repeat step 8 but try many different combination of appropriate and inappropriate fingers. | A prompt informs the user that he is locked out. Use the authentication server control console to unlock the user. | |
| 11 | Perform normal authentication and logon. | The user can log on normally. | |

**Special Considerations**

None.

[20] Optional. See 'Validation phrase' in Definitions section.

**Notes**

## 4.9. SRT0014 DEVICE SUBSTITUTION

**Testing Conditions**

| # | Condition | ✓ |
|---|---|---|
| 1 | For general test setup, please refer to the User Guide's *Installation* section. | |
| 2 | This test uses 2 legitimate V&A devices, A and B. B will be removed from the authentication server database, to emulate a rogue device. | |
| 3 | A serial switch box (9 pin) is necessary for some steps. | NA |

**Testing Procedure and Expected Results**

| # | Procedure | Expected Result | ✓ |
|---|---|---|---|
| 1 | Perform normal authentication and logon with device A. | The user can log on normally. | |
| 2 | Disconnect device A serial cable. | The CCD and Windows lock the computer. An alert is sounded on the server, the event is logged and/or actions prescribed by the security policy are taken. | |
| 3 | Connect device B to the workstation. | The event (security alert) appears in the authentication server's Windows application log. | |
| 4 | Re-boot the workstation, leaving device B connected to the workstation. Try to perform normal authentication. | A message like "Trusted path creation refused" is displayed on the LCD.<br>Device B cannot show the correct validation phrase[21], alerts are triggered. | |
| 5 | Connect both Trusted DAVE units to the workstation using a serial switch box. Re-boot unit A and while you perform each step of the authentication and logon process, switch back and forth between device A and device B. The goal is to destabilize either unit A to put it in an abnormal state. | Depending on whether or not you stay within the policy determined communication timeout limit, the results can include:<br>1. communication timeout recorded in the application logs (server and CCD)<br>2. workstation locked<br>3. unit A either locked or working normally.<br>4. At no time should unit A become unstable, crash or reboot. | NA |
| 6 | While you use device functionalities normally, use an arbitrary function generator to grab data packets from the device and then replay them. Also it is recommended to use a logic analyzer or other logging tool to trace the signal and try to make correlations with several packets to see if packet structure may be identified and altered. Repeat this step on all device ports (Smartcard, serial, etc.) Use computer generated random data and insert it in packet frame to find a random packet that passes signature verification and causes an error or even an unexpected security status. | The unit remains stable. It does not enter any maintenance or administrative mode.<br>If the proportion of fake packets exceeds the security policy prescribed threshold for noise:<br>• the CCD and Windows lock the workstation,<br>• the unit locks itself,<br>• the authentication server sound an alarm<br>• the event is logged<br>• other actions prescribed by the security policy can be taken. | NA |
| 7 | Un-initialize a device (see 2.3.2. Trusted DAVE Configuration, in the User Guide). Connect it to | A message like "Device not initialized. No cryptographic key loaded" is displayed on the | |

[21] Optional. See 'Validation phrase' in Definitions section.

| | | | |
|---|---|---|---|
| | the host workstation and reboot the PC and the DAVE. | LCD. | |

**Special Considerations**

1. Verify testing conditions.
2. Step 5 and 6 shall not be performed on demonstration devices.

**Notes**

# 5. CONCLUSION

## 5.1. PROJECTS RESULTS

At the time of writing, we are still uncertain about the US CBIS Project. It is thus impossible to evaluate if the device we developed can interface easily with the CBIS system.

As for the only intended use of Trusted DAVE so far, a secure Windows logon, the project is a success. Our experiments show that booting the V&A device takes 5 seconds and establishing the Trusted path takes approximately 3 seconds. Furthermore, at around 6 seconds, the authentication process is short enough to be totally unproblematic to users. Our experimentations reveal that the time needed to process, send and verify a PIN is 1 seconds. To perform the same task with fingerprints, the demonstration system takes 2 seconds. If we add these two waiting periods together, the system is within the 3 seconds specification[22].

Also, removal of the authenticated logged-on user's smart card results in the associated workstation becoming locked 4 second later.

## 5.2. FUTURE OPPORTUNITIES

As mentioned in the Detailed Design document, if a military, fully tamper protected version is produced, each unit would cost approximately 719 US dollars in components alone. This cost is based on a production of 1000 units. We estimate that development would take between 12 and 18 months before obtaining the first units. This can represent costs between $US 1.5 and $US 2.5 millions. We think that developing such a device would be hard to justify if it was to be connected to a software secure endpoint on a regular computer, vulnerable to Trojan horses or electronic spying.

A precise evaluation as not yet been done about a commercial version, protecting low to medium valued assets. It might be a valuable product to develop. It would be less protected than the military version but also less expensive. "EAL4-5 would be adequate for most commercial applications, with low to medium valued assets."[23] A market analysis would have to be conducted prior to any further development of such a device.

[22] System Requirements Specification, Ver. 001, Rev. 004, page 25.
[23] Security Target, Version 004, Revision 001, page 23.

### 5.2.1. Liveness Detection

Liveness detection would have been a fascinating subject to conduct experimentation on. Unfortunately, budget and time were too narrow so we had to limit our efforts to a review of the body of knowledge about that subject and a careful analysis of the problem. As sated in the 'Definition of sub-component options' document[24], we suggest three research paths to improve the system's liveness detection capability: counter measures, embedded liveness detection and combined biometrics.

[24] Definition of sub-component options, Version 001, Revision 005, page 37.

## DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Labcal. Group
400 boul. Jean-Lesage, hall Ouest
Quebec, Que G1K 8W1

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

DRDC Ottawa V&A Device System (U)

4. AUTHORS (Last name, first name, middle initial)

Labcal.Group

5. DATE OF PUBLICATION (month and year of publication of document)

March 2003

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

37

6b. NO. OF REFS (total cited in document)

29

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contractor Report (final)

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

DRDC Ottawa, Information Operations Section, 3701 Carling Avenue Ottawa
K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

15bf30

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

W7714-010573/001/SV

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

DRDC Ottawa CR 2003-039

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

( x ) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Unlimited distribution of the announcement

13. ABSTRACT ( a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

Trusted DAVE project's main purpose was the development of a trusted device for authentication and verification. Analysis involved in this R&D project determined the following choices of technologies: contact smart card, capacitive fingerprint sensor, Intel StrongARM SA-1110 CPU, Intel Flash memory, Neutrino™ real-time operating system from QNX, use of the Five-Pass Authentication Protocol, etc. And, more specifically for tamper protection: multi-layer flexible printed circuit, metal case, special stacking of the printed circuit, use of double access memory, Shamir power supply, etc.

A prototype and a demonstration system were developed. Although different to some extent from the designed device, this proof of concept helped evaluate performance and feasibility. It will also be useful in demonstrating the concept to other parties involved.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Biometrics, authentication