Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

A strong three-factor authentication device: Trusted DAVE and the new Generic Content-Based Information Security (CBIS) architecture

J. Savoie

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2004-198
November 2004

Canada

A strong three-factor authentication device: Trusted DAVE and the new Generic Content-Based Information Security (CBIS) architecture

J. Savoie

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2004-198

November 2004

Abstract

This report has three objectives. The first objective is to provide a description/analysis of the Trusted DAVE activity performed by DRDC Ottawa and its contractors. The second is to describe different systems where the demonstrator produced under this activity could be used. The last is to analyse, study, and compare different types of network/system architectures.

The activity involved the development of three elements: A secure design for a three-factor Trusted Device for Authentication and VErification (Trusted DAVE), a device demonstrator implementing some of those design elements, and an authentication and verification demonstration system that utilises the device demonstrator. The purpose of the device is to provide the user interface component to be used as a part of a strong Verification and Authentication (V&A) capability for systems used to process classified or sensitive data.

Four possible systems that could use Trusted DAVE are presented. Two of them are related to the CBIS (Content-Based Information Security) concepts and one integrates CBIS and Kerberos. Finally, three architectures for network systems are presented with their advantages and their limitations. A Generic CBIS architecture covering the one specified in the US CBIS ACTD is defined and compared with the two others. The purpose of the Generic CBIS architecture is threefold: (1) provide an architecture for systems generalizing the US ACTD one, (2) illustrate the architecture's fundamental aspects, and (3) introduce an architecture where Trusted DAVE could be useful.

Résumé

Ce rapport a trois objectifs. Le premier est de donner une description/analyse de l'activité Trusted DAVE fait par RDDC Ottawa et ses contractants. Le second est de décrire différents systèmes ayant comme composante possible le démonstrateur développé sous cette activité. Le dernier est d'analyser, de définir et de comparer diverses architectures de système-réseau.

L'activité Trusted DAVE est composée du développement de trois éléments: Un design sûr pour un appareil de haute sécurité (Trusted DAVE) servant à l'acquisition de trois facteurs d'authentification et de vérification; un appareil de démonstration basé sur ce design; et un système de démonstration d'authentification et de vérification utilisant l'appareil de démonstration. Le but de l'appareil de haute sécurité est d'être l'interface utilisateur de systèmes d'authentification et de vérification pour des systèmes utilisés pour traiter des données classifiées ou sensibles.

Quatre exemples de systèmes où Trusted DAVE pourrait être utilisé comme composante sont présentés. Deux d'entre eux sont reliés aux concepts CBIS (Content-Based Information Security) dont l'un intègre Kerberos et CBIS. Finalement, nous présentons trois architectures de système réseau avec leurs avantages et limitates. Une architecture CBIS couvrant celle du projet américain "CBIS ACTD" est définie et comparée aux deux autres. Le but de cette architecture CBIS est triple: (1) définir une architecture plus générale que celle du "CBIS ACTD"; (2) mettre en relief les aspects fondamentaux de l'architecture; et (3) présenter une architecture où Trusted DAVE pourrait être utile.

This page intentionally left blank

Executive summary

Solutions providing secure, effective, and reliable interoperability among partners in multinational coalitions that involve Canada are needed by the Canadian Forces. CF requirements are evolving at the national level to allow multi-level secure (multiple information domains) interoperability among our various tactical and strategic command and control systems.

In the year 2000, DRDC Ottawa personnel became aware of a US Advanced Concept and Technology Demonstrator (ACTD) project entitled Content Based Information Security (CBIS). Discussions with CBIS project management staff revealed that the ACTD directly addresses many of the secure interoperability issues of interest to the CF and is focused on the use of commercial technology to achieve these aims. Because of this similarity of goals and objectives, DRDC decided to start the development of new technologies supporting solutions and systems based on CBIS concepts. Trusted DAVE was the first activity in this direction.

The Trusted DAVE activity involved the development of three elements: A secure design for three-factor Trusted Device for Authentication and VErification (Trusted DAVE), a device implementing some of those design elements, and an authentication and verification demonstration system that utilises the device. The purpose of the device is to provide the user interface component to be used as part of a strong Verification and Authentication (V&A) capability for systems used to process classified or sensitive data.

This report has three objectives. The first objective is to provide the description, analysis, and results of the Trusted DAVE activity performed by DRDC Ottawa and its contractors. The second objective is to describe different systems in which the demonstrator produced under the activity could be used. The last objective is to study/define/compare different types of architectures for network systems with respect to security, functionality, and cost.

To achieve the first objective, we state the objectives of the activity, show the approach taken by DRDC Ottawa to achieve them, and provide an overview of the contractor effort in the activity. Then, we describe the technology selected to support the chosen device design and provide a description of the demonstration system that comprises a Trusted DAVE demonstration device, which implements partly that device design.

Four examples of systems where Trusted DAVE could be used as a component are presented to fulfill the second objective. The last two examples are related to CBIS, where the last one presents a new system concept integrating Kerberos and CBIS. The Kerberos and CBIS example has been introduced to solve some possible CBIS ACTD's security issues.

Finally, three architectures for network systems are presented along with their advantages and limitations. A Generic CBIS architecture covering the one specified in the CBIS ACTD is defined and compared with the two others. The purpose of the Generic CBIS architecture is threefold: (1) to provide an architecture for systems generalizing the US ACTD one, (2) to illustrate the architecture's fundamental aspects, and (3) to introduce an architecture where Trusted DAVE could be useful.

Savoie, J. 2004. Trusted DAVE project and CBIS. DRDC Ottawa TM 2004-198. Defence R&D Canada - Ottawa.

Sommaire

Des solutions permettant une interopérabilité sûre, efficace, et fiable entre les associés multinationaux de coalitions auxquelles le Canada participe sont nécessaires pour les Forces canadiennes. De plus, les demandes des Forces canadiennes en ce qui concerne la sécurité nationale évoluent vers la conception de divers systèmes tactiques et stratégiques de commandement et contrôle permettant l'interopérabilité avec niveaux de sécurité multiples (domaines d'information multiples).

En l'an 2000, le personnel du RDDC Ottawa a pu se familiariser avec le projet de prototype de technologie américain nommé « Content Based Information Security » (CBIS), où la sécurité est fondée sur le contenu de l'information et non sur le niveau de sécurité des réseaux. Les discussions avec le personnel de gestion du projet CBIS ont indiqué que le prototype aborde directement plusieurs questions d'interopérabilité pertinentes aux Forces canadiennes en plus de prôner l'utilisation de la technologie commerciale pour réaliser ses objectifs. En raison de cette similitude des buts et des objectifs, RDDC a décidé de s'engager dans le développement de nouvelles technologies soutenant des solutions et des systèmes basés sur des concepts de CBIS. Trusted DAVE a été la première activité dans cette direction.

L'activité Trusted DAVE a porté sur le développement de trois éléments: Un design sûr pour un appareil de haute sécurité servant à l'acquisition de trois facteurs d'authentification et de vérification; un appareil de démonstration basé sur ce design; et un système de démonstration d'authentification et de vérification utilisant l'appareil de démonstration. Le but de l'appareil est d'être l'interface utilisateur de systèmes d'authentification et de vérification de haute sécurité pour des systèmes utilisés pour traiter des données classifiées ou sensibles.

Ce rapport a trois objectifs. Le premier est de donner une description, une analyse et les résultats de l'activité Trusted DAVE. Le second est de décrire des systèmes où le système Trusted DAVE pourrait être utilisé. Le dernier est d'étudier/définir/comparer différents types d'architecture de système réseau en rapport avec la sécurité, les fonctionnalités, et les coûts.

Pour atteindre le premier objectif, nous énonçons d'abord les objectifs de l'activité Trusted DAVE, montrons l'approche adoptée par RDDC Ottawa pour les réaliser et fournissons une vue d'ensemble de l'effort fait par le contractant à l'activité. Ensuite, nous décrivons une technologie permettant la conception d'un appareil répondant au design établi et un système d'authentification et de vérification de démonstration. Le deuxième objectif est atteint par la présentation de quatre exemples de systèmes où Trusted DAVE peut être employé. Les deux derniers sont liés à CBIS, et le dernier présente un nouveau concept de système intégrant Kerberos et CBIS. Ce dernier exemple a été ajouté pour résoudre certains problèmes notés dans le CBIS ACTD. Finalement, nous présentons trois architectures de système réseau avec leurs avantages et limites. Une architecture CBIS couvrant celle du projet américain de prototype CBIS est définie et comparée avec les deux autres. Le but de cette architecture CBIS est triple: (1) définir une architecture qui est plus générale que celle du prototype CBIS; (2) mettre en relief les aspects fondamentaux de l'architecture; et (3) présenter une architecture où Trusted DAVE peut être utile.

Savoie, J. 2004. Trusted DAVE and CBIS. DRDC Ottawa TM 2004-198. R & D pour la défense Canada - Ottawa.

Table of contents

List of figures

This page intentionally left blank

1. Introduction

Solutions providing secure, effective, and reliable interoperability among partners in multinational coalitions that involve Canada are needed by the Canadian Forces (CF). Furthermore, CF requirements are evolving at the national level to allow multi-level secure (multiple information domains) interoperability among our various tactical and strategic command and control systems. Defence Research and Development Canada (DRDC) is focused on developing new technology supporting solutions that address these needs.

In the year 2000, DRDC Ottawa personnel became aware of a US Advanced Concept and Technology Demonstrator (ACTD) project entitled Content-Based Information Security (CBIS) [1, 2]. Discussions with CBIS project management staff at Space & Naval Warfare Systems Command (SPAWAR) Systems Center in San Diego revealed that the ACTD directly addresses many of the secure interoperability issues of interest to the CF and is focused on the use of commercial technology to achieve these aims. Because of this similarity of goals and objectives, DRDC decided to start the development of new technologies supporting solutions and systems based on CBIS concepts.

Trusted DAVE was the first activity in that direction. It involved the development of a secure design for a three-factor Trusted Device for Authentication and VErification (Trusted DAVE), a demonstration device implementing some of those design elements, and an authentication and verification demonstration system that utilises the device.

The purpose of the device is to provide the user interface component to be used as part of a strong 3-factor Verification and Authentication (V&A) capability for systems used to process classified or sensitive data. This device is referred to as Trusted DAVE, the V&A device, or the device. The device's primary role is to interact securely with the user to collect three factors of authentication: a biometric measurement, a secure token, and a PIN. These factors are then sent to a secure endpoint of an overall system. Trusted DAVE is deemed trusted because it is physically protected and it shares a secret with the overall system. The secret can be used both to mutually authenticate the device and the overall system and to create trusted paths between them.

Generally, in most overall systems where Trusted Dave is intended to be used, the secure endpoint would not directly authenticate the user using the three factors. In the demonstration system set up under this activity, the secure endpoint sends the factors to an authentication and authorization server, which is the component of the overall system that compares the factors with those in a database. When the comparisons match, the user is deemed authenticated and the server sends authorization data to the secure endpoint through a trusted path. Trusted paths are created between Trusted DAVE, the secure endpoint, and the server using a shared secret.

The report's three objectives and their corresponding sections are described below.

The first objective is to provide the description, analysis, and results of the Trusted DAVE activity performed by DRDC Ottawa and its contractors. In Section 2, we state the objectives of the Trusted DAVE activity, show the approach taken by DRDC Ottawa to achieve them, and provide an overview of the contractor effort in the activity. In Section 3, we describe the technology selected to support the chosen device design and provide a description of the demonstration system that comprises a Trusted DAVE demonstration device, which implements partly that device design.

The second objective is to describe different systems in which the demonstrator produced under the activity could be used. In Section 4, we provide four examples of systems where Trusted DAVE is used as a component. The last two examples are related to CBIS, where the last one presents a new system concept integrating Kerberos and CBIS. The last example has been chosen to solve some possible CBIS ACTD's issues that we identified.

The last objective is to analyse, define, and compare different types of architectures for network systems with respect to security, functionality, and cost. In section 5, we introduce the concepts of information domains, security policies, and security models, and then show some relationships between them. Note that the information domain concept generalizes the concept of classified domains used in the military. Following these preliminaries, three architectures for network systems are presented with their advantages and limitations. The Generic CBIS architecture covering the one specified in the CBIS ACTD is defined and compared with the two others. The purpose of the Generic CBIS architecture is threefold: (1) to provide an architecture for systems generalizing the US ACTD one, (2) to illuminate the architecture's fundamental aspects, and (3) to introduce an architecture where Trusted DAVE could be useful.

2. Trusted DAVE activity

The Trusted DAVE activity was a collaborative effort of DRDC Ottawa and its contractor Labcal Group, a Quebec city company. This activity started in summer 2001 and finished in March 2003. In this section we describe the objectives of the Trusted DAVE activity and the DRDC approach to achieve them, and provide an overview of the contractor effort in the activity.

2.1 Activity objectives

The DRDC Ottawa Trusted DAVE activity had the following objectives:

1. Design a device that

    a. can be a part of different overall (computer) systems with strong V&A capability. Intended systems are those processing classified or sensitive information as the one defined in the CBIS ACTD.

    b. is a telephone-sized single physical device with processing power that comprises a fingerprint reader, a token or smart card reader, a keypad or keyboard, and a screen.

    c. is capable of interacting with a user to collect his/her three authentication factors: fingerprints, PIN, and token or smart card.

    d. is responsible for sending the authentication data to a secure endpoint of the overall system considered. The authentication is made on a component of the overall system that is usually different from the secure endpoint.

    e. is responsible for protecting the user's authentication data against disclosure.

    f. is able to communicate securely with the secure endpoint

    g. provides tamper resistance through integrated tamper-proof technology

    h. provides a good basis to achieve a highly secure product that would be certifiable against the Common Criteria (CC) and/or Federal Information Processing Standards Publications **(**FIPS) 140-1 criteria

2. Build a device satisfying as much as possible the activity's objectives within the limited resources of the contract.

3. Build a demonstration system that provides an example of a simple overall system where the device is used.

2.2 DRDC approach to achieve objectives

The initial design concepts for the V&A device were derived from the US project researching CBIS. DRDC Ottawa decided to explore the development of a flexible three-factor V&A device

that could also have applications to other secure systems. The V&A device's first role is to interact with the user to collect three factors for authentication: a biometric measurement, a secure token and a PIN.

DRDC's approach to get the device's design was first to provide documentation to the contractor. This documentation was composed of a set of CBIS ACTD documents, a Statement Of Work, and a set of documents [3-12] some of which were Protection Profiles (PPs). The contractor, in consultation with DRDC's Scientific Authority, had to determine the final design of Trusted DAVE from an analysis of the documentation, a scaled-down Threat and Risk Assessment, an informal Security Target (ST) document, and an analysis of the cost factors and technology available. Moreover, the contractor had to keep in mind that the design should be strong enough to provide a good basis for the development of a product that would provide a high assurance level against the CC or FIPS-140 criteria.

Finally, the contractor had to build two demonstration devices satisfying a representative subset of the design requirements and a simple overall system where the device is used.

2.3 Overview of the contractor's efforts

First, a review of the background information on the CBIS ACTD, the DRDC activity documentation, and other documents [3-12] was performed. It allowed production of a scaled-down Threat and Risk Assessment [13] involving a comparison between the CBIS Identification and Authentication components with Trusted DAVE. Arguments showing why the Trusted DAVE authentication subsystem is more secure than the CBIS authentication subsystem were provided. However, this conclusion was mainly based on the fact that some pieces of the CBIS authentication subsystem were not well physically protected, which was a correct assumption in the initial CBIS ACTD documentation but clearly not a correct one in later documentation.

Second, a review of System Requirement Specifications [14] was conducted to establish a list of requirements that a production level device should meet.

Third, the contractor had 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 [15]. 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, [16] was used to that purpose.

Fourth, the contractor then presented a Preliminary Design presentation to DRDC. An informal Security Target document [17] and the Detailed Design document [18] were also presented. The Security Target document, although informal, is helpful as a global security and assurance level evaluation. However, a more thorough document would be needed for the purpose of a CC product evaluation. The Detailed Design document is a low-level explanation of the V&A device 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.

Fifth, concurrently a demonstration system and a demonstration device were developed. A Test Plan [19] and a User Guide [20] were produced. The Test Plan is applicable to a production-level

device as well as to the demonstration-level device developed. However, the User Guide describes only the demonstration system.

Sixth and finally, a Final Report document [21] was produced.

3. Activity's output

In the first part of this section we present the technology choice made by the contractor to implement the design of a trusted device that should achieve a high assurance level with respect to the CC and/or FIPS-140 evaluation criteria and provide the shown or expected functionalities of the Trusted Dave device demonstrator. In the second and third parts, a physical description and a functional description of the demonstration system respectively, are provided.

3.1 Technology choices for the device design

The technologies listed below were selected or suggested for implementing the device as designed. However, items 7, 8, 9, 10, 12, 13, 14, and 15 were not implemented in the Trusted DAVE demonstration device. Moreover, item 1 was modified because contactless smartcards were used. For information on the detailed design, see [18].

1. Contact smart card technology was selected for its flexibility and built-in cryptographic features

2. Capacitive sensor technology was selected for its availability, low cost, solidity, small size, and design flexibility.

3. The Neutrino real-time operating system from QNX and the Momentics development environment were selected mainly for good OS-development, tools integration, driver availability, technical support, reliability, serviceability, and real-time performance.

4. The Intel StrongARM SA-1110 main CPU was selected because it is well supported, offers sufficient computing power, and promises an interesting future.

5. Intel Flash memory was selected because it has widespread deployment and not very expensive.

6. An authentication protocol based on the Five-Pass Authentication Protocol described in section 6.2 of ISO/IEC 9798-2:1999 was selected.

7. Multi-layer flexible printed circuit was selected to provide an intrusion detection envelope. Arrangement: TGVTTVGT (T= trace layer, V=Vcc and G=GND)

8. A metal case acting as a Faraday cage against electromagnetic emissions was selected. It is low cost and fast to produce.

9. Stacking of the printed circuit in a pattern that reduces electromagnetic wave emission was strongly suggested.

10. Double access memory to allow simultaneous read and write access was selected. This decreases emitted noise.

11. A Shamir power-supply to uncouple the components containing secrets from the external power-supply was selected.

12. A removal detector for: keyboard, smart card, LCD, fingerprint sensor, and casing was selected.

13. A wall plug powered Electronic Tamper Detection mechanism was selected.

14. A microprocessor supervisory circuit was selected to allow powering of the low power section, generation of the board RESET when sector power is out, etc.

15. The use of bus switch was selected. This component is used to isolate the electric signals from the USB port, fingerprint sensor and LCD display, which are connected to the CPLD.

16. The use of a switch debouncer was selected to simplify the keypad control software.

17. The Altera's MAX 3000A Family CMOS EEPROM Base CPLD was selected to control peripherals and memory.

18. A permanent RAM memory was selected to conserve secrets in case of power outage.

3.2 Physical description of the demonstration system

Figure 1 illustrates what constitutes the Trusted DAVE demonstration system. It is composed of four main components: Trusted DAVE (a V&A device), a workstation connected to Trusted Dave, an authentication server connected to the workstation, and a Smart Print Enroller connected to the server. Figures 2 and 3 show a V&A device while Figure 4 shows a SmartPrint Enroller.

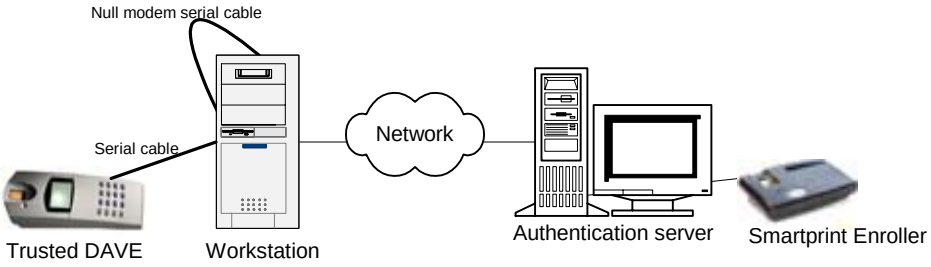

Figure 1-Demonstration System

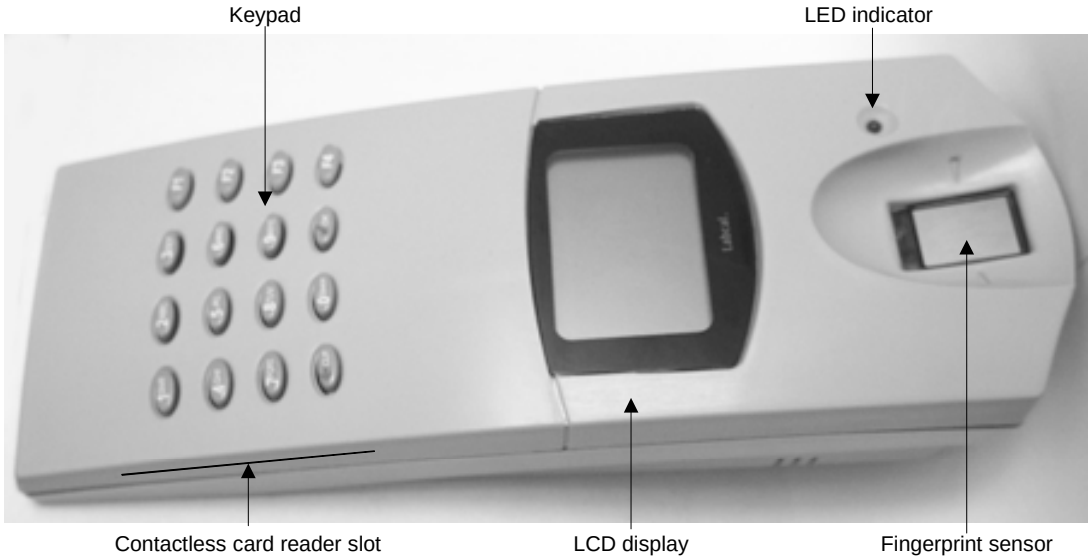

Figure 2-V&A device (Trusted DAVE)

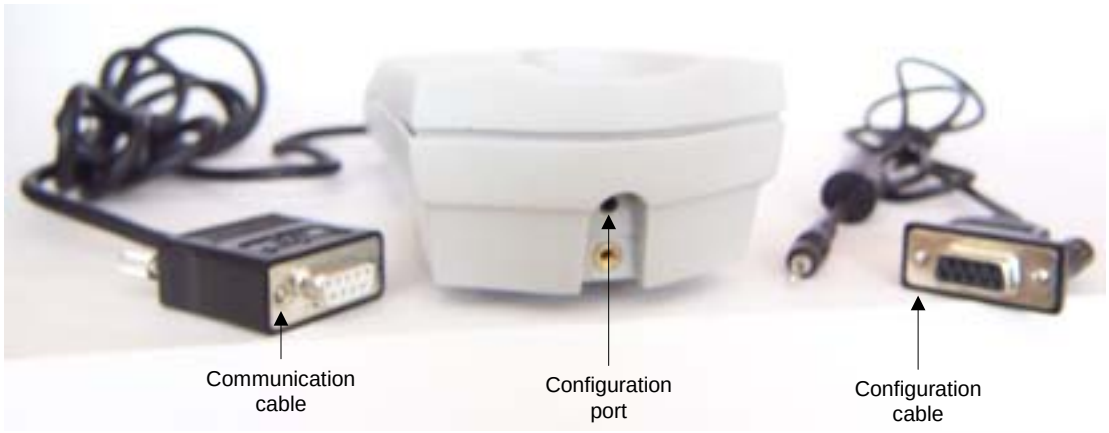

Figure 3 - V&A Device Communication and Configuration

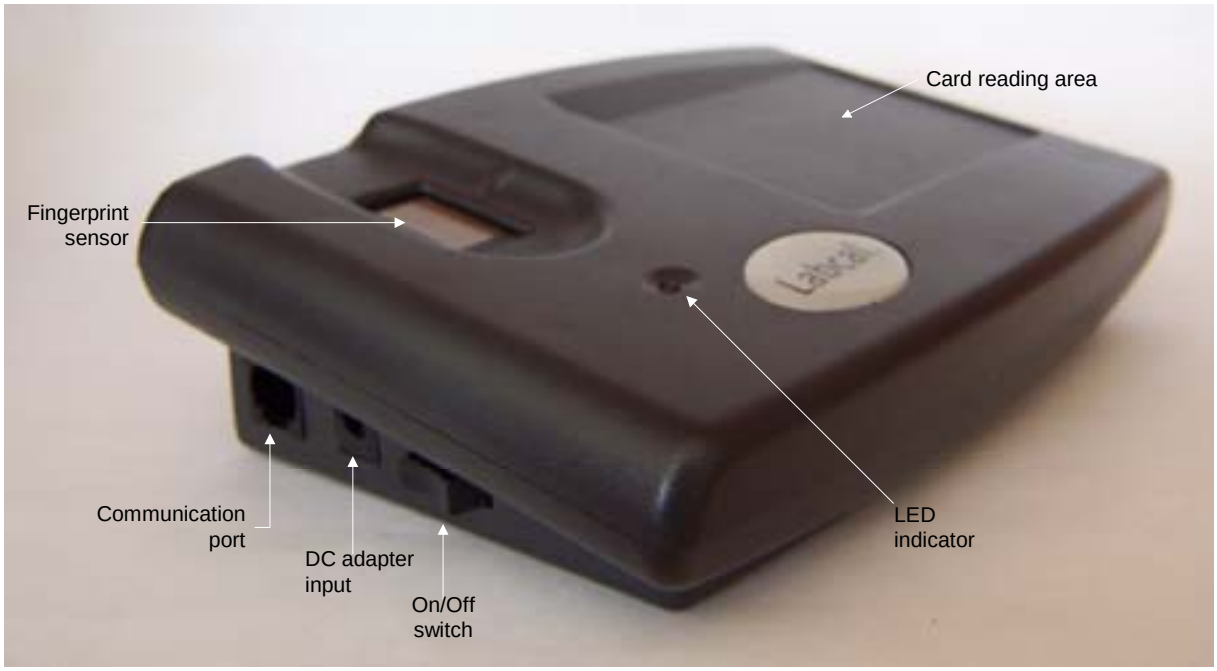

Figure 4-SmartPrint™ Enroller

3.3 Functional description of the demonstration system

The demonstration system is made of six main functional components (see Fig. 5): Trusted DAVE, the V&A device simulator software, the software secure endpoint, the server software, the SmartPrint software, and the SmartPrint Enroller. In the following subsections, we provide a functional description of these components while the system (1) initialises, (2) authenticates or logs on users, and (3) enrols users.

3.3.1 System initialisation

While the four physical components (see Fig. 1) boot up, the six functional components start and establish communication channels and trusted paths between each other.

When Trusted DAVE starts, it performs a self-test and then establishes a communication channel with the V&A device simulator software. The simulator was introduced in the design of the demonstration system because of cost constraints. The simulator was originally intended as Trusted DAVE's software component. Hence, Trusted DAVE and the simulator should be seen as a single physical component outside the workstation that is connected to the workstation (secure endpoint). For mimicking a physical connection between Trusted DAVE with the workstation, the simulator is connected to the secure endpoint through a null modem cable.

The simulator establishes a trusted path with the software secure endpoint and the authentication server. The trusted paths protect all communication between system elements, if we assume that Trusted DAVE and the simulator form a single component. The simulator software, the software

secure endpoint, and the authentication server exchange or relay information in the same way the intended system would have. The V&A device simulator software relays information from Trusted DAVE to the rest of the system and vice-versa. The trusted path is created from two shared secrets: one between the simulator and the server and one between the secure endpoint and the server.

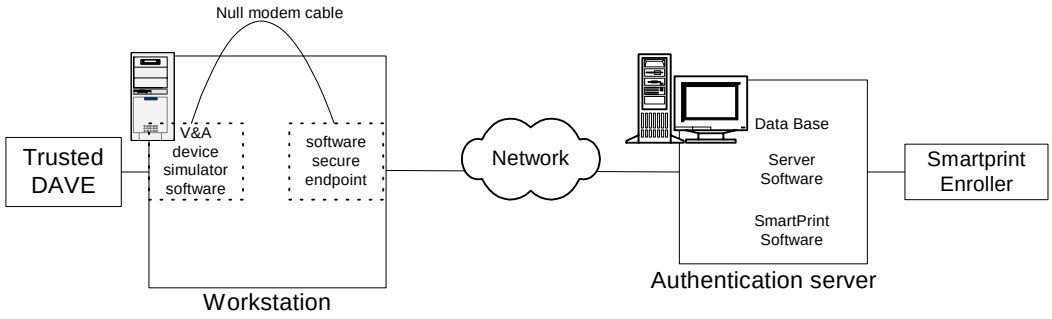

Figure 5-Functional Overview

3.3.2 User authentication and logon

After the demonstration system initialises, users can authenticate to the system to log on to the Windows 2000 workstation.

In order to log on first, a user inserts a valid smart card into Trusted DAVE. Trusted DAVE then reads the card's serial number and sends it to the server, which looks it up in the database and sends back the user's validation phrase— The validation phrase has been introduced in the design as a security measure mitigating the risk that a user provides his/her credentials to a rogue Trusted DAVE. These credentials could then be used later in a replay attack.— Trusted DAVE then gathers the user's PIN and biometric measurement. Trusted DAVE forwards these to the server, which uses Enroller to perform comparison between the template received and the user's template stored in the database. If it is positive, the software secure endpoint logs the user onto Windows® 2000, according to information entered in the database during enrolment. If it is negative, the host workstation remains locked. Note that the template comparison was originally intended to be done on the server and not the enroller. It was implemented this way to decrease implementation and development costs. Nevertheless, the server and enroller should conceptually be seen as the server's software component.

When the smart card is removed from Trusted DAVE, it warns the V&A device simulator software, which warns the software secure endpoint, which in turn locks the host workstation. The 'Trusted Dave status viewer' is a system tray application installed on the host workstation. It shows the user security level at any given point in time.

The software secure endpoint and the V&A device simulator software are constantly checking for Trusted DAVE's presence, so as soon as either its communication cable or its power cord is unplugged, the host workstation is securely locked.

Each meaningful system-related event is audited through a Windows application log. The audit database is stored on the server. A monitoring console on the server allows easy event viewing.

3.3.3 Enrolment

The Enroller has two functions in the demonstration system: It makes template comparisons, as stated previously, and gets the initial fingerprint templates from users that are enrolled.

Enrolment into the demonstration system is a bit simpler than in a production version because it makes direct use of the authentication server and the Enroller linked to it. So any person logged onto the authentication server and launching the Enrolment application is assumed to be an enrolment officer/administrator and can enrol users— no supplementary authentication is necessary.

4. Possible systems using Trusted Dave

In this section, we describe four systems in which Trusted DAVE may be used as a component. The first two are simple systems. The third system is based on a simplified view of the CBIS ACTD. It is shown that such a system can be used as a Multi-Single-Level-Security (MSLS) system or a Multi-Level-Security (MLS) system. Finally, the last system is a modification of the third one in which Kerberos authentication is integrated.

4.1 Basic System

The first system considered is the Basic System (see Fig. 6) made up of two components: a desktop component and an Authentication and Authorization (AA) component.

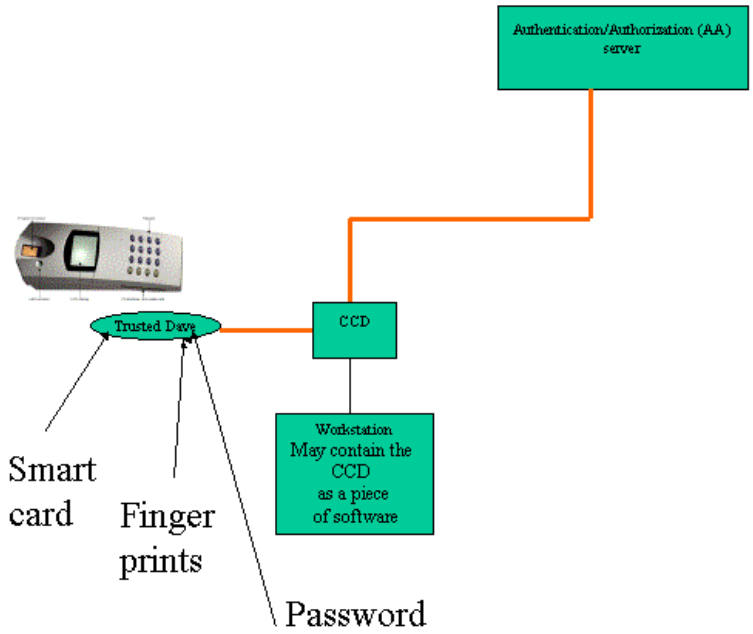

Figure 6- Basic System

The desktop component is the user interface to the system. It is composed of three subcomponents: Trusted DAVE, a Compatible Connected Device (CCD), and a workstation. The CCD subcomponent can be either a piece of software running on the workstation or a distinct physical subcomponent. The CCD can be seen as a secure endpoint of the overall system. If the CCD is a piece of software, the system is very similar to the intended demonstration system described previously; otherwise, the CCD has some similarity with the CBIS Security Card (CSC) component of the CBIS ACTD and the desktop is similar to the CBIS ACTD desktop [1]. In all cases the CCD is the single network access point of the desktop.

Trusted Dave and the CCD have embedded secrets known only by the AA server. These secrets are used to create a Trusted path between Trusted DAVE, the CCD, and the AA server. The trusted path between these components is shown in orange.

To access the workstation, a user provides Trusted DAVE with three credentials: a token (smart card), a fingerprint, and a PIN. The credentials are sent and compared on the AA server—not on Trusted DAVE. After a successful authentication, the CCD logs the user on to the workstation and gets the authorization data from the AA server. The nature of this data remains unspecified here. For instance, this data could be credentials to access remote servers and/or be encryption/decryption keys. It is assumed that the CCD stores securely the authorization data. Hence, neither applications on the workstation nor Trusted DAVE can access the authorization data. No further functionalities are specified for the CCD of the Basic system. However, the CCD could also play a role similar to the CSC in the CBIS ACTD, get encryption keys and secrets from the AA server, encrypt and decrypt data, and/or interact with a hard drive.

4.2 Physical Access Control System

The Physical Access Control System (see Fig. 7) is a system used to control access to a closed room. Users are authenticated as in the Basic System. This system unlocks the door after a user is authenticated. The door and the closed room components replace respectively the CCD and the workstation of the Basic System.

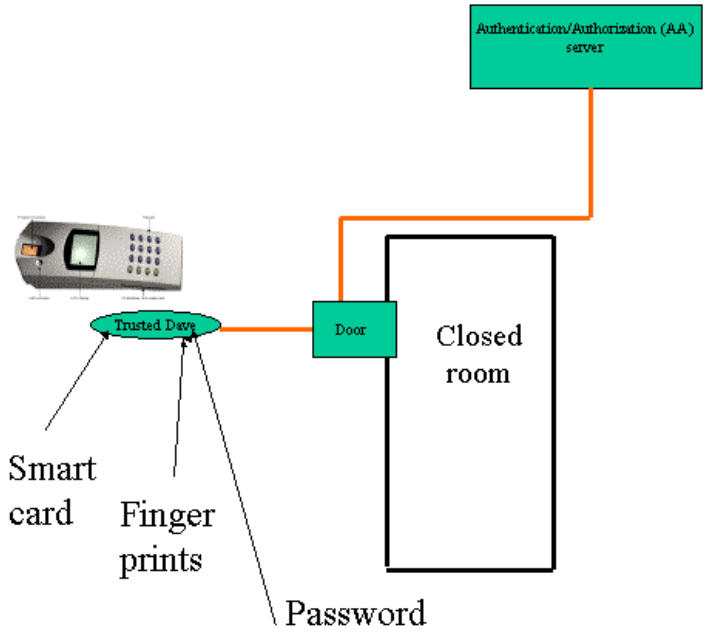

Figure 7- Physical Access Control System

4.3 CBIS-Like System

The CBIS-Like system (see Fig. 8) is a simplified version of the CBIS ACTD LAN system where the CCD replaces the CSC. It is also the Basic System in which the desktop is replicated and an encrypted file server is added. Note that only one desktop is shown in Figure 8.

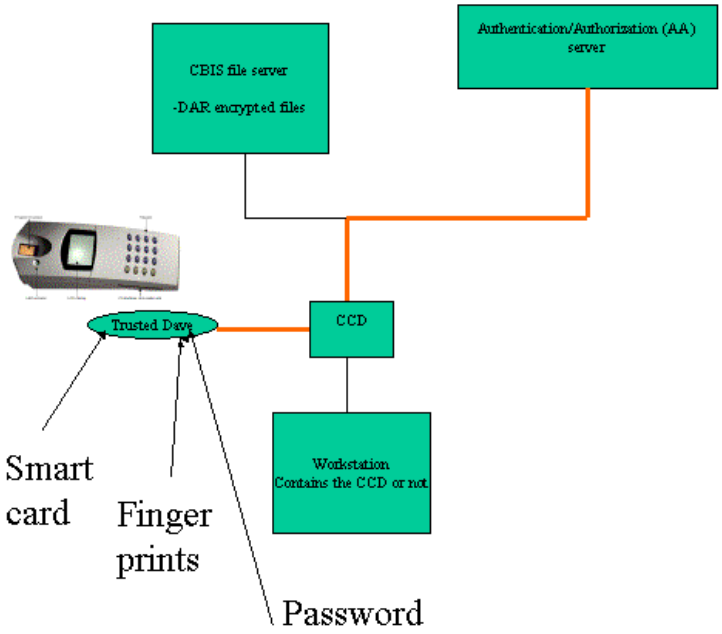

Figure 8-CBIS-Like System

For a given desktop, users access the workstation and the CCD gets the authorization data as in the Basic System. The authorization data contains one or more group-keys, which are keys associated with some groups the user belongs to. Note that there is a one-to-one mapping between group-keys and user groups in the system. The number of group-keys received by the CCD is implementation dependent.

The server is a repository of encrypted files. More precisely, a file is encrypted by a symmetric key that is unique to the file. This key is also encrypted by one or more group-keys. Encrypted symmetric keys and the file are bundled together to form an encrypted file. An encrypted file is said to belong to a group if the encrypted file includes the file's symmetric key encrypted by the group's group-key. Hence, an encrypted file may belong to many groups, which can be hierarchical. Note that a user group along with information in files belonging to the group and a security policy related to the group constitute an information domain as defined in Section 5.1.

The CCD main functions are to store group and symmetric keys securely, perform decryption/encryption of symmetric keys and files, and interact with the network. Hence, group and symmetric keys are protected from the workstation's applications, which can be Trojan horses impersonating a user.

MSLS and MLS systems can be built from the CBIS-Like system if both functionalities are added to CCDs, and workstations are modified. Let us see how this can be done through two examples described in Sections 4.3.1 and 4.3.2 respectively. The first example is an MSLS system while the second is an MLS system based on workstations not running an MLS OS.

In both examples, we consider a CBIS –Like system where user groups form a hierarchy in which each group corresponds to a couple (classification, category). Secret and top secret are examples of classifications while CANUS and NATO are examples of categories. Categories are sometimes called warning terms in the literature. In such a system information of different classifications and categories coexist. The system is an MSLS system if it enforces the MSLS policy stating that no information flows are allowed between the groups. It is an MLS system if it enforces a policy that disallows unprivileged information flows between any two groups if the sending group is not lower in the hierarchy than the receiving group. Such policies are called MLS policies. Note that MLS policies may allow privileged information flows from a high to a low classification or between any two groups. Usually, privileged information flows are processed only by privileged users such as degraders or releasers.

Since the notion of information flows has not been defined yet, the MSLS and MLS policies are relative to the definition of information flows. The following definition is used and doesn't include the notion of covert channels.

> *Information flow. An information flow is said to occur from a group1 to a group2 while a group1's encrypted file not in goup2's encrypted files becomes accessible in clear to group2's users not in group1's users*.

4.3.1 Example of an MSLS system

A possible implementation of MSLS system is presented here. It is assumed that the CCDs, AA server, and Trusted DAVEs are the trusted components enforcing the MSLS policy defined above.

In this system, while a user logs on, it selects a switch on the CCD or Trusted Dave indicating a group the user belongs to. After authentication, the CCD gets the group's group-key from the AA server and the user is logged on to the workstation. It is assumed here that the workstation's OS is a standard OS such as Windows 2000.

When a user wants to read an encrypted file on the file server, the file is sent to the workstation through the CCD. The CCD decrypts the file first, if the file belongs to the group's files, and sends it in clear to the workstation. The user then works on the file. The user may send the resulting file or other files to the file server. The CCD intercepts those requests and sends encrypted files to the file server. The group-key encrypts all symmetric keys used in the process.

Even though such a system may prevent workstation's Trojan Horses to write information belonging to a group different of the selected user group, it is possible that a Trojan or the user (unintentionally) writes on workstation's local files. This information would then be accessible to the next user, which can be member of a different group. So, a desktop must not allow residual information between user sessions. This can be done if there is no static storage device directly controlled by the workstation's OS. Otherwise, if static storage is provided, it needs to be controlled by the CCD.

4.3.2 Example of an MLS system

A possible implementation of an MLS system not based on an MLS OS for workstations is presented here. It is assumed that the CCDs, AA server, and Trusted DAVEs are the trusted components enforcing the MLS policy defined above.

While a user logs on to the system, he selects one or more switches on the CCD or Trusted Dave indicating one or more groups the user belongs to. After authentication, the CCD gets the selected groups' group-keys from the AA server, assuming that the user is member of those groups. The CCD may also get some user privileges such as declassify or release privileges. The user is then logged on to the workstation.

It is assumed that the workstation contains information of a single group at any given time. So, no static information is stored on the workstation if the information is not encrypted and controlled by the CCD. In this system many operations such as declassification and releasing may be implemented. Let us consider the following declassification operation: A user members of two groups, group1 and group2, having the declassify privilege from group1 to group2, wants to declassify a group1's file to a group2's file. The user sends a message to the CCD that he wants to work as a group1's member. The CCD then reboots the workstation or erases important parts of workstation's memory. The group1's file is then loaded in the workstation as in the MSLS example. The file is sent back to the CCD for declassification. Since the CCD cannot trust the workstation's OS, the user to ask the CCD to perform the file declassification either selects a switch on the CCD –if the CCD is hardware— or sends a message to the CCD through a trusted path. The CCD then checks the user privilege and then encrypts the file appropriately. The encrypted file is sent to the file server.

This example can be extended. An MLS system involving desktops and other sub-systems is described in Section 5.4.

4.4 Kerberos CBIS-Like System

There are two issues with the CBIS-Like system introduced above. First, there are no authentication mechanisms between CCDs and the file or other servers. Second, group-keys are stored in the system's CCDs, which can be risky because the system provides many access points (CCDs) to keys that can decrypt files. The Kerberos CBIS-Like system (see Fig. 9) addresses both issues. It provides an authentication mechanism based on the Kerberos protocol and adds an Encryption Key (EK) server to mitigate the risk associated with the fact that group-keys can be located in many places. This system has also another advantage over the CBIS-Like system because revoking a user without affecting other users becomes easier to implement.

In the Kerberos CBIS-Like system, a user authenticates to the AA server as in the Basic system. The authorization data sent to the CCD is now containing the user's Kerberos key and no group-keys. The Kerberos protocol is then used for later authentication and creation of trusted paths. The EK server is the unique group-key repository and it provides encryption/decryption services of symmetric keys to CCDs. The EK server provides these services to Kerberos authenticated users based on the groups they belong to. To get a symmetric key for decrypting a document, a CCD sends the encrypted symmetric key to the EK server for decryption and then gets the symmetric key.

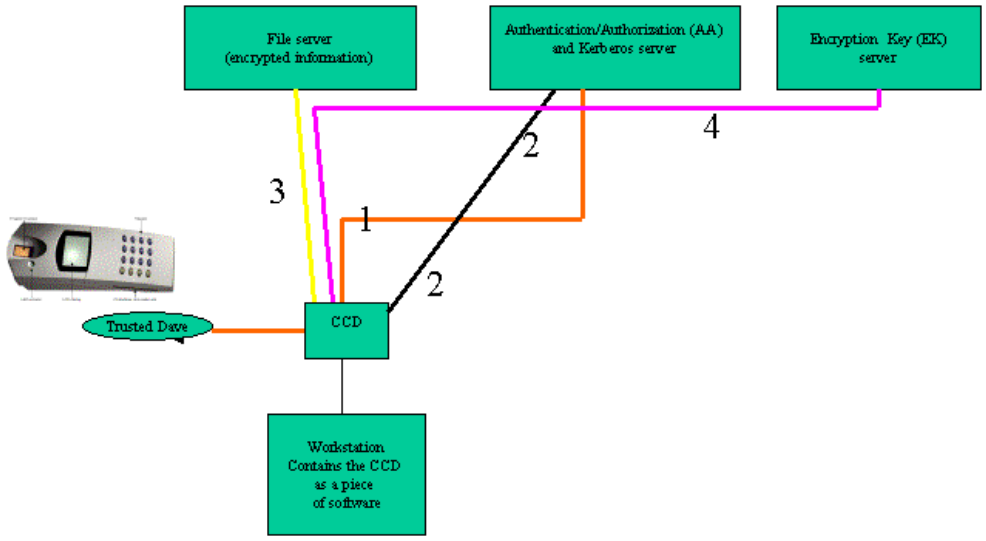

Figure 9-Kerberos CBIS-Like System

The following shows the steps involved while a user reads an encrypted file stored on the File server.

1. While Trusted DAVE initializes, a Trusted Path (numbered 1 and shown in orange in Figure 9) is created between Trusted DAVE, the CCD, and the AA/Kerberos server.

2. After a user is authenticated, the AA server sends the user's Kerberos key to the CCD as authorization data.

The following three steps relate only to the Kerberos protocol.

3. The CCD requests a Ticket Granting Ticket (TGT) from the Kerberos server. The TGT contents need to be specified. However, it would probably contain information on the user's group, classification, and/or domain, all of which are encrypted with the Kerberos server's Kerberos key. Note that steps 2 and 3 can be done in a single step.

4. The CCD uses the TGT to get two Server Tickets (STs) both accompanied with a session key. These session keys are encrypted with the user's Kerberos key. Each ST also contains the accompanying session key encrypted with the intended server's Kerberos key.

5. Two Trusted paths (numbered 3 and 4) are established using the session keys.

The final steps allow the CCD to read a file coming from the File server.

6. The requested encrypted file is sent through the Trusted path 3 to the CCD.

7. The CCD retrieves the encrypted symmetric key from the file and sends it through the Trusted Path 4.

8. The EK server returns the symmetric key through the trusted path 4.
9. Using the symmetric key, the CCD decrypts the encrypted file.

5. Generic CBIS architecture defined and compared

In this section, we introduce some definitions and concepts related to information domains and their implementations, provide a short overview on the traditional architecture for systems implementing one or more information domains and describe the Generic CBIS architecture for systems that support multiple information domains. Furthermore, for each of these architectures, we provide some of their advantages and limitations. Note that Sections 4.3 and 4.4 are particularly relevant to the Generic CBIS architecture because desktops defined in these sections could be used as local sub-systems when implementing the Generic CBIS architecture.

5.1 Some security concepts and definitions

We will use the following Technical Architecture Framework for Information Management (TAFIM) definitions and concepts [22]:

> *An information domain is a set of users, their information objects, and a security policy. An information domain security policy is a statement of the criteria for membership in the information domain and the required protection of the information objects.*
>
> *Information objects can be transferred between two information domains only in accordance with established rules, conditions, and procedures expressed in the security policy of each of them.*
>
> *The transfer can be accomplished only by a user who is member of both the sending and receiving information domain policies and, if required by the information domain policies, has been granted the appropriate privileges (e.g."release authority").*

Hence, an information domain security policy states the required protection of the information objects. Statements of security policies vary from policy to policy. Some require a security model for the system implementing the information domain (and possibly some other information domains). Security models have been developed to protect information from different types of attacks. Examples of well-known security models include Bell-Lapadula and non-interference.

5.2 Traditional architecture for a single information domain

The traditional architecture for a system (along with its environment) implementing a single information domain is shown in Figure 10. The system is composed of different unencrypted LANs connected together through a VPN. Each LAN is composed of connected workstations, servers, routers, and possibly other types of network nodes. The VPN is usually implemented through firewalls or Network Encryption Units (NEUs). The information domain's users are the authorized users and they are the only ones that are authorized to logically access the system. Physical access to the system is restricted. For instance, authorized users cannot usually access servers, routers, and boundary controllers. However, they can logically access the system through an entry point that is usually a workstation. These workstations may or may not physically protected.

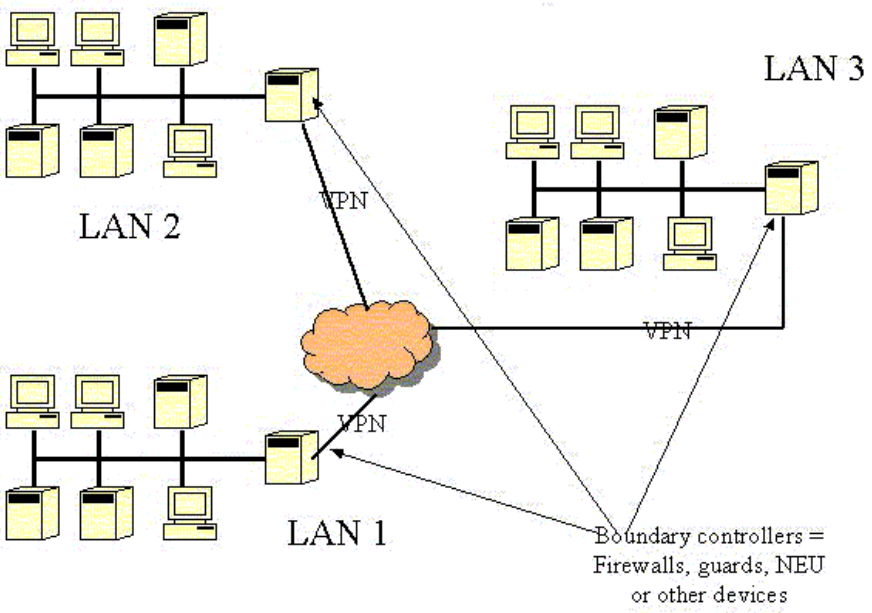

Figure 10: Classical architecture for systems implementing an information domain

There are a number of advantages and limitations of such systems:

Advantages:

A1) Physical protection. The system's physical environment enforces the protection of information objects from physical attacks made by unauthorized users that do not have physical access to the system.

A2) Logical protection. Firewalls/NEUs enforce protection of information objects from logical attacks made by non-domain users.

A3) Security model based. The system can easily satisfy/implement security models such as Bell-Lapadula and non-interference because only one information domain is involved.

Limitations:

L1) No automated inter-domain exchange mechanisms. Such a system does not allow any automated information object exchanges between the information domain implemented by the system and any other information domain.

L2) High hardware and management costs. Two systems and networks are needed to implement two information domains. This implies high costs.

L3) Confidentiality/integrity/authentication weaknesses. Such systems do not necessarily provide

- Confidentiality/integrity protection of information while information is in transit within LANs.

- Strong authentication mechanisms to prevent logical access to unauthorized users that have physical access to LANs.

5.3 A multiple information domain architecture

The system architecture shown at Figure 10 is modified as follow to become the multiple information domain architecture.

Firewalls/NEUs become guards. Each guard is a multiple information domain machine that enforces the inter-domain flow control sub-policy of an information domain. The information domain is said to be the guard's information domain. The sub-policy controls the automated information flow from and to the domain.

All information objects that are located on a given LAN but its guard belong to a single information domain, which is the guard's information domain. Therefore, a LAN without its guard supports a single information domain. This domain is also said to be the LAN's information domain.

The architecture has the following advantages and limitations:

Advantages:

A1) Physical protection.

A2) Logical protection.

A4) Automated inter-domain exchange mechanisms. Transfers of information objects between domains are now possible.

Limitations:

L3) Confidentiality/integrity/authentication weaknesses.

L4) Guard implementation problem. It is difficult to implement such guards.

L5) Security model problem. It is not clear if it is possible to design a guard implementing a known security model.

L6) Single information domain support for LANs. Two LANs are necessary to implement two information domains.

5.4 Generic CBIS architecture

The system architecture shown in Figure 10 is modified as stated below to become the Generic CBIS architecture. Figure 11 shows an example of a resulting system architecture. The security in this architecture is no longer based on networks but on the content of information. There is no need to assign an information domain to each LAN: security is based on encrypted communication channels and encryption at origin (nodes).

The following points describe briefly the Generic CBIS architecture. These points are analysed in Sections 5.4.1-5.4.5. Section 5.4.6 states the architecture's advantages and limitations.

Elements of the Generic CBIS Architecture:

- **Network and specialized nodes**. The network is a set of connected nodes that are either supporting nodes, or Local Sub-System (LSS) nodes. LSS nodes are sub-systems composed of two or three nearby inter-connected physical components: a security card, an end-system, and possibly an authentication terminal. Note that Figure 11 needs to be interpreted in the context of the Generic CBIS architecture. The represented nodes are the LSS nodes and some supporting nodes. Boundary controllers and some other nodes can be either LSS nodes or supporting node depending on the CBIS architecture considered. In Figure 11, the boundary controllers shown are LSS nodes. However, they could be also simple supporting nodes (firewalls/NEUs)
- **Encrypted network communications**. Communications between LSS nodes are network encrypted with network-keys.
- **Encrypted information objects.** Information is stored in information objects that are always object encrypted outside LSSs. Information objects are encrypted by object-keys, which are encrypted by group-keys. There exists a one-to-one mapping between information domains and group-keys. A user can access an information object in the clear only if the object belongs to an information domain in which the user belongs to.
- **Information exchange mechanisms.** Mechanisms exist to allow intra-domain information exchanges. Inter-domain information exchange mechanisms may be present, as well. Different types of LSS nodes may implement these mechanisms.
- **VPNs** . VPNs can be implemented by firewalls/NEUs.

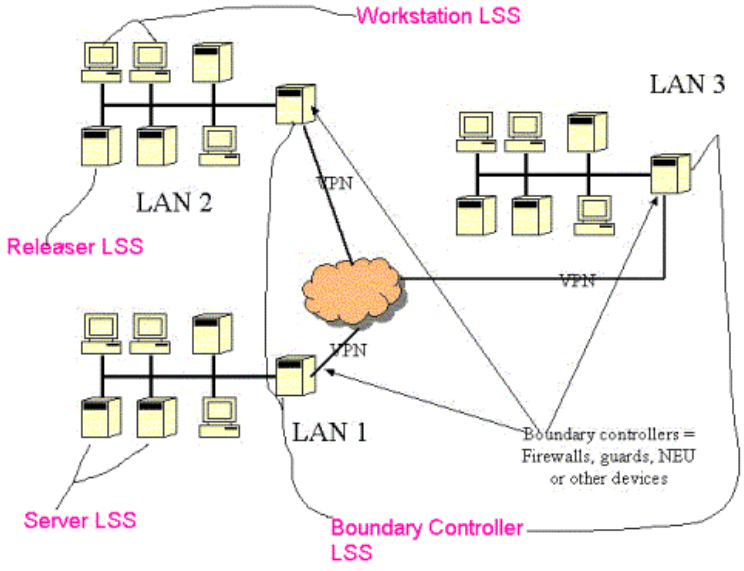

Figure 11: Generic CBIS Architecture

5.4.1 CBIS networks and LSS nodes

A CBIS network is a set of connected nodes that are either supporting nodes, or LSS nodes. A router is an example of supporting node, while LSS nodes are sub-systems composed of two or

three nearby inter-connected physical components: a security card, an end-system (e.g. computer or workstation), and possibly an authentication terminal. Therefore, workstations, and usually servers, or other types of end-systems are no longer network nodes; they are components of LSS nodes.

The security card is uniquely the LSS's external interface to the network; other LSS's components are attached to it. The main roles of the security card within an LSS are to perform network and object encryption/decryption, and securely store keys and credentials. Hence, the security card performs operations for which the end-system is deemed insecure. This is particularly true for user LSSs, which are defined below, because workstations are deemed insecure for the storage of keys and credentials and for authentication.

Different types of LSSs are possible. There are user and server types and some special types such as guard and releaser types. A type is associated with a functionality. For instance, an LSS that has the guard functionality is of the guard type. Not all types are necessarily present in a given implementation. However, all implementations of the Generic CBIS architecture have user-LSS nodes, which are the nodes from which users work. In all implementations we assume the following: each user-LSS node contains an authentication terminal; end-systems in user-LSS nodes are workstations; nodes of other types may or may not contain an authentication terminal depending of the architecture's implementation.

User-LSS nodes are multi-single-user secure nodes. This means that many users can use the node but at different time. Implementation of this could be made through period processing or through MLS OS. Normal users interact with the system only through user-LSS node. This interaction is through an authentication terminal for authentication and through a workstation for other purposes. Desktops defined in Sections 4.3 and 4.4 may be seen as examples of possible user-LLS nodes.

5.4.2 Network encryption

All communications between LSS nodes are network encrypted with network-keys. It is possible that some non-LSS nodes can be part of the network encryption system. Therefore, the network encryption system is not necessarily dependent on the object encryption system introduced below. For LSS nodes though, we assume that network encryption is performed and protected by security cards.

5.4.3 Information objects

Information is stored in information objects. An information object is object encrypted with an object-key (i.e. a symmetric key in Section 4), which is encrypted by one or more group-keys. There exists a one-to-one mapping between information domains and group-keys. Encrypted object-keys are bound with their respective encrypted information objects. Note that only LSS nodes are allowed to encrypt/decrypt information objects.

A user can decrypt an encrypted information object only if the user belongs to an information domain for which the information domain's group-key can decrypt the object's object-key.

5.4.4 Information exchange mechanisms

Different information exchange mechanisms can be implemented but all are dependent on the initialization of the LSS nodes. Therefore, before describing some possible implementations of these mechanisms we will focus our attention on the initialization of LSS nodes. There are two types of initialization: the initialization of LSSs with an authentication terminal and those without authentication terminal.

If an LSS has an authentication terminal, the initialization can be performed in one or two phases. If it is performed in two phases, the first phase is very similar to what is described in the next paragraph. The second phase occurs when the LSS authenticates a user. The authentication terminal gets the user's credentials (e.g. PIN, fingerprints, token) and collaborates with the security card and a key-server LSS in authenticating the user. After authentication, the security card obtains, from a key-server LSS, the authorization information and/or group-keys associated with the user, which allow it to perform object and network encryption/decryption on behalf of the user. If the LSS's initialization is performed in one phase, everything is done while a user is authenticated.

If an LSS does not have an authentication terminal, the security card initializes its network encryption function. This can be implemented in several ways. For example, the credentials needed to perform encryption and negotiate session-keys can be loaded dynamically from a server or loaded manually at installation time. Normally, these LSSs are not able to encrypt/decrypt information objects because they cannot decrypt object-keys. This is the case for server-LSS nodes. However, it is possible that other types of LSSs will use embedded credentials in the security card to get authorization information and/or group-keys from a key-server LSS.

After initialization, there are two types of LSSs: those that can encrypt/decrypt objects and all others. Let us define the first type as type O and the second type as type N. We may now consider different exchange mechanisms. Only three cases are considered here. The first two exchange mechanisms provide intra-domain information exchange examples while the last provides an inter-domain information exchange example.

Case 1: No direct exchanges between LSSs of type O. This is used by the CBIS ACTD. Information from an LSS node of type O is sent to/received from a node of type N. The node of type N serves as a repository. In order for users to exchange information, they must belong to the same information domain and communicate through the repository.

Case 2. Direct exchanges between LSSs of type O.

Case 3: Information exchanges through a releaser LSS. In this case, a user sends information from an information domain to another. It is assumed that the releaser LSS can encrypt/decrypt object-keys from the two information domains. In this case, the user sends information from a user LSS (type O) to a releaser LSS (type O). The releaser then decrypts the object-key and encrypts it with the second information domain's group-key. Therefore, any user from the second domain may now get the information from the releaser's LSS.

5.4.5 VPNs

VPNs can be implemented by supporting nodes and be based on firewalls/NEUs. Even though guards are not required, they can be used as LSS nodes in place of firewall/NEUs if the system is connected to none CBIS systems for instance.

5.4.6 Generic CBIS architrecture : advantages and limitations

The Generic CBIS architecture has the following advantages and limitations:

Advantages:

A1) Physical protection. As noted in L9 below, the physical security of the two previous architectures must be reinforced because users of different information domains may be present in a LAN.

A2) Logical protection. Guards enforcing information domain security policies are not assumed here even if there exist inter-domain information exchange mechanisms. Hence, firewalls/NEUs can be used as LANs' boundary controllers.

A4) Automated inter-domain exchange mechanisms. It is assumed here that at least one LSS can perform the exchange operation. For instance, this LSS can be an MLS-user LSS or an MLS-guard LSS if domains support an MLS security policy.

A5) Confidentiality/integrity/strong authentication. The architecture provides

- Confidentiality/integrity protection of information while information is in transit within and outside LANs.

- Strong authentication mechanisms to prevent logical access to unauthorized users that have physical access to LANs.

A6) Multiple domain support for LANs. The Generic CBIS architecture compared to the two previous architectures minimizes the number of LANs necessary for a system.

Limitations: L1-L4 and L6 are no longer limitations.

L5) Security model problem.

L7) New mechanisms for information exchange needed. Even though (L4) is not a limitation because firewall/NEUs can be used, if exchanges between information domains are needed, this exchange service needs to be done by one or more LSSs. It is not clear if it is easier to make such LSSs than to make a guard for the previous architecture. However, in a sytem with many LANs, it is possible that a single LSS node provides an exchange service for all the system.

L8) Cost of LSS nodes. LSSs are more expensive than end-systems. Moreover, different types of LSS systems need to be developed to achieve systems with desired functionalities, implying development costs.

L9) The problem of unauthorized information flows due to workstations. In the Generic CBIS architecture, a workstation may contain information from different information domains over a period of time; this risk is not present in the two other architectures. For instance, a member of a domain1 that is not member of a domain2 may have physical access to domain2's residual information located on workstations. So, measures such as those stated in Section 4.3 must be implemented to prevent/mitigate leakage of information on workstation between user sessions. Note that this problem may be present also for servers. However, servers may not be physically accessible to users.

L10) Cost of strong authentication mechanisms needed. Strong authentication mechanisms are needed because users can belong to different information domains and work in a same physical environment. In the two other architectures, strong authentication may be not required because all users of a LAN belong to the same information domain. Trusted DAVE is an example of system that could provide strong authentication to CBIS systems.

Advantages\ Architectures	Traditional architecture/Single information domain	Multi information domain architecture	Generic CBIS architecture
A1) Physical protection	X	X	X
A2) Logical protection	X	X	X
A3) Security model based	X		
A4) Automated inter-domain exchange mechanisms		X	X
A5) Confidentiality/integrity/ Strong authentication			X
A6) Multiple domain support for LANs			X
Limitations:			
L1) No automated inter-domain exchange mechanisms	X		
L2) High hardware and management costs	X		
L3) Confidentiality/Integrity/ authentication weaknesses	X	X	
L4) Guard implementation problem		X	
L5) Security model problem		X	X
L6) Single information domain support for LANs	X	X	
L7) New mechanisms for information exchanges needed			X
L8) Cost of LSS nodes			X
L9) The problem of unauthorized information flows due to workstations.			X
L10) Cost of strong authentication mechanisms needed			X

Table 1: Advantages and limitations of the three architectures

References

1. CDE White Paper Content Based Information Security (CBIS), Saclant, http://www.saclant.nato.int/cde/projects/CBIS White Paper v3 complete.doc

2. McGovern, C, Susan (2001). Information Security Requirements for a Coalition Wide Area Network, Naval Postgraduate School Thesis, http://cisr.nps.navy.mil/downloads/thesis/01thesis_mcgovern.pdf

3. Controlled Access Protection Profile, Version 1.d, http://commoncriteria.org/protection_profiles/CAPP-1.c.pdf

4. Biometric Device Protection Profile (BDPP), Draft Issue, Version 0.82, http://www.cesg.gov.uk/assurance/iacs/itsec/documents/protection-profiles/index.htm

5. SCSUG Smart Card Protection Profile, Version 3.0, http://csrc.nist.gov/cc/sc/sclist.htm

6. Protection Profile Smart Card Integrated Circuit With Embedded Software, Version 2.0, http://www.eurosmart.com/Activities/DownloadArea/Download.html

7. Transactional Smart Card Reader Protection Profile Version 2.0, http://www.scssi.gouv.fr/fr/confiance/pp.html

8. Labelled Security Protection Profile, Version 1b, http://www.cesg.gov.uk/assurance/iacs/itsec/documents/protection-profiles/index.htm

9. Best Practices in Testing and Reporting Performance of Biometric Devices, Version 1.0, http://www.biometrics.org/html/standards.html

10. Draft Authentication Module Interface Standard, NIST, http://www.biometrics.org/html/standards.html

11. FIPS 140-2 Security Requirements for Cryptographic Modules, http://cnscenter.future.co.kr/resource/crypto/standard/fips/fips1402.pdf

12. IEEE Std 1233 - 1998 IEEE Guide for Developing System Requirements Specification, IEEE New-York, 1998. http://www.computer.org/cspress/CATALOG/st01111.htm

13. Labcal.Group, Trust Analysis Comparison CBIS I&A / DREO V&A P270 - DREO V&A Device System, Version 001 (rev. 005) (DRDC Ottawa internal contractor report), Labcal.Group.

14. Labcal.Group, System Requirements Specification P270 - DRDC-Ottawa V&A Device System, Version 001 (Rev. 004) (DRDC Ottawa internal contractor report), 2002-10-14, Labcal.Group.

15. Labcal.Group, Definition of Subcomponent Options P270 - DRDC-Ottawa V&A Device System, Version 001 (DRDC Ottawa internal contractor report), 2002-11-01, Labcal.Group.

16. Labcal.Group, Two Design Concepts P270 - DRDC-Ottawa V&A Device System, Version 001 (DRDC Ottawa internal contractor report), 2002-10-29, Labcal.Group.

17. Labcal.Group, Security Target P270 - DRDC-Ottawa V&A Device System, Version 004 (DRDC Ottawa internal contractor report), 2002-12-11, Labcal.Group.

18. Labcal.Group, Detailed Design P270 - DRDC-Ottawa V&A Device System, Version 004 (DRDC Ottawa internal contractor report), 2003-01-08, Labcal.Group.

19. Labcal.Group, Test Plan P270 - DRDC-Ottawa V&A Device System, Version 003 (DRDC Ottawa internal contractor report), 2003-02-19, Labcal.Group.

20. Labcal.Group, User Guide P270 - DRDC-Ottawa V&A Device System, Version 002 (DRDC Ottawa internal contractor report), 2003-03-29, Labcal.Group.

21. Labcal.Group, Final Report P270 – DRDC-Ottawa V&A Device System, Version 001 (DRDC Ottawa internal contractor report), 2003-03-30, Labcal.Group.

22. Technical Architecture Framework for Information Management (TAFIM), DISA, http://in.disa.mil/tafim.html

List of acronymes

AA	Authentication and Authorization
ACTD	Advanced Concept Technology Demonstrator
CBIS	Content Based Information Security
CC	Common Criteria
CCD	Compatible Connected Device
CF	Canadian Forces
CMOS	Complimentary Metal-Oxide Semiconductor
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CSC	CBIS Security Card
DAR	Data at Rest
DRDC	Defence Research and Development of Canada
EEPROM	Electrical Erasable Programmable Read-Only Memory
EK	Encryption Key
FIPS	Federal Information Processing Standards Publications
LAN	Local Area Network
LCD	Liquid Crystal Display
LSS	Local Sub-System
NATO	North Atlantic Treaty Organization
MLS	Multi Level Security
MSLS	Multi Single Level Security
NEU	Network Encryption Unit
OS	Operating System
PIN	Personnel Identification Number

PP	Protection Profile
RAM	Random Access Memory
RDDC	Recherche et développement pour la defence Canada
SOW	Statement Of Work
SPAWAR	Space & Naval Warfare Systems Command
ST	Security Target
ST	Service Ticket
TAFIM	Technical Architecture Framework for Information Management
TGT	Ticket Granting Ticket
Trusted DAVE	Trusted Device for Authentication and VErification
USB	Universal Serial Bus
V&A	Verification and Authentication
VPN	Virtual Private Network

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.)

   Defence R&D Canada – Ottawa
   Ottawa ON K1A 0Z4

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.)

   A strong three-factor authentication device: Trusted DAVE and the new Generic Content-Based Information Security (CBIS) architecture (U)

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

   Savoie Jean

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

   November 2004

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

   39

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

   22

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.)

   DRDC Technical Memorendum

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

   DRDC Ottawa, Network 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)

   15bf27 and 15bf30

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

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.)

   DRDC Ottawa TM 2004-198

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

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).

This report has three objectives. The first objective is to provide a description/analysis of the Trusted DAVE activity performed by DRDC Ottawa and its contractors. The second is to describe different systems where the demonstrator produced under this activity could be used. The last is to analyse, study, and compare different types of network/system architectures.

The activity involved the development of three elements: A secure design for a three-factor Trusted Device for Authentication and VErification (Trusted DAVE), a device demonstrator implementing some of those design elements, and an authentication and verification demonstration system that utilises the device demonstrator. The purpose of the device is to provide the user interface component to be used as a part of a strong Verification and Authentication (V&A) capability for systems used to process classified or sensitive data.

Four possible systems that could use Trusted DAVE are presented. Two of them are related to the CBIS (Content-Based Information Security) concepts and one integrates CBIS and Kerberos. Finally, three architectures for network systems are presented with their advantages and their limitations. A Generic CBIS architecture covering the one specified in the US CBIS ACTD is defined and compared with the two others. The purpose of the Generic CBIS architecture is threefold: (1) provide an architecture for systems generalizing the US ACTD one, (2) illustrate the architecture's fundamental aspects, and (3) introduce an architecture where Trusted DAVE could be useful.

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, CBIS, Kerberos, security architecture

Defence R&D Canada

Canada's leader in defence
and national security R&D

R & D pour la défense Canada

Chef de file au Canada en R & D
pour la défense et la sécurité nationale

www.drdc-rddc.gc.ca