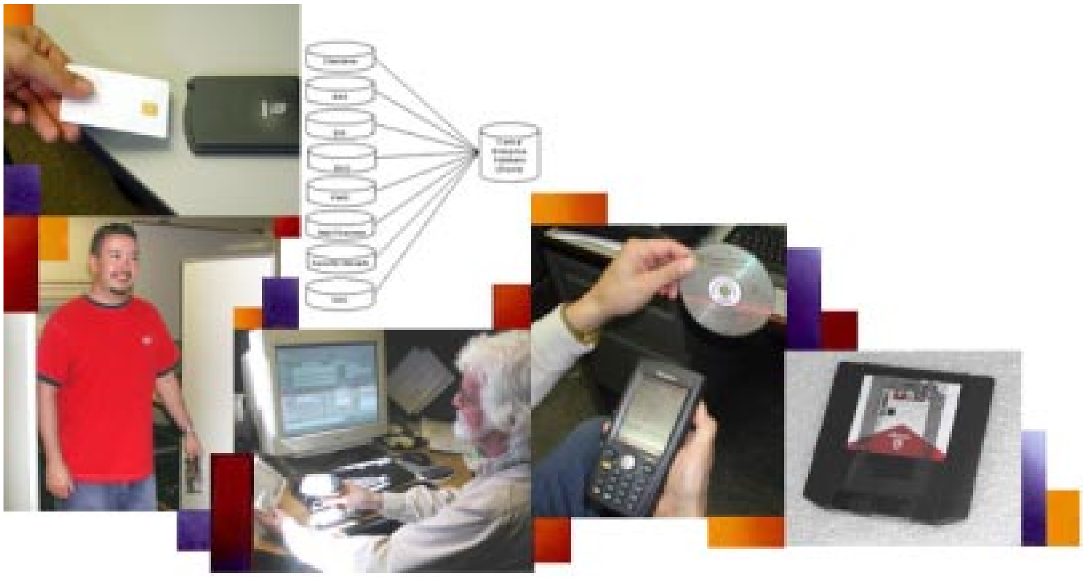
LA-14021

Sixty Percent Conceptual Design Report: Enterprise Accountability System for Classified Removable Electronic Media



1943 - 2003
Los Alamos
NATIONAL LABORATORY
Ideas That Change the World

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the Regents of the University of California, the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Regents of the University of California, the United States Government, or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the Regents of the University of California, the United States Government, or any agency thereof. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

LA-14021
Issued: May 2003

Sixty Percent Conceptual Design Report: Enterprise Accountability System for Classified Removable Electronic Media

Beth Gardiner
Luca Graton
Joseph Longo
Thomas Marks, Jr.
Benny Martinez
Richard Strittmatter
Collis Woods

Compiled by Joshua Joseph, Jr.

1943 - 2003
Los Alamos
NATIONAL LABORATORY
Ideas That Change the World

Acknowledgements

The authors would like to acknowledge the hard work and expertise of the CREM Control Project team members.

NIS-7: Safeguards Systems
Robert Landry Dana Maestas Margaret Manzanares
Joline Martinez Lorraine Medina Lee Taylor

IM-8: Advanced Information and Business Application Development
John Brown Shirley Herrera Patricia Hummer
Donna Moniz

NIS-5: Safeguards, Science, and Technology
Kenneth Baird, III Richard Siebelist

Contents

List of Figures

List of Tables

List of Acronyms

ADC	authorized derivative classifier
ADC DS	ADC detection system
BUS	Business Operations Division
CAS	CREM Accountability System
CCN	Computing, Communications, and Networking Division
CIP	cryptographic interface
CMC	classified media custodian
CPU	central processing unit
CREM	classified removable electronic media
DBA	database administrator
EAS	Electronic Authorization System
EDS	Employee Development System
EIS	Employee Information System
EVB	eMbedded Visual Basic™
FMIS	Financial Management Information System
FTE	full-time employee
GW	gateway
HD	hard drive
HPSS	high-performance storage system
HTML	hypertext markup language
ICN	integrated computing network
ID	identification
IDE	integrated drive electronics
IM	Information Management Division
LANL	Los Alamos National Laboratory
Merc DS	Mercury detection system
MFC	mainframe computer
MTM	MediaTracker Manager
NIS	Nonproliferation and International Security Division
OS	operating system
OSI	Office of Security Inquiries
PC	personal computer
PC/SC	personal computer/smart card
PCMCIA	Personal Computer Memory Card International Association
PIN	personal identification number
PKI	public key infrastructure
R	register
RAM	random access memory
RF	radiofrequency
RFID	radiofrequency identification
RFP	request-for-proposal
SAS	Signature Authority System
S-Division	Analysis and Assessment Division
SM	South Mesa site
SCC	Strategic Computing Complex

SSM	specialist staff member
TA	technical area
TSM	technical staff member
UPN	unclassified protected network
USB	universal serial bus
VTR	vault-type room
X-Division	Applied Physics Division

Sixty Percent Conceptual Design Report: Enterprise Accountability System for Classified Removable Electronic Media

Compiled by Joshua Joseph, Jr.

Abstract

Classified removable electronic media (CREM) are tracked in several different ways at the Laboratory. To ensure greater security for CREM, we are creating a single, Laboratory-wide system to track CREM. We are researching technology that can be used to electronically tag and detect CREM, designing a database to track the movement of CREM, and planning to test the system at several locations around the Laboratory. We focus on affixing "smart tags" to items we want to track and installing gates at pedestrian portals to detect the entry or exit of tagged items. By means of an enterprise database, the system will track the entry and exit of tagged items into and from CREM storage vaults, vault-type rooms, access corridors, or boundaries of secure areas, as well as the identity of the person carrying an item. We are considering several options for tracking items that can give greater security, but at greater expense.

Overview

In the last several years, Los Alamos National Laboratory (LANL) has implemented solutions to enhance the protection of classified materials. In particular, a number of database applications have been created to augment the Laboratory's ability to track and account for CREM. The most widely used application, MediaTracker/MediaTracker Manager (MTM) Suite, has been deployed in more than 45 groups at LANL. Other organizations, such as X-Division, have also created database applications that have improved their ability to track CREM. These systems have reduced human error and increased efficiency in accounting for CREM.

Given the success of these systems, LANL is developing requirements for an enterprise system to track and account for CREM. An enterprise system is a single, centralized application that can be used by organizations throughout the Laboratory to access real-time CREM information from a central database management system.

The following are major benefits of an enterprise CREM Accountability System (CAS):

- Increased efficiency in accounting for CREM
- Electronic notifications of events such as change of ownership or CREM sent to an external organization
- Enforcement of a consistent set of business rules
- Real-time inventory status

- Transaction history (e.g., reporting capabilities for item origination, transfer, and destruction)
- Real-time access to CREM data
- Integrated information (e.g., employment status, training status, clearance level, and citizenship) to control access
- Use of infrastructure currently in place at LANL
- Backup and disaster recovery plans
- Elimination of duplicate data entry
- The ability to exchange data between the central database and the portal workstations

An enterprise system can also provide an integrated, systematic approach to CREM security by supporting engineered controls such as portals, electronic tags, and smart cards. A central database that interfaces with engineered controls can deliver an integrated system that helps eliminate the inadvertent removal of CREM. An enterprise system will help meet the Laboratory's need for real-time tracking, accountability, and access to required CREM data.

Project Summary

The goal of this project is to ensure the most programmatically efficient, cost-effective, and secure management of classified removable electronic media by implementing an enterprise-wide inventory and tracking system that incorporates engineered controls.

To date the CREM project team has accomplished the following:

- Analyzed current practices for tracking CREM at LANL
- Met with LANL business users to develop new processes for tracking CREM using an enterprise system
- Documented new processes and reviewed them with LANL business users
- Acquired hardware for smart card, portable inventory, portal and radio frequency identification (RFID) pilots
- Developed pilot strategies for the use of smart cards, portable inventory, and radio frequency (RF) portal monitors
- Completed the first draft of the customer's requirements document
- Documented the entities and attributes needed for the enterprise system

The next steps are to

- implement the smart card, portable inventory, portal, and RFID pilots;
- develop prototypes of screens and reports to be used in the enterprise system;
- develop a request-for-proposals (RFP) to send to vendors; and
- solicit vendor responses to the RFP.

Program Requirements

Four key steps may reduce the possibility of CREM being removed from our site without detection:

1. A Laboratory-wide inventory, consolidation, and tracking of all classified media

2. A priority investigation into state-of-the-art detection devices and portal monitors at the exits of classified facilities
3. An increase in accountability through verification, such as random searches of individuals leaving a classified facility
4. Replacing local office access to CREM with a keyboard-video-mouse medialess computing environment

Accountability and control are two primary objectives in controlling CREM. Each can be enhanced through the use of engineered controls and advanced systems that reduce reliance on manual accounting thereby reducing human error. The goal of this project is to provide an enterprise-wide system for tracking CREM that integrates engineered controls. The system has one main objective: to identify the location and person responsible for any CREM in the database.

Additionally, this project should

- support and expand the functionality available in existing departmental systems used to track CREM,
- reduce the work required to track CREM,
- provide real-time access to CREM data stored in a single Laboratory-wide database,
- provide a central repository for portal data,
- replace administrative controls with engineered controls,
- improve data accuracy and consistency,
- enhance enforcement of clearance requirements for handling CREM,
- enhance enforcement of training requirements for handling CREM,
- provide automatic data backups, and
- provide an auditable trail of all CREM transactions.

Design Options

An enterprise system to track CREM can use a number of different designs. At the system's core there is a central database and a common application that most groups at the Laboratory use to account for CREM (there are exceptions, such as the Sensitive Compartment Information Facility). Additional capabilities can be added to the system by incorporating engineered controls such as portals, RFID tags, and smart cards. The portal is the physical entry or exit through which patrons will carry CREM; an RFID tag is an electronic tag attached to each piece of CREM, which will be monitored by an RF gate antenna at the portal; and a smart card is an identification card with a readable-writable computer chip.

The Laboratory has experience with some of these technologies, but others are in the pilot or research phase; therefore, we recommend a three-phased implementation of a full-capability system to track CREM. This approach allows the Laboratory to begin implementing proven technologies immediately while continuing to pilot new technologies before they are moved into a production environment. It also allows the Laboratory to implement a system that is flexible enough to incorporate new engineered controls when those technologies are ready.

Phase 1: CAS with Portable Inventory Capability

In Phase 1, the Laboratory implements the core technology for a Laboratory-wide system to track CREM (the CAS). Figure 1 illustrates the general organization of the system in this initial stage.

An enterprise system requires a central database to store most of the CREM data generated at Los Alamos. All users will interact with the CAS via a common application. Bar-code readers will be the default technology.

The central database will be an Oracle® database hosted on a machine connected to the unclassified protected (yellow) network and maintained by IM-3. The central database will be accessed from workstations that are also connected to the yellow network. The connected workstations will access and update the central database in real time.

The central database will retrieve data from other LANL databases (e.g., employee data, training and authorities, classified mail stops, and approved mailing addresses). This data will be used to enforce the system business rules (e.g., verifying that a user has the necessary authorities and training to access a system function). It will also be used to populate fields with consistent values. For example, the user will populate the location field selecting from a drop-down list of technical areas, buildings, and rooms.

The CAS software will be Web-based, and the client software will be a LANL-standard Web browser such as Netscape or Internet Explorer, allowing the application to be used from Unix, Windows®, or Macintosh® computers. Web-based software is also easier to update because the updates only need to be distributed to one location. Existing CRYPTOCard™ technology will be used for authentication and electronic signatures.

There will be four types of client workstations:

1. the full-scale configuration (typically used by classified media custodians, or CMCs)
2. the minimal configuration (a user's standard workstation)
3. the kiosk configuration (to check CREM in and out)
4. a mobile computer configuration (for mobile tasks such as inventory and package delivery)

Benefits, Relative Cost, and Risks

Phase 1 implements the core technology that needs to be in place before engineered controls can be implemented Laboratory-wide. It also meets the stated goal of providing an enterprise system to identify where a piece of CREM is and who is responsible for it.

There are several benefits of implementing a Laboratory-wide system:

- Real-time access to all CREM data from one system
- Enforcement of authorities and training needed to access CREM
- Increased efficiency through reduced use of paper forms and hard-copy signatures
- E-mail notifications and reminders that track CREM more closely
- Greater consistency of data
- Greater consistency in procedures to account for CREM
- Enterprise-wide system support

There are risks associated with a Laboratory-wide system:

- It depends on access to the unclassified protected network
- Classified data could be inadvertently introduced into an unclassified database
- The network may be busy or unavailable

All technologies proposed in Phase 1 have been successfully implemented in other Laboratory-wide systems. Our design includes only the essential functions needed to track CREM.

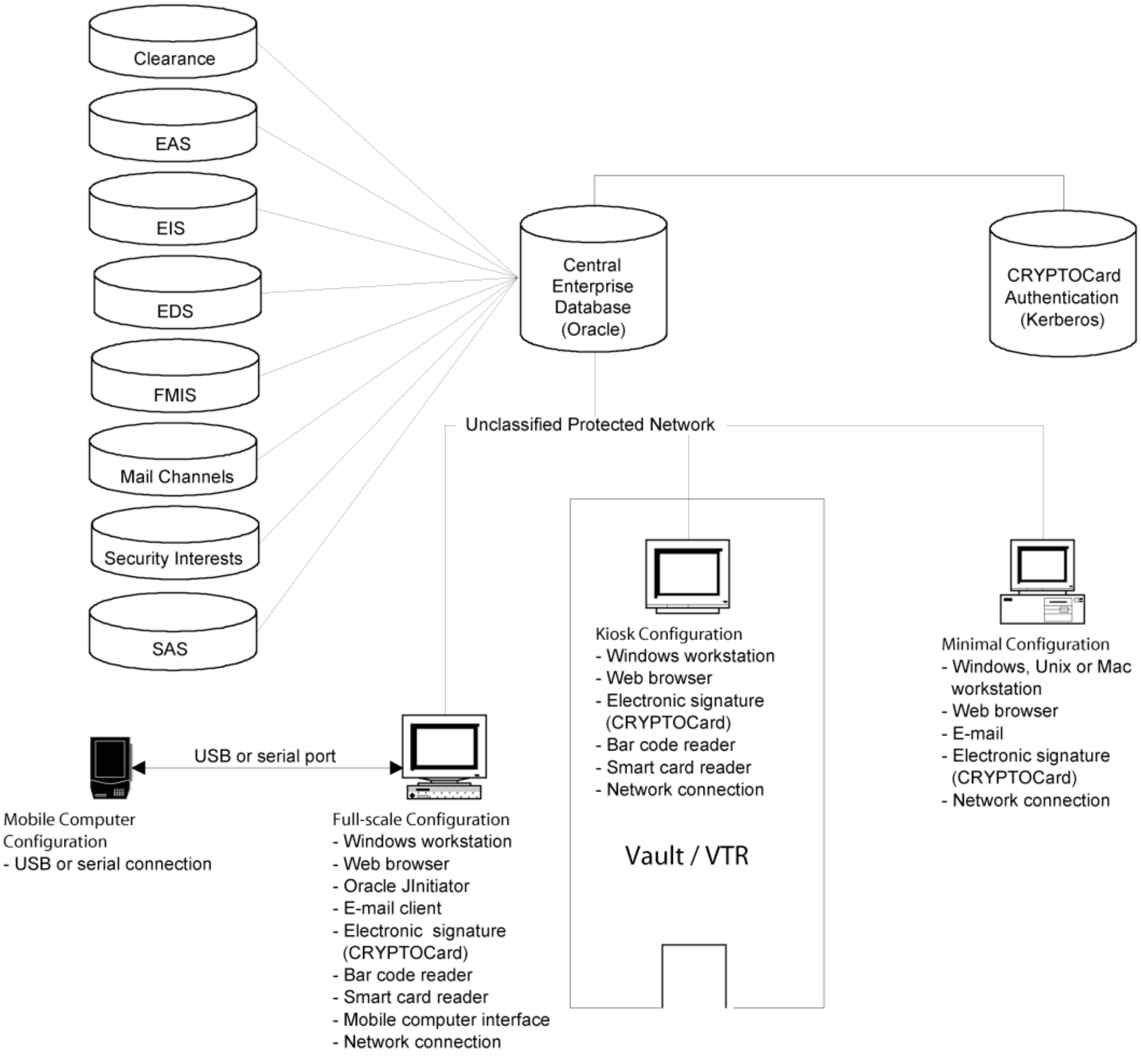


Figure 1. This diagram shows the basic components and organization of the CAS in the first phase. At left are the organizational databases that will access the CAS.

Phase 2: CAS with Portals and RFID Tags

Phase 2 will maintain all the capabilities of Phase 1 and also allow data exchange between the portals and the central database. Figure 2 illustrates the organization of the CAS in Phase 2.

In Phase 2, each portal will have a workstation that will capture the portal transactions locally, i.e., movement of CREM through the portal. In this design, the user checks out the CREM in the CAS before moving through the portal. This transaction will then be recorded in the central database.

Subsequently, as a user carries CREM through a portal, the gate antenna reads the RFID tag on the CREM. The portal workstation then submits two transactions to the central database: the transaction itself (CREM moving through a portal) and a query asking if the CREM is checked out. The central database records the transaction, including the portal location, and then responds to the query with a true or false reply. The query result will trigger appropriate actions, such as sounding an alarm or generating a report. Exact actions will be determined during the portal pilot.

Benefits, Relative Cost, and Risks

Phase 2 incorporates engineered controls and decreases LANL's dependence on administrative controls.

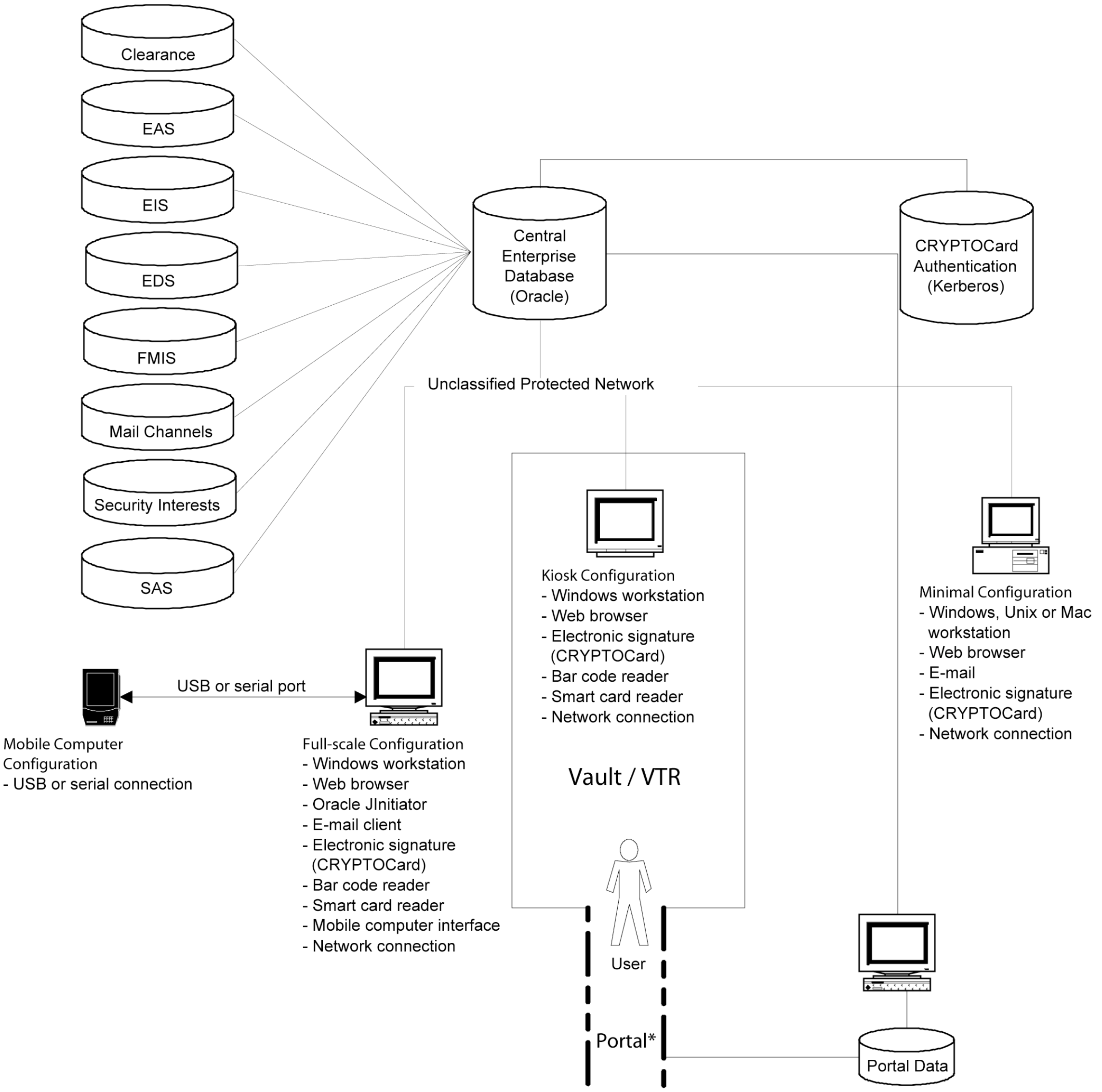
The benefits of portals are

- automated detection of inadvertent removal of CREM and
- increased efficiency in tracking CREM.

The risks associated with portals are

- portal and RFID technology may not reliably detect movement of CREM through the portal,
- central database response time may be too slow, and
- the network may be down.

Phase 2 can begin once the portal and RFID tag pilots are completed. We will need additional pilots to determine the best way to move data between the central database and the portal workstations.



*Portal location may be at a vault or VTR exit, a security area exit, a building exit, a guard station, etc.

Figure 2. In the second phase, a computer system at the portal will track the entry and exit of users carrying CREM out of a vault or vault-type room (VTR).

Phase 3: CAS with Portals, RFID Tags, and Smart Badges

Phase 3 will maintain all the capabilities of Phase 2 and will also use a new technology called smart badges, which are badges that use incorporate a smart-card chip, for user authentication and electronic signatures. Our goal is to end the need for both a badge and a CRYPTOCard, and combine their functions in one smart badge. In this phase, the system will determine both the movement of CREM and the person moving it. Figure 3 illustrates the general organization of the system in this stage.

In this phase, the user will still check out the CREM in CAS before moving through the portal. This transaction will be recorded in the central database. The smart badge is used to identify the user to the system and to electronically sign for the CREM.

At the portal entrance, the user swipes his or her smart badge and then moves through the portal with the CREM. The portal workstation captures the user's identification and the RFID information, identifying both the person moving through the portal and the CREM he or she is carrying. The portal workstation submits two transactions to the central database: the transaction itself (i.e., user X is moving through portal Y with CREM) and a query asking if the CREM is checked out and, if so, to whom. The central database records the transaction, including the portal location and user, and responds to the query with a true or false reply. The query reply will trigger appropriate actions, such as alerting the closest guard station. Exact actions will be determined during the smart badge pilot.

Benefits, Relative Cost, and Risks

Phase 3 incorporates additional engineered controls and further decreases LANL's dependence on administrative controls.

The benefits of smart badges are

- no need to carry both a badge and a CRYPTOCard and
- information can be written to the smart badge.

The risks associated with portals are

- smart badge technology must be approved for use at LANL,
- current methods for accessing enterprise systems will need to be modified to use smart badge technology, and
- an administrative processes for issuing smart badges must be created.

This phase can begin once the smart badge pilot is completed, the Laboratory has approved the use of smart badges, and the infrastructure is in place to support smart badges.

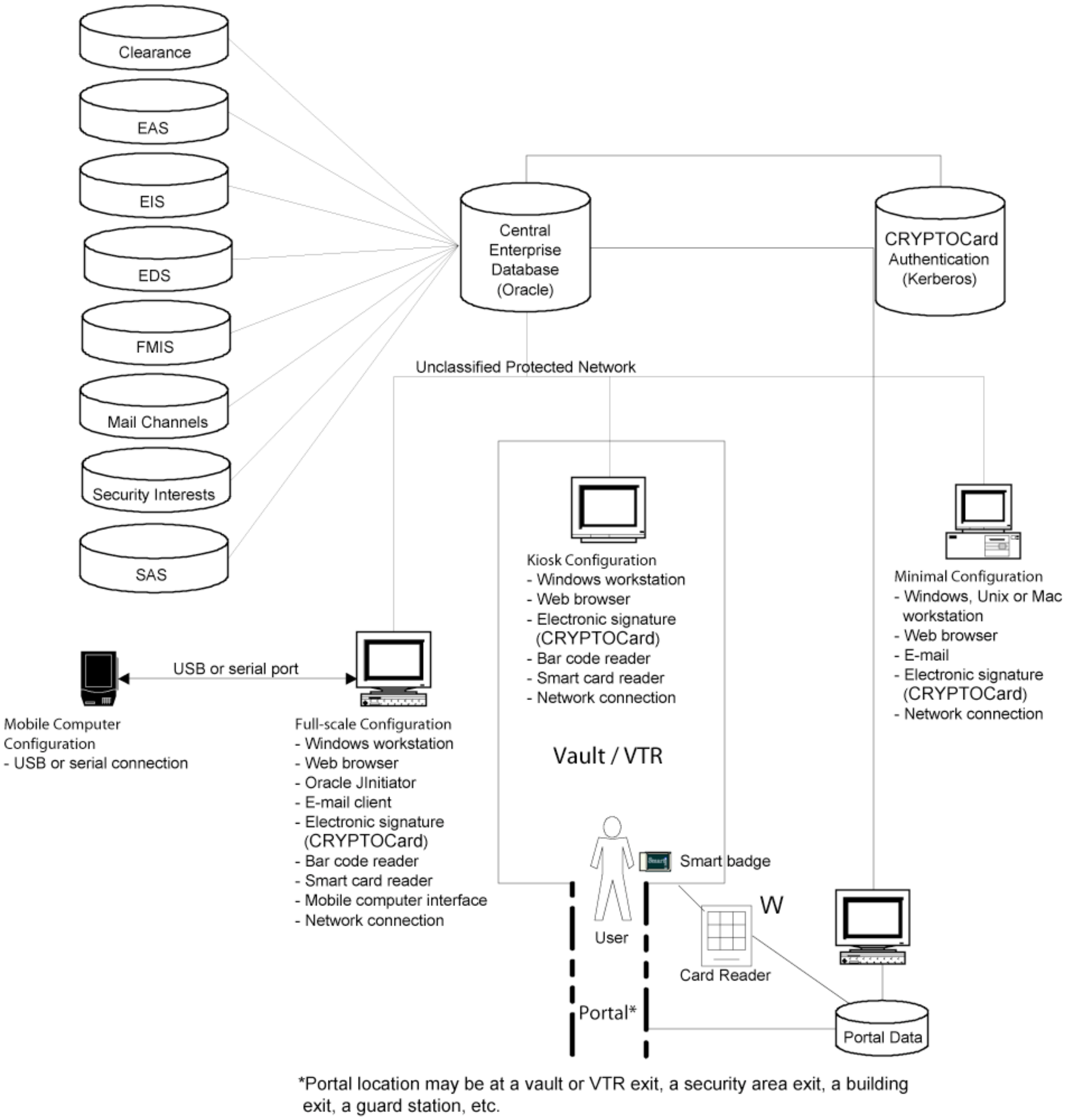


Figure 3. A smart-badge reader verifies the identity of the patron before he or she carries CREM through the portal and checks the CAS to see if the CREM is checked out.

Portable Identification Devices

Introduction

This section describes the engineered controls, features, functions, applications, advantages, and barriers to implementation of the portable identification devices selected for CAS.

Objectives

Portable identification devices, such as hand-held scanners, will be used to automate physical inventories. These devices will increase the efficiency of inventories by automatically and instantaneously reconciling discrepancies. This portable equipment will also facilitate seamless electronic transactions.

Functions

A physical inventory may be required for annual or special inventories, custodial changes, or to resolve system anomalies. Traditionally, these exercises required an individual to physically identify an item and validate the identification number of the item against a paper list. Through this process, a physical location to be inventoried was selected, all items were identified, and all anomalies were reported. This process will be automated.

In a physical inventory, someone must manually reconcile discrepancies. In the past, this required new transactions to correct the status of the item being inventoried. This process will also be automated.

Bulk transactions allow an “operation” to occur on one or more items. An operation might be to destroy, transfer, check in, check out, originate, reproduce, change class, receive, transmit, or verify an item or group of items. This once cumbersome process of tracking the movement of items will also be automated.

System Description

System Environment

Communication

Portable inventory devices will work with standalone workstations or may be used in conjunction with an existing network. The following list describes the process:

- Inventory items are downloaded to the Intermec 700c Color Mobile hand-held computer or similar device, which contains a built-in bar code scanner. This hand-held computer may be connected to a desktop computer through a docking station that includes universal serial bus (USB) or serial communication ports. Figure 4 illustrates the portable inventory system.

- A subset of the central database is stored within the hand-held computer (see Figure 5). That information may include, but is not limited to, bar code number, description, storage location, owner, and classification level of a piece of CREM.
- The hand-held computer may then be removed from the docking station and taken into the field for use. Operators must scan their badges to be identified as the person doing the inventory.
- The operator may then scan items. The hand-held computer verifies information for each item and records the date and time of scan as well as the person scanning the item. It records discrepancies for reconciliation at a later time. Other information, such as the number of items scanned versus the total number of items and a list of items scanned, is provided to facilitate the inventory process.
- The operator may upload information to the desktop computer at any time to view, print, or reconcile the inventory.
- The inventory is closed when all items have been scanned and reconciled. The hand-held computer docks with the workstation, and the information is uploaded to the central database.

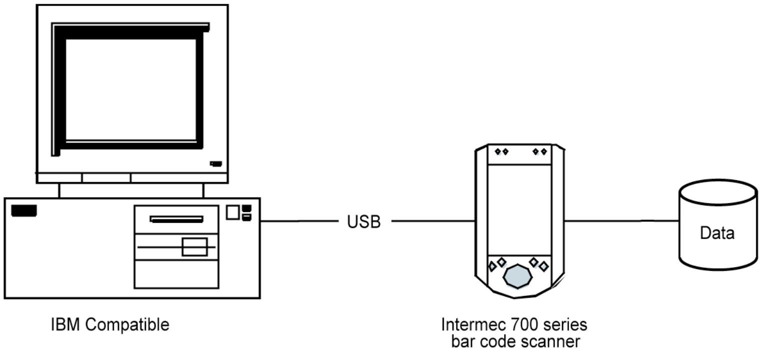
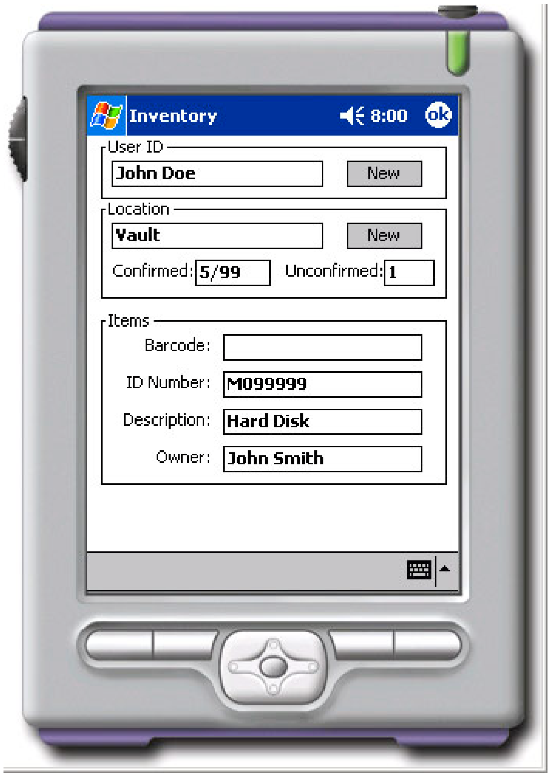


Figure 4. The hand-held computer is used to inventory CREM, and the data is uploaded to a personal computer (PC) workstation.



User ID: John Doe

Location: Vault

Confirmed: 5/99 Unconfirmed: 1

Items

Barcode:

ID Number: M099999

Description: Hard Disk

Owner: John Smith

Figure 5. The hand-held computer will display the information shown here.

The operator may also use the hand-held computer to record item transactions by scanning the item and selecting the type of transaction desired. The hand-held computer can then be placed in the docking station, and transactions can be uploaded directly to the central database.

Systems Classification

Currently, tracking systems reside on both the classified and unclassified networks. The decision to locate the tracking system on either one or both networks will affect the applicability and efficacy of CAS.

System Interface

Existing Applications

The MediaTracker Suite is the application now in use. This system contains information on all items in the inventory.

New Technologies

We are considering using smart cards for personnel identification and electronic signatures. We are also considering using portable RFID equipment for item identification.

Future Applications

CAS, as a Laboratory-wide system, will integrate existing portable inventory equipment and procedures.

System Requirements

Functional Requirements and Specifications

Bar-code readers must be easily transportable and allow user interaction. These devices must also be able to store information in a format that can be accessed from a workstation. See Appendix 1 for more information about hand-held computers.

Hardware Requirements

- Computer
    - 128 MB of random access memory (RAM)
    - 10-GB hard drive
- Intermec 700c Color Mobile Computer
    - 64 MB RAM
    - Laser scanner
    - Battery
    - Stylus
- Single Docking Station
    - RS-232 or USB connection
    - AC power adapter
- USB cable
- Scanner handle

The estimated cost for this system is $2156.

Software Requirements

- Computer
    - Windows2000 or later
    - ActiveSync 3.5 or later

Prototype Software and Hardware

Each of the systems' portable bar code scanners will interface with the existing MTM application.

Software Development

To allow the appropriate interface between MTM and the portable bar code scanners, we will add a new module and tables to MTM. We will develop an Intermec 700 application to enforce business rules for the inventory process. We will test software and document the results.

Client Platforms

Introduction

There will be three client platforms for CAS that will allow a user to access or interact with the application: a desktop workstation, a kiosk, or a mobile computer. The system will have a variety of users. The primary users will be the CMCs, but access must also be provided to S-Division, classified mail stop custodians, Business Operations Division (BUS)-4, vault users, and other authorized personnel who need to check out CREM, check the status of CREM, or query CREM information. There are therefore four types of client configurations:

1. A full-scale configuration
2. A minimal configuration
3. A kiosk configuration
4. A mobile computer configuration

Objectives

The full-scale client platform will be able to interface to a stationary bar-code reader, a smart-card reader, and a mobile computer. Users will be able to perform most transactions without these additional devices; however, there would be some loss of efficiency and accuracy as the user would have to manually enter the data using a keyboard and mouse. The operating system will be Windows2000 or later; we will determine later what versions of the operating system to support.

The minimal client platform will be a user's existing workstation. The application interface will be Web-based and will run under any of these operating systems: Windows, Macintosh, or Unix. The kiosk client platform will interface to a stationary bar-code reader and a smart-card reader. The mobile computer will interface to the full-scale client platform to upload data to and download data from the CAS database. The application software should require minimal resources to deploy and maintain. Either a Web-based or client-server (e.g., Citrix) approach should be used.

Functions

The full-scale client platform will deliver the application to CMCs, classified mail stop custodians, BUS-4, and S-Division. This client platform will provide access to the database, allow bar codes to be entered electronically with a bar code scanner, support electronic signatures using CRYPTOCards™ or smart cards, and interface to mobile computers for uploading and downloading data.

The minimal client platform will deliver limited database access to check out or check in CREM and query CREM data, and it will support electronic signatures using CRYPTOCards™.

The kiosk client platform will provide limited database access to check out and check in CREM, allow bar codes to be entered electronically using a stationary bar code scanner, and support electronic signatures using CRYPTOCards™ or smart cards. Kiosk computers may use touchscreen technology.

The mobile computer platform will allow for electronic scanning of bar codes and offline storage of CREM data to support the mobile inventory function. It will interface to a full-scale client platform to upload data to and download data from the enterprise database.

Description

System Environment

All of the client platforms will be connected to the unclassified protected network.

Client Platform Configurations

Full-Scale Configuration

- Windows workstation
- Web browser (Netscape or Internet Explorer)
- Oracle JInitiator (needed for Oracle Web forms)
- Electronic signature (CRYPTOCard)
- E-mail client (Eudora)
- Stationary bar-code reader
- Smart-card reader
- Mobile computer connection (USB, USB II, or serial connection)
- Unclassified protected network connection

The full-scale configuration will only run the Windows operating system (OS). This constraint stems from the need to support a number of hardware devices (bar-code readers and smart-card readers) that require OS-specific drivers. Also, the majority of the intended users for this configuration now use Windows workstations. The application interface will be Web-based.

Minimal Configuration

- Windows, Unix, or Macintosh workstation
- Web browser (Netscape or Internet Explorer)
- E-mail client (Eudora)
- Electronic signature (CRYPTOCard)
- Unclassified protected network connection

Bar-code readers will not be installed at the user workstations, but the application interface will provide a dropdown box with a list of bar codes. The application interface will be Web-based.

Kiosk Configuration

- Windows workstation
- Web browser (Netscape or Internet Explorer)
- Electronic signature (CRYPTOCard)
- Bar-code reader
- Smart-card reader
- Unclassified protected network connection

The application interface will be Web-based. When turned on, the kiosk will open the CAS application and will run only the CAS.

Mobile Computer Configuration

- Mobile computer
- USB, USB II, or serial connection

CREM Tags and Portals

Introduction

This section discusses operational, cost, and technical aspects of monitoring pedestrian portals as part of the CREM Control Project. Operational aspects of possible portal monitors determine which monitors best fit the needs of the CAS.

The portal monitors will be placed at strategic locations in pedestrian corridors where CREM are commonly transported. The primary and immediate purpose of the pedestrian portals will be to manage and track CREM assets. The portals would, therefore, provide engineered controls to confirm compliance with CREM archival and distribution-release procedures. Portals will identify when a distracted or forgetful CREM user has neglected to record a transaction or when a record of a transaction was not successfully completed by the distribution workstation.

If the hardware is improved, RF portal monitors could be used to keep CREM secure. Portal monitors will need to resist measures an individual might take to avoid detection by the system. If an RF portal monitor is to keep CREM secure, it must have reliable signal penetration and spatial uniformities, or it will not consistently detect CREM. The greater performance demands and more-detailed evaluation make the RF portal monitors less useful for CREM security than for innocent-infraction and warning applications.

Objectives

This section describes systems that monitor pedestrian portals. The monitor technologies considered here operate exclusively on RF communication principles. Conceivably, contact-based (i-wire) and line-of-sight (bar-code readers) technologies can identify items. The reasons for using only RF technologies are nonintrusive proximity detection, identification without a line of sight between item and reader, and the possibility of a high degree of spatial uniformity that reliably detects ID tags in the interrogation zone (the interrogation zone is the area within range of the RF portal monitor's gate antenna). RF systems also allow the user to carry though multiple items simultaneously, while technologies such as bar code scanners require the user to stop and survey each item individually.

Functions

The RFID system functions are determined by the features of specific components. The functions are furthermore determined by special capabilities and configurations. The components, capabilities, and configurations subsequently determine the system vulnerabilities.

Description

The RF systems we describe here operate in one of two modes. In both modes, an electronic tag or tape is attached to an item. Most systems are capable of resolving identification names or numbers assigned to individual tags when the tag enters the interrogation zone. Wireless systems capable of resolving individual items operate in RFID. Other systems detect an electromagnetic field disturbance when a sensitized tag or tape enters the zone of coverage. However, these systems are not capable of identifying individual items, as they only discern that a tag or tape has been introduced. These systems operate in an RF detection mode, also called electronic article surveillance, which is a generalization of the identification mode. Some RFID-capable systems can operate in detection mode at the user's option.

The RFID systems we considered for the CREM Control Project use a passive backscatter principle, in which the energy necessary to activate the tag circuitry and RF transmission is radiated to the tag. For a passive backscatter RFID system, the tags require no internal batteries, and highly compact tags (e.g., paper-thin labels) are possible. However, the method requires adequate RF coupling between the tag and reader, or the energy radiated to the tag will be insufficient for the tag to generate a detectable response, resulting in a misread. Adequate RF coupling is determined by numerous factors including relative orientation, hardware tuning, materials placed between tag and reader, or the material to which the tag is affixed.

System Component Requirements

A fully functional, standalone RFID system will require at least four hardware components. More hardware may be required for systems with unique features. The four requisite components are

- antenna,
- reader (transceiver),
- tag (backscatter circuits), and
- host computer.

The antenna enables RF transmission and reception between the reader and the tag. The antenna can be linearly or circularly polarized to afford different signal beam widths, signal gains, and degrees of RF coupling for specific tag orientations. In portal monitoring, gate antennae most often use circular polarization to reduce sensitivity to tag orientation. The reader is an electronics package that converts analog signals from the tag to a digital code that passes to the host computer. The reader also transmits modulated analog signals to the tag to energize the circuitry and to communicate data (if the tag is a read-write tag capable of data reception). The tag itself consists of an integrated circuit and a small antenna. The tag circuit includes a chip that executes perfunctory logical operations on the tag. Finally, a host computer runs the system management and data acquisition software.

System Capabilities

Performance evaluations for the CREM Control Project are primarily focused on four functional characteristics of RFID systems:

- Collision protocols
- Read ranges
- Penetrability
- Read-write many capabilities

Collision protocols determine how the RFID reader prioritizes data transmission and processing when multiple tags enter the interrogation zone simultaneously. Systems without a collision protocol (generally dubbed "anticollision capability") will lose data or may hang when receiving simultaneous responses from multiple tags. If data loss occurs, it generally results in a misread.

The distance at which data is reliably communicated between tag and antenna is the read range. Read range is significantly influenced by the shape and material of the item to which the tag is attached, the relative orientation of the tag antenna to the gate's reader antenna, and any materials introduced between the tag and the reader antenna (including the human body). Humidity and air temperature may also influence read range. Generally, maximum read ranges are observed for "open" or "free space" measurements, in which the antenna reads an isolated tag with no physical obstructions between tag and reader antenna. Free space measurements are generally the upper-bound of the system's read range performance.

Signal penetration is important in a portal because the tag is placed upon an object, and the geometry and packaging of the object and any neighbors is likely to obstruct the signal between tag and antenna on at least one side. Obstruction is more likely when tagged items are carried through the interrogation zone by humans, perhaps placed in bags, pouches, purses, cases, boxes, or some other package. Signal obstruction (or shielding) by metal is a significant challenge for RFID system performance in general.

Some tags possess local, user-configurable on-chip memory. When this memory can be configured, read, and reconfigured wirelessly by the reader, it has a so-called "read-write many" capability. A read-write many capability is useful in bridging partitioned information infrastructures or data/communication networks, as pertinent information can be written and stored on-tag and made available to remote systems with tag readers solely by introduction of the tag itself. For the CREM Control Project, read-write many capabilities give us more flexibility in designing the network than do write-once, read-many RFID systems.

System Configurations

A pilot evaluation for the CREM Control Project will introduce RF portal monitors at CREM storage vaults, vault-type rooms, access corridors, or boundaries of secure areas. The RF portal monitoring stations can be standardized so that they are modular, yet adaptable to architectural features and space constraints of the site. The portal monitors would be deployed in incrementally more complicated configurations (described below as Options I, II, and III) in as many as three phases. Option I will consist of networked portal stations but will have no identification confirmation display (i.e., intelligent warning system). Option II will consist of networked portal stations with intelligent warning systems, but no visible or audible alarms for unresolved item identifications. In Option III, alarms could include visible alerts (strobes and beacons), audible alarms (bells and sirens), digital video detection systems (the patron's picture is taken when an infraction is detected), and physical barriers (such as a locking turnstile). The types and locations of alarms would be use-specific, depending on the needs of the location. In the final phase, a stable configuration would integrate RFID host-controller software with the Enterprise information application. The first, second, and deployment options are discussed below.

Option I Portal Deployment

All locations will initially have portals using this option, which is part of Phase 2 of the system. In Option I, patrons will not be asked to confirm that they are in fact carrying the CREM that the system has identified as they passed through the portal. Option I will not distinguish between patrons entering or leaving a facility. The more basic functions of Option 1 have several advantages:

- Greater simplicity in use
- No delay to patrons going through portals
- Reduced software requirements
- Only need one-way (outgoing) data communications from RFID host controller to the network
- No need to download classified title information to the RFID host controller from other network nodes

Option II Portal Deployment

Figure 6 illustrates the major components and connections in Option II. Option II will be implemented in Phase 3 and could remain the preferred RFID configuration. If the location is a vault or vault-type room, the portal gate will be placed inside the room with the CREM. If the location is a corridor or security boundary, CREM will be somewhere within the perimeter on which the gate resides. In any circumstance, some type of CREM will be located outside the gate, albeit at a distance in many circumstances.

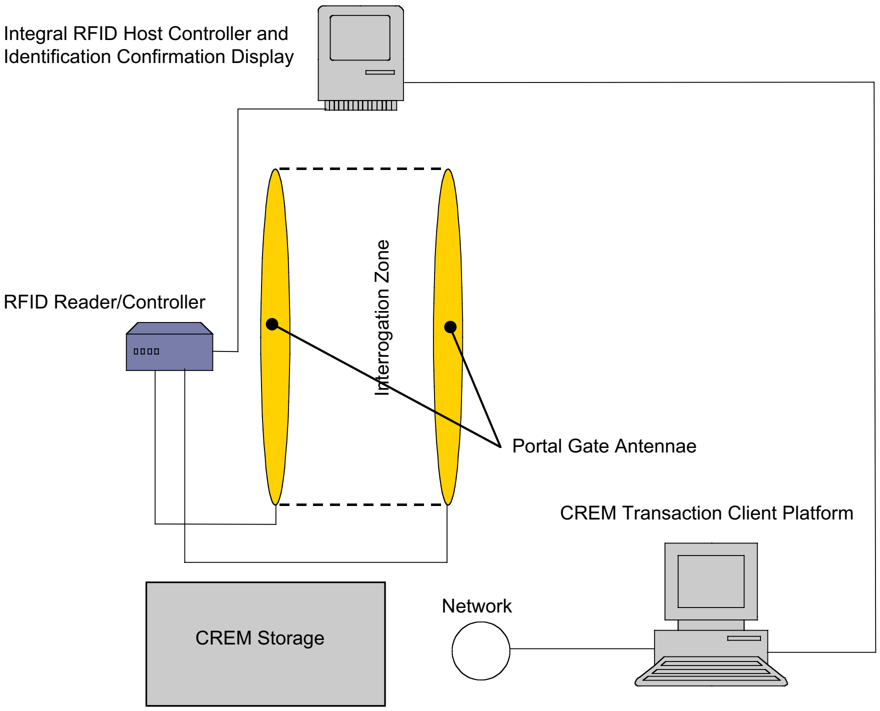

Integral RFID Host Controller and
Identification Confirmation Display
RFID Reader/Controller
Interrogation Zone
Portal Gate Antennae
CREM Transaction Client Platform
Network
CREM Storage

Figure 6. Schematic of an RFID portal monitoring station with an intelligent warning function (identification confirmation display), to be used in Option II of the CREM Control Project.

Wherever the patron retrieves or returns CREM, an electronic transaction will be logged at the appropriate CREM client station. Note that the client station is not a component of the RFID portal system. Patron and CREM information will be entered at the client station. When a retrieval transaction is completed, the patron will proceed through the RFID portal with the CREM. The gate antennae read the CREM tags as the patron walks through the gate, and it uploads the item IDs (and any configurable information) to the integral RFID host controller and transaction confirmation central processing unit (CPU). If any configurable information is to be written to the tag, it will be written in the interrogation zone immediately after the tag's information is uploaded. The patron will proceed through the portal to a touchscreen display that will list the patron's identification and the IDs of the items he or she carried through the portal. The patron may correct any discrepancies between the items read by the RFID system and the items he or she is actually carrying.

While waiting, the system will post a query message on the touchscreen display. The query will ask if an item is being returned and will display "yes" and "no" buttons. This query will serve two purposes. First, when a patron intends to proceed through the portal to return CREM to storage, he or she will first pause at the display, touch "yes," and provide a patron identification. Once the patron has entered his or her identification, the screen will display a countdown to let the patron know how much time he or she has to go through the portal. The system will read items that pass through the portal within the countdown period as returns and correlates the items with the patron identification just entered. The patron and returned CREM information collected at the portal should correlate to a subsequent transaction at one of the CREM client stations.

Second, allowing a patron to enter "no" to the query allows the patron to correct a catastrophic misread. It is possible that none of the tagged CREM that a patron carries through a portal will be read successfully. In this circumstance, the RFID portal monitor will not recognize that CREM have traversed the portal, and the system will maintain a "wait state." For catastrophic misreadings, the patron will need to touch "no" on the touchscreen and then enter his or her identification information. The integral controller/confirmation CPU will then search client stations for the most recent transaction associated with the patron identification and download a list of CREM most recently checked out. The patron will be asked to confirm that the downloaded list matches what he or she is actually carrying.

Option III Portal Deployment

In Option III, various audible and visual alarms and digital video surveillance systems triggered by infractions may be integrated with the portals. Option III would only be implemented in Phase 3. The specific types of alarms added will vary according to the needs of the location.

System Constraints

The RFID systems are susceptible to RF interference, dead zones, and tag shielding. Interference from external RF sources may constructively or destructively modify the frequency-modulated signals transmitted from the tags, or may even spuriously activate tags. The RFID systems are most susceptible to interference from RF frequencies near the nominal system frequency. We can reduce the potential for interference by distancing the RFID system from external RF sources or by placing the system in locations that provide a degree of shielding from external RF.

Dead zones can be observed within the larger RFID interrogation zone. In the dead zones, the reader will not read the tags because of severely diminished coupling between a tag and the reader antenna. We can reduce or eliminate the incidence and size of dead zones by properly placing and tuning the gate's reader antenna (assuming that the tag works efficiently).

Shielding the tag will also reduce the RF coupling between tag and reader antenna and may lead to reduced system response overall. Metal and magnetic materials are efficient tag shields. Materials with high water content also effectively attenuate RF signals in systems operating at frequencies above 800 MHz. Increasing the RF power level may compensate for the reduced performance caused by shielding materials.

Evaluation and Pilot Systems

After we test and evaluate RFID systems, we will choose systems to install at each pilot location. We will modify the pilot systems in phases, as described above in the *System Configuration*s section. Although we are still evaluating the systems, we can make some performance appraisals based on our preliminary results.

Introduction

To support feasibility studies for the CREM Control Project, we performed preliminary performance tests of three RFID portal monitor systems. The three systems are derivatives of the following manufacturer's RFID controller product lines (the internal designation for the system is provided in parentheses):

1. Omron Model V720 (System A)
2. Matrix Stationary Reader RDR-001 (System B)
3. Intermec Model 2100 UAP (System C)

We also evaluated a 3M Model 3802 Tattle-Tape Security System (System D) exclusively for the management of CDs and VHS videocassettes.

We wanted to determine the feasibility, the performance, and the reliability of each of these systems in detecting CREM being carried by patrons through a portal. We evaluated the ability of each system to detect

- CD-ROMs,
- 3.5 inch disks,
- removable hard drives,
- Jaz disks,
- Zip disks,
- memory sticks, and
- VHS videocassettes.

Detailed descriptions and features of each system are given in Appendix 2.

Hardware Costs

Retail Acquisition

In addition to differences in tag-reading performance, the systems' hardware costs also vary. We estimate that the installation and maintenance costs will be approximately equivalent, though no quantitative estimates are currently available.

Based on the retail price of the hardware needed for each system, System C is the best value, followed by System B, and System D, with System A being the most expensive. Tag costs per unit are substantially lower for System D, and progressively more expensive for Systems B, A, and C. Total costs for each system are given below; a breakdown of these costs is given in Appendix 2.

System A

System A Total for One Station (without tags): $11,350.00

System B

System B Total for One Station (without tags): $5,699.00

System C

System C Total for One Station (without tags): $5,195.00

System D

System D Total for One Station (without tapes): $10,000.00

CPU

Host Controller/Confirmation Computer (IBM SurePOS 500 Model 4840-521): $2,800.00

Volume Purchase Costs

We have talked to some vendors about price reductions for wholesale or volume acquisitions of the aforementioned RFID systems. Preliminary talks indicate that we may be able to reduce unit-cost between 15% and 35% from the retail price.

Evaluation Testing

We should note that the number of observations (i.e., samples) made at each location for each combination of medium and tag roughly indicates performance, though statistically insignificant. The following preliminary conclusions, therefore, should be taken quite cautiously, and are subject to revisions as more data is acquired in continuing evaluations.

Overall, System B is the superior performer for tracking the various types of media that we used in the evaluation. Systems A, B, and C are directly comparable. System D detects only infractions and provides no identification information for the detected items. The inability to identify individual items passing through the interrogation zone makes this system less useful for securing CREM.

We observed that System A had difficulty reading both tagged 3.5-inch floppy disks and tagged Zip disks at the low and peripheral (near-antenna) locations in the interrogation zone. System A also would not read tagged Jaz disks or tagged CD-ROMs (with the tag on CD-ROM and the CD-ROM in the jewel case) at any of the nine discrete measurement locations in the interrogation zone. System A also exhibited difficulties reading tagged removable hard drives (HD) at all vertical positions along the lateral center of the interrogation zone. Based on our prior experience with System A, it is possible that the gate antennae require additional tuning, and that our observations do not reflect the performance levels attainable with System A.

For the following media, we observed no misreadings with System B at any of the nine measurement locations in the interrogation zone when the tag was oriented to maximize radio-coupling to the antenna: 3.5-inch floppy disks, Zip disks, Jaz disks, and removable HD. We observed misreadings at both the vertically high and low positions, at all lateral stations, for tagged CD-ROMs. System B's performance degraded further for tagged CD-ROMs when the tag was oriented in each of the two remaining orthogonal directions (the so-called Y and Z orientations). We did not see significant reductions in performance in the orthogonal tag orientations for tagged 3.5 inch floppy disks, Jaz disks, Zip disks, or removable HD. Though not formally reported in Appendix 3, placing a half-inch foam spacer between the tag and CD-ROM improved System B's read performance at the high and low positions. We believe that a custom-fabricated and -calibrated backing substrate for the DDS-001 tags may enhance the RF coupling between tag and reader antenna for System B at the high and low positions, thereby increasing the read percentages. Without the use of spacers, successful read percentages were higher in all orientations and positions with the tag affixed directly to the CD-ROM in the jewel case than with the tag affixed directly to the inside of the jewel case and separated from the CD-ROM by the case label.

System C provided acceptable successful read percentages (greater than 75%) for smart labels on 3.5 inch floppy disks and Zip disks, except at mid-elevation in the X and Y orientations, and at all locations in the Z orientation. Both CD-ROMs (in jewel cases with Smart Labels affixed to the CDs) and Jaz disks were effectively unreadable in all orientations throughout the interrogation zone. The successful read percentages for the tagged removable HD were poor at mid-elevation in all orientations.

For the System C strip tag on VHS videocassettes, we observed successful read percentages between 90% and 100% at all locations with the tag oriented on the X axis to maximize radio-coupling to the antennae. In the orthogonal orientations, read performance generally remained acceptable, though performance diminished near the right antenna bank. When we revolved the cassette about one axis while we kept the tag in the Y orientation, we observed linear polarization of the tag antenna. Performance improved when we moved the strip tags to a vertical (rather than horizontal) orientation.

System D's detection of CD-ROMs and VHS videocassettes was neither sufficiently accurate nor precise to afford it an advantage over the RFID systems. System D was also unable to resolve and identify individual CREM within the interrogation zone. CREM detection at high and middle vertical positions within the interrogation zone (at all lateral positions and all principal tape orientations) was poor to unacceptable for both the CD-ROM and VHS tapes. System D also failed to detect individual CREM items in the interrogation zones and missed stacks of five identical items (e.g., a stack of five CD-ROMs). Moreover, the system could not reliably repeat the successful detections of some media at select locations. The quirky behavior led us to rate the system's precision as poor. Finally, we observed some type of radio-coupling and interference between the portal system and a nearby electric sliding door. If the door was closing while the portal security alarm was activated (i.e., when CREM were detected), the door would stick until the CREM was removed from the interrogation zone. Also, when tapes were near the gate (but not in the interrogation zone) immediately after the sliding doors opened, the alarm sounded. The spurious alarms were not triggered by tapes outside the interrogation zone when the sliding doors were closed.

Preliminary Evaluation Test Data

We evaluated the RFID Systems A and B on November 7, 2002, in the service area of Room 104, Building 27, in Technical Area (TA)-35. We evaluated the field disturbance system (System D) on November 13, 2002, at the main entrance to the Oppenheimer Research Library in TA-3, and evaluated RFID System C on November 26 and December 17, 2002, in Room 104, Building 27, in TA-35. We performed additional evaluations of System B on December 11, 2002, in Room 104, Building 27, in TA-35. Evaluation observations are detailed in Appendix 3.

For both systems and for all media, results depended on the tag orientation. Tag orientation on the X axis provides a coincident surface normal for both the tag and portal gate antennae (i.e., tag is oriented as if placed flat upon the face of the portal gate). This orientation theoretically provides the best radio-coupling between tag and antennae and the strongest read signal and most balanced read response. Orientation on the Y axis provides a tag surface normal that is orthogonal to those for the portal gate antennae, with the tag surface normal coincident with the direction of pedestrian movement through the portals (i.e., as if one were holding a shield or mirror). Orientation on the Z axis provides a vertical tag surface normal (i.e., as if holding a flat plate with one's palms extended). We introduced tagged media to the interrogation zones one item at a time, unless stated otherwise. Evaluation results are based on the percentage of successful readings at nine discrete locations within the interrogation zone of each system.

Pilots

Based on the results of our evaluation, we will choose one or two systems for the pilot study. The system's configuration and performance parameters in the pilot should be similar to system parameters in the evaluation.

Possible locations to pilot RFID portal systems are the Strategic Computing Complex (SCC), TA-55, TA-3 SM43, and the Applied Physics (X)-Division exclusion area. We are currently considering locations, location architecture, and system specifications for the pilot. The pilot selection and implementation effort is on schedule as of this writing.

Pilot Schedule

The CREM tagging and portals effort is grouped into five activities: prototype system procurements, pilot system selection and hardware specification, pilot system acceptance, pilot system installation, and pilot system operational testing. Tables 1, 2, 3, 4, and 5 detail the activities and schedule in each grouping.

Table 1: Prototype System Procurements Activities and Schedule

Activity	Scheduled Completion Date
Procure evaluation systems	10/31/2002
Select RFID laboratory space	10/02/2002
Assemble evaluation systems	11/27/2002
Write test and evaluation plan	01/20/2003
Evaluate RFID systems	01/20/2003
Document system evaluations	01/27/2003
Identify pilot sites	01/31/2003
Initiate security approvals	01/31/2003
Select software and user interface specifications	04/11/2003

Table 2: Pilot System Selection and Hardware Specification

Activity	Scheduled Completion Date
Complete system testing	04/18/2003
Document testing results	04/18/2003
Select systems for pilot installations	02/03/2003
Create specifications document	02/14/2003
Complete pilot system specification	02/14/2003
Order pilot installation components	02/21/2003
Monitor procurements	03/03/2003
Complete procurement of pilot hardware	03/10/2003
Write and debug interface software	04/07/2003
Upgrade integrated review software	04/07/2003

Table 3: Pilot System Acceptance

Activity	Scheduled Completion Date
Assemble pilot systems in laboratory	04/21/2003
Test software	04/21/2003
Develop operational procedure	04/21/2003
Obtain security approvals for procedure	04/21/2003
Pilot system acceptance completed	04/21/2003

Table 4: Pilot System Installation

Activity	Scheduled Completion Date
Install pilot systems at sites	05/09/2003
Provide system training for users	05/16/2003
Adjust/tune pilot systems for specific use	05/16/2003
Complete pilot system installation	05/16/2003

Table 5: Pilot System Operational Testing

Activity	Scheduled Completion Date
Operational testing by users	07/24/2003
Technical support	07/02/2003
Upgrade procedures	07/02/2003
Propose follow-on tasks	05/13/2003
Document results	08/14/2003
Upgrade procedures and specifications (includes Phase II deployment decision)	08/28/2003
Complete pilot system operational testing	08/28/2003

Smart Cards and Digital Signatures

Introduction

When used as part of an infrastructure that incorporates public-key cryptography, smart cards provide tamper-resistant storage for digital credentials, private cryptographic keys, and other personal or institutional information. A smart card is the only alternative that can combine several applications and technologies securely on one card, providing both convenience and security. In the belief that CREM management can be made more secure, easier and less error-prone with the introduction of smart cards, we are piloting the use of this technology with the existing MediaTracker product.

For the CREM pilot, we want two security applications on a single card: strong authentication of personnel through a digital signature and an encryption capability. Both features will enhance CREM management via the MediaTracker. Strong authentication is created when a MediaTracker user or custodian must have the card and know the card's personal identification number (PIN) in order to gain access to the MediaTracker system. The MediaTracker is used to perform formal transactions with CREM; these transactions often require a paper form to be prepared with signatures of the custodian and the user. The smart card, combined with the LANL Entrust™ public key infrastructure (Entrust PKI), allows us to sign these transactions digitally, creating a permanent record of who signed the transaction, when it was signed, and what was signed. The signature and transaction record cannot be modified subsequently without detection, and the signed transactions can be transmitted electronically to other parts of the LANL organization (such as security or General Counsel).

Objectives

The current pilot project is integrating smart card use into the MediaTracker product. The card will be used as an identification for authenticating a user to the MediaTracker, a cryptographic token for creating digitally signed MediaTracker transactions, and possibly a portable inventory card. MediaTracker is a PC-based application that tracks and manages CREM and is widely used at the Laboratory. Because it is PC-based, the MediaTracker can take advantage of the built-in Windows2000 smart card features. A natural extension is to allow users to sign on to MediaTracker with a smart card rather than by scanning or swiping a bar code from the LANL badge. When a user signs on with a smart card, the card will provide a digital signature for each MediaTracker transaction, replacing the current paper-based process.

Because the card has the same form as the current DOE badge, it can be used with the existing LANL badge (see Figure 7) without changing any badge issuance, deployment, or maintenance processes. Indeed, the current CRYPTOCard functionality can now be performed on a smart card (with access to a keypad to enter the PIN), and the card can securely contain all the information found on the badge as well as important information such as clearance, training qualification, and expiration dates; property IDs allocated to the card holder; and extended personal information, such as emergency medical information. Envision combining the existing LANL badge with additional secured personal data and the capabilities of the smart card, merging the CRYPTOCard functionality into a single LANL smart-card badge, or smart badge.

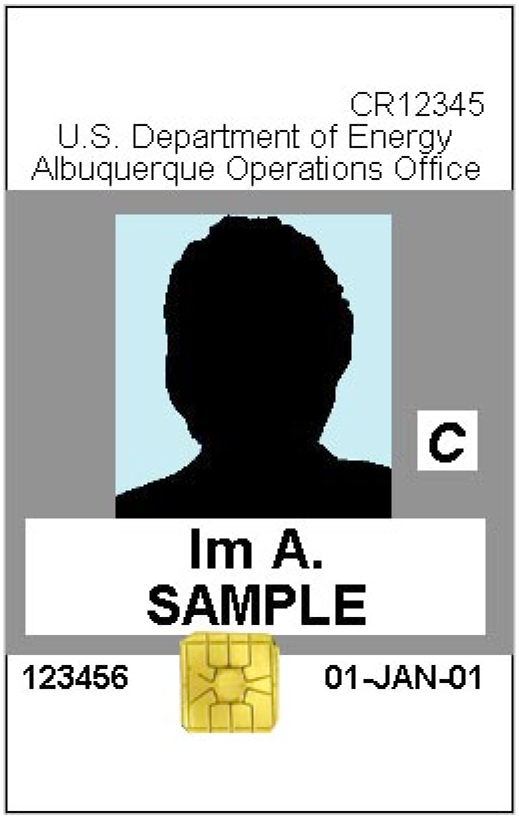


Figure 7. A typical LANL badge with an added computer chip, making the badge a smart badge.

Functions

Operating Environment

The LANL MediaTracker environment consists of standalone or networked PCs, with input devices including touchscreens, bar-code readers, and PC-based servers, all running the Windows2000 OS and using a typical (optional) Ethernet network for communication (see Figure 8). Paper reports and receipts are printed out for signatures for specific transactions. Adding the smart card to this environment requires obtaining compatible smart-card readers, the cards, and supporting client software. Windows2000 features native support for smart-card readers. The MediaTracker smart card will contain user identification similar to what is carried on the existing LANL badge bar code and magnetic stripe, plus a digital credential supplied by the existing Entrust PKI system in use at LANL.

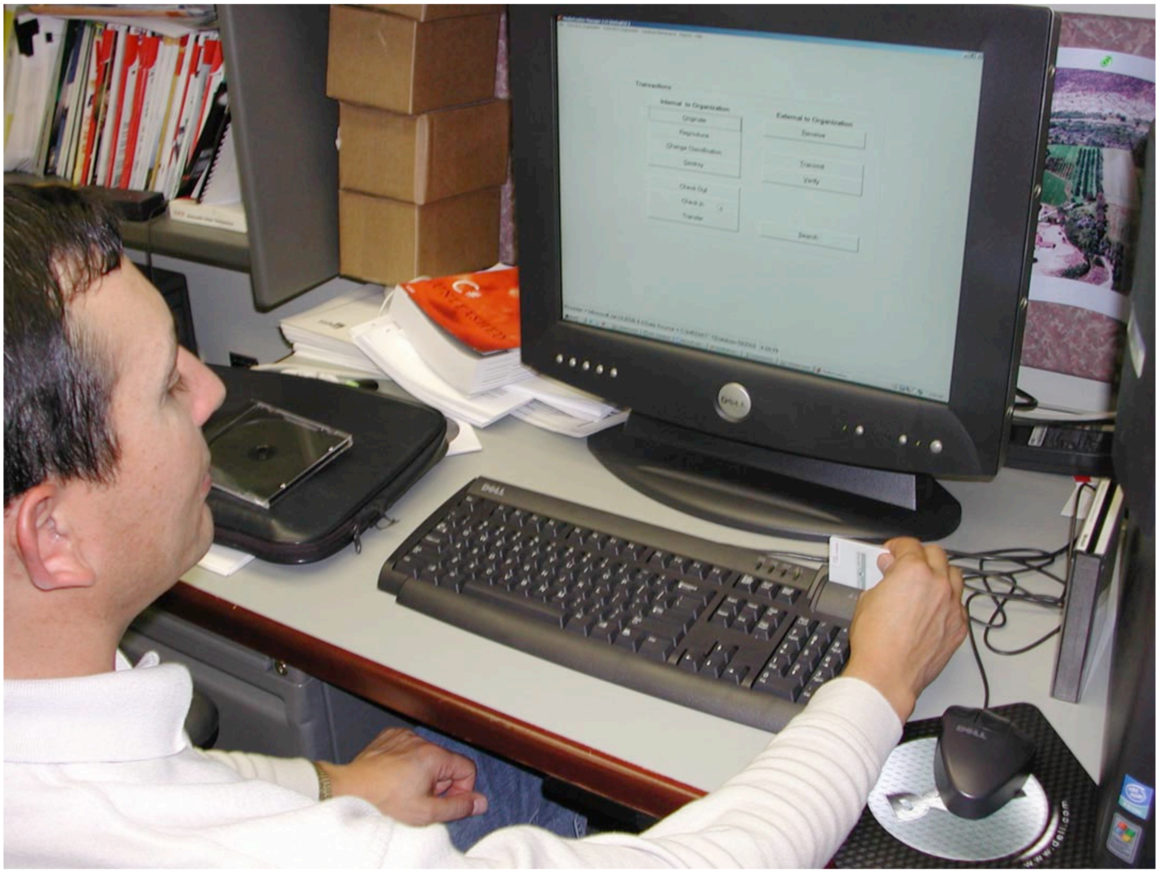


Figure 8. A user will run his smart card, or smart badge, through a reader to access the CAS.

The project to add smart card use to the MediaTracker system is being performed by a single engineer under the guidance of the principal engineers of the MediaTracker product. We have already successfully developed a preliminary prototype showing authentication and digital signature creation and retention.

Decision Process

The MediaTracker team is seeking to make daily management of CREM easier, less error-prone, and quicker for all parties involved. Smart-card technology offers a solution that creates a strong authenticated user, digital signature capacity for that user and rapid transaction processing, all without paper. A Windows2000 MediaTracker product is in place and deployed throughout the Laboratory, so the MediaTracker team sought an incremental way to add the smart-card technology to the existing system. We sought low-cost, proven technology known to work with the existing environment (Entrust PKI, Windows2000). In addition, we had a requirement that the smart-card vendor provide middleware support that was easy to integrate into the existing MediaTracker software. After some initial experimentation with smart-card vendors, one that fulfilled the requirements was chosen for the initial pilot project.

Anticipating widespread smart-card usage at LANL in the future, we require that

- the card provide a substantial amount of data for future application expansion,
- the card fulfill the minimal standards for cryptographic security established by the U.S. National Institute of Standards and Technology, FIPS 140-1 Level 2,
- the card vendor be a U.S. government-approved successful smart-card token and software vendor,
- the card work with our existing PKI system at LANL, and the PKI system must be approved for DOE unclassified use (i.e. Entrust PKI),
- the card provide standard programming interface to the card data and cryptographic features (PKCS #11 is one standard, Java Card provides another such standard),
- the card and supporting software be priced in line with industry competitors,
- the vendor provide a migration path to contact-less card usage,
- the vendor offers a biometric identification capability for future expansion (fingerprint, iris, voice, odor and hand geometry are examples of biometric identifiers),
- the card contain a magnetic strip, in anticipation that the current LANL badge will someday incorporate a smart card chip, and
- for this pilot only, the software programming of the card be easily added to the existing MediaTracker products, written in Visual Basic and C++.

It turns out that in mid-2002 several vendors could fulfill these requirements. We looked at ACS, Schlumberger, and Datakey. Our decision was based on the ease of integrating their card and software and our preexisting LANL Entrust PKI with the existing MediaTracker software. Datakey is a smaller, yet credible, vendor of these products. By far, the dominant card vendor is now Schlumberger with their Java-based smart card systems, because of widespread use by the Department of Defense. The current pilot did not need to expend the additional effort to add Java language to our existing software products, so we chose Datakey.

Business Issues

Using smart cards with MediaTracker will reduce errors and paperwork for routine daily transactions. It will also create a strong history of the transactions via the digital signature and increase security by requiring a smart-card holder to authenticate his or her identity to the smart card itself as well as to the MediaTracker. To use the MediaTracker and sign transactions, the user must have the card and know the card PIN. Current practice requires working the transaction through the MediaTracker software, printing the receipt, and physically signing the document. A digitally signed transaction takes approximately two seconds, a significant savings in time and effort over the current system.

If we use smart cards for general employee access at LANL, it may be useful to note that a smart card has same form as the existing LANL badge, and adding the chip to the badge will provide a more secure identification card. Successive smart-card applications can piggyback on the existing badge system at the Laboratory. The smart card offers increased protection against theft and forgery because it is extremely difficult to copy the smart-card content. A stolen smart badge cannot be used if the thief does not have the badgeholder’s PIN.

Application Description

The MediaTracker smart-card pilot uses the cryptographic capability of the smart card to authenticate users and digitally sign MediaTracker transactions, thus creating records that cannot be repudiated of these formal transactions. The MediaTracker pilot works with Windows2000/XP and the Entrust PKI solution. The card chosen for this pilot is Datakey’s 300 PKI smart card with a 32K chip and the Datakey Cryptographic Interface Provider (CIP) middleware. This software is to be installed on each MediaTracker-equipped PC, along with a standard personal computer/smart card (PC/SC)-compliant smart-card reader.

The existing MediaTracker software has been enhanced to detect the presence of a smart card in a local reader, access the digital credentials on the card, and use Laboratory-issued Entrust PKI digital certificates and software to provide digital signature services.

For this pilot, each participant will be issued an Entrust PKI digital identification and profile and a smart card that has been personalized by the CREM MediaTracker team.

Deploying the software and hardware requires that a reader, the Datakey middleware, the Entrust PKI 6.x client software, and the pilot version of MediaTracker be installed on each MediaTracker-equipped PC. In the MediaTracker installation, the card holder must be an authorized user of MediaTracker.

Implementation Overview

Pilot Management and Support

The MediaTracker smart-card team provides software and hardware installation, training on the use of the smart card and the reader, and training on using the smart card to log in to MediaTracker and digitally sign a transaction. The MediaTracker smart-card team can also provide training in the use of the Entrust PKI system as part of the digital signature MediaTracker training. For the initial pilot, cards will be issued on an individual basis because of the small number of people involved. Damaged, compromised, and lost cards will need to be replaced as needed. At the conclusion of the pilot, all smart cards will be returned to the MediaTracker team for erasure and reuse in subsequent projects.

Cost Analysis

Hardware and Software Costs

A typical USB or serial card reader is available for less than $50, while Personal Computer Memory Card International Association (PCMCIA) readers are slightly more. Datakey supplies the 330 PKI smart card for test purposes for approximately $20 each. In bulk these cards cost approximately $8 each, and that price is dropping rapidly. The

Datakey USB or serial card reader, plus license for the CIP middleware, is less than $90. PCMCIA readers are slightly more.

Entrust PKI is already used at the Laboratory. Cost for an individual license is $30, and one license per PC is required.

For each PC, the software and hardware cost will be as follows:

$ 90 for a generic PC/SC-compliant card reader plus Datakey middleware and license
$ 30 for Entrust PKI client software and license
——
$120

Each card will be $20 at most, and for the pilot we will have 30 cards available for testing by approximately 15 users. If the pilot involves 30 cards for 15 users, and 15 PC MediaTracker installations, total cost will be as follows:

$600 = 30 cards × $20 each
$1350 = 15 installations × $90 each
———
$1950

Please note these figures are not final and are only an estimate.

Development Costs

Development costs include the time taken to produce the working prototype; support the deployment, operation, and termination of the pilot effort; and compile the lessons learned from the project.

Deployment Costs

Deployment costs include the costs for

- time taken to install the hardware and software,
- testing of the installations,
- training users on the use of the readers and the cards,
- training users on the new login and digital signature features of the MediaTracker, and
- personalizing and issuing a functioning smart card for each user (personalization involves placing an Entrust PKI ID on the card and storing MediaTracker-specific information the card).

Maintenance Costs

Maintenance costs will include technical support, ongoing training, reissuing lost or damaged cards, terminating the pilot project, and collecting the issued cards and erasing the card content.

Enterprise Database

Introduction

This section describes the enterprise database for the CAS. The enterprise database is the central repository for all CREM records and audit data.

Currently at LANL, there are a number of different systems used to account for CREM, from paper logs to electronic systems specifically designed to track CREM (e.g., MTM and X-Division's CREM Accountability Tracking System). The introduction of electronic systems has greatly improved the Laboratory's ability to track CREM. These systems are typically deployed at the group or division level.

The next logical step is to use the capabilities of these existing systems in a Laboratory-wide enterprise system. An enterprise system will provide a single, centralized application that can be used by organizations throughout the Laboratory to access real-time CREM information from a central database.

Objectives

The enterprise system to track and account for CREM will be built around a central database management system, which includes an enterprise database.

The enterprise database will

- contain all required CREM data (e.g., bar code number, title, classification, category, caveats, originator name, owner name) for every piece of CREM in the database,
- contain all audit data for the system (the system will record every change to the data including the date, time, person making the change, and application used),
- interface with Laboratory-wide databases for data lookup and validation (the Laboratory-wide databases are the Employee Information System (EIS), Signature Authority System (SAS), Employee Development System (EDS), and Mail Channels,
- interface with the Kerberos system for authentication and electronic signatures via current CRYPTOCard technology,
- enable real-time reporting on all CREM in the database,
- eliminate the need for separate, customized databases, and
- interface with new technologies as they are implemented (smart cards and RF portal monitors).

Functions

The enterprise database will allow the user to create, read, and update all CREM records. Deleting a record will be allowed only in special circumstances [e.g., per an Office of

Security Inquiries (OSI) directive]. Instead, records will be marked “deleted” when they are no longer needed by the application but will remain in the database. These records will not be visible in the application. User authorities will determine the access rights to each database record.

The enterprise database will use lookup tables where feasible to ensure consistency of data and reduce data entry errors. Lookup tables will have real-time links to enterprise databases (e.g., EIS, SAS).

The enterprise database will store electronic signatures that are generated using the current LANL CRYPTOCard technology. It will also be able to store electronic signatures that are generated using smart-card technology.

The enterprise database will interface with the portal hardware and software. When a piece of CREM with an electronic tag moves through a portal, it will be recorded in the enterprise database. The enterprise database interface will also allow the portal to determine if the CREM has been checked out as the person transporting it moves through the portal.

Description

System Environment

The enterprise database will be hosted on servers managed by IM-3 and supported by the LANL enterprise infrastructure. The servers will be connected to the unclassified protected network. This infrastructure includes database administrator (DBA) support, system administration, backups, production control, and twenty-four-hour-a-day, seven-day-a-week on-call support from IM-3.

The information management standard for relational databases is Oracle. This database will use Oracle 8.17 or higher. Existing electronic CREM data will be converted to this standard and then uploaded to the central database. CREM data that is tracked in paper logs will be manually entered into the new system.

The database will use Oracle’s journaling capability. This feature automatically generates audit data for every database transaction whether it is performed through the application interface or directly on the database by a DBA.

Analysis of Networking Options

Introduction

We analyzed networking options for an enterprise system to track CREM. The system will reside on the unclassified protected network. Also, the data will not require an authorized derivative classifier (ADC) review before the record is stored in the central database. The information used to reach these decisions is documented in the following sections.

LANL has three computing environments: the open (green) network, the unclassified protected (yellow) network, and the secure integrated computing (red) network. Both the yellow network and the red network are suitable network environments for this system.

One option that we considered was to host the system on both the yellow and the red networks, i.e., the application, Web, and database servers would reside on either the yellow or red network (one would be selected), but the client machines could reside on both the yellow and the red networks. Data would be exchanged between the two networks as needed.

We decided that this arrangement was unworkable for an enterprise system because there is no real-time interface between the two networks. The only interface available is the Mercury system (described later in this section). The Mercury system does not provide the automated, real-time interface that would be needed for an enterprise system spanning both networks.

Objectives

To track CREM, the enterprise system should ideally reside in a computing environment that is

- appropriate for the data stored in the system,
- network-accessible from all of the sites where it will be used,
- integrated with LANL's enterprise systems,
- supported by LANL's enterprise infrastructure,
- able to support real-time transactions, and
- less reliant on administrative controls.

At LANL there is no one computing environment that meets all of these objectives. The pros and cons of each environment are presented in Table 6.

Table 6: Considerations for Choosing the Yellow or Red Network

	Pros	Cons
Classified	• Classified data is allowed • ADC reviews are not needed to convert existing CREM data	• Network connections may not be available • There is no real-time integration with LANL enterprise systems • There may be additional costs to support a Mercury interface • Developers need Q clearances and a classified computing work area • Portal stations would need to be connected to the red network • Users need CRYPTOCards™ to access the red network • E-mail on the red network is available but not widely used
Unclassified	• Real-time integration with LANL enterprise systems is possible • Network connections are more widely available • System can easily integrate BUS-4 mail services • Enterprise support exists • Most commonly used types of E-mail are available	• Classified data may be introduced to an unclassified system • ADC must review data to avoid introducing classified data • System downtime would be needed to remove classified data • Existing CREM data may require ADC review before data conversion • Some groups may not want to install an unclassified system in a classified area

Options

There are options in each computing environment to mitigate some of the disadvantages.

Classified Environment

The two biggest challenges in this environment are network availability and interfaces with the enterprise systems that reside on the unclassified network.

The issue of network availability is being addressed by a Laboratory-wide project to extend the classified network to a number of new locations; however, it is estimated that it will be several years before this network infrastructure is in place.

An interface to LANL's enterprise systems is possible, but a real-time interface is not currently possible. Data can be exchanged between the red and yellow networks using the

Mercury system (see http://mercury.lanl.gov/). However, moving data from the yellow to the red network requires less work.

To move data from the yellow to the red network, we can use a somewhat automated process through the Mercury system. Once this process is set up and tested, it should run "automatically" (moving the data is a manual step that is handled by the Mercury staff).

Given this interface through Mercury, it is possible to implement a system that requires data to be moved from the yellow to the red network. However, the overhead of maintaining and supporting this process would be significant, and the system would not be real-time. Recently the Mercury system was not available for several days; relying on this interface is a significant risk.

Data will be moved manually from the red to the yellow network. This requires both an ADC review and a review by an additional person. Once the data move is approved by the reviewers, the Mercury system is used to manually upload the data to the yellow network.

Because of the time required for the reviews and the manual process, it is not practical to implement a system that requires data to be moved from the red to the yellow network at frequent intervals.

Unclassified Environment

If we place the database in the unclassified environment there is a risk of introducing classified data into the system. There will also be the complications of ADC reviews and potential system downtime. Some existing CREM systems are operated as classified databases to allow the classified descriptions needed to retrieve information.

The software interface can be designed to give users access only to unclassified data. However, the "unclassified title" and "notes" fields are free-form text fields where classified data could inadvertently be entered.

One solution is to require an ADC to review a CREM record before it is moved into the central database on the unclassified network. In this solution, two databases are implemented: a staging database where all CREM records are first entered and an enterprise CREM database where the reviewed records are stored (see Figure 9). An ADC reviews a new record in the staging database and, once he or she determines there is no classified data in the record, the system moves the record to the enterprise database. When the record is moved into the enterprise database, the title field is set to read-only to prevent users from entering classified data.

The disadvantages to this solution are that it requires additional ADC resources and also delays moving the CREM data into the enterprise database. The advantage is that if classified data is introduced into the staging database only that database is affected; the enterprise database will remain available while the staging database is "scrubbed."

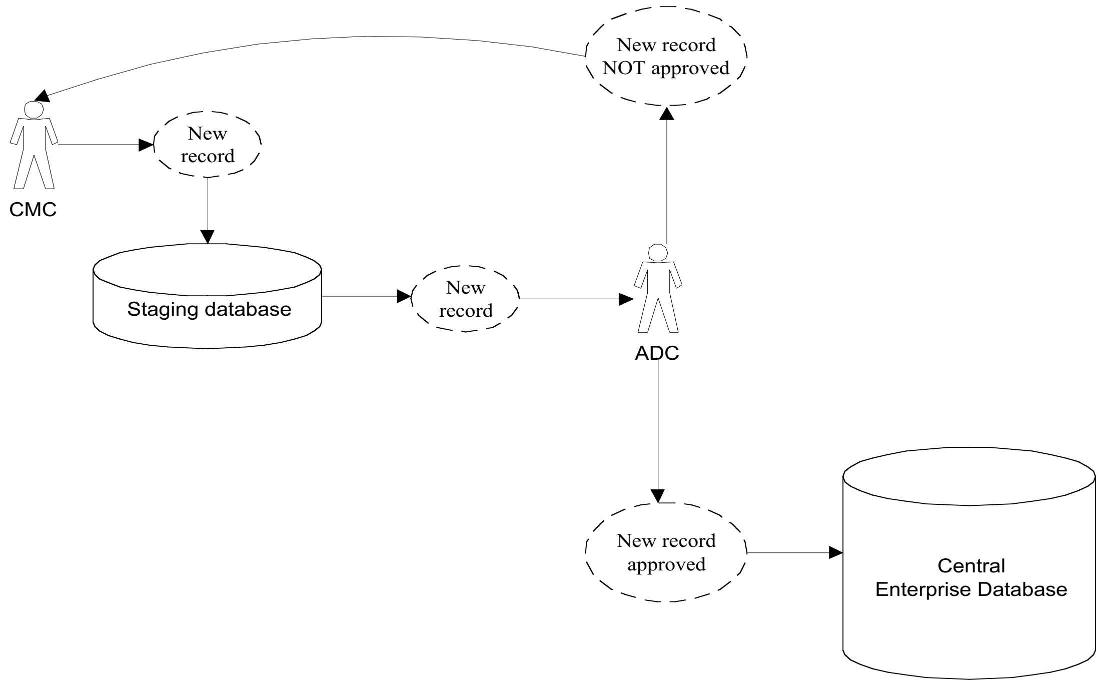


Figure 9. Moving information from the classified to the unclassified network will require an ADC review.

Schedule and Costs

Schedule

Vendor Selection and Approval

We have several tasks remaining:

- Obtain final approval of the customer requirements document
- Identify vendors
- Develop an RFP for an enterprise CREM accountability system, Phase 1
- Distribute RFP to identified vendors
- Evaluate RFP vendor responses
- Determine if the system will be developed by LANL or by an outside vendor with LANL assistance
- Obtain chief information officer and policy board approval of selected system

We will perform these tasks from January 6, 2003 to April 1, 2003. We estimate the cost will be $100,000.

CAS—Phase 1

This section describes the standard development process at LANL for creating enterprise applications. These tasks will continue in parallel with the vendor selection process and the pilots for engineered controls.

The tasks do not necessarily occur in order but all tasks must be completed to develop and deploy the application. Some of the tasks have been completed, and others are in progress (see Tables 7 and 8). The schedule and resources are given for tasks not yet completed.

The schedule assumes funding for and availability of four Information Management Division (IM)-8 full-time employees (FTEs) through the end of the project. It also assumes the funding for and availability of personnel from other groups involved [i.e., the users, IM-2, IM-3, Analysis and Assessment Division (S-Division), Nonproliferation and International Security Division (NIS)-7] in this effort.

Table 7: Completed Tasks

	Task	**Schedule**
1.	*Process Flows:* Document current and proposed business processes.	Completed FY03 Q1
2.	*Functional Diagram:* Translate process flows into functional hierarchy diagram that is used to determine menu options, entry screens, reports, etc. Automated functions are identified.	Completed FY03 Q1

From this point on, the technical process of developing the system becomes iterative.

Table 8: Remaining Tasks

	Task	**Schedule**	**Resources**
3.	*Entity Relationship Diagram:* Define and diagram entities and attributes for the application including interfaces to other enterprise systems.	FY03 Q1, Q2 80% complete	IM-8
4.	*Functional Diagram Update:* Assign entities and attributes to automated functions. Each entity attached to an identified automated function is assigned its CRUD [Create (Insert), Retrieve (Select), Update and Delete] matrix.	FY03 Q1, Q2 40% complete	IM-8
5.	*Development Database Setup:* Work with IM-3 DBAs to create database instance and the necessary accounts and authorities	FY03 Q1, Q2 80% complete	IM-8 IM-3
6.	*Quality Checks:* Run repository reports in Oracle Designer to cross-reference all objects documented thus far and determine if there are any discrepancies. Modify as needed.	FY03 Q2	IM-8

7.	*Database Design Reviews:* Request and complete a formal design review. Following the review, the database design is modified as needed.	FY03 Q2	IM-8 IM-3
8.	*Mockup Forms and Reports:* Create paper and pencil images of forms and reports. Review with users and modify as needed. Provide to developers to use as models during development.	FY03 Q2	IM-8 Customer Users
9.	*Database Design Transformation:* Generate the server model to be used in developing the database tables.	FY03 Q1, Q2 50% complete	IM-8
10.	*Application Design Transformer:* Generate the modules needed for deploying forms and reports.	FY03 Q2	IM-8
11.	*Physical Data Model:* Generate tables and indexes.	FY03 Q2	IM-8
12.	*Review Application:* Customer reviews application. This is an ongoing process. At each review the customer approves the work done to date before additional work is done.	FY03 Q2 - Implementation	IM-8 Customer
13.	*Testing Plans:* Develop testing plans for usability, unit, integration, stress, and acceptance tests.	FY03 Q2, Q3	IM-8 Customer
14.	*Client Platform:* Acquire and configure the client software and hardware needed to test all client platforms.	FY03 Q3	IM-8
15.	*Develop Application:* Develop forms and reports based on the mock forms and reports. Write code to implement business rules and generate HTML forms.	FY03 Q3, Q4	IM-8
16.	*Infrastructure Review:* Meet with IM-3 to establish infrastructure and deployment requirements	FY03 Q3	IM-8 IM-3
17.	*Consultants:* Meet with Enterprise Information Application consultants (IM-2) and customer to discuss how they will provide training for the application. Provide documentation as needed.	FY03 Q4	IM-8 IM-2 Customer
18.	*Perform Usability Testing:* Determine whether the application can be used by the intended users without formal training. This can begin early and be done several times throughout the development process	FY03 Q2 - Implementation	IM-8 Customer Users
19.	*Perform Unit Testing:* Determine that all requirements have been developed and that the application is performing as specified in the requirements documentation.	FY03 Q3 - Implementation	IM-8
20.	*Perform Acceptance Testing:* Customers test to see that the requirements have been met.	FY03 Q3 - Implementation	Customer Users
21.	*Data Conversion:* Convert existing CREM data and upload into enterprise database. Run quality checks on data.	FY03 Q3 - Implementation	IM-8 Users

22.	*Perform Integration (alpha) Testing:* Determine if application is working within other applications and whether it impacts or is impacted by other applications.	FY04 Q1	IM-8
23.	*Perform Stress (beta) Testing:* Determine if the application is configured correctly so the response times are appropriate.	FY04 Q1	IM-8
24.	*Training Plan:* Work with IM-2 and the customer to develop a training plan.	FY04 Q1	IM-8 IM-2
25.	*Deployment Plan:* Develop a deployment plan with all groups involved. The plan defines all the steps, schedule, and people involved in deploying the application. The deployment plan will also address obtaining and configuring client hardware and user training.	FY03, Q4 – FY04 Q1	IM-8 IM-2 IM-3 CCN-4 Customer Users
26.	*Develop Security Plan:* Work with Operational Computer Security representatives to develop the required security plan. Submit for approval.	FY04 Q1	IM-8 S-Division
27.	*User Training:* IM-2 begins user-training classes.	FY04 Q2	IM-2 Users
28.	*Implementation Plan:* Working with the customer, the team develops an implementation plan for putting the application into production. Determine whether there will be a limited pilot or a general rollout of the application. The plan includes the resources needed, schedule, advertising (if needed), E-mail list, and necessary signatures.	FY04 Q1	IM-8 Customer Users
29.	*Migration:* Use IM-8 migration tool and deployment plan to move application into production.	FY04 Q2	IM-8
30.	*Implement:* Get signature approvals to move system into production. Final testing in production environment. Make application available.	FY04 Q2	IM-8 Customer Users
31.	*Transitional Support:* Support provided by developers during the first month of implementation to answer questions and fix problems.	FY04 Q2	IM-8
32.	*Ongoing Application Support:* Provides any maintenance and enhancements requested through proper channels and approved by the Change Control Management Board.	FY04 Q3 and is ongoing	IM-8

Costs

The total cost of the project cannot be estimated accurately until the system requirements document is approved. A rough *estimate* of the Phase 1 cost is approximately $2.3 million, based on the following assumptions:

1. We estimate that Phase 1 of the project will require one and a half years to complete with three IM-8 technical staff members (TSMs) FTEs and one IM-8 specialist staff member (SSM) FTE. The burdened recharge rate for an IM-8 TSM is approximately $241,000 per year. The burdened recharge rate for an IM-8 SSM is approximately $168,000 per year. Therefore, the cost for the main application development team is approximately $1.3 million.
2. We assume another $650,000 for other personnel involved in the planning, development, deployment, and testing of Phase 1 of the system [i.e., S-Division, IM-2, IM-3, Computing, Communications, and Networking Division (CCN)-5, NIS-7, and users from X-Division, Materials Science and Technology Division, Nuclear Materials Technology Division, NIS, etc.].
3. We assume hardware, network, and system configuration costs of $2500 per full-configuration machine and $1000 per kiosk machine. Assuming the need for 100 full-configuration machines and 50 kiosk machines, the total hardware cost is estimated at $300,000.
4. System hardware and software costs (i.e., database, Web and application servers, and Oracle software) will most likely be covered by a monthly charge from IM-3. We do not anticipate buying server hardware. If that assumption changes there will be additional costs for server hardware. Oracle software costs should be covered by the Laboratory-wide Oracle license.
5. These costs do *not* include ongoing fees that IM-Division charges to host, maintain, and support the system once it is in production.

Risks

As with any system, the development and deployment of an enterprise CREM accountability system involves some risks.

The following are the risks identified to date:

- Introduction of classified data into an unclassified database
- Long-term institutional commitment and funding
- Vague and frequently changing DOE and Laboratory Implementation Requirements policies
- Inconsistent business processes across organizations for tracking CREM
- Varying customer priorities across organizations
- Institutional approval/acceptance of paperless system and electronic signatures
- Newness of system enforcement of training requirements
- Newness of system enforcement of classification requirements
- Necessary CIO Policy Board approval
- Network accessibility (need unclassified protected network drops in areas where system will be used)
- Availability of technical personnel to implement and support the system
- Managing CREM when system is unavailable
- Data migration of CREM data from existing systems to the enterprise system

- Approval of new technologies by LANL/DOE (e.g., smart cards, mobile computers, and portals with RFID tagging)
- Incorporating new technologies into existing LANL infrastructures
- Requiring CRYPTOCards™ for the unclassified protected network to access application

Understanding the risks early in the project allows us to develop strategies to mitigate the risks wherever possible. For example, to limit the risk of introducing classified data into an unclassified database, the application will limit the number of fields that will allow free-text entry. Most values will be selected from dropdown lists or other controlled inputs.

Readiness to Proceed

The CREM software team is ready to proceed with Phase 1 of the project. The development and implementation of an enterprise application built around a central database has been done at LANL before. There is a well-defined approach for this process, and the issues are well understood. It is also necessary to have this system in production before a Laboratory-wide test of the portal technology can be implemented.

The portal, RFID tags, and smart-card pilots are ready to proceed in parallel with Phase 1. Once these pilots are completed, the other phases of the project can be initiated.

References

B. Gardiner, S. Herrera, P. Hummer, and J. Martinez, “Classified Removable Electronic Media Accountability System (CREMS) Requirements Specifications,” Los Alamos National Laboratory report LA-UR-03-0676 (2003).

United States Department of Energy, “Requirements Specification Template,” U.S. DOE working document. (available URL: http://cio.doe.gov/ITReform/sqse/download/reqspc.doc), accessed January 2003.

Appendix 1: Portable Inventory System Pilot

Benny J. Martinez, Richard B. Strittmatter, and Joshua Joseph, Jr.

Objectives

Portable identification devices such as hand-held scanners will be used to automate physical inventory. These devices will increase the efficiency of the process by allowing for automatic and instantaneous reconciliation of inventory as items are verified during the physical inventory.

Functions

A physical inventory may be required for annual or special inventories, custodial changes, and/or resolving system anomalies. Traditionally, these exercises have required an individual to physically identify an item and validate the identification number of the item against a paper list of the book inventory. Through this process, a physical location to be inventoried was selected; all items were identified; and all anomalies were reported. This process would be automated.

System Overview

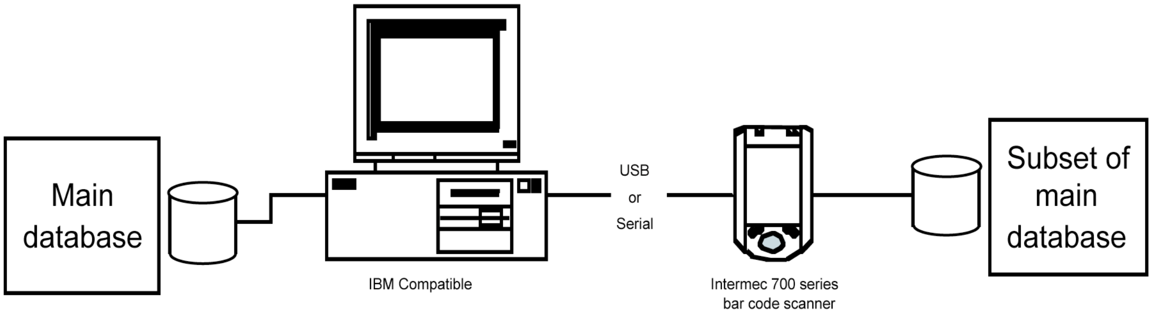


Figure A1-1. This diagram shows the organization of the portable inventory system.

Inventory items are downloaded to the Intermec 700c Color Mobile hand-held computer, which contains a built in bar code scanner. The hand-held computer may be connected to a desktop computer through a docking station that includes a USB or serial communication port.

A subset of the central database is downloaded to the hand-held computer; information may include a bar code number, description, storage location, owner, classification level, etc. The hand-held computer may then be removed from the docking station and taken into the field for use. Users must scan their identification number (Z number) to identify who is doing the inventory. Items may then be scanned and information for each item verified. The date and time that the item was scanned is recorded along with the person scanning the item. Discrepancies are recorded for reconciliation at a later time. Information such as the number of items scanned vs. total items and a list of items scanned is provided to the user to facilitate the inventory process.

Information may be uploaded to the desktop computer at any time to view, print, and reconcile the inventory. When all items have been inventoried and reconciled, the inventory is closed and transactions are generated recording the inventory process in the historical database. (See Figures A1-2 and A1-3.)

User Feedback

Based on the pilots, the following feedback was received:

1. Bar codes scanned could not be reviewed
2. Bar codes not scanned could not be reviewed
3. Users liked the ability to view their data out in the field while doing a physical inventory
4. Users could easily compare the book inventory to the physical inventory
5. Communications between the hand-held computer on the docking station and the workstation were not always reliable
6. When an item was scanned, the wrong bar code was read (the manufacturer's bar code instead of the LANL-issued bar code

Modifications Based On Results

1. Additional options have been added to provide the ability to view information on items that have been scanned and not scanned, thereby allowing the users to display items that still needed to be found or verify that an item had already been scanned.
2. Provided an option to delete bar codes that were inadvertently read.

Lessons Learned

Overall System

The use of portable bar code equipment in a classified environment is difficult under the current DOE and LANL requirements. We recommend that DOE and LANL provide users with guidelines for the use of hand-held computers in a classified environment.

Software Development

The tools used to synchronize the Microsoft database from the portable hand-held device with the workstation (ActiveSync 3.5) caused problems when three or more devices were used to synchronize the same database on the workstation.

We recommend the use of an XML-formatted file to transfer information back and forth between the hand-held computer and the workstation. This will eliminate the requirement of using (ActiveSync 3.5) to synchronize the Microsoft Access databases on the workstation and on multiple hand-held devices. Using an XML file will allow more universal connectivity.

Because development tools are soon to be outdated, we recommend that when new development tools for the Pocket PC™ are released (expected in the first quarter of 2003), it would be beneficial to port the existing application to the new development tools. The benefits of going to this new toolset include the following:

- Same development environment as normal window applications
- A fully compiled executable language (eMbedded Visual Basic, or EVB, is an interpreted language)
- Enhanced debug and development interface
- Ability to reuse code developed for window applications

Hardware

Ease of development on hand-held devices was based on the manufacturer and the model. Hand-held technology is changing quickly, and identifying hand-held devices that will work with current and future development tools is difficult. The two hand-held devices that were evaluated had different operating systems and required different development environments. Careful selection of the hand-held devices and their specifications need to be reviewed.

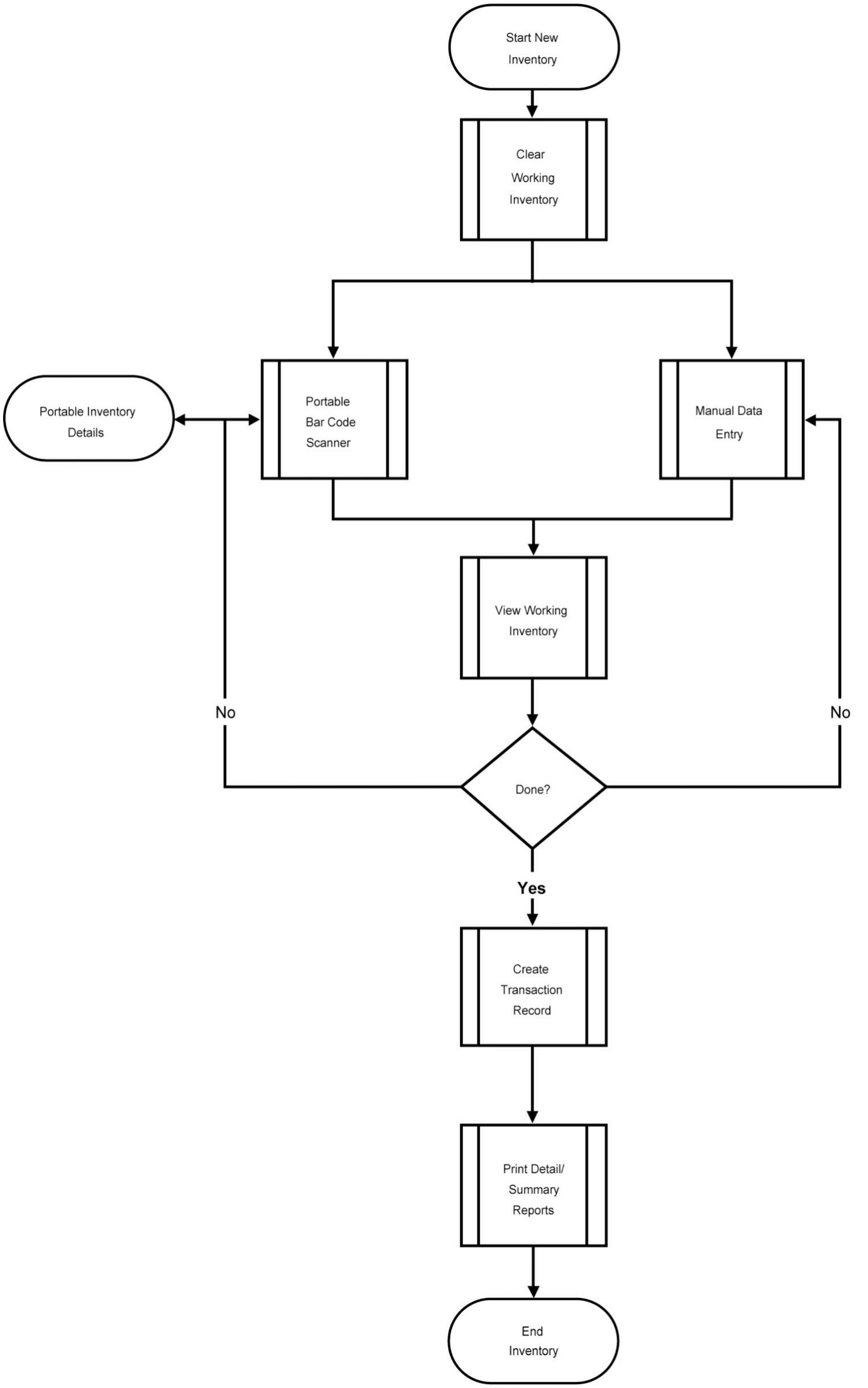


Figure A1-2. Overview of portable inventory system process flow diagram.

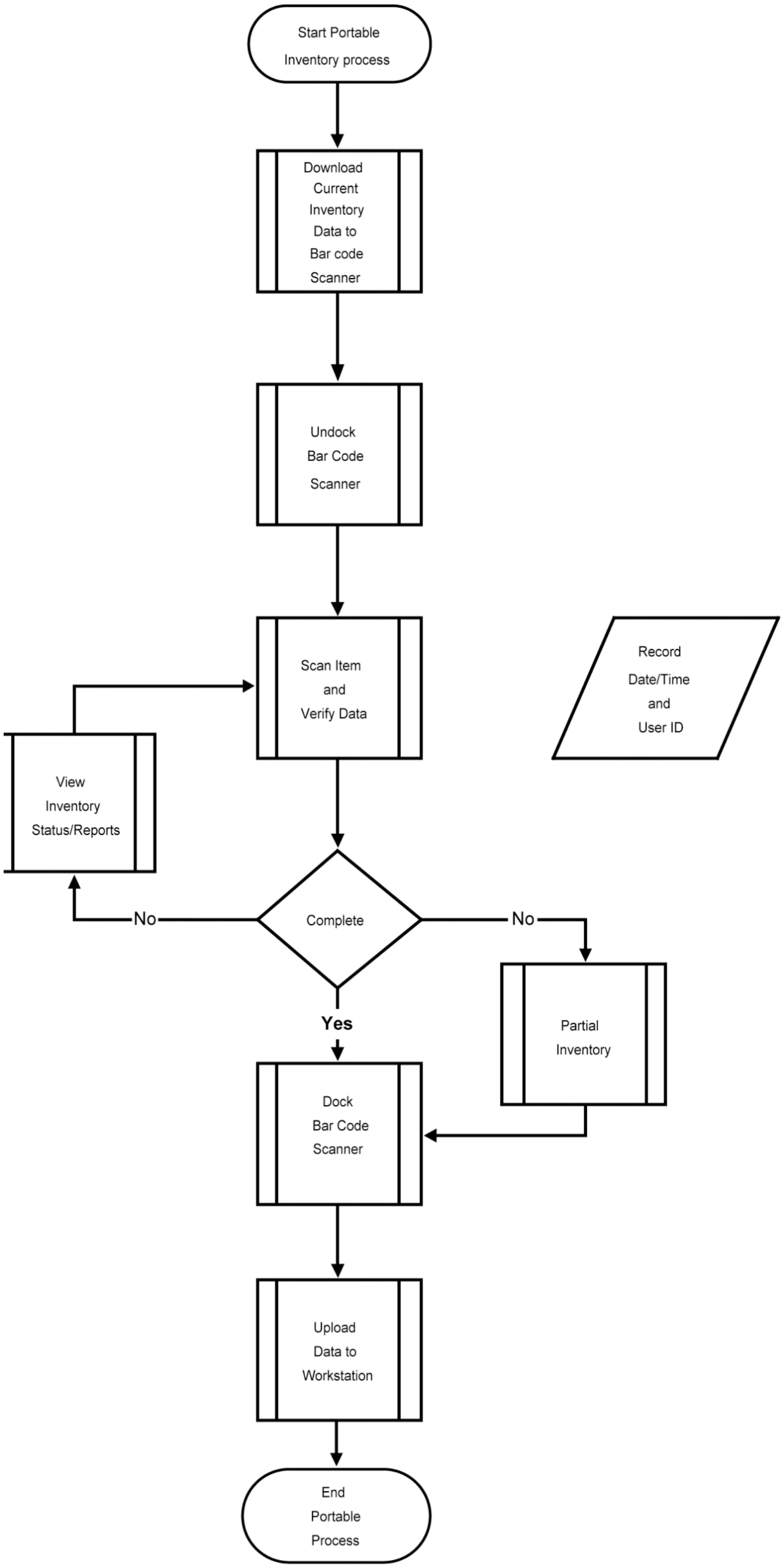

Start Portable Inventory process
Download Current Inventory Data to Bar code Scanner
Undock Bar Code Scanner
Scan Item and Verify Data
Record Date/Time and User ID
View Inventory Status/Reports
Complete
No
No
Yes
Partial Inventory
Dock Bar Code Scanner
Upload Data to Workstation
End Portable Process

Figure A1-3. Portable inventory process flow diagram.

Devices Evaluated

An Intermec 700 Color Mobile hand-held computer and Symbol 8100 hand-held computer were purchased for evaluation. The specifications for each device are given below.

The Intermec 700

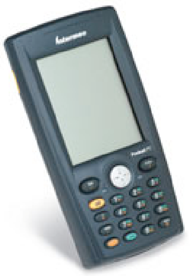


Figure A1-4. Intermec 700c Color Mobile Computer.

Physical Characteristics	Length: 191 mm (7.53 in.) Width: 90 mm (3.5 in.) Height: 50 mm (1.97 in.) Weight: 483-568 grams (17-20 oz) depending on options
Environmental	Operating Temp: -10° to +60°C (+14° to +140°F) application dependent 0° to +40°C (+32° to +140°F) for Bluetooth compatible devices Storage Temp: -20° to +60°C (-4° to +140°F) Relative Humidity: 5% to 95% (non-condensing) Rain and Dust Resistance: IP64 compliant Drop Spec: Withstands 5' drop, 26 times onto concrete
Power	Battery Type: Lithium-Ion, 7.2V, (2 x 2000 mAh cells), customer replaceable Battery Capacity: 14.4 Watt-hours Battery Life: 6-10 hours, application dependent Recharging Time: 4 hours Operating System Microsoft® Windows® for Pocket PC™ 2002
Microprocessor	Intel® XScale™ PXA250 Applications Processor, 400 MHz
Memory and Storage	RAM Memory: 64 MB (128 MB optional)

	Flash ROM: 32 MB; includes ROM folder for application storage
Internal Slots	Secure Digital (SD) CompactFlash (CF) Type I
Display	Reflective TFT daylight readable color display with CCFL frontlight, 240x320 pixels, 3.8 in. (97 mm) diagonal, 64 K colors
Standard Communications	RS232, IrDA 1.1 (115 kbps), 10 Base-T Ethernet, USB
Integrated Radio Options	LAN: 802.11b (Wi-Fi certified) WAN: GSM/GPRS, CDMA/1XRTT Bluetooth™ compatible module
Integrated Scanner Options	APS linear imager** Linear or PDF417 laser scanner 2D imager
Laser Scan Engine Specifications	Minimum/Maximum 5 mil 2.0 in. (5.1 cm)/5.2 in. (13.2 cm) 7.5 mil 1.7 in. (4.3cm)/8 in. (20.3 cm) 10 mil 1.8 in. (4.6 cm)/10 in. (25.4 cm) 100% UPC 1.9 in. (4.8 cm)/13 in. (33 cm) 20 mil † /20 in. (50.8 cm) 40 mil † /25 in. (63.5 cm) 55 mil † /30 in. (76.2 cm) †Dependent on symbol width
Key Accessories	Portable and vehicle-mounted printers Vehicle dock Desktop connectivity dock Desktop dock with integrated modem Ethernet multidock Battery pack chargers Scanning handles
Regulatory Approvals	FCC Part 15 Class B UL Listing CE Mark CB Report

The Symbol 1800

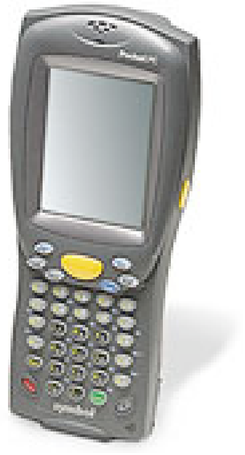


Figure A1-5. Symbol 8100 hand-held computer.

Physical Characteristics	
Overall	8.4” L x 3.7” W x 1.8” D/213 mm L x 93.9 mm W x 45.7 mm D
Grip Area	3.0” W x 1.0” D/76.1 mm W x 25.4 mm D
Weight (including battery)	14.5 oz./410 g w/battery (batch version); 15.5 oz./440 g (wireless version)
Drop Specification	4 ft. (1.2m) to concrete
Display	1/4 VGA (320 x 240 portrait) with16-level grayscale, optional 64k color
Battery	1550 mAh lithium-ion
Environmental Sealing	IP54 (windblown dust and rain)
Operating Temperature	-4° to 122° F/-20° to 50° C (or better depending on the application) 32° to 122° F/0° to 50° C (or better depending on the application)
Storage Temperature	-13º to 122º F/-25º to 50º C
Humidity	5% to 90% RH noncondensing
Electrostatic Discharge (ESD):	8 kVdc air; 4 kVdc contact
Expansion Capabilities:	Type 2 PC (internal); Type 2 CF (user-accessible)
Back-lit Display:	EL
Back-lit Keyboard	LED
Keypads	Choice of 28-, 37-, 47-keys; plus 2 side scan keys
Performance Characteristics	
CPU	Intel SA1110 @ 206MHz

Operating Platform	Microsoft Pocket PC
Memory	64 MB RAM 32 MB ROM
Application Development	Fully compatible with Microsoft SDK for Pocket PCs Symbol SDK available to support bar code scanning
Communications	IrDA 1.1 RS-232
Regulatory	
Electrical Safety	Certified to UL 1950, CSA C22.2 No 950, EN60950/IEC950
EMI/RFI	FCC Part 15 Class B, ICES-003 Class B, European Union EMC Directive, Australian SMA
Laser Safety	CDRH Class II, IEC Class 2

Software Development

Currently Microsoft supports the development of software with a tool called eMbedded Visual Basic® (EVB) that allows development in a Windows environment and debugging on the actual device selected. This tool has been selected based on the experience of the developers, availability, and the ease of use.

The Microsoft eMbedded Visual Basic 3.0 IDE is the most productive way for developers to build applications for the next generation of Windows CE-based communication, entertainment, and information-access devices. A comprehensive, rapid application development environment helps developers quickly create, debug, and deploy Windows CE applications for a wide range of devices using well-known Visual Basic programming tools and techniques.

In addition, developers can take advantage of a familiar development environment by building Windows CE applications using a standalone IDE designed to target Windows CE development.

eMbedded Visual Basic's IntelliSense technology provides on-the-fly syntax and error checking, parameter information, and more. The integrated debugger allows applications running on a remote device or emulator to be locally debugged inside the eMbedded Visual Basic IDE. We can build highly mobile applications that can access remote data stores and communicate with networked servers.

System Requirements

To use eMbedded Visual Tools 3.0, you need to have the following:

Table A1-1: Minimum Requirements

Processor	A personal computer (PC) with a Pentium-class processor; 150-MHz
Operating System	Windows2000 Professional; Microsoft WindowsNT Workstation 4.0 with SP5, Internet Explorer 5.01, and MDAC 2.1; or Windows 98 Second Edition. Windows2000 Professional or WindowsNT Workstation 4.0 is the recommended debug host for the development environment. The eMbedded Visual Tools can be installed on Windows98, and the application can be built from there. However, emulation does not work on Windows98; instead use Windows2000 or WindowsNT as the host machine.
Memory	• Windows98 Second Edition 32MB RAM (48MB RAM recommended) • Windows NT Workstation 4.0 32MB RAM (48MB RAM recommended) • Windows2000 32MB RAM (48MB RAM recommended)
Hard Disk	• eMbedded Visual Basic and one SDK, 360MB • Full installation: eMbedded Visual Basic, eMbedded Visual C++, and three SDKs. 720MB
Drive	CD-ROM drive
Display	VGA or higher-resolution monitor required. Super VGA monitor recommended.
Mouse	Microsoft Mouse or compatible pointing device.

The .NET Compact Framework

Microsoft is currently in the process of releasing a new tool for developing applications in the Pocket PC/Windows CE world. As of this writing, the .NET Compact Framework was still in beta and had not yet been released. Because it is expected to ship soon after this writing, it is worth discussing. Some of what is discussed here may have changed in the final product.

The.NET Compact Framework provides a subset of the desktop Framework, the .NET Framework, in the same way that MFC on Windows CE .NET and Win32 on

Windows CE .NET are a subset of their desktop equivalents. The .NET Framework represents the next step in the continuing evolution and refinement of a programming interface. The .NET Framework, and by extension the Windows CE .NET equivalent, the .NET Compact Framework, solves many of the problems that Win32 and MFC programmers have been grappling with over the years. When the final version ships, the .NET Compact Framework will support the Pocket PC, Pocket PC 2002 and all appropriately configured Windows CE. NET-based platforms.

Visual Studio .NET 2003 integrates device development as a first-class citizen within the IDE. Visual Studio .NET 2003 provides native support for the .NET Compact Framework.

For the broadest possible reach to Internet-enabled devices, developers using Visual Studio .NET 2003 can use ASP.NET mobile controls (formerly Microsoft Mobile Internet Toolkit) to build a single mobile Web interface to support a broad range of devices, 200 at last count. Supported mobile technologies include WML 1.1 for WAP-enabled cellular phones, compact HTML (cHTML) for i-mode phones, and hypertext markup language (HTML) for Pocket PCs™, Palm™ devices, and pagers.

Appendix 2: Features and Descriptions of RF Portal Monitoring Systems

System A

Reader

Make: Omron
Model: V720-BC5D4-E
Frequency: 13.56 MHz +/- 7 kHz
System Type: Backscatter
Available Modes: Read-Only and Read-Write (user selection)
Emission Type: Stable Frequency
Emissive Power: < 4.0 W
Communications: ASCII7
Host Connection: Serial RS232C
Anticollision: Yes

Antennae

Make: Omron
Model: V720-HS71S
Polarization: Circular
Lateral Separation: 36 inches

Tag

Make: Omron
Model: V720-D52PO1
Battery: None

System A Costs

Reader and Antennae: $9,550.00
Tag Insert (each): $2.25
Software (each install): $1,800.00

System A Total for One Station (without tags): $11,350.00

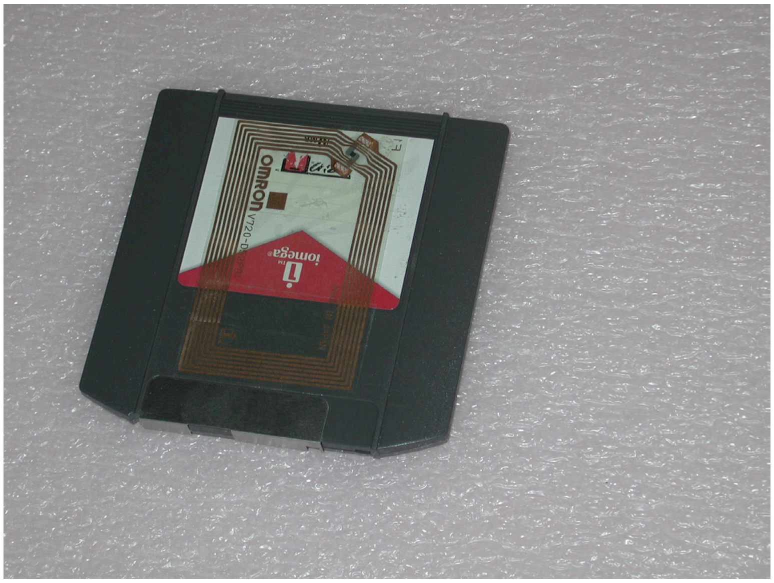


Figure A2-1. An Omron model V720-D52P01 smart tag affixed to a Zip disk.

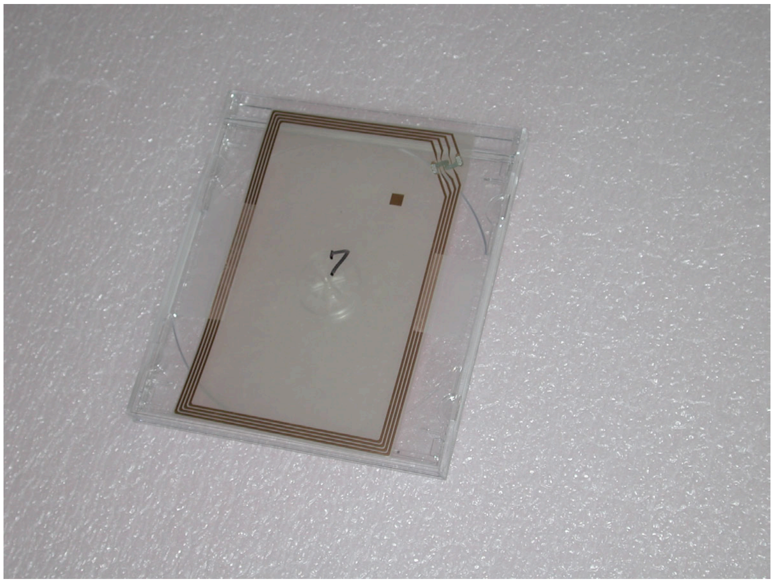


Figure A2-2. The Omron model V720-D52P01 smart tag is affixed to a CD jewel case in some test configurations. We tested the tag with the CD in the case.

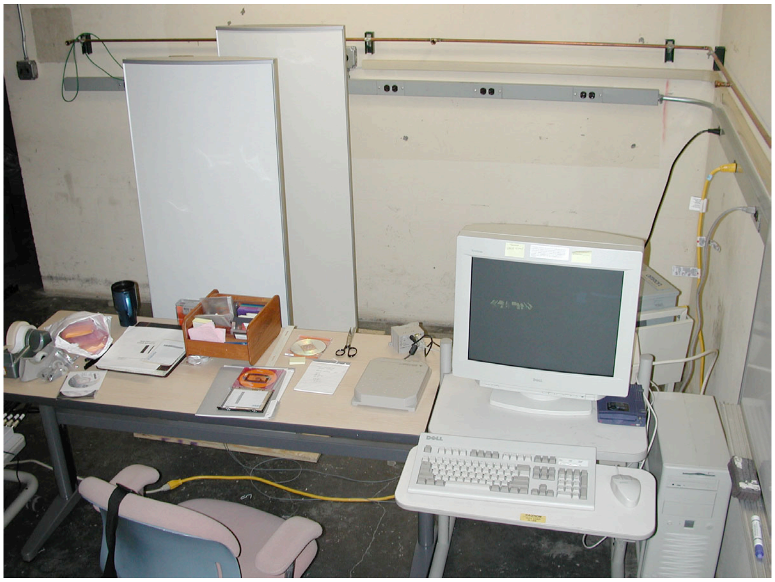


Figure A2-3. The gate antennae for System A (background) are connected to the standalone PC host, shown in the foreground.

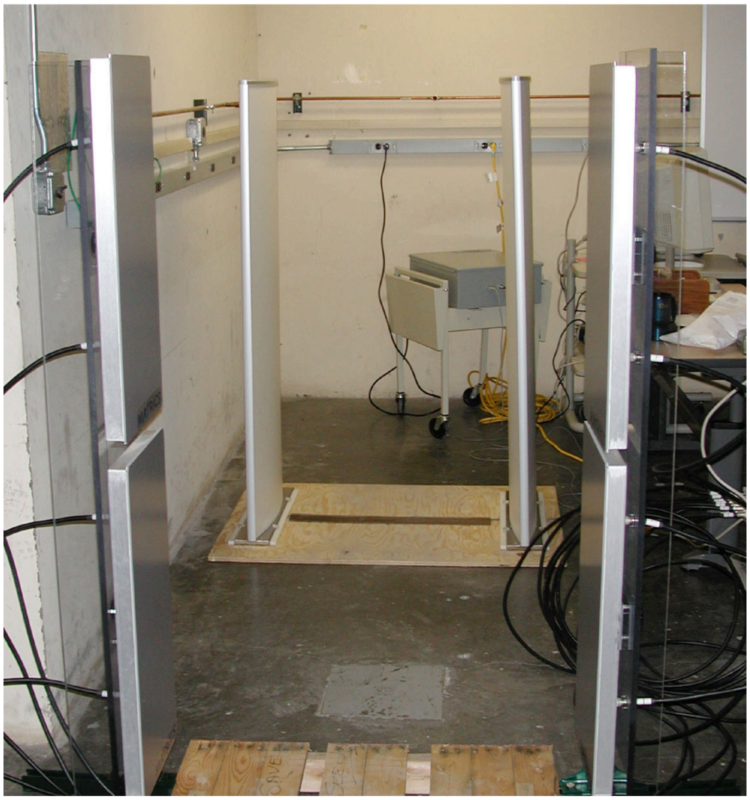


Figure A2-4. A runway view of the portal antennae shows System A in the background, and System B in the foreground.

System B

Reader

Make: Matrics
Model: Stationary Reader RDR-001
Frequency: 902-928 MHz
System Type: Backscatter
Available Modes: Read-Only
Emission Type: Frequency Hopping, Spread Spectrum
Emissive Power: 4.0 W (1.0 W per antenna)
Communications: ASCII
Host Connection: RS485-to-USB
Anticollision: Yes

Antennae

Make: Matrics
Model: General Purpose Antenna ANT-001
Polarization: Circular
Lateral Separation: 36 inches

Tag

Make: Matrics
Model: Double Dipole DDS-001
Battery: None

System B Costs

Reader and Antennae: $4,499.00
Tag Insert (each): $1.09
Software (each install): $1,200.00

System B Total for One Station (without tags): $5,699.00

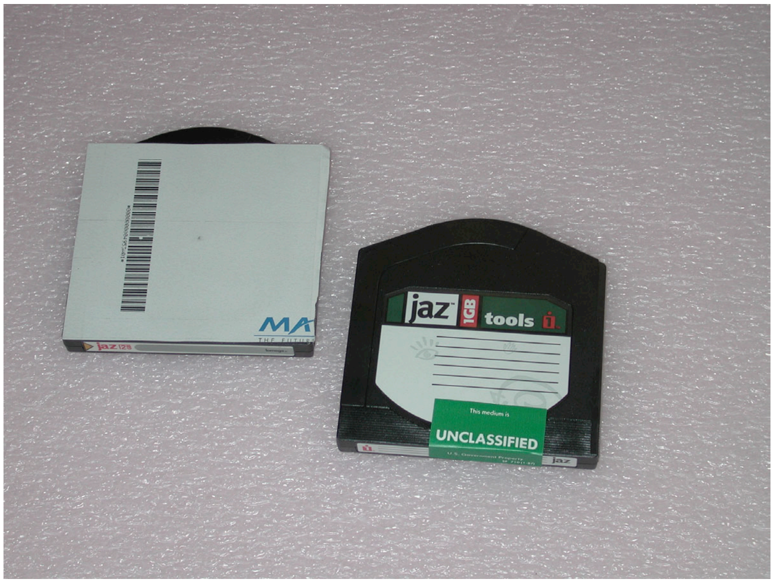


Figure A2-5. A Matrics model DDS-001 tag affixed to a Jaz disk.

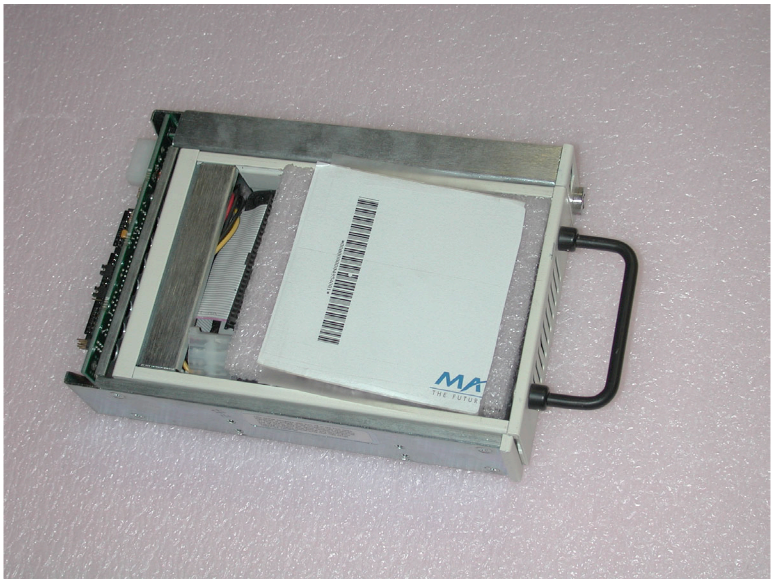


Figure A2-6. The Matrics model DDS-001 tag is affixed to a removable hard drive case, with a half-inch polyurethane foam spacer between drive and tag.

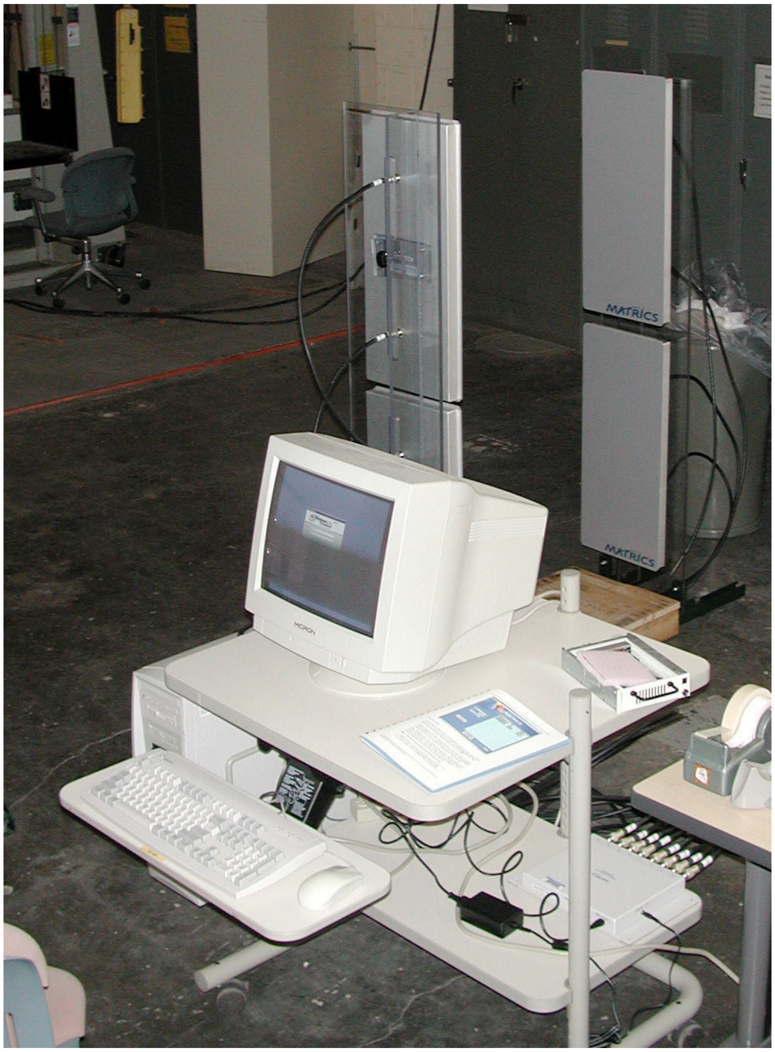


Figure A2-7. A lateral view shows the gate antennae for System B behind the standalone PC host in the foreground.

System C

Reader

Make:	Intermec
Model:	Reader 2100 UAP
Frequency:	902-928 MHz
System Type:	Backscatter
Available Modes:	Read-Only and Read-Write (user selection)
Emission Type:	Direct Sequence, Spread Spectrum
Emissive Power:	< 4.0 W
Communications:	UDP
Host Connection:	RJ45
Anticollision:	Yes

Antennae

Make:	Cushcraft
Model:	S9028PC
Polarization:	Circular
Lateral Separation:	36 inches

Tag

Make (VHS):	Marconi
Model (VHS):	strip tag
Make (Other media):	Intermec
Model (Other media):	smart label
Battery:	None

System C Costs

Reader and Antennae:	$3,995.00
Tag Insert (each):	$4.50 to $13.20
Software (each install):	$1,200.00

System C Total for one station (without tags):	$5,195.00

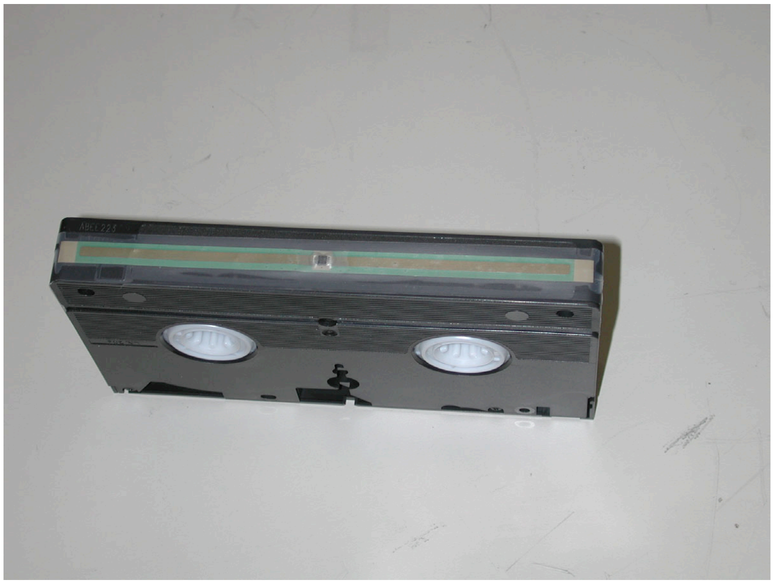


Figure A2-8. The Marconi strip tag is affixed to a VHS videocassette.

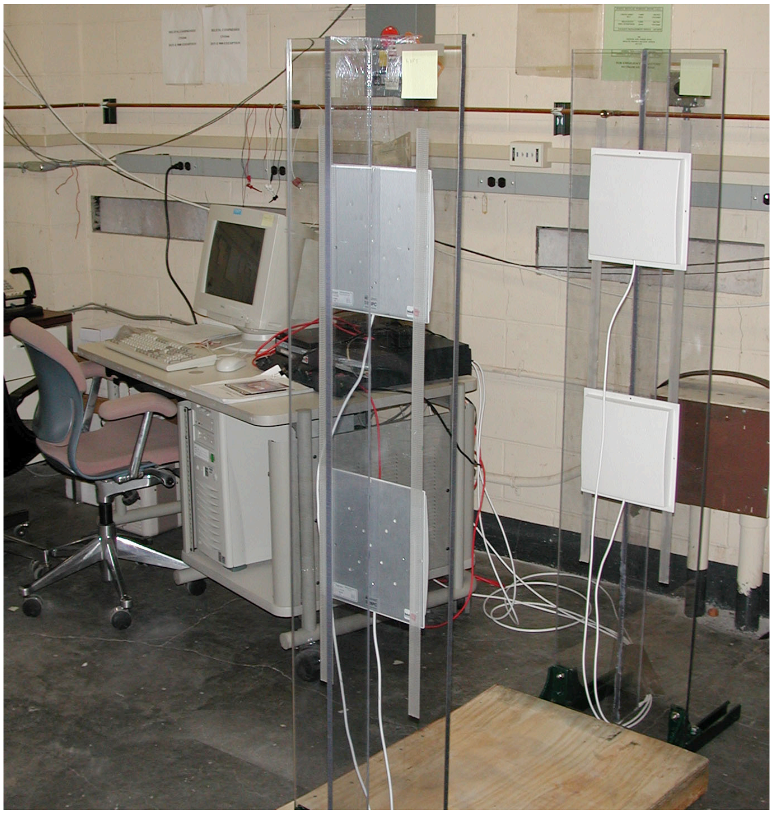


Figure A2-9. The image shows the arrangement of the gate antennae for System C.

System D

Detection Gate and Antennae

Make: 3M
Model: 3802 Series Library Security System
Frequency: N/A (probably 10 to 100 kHz range)
System Type: Field Disturbance
Available Modes: Detect-Only
Emission Type: N/A
Emissive Power: N/A
System Power: 720W to 1000W
Communications: None
Host Connection: None
Anticollision: N/A
Lateral Separation: 36 to 36.5 inches

Tape

Make: 3M
Model (CD-ROM): DCD-2
Model (VHS): DVM-1

Battery: None

System D Costs

Detection Gate:	$10,000.00
Tape Insert (each):	$0.23
Software (each install):	N/A

System D Total for one station (without tapes): $10,000.00

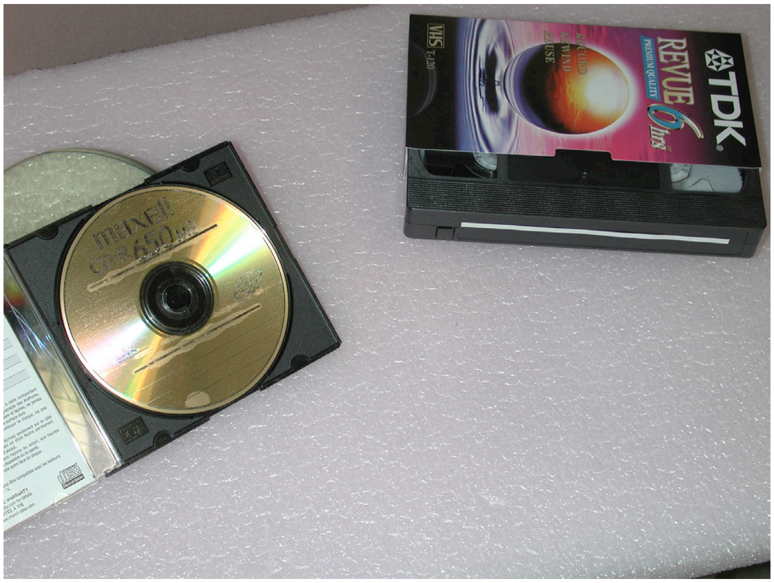


Figure A2-10. The image shows a 3M model DCD-2 tape affixed to a CD-ROM in the jewel case, and a 3M model DVM-1 strip tape affixed to a VHS videocassette in the sleeve.

Appendix 3: Performance Data for Preliminary Testing of CREM RFID Portals

Luca Gratton and Richard Siebelist

Introduction

This appendix summarizes operational and technical observations of pedestrian portal monitor performance for the Classified Removable Electronic Media (CREM) Control Project. Operational aspects of candidate portal implementations influence the pertinence of individual candidates in satisfying the general purpose of CREM Control endeavor.

Preliminary performance tests of three radio frequency identification (RFID) portal monitor systems were performed in support of feasibility studies for the CREM Control project. The three systems are derivates of the following manufacturer RFID controller product lines (the internal designation for the system is provided in parentheses): Omron Model V720 (System A), Matrix Stationary Reader RDR-001 (System B), and Intermec Model 2100 UAP (System C). Additionally, a 3M Model 3802 Tattle-Tape Security System (System D) was evaluated exclusively for the management of CDs and VHS videocassettes.

The objectives of the investigations were the determination of feasibility, and the quantitative examination of performance and reliability where feasible, for the detection of removable electronic media with RFID pedestrian portal gates. The types of media subject to this determination were (1) CD-ROM, (2) 3.5 inch storage disks, (3) removable hard drives, (4) Jaz disks, (5) Zip disks, (6) memory sticks and (7) VHS videocassettes. Preliminary data were successfully acquired for Systems A, B, C and D.

Data

Evaluations were performed with RFID Systems A and B on November 7, 2002, in the service area of Room 104, Building 27, in TA-35. Evaluations for the field disturbance system (System D) were performed on November 13, 2002, at the main entrance to the Oppenheimer Research Library, in TA-3. Evaluations of RFID System C were performed on November 26 and December 17, 2002, in Room 104, Building 27 in TA-35. Additional evaluations of System B were performed on December 11, 2002, in Room 104, Building 27, in TA-35.

For both systems, and for all media, evaluation results are associated with a tag orientation. Tag orientation “X” provides a coincident surface normal for both the tag and portal gate antennae (i.e., tag is oriented as if placed flat upon the face of the portal gate). This orientation is theoretically providing the best radio-coupling between tag and antennae, and therefore, providing the strongest read signal and most balanced read response within the interrogation zone. Orientation “Y” provides a tag surface normal, that is orthogonal, to those for the portal gate antennae, with the tag surface normal coincident with the direction of pedestrian movement through the portals (i.e., as if one were holding a shield or mirror). Orientation "Z" provides a vertical tag surface normal (i.e., as if holding a flat plate with one's palms extended).

Tagged media were introduced to the interrogation zones individually, unless stated otherwise. The introduction of individual tags to the interrogation antennae of Systems A and B does not allow evaluation of the RFID system collision properties. For the field disturbance device, items may be detected individually without accompanying identifications. However, tests were performed with System D to determine performance with multiple items in the interrogation zone. For System D, determinations of the inventory fractions actually detected could not be made when multiple taped items were introduced to the interrogation zone simultaneously.

The results of the evaluations are organized by system type below. For each trial, the tag type, medium, location and success rate are provided in tabular form. Locations are categorized in 3 horizontal and 3 vertical descriptors, respectively. The vertical height "high" is defined to be 58 inches from the floor, "middle" at 38 inches from the floor, and "low" at 24 inches from the ground. Horizontal "center" corresponds to the lateral midpoint between gates (i.e., 19 inches from both portals). "Left" and "right" correspond to approximate 6 inch lateral stand-off distances from the respective gate antenna. Success rates are the fraction of committed, registered readings in a series of observation trials. Success rate is based on the observations from 5 or more trials at a specific location.

System A

Orientation : X System A

Tag Type	Medium	Location	Success Rate (%)
V720-D52PO1	3.5 inch floppy	center, high	100
V720-D52PO1	3.5 inch floppy	center, middle	100
V720-D52PO1	3.5 inch floppy	center, low	20
V720-D52PO1	3.5 inch floppy	right, high	0
V720-D52PO1	3.5 inch floppy	right, middle	40
V720-D52PO1	3.5 inch floppy	right, low	0
V720-D52PO1	3.5 inch floppy	left, high	40
V720-D52PO1	3.5 inch floppy	left, middle	40
V720-D52PO1	3.5 inch floppy	left, low	0

Orientation : X System A

Tag Type	Medium	Location	Success Rate (%)
V720-D52PO1	Zip disk	center, high	100
V720-D52PO1	Zip disk	center, middle	100
V720-D52PO1	Zip disk	center, low	0
V720-D52PO1	Zip disk	right, high	0
V720-D52PO1	Zip disk	right, middle	40
V720-D52PO1	Zip disk	right, low	40
V720-D52PO1	Zip disk	left, high	0
V720-D52PO1	Zip disk	left, middle	0
V720-D52PO1	Zip disk	left, low	40

Orientation : X System A

Tag Type	Medium	Location	Success Rate (%)
V720-D52PO1	Jaz disk	center, high	0
V720-D52PO1	Jaz disk	center, middle	0
V720-D52PO1	Jaz disk	center, low	0
V720-D52PO1	Jaz disk	right, high	0
V720-D52PO1	Jaz disk	right, middle	0
V720-D52PO1	Jaz disk	right, low	0
V720-D52PO1	Jaz disk	left, high	0
V720-D52PO1	Jaz disk	left, middle	0
V720-D52PO1	Jaz disk	left, low	0

Orientation : X System A

Tag Type	Medium	Location	Success Rate (%)
V720-D52PO1	CD-ROM in case	center, high	0
V720-D52PO1	CD-ROM in case	center, middle	0
V720-D52PO1	CD-ROM in case	center, low	0
V720-D52PO1	CD-ROM in case	right, high	0
V720-D52PO1	CD-ROM in case	right, middle	0
V720-D52PO1	CD-ROM in case	right, low	0
V720-D52PO1	CD-ROM in case	left, high	0
V720-D52PO1	CD-ROM in case	left, middle	0
V720-D52PO1	CD-ROM in case	left, low	0

Orientation : X System A

Tag Type	Medium	Location	Success Rate (%)
V720-D52PO1	Removable HD	center, high	0
V720-D52PO1	Removable HD	center, middle	0
V720-D52PO1	Removable HD	center, low	0
V720-D52PO1	Removable HD	right, high	100
V720-D52PO1	Removable HD	right, middle	100
V720-D52PO1	Removable HD	right, low	100
V720-D52PO1	Removable HD	left, high	100
V720-D52PO1	Removable HD	left, middle	40
V720-D52PO1	Removable HD	left, low	100

Orientation : X System A

Tag Type	Medium	Location	Success Rate (%)
Lot 120	Smart Card / no medium	center, high	100
Lot 120	Smart Card / no medium	center, middle	40
Lot 120	Smart Card / no medium	center, low	100
Lot 120	Smart Card / no medium	right, high	100
Lot 120	Smart Card / no medium	right, middle	20
Lot 120	Smart Card / no medium	right, low	40
Lot 120	Smart Card / no medium	left, high	100
Lot 120	Smart Card / no medium	left, middle	20
Lot 120	Smart Card / no medium	left, low	100

System B

Orientation : X System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	3.5 inch floppy	center, high	100
DDS-001	3.5 inch floppy	center, middle	100
DDS-001	3.5 inch floppy	center, low	100
DDS-001	3.5 inch floppy	right, high	100
DDS-001	3.5 inch floppy	right, middle	100
DDS-001	3.5 inch floppy	right, low	100
DDS-001	3.5 inch floppy	left, high	100
DDS-001	3.5 inch floppy	left, middle	100
DDS-001	3.5 inch floppy	left, low	100

Orientation : Y System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	3.5 inch floppy	center, high	100
DDS-001	3.5 inch floppy	center, middle	100
DDS-001	3.5 inch floppy	center, low	100
DDS-001	3.5 inch floppy	right, high	100
DDS-001	3.5 inch floppy	right, middle	100
DDS-001	3.5 inch floppy	right, low	100
DDS-001	3.5 inch floppy	left, high	100
DDS-001	3.5 inch floppy	left, middle	100
DDS-001	3.5 inch floppy	left, low	100

Orientation : Z System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	3.5 inch floppy	center, high	100
DDS-001	3.5 inch floppy	center, middle	100
DDS-001	3.5 inch floppy	center, low	100
DDS-001	3.5 inch floppy	right, high	100
DDS-001	3.5 inch floppy	right, middle	100
DDS-001	3.5 inch floppy	right, low	100
DDS-001	3.5 inch floppy	left, high	100
DDS-001	3.5 inch floppy	left, middle	100
DDS-001	3.5 inch floppy	left, low	100

Orientation : X System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Zip disk	center, high	100
DDS-001	Zip disk	center, middle	100
DDS-001	Zip disk	center, low	100
DDS-001	Zip disk	right, high	100
DDS-001	Zip disk	right, middle	100
DDS-001	Zip disk	right, low	100
DDS-001	Zip disk	left, high	100
DDS-001	Zip disk	left, middle	100
DDS-001	Zip disk	left, low	100

Orientation : Y System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Zip disk	center, high	100
DDS-001	Zip disk	center, middle	100
DDS-001	Zip disk	center, low	100
DDS-001	Zip disk	right, high	100
DDS-001	Zip disk	right, middle	100
DDS-001	Zip disk	right, low	100
DDS-001	Zip disk	left, high	100
DDS-001	Zip disk	left, middle	100
DDS-001	Zip disk	left, low	100

Orientation : Z System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Zip disk	center, high	100
DDS-001	Zip disk	center, middle	100
DDS-001	Zip disk	center, low	100
DDS-001	Zip disk	right, high	100
DDS-001	Zip disk	right, middle	100
DDS-001	Zip disk	right, low	100
DDS-001	Zip disk	left, high	100
DDS-001	Zip disk	left, middle	100
DDS-001	Zip disk	left, low	100

Orientation : X System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Jaz disk	center, high	100
DDS-001	Jaz disk	center, middle	100
DDS-001	Jaz disk	center, low	100
DDS-001	Jaz disk	right, high	100
DDS-001	Jaz disk	right, middle	100
DDS-001	Jaz disk	right, low	100
DDS-001	Jaz disk	left, high	100
DDS-001	Jaz disk	left, middle	100
DDS-001	Jaz disk	left, low	100

Orientation : Y System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Jaz disk	center, high	100
DDS-001	Jaz disk	center, middle	100
DDS-001	Jaz disk	center, low	100
DDS-001	Jaz disk	right, high	100
DDS-001	Jaz disk	right, middle	100
DDS-001	Jaz disk	right, low	100
DDS-001	Jaz disk	left, high	100
DDS-001	Jaz disk	left, middle	100
DDS-001	Jaz disk	left, low	100

Orientation : Z System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Jaz disk	center, high	100
DDS-001	Jaz disk	center, middle	100
DDS-001	Jaz disk	center, low	100
DDS-001	Jaz disk	right, high	100
DDS-001	Jaz disk	right, middle	100
DDS-001	Jaz disk	right, low	100
DDS-001	Jaz disk	left, high	100
DDS-001	Jaz disk	left, middle	100
DDS-001	Jaz disk	left, low	100

Orientation : X System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	20[a] ; 30[b]
DDS-001	CD-ROM in case	center, middle	100[a] ; 100[b]
DDS-001	CD-ROM in case	center, low	0[a] ; 20[b]
DDS-001	CD-ROM in case	right, high	0[a] ; 50[b]
DDS-001	CD-ROM in case	right, middle	40[a] ; 80[b]
DDS-001	CD-ROM in case	right, low	0[a] ; 10[b]
DDS-001	CD-ROM in case	left, high	0[a] ; 60[b]
DDS-001	CD-ROM in case	left, middle	100[a] ; 30[b]
DDS-001	CD-ROM in case	left, low	0[a] ; 30[b]

NOTE: a = measurements taken 11/07/02 ; b = measurements taken 12/11/02. Tag on disk.

Orientation : Y System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	80
DDS-001	CD-ROM in case	center, middle	90
DDS-001	CD-ROM in case	center, low	10
DDS-001	CD-ROM in case	right, high	20
DDS-001	CD-ROM in case	right, middle	20
DDS-001	CD-ROM in case	right, low	10
DDS-001	CD-ROM in case	left, high	10
DDS-001	CD-ROM in case	left, middle	0
DDS-001	CD-ROM in case	left, low	0

NOTE: Tag on disk.

Orientation : Z System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	0
DDS-001	CD-ROM in case	center, middle	0
DDS-001	CD-ROM in case	center, low	0
DDS-001	CD-ROM in case	right, high	50
DDS-001	CD-ROM in case	right, middle	0
DDS-001	CD-ROM in case	right, low	0
DDS-001	CD-ROM in case	left, high	50
DDS-001	CD-ROM in case	left, middle	30
-DDS-001	CD-ROM in case	left, low	10

NOTE: Tag on disk.

Orientation : X System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	80
DDS-001	CD-ROM in case	center, middle	100
DDS-001	CD-ROM in case	center, low	40
DDS-001	CD-ROM in case	right, high	40
DDS-001	CD-ROM in case	right, middle	50
DDS-001	CD-ROM in case	right, low	40
DDS-001	CD-ROM in case	left, high	100
DDS-001	CD-ROM in case	left, middle	90
DDS-001	CD-ROM in case	left, low	100

NOTE: Tag inside jewel case, with paper case label between tag and CD-ROM.

Orientation : Y System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	10
DDS-001	CD-ROM in case	center, middle	90
DDS-001	CD-ROM in case	center, low	100
DDS-001	CD-ROM in case	right, high	10
DDS-001	CD-ROM in case	right, middle	10
DDS-001	CD-ROM in case	right, low	10
DDS-001	CD-ROM in case	left, high	80
DDS-001	CD-ROM in case	left, middle	0
DDS-001	CD-ROM in case	left, low	0

NOTE: Tag inside jewel case, with paper case label between tag and CD-ROM.

Orientation : Z System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	10
DDS-001	CD-ROM in case	center, middle	10
DDS-001	CD-ROM in case	center, low	0
DDS-001	CD-ROM in case	right, high	40
DDS-001	CD-ROM in case	right, middle	40
DDS-001	CD-ROM in case	right, low	0
DDS-001	CD-ROM in case	left, high	30
DDS-001	CD-ROM in case	left, middle	80
DDS-001	CD-ROM in case	left, low	30

NOTE: Tag inside jewel case, with paper case label between tag and CD-ROM.

Orientation : X System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	80
DDS-001	CD-ROM in case	center, middle	100
DDS-001	CD-ROM in case	center, low	20
DDS-001	CD-ROM in case	right, high	10
DDS-001	CD-ROM in case	right, middle	50
DDS-001	CD-ROM in case	right, low	0
DDS-001	CD-ROM in case	left, high	70
DDS-001	CD-ROM in case	left, middle	20
DDS-001	CD-ROM in case	left, low	40

NOTE: Tag on jewel case exterior.

Orientation : Y System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	20
DDS-001	CD-ROM in case	center, middle	0
DDS-001	CD-ROM in case	center, low	10
DDS-001	CD-ROM in case	right, high	100
DDS-001	CD-ROM in case	right, middle	30
DDS-001	CD-ROM in case	right, low	0
DDS-001	CD-ROM in case	left, high	0
DDS-001	CD-ROM in case	left, middle	0
DDS-001	CD-ROM in case	left, low	0

NOTE: Tag on jewel case exterior.

Orientation : Z System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	CD-ROM in case	center, high	0
DDS-001	CD-ROM in case	center, middle	10
DDS-001	CD-ROM in case	center, low	0
DDS-001	CD-ROM in case	right, high	0
DDS-001	CD-ROM in case	right, middle	2
DDS-001	CD-ROM in case	right, low	0
DDS-001	CD-ROM in case	left, high	0
DDS-001	CD-ROM in case	left, middle	1
DDS-001	CD-ROM in case	left, low	0

NOTE: Tag on jewel case exterior.

Orientation : X System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Removable HD	center, high	100[a] ; 100[b]
DDS-001	Removable HD	center, middle	100[a] ; 100[b]
DDS-001	Removable HD	center, low	100[a] ; 100[b]
DDS-001	Removable HD	right, high	100[a] ; 100[b]
DDS-001	Removable HD	right, middle	100[a] ; 100[b]
DDS-001	Removable HD	right, low	100[a] ; 100[b]
DDS-001	Removable HD	left, high	100[a] ; 100[b]
DDS-001	Removable HD	left, middle	100[a] ; 100[b]
DDS-001	Removable HD	left, low	100[a] ; 100[b]

NOTE: a = measurements taken 11/07/02 ; b = measurements taken 12/11/02.

Orientation : Y System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Removable HD	center, high	100
DDS-001	Removable HD	center, middle	100
DDS-001	Removable HD	center, low	100
DDS-001	Removable HD	right, high	100
DDS-001	Removable HD	right, middle	100
DDS-001	Removable HD	right, low	100
DDS-001	Removable HD	left, high	100
DDS-001	Removable HD	left, middle	100
DDS-001	Removable HD	left, low	100

Orientation : Z System B

Tag Type	Medium	Location	Success Rate (%)
DDS-001	Removable HD	center, high	70
DDS-001	Removable HD	center, middle	100
DDS-001	Removable HD	center, low	100
DDS-001	Removable HD	right, high	100
DDS-001	Removable HD	right, middle	100
DDS-001	Removable HD	right, low	100
DDS-001	Removable HD	left, high	90
DDS-001	Removable HD	left, middle	100
DDS-001	Removable HD	left, low	100

System C

Orientation : X System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	3.5 inch floppy	center, high	70
Smart Label	3.5 inch floppy	center, middle	60
Smart Label	3.5 inch floppy	center, low	100
Smart Label	3.5 inch floppy	right, high	70
Smart Label	3.5 inch floppy	right, middle	80
Smart Label	3.5 inch floppy	right, low	100
Smart Label	3.5 inch floppy	left, high	100
Smart Label	3.5 inch floppy	left, middle	50
Smart Label	3.5 inch floppy	left, low	50

Orientation : Y System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	3.5 inch floppy	center, high	100
Smart Label	3.5 inch floppy	center, middle	80
Smart Label	3.5 inch floppy	center, low	100
Smart Label	3.5 inch floppy	right, high	100
Smart Label	3.5 inch floppy	right, middle	80
Smart Label	3.5 inch floppy	right, low	100
Smart Label	3.5 inch floppy	left, high	100
Smart Label	3.5 inch floppy	left, middle	90
Smart Label	3.5 inch floppy	left, low	100

Orientation : Z System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	3.5 inch floppy	center, high	40
Smart Label	3.5 inch floppy	center, middle	10
Smart Label	3.5 inch floppy	center, low	70
Smart Label	3.5 inch floppy	right, high	50
Smart Label	3.5 inch floppy	right, middle	70
Smart Label	3.5 inch floppy	right, low	70
Smart Label	3.5 inch floppy	left, high	60
Smart Label	3.5 inch floppy	left, middle	80
Smart Label	3.5 inch floppy	left, low	70

Orientation : X System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Zip disk	center, high	90
Smart Label	Zip disk	center, middle	70
Smart Label	Zip disk	center, low	100
Smart Label	Zip disk	right, high	100
Smart Label	Zip disk	right, middle	60
Smart Label	Zip disk	right, low	90
Smart Label	Zip disk	left, high	100
Smart Label	Zip disk	left, middle	100
Smart Label	Zip disk	left, low	90

Orientation : Y System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Zip disk	center, high	90
Smart Label	Zip disk	center, middle	100
Smart Label	Zip disk	center, low	100
Smart Label	Zip disk	right, high	100
Smart Label	Zip disk	right, middle	20
Smart Label	Zip disk	right, low	100
Smart Label	Zip disk	left, high	100
Smart Label	Zip disk	left, middle	100
Smart Label	Zip disk	left, low	90

Orientation : Z System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Zip disk	center, high	90
Smart Label	Zip disk	center, middle	60
Smart Label	Zip disk	center, low	100
Smart Label	Zip disk	right, high	50
Smart Label	Zip disk	right, middle	40
Smart Label	Zip disk	right, low	40
Smart Label	Zip disk	left, high	50
Smart Label	Zip disk	left, middle	80
Smart Label	Zip disk	left, low	90

Orientation : X System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Jaz disk	center, high	0
Smart Label	Jaz disk	center, middle	0
Smart Label	Jaz disk	center, low	0
Smart Label	Jaz disk	right, high	20
Smart Label	Jaz disk	right, middle	0
Smart Label	Jaz disk	right, low	10
Smart Label	Jaz disk	left, high	0
Smart Label	Jaz disk	left, middle	0
Smart Label	Jaz disk	left, low	20

Orientation : Y System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Jaz disk	center, high	20
Smart Label	Jaz disk	center, middle	0
Smart Label	Jaz disk	center, low	0
Smart Label	Jaz disk	right, high	90
Smart Label	Jaz disk	right, middle	0
Smart Label	Jaz disk	right, low	90
Smart Label	Jaz disk	left, high	0
Smart Label	Jaz disk	left, middle	0
Smart Label	Jaz disk	left, low	0

Orientation : Z System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Jaz disk	center, high	0
Smart Label	Jaz disk	center, middle	0
Smart Label	Jaz disk	center, low	0
Smart Label	Jaz disk	right, high	30
Smart Label	Jaz disk	right, middle	0
Smart Label	Jaz disk	right, low	40
Smart Label	Jaz disk	left, high	0
Smart Label	Jaz disk	left, middle	0
Smart Label	Jaz disk	left, low	0

Orientation : X System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	CD-ROM in case	center, high	0
Smart Label	CD-ROM in case	center, middle	0
Smart Label	CD-ROM in case	center, low	0
Smart Label	CD-ROM in case	right, high	0
Smart Label	CD-ROM in case	right, middle	0
Smart Label	CD-ROM in case	right, low	0
Smart Label	CD-ROM in case	left, high	0
Smart Label	CD-ROM in case	left, middle	0
Smart Label	CD-ROM in case	left, low	0

Orientation : Y System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	CD-ROM in case	center, high	0
Smart Label	CD-ROM in case	center, middle	0
Smart Label	CD-ROM in case	center, low	0
Smart Label	CD-ROM in case	right, high	0
Smart Label	CD-ROM in case	right, middle	0
Smart Label	CD-ROM in case	right, low	0
Smart Label	CD-ROM in case	left, high	0
Smart Label	CD-ROM in case	left, middle	0
Smart Label	CD-ROM in case	left, low	0

Orientation : Z System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	CD-ROM in case	center, high	0
Smart Label	CD-ROM in case	center, middle	0
Smart Label	CD-ROM in case	center, low	0
Smart Label	CD-ROM in case	right, high	0
Smart Label	CD-ROM in case	right, middle	0
Smart Label	CD-ROM in case	right, low	0
Smart Label	CD-ROM in case	left, high	0
Smart Label	CD-ROM in case	left, middle	0
Smart Label	CD-ROM in case	left, low	0

Orientation : X System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Removable HD	center, high	80
Smart Label	Removable HD	center, middle	100
Smart Label	Removable HD	center, low	100
Smart Label	Removable HD	right, high	100
Smart Label	Removable HD	right, middle	70
Smart Label	Removable HD	right, low	80
Smart Label	Removable HD	left, high	100
Smart Label	Removable HD	left, middle	40
Smart Label	Removable HD	left, low	80

Orientation : Y System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Removable HD	center, high	60
Smart Label	Removable HD	center, middle	20
Smart Label	Removable HD	center, low	100
Smart Label	Removable HD	right, high	100
Smart Label	Removable HD	right, middle	70
Smart Label	Removable HD	right, low	70
Smart Label	Removable HD	left, high	90
Smart Label	Removable HD	left, middle	10
Smart Label	Removable HD	left, low	70

Orientation : Z System C

Tag Type	Medium	Location	Success Rate (%)
Smart Label	Removable HD	center, high	80
Smart Label	Removable HD	center, middle	90
Smart Label	Removable HD	center, low	100
Smart Label	Removable HD	right, high	10
Smart Label	Removable HD	right, middle	100
Smart Label	Removable HD	right, low	80
Smart Label	Removable HD	left, high	100
Smart Label	Removable HD	left, middle	100
Smart Label	Removable HD	left, low	80

Orientation : X System C

Tag Type	Medium	Location	Success Rate (%)
Strip Tag	VHS in sleeve	center, high	100
Strip Tag	VHS in sleeve	center, middle	100
Strip Tag	VHS in sleeve	center, low	100
Strip Tag	VHS in sleeve	right, high	100
Strip Tag	VHS in sleeve	right, middle	100
Strip Tag	VHS in sleeve	right, low	90
Strip Tag	VHS in sleeve	left, high	100
Strip Tag	VHS in sleeve	left, middle	90
Strip Tag	VHS in sleeve	left, low	100

Orientation : Y (horizontal orientation of major strip dimension)

Tag Type	Medium	Location	Success Rate (%)
Strip Tag	VHS in sleeve	center, high	20
Strip Tag	VHS in sleeve	center, middle	10
Strip Tag	VHS in sleeve	center, low	10
Strip Tag	VHS in sleeve	right, high	0
Strip Tag	VHS in sleeve	right, middle	0
Strip Tag	VHS in sleeve	right, low	0
Strip Tag	VHS in sleeve	left, high	100
Strip Tag	VHS in sleeve	left, middle	10
Strip Tag	VHS in sleeve	left, low	100

Orientation : Y (vertical orientation of major strip dimension)

Tag Type	Medium	Location	Success Rate (%)
Strip Tag	VHS in sleeve	center, high	100
Strip Tag	VHS in sleeve	center, middle	100
Strip Tag	VHS in sleeve	center, low	100
Strip Tag	VHS in sleeve	right, high	90
Strip Tag	VHS in sleeve	right, middle	100
Strip Tag	VHS in sleeve	right, low	100
Strip Tag	VHS in sleeve	left, high	100
Strip Tag	VHS in sleeve	left, middle	80
Strip Tag	VHS in sleeve	left, low	100

Orientation : Z System C

Tag Type	Medium	Location	Success Rate (%)
Strip Tag	VHS in sleeve	center, high	100
Strip Tag	VHS in sleeve	center, middle	100
Strip Tag	VHS in sleeve	center, low	100
Strip Tag	VHS in sleeve	right, high	70
Strip Tag	VHS in sleeve	right, middle	50
Strip Tag	VHS in sleeve	right, low	70
Strip Tag	VHS in sleeve	left, high	100
Strip Tag	VHS in sleeve	left, middle	100
Strip Tag	VHS in sleeve	left, low	100

System D

Orientation : X System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM in case	center, high	0
DCD-2	CD-ROM in case	center, middle	0
DCD-2	CD-ROM in case	center, low	100
DCD-2	CD-ROM in case	right, high	0
DCD-2	CD-ROM in case	right, middle	0
DCD-2	CD-ROM in case	right, low	60
DCD-2	CD-ROM in case	left, high	0
DCD-2	CD-ROM in case	left, middle	0
DCD-2	CD-ROM in case	left, low	40

Orientation : Y System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM in case	center, high	0
DCD-2	CD-ROM in case	center, middle	0
DCD-2	CD-ROM in case	center, low	80
DCD-2	CD-ROM in case	right, high	0
DCD-2	CD-ROM in case	right, middle	0
DCD-2	CD-ROM in case	right, low	100
DCD-2	CD-ROM in case	left, high	0
DCD-2	CD-ROM in case	left, middle	0
DCD-2	CD-ROM in case	left, low	40

Orientation : Z System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM in case	center, high	0
DCD-2	CD-ROM in case	center, middle	0
DCD-2	CD-ROM in case	center, low	40
DCD-2	CD-ROM in case	right, high	0
DCD-2	CD-ROM in case	right, middle	0
DCD-2	CD-ROM in case	right, low	10
DCD-2	CD-ROM in case	left, high	0
DCD-2	CD-ROM in case	left, middle	0
DCD-2	CD-ROM in case	left, low	0

Orientation : X System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM, no case	center, high	0
DCD-2	CD-ROM, no case	center, middle	0
DCD-2	CD-ROM, no case	center, low	100
DCD-2	CD-ROM, no case	right, high	0
DCD-2	CD-ROM, no case	right, middle	0
DCD-2	CD-ROM, no case	right, low	40
DCD-2	CD-ROM, no case	left, high	0
DCD-2	CD-ROM, no case	left, middle	0
DCD-2	CD-ROM, no case	left, low	60

Orientation : Y System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM, no case	center, high	0
DCD-2	CD-ROM, no case	center, middle	0
DCD-2	CD-ROM, no case	center, low	100
DCD-2	CD-ROM, no case	right, high	0
DCD-2	CD-ROM, no case	right, middle	0
DCD-2	CD-ROM, no case	right, low	0
DCD-2	CD-ROM, no case	left, high	0
DCD-2	CD-ROM, no case	left, middle	0
DCD-2	CD-ROM, no case	left, low	20

Orientation : Z System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM, no case	center, high	0
DCD-2	CD-ROM, no case	center, middle	0
DCD-2	CD-ROM, no case	center, low	20
DCD-2	CD-ROM, no case	right, high	0
DCD-2	CD-ROM, no case	right, middle	0
DCD-2	CD-ROM, no case	right, low	40
DCD-2	CD-ROM, no case	left, high	0
DCD-2	CD-ROM, no case	left, middle	0
DCD-2	CD-ROM, no case	left, low	0

Orientation : X Stack of 5 CREM System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM in case	center, high	0
DCD-2	CD-ROM in case	center, middle	60
DCD-2	CD-ROM in case	center, low	0
DCD-2	CD-ROM in case	right, high	0
DCD-2	CD-ROM in case	right, middle	0
DCD-2	CD-ROM in case	right, low	0
DCD-2	CD-ROM in case	left, high	20
DCD-2	CD-ROM in case	left, middle	0
DCD-2	CD-ROM in case	left, low	20

Orientation : Y Stack of 5 CREM System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM in case	center, high	0
DCD-2	CD-ROM in case	center, middle	20
DCD-2	CD-ROM in case	center, low	0
DCD-2	CD-ROM in case	right, high	0
DCD-2	CD-ROM in case	right, middle	0
DCD-2	CD-ROM in case	right, low	60
DCD-2	CD-ROM in case	left, high	20
DCD-2	CD-ROM in case	left, middle	0
DCD-2	CD-ROM in case	left, low	0

Orientation : Z Stack of 5 CREM System D

Tag Type	Medium	Location	Success Rate (%)
DCD-2	CD-ROM in case	center, high	0
DCD-2	CD-ROM in case	center, middle	20
DCD-2	CD-ROM in case	center, low	0
DCD-2	CD-ROM in case	right, high	0
DCD-2	CD-ROM in case	right, middle	0
DCD-2	CD-ROM in case	right, low	0
DCD-2	CD-ROM in case	left, high	40
DCD-2	CD-ROM in case	left, middle	0
DCD-2	CD-ROM in case	left, low	0

Orientation : X System D

Tag Type	Medium	Location	Success Rate (%)
DVM-1	VHS in sleeve	center, high	20
DVM-1	VHS in sleeve	center, middle	60
DVM-1	VHS in sleeve	center, low	0
DVM-1	VHS in sleeve	right, high	20
DVM-1	VHS in sleeve	right, middle	20
DVM-1	VHS in sleeve	right, low	40
DVM-1	VHS in sleeve	left, high	0
DVM-1	VHS in sleeve	left, middle	20
DVM-1	VHS in sleeve	left, low	100

Orientation : Y System D

Tag Type	Medium	Location	Success Rate (%)
DVM-1	VHS in sleeve	center, high	0
DVM-1	VHS in sleeve	center, middle	0
DVM-1	VHS in sleeve	center, low	0
DVM-1	VHS in sleeve	right, high	60
DVM-1	VHS in sleeve	right, middle	20
DVM-1	VHS in sleeve	right, low	40
DVM-1	VHS in sleeve	left, high	60
DVM-1	VHS in sleeve	left, middle	100
DVM-1	VHS in sleeve	left, low	100

Orientation : Z System D

Tag Type	Medium	Location	Success Rate (%)
DVM-1	VHS in sleeve	center, high	60
DVM-1	VHS in sleeve	center, middle	60
DVM-1	VHS in sleeve	center, low	60
DVM-1	VHS in sleeve	right, high	0
DVM-1	VHS in sleeve	right, middle	0
DVM-1	VHS in sleeve	right, low	60
DVM-1	VHS in sleeve	left, high	0
DVM-1	VHS in sleeve	left, middle	100
DVM-1	VHS in sleeve	left, low	80

Orientation : Y Stack of 5 CREM System D

Tag Type	Medium	Location	Success Rate (%)
DVM-1	VHS in sleeve	center, high	0
DVM-1	VHS in sleeve	center, middle	40
DVM-1	VHS in sleeve	center, low	20
DVM-1	VHS in sleeve	right, high	0
DVM-1	VHS in sleeve	right, middle	0
DVM-1	VHS in sleeve	right, low	40
DVM-1	VHS in sleeve	left, high	100
DVM-1	VHS in sleeve	left, middle	40
DVM-1	VHS in sleeve	left, low	60

NOTE: Informed by the performance information for test configurations involving individual CREM , only evaluations in the Y orientation were conducted for stacks of 5 VHS tapes because this orientation was suspected of being the most performance-limiting.

Los Alamos
NATIONAL LABORATORY

Los Alamos NM 87545