



SYSTEM DESCRIPTION



May 1, 2005
Version 3.0

Table of Contents

A98 Overview..... 3

The Unique Key per ATM Problem 4

System Overview 4

System Description – The Comvelope™ Process 5

System Description – Remote Re-Key Process..... 5

Operational Flow 9

System Components..... 10

Register the ATMs..... 11

Enroll the Users 12

Prepare Comvelopes™ 13

Sample Printed Comvelope..... 14

Database Layout 15

Programming Architecture 16

Backup Services and Strategies 16

HDD Failures 16

Disaster Recovery A98 System Unit 16

Cryptographic Processing..... 17

 Generate Component 18

 Print Component..... 18

 Combine Components..... 18

 Generate Authentication Parameter..... 18

 Verify Authentication Code..... 18

Host Connection 19

Cryptographic Subsystem Description 20

 Overview 20

 Tamper Resistant Security Module..... 20

 Functional Control..... 21

 Secure Application Module 21

 Major Features 21

 Software Interface..... 22

 ESAPI 22

 RSAAPI 22

 Performance Specifications (CSA-7000) 22

Key Management 23

 Local System Users..... 23

 Public “User” 23

 System Administrators 23

 Key Custodians..... 24

 Master Key Generation..... 24

 Master Key Loading..... 24

 Key Encrypting Key Generation 27

 Key Encrypting Key Loading..... 27

 Key Encrypting Key Usage..... 30

 Comvelopes™ supplied by TSS to the Customer 31

A98 Overview

Trusted Security Solutions, Inc. was formed by Abraham & Associates, Inc. and J.S. Walker & Company, Inc. for the purpose of bringing unique security solutions to the transaction processing industry.

Abraham & Associates, Inc. located in Concord, North Carolina specializes in consulting services for the financial transaction processing industry with an emphasis on PIN based transactions.

J.S. Walker & Company, Inc. located in Charlotte, North Carolina specializes in providing consulting services and the development of automation solutions for financial institutions, insurance companies and related businesses.

Trusted Security Solutions, Inc. is offering the A98 ATM Initial Key Establishment System to institutions that manage the cryptographic keys for ATMs. For conventional ATMs, the A98 works with all ATMs, requires no hardware or programming changes to the ATMs and avoids the cumbersome requirements normally associated with compliant key management. Service personnel communicate with the A98 system via a touch tone telephone to establish the initial ATM keys in a manner which is fully compliant with the applicable ANSI standards and network operating rules. Once established, the initial keys are securely communicated to the host computer that drives the ATMs. All activity and events are securely logged and detailed reports provide concise audit trail information. For Remote Key ready ATMs, the A98 provides key transport using the Diebold (CBP) and NCR (SBP) protocols.

The A98 System is packaged in a standard 19" locking rack-mounted enclosure. All information is mirrored to a second hard drive under hardware control. Additional backup and recovery is available using an optional redundant A98 System Unit. The locked and pluggable hard drives are removed from the failing A98 System Unit and plugged into the redundant A98 System Unit to provide fast recovery.

For additional information concerning A98 or other products and services please contact:

Trusted Security Solutions, Inc.
416 West John Street
Matthews, NC 28105
(704)849-0036
info@trustedsecurity.com

The Unique Key per ATM Problem

ANSI Standard X9.24 – Retail Key Management requires each PIN encryption device to contain a unique key. Many organizations that drive ATMs mistakenly assume that downloading a unique key encrypted by a manually loaded key that is global in scope or is not secret is compliant with standard X9.24. However, the initial key must also be unique as well as secret. Providing a unique key per ATM is a particularly daunting task due to the complexity of the key management procedures traditionally employed. The secure distribution and storage of a unique key per ATM presents formidable challenges. Solutions employing public key cryptography have been proposed, but are not compliant with X9.24 and there are no changes planned to include such solutions. Using traditional methods of key management involving the control of individual key components requires large numbers of key custodians. The proposed solution described here avoids all of these problems and provides an easily implemented and non-intrusive method that has a minor impact on the currently installed system and infrastructure.

System Overview

Conventional ATMs - The A98 method of establishing a unique key per ATM avoids the management of a large number of key components for specific keys. Instead of generating a key and then splitting it into components or generating components and assigning the components to a specific key, the components are not assigned until the point at which the components are actually loaded into the ATM and are combined to form a unique key. A control number identifying each component is communicated to a Tamper Resistant Security Module (TRSM) where the identified components, stored encrypted by the Master Key of the TRSM, are combined within the TRSM to form the same key that was loaded into the ATM. The newly created key is immediately encrypted within the TRSM using a Key Encrypting Key shared with the host system to which the ATMs are connected. The encrypted ATM key is sent to the ATM host where it is loaded into the database defining the ATM and the cryptogram of the key in the ATM. When the "ATM Connect" message is received, the current ATM application software proceeds as normal to generate a PIN-encrypting key in two forms – encrypted by the newly loaded ATM key and encrypted by the Master File Key. Once the ATM connects to the system, processing proceeds in the normal manner. The only change required to the ATM host application is the addition of a module to receive the message containing the new key and mimic the operation of the current procedure where the cryptogram of the key is currently entered. This change is minor and does not impact mainstream processing.

Remote Key for Remote Key Ready ATMs - Building on the success of the A98 platform, Trusted Security Solutions has released its "Remote Re-Key" module. For public key enabled ATMs, the A98 will fully automate key generation and distribution, eliminating the need for manual key loading. The A98 is the only system providing efficient, compliant, and comprehensive key management simultaneously for both legacy ATM's and new ATM's with Remote Re-Key enabled EPP's.

The A98-R implements both Diebold's Certificate Based Protocol (CBP) and NCR's Signature Based Protocol (SBP) that are defined in the emerging ANS X9.24-2 Standard on Retail Cryptographic Key Management. The Diebold approach uses X.509 certificates and PKCS message formats to transport key data. NCR's method, Signature Based Protocol (SBP), relies on digital signatures to ensure data integrity. In lieu of PKCS message formats, SBP information is transported in simple data structures. Both processes require the ATM's EPP to be loaded at the factory with signed Public Keys or Certificates. In addition, an A98 public key must be signed by a Certificate Authority (i.e. Diebold or NCR) and imported back into the A98 during system initialization.

The A98 Remote Re-Key module, implements an XML interface to the terminal handler or device driver. Trusted Security Solutions has defined the XML DTD that is used to communicate with the driver over a TCP/IP link. This approach confines modifications to the ATM device driver and eliminates any need to change the host security module or terminal driving application software. All the public key cryptography, message formatting, database access, and user interface programming is provided in the A98 Remote Re-Key module.

System Description – The Comvelope™ Process

The System Overview is shown in Figure 1 – System Overview. Random Numbers are generated and sealed in control numbered security envelopes very similar to PIN mailers. A unique control number is printed inside the PIN mailer. Each random number is encrypted under the A98 Master Key and stored in an Access2000 database indexed by the control number for future retrieval. The envelopes are distributed to the bank employee at the branch office closest to the ATM and the ATM service personal. Alternatively, the envelopes may be stored with each ATM for future use. Each key custodian or key component loader is assigned a unique UserID and an initial access code similar to a PIN. Each user can manage his own access code and is required to change it during his initial log-on. Each ATM is assigned a unique terminal ID. Customer supplied electronic reports from the current system can be used to provide the UserIDs and Terminal Ids to the A98 System.

The rack mounted A98 System Unit installed at the customer location, holds a database of the random numbers, UserIDs and ATM IDs. The A98 System Unit contains an Eracom cryptographic adapter along with a voice response card. A network adapter card is used to connect the A98 System Unit to the ATM host system and a Key Encrypting Key (KEK) is shared, using manual key management, with the host system driving the ATMs.

To establish an initial key in an ATM, each key loader selects an envelope at random and loads the contents of the envelope into the ATM following the instructions of the ATM manufacturer. He then calls the A98 System Unit's voice response unit using any touch-tone telephone. The user is invited to enter his UserID and if valid, is invited to enter his access code for verification. Once verified, the user identifies the ATM and selects the desired function. The control number of the selected random number is entered and the database entry indexed by the control number and is marked as being entered into the identified ATM. The second random number loaded into the ATM and the identification process is repeated for user number 2. The two random numbers are combined inside the TRSM cryptographic adapter to form an initial key and this key is encrypted under the shared KEK. The cryptograms and terminal ID are sent to the host using the network adapter and ISO-8583 messaging protocol. The host enters this cryptogram into the ATM database and marks the ATM as ready for initialization. The host reports successful processing of the ATM key cryptogram to the A98 using the A98 message formats and ISO-8583 messaging protocol. When the ATM then connects, the application program requests a new PIN encryption key be created by the host security module and sent to the ATM. The result is the ATM now has a unique initial key installed without the problems of managing key components. The two random numbers are discarded and not reused. No record of the newly created ATM key is maintained on the A98 System Unit. The newly created ATM key exists only encrypted by the shared KEK and encrypted by the ATM host MFK. The cryptogram of the newly created key under the KEK may be erased as soon as the key has been encrypted under the MFK on the ATM host and a confirmation message is received from the host.

Note: In reality, each envelope contains two random numbers to be entered into the ATM. One is used as a component of the A-Key and the other is used as a component of the B-Key.

System Description – Remote Re-Key Process

With the introduction of its new "Remote Re-Key Module", A98-R automates both the generation and distribution of cryptographic keys for ATMs. A98-R is compatible with ATMs that use RSA-enabled encrypting pin-pads (EPPs). The A98-R delivers random master keys in full compliance with ANSI standards and with network mandates for Triple-DES and unique keys per ATM. The A98-R implements both Diebold's Certificate Based Protocol (CBP) and NCR's Signature Based Protocol (SBP) that are defined in the emerging ANS X9.24-2 Standard on Retail Cryptographic Key Management. The Diebold approach uses X.509 certificates and PKCS message formats to transport key data. NCR's method relies on digital signatures to ensure data integrity. Both processes require the ATM's EPP to be loaded at the factory with signed Public Keys or Certificates. In addition, an A98 public key must be signed by a Certificate Authority (i.e. Diebold or NCR) and imported back into the A98 during system initialization.

The remote re-key process requires the A98 to be authenticated by the ATM. In this step either the signed A98 public key or its certificate is sent from the A98 to the ATM. Once verified, the ATM will send its EPP public key to the A98.

(In the case of Diebold, both an encryption and verification EPP public key is sent.) The A98 stores the EPP data and then generates a new DES key, encrypts it with the EPP's public key, prepares the required message format, and sends this new master key to the ATM. When the EPP responds that it successfully loaded the key, A98 sends a cryptogram of this new key to the host for loading into the terminal data base.

In the initial release of the A98 Remote Re-Key module, the interface to the ATM will be implemented through the terminal handler or device driver. Trusted Security has defined an XML data structure that will be used to communicate with the driver over a TCP/IP link. This approach confines modifications to the ATM device driver and eliminates any need to change the host security module or terminal driving application software. All the public key cryptography, message formatting, database access, and user interface programming is provided in the A98 module. By integrating the remote re-key module into the conventional A98 platform, Trusted Security continues to lead the industry by providing the most efficient, compliant, and cost-effective key establishment solution for all ATMs. The A98-R system not only fully automates key distribution for public key-enabled ATMs, but also continues to support single- and triple-DES key loading for legacy ATMs.

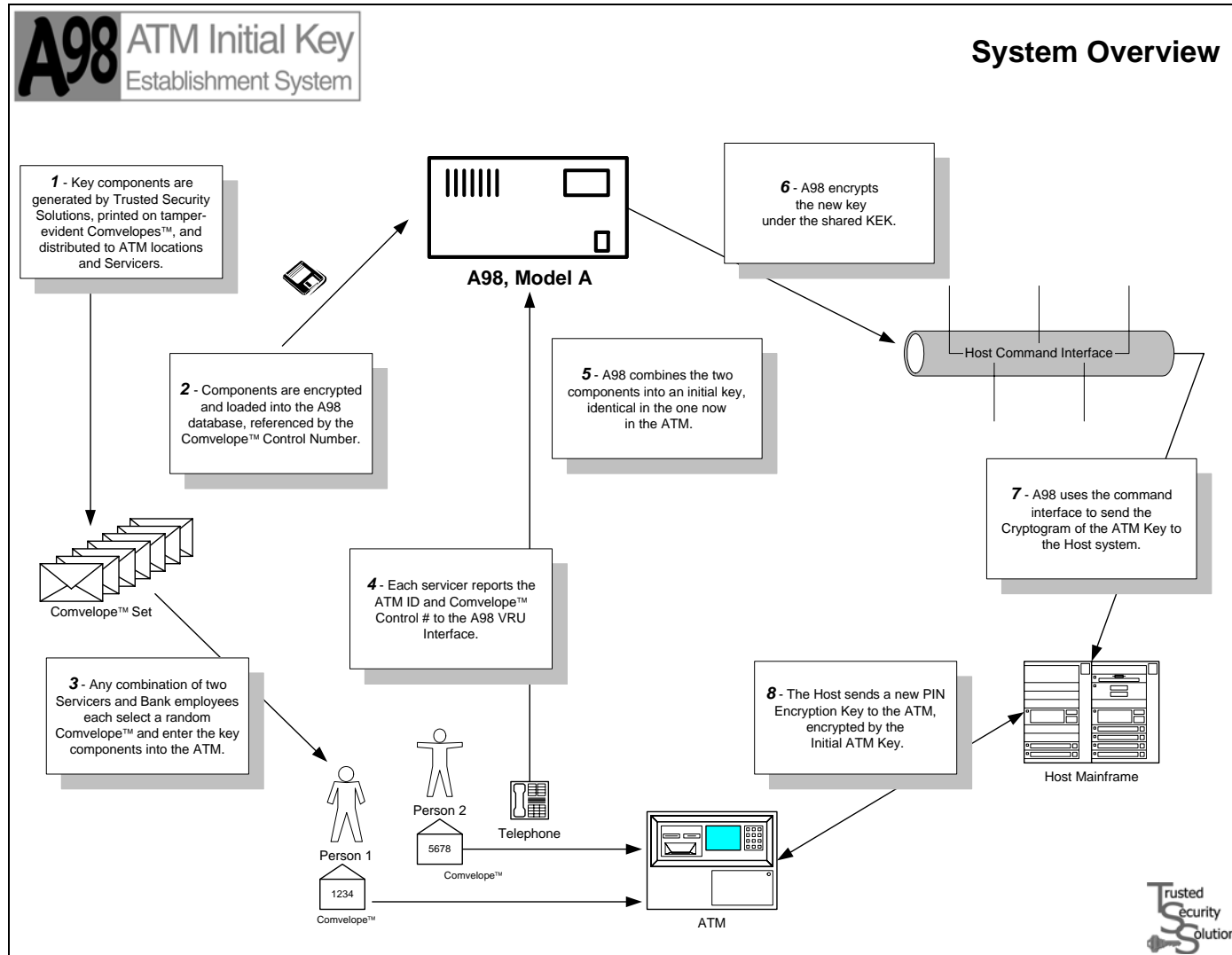


Figure 1 – System Overview



Operational Flow

The operational Flow is shown below. Two users randomly select envelopes containing the previously generated random numbers and enter them into the ATM as key components. The users then identify themselves to the system and the components are joined together to form the A-Key and B-Key just loaded into the ATM.

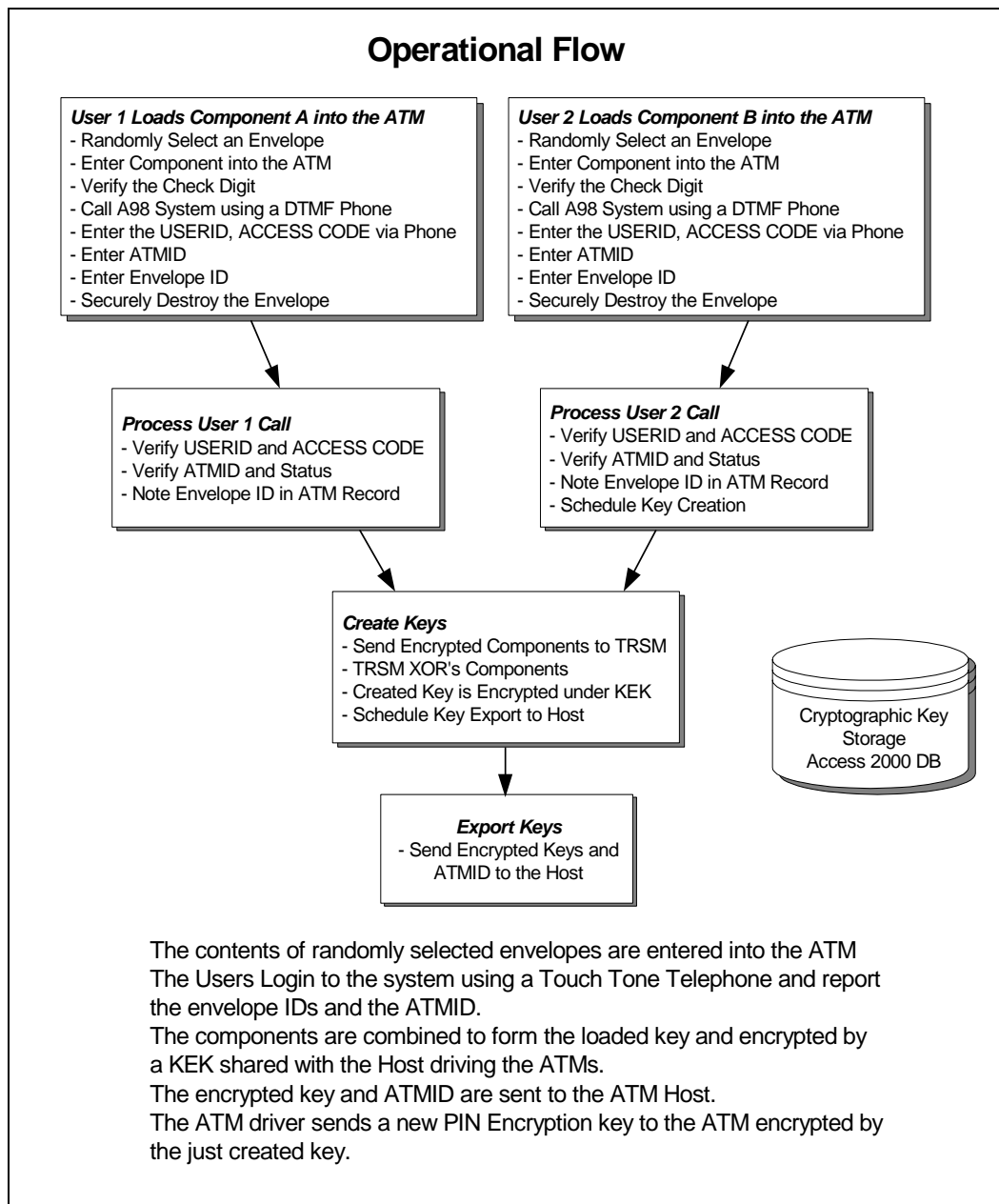


Figure 2 – Operational Flow

System Components

Hardware – A98 System Unit – Pentium 4, 2 x 20 G HDD, Network Interface Card, Voice Response Adapter, Eracom Cryptographic Adapter. An optional Lexmark 2490 forms printer can be attached to the Cryptographic Adapter for printing locally used cleartext keying material and passwords.

A98 Software – Windows 2000, Access, Custom programming, Cryptographic Adapter support.

Host Software – Customer supplied programming is required on the system to receive the cryptogram of the key and the ATM ID, add it to the host ATM database, and send a response back to the A98.

Packaging – System delivered as a total rack mounted package including the A98 unit, programming, installation and enough component envelopes for 1000 ATMs and up to 1000 UserIDs.

Models – The A98 is deliverable to support as low a 30 ATMs and as high a number of ATMs as 52,000. The number of phone lines configurable to the A98 is between one and 24 (T1 access). A DR unit (Disaster Recovery) is available. The Database from a failing unit is transferred to the Disaster Recovery unit.



Register the ATMs

Each ATM is assigned a unique Identifier – could be 4 digits – and “enrolled” in the database. The data base entry describes the ATM and contains any overrides of the global configuration parameters. For example, if the telephone used to report the Comvelope has CallerID, should it be checked and what action to take on the result of the check. ATM enrollment is accomplished via a customer supplied text file. This file could be created from a report generated using the existing ATM host database. (e.g. – the TDF of BASE24).

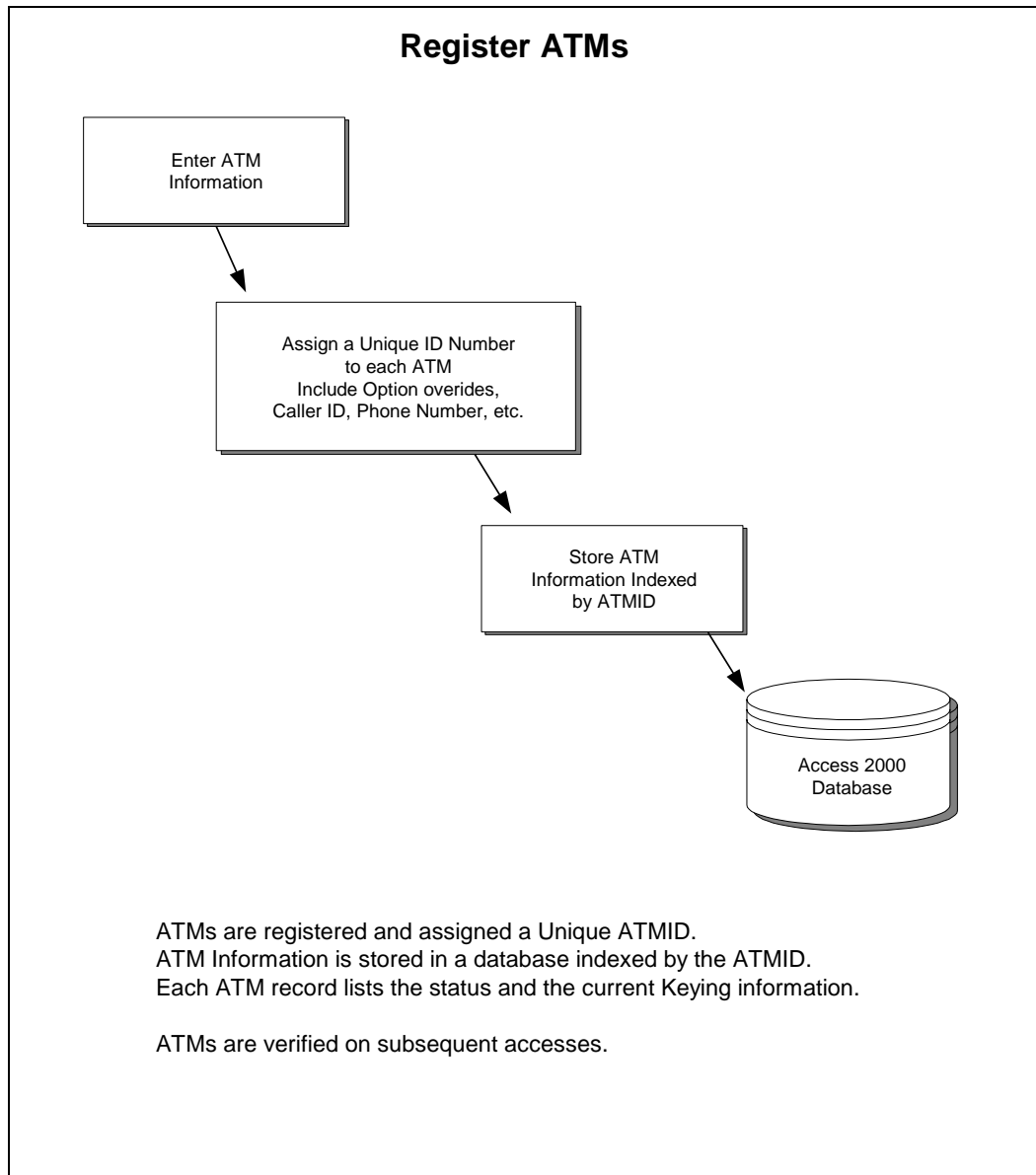


Figure 3 – Register ATMs

Enroll the Users

Each user is enrolled in the system and assigned a unique identifier. An initial access code is assigned which the user must change. Users are assigned roles as Administrative, Technician, Audit, etc.

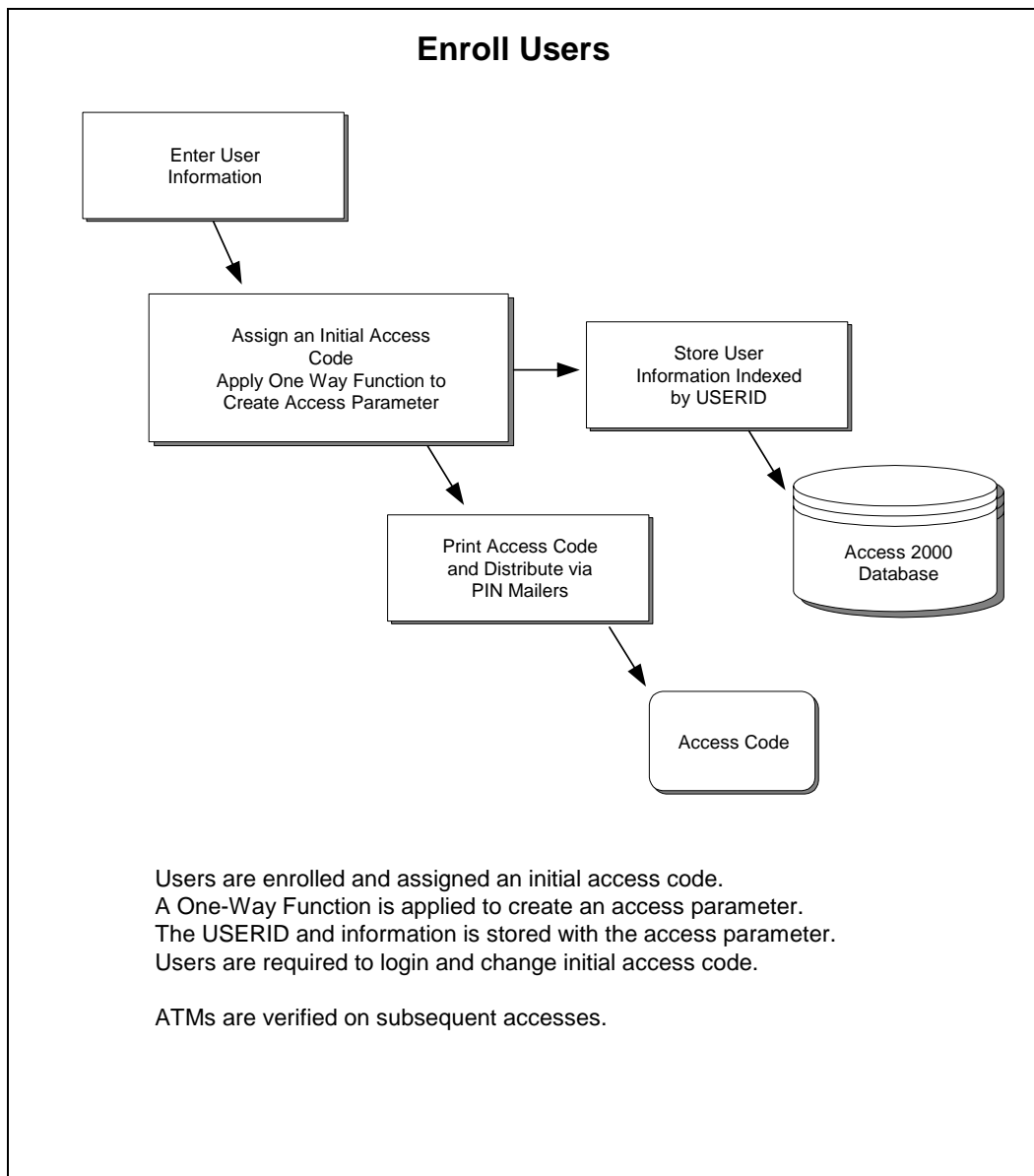


Figure 4 – Enroll Users

Prepare Comvelopes™

Random Numbers are generated and printed in the PIN mailer to serve as candidate key components. The envelopes are then distributed. There is no danger of an opponent opening an envelope to learn its contents for the purpose of defrauding the system. Users are instructed not to use tampered envelopes.

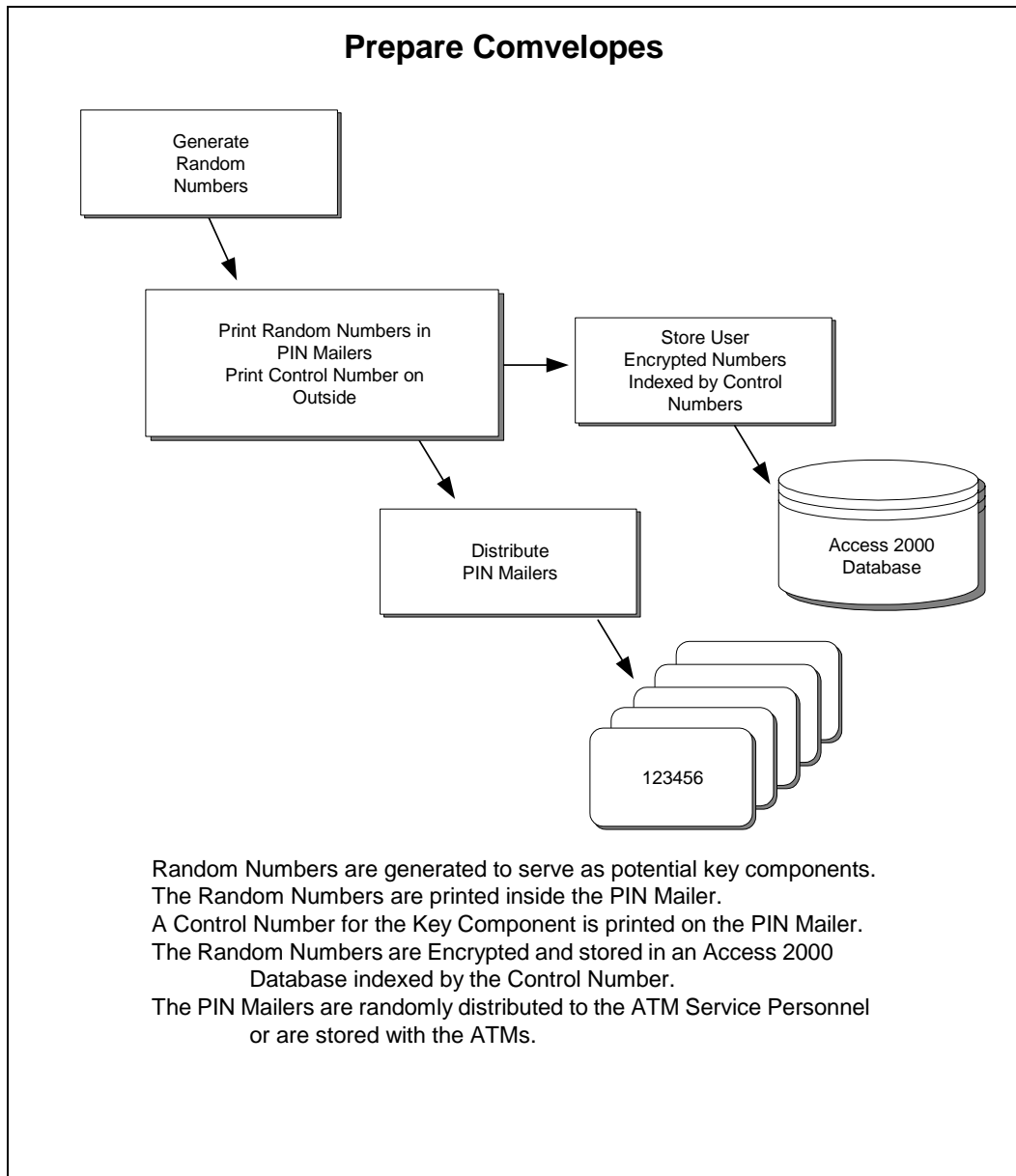



Figure 5 – Prepare Comvelopes

Sample Printed Comvelope

A sample of the printed key components printed inside of Comvelope is shown below in Figure 6. After the information is printed on the form, it is "Z" folded and sealed so that only the lower panel is visible. The value of the components and the control number are not visible through the envelope even under a bright light. Users are instructed not to use tampered envelopes.

Enter Components (below) Sign, Date and Return

Confirm Key Check Value (KCV)

Call (704) 849-0036
 Enter Your Servicer ID and Access Code _____
 Enter This ATM's ID _____
 Enter Comvelope ID 001 1002 000


Signature _____ Date _____
 Witness _____ Date _____
 Witness _____ Date _____

For technical support call: (704) 849-0036
 1999 Trusted Security Solutions, Inc.

Triple DES
 16-Character Key
 8-Character Key

A-KEY: B3 29 49 1F 70 75 C4 32 KCV: E0 1A B7

B-KEY: 89 E3 3B 20 AB 5D CB E0 KCV: DE 11 B6

TRIPLE DES KCV: A2 54 DA

Figure 6 - Sample Print of Triple DES Component Envelope

Database Layout

The Access 2000 database contains all the data defining the system. There is no sensitive information exposed in the database. All components and keys are encrypted. User Access codes are cryptograms obtained from one-way functions and cannot be hacked or used to gain access. Components are encrypted and remain unknown to an opponent.

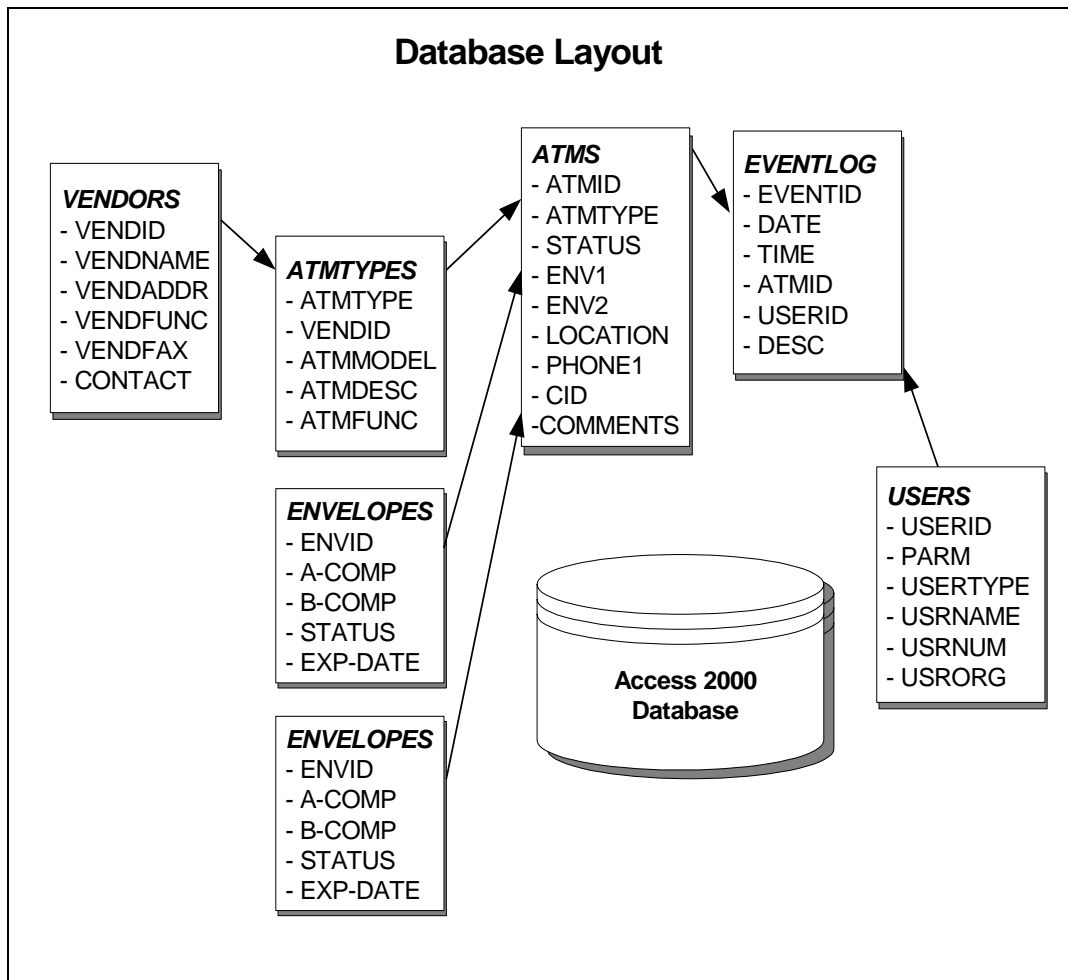


Figure 7 – Database Layout

Programming Architecture

The A98 system employs the Windows 2000 Operating System. Custom Access 2000 Database, Communications, cryptographic subsystem and all initialization programming are written in C++ 6.0 and Visual Basic 6.0 to run under Windows 2000.

Backup Services and Strategies

HDD Failures

All models of A98 incorporate hardware disk mirroring facilities. The primary and mirrored disks contain an exact duplicate of each other. In the event of a HDD failure, an audible alarm sounds. A98 automatically continues operations using the non-failing HDD. The current mirroring hardware does not currently support a hot swap. Recovery consists of stopping the system and powering it down. The damaged HDD is replaced. The system is then rebooted and restarted. Hard drive is recovered in approximately 1:30 minutes, by a system process.

Disaster Recovery A98 System Unit

Multiple system discount pricing is available to provide A98 System owners with the option of having one or more standby A98 Systems. The optional A98 Standby System is sold at a reduced price and does not include Hard Disk Drives (HDDs) containing the system programming and database. For the case where the processor or the internal power supply failed, the locking and front-panel-removable HDDs are physically removed from the failing system and moved over to the standby system. If not already connected, the telephone lines and network connection are moved from the failing system to the standby system. The Boot Password for the standby A98 System is stored in a tamper evident package so the second system cannot be used without opening the password envelope. To start the second system, transfer the HDDs from the primary system to the second system, retrieve the boot password to start the system. No changes are required to be made to the setup information. Depending on the nature of the failure, the failing A98 System Unit is either returned to TSS for repair or it is repaired on the customer premises. Once repaired, the boot password is changed and placed in a tamper evident envelope. The repaired system then becomes the backup system.

Cryptographic Processing

Cryptographic processing requires six basic functions:

1. Generate Component
2. Print Component
3. Combine Components
4. Generate Authentication Code
5. Verify Authentication Code
6. Key Management and Support

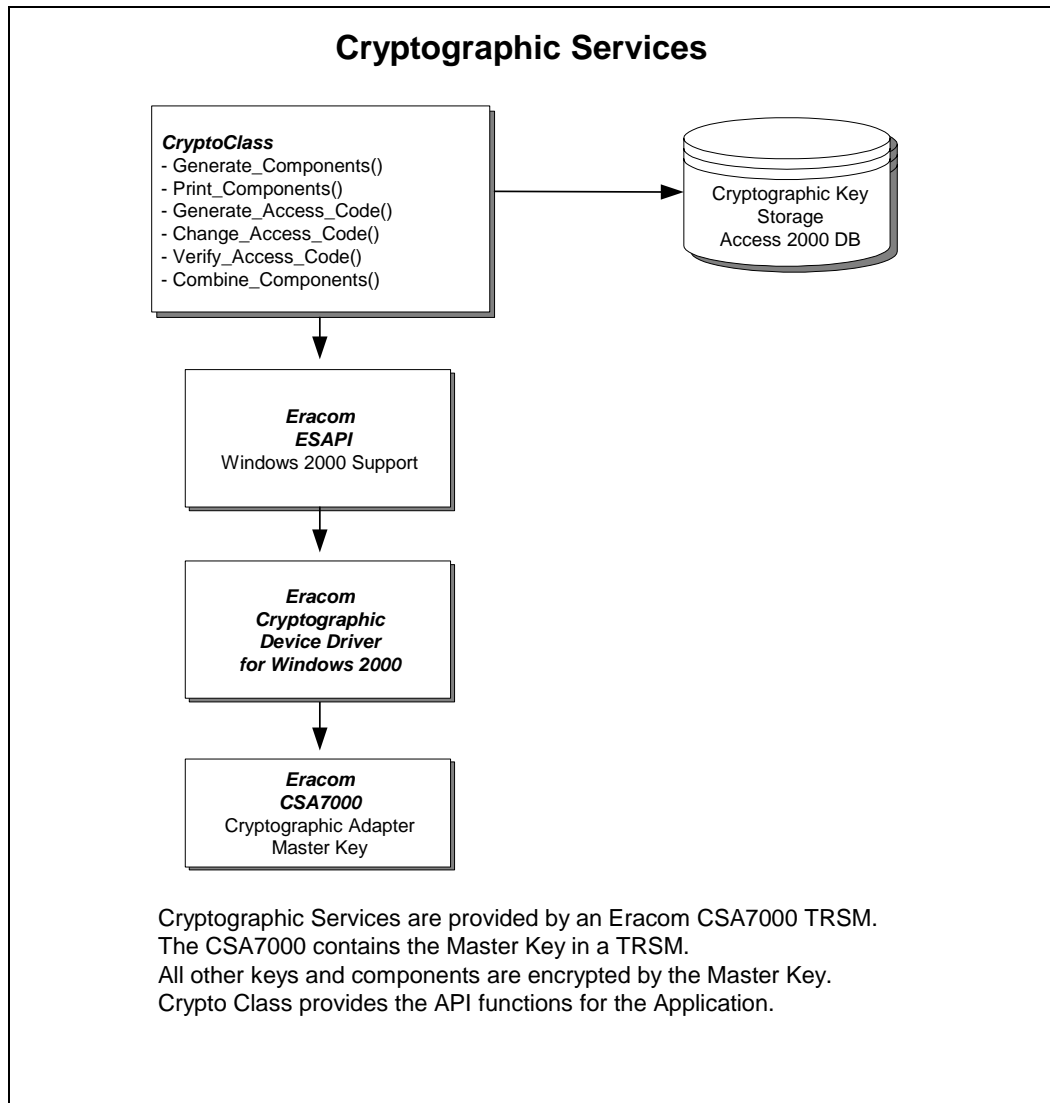


Figure 8 – Cryptographic Services

Generate Component

Description - Generate Component requires an encrypted 16 byte data key as an input argument and returns an 8-byte odd parity adjusted random number encrypted under the double length data key.

Input – A 16 byte data key encrypted by the Master Key.

Output – An 8-byte odd parity random number encrypted under the privacy key.

Print Component

Description - Print Component requires as input an encrypted 16 byte data key, a component encrypted by the data key and a cleartext component ID. The Print Component function is restricted and requires password activation by two key custodians from two separate groups of key custodians - e.g. KCA_PRI and KCC_SEC .

Input – A 16 byte data key encrypted by the Master Key; the component encrypted by the data key and a component ID to be printed on the envelope for identification purposes.

Output – The cleartext component is printed inside a PIN mailer privacy document and the component ID is printed on the outside of the envelope. The printed documents are emitted face down from the printer and are moved to the pressure sealer for closure. The documents remain under dual control until they are sealed.

Combine Components

Description - Combine Components requires as input two encrypted 16 byte data keys, two pairs of A and B components each pair encrypted by one of the data keys and an encrypted Key Encrypting Key (KEK) previously shared with the host system.

Input – Two data keys encrypted by the Master Key; two pair of encrypted A and B components, each pair encrypted by one of the data keys, a Key Encrypting Key encrypted by the Master Key and a control parameter describing the format of the components – i.e. 8 characters or 16 characters in length.

Output – The cleartext component is decrypted using data key A and is recovered inside the cryptographic adapter. They are combined by exclusive or for the 16 character components or concatenated together for the 8 character halves as directed by the control parameter and the resulting key encrypted by the KEK shared with the host system.

Generate Authentication Parameter

Description - Generate Authentication Parameter requires as input a UserID and a cleartext Authentication Code and returns an Authentication Parameter related to the Authentication Code and the UserID to be used the Verify Authentication Code.

Input – A cleartext UserID and a cleartext Authentication Code. Note that the term Authentication Code is preferred to be used in place of Personal Identification Number (PIN).

Output – The Authentication Parameter is formed by forming the UserID into an 8-byte quantity and encrypting it using the Authentication Code formed into an 8-byte quantity as a key. The result of the encryption is exclusive or'd with the cleartext input to decouple the result from the Authentication Code.

Verify Authentication Code

Description - Verify Authentication Code requires as input a cleartext UserID and a cleartext Authentication Code and a cleartext Authentication Parameter. It recalculates the Authentication parameter and compares it for equality with the input Authentication Parameter. Only a Yes/No result is returned.

Input – A cleartext UserID and a cleartext Authentication Code is a cleartext Authentication Parameter.

Output – A Yes/No response is developed by recalculating the Authentication Parameter and comparing it for equality to the input Authentication Parameter.

Host Connection

Connection to the host that drives the ATMs is via a TCP/IP connection. The following host connection options are being used by A98 customers and are currently available either from Trusted Security or the host software provider. These interfaces provide a fully-automated A98 solution:

- ACI BASE24® (Tandem platform)
- Mosaic Postilion® (PC-platform)
- eFunds Connex® (Tandem platform)
- CV Systems (IBM® mainframe platform)
- S2 ON/2 and OpeN/2 (Stratus platform)
- ACI/SDM OCM24® (IBM® mainframe platform)
- Other proprietary platforms

NOTE: An automated interface is NOT REQUIRED to utilize all the features of A98. Key updates can be retrieved using the Host Proxy Application and manually entered into host ATM terminal database.

Cryptographic Subsystem Description

Overview

The A98 Tamper Resistant Security Module (TRSM), is implemented using the Eracom CSA-7000 Intelligent Cryptographic Adapter. Eracom Pty. Ltd is headquartered in Burleigh Heads, Queensland, Australia. Eracom products are used widely in Australia, New Zealand, the Pacific Rim and throughout Europe. The component side of the CSA-7000 PCI adapter card is protected by a metal cover that is soldered in place. The wiring side of the card is protected from probing by an epoxy coating.

Keys and other sensitive information are stored in a battery backed up RAM. Removal of the card from its socket causes the immediate erasure of the contents of the battery backed up RAM. Additionally, the A98 implements tamper detection circuitry that is connected to the CSA-7000. Activation of the A98 tamper detection circuitry causes the immediate erasure of the contents of the battery backed up RAM on the CSA-7000.

The following information is excerpted from the Eracom product descriptions on the Eracom Web Page.

Tamper Resistant Security Module

The CSA-7000 Intelligent Cryptographic Adapter is shown in Figure 9. The ERACOM CSA-7000 is an intelligent adapter capable of providing a wide range of cryptographic services for IBM compatible Personal Computers using a PCI bus (CSA-7000). As an order time option, it may also contain circuitry specifically designed for exponentiation processing to speed up asymmetric cipher operations for up to 2048-bit modulus arithmetic.

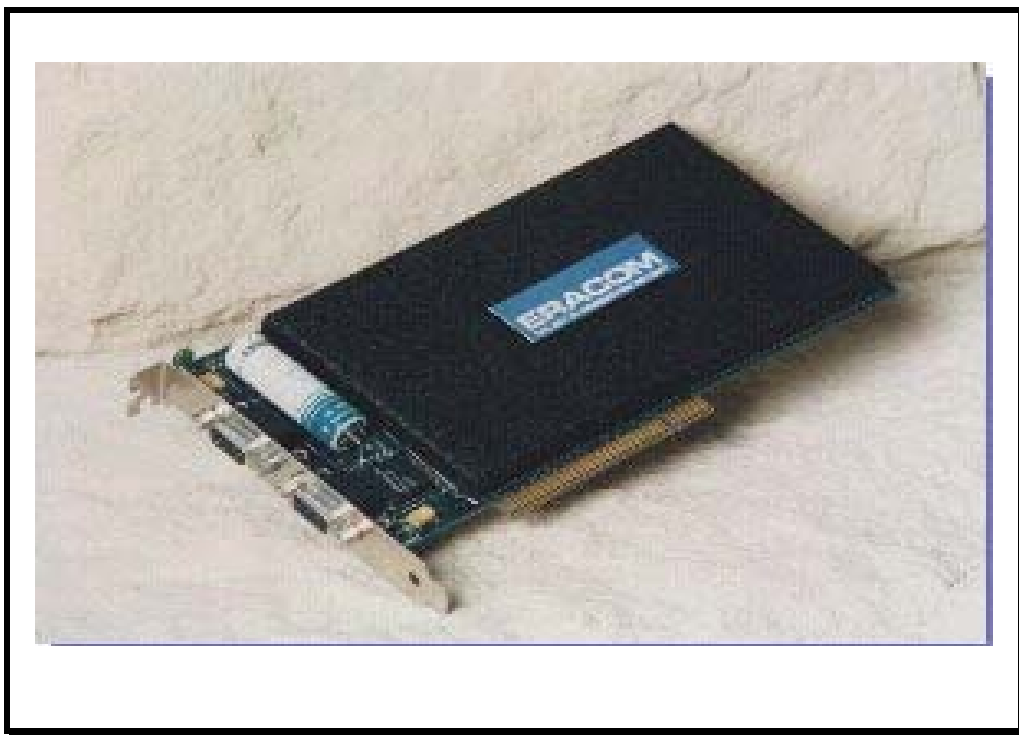


Figure 9 – Eracom CSA-7000 Cryptographic Adapter

Functional Control

The Encryptors' microprocessors have unrestricted access to all on-board hardware features. For security reasons the host system's microprocessor does not have this privilege. Instead, it must gain access to on-board facilities and services by making requests through the on-board processor that arbitrates the level of access allowed.

Secure Application Module

Although the standard on-board software provides an extensive suite of functions these may not always meet the needs of individual users. To cater for such situations, custom functions in the form of a Secure Application Module (SAM) can be loaded in a strictly controlled manner. These SAMs are either down-loaded each time the board is powered up or can be stored in an on the board flash memory module. In either case, the SAM is provided encrypted and digitally signed by the issuing authority to ensure secure and safe operation.

Major Features

- Intel's on-board microprocessor and associated on-board control software.
- A Triple DES Data Ciphering Processor supporting both single and double length keys. (Support for true triple length keys is available via an ERACOM provided SAM).
- RSA support with optional RSA hardware accelerator. Key lengths up to 2048 bits are supported.
- Tamper resistant, battery backed memory for the storage of sensitive data (32 Kbytes).
- Real Time Clock.
- Two local asynchronous communications ports. Access to these ports by the host system processor is only available via a SAM. Possible uses would be the attachment of Smart Card Readers or other peripheral hardware
- PCI bus Master mode (DMA) operation to perform fast DES and Triple DES encryption to and from memory independent of the host processor.

Software Interface

Two Application Programming Interfaces (APIs) are available to allow application software to make use of the adapter's services. Both consist of a range of 'C' language functions which are operating system independent. They support Microsoft 'C' (versions 5 and 6), Borland Turbo 'C' (version 3.0) and IBM C Set++ source languages and calling conventions. Other compilers which accept Microsoft object libraries should be compatible.

ESAPI

Provides support for Triple DES functions and secure memory access and is currently available for OS/2 2.x and higher, Windows 3.x, Windows NT, Windows 2000, SCO UNIX 4.1 and MS-DOS environments on IBM PC compatible systems.

RSAAPI

Provides support for RSA functions and is currently available for OS/2 2.x and higher, Windows 3.x, Windows NT, Windows 2000, SCO UNIX 4.1 and MS-DOS environment on IBM PC compatible systems.

The same source code will work with all forms of these APIs without modification. They are reentrant at the process and thread levels on operating systems where this is supported.

Performance Specifications (CSA-7000)

- DES encryption of over 3.5 Megabytes per second is possible using the adapter in PCI Slave mode, whereas encryption rates of up to 17 Megabytes per second are achievable in Master mode.
- 512 bit RSA key pair generation takes on average less than 7 seconds ('Safe' AS2805 mode - faster rates are possible if less comprehensive prime testing is required on key components).
- 768 bit RSA key pair generation takes on average less than 9 seconds.
- Public key encipherment takes 3 ms for keys up to 1024 bits.
- Private key encipherment takes 18-23 ms for 512 bit keys, 39-48 ms for 768 bit keys, and 68-84 ms for 1024 bit keys.

	512 bit	768 bit	1024 bit
Public Key	<3 ms	<3 ms	<3 ms
Private Key	18-23 ms	39-48 ms	68-84 ms

Note: Times quoted are for an adapter fitted with RSA accelerator hardware. More detailed performance specifications are available on request.

Key Management

Local System Users

In addition to the technicians that use the component envelopes to load keys into the ATMs, the A98 architecture provides for nine role based local users to provide for segregation of system management responsibilities. At installation time, each user creates an 8 character (A-Z, 0-9) password that the user manages. Each pair of custodians in a role i.e. KCA_PRI and KCA_SEC can reset the password of the other, for example for the situation where a password is forgotten. If the user password is reset by the other role within the group for some reason, the user must change the password the first time the user logs onto the A98 system before the user is permitted to exercise their normal roles.

-USERID-	Role Description.
PUBLIC	Normal state when no user is logged on.
ADMINPRI	The Primary System Administrator.
ADMINSEC	The Secondary System Administrator.
KCA-PRI	The Primary Key Custodian for Component A.
KCA-SEC	The Secondary Key Custodian for Component A.
KCB-PRI	The Primary Key Custodian for Component B.
KCB-SEC	The Secondary Key Custodian for Component B.
KCC-PRI	The Primary Key Custodian for Component C.
KCC-SEC	The Secondary Key Custodian for Component C.

Public "User"

The Public User is logged on when no other local user is logged onto the A98. This is the normal state A98 and most of the time the A98 will be in the PUBLIC user state. In this state, none of the critical key management functions are available.

System Administrators

Two system administrators, a primary and a secondary, are defined. The system administrators cannot execute any of the key management functions that deal with cleartext key components. Their function is system maintenance in the form of user management and log keeping. The administrators can add new users, both local and remote, block and unblock UserIDs etc. Either administrator can perform all the duties of the other. Log entries are kept for every system administrator action. Additionally, the administrators keep the access logs and combination of the Rhino2 Safe in which the three Sentry lock-boxes managed by the key custodians are stored. The system administrators also manage the appropriate logs for the various key management activities.

Key Custodians

The A98 architecture provides for three pairs (a primary and a secondary) of key custodians. Each pair of key custodians are charged with managing one of the three components of the Master Key and any Key Encrypting Keys exchanged with systems with which the A98 cryptographically communicates. The pair of key custodians co-manage a Sentry lock-box in which is stored their respective component of any keys they manage. The primary key custodian and the secondary key custodian each have an identical key to the Sentry lock box they jointly manage. Either key custodian can exercise all the duties within the scope of the group. Within this document, a reference to key custodian A is intended to mean either the KCA-PRI or KCA-SEC roles. Similarly for the other two key custodian roles.

A special case exists for the printing of the ATM key components. For this case, two key custodians, each from a separate pair e.g. KCA-SEC and KCC-PRI, or KCB-PRI and KCC-PRI etc., must enter their logon passwords.

Master Key Generation

The A98 uses a unique double length master key. The A98 master key may be generated by the A98 system or generated by a process external to the A98 system. The double length master key is managed by three 32 character printed components. The A98 includes a master key generation utility.

The Master Key Generation Utility requires each key custodian in turn to logon. The Lexmark 2490 Forms Printer attached to the CSA-7000 is loaded with PIN mailer forms (Moore catalog number K13715). Alignment forms can be printed and the printer/form combination adjusted until an acceptable alignment is achieved. The first 32-character key component and component check value is then generated and printed into the PIN mailer. Key custodian B is invited to logon and the second key component is generated and printed into the PIN mailer. The third key component is printed after key custodian C has been invited to logon. The three key custodians remove the PIN mailers from the printer and each assumes control of their particular PIN mailer containing their component. The outside of the PIN mailer clearly indicates which mailer contains which component. Each key custodian stores their PIN mailer in their respective Sentry lock-box. The lock-boxes are then stored in the Rhino2 Safe. The key generation event is logged by the key administrator and the safe is locked by the key administrator.

All the events are logged within the CSA-7000, and on the A98 log. The Master Key Generation process is shown in Figure 10.

Master Key Loading

Loading of the A98 Master Key is accomplished using the Master Key Loading Utility available on the user interface.

After the key administrator opens the Rhino2 Safe, the three key custodians assume custody of their respective Sentry lock-boxes. The Master Key Loading Utility requires each key custodian in turn to logon. Each key custodian enters their 32 character key component via the A98 system keyboard twice and compares the displayed component check value with the correct component check value provided by the PIN mailer. After key custodian C has entered the final key component, the key check value for the newly loaded master key is displayed and entered into the key loading log by the key administrator. The other key custodians verify the correct key check value has been recorded. Each key custodian places their respective paper copy of their key component into a tamper evident and serial numbered security bag and seals the bag. The Block and Company, Inc., Wheeling, IL catalog number 136-1080-06 is particularly suited for this purpose. The key custodian removes the tag containing a duplicate of the bag serial number and the number is recorded in the key loading log by the key administrator. The sealed bags are then locked into the respective Sentry lock-boxes and the lock-boxes returned to the Rhino2 Safe. The key administrator makes the appropriate log entries.

All the events were logged within the CSA-7000, and on the A98 log. The Master Key Loading process is shown in Figure 11.

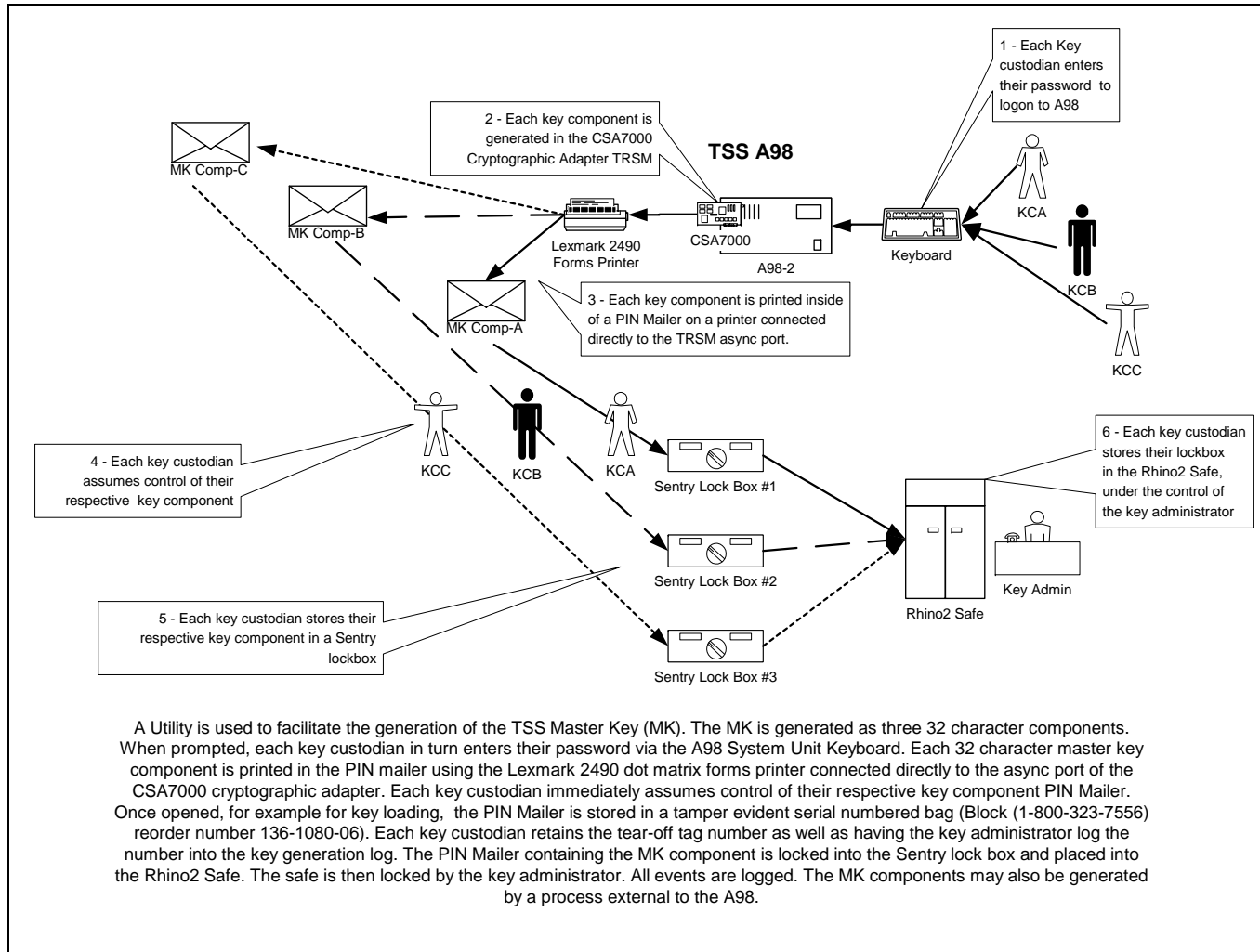


Figure 10 – Master Key Generation

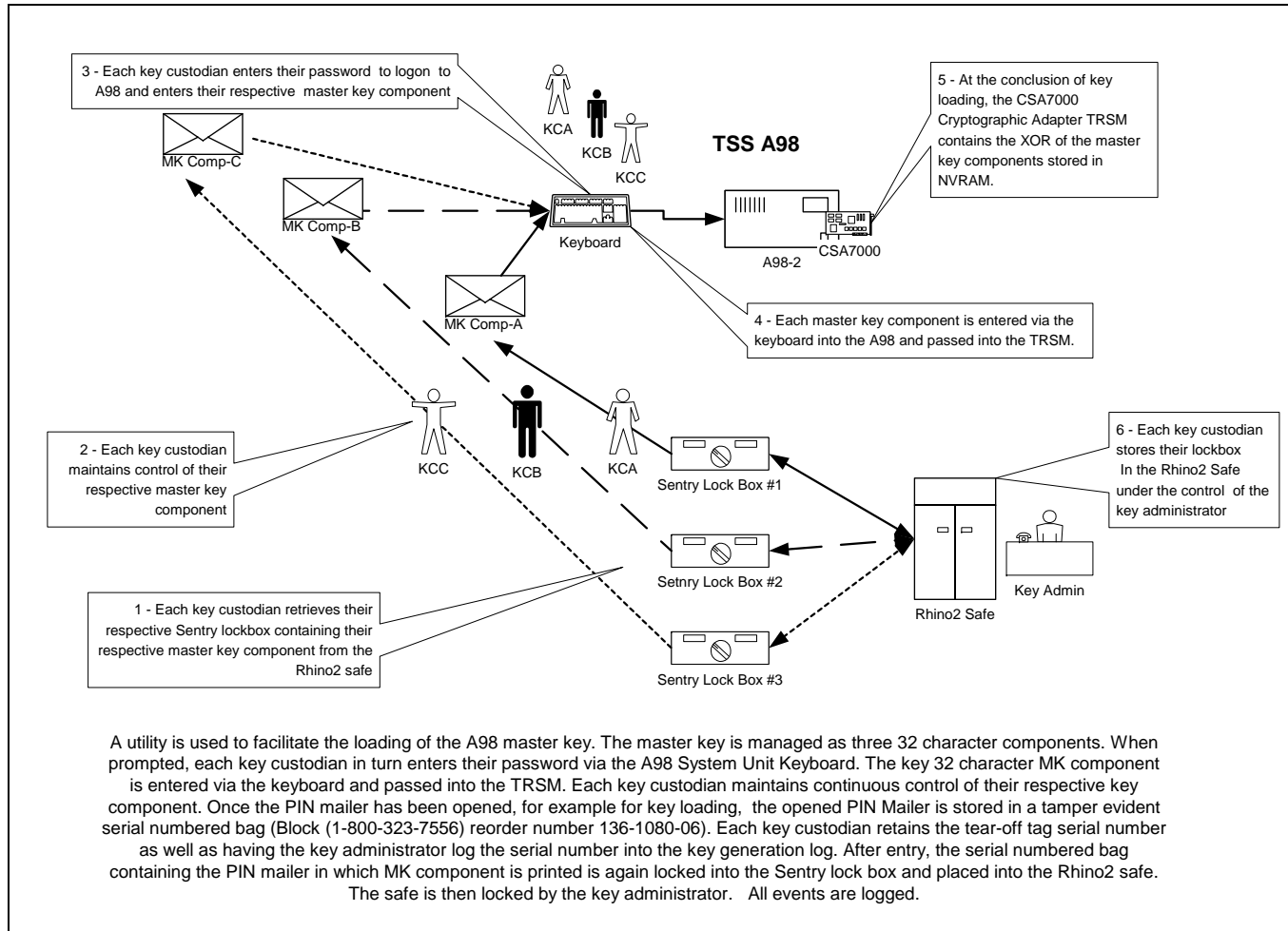


Figure 11 – Master Key Loading

Key Encrypting Key Generation

The A98 manages Key Encrypting Keys (KEK) as three 32-character components. Key Encrypting Keys may be generated by the A98 system or generated by a process external to the A98 system. The A98 includes a KEK generation utility function available on the A98 user interface during normal operations.

Both KEK Generation functions require each key custodian in turn to logon. The Lexmark 2490 forms printer attached to the CSA-7000 is loaded with PIN mailer forms (Moore catalog number K13715). Alignment forms can be printed and the printer/form combination adjusted until an acceptable alignment is achieved. The first key 32-character key component and component check value is then generated and printed into the PIN mailer. Key custodian B is invited to logon and the second key component is generated and printed into the PIN mailer. The third key component is printed after key custodian C has been invited to logon. The three key custodians remove the PIN mailers from the printer and each assumes control of their particular PIN mailer containing their component. The outside of the PIN mailer clearly indicates which mailer contains which component. Each key custodian stores their PIN mailer in their respective Sentry lock-box. The lock-boxes are then stored in the Rhino2 Safe. The key generation event is logged by the key administrator and the safe is locked by the key administrator.

All the events were logged within the CSA-7000 and all operations are logged into the A98 activity log. The KEK Generation process is shown in Figure 12.

Key Encrypting Key Loading

Loading of the A98 Master Key is accomplished using the KEK Loading Utility or the KEK loading function available on the user interface during normal operations.

After the key administrator opens the Rhino2 Safe, the three key custodians assume custody of their respective Sentry lock-boxes. The KEK Loading function requires each key custodian in turn to logon. Each key custodian enters their 32 character key component via the A98 system keyboard twice and compares the displayed component check value with the correct component check value provided by the PIN mailer. After key custodian C has entered the final key component, the key check value for the newly loaded KEK is displayed and entered into the key loading log by the key administrator. The other key custodians verify the correct key check value has been recorded. Each key custodian places their respective paper copy of their key component into a tamper evident and serial numbered security bag and seals the bag. The Block and Company, Inc., Wheeling, IL catalog number 136-1080-06 is particularly suited for this purpose. The key custodian removes the tag containing a duplicate of the bag serial number and the number is recorded in the key loading log by the key administrator. The sealed bags are then locked into the respective Sentry lock-boxes and the lock-boxes returned to the Rhino2 Safe. The key administrator makes the appropriate log entries.

All the events were logged within the CSA-7000 and all operations are logged into the A98 activity log. The KEK Loading process is shown in Figure 13.

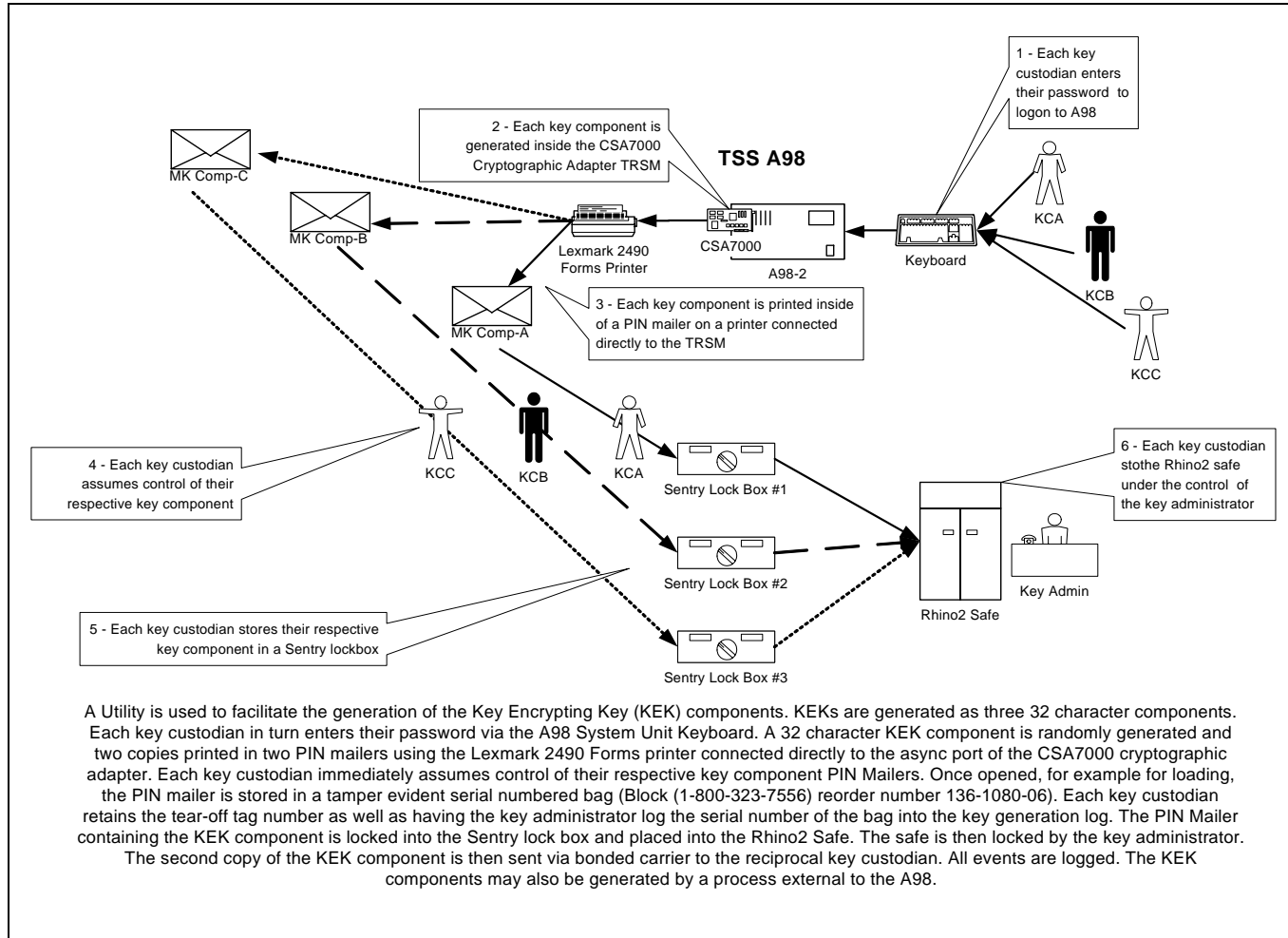


Figure 12 – Key Encrypting Key Generation

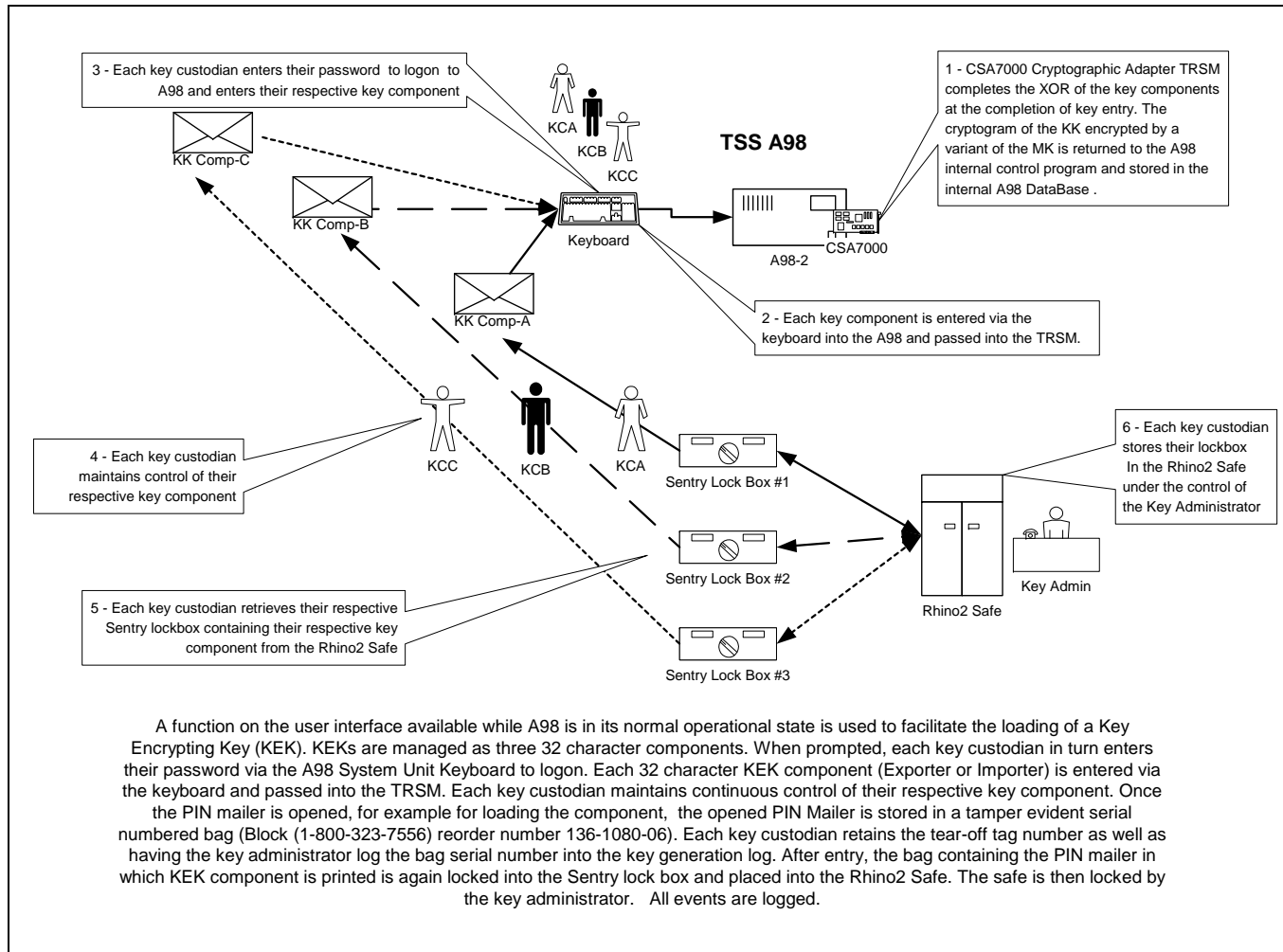


Figure 13 – Key Encrypting Key Loading

Key Encrypting Key Usage

In addition to a different Master Key being used for the A98 System, a different and separate Key Encrypting Key (KEK) is used for every cryptographic relationship between the A98 system and any other system as shown in Figure 14. In this figure MFK_a is the Master Key for the TSS A98 system, MFK_b is the Master Key of the system at the Bank and MFK_c is the Master Key of the Atalla A7000 attached to the host computer that runs the host application – e.g. BASE24. The cipher key (K_{cip}) used to encipher the ATM component set needs to be provided to the Bank A98. Therefore KEK KKB is established using manual key management.

The key established in the ATM (ATMA) will need to be sent from the Bank A98 to the Host machine running BASE24. Therefore KKA is established between the Bank A98 and the host Atalla A-7000 using manual key management.

The KEK relationships are shown in Figure 14.

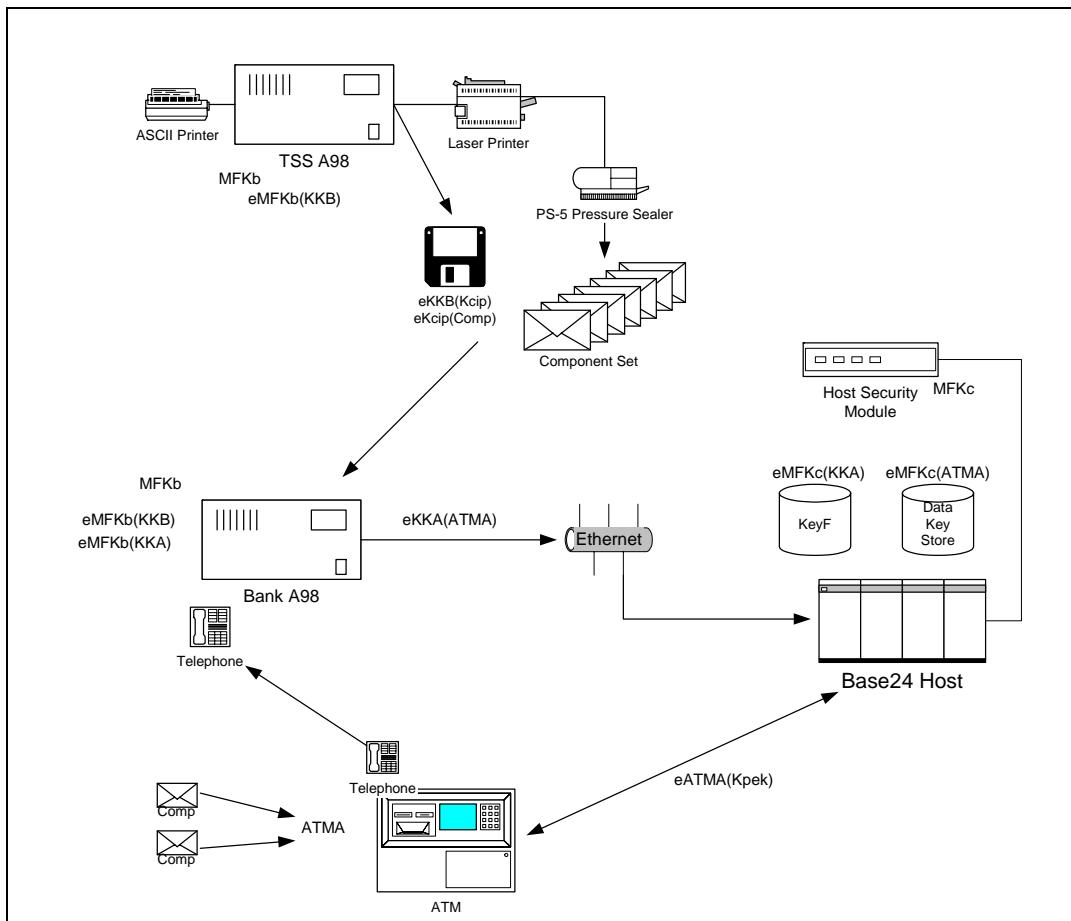


Figure 14 – KEK Usage

Comvelopes™ supplied by TSS to the Customer

Sealed documents containing the potential ATM key components can be supplied by Trusted Security Solutions, Inc. to the customer or the customer's servicer as desired. A KEK must be established between the Trusted Security Solutions A98 and the Customer A98 that is to receive the component envelopes. The process is shown in Figure 15. Components are supplied in sets of 1000. The cipher key used to encrypt the components, along with the components encrypted by the cipher key, is supplied to the customer on a diskette. The receiving A98 uses the Import Component Set function on the user interface to move the cipher key from encipherment under the KEK to encipherment under the customer's A98 MFK. The encrypted ATM key components are copied to the database and no additional cryptographic processing needs to be done on them.

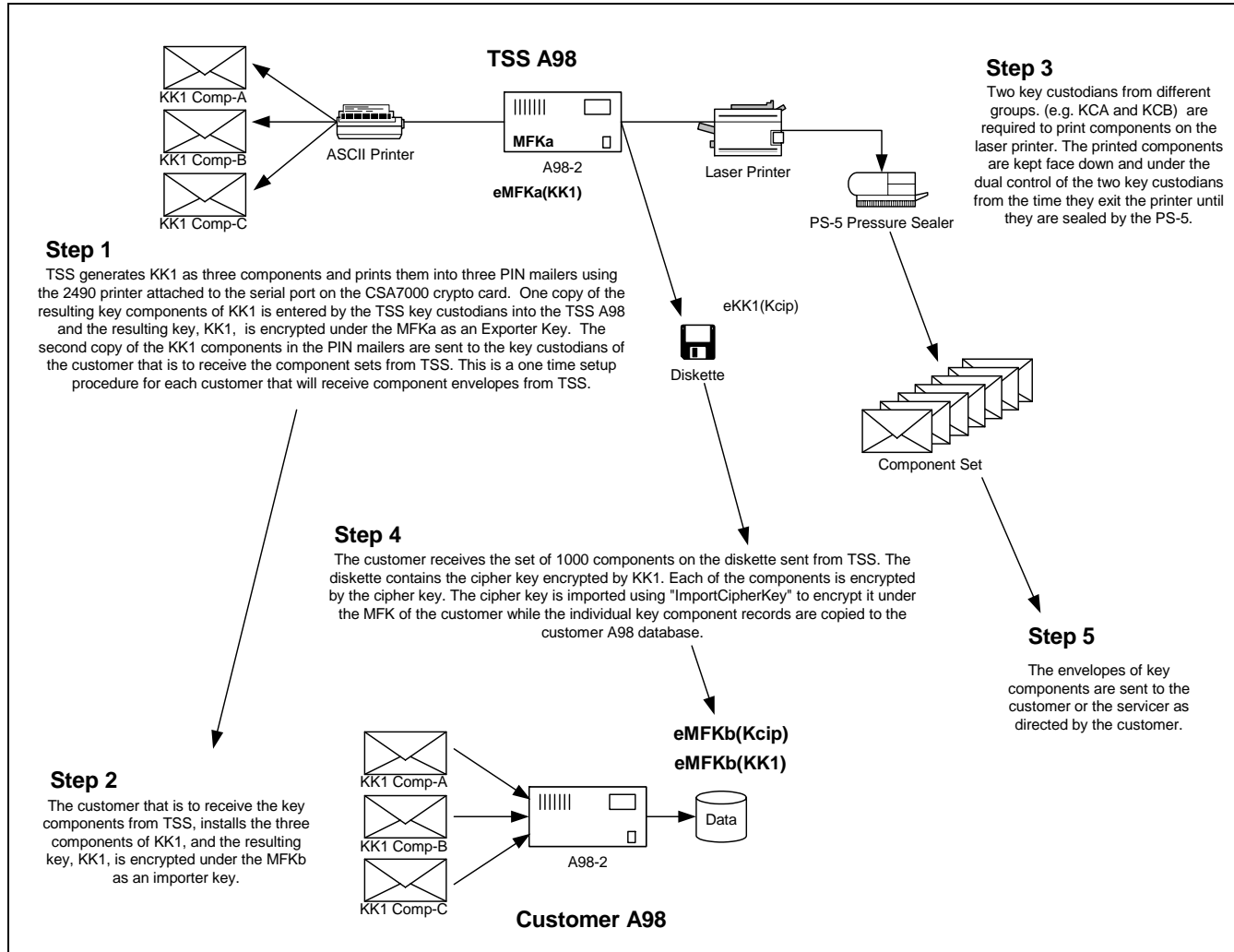


Figure 15 – TSS Supplies Component Envelopes (Comvelopes™)