



SERVICE BUREAU FOR INITIAL ATM KEY ESTABLISHMENT



May 16, 2005

Version 3.0

A98 Overview

Trusted Security Solutions, Inc. is offering the A98 ATM Initial Key Establishment System to institutions that manage the cryptographic keys for ATMs. 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.

The A98 system can be purchased and installed at the your data center. The turnkey A98 solution comes pre-configured with the A98 software and is packaged in a standard, locking rack-mounted enclosure. Installation and on-site training is included.

For institutions for which the purchase of an A98 may not be economically justified, TSS offers a Service Bureau to assist in the establishment of the initial ATM Keys.

For additional information concerning A98 or other products and services please visit our web site at www.trustedsecurity.com or contact:

info@trustedsecurity.com

Telephone: (704)849-0036

The Unique Key per ATM Problem

American National Standard X9.24 (ANS X9.24) – Retail Key Management and most network operating rules 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 ANS 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 especially when one considers the number of individuals potentially involved in the process. Solutions employing public key cryptography have been proposed, but are currently not compliant with ANS X9.24 and there are no immediate changes planned to include such solutions. Public key solutions also require software and perhaps hardware changes to the ATMs, the payment of a patent royalty as well as having a major impact on the current infrastructure and systems. Using traditional methods of key management involving the control of individual key components requires large numbers of key custodians. The A98 solution described here avoids all of these problems and provides an easily implemented and non-intrusive method that has either no impact or a minor impact on the currently installed system and infrastructure. When public key systems become adopted and ATMs that support public key are available, the A98 can be enhanced to include those ATMs as well with no changes to the A98 operations and host software or the Host Security Module.

A98 System Overview

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

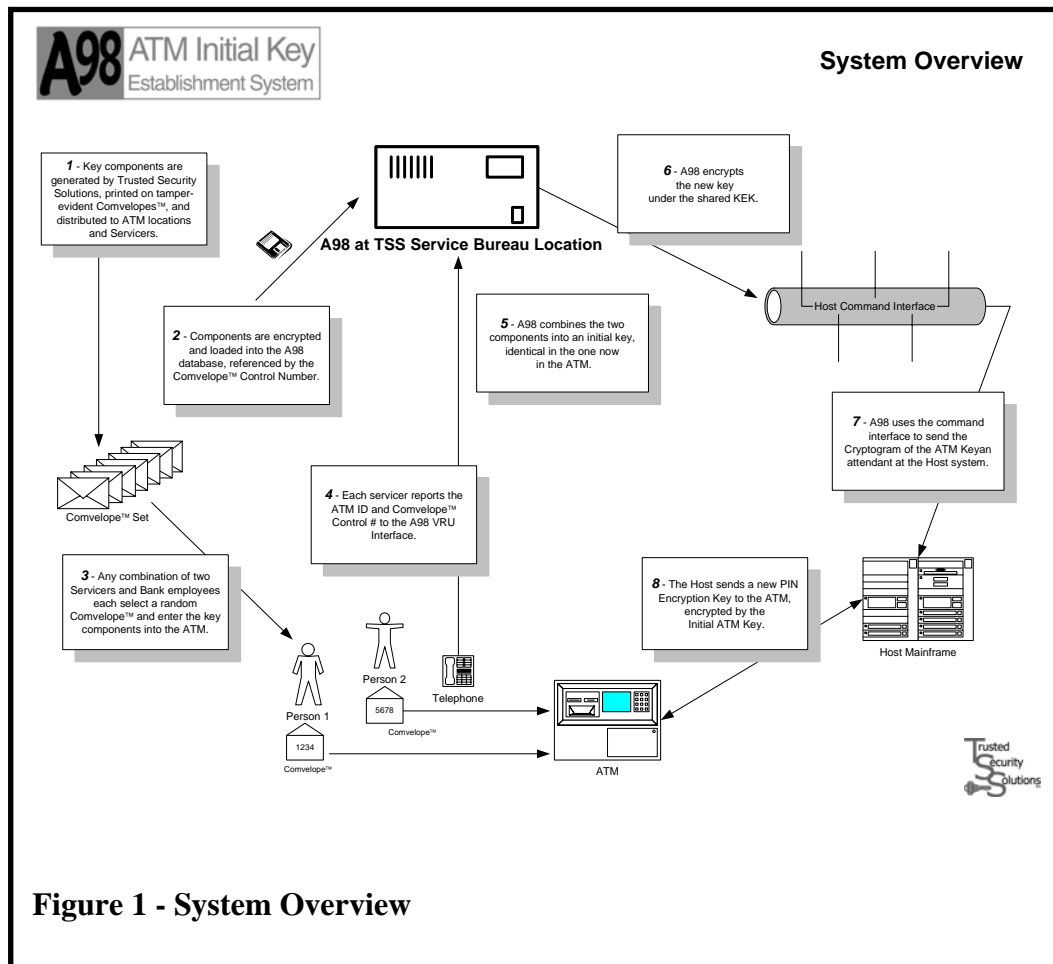


Figure 1 - System Overview

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.

A98 System Description

The System Overview is shown in Figure 1 – System Overview. Random Numbers are generated and sealed in serial numbered tamper evident packaging known as Comvelopes. Each random number is encrypted under the Master Key and stored with the serial number for future retrieval. The Comvelopes are distributed to the bank employee at the branch office closest to the ATM and the ATM service personal. Alternatively, the Comvelopes may be stored with each ATM for future use. Each key custodian or key component loader is assigned a unique ServicerID and an initial Access Code similar to a PIN. Each Servicer 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.

The A98 System Unit holds the database of random numbers, Servicer IDs and ATM IDs. The A98 System Unit contains an Eracom cryptographic adapter along with an industry standard Interactive Voice Response (IVR) unit. 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 with the host driving the ATMs.

To establish an initial key in an ATM, each Servicer selects a Comvelope at random, verifies it has not be tampered, opens it and enters the component it contains into the ATM following the ATM vendors normal instructions. The Servicer then calls the A98 System Unit's voice response unit using a touch-tone telephone. The Servicer is invited to enter his ServicerID and if valid, is invited to enter his Access Code for verification. Once verified, the Servicer identifies the ATM by entering the established ATMID and selects the desired function. The control number of the selected Comvelope is entered and the database entry is marked as being entered into the identified ATM. The second Servicer selects a second Comvelope and inspects it to ensure it has not been tampered. The random number contained in the second Comvelope is loaded into the ATM following the ATM vendor's instructions and the identification process is repeated for the second Servicer. The two random numbers – now key components - are combined inside the A98's TRSM cryptographic adapter to form an initial key and this key is encrypted under the KEK. The cryptogram and ATMID are made available to the host. The host enters this cryptogram into the ATM database and marks the ATM as ready for initialization. When the ATM then connects, the application program requests the host security module to create a new PIN encryption key and send it to the ATM when it connects. 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 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.

Note: In reality, as shown in Figure 2, each Comvelope 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.



Figure 2 - Comvelope Contents

Cryptographic Keying Relationships

The KEK relationships are shown in Figure 3 - KEK Usage. Figure 2 covers the case where the customer owning an A98 purchases the Comvelopes from TSS. A KEK (KKb) is established between TSS and the Customer A98. An additional KEK (KKa) is established between the Customer A98 and the Customer program that is driving the ATMs. KKa is used to encrypt the ATMA and ATMB keys prior to sending the cryptograms to the Host system. The Host system uses the KKa to recover the ATMA and ATMB keys and reencipher them to the MFK of the HSM. KKb is used to send the cryptograms of the Comvelope contents to the Customer's A98. The cryptograms are sent on diskette encrypted by a double length key that is in turn encrypted by the double length KKb. The cryptogram of the encrypted cipher key is included on the diskette. The customer performs an import operation at the A98 to add the new Comvelopes prior to distributing them to the ATMs. Note that if the HSM's MFK is used as KKa, no additional cryptographic processing is required. The cryptograms can be placed directly into the database.

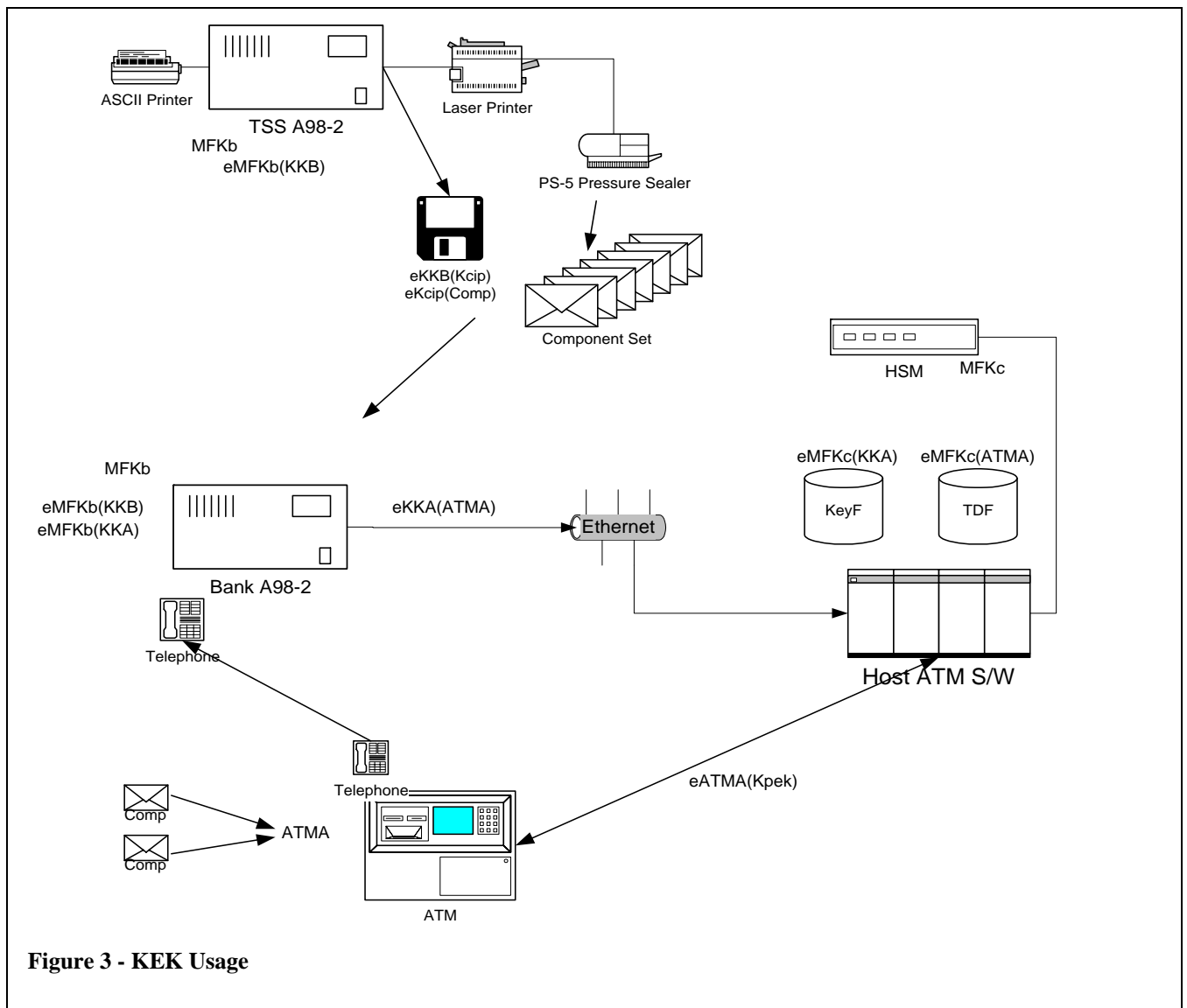


Figure 3 - KEK Usage

Outsourcing - The TSS A98 Service Bureau

Overview

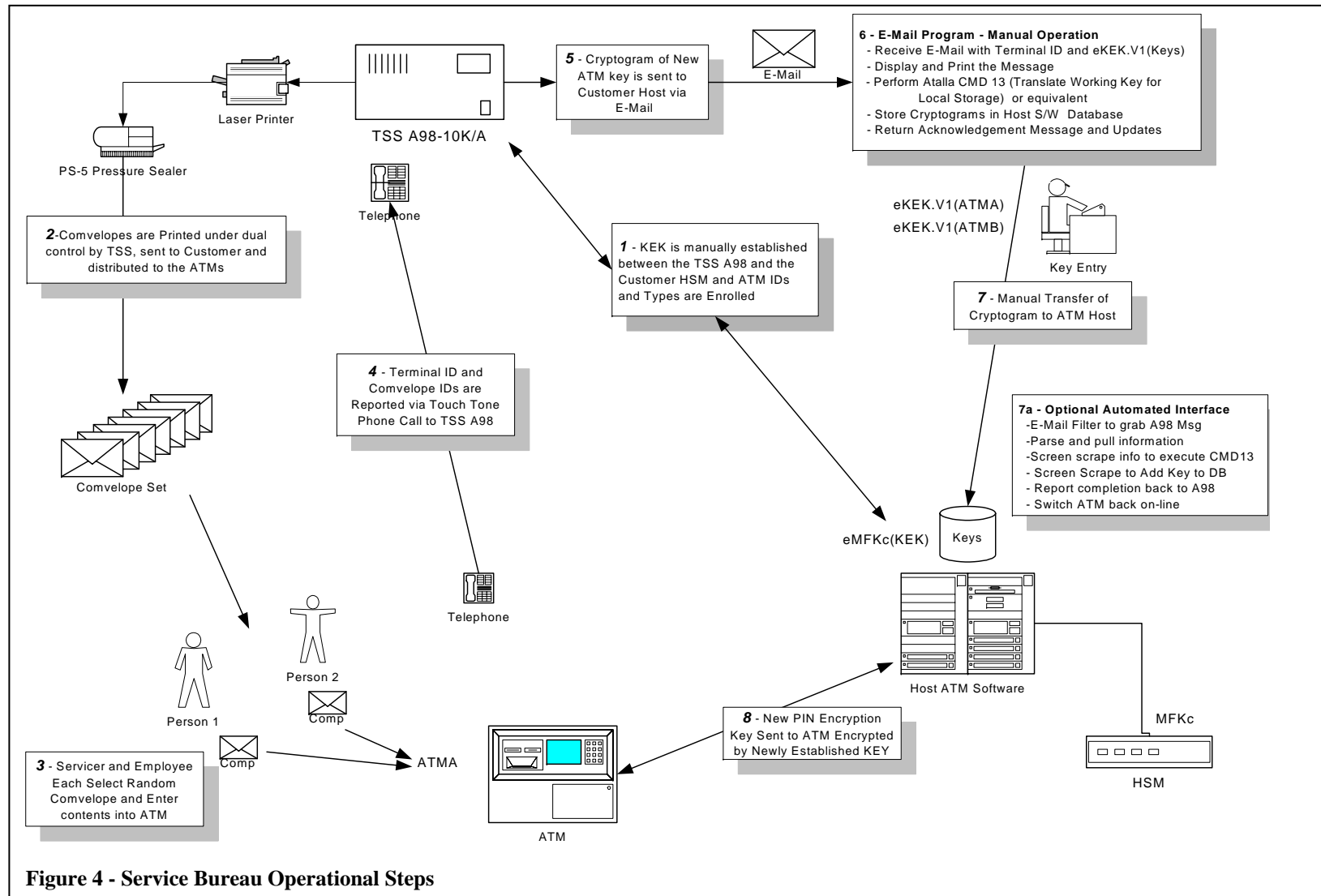
Trusted Security Solutions (TSS) offers a Service Bureau for the management of initial ATM keys for organizations for which the purchase of an A98 is not justified. The Service Bureau Customer (Customer) registers his ATMs by providing the Vendor and Model along with a unique identification number and the type of key management employed by the ATM – full length multiple key components or split left and right key halves. Comvelopes are purchased from TSS in quantities of 100 and distributed to the Customer's ATMs. The Customer's servicers load the contents of the Comvelopes into ATMs as required and places a phone call to the A98 located at TSS in Charlotte, NC. The servicers report the ATM ID and Comvelope ID. The A98 retrieves the contents of the Comvelopes within the Tamper Resistant Security Module (TRSM) and creates the same key that was just loaded into the ATM. A Key Encrypting Key shared between the Customer and TSS encrypts the just loaded ATM key. The A98 sends this cryptogram and the ID of the ATM to the Customer. The information in the message is extracted and entered into the database of the Host ATM Software package. This process could be manual or automated. Each time the A98 Service Bureau is used, a new unique key is established in that ATM in a fully compliant manner.

The Operational Steps

The Operational Steps of the A98 Service Bureau Steps are shown in Figure 4 - Service Bureau Operational Steps. These steps are described below.

1. **Establish the KEK** - A Key Encrypting Key (KEK) is established between TSS and the Customer using manual key management methods. TSS will generate this KEK and send the components to the key custodians designated by the Customer. This KEK is generated as three (3) double length (112 bits) components and is printed directly into tamper evident envelopes. The three components are sent to each of the three key custodians using three separate express couriers. The ATMs will also be registered at this time. The ATM vendor and model the type of key management – either multiple full length key components, or split Left and Right halves – as well as a unique numeric identifier is established for each ATM. The ServicerIDs and their initial Access Codes will also be established at this time.
2. **Print and Distribute the Comvelopes** –TSS will generate and print the Comvelopes. A Single ADMIN role can generate the Comvelopes and the Cipher Key to protect them, but two (2) TSS key custodians are required to enter their passwords to emit the Comvelopes to the printer. The printed Comvelopes exit the printer attached to the TSS A98 face down. None of the contents of any Comvelope are visible. The face down Comvelopes are taken to the pressure sealer under dual custodianship and sealed on the Moore PS-5 pressure sealer. The contents of the Comvelopes are encrypted by the cipher key and copied to a diskette. The Cipher key is encrypted by the KEK established in 1 above and the cryptogram copied to the diskette. The cipher Key and Comvelope contents are imported into the TSS A98 by a TSS ADMIN role. The physical Comvelopes are packaged together and sent to the Customer. The customer then distributes the Comvelopes to the various ATMs or to the appropriate staging locations.
3. **Load Key into ATM** – When it is time to load an initial key into an ATM, two Customer people each select a Comvelope at random from the population of Comvelopes. The first person inspects the Comvelope for any signs of tampering. If it has not been tampered, the Comvelope is opened and the contents loaded into the ATM following the manufacturer's instructions. If the ATM reports the Key Check Value (KCV), the first person verifies the KCV corresponds to the one printed in the Comvelope.
4. **Report the Terminal ID and Comvelope ID** – The first person calls the TSS A98 and enters their ServicerID and Access Code. After verification, the Servicer is invited to enter the ATMID and Comvelope ID. The A98 reports the KCV back via the IVR and the first person verifies the KCV is as expected.

- **The Second Person Repeats Steps 3 and 4** – A Second person selects a Comvelope at random from those available and repeats steps 3 and 4 above. At this is point a unique key has been established in the ATM. That same key now exists on the A98 encrypted under the KEK shared with the Customer.
5. **Cryptogram of ATM Keys are Sent to the Host** – The TSS A98 formats an E-mail message containing the ATM ID, the cryptograms of the ATM keys just established and the Key Check Values for the KEK and the newly established ATM Keys. The E-Mail message is sent to the Customer.
6. **The Customer Receives the E-Mail Message** – The E-Mail message is received at the Customer and is processed to parse out the Terminal ID, the Cryptograms of the ATM keys and the KCV's. The ATM keys must be translated from encryption under the KEK to encryption under MFK. For an HSM that implements the Atalla architecture, a CMD 13 – Translate Working Key for Storage is used.
7. **Enter the Information into the Host ATM Software** – A Manual process can be used to enter the cryptograms and ATM ID information into the Host ATM Software. Alternatively, the process may be automated.
8. **A New PIN Encryption Key is Sent to the ATM** – After the ATM reconnects, most ATM software packages will send a new PIN encryption key to the ATM encrypted by the AT key that was just established and normal operations resume.



Entering the Cryptogram

The steps of entering of the cryptogram into the Host ATM Software is shown in Figure 5 – Service Bureau – Entering the Cryptogram. This section is intended to expand on the description of those steps.

1. **Establish the Key in the ATM** – This process is described above in the section titled The Operational Steps. This includes the steps of:
 - Placing the ATM in an “Off-Line” or disabled condition as required by the ATM Manufacturer
 - The Entering of the contents of the Comvelopes as required per policy and the ATM manufacture’s instructions
 - Placing the Calls to the A98 to report the ATM ID and Comvelope Ids
 - Informing the Customer Help desk to inform it of the ATM rekey operation
2. **The A98 E-mails the cryptogram and ATM ID to the Customer** – An E-Mail message is composed in a specified format and sent to the Customer’s designated E-Mail Address.
3. **Parsing the E-Mail** – The E-Mail Software is used to detect the arrival of the message from the A98 containing the ATM Id and cryptograms of the established keys. Software is used to parse the message into the various fields and either display it or submit it for automated processing.
4. **Translate the Cryptograms** – The cryptograms need to be translated from encryption under the KEK to encryption under the MFK of the Host Security Module. For an HSM using Atalla architecture, a CMD 13 – Translate Working Key for Local Storage needs to be executed. CMD 13 accepts the Cryptogram of the ATM Key under the KEK along with the cryptogram of the KEK under the MFK as input and returns the cryptogram of the ATM Key under the MFK. The cryptogram as returned is then suitable for storage in the ATM database used by the Host ATM Software. The CMD 13 can be executed manually using an interface supplied by the vendor of the Host ATM Software or a program supplied by the HSM Vendor or a special Customer supplied program to accomplish the translation.
5. **Manual Transfer of the Cryptogram to the DB** – The cryptogram of the ATM key under the MFK of the HSM can be input to the Host ATM Software Database using a manual or automated process
6. **Manual Transfer of the Cryptogram to the DB** – The Manual Interface of the Host ATM Software can be used to enter the cryptogram of the ATM key under the MFK obtained from the CMD 13 into the ATM Database.
7. **Reconnect the ATM** – Have the ATM reconnected or enabled so the Host ATM Software can “see” it. This action should trigger the creation of a new PIN Encryption Key (PEK) using CMD 10 – Create Working Key for Distribution. The PEK is encrypted under the MFK and the newly established ATM key. The form of the PEK encrypted by the ATM Key is sent to the ATM and normal operations resume.

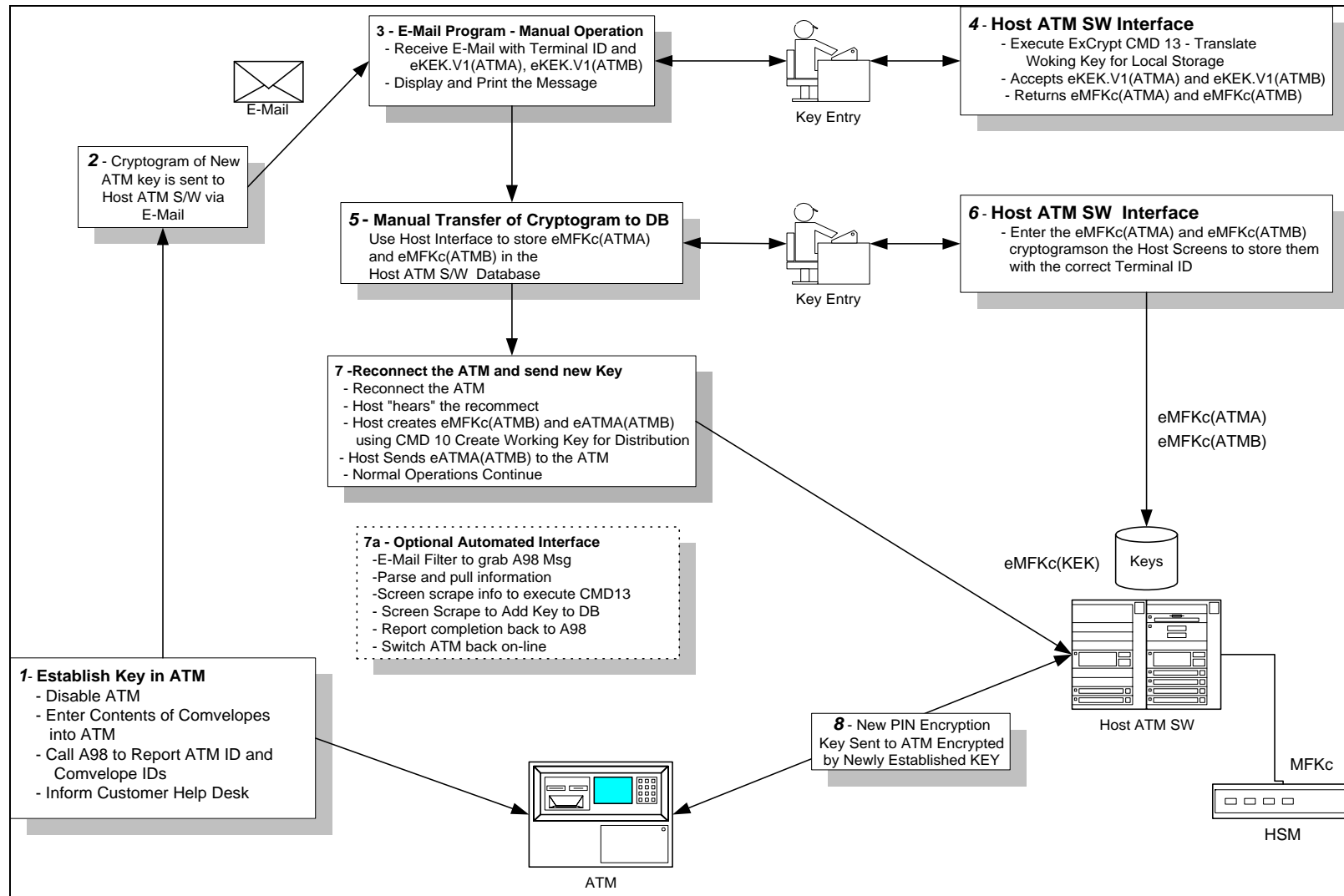


Figure 5 - Service Bureau – Entering the Cryptogram

Automating the Process

The entire process of receiving the cryptograms and placing the ATM back in operation with a new unique key could be automated with no or very few changes to the Host ATM Software. Additional programming is required, but not to change the vendor's Host ATM Software. The changes are entirely under the control of the Customer. The actions that would normally be done by a human executing the manual process described above could be automated by employing the tried and tested "screen scraping" technology. "Screen Scraping" or Enhanced High Level Application Programming Language (HLAPI) has been employed since the 1970's to automate processes. HLAPI is used at a customer supplied PC connected to the Host System. Some custom programming is required, but it is confined to the terminal connected to the Host ATM Software and does not require any changes the Host ATM Software itself. The required programming is more like a Script or Macro language that involves "recording" the actions taken by a human to transfer the cryptogram and ATM ID to the Host ATM Software Database. The cost of this approach is far lower than comparable changes to the Host ATM Software.

The Fee

The Fee for the Service Bureau is in two parts. There is a one time set up fee and there is an on going fee for each ATM. The fees are shown below.

Any Customer-initiated modifications to the Customer Setup requested 45 days following the Effective Date will be charged at the rate of \$50 per individual change with a maximum of \$200 per event, if the changes are provided electronically in the specified format.

Description	Amount
One Time Setup Charge	\$2,500
Annual Fee per ATM ¹	
First 50 ATMs	\$120/ATM
Next 50 ATMs	\$ 75/ATM
Additional ATMs	\$ 50/ATM
Comvelopes per 100	\$100.00
Servicer ID's per 100	\$100.00
Setup Modifications:	
Individual ATM or Servicer event	\$ 50.00
Maximum charge per event ²	\$200.00
Billing:	
Quarterly	
Purchase Option:	
A credit equal to 50% of Annual Fees paid in the most recent 2-year period will be applied to the purchase of an A98 system.	