

A98™ Process: Service Bureau

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 and avoids the cumbersome requirements normally associated with compliant key management.

ANSI Standard X9.24, Retail Key Management, requires each PIN encryption device to contain a unique triple DES 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 initial key per ATM is a particularly difficult task due to the complexity of the required key management procedures. Traditional methods, which focus on the control of individual key components, require large numbers of key custodians making them cumbersome and inefficient. The A98 solution avoids all of these problems and provides an easily implemented and non-intrusive method to achieve compliance to ANSI standards and network operating rules. Solutions employing public key cryptography, such as the A98-R Remote Key Module, are now available for ATMs that are "remote key ready". Public key options generally require hardware and software changes to installed ATMs.

With the A98 approach, 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 they are actually loaded into the ATM. These potential key components are contained within Trusted Security's innovative tamper-evident Comvelopes[®], which are randomly distributed and stored at the ATM, branch office, or with the servicer. After entering the key component from a randomly selected Comvelope into the ATM, each servicer calls the A98 voice response unit and enters the control number identifying the Comvelope. The two identified components, stored encrypted by the A98 Master key, are combined within the A98 Tamper Resistant Security Module (TRSM) to form the same key that was loaded into the ATM. The newly created key is encrypted within the TRSM using a Key Encrypting Key shared with the ATM host system. The encrypted ATM key is sent to the host via an ISO8583 message format or XML. When the "ATM Connect" message is received, the host software proceeds as normal to generate a PIN encrypting key in two forms, encrypted by the newly loaded ATM initial key and by the host Master File Key. The first is sent back to the ATM and the second is stored in the host's database.

The ATM has now been re-keyed using a unique triple DES initial key in a fully compliant manner.

A98 ATM Initial Key Establishment System

developed by Trusted Security Solutions, Inc.

Comvelopes[®] – Trusted Security Solutions produces custom envelopes including customer's company logo (in units of 1,000) to be distributed to branches, service companies, or field personnel that service the customer's ATMs. As a benefit, there is no requirement to generate keys for these ATMs.

ATM Administration – When a customer signs up with the A98 Service Bureau, TSS assists in creating and sending back the necessary ATM and servicer information required. If there is a need to add or change ATM information, our A98 Service Bureau administrators are available to help, allowing TSS to stay current with each of our customer's portfolio of ATMs.

Triple DES Support – The A98 Service Bureau fully supports all Triple DES requirements.

Host Interface and Shared KEK – During initial deployment, a decision will be made for either the customer to send TSS a KEK to use or for TSS to send the customer one. Once the KEK is established, TSS will work with the individual client to achieve a convenient means to accept the email cryptogram from the A98 Service Bureau and use it to establish the newly created key into the host ATM database.

Service Bureau Rates – Trusted Security Solutions charges a one time Set Up Fee, an annual fee per ATM, and a nominal charge for Comvelopes, Servicer IDs, and ongoing administrative support. Contact us at info@trustedsecurity.com to receive a formal quote.

```
Email Cryptogram

From: a98sb [mailto:a98sb@trustedsecurity.com]
Sent: Wednesday, November 17, 2003 2:23 AM
To: 'YourEmailAddress.com'
Subject: A98: Key Change Notification

The included initial ATM keys were generated by the
A98 Outsourcing Service located in Matthews, North
Carolina. If you have any questions please contact
Trusted Security Solutions at (704) 849-0036

*** GENERAL INFORMATION
Message Type: Key Update
Message Number: 6
Date/Time Sent: 11/17/03 2:26:33PM
Sender: $A98$
Receiver: **Customer Name**
Terminal ID: IX65
```



Trusted Security Solutions, Inc.
1500 Orchard Lake Drive
Charlotte, North Carolina 28270
704.849.0036

A98 Service Bureau for OUTSOURCING Key Management

- The A98 brings your ATMs into compliance with Unique Initial Key requirements
- Requires no hardware investment or site installation
- Requires no changes to your ATMs
- Avoids traditional logistics problems associated with key management
- Keeps detailed audit reports on all ATM keying activity

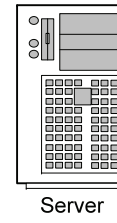
A98 ATM Initial Key Establishment System

System Overview

1 - Key components are generated by Trusted Security Solutions, printed on tamper-evident Comvelopes, and distributed to ATM locations and Servicers.



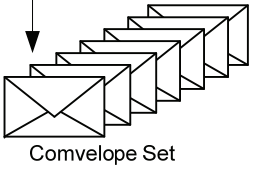
6 - A98 encrypts the new key under the shared KEK and creates a Cryptogram that is sent to the A98 Service Bureau email server



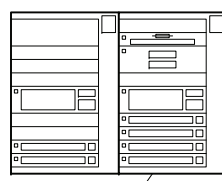
7 - A98 sends the Cryptogram email to the client Administrator who then inserts the Cryptogram of the ATM Key into the ATM Host software database.

2 - Components are encrypted and loaded into the A98 database, referenced by the Comvelope Control Number.

5 - A98 combines the two components into an initial key, identical to the one now in the ATM.



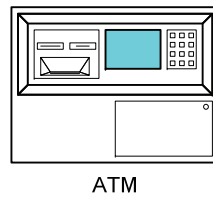
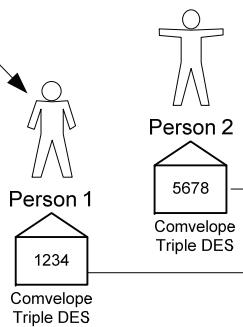
4 - Each servicer reports the ATM ID and Comvelope Control # to the TSS Service Bureau A98 VRU Interface through a toll 800 number.



ATM Host System

3 - Any combination of two Servicers and Bank employees each select a random Comvelope and enter the single or double-length key components into the ATM.

8 - The Host sends a new PIN Encryption Key to the ATM, encrypted by the initial ATM Key.



ATM

Comvelope® Triple DES Version

