

# Trusted Security Solutions

## A98 ATM Initial Key Establishment System

### Frequently Asked Questions

**Q:** What is the A98?

**A:** The A98 is a fully vendor neutral, total system solution that is used to establish a unique initial key in each ATM.

**Q:** Is the A98 hardware or software?

**A:** Both. The A98 is a total system solution consisting of a rack mounted system unit containing a Tamper Resistant Security Module (TRSM) for all cryptographic processing, color display, key board, industry standard voice response unit, system network connection, the key management safe and lock boxes, Windows Professional 2000 operating system and A98 system application programming.

**Q:** Are there any hardware or software changes required to my ATMs to use the A98?

**A:** No. There are absolutely no changes of any kind required or needed to the ATMs for conventional (manual) key loading. To utilize automatic key loading (Remote Key Loading), your ATM must have an encrypting PIN pad (EPP), software, and firmware capable of supporting remote key loading.

**Q:** Will the A98 work with my ATMs?

**A:** The A98 patented Comvelope™ process works with any and all ATMs.

**Q:** How does it work?

**A:** Random numbers are printed into tamper evident documents called Comvelopes for "Component Envelopes" and a control number is assigned to each Comvelope that is visible only when the Comvelope is opened. The contents of each Comvelope are encrypted on the A98 system unit. Comvelopes are distributed at random to each ATM or a location where they are accessible to the individuals that load the key into the ATM. To load a key, one person selects a Comvelope at random, opens it and enters it into the ATM following the ATM manufacturer's instructions. This individual then places a phone call to the A98 on any touch-tone phone and follows the IVR prompts to enter the user ID, Access Code, ATM-ID and Comvelope ID. A second person selects a second Comvelope at random and repeats the process. The A98 then combines the two key components that were entered into the ATM within the cryptographic adapter to create the key that was just loaded into the ATM. The newly created key is then encrypted by a Key Encrypting Key (KEK) shared with the host and sent to the host to be added to the ATM database.

**Q:** Do the Comvelopes require any special protection?

**A:** No. They do not contain key components only POTENTIAL key components. It is only once the Comvelope contents have been entered into the ATM that the content of the Comvelope becomes a key component. If an opponent opens one or more of the Comvelopes prior to their being used, nothing is lost.

**Q:** Is there any special cryptographic processing required on the ATM host?

**A:** If the Master File Key of the Host Security Module is used as the KEK, the cryptograms of the ATM keys are in the correct form to be stored in the ATM database. If a different KEK is used, the cryptogram must be translated from encryption under the KEK to encryption under the MFK.

**Q:** Will I have to consider changing my Host Security Module to accommodate Remote Re-Key Loading?

**A:** No. Because all the cryptography functions revolving around Remote Key Loading are performed in the A98, you do not need to have a Host Security Module with RSA capabilities for ATM initial key establishment.

**Q:** Is there any significance to the name "A98"?

**A:** The Visa directive required all ATMs to have a unique key by August 31, 1998. Hence the name A(ugust) 98. The PLUS operating rules state in section 2.8 (E) – ***“Effective August 1, 1998, the use of unique encryption keys per ATM is required.”***

**Q:** Does the A98 system meet the requirements for a unique key per ATM?

**A:** The A98 system is fully compliant with all applicable ANSI Standards (X9.24 and X9.8), all network operating rules and the Visa directive.

**Q:** Will Visa certify the A98 as being compliant with its directive?

**A:** Visa does not "certify" or endorse specific products. Also, there may be variations in specific implementation details of any given installation. Contact Visa for specific information about your proposed implementation.

**Q:** Are there any changes required to my host ATM software to use the A98?

**A:** No. The A98 can be used without any changes to your host ATM software. With the use of TSS's Host Proxy Application, an operations attendant can receive a cryptogram from the A98 and manually enter in the cryptogram into your host application. To achieve a seamless transaction from the A98 to your host so that the interaction of an operations attendant is not necessary, the A98 can be integrated into your host ATM software through several means. One popular integration method with the host has been through "screen scraping" technology. "Screen scraping" is technology that simulates the entry of keystrokes by an individual. It has a well-defined interface called HLAPI (High Level Application Programming Interface). Alternatively, custom software may be written to accept the key newly added to the ATM should you not want to use a HLAPI approach. Many popular host solutions offer A98 interfaces. In addition, TSS sells and supports a BASE24® interface for both legacy and remote key loading ATMs.

**Q:** How does the A98 attach to my host ATM System?

**A:** The A98 attaches to the host system via a TCP/IP connection.

**Q:** I manually load the same key into several (or all) of my ATMs. I then send a unique PIN encryption key to the ATM encrypted by the key that was manually loaded into the ATM. Isn't implementation compliant with the requirements for a unique key per ATM?

**A:** NO, it is not.

ANSI X9.24-2004 Part 1 section 7.6 Key Utilization reads:

*ANY* (emphasis added) key used by a communicating pair **MUST** be unique (other than by chance).

Additionally, the TG-3 Compliance Guideline section 4.3.9 states:

Documented procedures exist and are followed that ensure **ALL** (emphasis added) keys in PIN entry devices are, except by chance, unique to that device.

**Q:** How soon can I expect to receive the A98 after ordering?

**A:** Your A98 will normally be shipped within 30 days of placing your order.

**Q:** How about training and installation?

**A:** Trusted Security Solutions will install and train you on your A98 in two the three days. The cost of a normal installation of training within the continental US is usually quoted between \$3,500 and \$5,000 depending on whether or not both modules (Comvelope process for legacy ATMs and Remote Key Module) are installed.

**Q:** What is the capacity of the A98?

**A:** There are fourteen models of the A98 based on the number of ATMs they support and which keying method(s) you chose to use. The capacity of each model is listed below:

**A98/A for Conventional Key Loading Using Comvelopes**

**A98/R for Remote Re-Key**

A98/125/A	= Max. 125 ATMs	A98/125/R	= Max. 125 ATMs
A98/250/A	= Max. 250 ATMs	A98/250/R	= Max. 250 ATMs
A98-500/A	= Max. 500 ATMs	A98-500/R	= Max. 500 ATMs
A98-1K/A	= Max. 1000 ATMs	A98-1K/R	= Max. 1000 ATMs
A98-5K/A	= Max. 5000 ATMs	A98-5K/R	= Max. 5000 ATMs
A98-10K/A	= Max. 10,000 ATMs	A98-10K/R	= Max. 10,000 ATMs
A98-32K/A	= Max. 32,000 ATMs	A98-32K/R	= Max. 32,000 ATMs

**Q:** How many phone lines can the A98 support?

**A:** The number of phone lines supported increases with the ATM capacity:

A98-125/A	= 1 phone line
A98-1K/A	= 2 phone lines
A98-5K/A	= 2 phone lines
A98-10K/A	= 4 phone lines
A98-32K/A	= 4 phone lines

**Q:** What is Remote Rekey?

**A:** Remote Rekey (aka Remote Key Loading (RKL) or Remote Key Transport (RKT)) is an emerging keying process using RSA or public key cryptography. Using Remote Key Loading in most cases eliminates the need for a field technician to be at the ATM to establish a new initial key in the terminal. Remote Key technology stands to save ATM owners a substantial amount of operational cost by reducing the number of times that an ATM technician has to visit the ATM. With the introduction of it's new "Remote Key Module", A98-R automates both the generation and distribution of cryptographic keys for ATMs. The A98-R is compatible with ATMs that use RSA-enabled encrypting pin-pads (EPPs). The A98-R implements both Diebold's Certificate Based Protocol (CBP) and NCR's Signature Based Protocol (SBP) that are defined in the ANS X9.24 Part 2:2006 Standard on Retail Cryptographic Key Management.