

# A98 for TRIPLE-DES

- A98 brings your ATMs into compliance with Unique Initial Key requirements
- Provides complete support for Triple-DES
- Requires no ATM changes
- Is compatible with all ATMs
- Avoids traditional logistics problems associated with key management
- Keeps detailed audit reports on all ATM key activity
- Automates the interface to many host software platforms
- Supports the new A98 Remote Re-Key Module

## A98™ Process: Conventional Mode

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.

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. The latest guidelines phase in the requirements for Triple-DES.

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. Solutions employing public key cryptography have been proposed, but are not compliant with the X9.24 standard. Public key options also require hardware/software changes to installed ATMs, disrupting current infrastructure and systems. 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.

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 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. 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 single or double-length initial key in a fully compliant manner.



developed by Trusted Security Solutions, Inc.

**A98 System Unit** - Pentium processor, two mirrored hard disk drives, Windows 2000, network interface card, internal voice response unit, Eracom® cryptographic unit, Zip drive, color monitor, keyboard with mouse, rack mounted enclosure with dual-key access control.

**A98 Printer** - an optional dot matrix printer can be attached directly to the cryptographic unit to securely print locally generated key components for KEKs and master keys.

**A98 System Software** - Custom application with cryptographic unit support, voice response processing, key management module, and complete administrative functions. A browser-based remote help desk module is now included.

**A98 Key Security** - The A98 system comes complete with serial numbered tamper-evident envelopes for storing cleartext-keying material in the three lock boxes, and a floor safe for storing the three lock boxes.

**Triple-DES Support** - The A98 software fully supports all Triple-DES requirements.

**Public Key Support** - The A98 Hardware as shipped supports key management protocols using Public Key Cryptography. A98's Remote Re-Key Module is now available.

**Host Interface** - TSS supplies an automated interface to BASE24® via terminal emulation. Custom integration with BASE24 is also available using an ISO-8583 message format. Interfaces to Mosaic®, Connex®, CV Systems®, and others are available directly from the respective vendors.



Trusted Security Solutions, Inc.  
416 West John Street  
Matthews, NC 28105  
704.849.0036  
www.trustedsecurity.com

