

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 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.



developed by Trusted Security Solutions, Inc.

A98 System Unit – Pentium processor, two mirrored hard disk drives plus hot spare, Windows Server 2003, RAID 1 mirrored drives, redundant power supplies, two network interfaces, internal voice response unit, SafeNet[®] cryptographic unit, front mounted USB ports, 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 (**eHelpDesk**) 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.

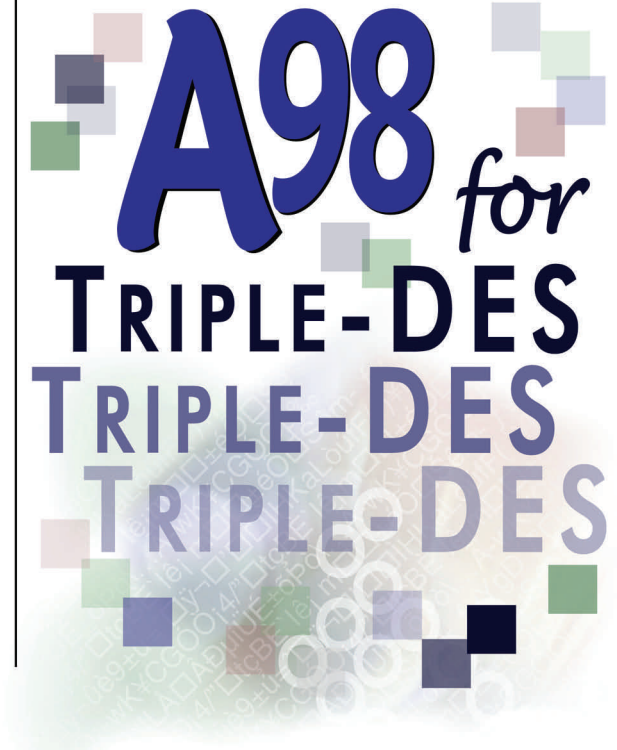
Triple-DES Support – The A98 software fully supports all Triple-DES requirements.

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 with interfaces for all ATMs manufactured to be remote key enabled.

Host Interface - TSS supplies an automated interface to BASE24[®], Interfaces to Postillion[®], Connex[®], CV Systems[®], and others are available directly from the respective vendors. TSS also uses a standard XML schema to interface to proprietary systems.



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



- **The A98 brings your ATMs into compliance with Unique Initial Key requirements**
- **Provides complete support for Triple-DES**
- **Requires no changes to your ATMs**
- **Avoids traditional logistics problems associated with key management**
- **Optional interfaces to many host software platforms available**
- **Supported by the A98 Remote Key Module**

