

Is your ATM network NETWORK compliant?

Visa, Star, NYCE, and other networks have established certain security standards. Use these sample questions from the Accredited Standards X9 Committee's TG-3 PIN Security Compliance Guideline¹ to evaluate the status of your own ATM network.

This evaluation is provided by Trusted Security Solutions, developers of the A98 ATM Initial Key Establishment System. The A98 solution provides an automated, efficient process to meet the requirements specified in the TG-3 guideline.



Trusted Security Solutions, Inc.
(704)849-0036

info@trustedsecurity.com
www.trustedsecurity.com

¹American Bankers Association, Accredited Standards Committee X9 – Financial Services, TG-3-2004 PIN Security Compliance Guideline, approved February 6, 2004. For more information, contact ABA/X9 at 202.663.5087 or at www.x9.org.

Section 3.3 of the TG-3 guideline covers “general key management and controls”. It is based upon the X9.24 standard and deals specifically with managing “keys which encrypt PINs and keys which encrypt PIN encrypting keys”. This standard is concerned with both keys in an ATM – not only the “B-key” which typically encrypts PINs, but also the “A-key” which is loaded initially and used to encrypt the PIN encrypting key.

It is the requirements addressed by this section regarding initial ATM keys that are often problematic for institutions and frequently raise issues during a security audit. It is in response to these procedures that Trusted Security Solutions’ A98 system was developed.

An institution that employs the A98 solution for establishing initial ATM keys, supplemented by appropriate key management procedures, will be compliant with all the relevant provisions addressed by TG-3 and X9.24.

Take the Test

Selected questions from the TG-3 are provided below. See if your current procedures for creating or re-establishing an ATM’s initial key are compliant.

TG-3-2004 Section 3.2.2 “Documented procedures exist and are followed to ensure that each type of TRSM (e.g., ATMs, POS devices, host security modules and key loading devices) has been evaluated using the criteria referenced in Annex A of X9/TG-3-2004 and found to meet the applicable requirements.” TRUE FALSE
Reference X9.8 - Sec. 6.3; X9.24 Sec. 7.2

A98 Solution:

Until the discontinuance of the STAR approved equipment list, the A98 was listed as an approved key management solution. Further, STAR has installed A98’s for keying the ATMs it drives for its members and requires that all ATMs driven by STAR be keyed using the A98.

TG-3-2004 Section 3.2.4 “Any TRSM capable of encrypting a key and producing cryptograms of that key (e.g., HSM, KLD) is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of both of the following:
– Dual access controls are required to enable the key-encryption function.
– Physical protection of the equipment (e.g., locked access to it) under dual control.” TRUE FALSE
Reference X9.24 - Sec. 7.2, Sec. 7.3, Sec. 7.5

A98 Solution:

The A98 is a TRSM and enforces dual-control and split knowledge for all functions involving the entry of key components at the A98.

TG-3-2004 Section 3.2.5 “Documented procedures exist and are followed to ensure that a TRSM has not been subject to unauthorized modification or substitution before loading cryptographic keys. This assurance takes the form of, at a minimum, the following procedures:
– Physical inspection and/or testing of the equipment immediately prior to key loading;
– Physical protection of the equipment to prevent or detect access by unauthorized personnel from the time of manufacture or removal from service to the time of key loading (e.g., bonded carrier, device authentication code injected by terminal vendor and verified by terminal deployer, tamper evident packaging).” TRUE FALSE
Reference X9.8 – Sec. 6.1.1, Sec. 6.3.1, Sec. 6.3.3, X9.24 – Sec. 7.2

A98 Solution:

In addition to the intrusion detection and response mechanisms to erase keys when an opponent attempts penetration of the A98, the keyboard can be locked via a switch located behind a locked panel. The disk drives are key-locked into the RAID-I unit behind the same locked panel. All sensitive information stored on the disks are encrypted using 2K3D encryption.

TG-3-2004 Section 3.2.6 “Documented procedures exist and are followed to ensure that a stored TRSM is physically protected to protect against the possibility that the TRSM might be stolen, modified in an unauthorized way, and then returned to storage without detection (e.g., locked access).” TRUE FALSE
Reference X9.8 – Sec. 6.3.4; X9.24 - Sec. 7.2, Sec. 7.5

A98 Solution:

The A98 is a rack mounted unit that deters attempts to remove it. The keyboard can be logically locked by a switch located behind a locked access panel.

TG-3-2004
Section 3.3.1

“Documented procedures exist and are followed to ensure a person entrusted with a key component reasonably protects that component such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.”

Reference X9.24 – Sec. 7.1, Sec. 7.5

TRUE FALSE

A98 Solution:

The A98 key components are provided in our innovative, tamper-evident Comvelopes™, which totally restrict unauthorized viewing. Furthermore, in the A98 process, the random number in any Comvelope has NOT been pre-assigned to a specific ATM, reducing the threat of compromising the key. Prior to the new TMK being created on the host system, the contents of the Comvelopes are merely random numbers. Since the contents of the Comvelopes do not become components until the new TMK is established on the host system, it can be said that the components were under the full control of the custodians from the time of generation (each randomly selected a Comvelope) to the time of destruction of the Comvelope.

TG-3-2004
Section 3.3.2

“Documented procedures exist and are followed to ensure keys and key components are generated using a random or pseudo-random process such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys. A variant of a key must only be used for key separation, and not key generation.” Reference X9.24 – Sec. 7.4, Sec. 7.1

TRUE FALSE

A98 Solution:

A98 avoids the use of global initial ATM keys by creating keys by combining two randomly selected Comvelopes™, which contain random numbers generated by the A98 cryptographic unit at the time of Comvelope creation. The A98 prevents reuse of a Comvelope.

TG-3-2004
Section
3.3.14

“Documented procedures exist. Such procedures are followed if a key is compromised to ensure each of the following:

- A key is changed if its compromise is known or suspected;
- Keys encrypted under or derived from a compromised key are changed;
- A key is not changed to a variant or a transformation of the compromised key;
- Each occurrence of the compromised key, or component, is erased or destroyed;
- Any key(s) protected by or derived from the compromised key is erased or destroyed;
- Any key, shared with a communicating party, is changed if compromise is known, or suspected, and then communicating parties are immediately informed of the compromise and change in key(s), even if the key(s) is no longer in use;
- Appropriate records document the erasure or destruction of compromised keys, their key components, and cryptograms; and
- The amount of time in which the compromised key remains active is consistent with the risk to affected parties.”

Reference X9.24 – Sec. 7.1, Sec. 7.7, Sec. 7.8

TRUE FALSE

A98 Solution:

Traditionally, it has been difficult and inefficient to change ATM keys in a compliant manner. However, with A98 it's easy... A98's automation removes the resistance to changing a compromised key.

TG-3-2004
Section 3.3.3

“Documented procedures exist and are followed to ensure that when a key is manually loaded, its components are combined only within a TRSM.” Reference X9.24 – Sec 7.5.1

TRUE FALSE

A98 Solution:

The identity of the key components loaded into an ATM from Comvelopes™ is reported to the A98 system via an integrated Voice Response Unit (VRU), using a control number, not the actual Comvelope contents. Using this reference number, the A98 system retrieves the cryptograms of the contents of these two Comvelopes from its database and sends them into its integrated cryptographic unit. Within the A98 TRSM, they are decrypted from under the Master File Key, combined using xor to form the new ATM key, and then encrypted under a Key Encrypting Key for transport to the host. The use of Comvelopes simplifies policies for enforcement of dual-control at the ATM.

TG-3-2004 Section 3.3.5 “Documented procedures exist and are followed to ensure that, when transported, cleartext key components are protected from compromise in one or more of the following manners:

- Key components are transported in separate, tamper-evident, and authenticatable packaging;
- Key components are transported in a physically secure TRSM.”

Reference X9.24 – Sec. 7.5.1, Annex C

TRUE FALSE

A98 Solution:
 There are never any cleartext components transported in an A98 implementation. All Comvelopes contain only random numbers until the time they have been entered into an ATM AND their control numbers communicated to the A98 AND the new TMK is established on the host system.

TG-3-2004 Section 3.3.6 “Documented procedures exist and are followed to ensure a cleartext key component is maintained in one or more of the following manners:

- Under the supervision of an authorized person with access to this component;
- Locked in a security container in such a way that it can be obtained only by a person with authorized access;
- In secure transit (see 3.3.5);
- In a physically secure TRSM”.

Reference X9.24 – Sec.7.5

TRUE FALSE

A98 Solution:
 Secure supervision and transport of cleartext components are not an issue with the A98 solution. The A98 Comvelopes™ contain randomly generated, potential key components that have been pre-printed and stored in the A98 database along with a corresponding control number. Since they have not been assigned to any specific ATM, these Comvelopes™ can be distributed throughout the customer’s ATM network without risk of compromise and without the need for secure handling. Components are created when the Comvelope is opened, loaded into the ATM AND reported to the A98.

TG-3-2004 Section 3.3.8 “Documented procedures exist and are followed to protect the transfer of a key or key components into a TRSM to prevent the disclosure of a key or key components (e.g., minimal procedures include: visual inspection of TRSM equipment to detect evidence of monitoring and dual control of the loading process).”

Reference X9.24 – Sec.7.5

TRUE FALSE

A98 Solution:
 This provision is enforced by the A98’s requirement for two different servicers to report the Comvelope™ control numbers to the A98 VRU for the establishment of an ATM key. While appropriate procedures are required at the ATM, all manual ATM key management is eliminated at the Host side. Host side manual key management is required for the A98 Master Key as well as any Key Encrypting Keys shared with an HSM. All such keys are 3 component double length.

TG-3-2004 Section 3.3.9 “Documented procedures exist and are followed to ensure that all keys in PIN entry devices are, except by chance, unique to that device.”

Reference X9.24 – Sec. 7.6

TRUE FALSE

A98 Solution:
 A98 provides an efficient solution to avoid having a global initial key in a group of ATMs. There is a negligible probability that any two random Comvelopes selected by two servicers would produce the same key. Once two Comvelopes™ are used to create an ATM key, the A98 marks them as “used” and makes them unavailable for re-use.

TG-3-2004 Section 3.3.16 “Documented procedures exist and are followed to ensure that if key components of an operational key are no longer required; such components are destroyed using appropriate methods of destruction for each media type used.

Paper-based keying materials must be destroyed by crosscut shredding, burning or pulping. All residues should be reduced to pieces 5 mm or smaller. When material is burned, the residue should be reduced to white ash. Key components stored on other media must be destroyed so that it is impossible to recover by physical or electronic means. Destruction of keying materials must be accomplished under conditions of full accountability with appropriate records retained for audit trail purposes.”

Reference X9.24 - Sec 7.8

TRUE FALSE

A98 Solution:
 The top portion of an A98 Comvelope™ instructs the user to destroy the perforated bottom portion where the key component is listed. This top section also provides an optional “confidentiality statement” which the user can sign, have witnesses sign, and return to the audit department as an attestation that proper destruction procedures were followed. Furthermore, the A98 automatically logs all keying activity at each ATM.