

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 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
800-467-9146
info@trustedsecurity.com
www.TrustedSecurity.com

ection 3.3 of the TG 3 guideline covers “gen and deals specifically with managing “keys which encrypt PINs and keys which encrypt PIN encrypting both – not only the “B key” which typically -key” which is loaded initially and used to encrypt the PIN encrypting key.

I initial ATM keys that are often problematic for es 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-3-1997 “Each type of TRSM has been evaluated using the criteria in Appendix A and found to TRUE FALSE
Section 3.2.1 meet the applicable requirements.”

Reference X9.8 - Sec. 6.3; X9.24 Appendix G

A98 Solution:

The A98 is on the STAR approved equipment list. This is normally accepted as Prima Facie that the equipment is compliant.

TG-3-1997 “Any TRSM capable of encrypting a key and producing cryptograms of that key is TRUE FALSE
Section 3.2.3 protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or 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.”

Reference X9.24 - Sec. 3.1, Sec. 3.6, Appendix G

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-3-1997 “Procedures exist and are followed to determine that a TRSM has not been subject to TRUE FALSE
Section 3.2.4 unauthorized modification or substitution prior to loading cryptographic keys. This assurance takes the form of one or more of 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 initial key loading, (e.g. bonded carrier, device authentication code injected by terminal vendor and verified by terminal deployer, tamper evident packaging).”

Reference X9.24 - Sec. 3.2; X9.8 Sec. 6.1.1

A98 Solution:

The A98 implements intrusion detection and response mechanisms to erase keys when an opponent attempts penetration of the A98.

TG-3-1997 “Procedures exist and are followed to ensure that the TRSM, is physically protected TRUE FALSE
Section 3.2.5 (e.g., locked access) to protect against the possibility that the TRSM might be stolen, modified in an unauthorized way, and then returned to storage without detection.”

Reference X9.24 - Sec. 3.2

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-3-1997 “Procedures exist and are followed to control keys so they exist only in one or more of the TRUE FALSE
Section 3.3.1 following forms:
- in a TRSM (tamper resistant security module);
- encrypted under a DEA (“Data Encryption Algorithm” or DES) key;
- managed as two or more full-length components using the principles of dual control
and split knowledge.” Reference X9.24 – sec. 3.1, Sec. 3.5

A98 Solution:

The A98 system unit contains a Tamper Resistant Security Module. All clear-text cryptographic functions are handled inside the A98’s TRSM. All shared keys used by A98 are stored encrypted using DEA under a double length master file key. The A98 process simplifies enforcement of “dual control and split knowledge” when loading an ATM key by requiring the use of two (2) Comvelopes™, each containing a component secured in a tamper-evident envelope.

TG-3-1997 “Procedures exist and are followed to ensure a person entrusted with a key component TRUE FALSE
Section 3.3.2 reasonably protects that component such that no person (not similarly entrusted with that
component) can observe or otherwise obtain the component.” Reference X9.24 – Sec. 3.5

A98 Solution:

The A98 key components are provided in our innovative, tamper-evident Comvelopes™, which restrict unauthorized viewing. Furthermore, in the A98 process, the component in any Comvelope has NOT been pre-assigned to a specific ATM, reducing the threat of compromising the key. The components are not created until the Comvelope is opened by the custodian. It is therefore under the control of the custodian from creation to destruction.

TG-3-1997 “Procedures exist and are followed to ensure keys and key components are TRUE FALSE
Section 3.3.3 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.” Reference X9.24 – Sec. 3.4; X9.8 – Annex E

A98 Solution:

A98 avoids the use of global initial ATM keys by creating keys by combining two randomly selected Comvelopes™, which contain randomly generated key components. The A98 prevents reuse of a Comvelope.

TG-3-1997 “Procedures exist to ensure each of the following: TRUE FALSE
Section 3.3.4 - 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;
- the amount of time in which the compromised key remains active is
consistent with the risk to affected parties.” Reference X9.24 – Sec. 3.1

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-3-1997 “Procedures exist and are followed to ensure that when a key is installed TRUE FALSE
Section 3.3.6 under dual control via key components that these key components are
combined only within a TRSM.” Reference X9.24 – Sec 3.5

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 component value. Using this reference number, the A98 system retrieves the cryptograms of these two components from its database and brings them into its integrated TRSM. Within the A98 TRSM, they are decrypted from under the Master File Key, combined to form the actual ATM key, and then encrypted under a Key Encrypting Key for transport to the host. The use of Comvelopes simplify policies for enforcement of dual-control at the ATM.

TG-3-1997 “Procedures exist and are followed to ensure TRUE FALSE
Section 3.3.8 when in secure transit, cleartext key components are protected from compromise in one or
more of the following manners:
- Key components are transported in separate tamper-evident packaging;
- Key components are transported in a physically secure TRSM.”
Reference X9.24 – Sec. 3.5

A98 Solution:
A98’s cleartext components are printed in our innovative, tamper-evident packaging, known as Comvelopes™.

TG-3-1997 “Procedures exist and are followed to ensure a cleartext key component is: TRUE FALSE
Section 3.3.9 - under the supervision of a person authorized by management with access to this
component;
- locked in a security container in such a way that it can be obtained only by authorized
access;
- in secure transit;
in a physically secure TRSM.” Reference X9.24 – Sec. 3.5, Appendix B

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 fear of compromise and without the need for secure handling. Components are created when the Comvelope is opened AND loaded into the ATM AND reported to the A98.

TG-3-1997 “Procedures exist and are followed to protect the transfer of a key or key components into TRUE FALSE
Section TRSM so as to prevent the disclosure of key or key components. Examples of procedures
3.3.11 include: visual inspection of TRSM equipment to detect evidence of monitoring and dual
custody of loading process.”
Reference X9.24 – Sec. 3.1

A98 Solution:
This provision is enforced by 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.

TG-3-1997 “Procedures exist and are followed to prohibit, except by chance, the entry or use TRUE FALSE
Section of the same key in more than one PIN entry device.”
3.3.13 Reference X9.24 – Sec. 3.6

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 an institution using the A98 would produce the same key loaded into multiple ATMs. Once two Comvelopes™ are used to create an ATM key they are made unavailable for any other use.

TG-3-1997 “Procedures exist and are followed to ensure a key or key component that has been used TRUE FALSE
Section for a cryptographic purpose is erased or destroyed when it is no longer required, i.e. active
3.3.16 or archived, (e.g. appropriate records document that the erasure/destruction has
occurred.)”
Reference X9.24 - Sec 3.8

A98 Solution:
The top portion of an A98 Comvelope™ instructs the user to destroy the perforated middle 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. Furthermore, the A98 system automatically collects an extensive audit log of all keying activity at each ATM.