

A98 for Remote Re-Key

A98™ Remote Re-Key Process

Trusted Security Solutions Inc. offers the A98 ATM Initial Key Establishment System to institutions that manage the cryptographic keys for ATMs. A98's patented process is in use at banks, credit unions, and large processors throughout the US and UK.

With the introduction of its new "Remote Re-Key Module", A98-R automates both the generation and distribution of cryptographic keys for ATMs. A98-R is compatible with ATMs that use RSA-enabled encrypting pin-pads (EPPs). The A98-R delivers random master keys in full compliance with ANSI standards and with network mandates for Triple-DES and unique keys per ATM.

The A98-R implements both Diebold's Certificate Based Protocol (CBP) and NCR's Signature Based Protocol (SBP) that are defined in the emerging ANSI X9.24-2 Standard on Retail Cryptographic Key Management. The Diebold approach uses X.509 certificates and PKCS message formats to transport key data. NCR's method relies on digital signatures to ensure data integrity. Both processes require the ATM's EPP to be loaded at the factory with signed Public Keys or Certificates. In addition, an A98 public key must be signed by a Certificate Authority (i.e. Diebold or NCR) and imported back into the A98 during system initialization.

The remote re-key process requires the A98 to be authenticated by the ATM. In this step either the signed A98 public key or its certificate is sent from the A98 to the ATM. Once verified, the ATM will send its EPP public key to the A98. (In the case of Diebold, both an encryption and verification EPP public key is sent.) The A98 stores the EPP data and then generates a new DES key, encrypts it with the EPP's public key, prepares the required message format, and sends this new master key to the ATM. When the EPP responds that it successfully loaded the key, A98 sends a cryptogram of this new key to the host for loading into the terminal data base.

In the initial release of the A98 Remote Re-Key module, the interface to the ATM will be implemented through the terminal handler or device driver. Trusted Security has defined an XML data structure that will be used to communicate with the driver over a TCP/IP link. This approach confines modifications to the ATM device driver and eliminates any need to change the host security module or terminal driving application software. All the public key cryptography, message formatting, database access, and user interface programming is provided in the A98 module.

By integrating the remote re-key module into the conventional A98 platform, Trusted Security continues to lead the industry by providing the most efficient, compliant, and cost-effective key establishment solution for *all* ATMs. The A98-R system not only fully automates key distribution for public key-enabled ATMs, but also continues to support single- and triple-DES key loading for legacy ATMs.



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

A98™ Remote Re-Key Module

Software - Extension to the standard A98 software to support RSA encryption, PKCS certificates and digital signatures.

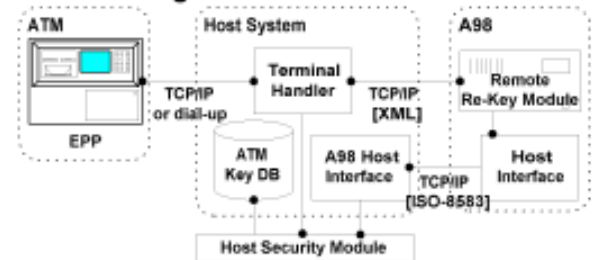
Protocols - NCR and Diebold protocols are supported using an XML structure.

Interface - TCP/IP connection to the terminal handler. Host interface uses the existing ISO-8583 message format or the new XML interface through the terminal handler.

A98™ Remote Re-Key Module

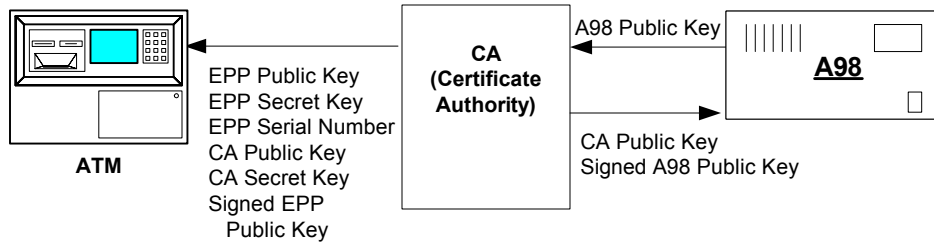
- Automatically creates and distributes ATM master keys
 - eliminates manual on-site key loading
 - reduces key management costs
 - conforms to ANSI security standards
- Implements NCR and Diebold protocols
- Incorporated into the existing A98 platform to provide the most efficient and complete solution for both legacy and EPP-enabled ATMs

A98-R Configuration

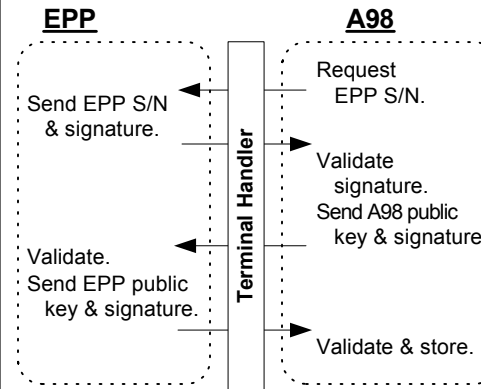


Trusted Security Solutions, Inc.
 416 West John Street
 Matthews, NC 28105
 704.849.0036
www.trustedsecurity.com

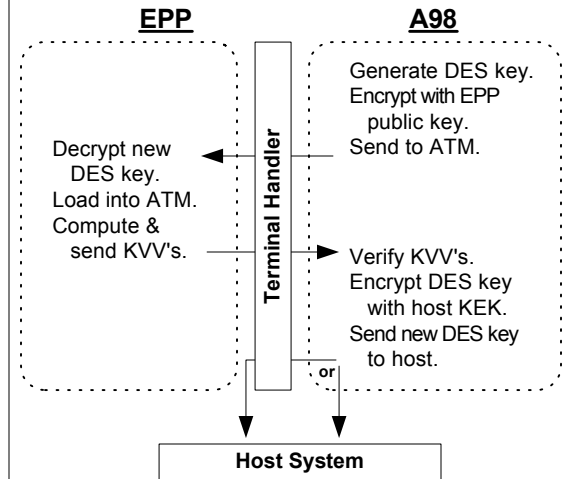
Signature Based Protocol (SBP) Set Up



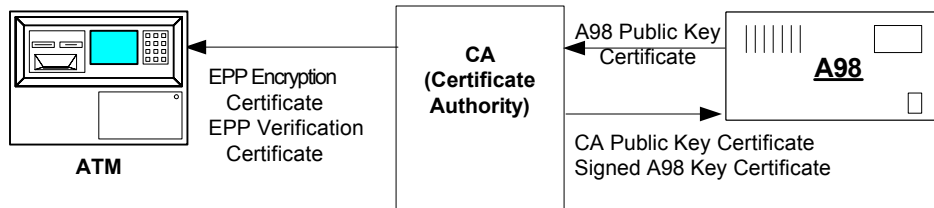
ATM Authentication



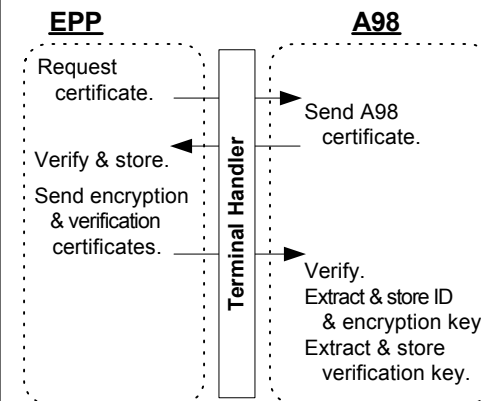
ATM Key Loading



Certificate Based Protocol (CBP) Set Up



ATM Authentication



ATM Key Loading

