A98™ Process: Remote Key

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, networks, and large processors throughout the US and internationally.

With the introduction of the Remote 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 implements both Diebold and Triton Certificate Based Protocols (CBP) and NCR and Wincor-Nixdorf's Signature Based Protocol (SBP) that are defined in the ANS X9.24 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, as part of the initialization process, at least one A98 key pair must be generated and the public key signed by a Certificate Authority and imported back into the A98 before the A98 can successfully communicate with the public key ATM. A separate key pair is required for each ATM manufacturer.

The remote key process requires that mutual authentication first be established between the A98-R and the ATM EPP. Communications between the A98-R and the EPP is controlled and mediated by a separate Terminal Handler if not directly connected to the A98-R. During the Authentication step, the EPP sends its Public Key information to the A98-R via the Terminal Handler. Once the appropriate EPP Public Key information is exchanged and verified, it is stored in the A98-R database associated with the EPP and the A98-R responds with its Public Key information to be sent to and verified by the EPP

Once mutual authentication is established, if a request for a new Terminal Master Key is received, the A98-R retrieves the previously stored EPP Public Key data, generates a new Terminal Master Key encrypted under the EPP's Public Key, formats the new Master Key payload appropriately, and sends it to the Terminal Handler to forward down to the EPP.

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-R module.

By integrating the remote 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.

A98 ATM Initial Key Establishment System

developed by Trusted Security Solutions, Inc.

A98 System Unit - Pentium processor, two mirrored hard disk drives and a hot spare, redundant power supplies, Windows Server 03 OS, RAID 1 mirrored drives, two network interfaces, internal voice response unit and SafeNet cryptographic unit, color monitor, keyboard with mouse, rack mounted enclosure with dual-key custodial control.

A98 System Software - Custom application with cryptographic unit support, voice response processing, scheduled unattended backup, key management module, and complete administrative functions. Supports all Triple-DES requirements. The browser-based remote eHelpDesk module allows support staff to pull reports and perform many tasks from their desks.

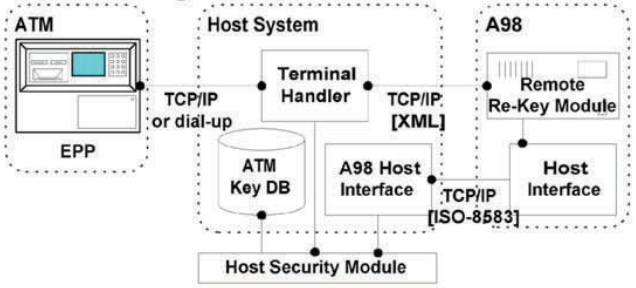
A98™ Remote Key Module

Software - Extension to the standard A98 software to support 2048 bit RSA encryption, PKCS certificates and digital signatures.

Protocols - NCR, Diebold, Triton, and Wincor-Nixdorf protocols are supported using an XML structure.

Interface - TCP/IP connection to the terminal handler. Host interface uses the either an XML interface or an ISO-8583 formatted message through the terminal handler.

A98-R Configuration



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

A98 for Remote Re-Key

A98™ Remote Key Module

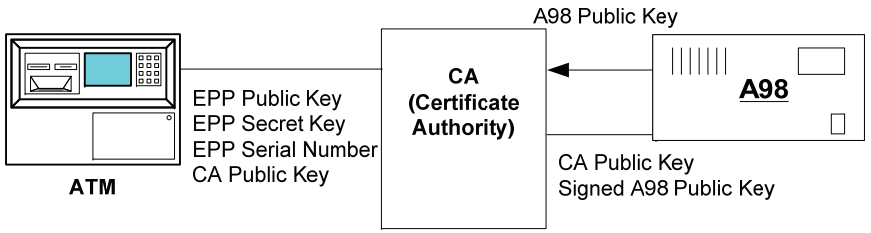
- **Automatically creates and distributes ATM master keys**
  - **eliminates manual on-site key loading**
  - **reduces key management costs**
  - **conforms to ANSI security standards**
- **Implements Diebold, NCR, Triton, and Wincor-Nixdorf protocols**
- **Incorporated into the existing A98 platform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

Trusted Security Solutions, Inc.
— US Patent #6,606,387 __

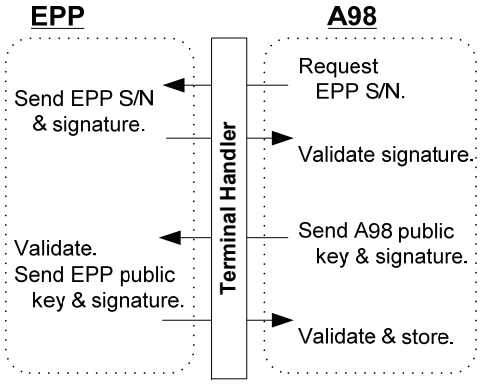
A98 ATM Initial Key Establishment System

A98-R System Overview

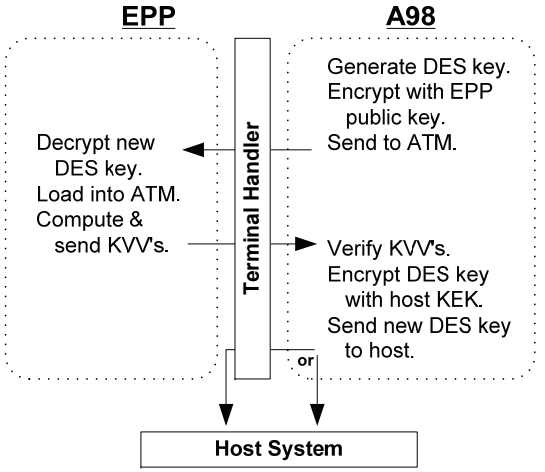
Signature Based Protocol (SBP) Set Up



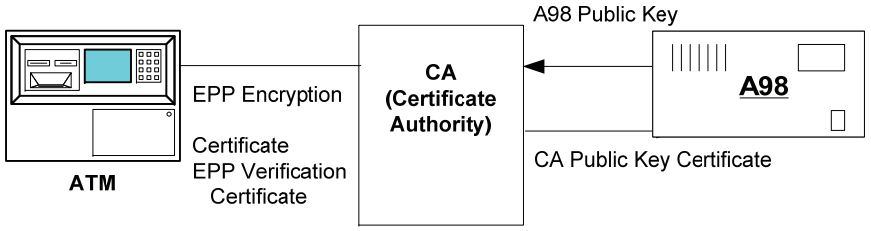
ATM Authentication



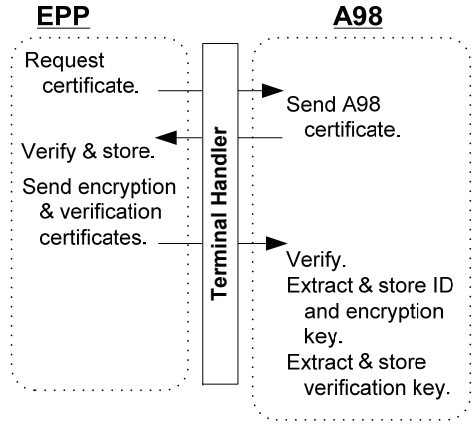
ATM Key Loading



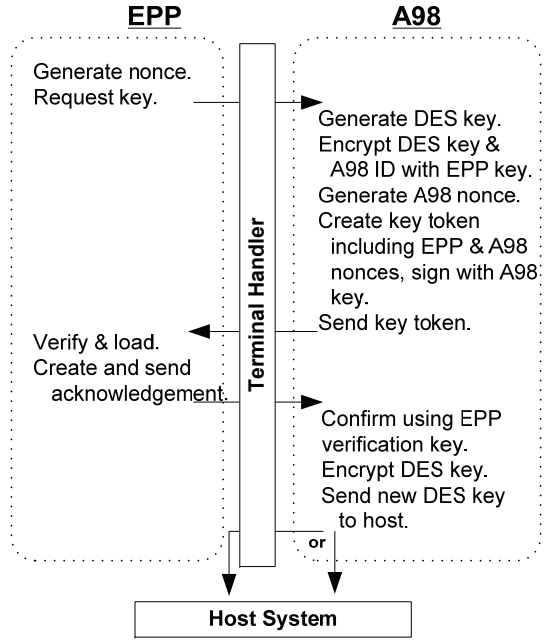
Certificate Based Protocol (CBP) Set Up



ATM Authentication



ATM Key Loading



Trusted Security Solutions

June 2009