A98™ Proceso: Remote Re-Key

Trusted Security Solutions Inc. ofrece su producto “A98 ATM Initial Key Establishment System “ a instituciones para que administren las claves de cryptografia de sus “ ATMs”. El proceso de A98’s esta patentado y es usado en los bancos., entidades de ahorro, redes y procesadores en US e Internacionalmente.

Con la introducción de “Remote Re-Key Module, A98-R” se logra automatizar tanto la generación como la distribución de los criptogramas para los “ATMs”. A98-R es compatible con ATMs que usan “ RSA-enabled encrypting pin pads (EPPs)”. A98-R implementa ambos protocolos “ Diebold’s Certificate Based Protocol (CBP)” y el “ NCR’s Signature Based Protocol (SBP)” como se indica en el manual “ANS X9.24-2 Standard on Retail Cryptographic Key Management”. Diebold usa el formato de mensaje “X.509 certificates and PKCS” como transporte de la llave. NCR’s se basa en el metodo de firmas digitales para asegurar la integridad de la data. Ambos procesos requieren que el “EPP” del “ATM’s” Sea cargado en le momento de ser manufacturado con su clave publica o Certificado. Adicionalmente como parte del proceso de inicialización, al menos un par de claves “A98 key” debe ser generado y la llave publica debe ser autenticada por una Autoridad Certificadora (EJ: Diebold o NCR) e importada dentro de la unidad “ A98” antes de que exitosamente se comunique con con la llave publica del ATM. Un par de claves o llaves separadas es requerida por “ SBP” y “ CBP”.

El proceso de “ re-key” requiere primero que se establezca una autentificación mutua entre “A98-R” y el “ATM EPP”. La comunicación entre el “A98-R” y el “ EPP es controlada por el manejador de terminales conocido como “Terminal Handler”. Durante el paso de autentificación, el “ EPP” envía la información de su “Public Key” a la unidad de “A98-R”. Una vez que la clave publica apropiada es intercambiada y verificada, ella es almacenada en la base de datos del “A98-R”, de igual forma la clave publica del “ EPP” y el “A98-R” regresa a el “EPP” para ser verificada.

Una vez que se ha establecido la autentificación mutua, el “A98-R” genera la nueva “Terminal Master Key” cifrada bajo la clave publica del “EPP’s”, se formatea la nueva “ Master Key” y se envía a el “ Terminal Handler” para su transmisión a el “EPP”.

Trusted Security ha definido una estructura de datos en “ XML” usada para comunicarse con el “diver” sobre un enlace TCP/IP. Este e nfoque confina modificaciones a el “ATM device driver” y elimina la necesidad de cambiar el “HSM” o el “ terminal driving application software” Todas las llaves de criptografía publica, formateo de mensajes, acceso a bases de datos e interfaces de programación son provistos por el modulo de “A98-R”. Trusted Security continua siendo el líder de la industria en proveer mas eficiente y a un costo razonable el establecimiento inicial de llaves “KEY” en todos los ATM’s.

A98 ATM Initial Key Establishment System

A98 System Unit – Procesador “Pentium”, Windows Server 2003, RAID 1 discos espejos “mirrored”, Fuentes de poder redundantes, Tarjeta para interface de red, unidad de respuesta de voz interna (IVR), “SafeNetâ cryptographic facility”, puertos USB en el frente, Monitor a color , teclado con ratón “mouse” incorporados en un “rack” Con una doble llave de control.

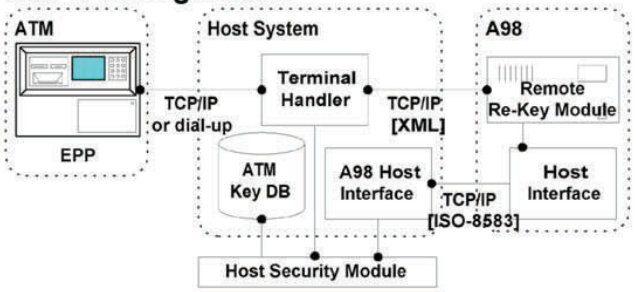
A98 System Software – Aplicación personalizada con Soporte criptográfico, procesamiento de respuesta de voz, programa de respaldo desatendido, modulo de gerencia de llaves, y funciones administrativas completas. Suporta todos los requeimientos triple DES. Un modulo de ayuda basado en tecnología “web browse” permite que el personal de sopotrte pueda generar reportes o ejecutar algunas tareas desde su puesto de trabajo.

Software - Extensión al software estándar de A98 para soportar cifrado RSA, PKCS, certificados y firmas digitales digital signatures.

Protocolos - Protocols NCR, Diebold, Wincor-Nixdorf, y Triton soportados usando estructuras XML. Wincor y otros basados en firmas digitales tambien estan disponibles.

Interface – Conexion TCP/IP ta el “ terminal handler”. Se usa formato ISO-8583 para interactuar con el “Host interface” o XML para el “terminal handler”.

A98-R Configuration



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

A98 for Remote Re-Key

- **Automáticamente crea y distribuye “Master keys” unicas**
  - **elimina la carga manual en sitio**
  - **reduce los costos de administración de llaves**
  - **conforme a los estándares de seguridad ANSI**
- **Implementa NCR, Diebold, Wincor-Nixdorf, Triton y otros protocolos basados en firmas**
- **Incorporado dentro de la plataforma existente de A98**
- **La plataforma provee la solución mas eficiente y completa para ambos tipos de carga de llaves en ATM’s tradicional y remota**

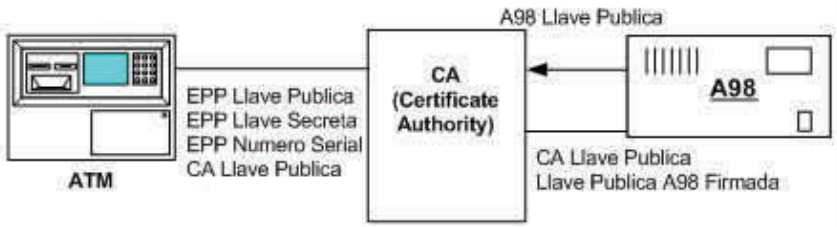
Trusted Security Solutions, Inc.
— US Patent #6,606,387 __

A98 ATM Initial Key Establishment System

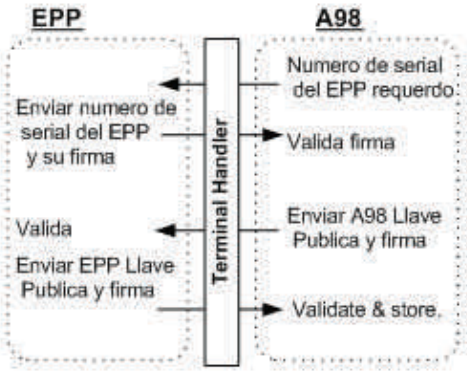
Descripción General de Sistema de A98-R

Signature Based Protocol (SBP)

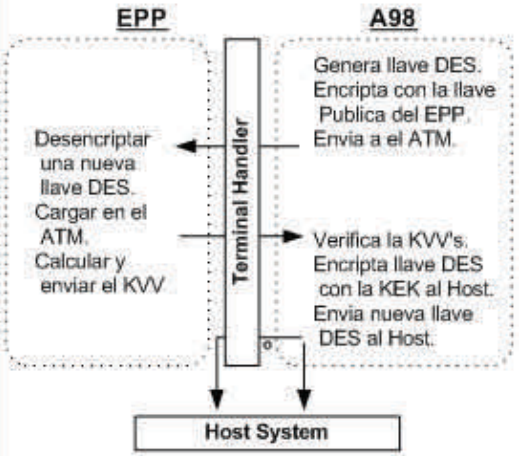
Set Up



ATM Authentication

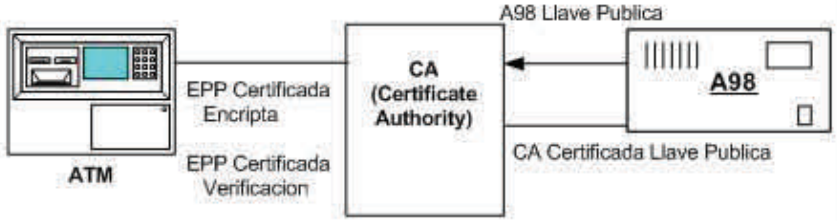


ATM Key Loading



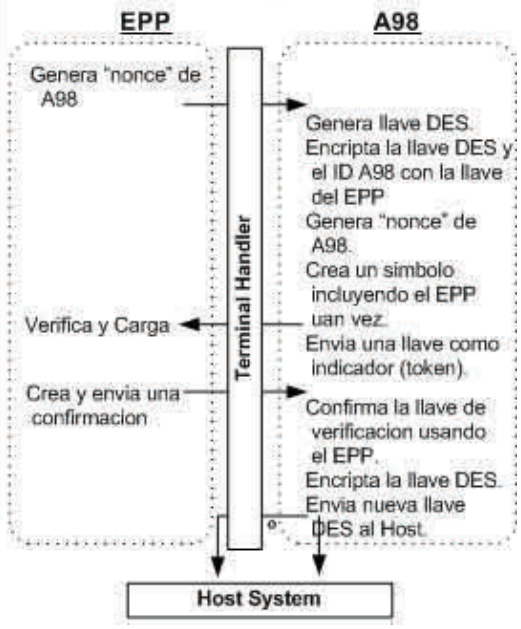
Certificate Based Protocol (CBP)

Set Up



ATM Authentication

ATM Key Loading



Trusted Security Solutions

June 2009