A98™ Proceso: Modo Convencional

Trusted Security Solutions Inc. ofrece la solución "A98 ATM Initial Key Establishment System" a instituciones que administrant las llaves criptográficas de sus "ATMs". A98 trabaja con todos los "ATMs" y evita requerimientos no apropiados asociados con la administración de llaves.

La norma "ANSI Standard X9.24, Retail Key Management", requiere que cada dispositivo de cifrado de claves "EPP" tenga una única llave en triple DES. Muchas organizaciones que manejan "ATMs" erróneamente asumen que
cargar una llave única manualmente en todos los ATM'S les permite cumplir con el estándar "X9.24". Sin embargo, la llave inicial debe ser única y también secreta.

Proveer una clave inicial por "ATM" es particularmente una tarea complicada debido a la complejidad del proceso de administración de llaves. Métodos tradicionales están centrados en un control de los componentes requiriendo de un gran número de custodios lo cual lo hace ineficiente y costoso. La solución de A98 evita todos estos problemas y permite su implementación de manera no Invasiva, cumpliendo con las reglas operativas de las redes y siguiendo los estándares ANSI . La solución incorpora el manejo de las llaves de criptografía publica, tal como el modulo "A98-R Remote Key" disponible para aquellos "ATMs" que soportan el "remote key ready". La opción de llaves publicas generalmente requieren de cambios de "hardware" y "software" en los ATM".

Con el enfoque de "A98", en vez de generar una llave y luego descomponerlo en componentes o generar componentes y asignarlos a una llave especifica, los componentes no son asignados hasta el punto en el cual ellos son cargados en el ATM. Estos componentes están contenidos en sobres de seguridad ("Trusted Security's innovative tamper-evident Comvelopes"), Los cuales son distribuidos en forma aleatoria ("random") y almacenados en las agencias, ATMs o custodios. Posteriormente esos sobres o componentes(" Comvelopes) seleccionados en forma aleatoria y almacenados en los ATMs, cada custodio llama por teléfono a la unidad de respuesta de voz del A98 (IVR) e ingresa el numero de control que identifica al sobre (" Comvelope"). Los dos componentes identificados son almacenados en forma encriptado bajo la "Master key" del A98, los mismos son combinados en el "A98 Tamper Resistant Security Module (TRSM)" para formar la misma llave que ha sido cargada en el ATM. La nueva llave creada es encriptada dentro del "TRSM" usando una "KEK" compartida con el servidor que administra la red de ATM's. La llave del ATM encriptada es enviada al servidor ("Host") vía un mensaje ISO8583 o en formato XML. Cuando el ATM es conectado , un mensaje es recibido, entonces el "software" del "Host" lo procesa normalmente generando una llave " PIN encrypting key" en dos formas (por la nueva llave cargada en el ATM y bajo la "Master File Key" del "Host".

El ATM ahora contiene una única clave o llave triple DES y completamente conforme a los estándares.

A98 ATM Initial Key Establishment System

developed by Trusted Security Solutions, Inc.

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 Printer – Opcionalmente se prove una impresora de matrix que puede conectarse directamente a la unidad de criptografía para imprimir en forma local los componentes de las llave (KEK y MFK).

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.

A98 Key Security – El sistema A98 viene con sobres que contiene serial numerado "tamper-evident" para almacenar el material "cleartext-keying" en tres cajas de seguridad .

Triple-DES Support – El "software" A98 soporta completamente todos los requerimientos triple DES.

Public Key Support – El "Hardware A98" como tal Suporta la administración de claves o llaves en forma remota usando la modalidad criptográfica de claves o llave publicas

Host Interface - TSS provee soporte para los interfaces de BASE24™, Postillion™, Connex™, CV Systems™, y otros también disponibles respectivamente de terceros. TSS también usa el esquema estándars de "XML" para interactuar con sistemas propietarios..

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

A98 for TRIPLE-DES

- **A98 le proporciona a sus ATM's cumplir con los requerimientos de llaves unicas**
- **Suministra un soporte completo de 3DES**
- **No se erquiere cambios en sus ATM's**
- **Evita los problemas logisticos asociados con la administracion de llaves**
- **Mantiene un registo detallado de auditoria para todas las actividades sobre los ATM's**
- **Mantiene un registo detallado de auditoria para todas las actividades sobre los ATM's**
- **Soportadas por el modulo de A98-R**

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

A98 ATM Initial Key Establishment System

System Overview

1 – Los componentes de las llaves son generados por Trusted Security Solutions e impresos en sobres de seguridad (Comvelopes) y distribuidos a las diferentes localidades

6 – A98 encripta la nueva llave bajo la KEK compartida

A98 Host Interface

7 – A98 usa el interfase de comandos para insertar el Criptograma del ATM en la B.D. del Manejador de ATM's (Host)

5 – A98 combina las dos componentes en una llave inicial identica a la del ATM

2 – Componentes son ecriptados y cargados en la B.D. del A98 y referenciado por el Nro. De control en el Comvelope.

ATM Host System

Grupo de Comvelopes©

4 – Cada custodio reporta el ATM ID y Nro de control del Comvelope a la unidad de respuesta de voz VRU

8 – El Host envia el nuevo PIN Encription Key a el ATM, encriptodo bajo la llave inicial del ATM

3 – Cualquier combinacion de custodios o empleados del banco purden selectionar al randon los sobres (Comvelope) e ingresar al ATM los componentes (simple o doble)

Person 1

1234

Comvelope™ Triple DES

Person 2

5678

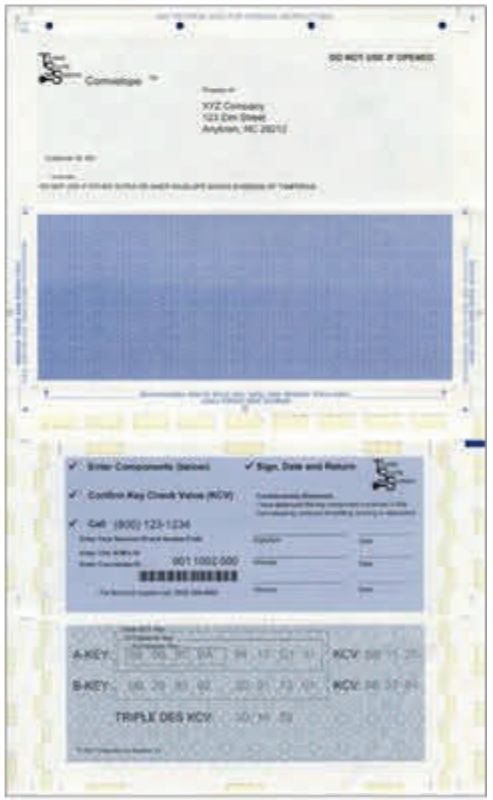
Comvelope™ Triple DES

Telefono

ATM

Comvelope©

Triple DES Versión



Trusted Security Solutions

Apr 2004