

## A98™ Módulos de Servicios para Tarjetas

El A98-C (Modulo de Servicios para Tarjetas) puede ser instalado desde fábrica o también una actualización para la familia de productos A98, disponible únicamente para los modelos A98-A, A98-R o A98-A/R. El A98-C es una aplicación individual sin dependencias externas de ningún tipo de unidad criptográfica y provee soporte para operaciones básicas de Tarjetas de Pago. El A98-C ha sido diseñado para aquellas instituciones que emiten sus propias tarjetas y calculan todos los componentes de la tarjeta, incluyendo banda magnética y PIN. La versión actual del A98-C se conecta a través de un interfase serial al puerto de la máquina embosadora utilizando como protocolo ## de Datacard® para impresión de tarjetas una a una o en lotes. Adicionalmente, el A98-C se conecta a una impresora láser o similar para imprimir en forma segura los sobres para entrega de PIN. Tanto el embosser como la impresora láser son manejados directamente a través de un puerto serial en la unidad criptográfica integrada en el A98-C. El cálculo de los campos de seguridad CVV1, CVV2, IBM3624 PIN, VISAPVV PIN y sus Offsets son realizados íntegramente dentro de la Unidad Criptográfica y transferidos DIRECTAMENTE al embosser o impresora de sobres de envío de PIN. Adicionalmente, la función de verificación de PIN (PINVER) del A98-C se encuentra disponible para los usuarios del A98. Por ejemplo, la función de verificación de PIN del A98-C permite realizar la verificación de PIN del ATM sin necesidad de un HSM (Host Security Module) adicional.

### Operación General

A través de tecnología TCP/IP y XML la aplicación del cliente, utiliza un interfase para acceder a la funcionalidad deseada del módulo A98-C y utilizar las funciones del A98-C con sus parámetros específicos, el A98-C recibe y procesa el mensaje XML, realiza las operaciones señaladas y envía de regreso los resultados indicando si la operación fue o no exitosa. Todas las operaciones criptográficas son ejecutadas por la unidad criptográfica del A98-C. Las llaves utilizadas son de doble longitud y son mantenidas encriptadas bajo la Master Key del A98 o una KEK (Llave de encriptación de trabajo Key Encryption Key) común entre el A98 y el HSM (Host Security Module) del cliente. El A98-C utiliza ANSI X.9 y procedimientos aprobados por las más grandes redes para el establecimiento de su Master Key File (MKF) y las necesarias llaves de comunicaciones.

La aplicación del cliente envía al embosser una trama de datos en formato apropiado. La posición de los campos seguros, como CVV1, CVV2 y OFFSET, son indicados en el mensaje por TOKENS. El A98-C reemplaza cada TOKEN con sus apropiados valores y envía la data al embosser. Las impresoras de sobres de tarjetas son manejadas de idéntica forma, la aplicación del cliente señala el TOKEN del PIN en la data.



developed by Trusted Security Solutions, Inc.

**Soporte e Instalación** - Introducir el A98-C en la operación actual del tarjetas es un proceso que se reduce al uso de las funciones especializadas y las aplicaciones que soportan la encriptación de los campos seguros (CVV1, CVV2 y OFFSET) y la verificación de PIN (PINVER) en la base de datos interna del A98. En organizaciones que utilizan más de una FI (Financial Institution), cada FI es referida por una etiqueta que permite acceder a toda su información particular. Una vez que las llaves y las tablas de decimalización se encuentran instaladas, estas son encriptadas bajo la Master Key del A98-C y la opción de Respaldo Desatendido del A98 se utiliza de acuerdo a las Reglas Generales de Recuperación de Negocio.

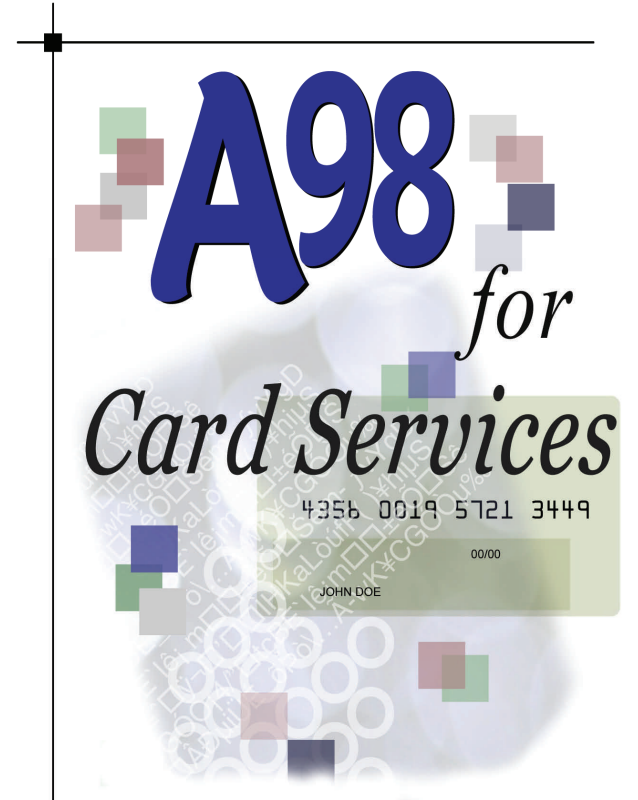
**Verificación de PIN** - Tanto la verificación IBM3624 como la Visa PVV PIN son ejecutadas dentro de la unidad criptográfica interna del A98-C. Aplicaciones de Host que han sido preparadas para soportar HSM standard pueden interfazarse directamente con el A98-C sin necesidad de realizar cambios a su programación, utilizando el interfase de TSS que es idéntico al interfase de un HSM Standard.

**Llave de Seguridad del A98** - El sistema A98 incluye el equipo y los procedimientos para crear y administrar de acuerdo a las reglas impuestas por la industria las necesarias Llaves de Archivos Maestros (Master File Keys) y otras llaves asociadas al uso del intercambio de llave simétrica utilizada por el A98-C. La información del emisor es manipulada sin tener acceso a la llave real.

**Otras Capacidades del A98** - El A98 se comporta como un sistema total de Administración de Llaves para ATMs, utilizando sea bajo su proceso patentado Comvelope™ o Llave Remota para los ATMs que lo soporten.



Trusted Security Solutions, Inc.  
1500 Orchard Lake Drive  
Charlotte, North Carolina 28270  
704.849.0036  
[www.trustedsecurity.com](http://www.trustedsecurity.com)



- **Permite a las instituciones financieras y otras organizaciones procesadoras de tarjetas tomar control de sus funciones de emisión de tarjetas y sobres de envío de PIN.**
- **Provee todas las funciones criptográficas para crear o reemitir tarjetas para producción en alto relieve y sobres de envío de PIN.**
- **Permite a los emisores mantener el PIN de un PAN a otro**
- **Genera los valores de PAN, CVV, PIN y OFFSET en forma transparente para la máquina embosadora e impresora de sobres de entrega de PIN.**

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

### Datos del A98-C

- PAN Original
- Nuevo PAN
- VNAME (Incluyendo llaves del emisor, Tablas de Decimalización, etc.)
- Fecha de Expiración
- Fecha de Servicio
- Cadena para el Embosser (...token.....)
- Data para la impresora de sobres (...token.....)
- Y mas .....

### Funciones Realizadas

- Emisión de tarjetas nuevas
- Re-emisión de tarjetas
- Conversión de tarjetas nuevas (batch)
- PIN bridging (nuevo PAN, mismo PIN)
- Calculo de CVV1 and CVV2
- PIN offset
- Algoritmos IBM y PVV
- Y mas .....



Card Embosser



Interfase A98-Systema Central

A98-C



RS232

RS232



Impresora de Sobres de Tarjetas

1 – El Sistema Central procesa los archivos de tarjetas para generar las cardenas de datos con el formato apropiado para la impresorara de tarjetas y la impresora de sobres de tarjetas, reemplazando los espacios de CVV y PIN por tokens.

2 – El interfase con el Sistema Central envia la información formateada para la impresora de tarjetas o impresora de sobres de tarjetas al A98-C utilizando XML sobre TCP-IP. A criterio de la institución especificos datos del cliente pueden ser encriptados para ser enviados entre el Sistema Central y el A98-C .

3 – El A98-C puede recibir data formateada en diskette o cualquier medio removible, como por ejemplo infomación de nuevos emisiores para el caso de un bureau de servicios, (tablas de decimalización, llaves, etc.) o datos de emisión de tarjetas o impresion de sobres. .

4 – El A98-C recibe cadenas de caracteres formateadas y reemplaza los tokens con los nuevos valores calculados. Con el uso de tokens, el formato de salida puede variar de acuerdo a la impresora de tarjetas o de la impresora de sobres de tarjetas.

5 – El A98-C envia a la impresora de tarjetas o a la impresora de sobres de tarjetas las cadenas de caracteres con los nuevos valores CVVs, PINs, y Offsets.