

A98™ Card Services Module

The A98-C (Card Services Module) is a factory or field installable module of the A98 family of products available only on an A98-A, A98-R or an A98-A/R. The A98-C is a self-contained application with no external dependencies on any other cryptographic unit and provides support for basic Payment Card functions. The A98-C is designed for those Card Issuers that prepare their own Magnetic stripe cards and PINs. The current version of the A98-C connects directly to the serial port of a Datacard® Embosser Unit to create cards for "Instant Issue" or custom batch processing. Additionally, the A98-C attaches to a laser or similar printer to securely print PIN Mailers. Both the Embosser and the PIN Mailer Printer are driven directly from a serial port on the A98-C integrated cryptographic unit. The calculation of CVV1, CVV2, IBM3624 PIN, VISAPVV PIN and Offsets for bridging from one PAN to another for the same PIN are performed entirely within the Cryptographic Unit and transferred DIRECTLY to the Embosser or PIN Mailer Printer. Additionally, the PIN verification function (PINVER) of the A98-C is made available to A98 users. For example, the A98-C PIN verification function permits moving PIN verification from the ATM to the host without the need for additional Host Security Module(s).

Overview of Operation

A Customer Supplied Application (CSA) running on a host computer, utilizes an XML interface to access the desired functionality of the TCP/IP attached A98-C Module. The CSA establishes a client socket with the A98-C server and specifies certain parameters to the A98-C as defined for each of the supported functions. The A98-C parses the XML message, performs the desired functions and returns the appropriate output data along with a completion code indicating the success of the operation or the reason why the operation could not be completed. All cryptographic operations are executed within the internal cryptographic unit of the host A98. All keys are double length and are held only in encrypted form either under the Master Key of the A98 or under a key encrypting key (KEK) shared between the hosting A98 and a customer Host Security Module (HSM). The A98-C uses ANSI X.9 and major network PIN security approved procedures in establishing the A98-C Master File Key and subsequent communication keys.

The CSA provides the Embosser input in the form of a text string. The position of the CVV1, CVV2 and OFFSET (for PIN bridging) are indicated by TOKENS that are inserted by the CSA. The A98-C replaces each TOKEN with the appropriate quantity and sends the completed Emboss String to the Embosser. PIN Mailers are handled in the same manner with the CSA supplying TOKENIZED PIN Mailer strings.



developed by Trusted Security Solutions, Inc.

Installation Support - Introducing the A98-C into an Issuer's operation is greatly simplified by the use of specialized functions and applications that support the encryption of clear-text CVV and PINVER keys into the Internal A98-C Database. For organizations that support multiple FIs, individual FIs are referred to by a user defined label that is used to access all additional information about that particular FI. Once installed, all keys and decimalization tables are encrypted under the A98 Master Key and the normal A98 scheduled unattended backup procedure are used to meet Business Resumption requirements. Recognized industry experts provide answers and solutions to challenges presented by the using institutions.

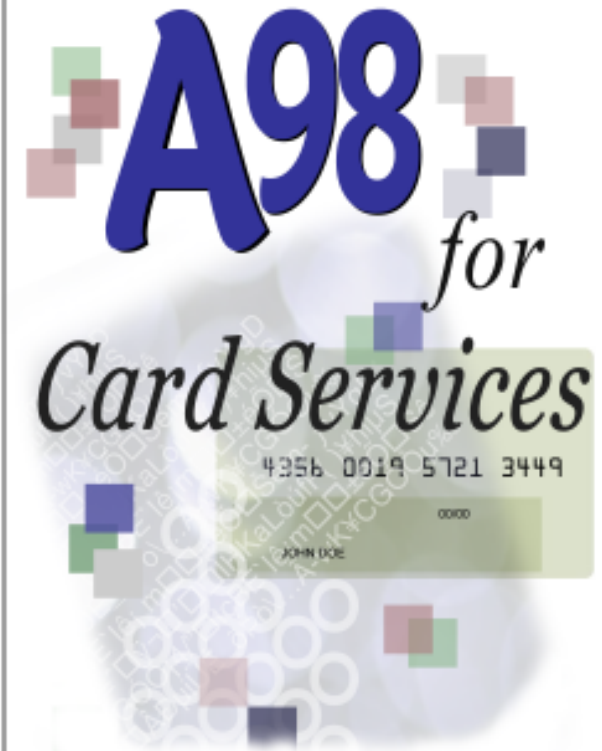
PIN Verification - The A98-C support of the verification of both IBM3624 and Visa PVV PINs is performed within the cryptographic unit. Host Software applications that have support for industry standard HSMs can interface directly to the A98-C without changes by using TSS provided interfaces that mimic the industry standard Host Security Modules.

A98 Key Security - The A98 system comes complete with the equipment and processes to compliantly create and manage necessary Master File Keys and other Key Encrypting Keys associated with the use of symmetric key exchange used in the A98-C. The issuer information can be manipulated from an authorized desktop user without having access to the actual key information.

Other A98 Capabilities - The A98 also performs as a complete ATM Key Management Solution for all ATMs using the patented Comvelope® process or Remote Key for remote key capable ATMs.



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



- Allows financial institutions and other card issuing organizations to take control of their card and PIN Mailer issuing functions.
- Provides a complete set of cryptographic tools and functions to create new or reissued cards for embossing and PIN Mailer production
- Allows card issuers to perform PIN bridging from one PAN to a new PAN without changing PIN value
- Delivers desired PAN, CVV, PIN, and offset values transparent to the embosser or PIN Mailer printer formats.

Trusted Security Solutions, Inc

A98-C Data Elements

- Original PAN
- New PAN
- VNAME (Includes issuer's keys, DecTabs, etc.)
- Expiry date
- Service date
- Emboss string (....token.....)
- PIN Mailer string (....token.....)
- more

Functions performed

- New card issuance
- Card reissue
- New card conversion (batch)
- PIN bridging (new PAN, same PIN)
- CVV1 and CVV2 calculation/output
- PIN offset
- IBM and PVV algorithms
- more



Card Embosser



PIN Mailer Printer

