

Using the Host Proxy Application

The A98 can be used to establish the initial key in ATMs and then communicate the newly established key to the host software to which that ATM is connected. The A98 sends the newly established ATM key as a cryptogram with the ATMA or ATMB key being encrypted by a Key Encrypting Key (KEK) that is shared between the A98 and the Host Security Module (HSM). The cryptograms are sent in ISO-8583 message format that are specified in the ISO-8583 Message Format Specification document. This same document also discusses the cryptographic connection to several types of Host Security Modules. Variant 1, Variant 5 or No Variant may be individually specified for the ATMA and ATMB keys. The A98 connects to the host system as a client using TCP/IP over either a Token Ring or Ethernet physical connection.

The TSS supplied Host Proxy Application (HPA) mimics a host connection for the A98. HPA is run on a customer supplied and network connected W9x or NT Workstation. The message from the A98 is received by the HPA and is parsed with the result being displayed on the screen and printed to an available printer. A human can transfer the cryptograms of the ATMA and ATMB keys under the shared KEK from the HPA screen to the same or a second workstation connected to the Current ATM Host Software system. The cryptograms are entered on the Host Software screen that is used to enter the cryptogram of a key encrypted by a KEK; change it to encryption under the Master File Key of the Host Security Module. The result is then stored in the Host Software Key Database and is ready for use by the System. This is the same function that is used to receive keys from a processor using dynamic key exchange.

Using this technique permits an A98 owner to use Comvelopes along with the A98 to establish unique keys in ATMs prior to having an automated software connection available. This strategy results in a smooth transition from a fully manual process to a semi-automated process to a fully automated process. It also avoids the need for doing any interim manual key generation or management while avoiding the need to retrain the field personnel from using the manual process to using the A98 once the software is available. Rather, the field personnel are trained once to use the Comvelopes and A98 to establish the ATM keys

An attractive variation to this approach is to use the MFK of the Host Security Module as the KEK loaded into the A98 and encrypted under the double length A98 MFK. With this approach, the newly established ATMA and ATMB keys are encrypted by the MFK of the Host Security Module and require no cryptographic processing. The cryptograms can be loaded directly into the Host Software key database. The A98 MFK is managed as three components and is at least as secure as the HSM MFK¹.

¹ Since the MFK is really a KEK, this technique is compliant with the applicable standards.