PCI requires the destruction of key components.

ARE YOU PCI v2 COMPLIANT?

Introducing the A98 Key Lock Box

TRUSTED SECURITY SOLUTIONS

www.trustedsecurity.com

The A98™ Key Lock Box (A98-KLB)

Eliminate stored paper components forever and become PCI v2 compliant.

Trusted Security Solutions, developer of the A98 ATM Initial Key Establishment System, is pleased to bring you an amazing new solution that **eliminates the need to store paper key components**:

The A98 Key-Lock-Box or A98-KLB

The A98 Key Lock Box is a simple solution for PCI compliance. With A98-KLB, you can destroy your paper components while using a compliant key decomposition and storage solution. If your institution manages cryptographic keys, you need the A98 Key Lock Box.

The A98-KLB server is a virtual lockbox.

Background: Paper components are widely used in the electronic payments industry to create and distribute cryptographic keys. After use, your paper component treatment must be formally documented, traced and stored in a permanent file in such a way to maintain "control-integrity" by your individual key custodians. Since most financial institutions and processors use many different keys, **the result is an increasing inventory of documents, logs and paper files, all of which are subject to audits**, both internal and external. And, with key components rarely used, they are easily lost, creating serious problems.

You'll Love A98-KLB's On-Demand Components

The A98-KLB eliminates the need for storing paper components. When a set of components is required for a given key, a cryptogram of the key serves as the input to the decomposition process. The A98-KLB produces 2 or 3 components sent to a printer using SSL/TLS. The printed form moves unobserved from the printer directly to the mechanically attached folder-sealer to produce tamper evident Comvelope™-like documents. Once opened by a custodian, the components **can be used and destroyed**. The A98-KLB provides components "on-demand," an industry first.

ARE YOU PCI v2 COMPLIANT?

PCI PIN Security Requirement v2 Control Objective 6, Requirement 24-2.3 states "Key components for keys other than the HSM MFK that have been successfully loaded and confirmed as operational must also be destroyed unless the HSM does not store the encrypted values on a DB but only stores the subordinate keys internal to the HSM."

The **A98 Key Lock Box System** uses the following steps to Decompose a Key:

STEP 1: You select a Key on the Host System for decomposition from the Key Database.

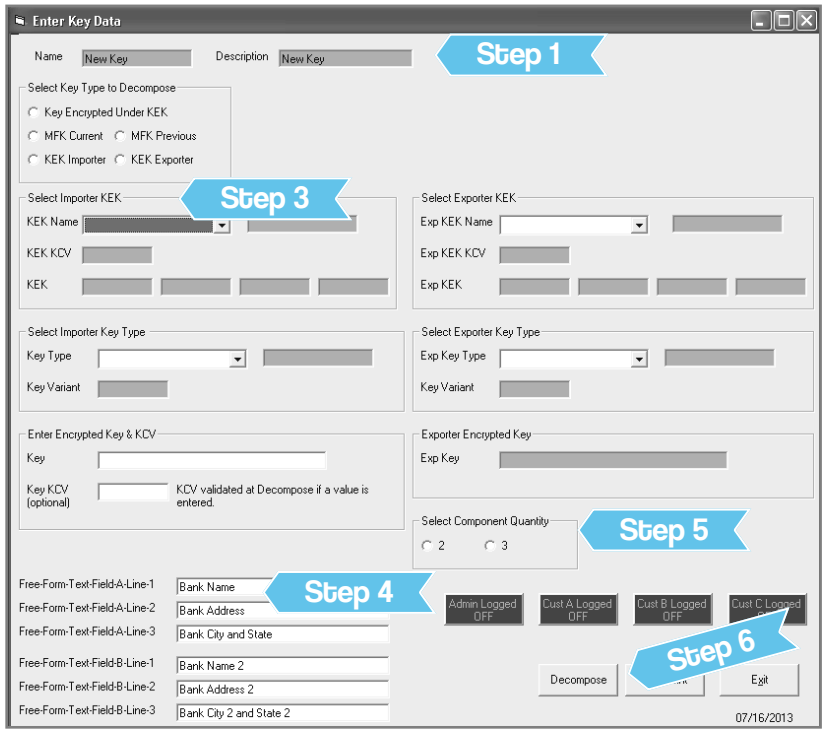
STEP 2: A cryptogram of the key is emitted from the Host, either electronically or on paper.

STEP 3: The KEK and Encrypted Key are selected. Entering the KCV for the Encrypted Key is optional.

STEP 4: Default, free-form text fields are verified or re-entered with correct information for the key rendering.

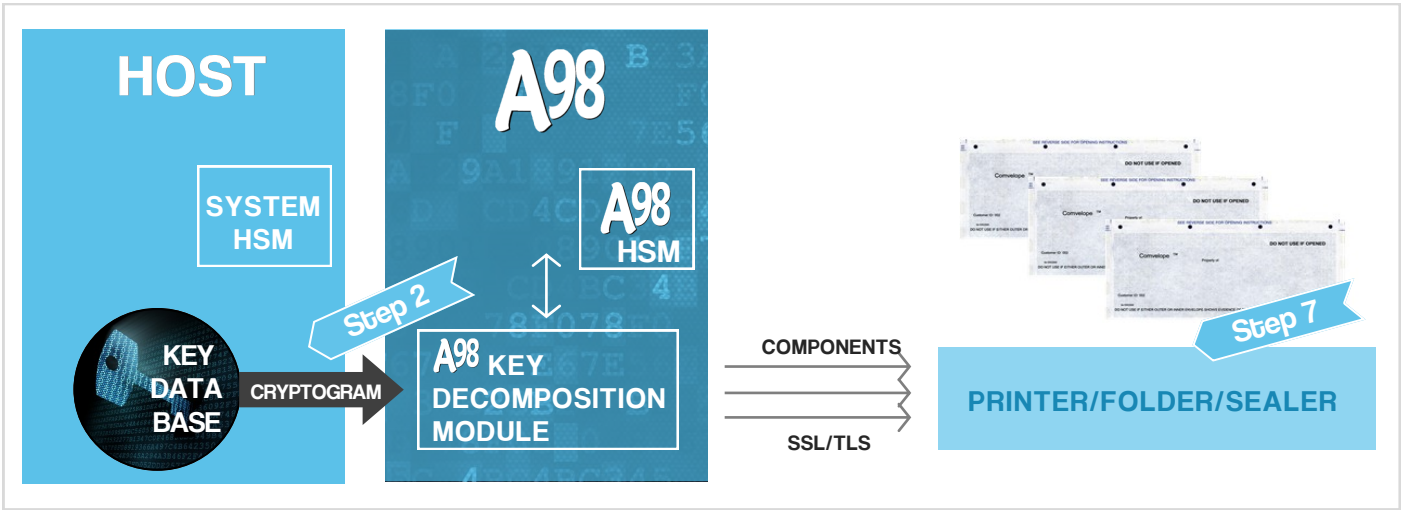
STEP 5: As the administrator, you can choose to decompose the key into either 2 or 3 components.

STEP 6: You select the Decompose button.



*Main **A98-KLB** Application Screen*

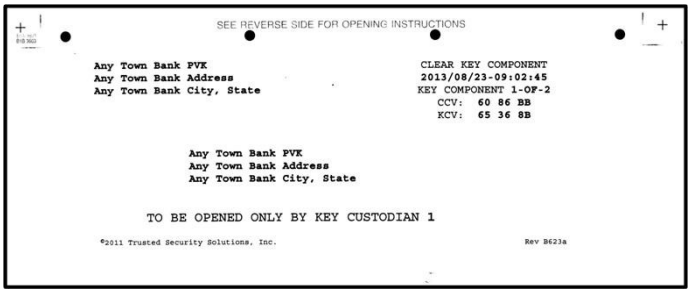
STEP 7: One at a time, each Component is sent to the printer using SSL or TLS where the information is printed, folded and sealed WITHOUT human intervention.



Now you have Components ready for use.

Exported Cryptograms

Keys can also be rendered in cryptogram form versus key components. The A98-KLB has the flexibility to "import" a key using an importer KEK and output the key in the form of a cryptogram using an exporter KEK.



*Sample Exterior View of **A98-KLB** Comvelope™*

Trusted Security Solutions Expands its Suite of A98 Key Management Systems

Trusted Security Solutions, Inc., your trusted key solutions provider for 20 years and developer of the industry leading A98 ATM Initial Key Establishment System, is pleased to add the A98 Key Lock Box module to its suite of A98 products:

A98 System Server and HSM Intel Xeon processor, two mirrored SSD drives (RAID 1), one SSD hot spare, and one additional SSD, hot spare, plus additional SSD, redundant power supplies, Windows Server 2012 OS, two network interfaces, connection to a FIPS 140-2 Level 3 cryptographic unit, in rack mountable enclosures.

A98 System Software - Custom application with cryptographic unit support, role based key management module, and complete administrative functions for managing keys used in A98-KLB processes.

A98™ Key Lock Box (A98-KLB)

Software - The A98-KLB Module, an extension to the A98 family of key management solutions supports 2048-bit RSA encryption, PKCS certificates, digital signatures, and key bundling for storage and transport.

Types of Keys - CVV, CVC, PIN Validation, Zone Keys, Key Encrypting Keys, and other important DES keys.

Interface - The A98-KLB shares a double length Key Encrypting Key (KEK) with applicable Hosts used to compliantly transport clear text keys in cryptogram form for decomposition. A98-KLB can have any number of KEKs and they can be easily changed and updated.

The A98 System, including the A98 Key Lock Box, provides a compliant solution to your key component management. For more information, please contact us.

For more information, call: **704.849.0036**

TRUSTED SECURITY SOLUTIONS
www.trustedsecurity.com

Trusted Security Solutions, Inc.
3838 Highway 49 South
Harrisburg, NC 28075