Remote Key Transport

White Paper

DIEBOLD
Remote Key Transport White Paper

Introduction

PIN encryption requirements for Automated Teller Machines (ATMs) are changing. Financial Institutions (FIs) have been using single-DES encryption for PIN entry security in ATMs for over twenty (20) years. However, the convergence of several factors has heightened the urgency for FIs to migrate the ATM infrastructure to a more secure triple-DES PIN encryption environment. First, a recent competitive challenge in a controlled environment showed that single-DES encryption could be successfully exhausted in less than 24 hours thus revealing the encrypted information. Second, the cost of the CPU processing power necessary to exhaust single-DES has decreased significantly creating an attractive return on investment for the hacker community. Lastly, the number of individuals in the global population who understand PIN encryption mechanics has grown significantly thereby increasing the number of individuals capable of successfully exhausting an encrypted PIN. Financial Institution Risk Management Groups are cognizant of the increased risk factor and support migration to a triple-DES PIN encryption algorithm for their ATMs. Visa and Master Card are leading the triple-DES migration effort within the FIs. The ATM and Host software must support the triple-DES PIN encryption message structure. The ANSI X9 and ISO Standards identify double-length key triple-DES encryption in a tamper-resistant security module (TSRM) for PIN encryption security.

The migration to triple-DES PIN encryption is underway. VISA, and Master Card, along with many other international networks and regulatory bodies have set time frames for the migration. Both the ANSI X9 and the ISO standards define that double-length key triple-DES encryption in a tamper resistant security module (TRSM) must be used for PIN encryption on an ATM. The length of the DES key is changing along with the cryptographic procedure utilized for encrypting. Diebold is delivering our double-length key triple-DES encryption solution in an Encrypting PIN Pad (EPP). We offer the EPP4 (with Remote Key Transport) to support triple DES for our ATMs. The terminal control software on the Diebold ATM may need to be upgraded to support the new EPP. In consideration of our customer's migration strategies, the new EPP will support both single-DES and triple-DES encryption. This feature enables our customers the flexibility and freedom to purchase our new EPP and operate it in single-DES mode until their HOST software vendor can support triple-DES encryption. At such a time, when the HOST can support triple DES encryption, Diebold’s Remote Key Transport (RKT) provides a safe and cost-effective method of delivering new DES keys. New versions of HOST system software are becoming available which support triple-DES PIN encryption and Remote Key Transport. FIs should check with their HOST software provider for the time frame for supporting this functionality.

CONTENTS

In the past, a two-person team practicing split knowledge, and dual control was the means for inserting the DES keys into the ATM. Each person keyed into

DIEBOLD®
We won’t rest.

the ATM his or her portion of the initial "B" key (dual control). Once installed, the key parts underwent a mathematical procedure that resulted in a sixteen (16) character key unknown to either person (split knowledge). Today, just as it was in the past, FIs are responsible for secure key management, inserting a unique initial "B" key, and periodically updating the DES keys. Clearly, the cost of dispatching two-person teams to each ATM can become prohibitive with a network of substantial size. In an effort to reduce key maintenance cost per ATM, some of our customers have requested the ability to load the DES keys on-line to the ATM in a secure fashion from the ATM host software. This eliminates the need for two-person teams visiting the ATMs for key loading. The secure on-line remote key transport feature dramatically enhances the efficiency, certainty, and security of DES key management. In response to our customers' requests, Diebold has worked with the industry to develop the Remote Key Transport (RKT) specification. Diebold is offering the EPP4 with Remote Key Transport (RKT) for our double-length-key, triple-DES PIN encryption solution that incorporates the ability to securely load the initial Master Terminal Key on-line to the ATM from the host software.

RKT requires a secure session be established between the ATM and the HOST system environment. Individual authentication is required from both the ATM and the Host. Authentication is achieved using digital certificates. Both the ATM and the Host are required to have digital certificates. These certificates are exchanged with the other party in a point to point communication, allowing each party to authenticate the other through Public Key Infrastructure (PKI) creating a secure session. Authentication minimizes the risk of exchanging keys with an unauthorized device. In conjunction with Host software supporting remote key loading capability, an on-line key management system is required to enable a secure remote installation of DES keys from a centralized key management system. The centralized key management system resides in the Host system environment. Computerized key management, if properly implemented, enables a more secure and efficient manner with which to manage DES keys and execute automatic frequent updates of DES keys. The FI benefits from enhanced DES key control and security using an on-line key management system. DES key control and security are two primary factors VISA's audits stress must be improved at most FIs.

Security

In the interest of increasing the security of DES keys, Diebold's RKT includes certain distinctive safeguards. Among these are random numbers, identifiers, and digital certificates.

Random numbers are used within a remote key transport session so that a recorded DES key exchange cannot be later replayed. Each time a DES key exchange takes place using RKT, a new random number is sent from the ATM to the HOST. The HOST must then include this same random number in the messages it sends back to the ATM.

As messages are sent between the HOST and ATM, identifiers provide further reassurance that only the intended parties are involved in the communication. Identifiers can be set to distinguish a specific ATM on a network. The ATM will verify that the identifier agrees with what was sent in previous messages in the protocol.

The Remote Key Transport protocol also requires that each entity have access to an authenticated copy of the public verification key and public encipherment key of the other entity. Exchanging public key certificates and requiring that all entities possess an authenticated copy of the Certificate Authority's public verification key fulfills this requirement.

A common Certificate Authority (CA) for both the ATM and HOST has been established in order to eliminate having to authenticate a chain of certificates. Our fourth generation Encrypting PIN Pad manufacturer will inject certificates issued by the Certificate Authority (CA) into the EPP4s on each ATM. Separate RSA key-pairs will be used for signature/verification and encipherment/decipherment. The Certificate Authority will also issue certificates to the HOSTs. Digital Signatures Trust (DST) has been chosen as the Certificate Authority. DST is a leader in guaranteeing the identity of entities involved in digital transactions.

The digital certificates can be used to guarantee the identity of ATM independent of sending DES keys. Authentication of the ATM promotes a secure network in general.

The ATM certificate follows the X.509 standard format to certify its public key. This can be read at the host according to the standard described. Therefore, once this certificate is received by the HOST and examined, the identity of the ATM has been confirmed. This verification of the ATM establishes a secure connection from the ATM to the HOST whether or not the DES keys are to be downloaded.

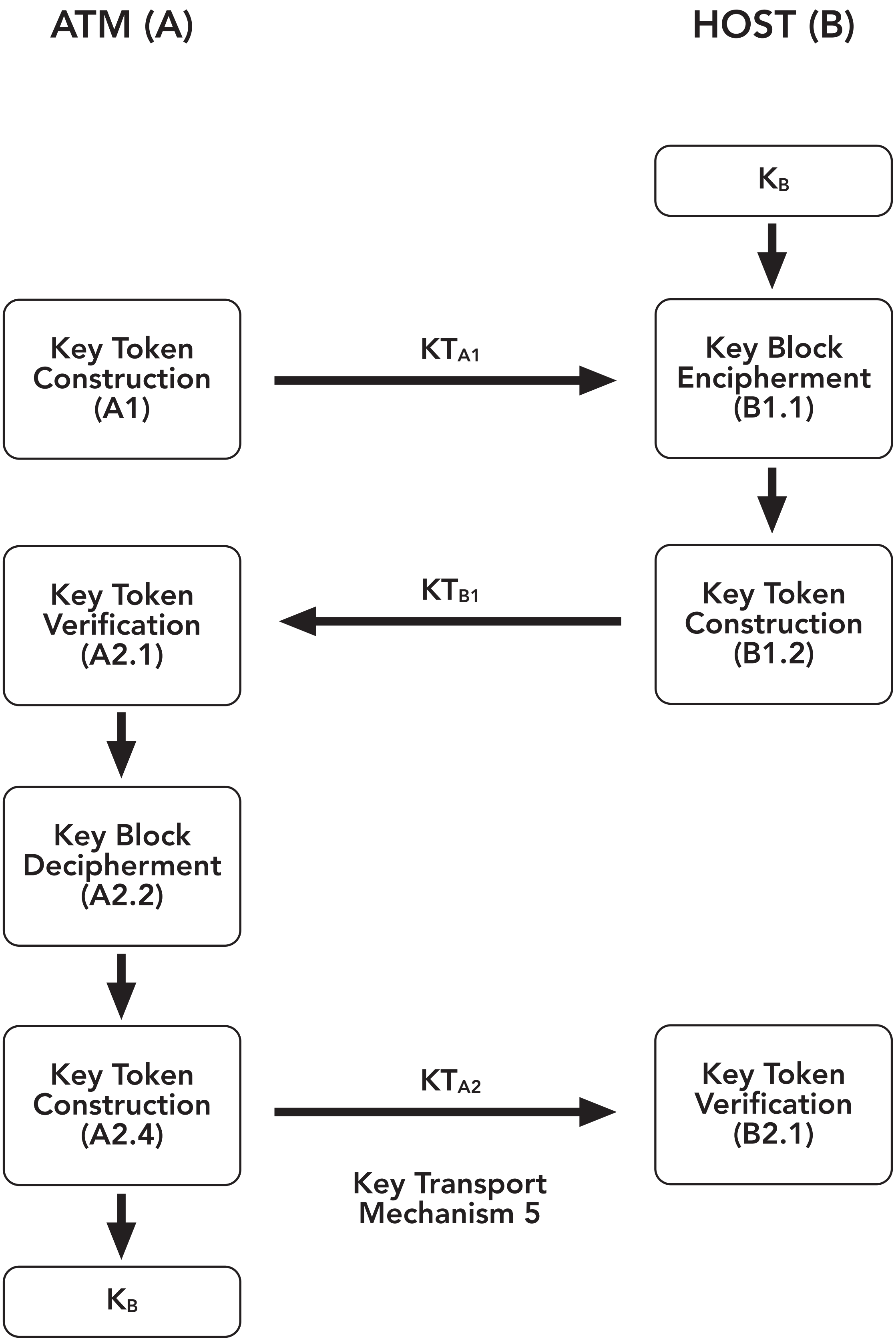
A disaster recovery scheme will be implemented in the unlikely event that the Certificate Authority's private key is ever compromised. This disaster recovery scheme requires that the Certificate Authority have two key pairs, a primary key-pair and a secondary key-pair. When a certificate is requested, the CA generates a primary certificate signed by the CA's primary private key, and a secondary certificate signed by the CA's secondary private key. Before disaster recovery, the primary certificate is exchanged and the primary private key is used for validation. Disaster recovery consists of revoking all certificates signed with the primary public key and notifying users to switch to their secondary certificates.

Remote Key Transport Messages

The Remote Key Transport messages are based on Key transport mechanism 5 of ISO/IEC 11770-3. The general key transport mechanism transfers two shared secret keys in three passes and provides mutual entity authentication and key confirmation. One key is transferred from A to B and one key from B to A. The proposed adaptation for the HOST to ATM application will provide unilateral key transport from HOST to ATM, thus eliminating one of the key block encipherment fields.

The asymmetric encipherment system (EX , DX) will use RSA, specifically RSAES-OAEP. The asymmetric signature system (SX , VX) will use RSA with a SHA-1 hash function. The size of the RSA modulus will be 2048 bits. Since only unilateral key transport from the HOST to the ATM is required, the field BE2 is omitted. Certificates will be exchanged prior to the protocol.

Key Transport Mechanism 5 of ISO/IEC 11770-3


ATM (A)
HOST (B)
K_B
Key Token Construction (A1)
KT_{A1}
Key Block Encipherment (B1.1)
Key Token Verification (A2.1)
KT_{B1}
Key Token Construction (B1.2)
Key Block Decipherment (A2.2)
Key Token Construction (A2.4)
KT_{A2}
Key Token Verification (B2.1)
Key Transport Mechanism 5
K_B

Key Transport Mechanism 5 of ISO/IEC 11770-3

Key Token Construction (A1) ATM randomly generates r_{ATM} and constructs the key token

$KTA1 = rATM$

and sends it to *HOST.*

Key Block Encipherment (B1.1) *HOST* has obtained a key K_{KTK} and wants to transfer it securely to the *ATM. HOST* constructs a block containing its own distinguishing identifier I_{HOST} and the key K_{KTK}, and enciphers the block, using the recipient's public encipherment transformation E_{ATM}

$BE1 = E_{ATM} (I_{HOST} || K_{KTK})$

Key Token Construction (B1.2) Then *HOST* randomly generates r_{HOST} and constructs a data block, containing r_{HOST}, r_{ATM}, the recipient's identity I_{ATM}, and the enciphered key block BE_1. *HOST* signs the block using its private signature transformation S_{HOST}, and sends the key token

$KT_{B1} = S_{HOST} (r_{HOST} || r_{ATM} || I_{ATM} || BE_1)$

to *ATM.*

Key Token Verification (A2.1) *ATM* verifies *HOST*'s signature on the key token KT_{B1} using *HOST*'s public verification transformation V_{HOST}, checks the distinguishing identifier I_{ATM} and checks that the received value r_{ATM} agrees with the random number sent in step (A1).

Key Block Decipherment (A2.2) *ATM* deciphers the enciphered block BE_1 using its private decipherment transformation D_{ATM} and checks the distinguishing identifier I_{HOST}. If all checks are successful, *ATM* accepts the key K_{KTK} and stores it.

Key Token Construction (A2.4) Then *ATM* constructs a data block, containing the random number r_{ATM}, the random number r_{HOST}, and the recipient's distinguishing identifier I_{HOST}. *ATM* signs the data block using its private signature transformation S_{ATM}, and sends the key token

$KT_{A2} = S_{ATM} (r_{HOST} || r_{ATM} || I_{HOST})$

to *HOST.*

Key Token Verification (B2.1) *HOST* verifies *ATM*'s signature on the key token KT_{A2}, using *ATM*'s public verification transformation V_{ATM}, checks the distinguishing identifier I_{HOST}, and checks that the received value r_{HOST} agrees with the random number sent in step (B1.2). In addition, *HOST* checks that the received value r_{ATM} agrees with the one contained in KT_{A1}.

To learn more about Diebold's Remote Key Transport, contact your Diebold sales representative.

Authored by:
Ernest Chapman
Product Manager
Global Product Management

Diebold, Incorporated
Post Office Box 3077
Dept. 9-B-16
North Canton, Ohio
44720-8077

DIEBOLD®
We won't rest.