DUKPT: Breaking Down the Process

DUKPT.12/12/17.09:41

TABLE OF CONTENTS

TABLE OF CONTENTS 1
DUKPT: BREAKING DOWN THE PROCESS 2
HOW IT WORKS 3
- CONFIGURATION 3
- REPEATED PROCESS 3

SOURCE 3

DUKPT: BREAKING DOWN THE PROCESS

Derived Unique Key Per Transaction is a type of encryption key management used for PIN encryption and safeguarding cardholder data. This document provides a high-level overview of the DUKPT process, outlining how derived keys are made and what they are used for. For more detailed information, consult the American National Standards Institute's ANS X9.24-1:2009 publication.

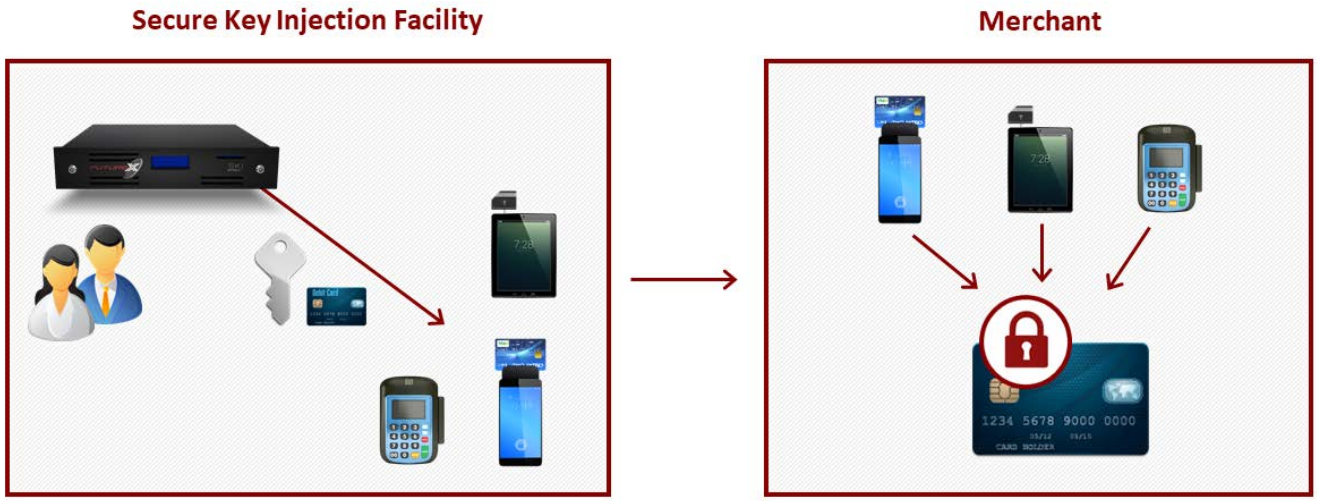
When customers use a Point of Sale terminal to make purchases, they expect their information to be kept secure. With countless electronic payment transactions occurring every day, merchants need ways to ensure that sensitive data stays safe from malicious individuals. To do so, they use key management technologies such as Derived Unique Key Per Transaction (DUKPT).

DUKPT is a key generation method defined by the American National Standards Institute, a regulatory standard responsible for specifying the requirements for key management and the secure processing of cardholder data throughout payment transactions.

DUKPT safeguards data, such as Personal Identification Numbers (PIN) or cardholder Primary Account Numbers (PAN), by providing unique encryption keys for every transaction. Each key cannot lead back to the original key upon which it was based. Furthermore, each transaction key is erased after use.

According to TR-39 objectives, which are maintained by ANSI's X9 committee, organizations are required to have a unique key for every device. While several methods of key management allow for unique keys per transaction, DUKPT saves organizations time and money while increasing security by significantly reducing the amount of effort required for key management. Instead of storing a unique key for every single device, organizations can compliantly store one base derivation key for use with hundreds of thousands of devices.

Key loading devices are used by merchants and POS manufacturers to inject DUKPT keys. Performing key injection using a hardware security module (HSM) ensures that knowledge of the BDK is kept to an absolute minimum. The HSM's physical and logical security keep the key secure during both storage and transit. Key injection must be done under dual control to enhance security, but can be performed either locally in a physically secure environment or remotely utilizing a Public Key Infrastructure.



HOW IT WORKS

The process of deriving keys is two-fold; each device goes through initial configuration and then the repeated act of creating keys. The following process uses PIN encryption as an example, although DUKPT has many other uses.

CONFIGURATION

There are two main components in creating a DUKPT transaction environment: a Base Derivation Key (BDK) and a unique Key Serial Number (KSN). The hardware security module responsible for injecting keys contains a counter that increments whenever a new device is added into the network. This counter is encrypted using the BDK, which results in the DUKPT initial key that is injected into the device. This initial key is used later to create a pool of transaction keys, each with a modifier for different key usages. The counter is also used to form the device's KSN. All transactions using DUKPT will include the KSN.

Key Serial Numbers play an integral role in the DUKPT process by enabling the HSM to identify which initial key was used to encrypt the data. As specified by ANS X9.24-1, DUKPT uses a 10-byte KSN, most often represented as a sequence of 20 hexadecimal characters in which each byte of the KSN is represented by a pair of hexadecimal characters.

The general format of the KSN is as follows:

Right-most 21 bits: Transaction counter for each successively derived key.

Following 43 bits: Unique data for each HSM using the same derivation key.

Left-most 16 bits: Data for initial key derivation.

REPEATED PROCESS

When a PIN is entered into the POS terminal, it is formatted into a PIN block. This PIN block is then encrypted using Triple DES using the current transaction key, which is chosen from the pool of keys created by the initial key. Along with information such as the KSN, the PIN block is sent to the host application, where the information is used to verify the identity of the originating device. Once in the hands of the host application, the PIN block can be translated using a different key management scheme.

After the PIN block is sent to the host application, the KSN is incremented by a user-defined amount, usually 1, and then used with the current transaction key to create more future keys. Once the future keys have been generated, the current transaction key is erased from the system, removing any information about a previous transaction from the device. Afterward, the device will be ready to pull a future key for the next transaction.

By using the current encryption key to form the key to be used in the next transaction, DUKPT forms a self-recycling system that promotes security, efficiency, and ease of implementation.

SOURCE

1. "ANS X9.24-1:2009." American National Standards Institute. October 2009.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163