WHITE PAPER

DUKPT *(Derived Unique Key Per Transmission)* vs. MTE® and MKE

Document ID: ECLYPSES-1532395320-269
Version: 3.0

www.eclypses.com

What is DUKPT?

DUKPT stands for "Derived Unique Key Per Transmission" and is a method for managing encryption keys between two parties. DUKPT offers a way of generating one-time-use encryption keys unique to every transmission within a communication stream. This method for generating single-use encryption keys is widely used in the financial industry on POS devices and will be used as an example to walk through the DUKPT process.

The POS and Service Provider must first establish a relationship based on an initial key and unique "Key Serial Number" (KSN). The service provider generates the initial key based on a Base Derivation Key (BDK) and a unique device identifier. The BDK can be the same for many devices, but the identifier is unique and is typically the POS device serial number. The KSN is based on the initial device identifier and an internal transaction counter.

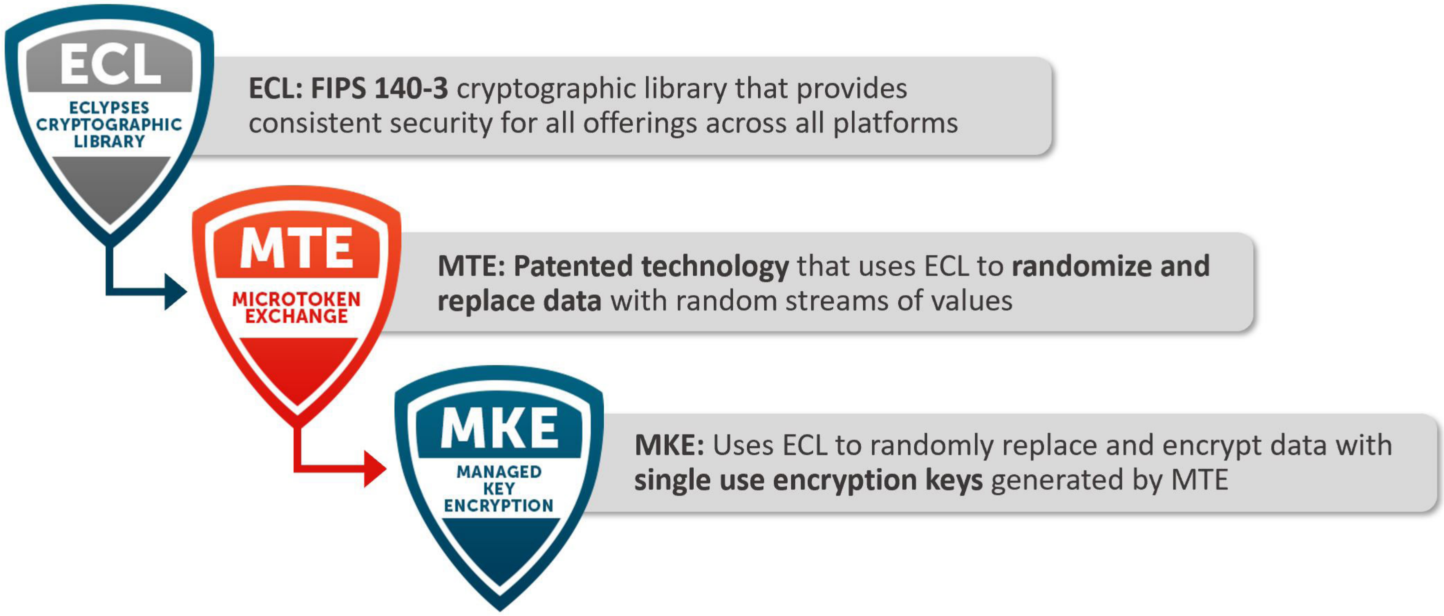
The initial key and the KSN created by the service provider get injected into the POS device upon manufacturing or installation. Once a POS is installed, it uses its initial key to generate a set of derived future keys and then erases the initial key so it cannot be discovered.

A "future key" is used to encrypt each transaction, and the correlating KSN is sent with the encrypted data. The KSN is sent with the encrypted data so that the service provider can correlate the transmission to the appropriate BDK and then use the counter information to generate the correct decryption key. The keys are never to be used again, and at some point, one of the transaction keys, or it could be the initial key if that is stored or a separately created session key, is used along with the current KSN to make the next pool of "future keys." This process keeps repeating for the life cycle of the device.

How MTE is Different

While DUKPT relates more to MKE in functionality it is still very important to understand how it is different than from the MTE technology. The primary difference between DUKPT and MTE is that DUKPT is a way of managing encryption keys while MTE is a security methodology that does not involve encryption at all. DUKPT does not actually secure data and instead is a way of generating unique encryption keys for individual transmissions that need to be provided to an encryption module.

On the other hand, MTE is a complete security offering that secures individual pieces of data at the application layer by doing random substitutions of every byte. DUKPT and MTE are similar in the fact that they allow for the unique securing of individual transmissions but achieve this in very different ways. By eliminating the use of encryption for securing data, MTE is impervious to common attacks and resistant to the methodologies of quantum computing, greatly improving any environment's security posture against the future.



ECL: FIPS 140-3 cryptographic library that provides consistent security for all offerings across all platforms

MTE: Patented technology that uses ECL to **randomize and replace data** with random streams of values

MKE: Uses ECL to randomly replace and encrypt data with **single use encryption keys** generated by MTE

How MKE is Different

MKE and DUKPT are both ways of handling key management for encryption, and both do so at the transmission level. Encrypting at the transmission level is far superior to session-based securities, and while they share a similar base functionality, there are a few significant differences. One fundamental difference between the two is the DUKPT is only a key management offering, while MKE also handles the encryption of the data. Since DUKPT does not orchestrate encryption, implementing a complete solution is much more complicated and opens the possibility of incorrect implementation. MKE generates random encryption keys for every transmission and encrypts the transmission, offering a comprehensive solution that is much easier to implement. Furthermore, DUKPT generates encryption keys for the application layer like MKE, but the keys DUKPT generates are related and produced in batches of 21. While DUKPT claims that a key cannot be used to discover other keys, this might change as quantum computing becomes more relevant.

Conversely, MKE generates keys by pulling them out of a Deterministic Random Bit Generator (DRBG) stream. While that may seem to make them related, that stream is also used for other process elements, making the data used for encryption keys disjointed from each other. DUKPT's method of generating keys in batches means those keys need to be stored somewhere, which is a security risk. MKE generates keys in real-time when needed and immediately throws them away once used, significantly reducing the risk of key exposure.

Lastly, DUKPT sends a KSN along with the encrypted data so the receiving side can recreate the initial key and arrive at the correct decryption key. This means that the KSN is connected to the initial key that starts the whole process. While right now, that correlation is too hard to figure out, the methods of quantum mathematics will have a much easier time. MKE never sends any key-related information and instead can generate the appropriate key in real time on both sides even if transmissions are dropped or arrive out of order. So, while DUKPT and MKE are solving similar problems, MKE is superior and far more resistant to future cyber-attacks.

For more information please visit our website www.eclypses.com or email our team at contact@eclypses.com.

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies and websites. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

With a focus in the mobile sector, this technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT US

contact@eclypses.com
www.eclypses.com
(719) 323-6680