



Futurex Support of Proprietary Master Key (MFK/LMK) Usage Methods

The definition for the Triple DES algorithm used by the International Standards Organization (ISO) is taken directly from the National Institute for Standards and Technology (NIST) Special Publication 800-67, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher". The same definitions for the American National Standards Institute (ANSI) X9 committee are outlined in the publication "ANS X9.52-1998 Triple DES Encryption for the Financial Industry."

The Triple DES standard as specified by the NIST publication is "the only FIPS approved DES algorithm" and, in addition to being the accepted standard within the payment processing industry, is the method used by Futurex devices. Futurex policy regards security and regulatory compliance as the top priority. This differs from organizations that design Host Security Modules (HSMs) with the intent of locking customers in to one solution set by using any or all of the following methods:

- *Implementing methods of Master Key storage such as through restriction of Master Key storage to non-interoperable smart cards*
- *Intentionally using a non-peer reviewed proprietary manipulation of a secret value to derive a Master Key that is unknown to the customer*

While Futurex strives to emulate command sets found across different HSM platforms in order to give customers greater control over their payment processing infrastructure, it is our policy to not deviate from any established standards that are required in order to maintain regulatory compliance and/or device security.

We believe that the use of proprietary methods of Master Key generation, storage, loading, and calculation result in the following negative consequences for the customer:

- *Significant costs arise and an entire infrastructure must be replaced if an organization wishes to incorporate HSMs manufactured by an alternate vendor*
- *The HSM vendor gains control of the most important key in an organization's payment processing infrastructure, allowing them to dictate the terms and conditions of use to the customer*
- *Implementing an enterprise payment solution across a vendor-neutral platform becomes impossible*

We have total confidence in the quality, performance, and security of our devices. Because of that confidence, we have followed industry standards for the full spectrum of our device capabilities. We understand that maintaining strict compliance with these standards will allow our customers to retain control of their master keys and move to a different HSM provider if Futurex does not deliver innovative solutions with quality support. We trust that the security, speed, and flexibility of our devices alongside the proactive dedication of our Xceptional Support Team will remain strong incentives for our customers to continue using and recommending our devices to protect their most sensitive data.

Americas

Global Headquarters

Futurex Technology Campus
864 Old Boerne Rd.
Bulverde, TX 78163 USA
Tel: 1-800-251-5112
info@futurex.com

Europe

2430 / 2440 The Quadrant
Aztec West
Almondsbury
Bristol, BS32 4AQ UK
Tel: +44 (0) 1454 877681
info.intl@futurex.com

Asia

One Fullerton
1 Fullerton Road
#02-01 One Fullerton
Singapore 049213
Tel: 65 6832 5176
info.asia@futurex.com

FUTUREX.COM