Compliance Attestation – Securus Key Loading Device

To whom it may concern:

This letter is in response to your request that Futurex provide attestation that the Securus, which contains the EXP9000 cryptographic module, has been validated as a FIPS 140-2 Level 3 Tamper Resistant Security Module (TRSM) and complies with the TR-39 standard for key loading devices.

Futurex TRSMs are designed and constructed to adhere to the specifications described in the American National Standard for Financial Services document ASC X9.24, Part 1 and Part 2. Provided are sections from X9's TR-39-2009 TG-3 Standards Guidelines and *italicized red* is the Futurex method for adherence to these specifications.

The EXP9000 Cryptographic Module contained within the Securus is a FIPS 140-2 Level 3 TRSM, validation number 1577. Futurex solutions have been deployed for many years in thousands of customer sites around the world. They have been subjected to independent audits at many of these sites and have never been judged to be lacking the characteristics and qualities required of a TRSM or a standards-compliant device.

Futurex devices are designed to meet the strict data security requirements necessary for the processing of sensitive data. Our constant monitoring of regulatory standards and involvement with their governing organizations ensures that our devices remain at the forefront of the rapidly changing technological landscape.

Futurex Management Team

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

Securus - Key Loading Device

4.1.1 Secure Environment for PINs and Keys

The secure environment is physically, logically, and procedurally protected with access controls or other mechanisms designed to prevent any penetration, which would result in the disclosure of all or part of any cryptographic key and / or PINs stored within the environment. Documented procedures exist and are followed that ensure the secured environment remains secure until all keying material has been removed or destroyed.

Reference X9.8-1 - Sec. 6.3.3; X9.24-1- Sec. 7.3 and 7.5.2; X9.24-2 – Sec 7.3

The Securus contains a secure boundary that has been validated to FIPS 140-2 Level 3 standards to store and encrypt keys. Additionally, the Securus is tamper-responsive and any attempt to penetrate the outer case will also result in zeroization.

4.2.2 TRSM Evaluation Criteria

Documented procedures exist and are followed that ensure each type of TRSM (e.g., ATMs, POS devices, host security modules and key loading devices) has been evaluated using the criteria in Reference and found to meet the applicable requirements.

Reference X9.8-1 - Sec. 6.3; X9.24-1- Sec. 7.2; X9.24-2- Sec**.** 6.5

The TRSM used with the Securus has been validated as compliant with FIPS 140-2 Level 3 standards. In addition, many different tamper detection techniques have been implemented.

4.2.4 Prevention of TRSM Misuse

Documented procedures exist and are followed that ensure any TRSM (e.g., HSM, KLD) capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of both the following:

- Dual control is required to load / inject clear keys and / or enter key components into this TRSM; and
- When not in use, the TRSM (e.g. HSM, KLD) is maintained in an environment that minimizes the possibility of unauthorized modifications, e.g. the insertion of active or passive tapping devices.

Reference X9.8-1- Sec. 6.3; X9.24-1– Sec. 7.2, Sec. 7.3, and Sec. 7.5

The Securus requires any type of configuration, both local and remote, to be performed under dual control.

4.3.2 Key Generation

Documented procedures exist and are followed that ensure keys and key components are generated using a random or pseudo-random process such that it is not possible to determine that some keys are more probable than other keys from the set of all possible keys. A variant of a key is only to be used for key separation, and not key generation.

Reference X9.24-1- Sec. 7.1, and Sec. 7.4; X9.24-2 – Sec 7.1.1, Sec 7.5.1

The PRNG used in the Securus has been validated as compliant with FIPS 140-2 Level 3 standards.

4.3.4 Combining Key Components Using XOR

Key components are combined to form a key by a process such that no active bit of the key could be determined without knowledge of all components. The resultant cryptographic key can only exist within the TRSM by automatically combining all entered key components using XOR.

Reference X9.24-1- Sec. 7.5.1; X9.24-2 – Sec 7.5.1

Key components can only be combined using the XOR function within the secure boundaries of the TRSM in the Securus.

4.3.7 Key Transportation Using a Key Loading Device

If keys are brought from the location of generation to the location of loading in an electronic key loading device, then documented procedures exist and are followed that ensure:

- The key loading device is or contains a physically secure TRSM;
- The key loading device is designed or controlled so that only authorized personnel can operate it; and
- The key loading device is operated under dual control while transferring cleartext keying material.

Reference X9.24-1- Sec. 7.1 and Sec. 7.5

The Securus contains a physically secure TRSM that has been validated as compliant with FIPS 140-2 Level 3 standards.

5.2.12 Strength of Symmetric Key Used to Encrypt Stored Private Keys

Documented procedures exist and are followed that ensure master keys used to encrypt asymmetric private keys for storage are at least double length keys used with TDEA algorithm and are of equal or greater strength than the asymmetric key.

Reference X9.24 - 2 – Sec. 7.5.1

In order to encrypt an asymmetric key under a symmetric key on the Securus, the symmetric key must be of equal or greater strength.