STANDARDS - FIPS 140

D17

galaxkey®
www.galaxkey.com

PROTECT YOUR COMPANY'S DATA - WHEREVER IT GOES

- Secure **Emails**
- Secure **Files**
- Secure **Signatures**
- Secure **Workspace**
- Secure **Messaging**

What is FIPS?

Federal Information Processing Standards (FIPS) are a set of standardisation developed by the US federal government for use in computer systems by all non-military government agencies and government contractors. FIPS includes numerous standards that are defined by US government such as Personal Identity Verification (201) and Minimum Security Requirement for Federal Information (200). The standard of interest in the context of Galaxkey is FIPS 140.

QUICK FACTS

- **Galaxkey:** FIPS publication 140-2 compiant.
- **AES:** Key size 256 bits. Mode GCM. FIPS publication 197.
- **RSA:** Key size 2048 bits. FIPS publication 186-2
- **SHA:** 512 bits. FIPS publication 180-3
- **TLS** version 1.2

FIPS 140

FIPS 140 is a US Government standard that defines a minimum set of the security requirements for products that implement cryptography.

This standard is designed for cryptographic modules that are used to secure sensitive but unclassified information. The current standard defines four-levels of increasing security, 1 through 4.

FIPS 140-1 is the original working version of the standard made official on January 11, 1994.

FIPS 140-2 is currently the active version of the standard. The security requirements of FIPS 140 cover areas related to the secure design and implementation of a cryptographic module.

These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

FIPS STANDARDS IN GALAXKEY

D17

ADVANCE ENCRYPTION STANDARD (AES)

- AES used in Galaxkey for symmetric encryption is fully FIPS compliant under publication FIPS 197 (Certificate number: 1168). Galaxkey uses 256 as its key size for encryption in GCM mode.

RSA

- RSA algorithm libraries used in Galaxkey for asymmetric encryption is fully FIPS compliant under publication FIPS 186-2 (certificate number 560). Galaxkey uses 2048 as its key size for RSA.

SECURE HASH ALGORITHM (SHA)

- SHA algorithm used in Galaxkey is FIPS compliant under publication FIPS 180-3 (certificate number 1081). Galaxkey SHA 512 is for hashing.

TRANSPORT LAYER SECURITY (TLS1.2)

- All communication between Galaxkey clients and server are secured using TLS1.2 (the latest protocol for secure communication communication).

SIMPLE OBJECT ACCESS PROTOCOL (SOAP)

- Galaxkey uses SOAP for its communication with server. SOAP is a widely accepted standard for communication with a webservice. SOAP communication over SSL3 makes communication very secure.

CHECKING FOR COMPLIANCE

While there are alternative methods for setting the FIPS local policy flag, the following method is included as a guide to users with Administrative access:

- STEP 1
  Open the 'Run' menu: either click Start > Run or press the combination 'Windows Key +R. On Windows Vista and later systems, using the Start Menu, you can use the search box at the bottom of the menu.
- STEP 2
  Type 'secpol.msc' and press 'Enter' or click the 'Ok' button.
- STEP 3
  In the Local Security Policy management console window that opens, use the left tab to navigate to Local Policies > Security Options.
- STEP 4
  Scroll down the right pane and double-click 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing'.
- STEP 5
  In the properties window, select the 'Enabled' option and click the 'Apply' button.
- STEP 6
  Close the properties window by clicking 'Ok' and close the Local Security Policy management console window by clicking the 'X' in the upper right corner, by going to the menu File -> Exit or by pressing 'Alt + F4'.