Go-Cort, Inc. Acceptable Encryption Policy

Last Update Status: Updated January 2021

1. Overview

See Purpose.

2. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

3. Scope

This policy applies to all Go-Cort, Inc. (DBA Apptoto) employees and affiliates.

4. Policy

4.1. Algorithm Requirements

4.1.1. Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

4.1.2. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to the date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) aSignature Algorithms

4.1.3. Algorithms are strongly recommended for asymmetric encryption.

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

4.2. Hash Function Requirements

In general, Go-Cort, Inc. adheres to the NIST Policy on Hash Functions.

4.3. Key Agreement, Authentication and Data Encryption

4.3.1. Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

4.3.2. End points must be authenticated prior to the exchange or derivation of session keys.

4.3.3. Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

4.3.4. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

4.3.5. All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.3.6. All application data is encrypted at rest.

4.3.7. Application data is encrypted in transit with TLS 1.2. All apptoto.com (application) traffic is routed through an AWS Application Load Balancer. That elbv2's listener is assigned security policy 'ELBSecurityPolicy-TLS-1-2-Ext-2018-06' with specification "SslProtocols": ["TLSv1.2"].

4.4. Key Generation

4.4.1. Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

4.4.2. Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5. Policy Compliance

5.1. Compliance Measurement

Go-Cort, Inc. will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback from employees.

5.2. Exceptions

Any exception to the policy must be approved by Go-Cort, Inc. in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Date of Change	Responsible	Summary of Change
October 2016	Frank Cort	Adopted and customized to Go-Cort LLC (DBA Apptoto)
January 2021	Frank Cort	Customized to Go-Cort, Inc. (DBA Apptoto) Data encryption updated