iDIRECT Government

RESILIENT. SECURE. INNOVATIVE.

TRANSMISSION SECURITY (TRANSEC)
Tech Brief

For today's military, situational awareness is a critical component to the success of their mission. Threat actors readily stand by to monitor, exploit or intercept communications for malicious intent. To mitigate this threat, iDirect Government (iDirectGov) has provided enhanced Transmission Security (TRANSEC) capabilities within our Evolution Defense software.

TRANSEC Features

iDirectGov has implemented the following solutions in response to the security vulnerabilities of a TDMA VSAT network:

- Masking Channel Activity
- Obfuscating Acquisition Activity
- Control Channel Information
- Hub and Remote Authentication
- FIPS 140-3 Level 3* (extending the cryptography standards to cover hardware, software, firmware, and hybrid configurations.

iDirectGov has implemented a TRANSEC-compliant network architecture that exceeds the requirements outlined by the U.S. government while still maintaining the quality of service needed to support voice, video and data over a satellite link. The iDirectGov platform secures VSAT transmissions from interception and exploitation by incorporating encryption inherent in COMSEC; conforming to 256-bit AES as specified by the Federal Information Processing Standard (FIPS) 140-3 Level 3, while masking traffic types, volumes, and acquisition of remote terminals. Through a combination of hardware and software, TRANSEC ensures data blocks are a uniform size. This conceals traffic activity while incorporating a Certificate Authority (CA) issued x.509 digital certificate to authenticate the remote terminal.

Adversaries monitoring a TRANSEC-enabled network will only see an obfuscation of secure data, precluding anyone from monitoring the network, or extracting any usable information joining a protected network. As an added measure, security keys are periodically rotated to continually maintain a strong security posture. Through these security measures, the use of TRANSEC adds an authentication mechanism that prevents adversaries from joining a protected network or launching "man-in-the-middle" attacks. Conversely, adversaries would not be able to re-direct a TRANSEC-enabled remote to joining another network without the proper identification and authentication.

By incorporating FIPS 140-3 certified 256-bit AES encryption and Over-The-Air key exchange features, iDirectGov can mask all Layer-2 and above to include High-level Data Link Control (HDLC) information. In addition to protecting the network infrastructure, our Network Management System, Protocol Processor, and Global Key Distribution servers are subjected to the Security Content Automation Protocol (SCAP) for vulnerability management and policy compliance.

Enhancing TRANSEC and Security with an Independent Module

With the 9-Series Satellite Routers and Defense Line Cards (DLCs), iDirectGov has expanded the existing FIPS certification from Level 2 to Level 3 requirements as defined by the National Institute of Standards and Technology (NIST). Through hardware and software development, the embedded yet independent TRANSEC module operates through a trusted path separate from all other interfaces on the product. The module also features strong physical security for tamper prevention and the capability to zeroize the security keys or critical security parameters (CSPs) stored on the module itself. If required, the revocation or zeroization of the keys can be accomplished either over-the-air (OTA) by the hub operator or locally on the remote by authorized personnel.

* Certification pending

TRANSMISSION SECURITY (TRANSEC)

Tech Brief (continued)

TRANSEC prevents an adversary from exploiting information available in a communications channel without having defeated encryption.

One-Way Networks

iDirectGov has further enhanced its TRANSEC capabilities by securing one-way broadcast transmissions. Based on the encapsulation method, LEGS, the iDirectGov platform can provide the same level of security for one-way networks by utilizing automatic OTA, one-way key distribution. For the 900 and 9350 remotes with dual-demodulator support, they are capable of dual-domain TRANSEC – the ability to establish two independent chains of trust (sets of X.509s) between two different CAs.

An example use case of this feature would be one demodulator on a two-way TRANSEC network while the second demodulator receives a separate one-way TRANSEC secured broadcast. Elliptical Curve Cryptography (ECC) is used for key generation along with x.509 certificates for authentication in each security domain. To better maintain TRANSEC networks, the user interface allows for the management of both one-way and two-way networks.

Single Chip Crypto

With the introduction of the 4-Series SDRs iDirectGov has implemented Single Chip Crypto (SCC) that allows the hardware to have multiple levels of security within one chip. Sometimes referred to as digital fencing, the TRANSEC module is isolated in a secure environment on a single chip. Any attempt to compromise the digital fencing will result in the chip being zeroized.

Crypto-agility

With the release of Evolution Defense 4.6 iDirectGov introduces their fourth generation TRANSEC includes crypto-agility. The Key Distribution Protocols (KDP) used in previous versions have been consolidated with two new protocols:

- Modified Global Key Synchronization and Backup (GKSB) which allows multiple key distribution on the Protocol Processor (PP) operating on Transport Layer Security (TLS) 1.3, the latest and strongest version of TLS. GKSB is used by the global key synchronization network and PP to distribute and synchronize the multiple encryption keys and Stream IDs across system components.
- Enhanced Key Distribution Protocol (KDP) allows cryptographic keys to be flexible and adapt to future methods of data protection.

Crypto-agility implementation also results in overall efficiency improvements by eliminating the Initialization Vector. These improvements will allow for adoption of future encryption capabilities to better protect users and their data.

Spectral Efficiency

The latest enhancements to iDirectGov's TRANSEC also bring spectral efficiency improvements to networks. Once a remote is in the network the upstream effciency of TRANSEC is equal to non-TRANSEC networks, thus eliminating the need for more space segment to support overhead.

iDirectGov has implemented a TRANSEC-compliant network architecture that exceeds the requirements outlined by the U.S. government while still maintaining the quality of services expected from an iDirectGov network.