Transmission Security (TRANSEC) Technology Brief

For today's military, situational awareness is a critical component to the success of their mission. Wherever this may be, threat actors readily stand by to monitor, exploit or intercept communications for malicious intent. To mitigate this threat, iDirect has provided enhanced Transmission Security (TRANSEC) capabilities with the release of the Evolution 4.2 software, extending protection to cover both one-way and two-way TRANSEC networks.

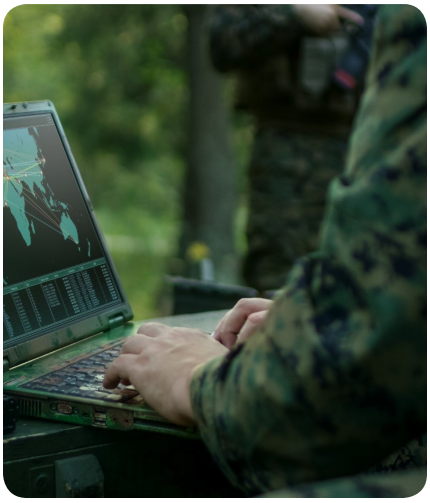
iDirect has implemented a TRANSEC-compliant network architecture that exceeds the requirements outlined by the U.S. government while still maintaining the quality of service needed to support voice, video and data over a satellite link. The iDirect platform secures VSAT transmissions from interception and exploitation by incorporating encryption inherent in COMSEC; conforming to 256-bit AES as specified by the Federal Information Processing Center (FIPS) 140-2, 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 redirect a TRANSEC-enabled remote to joining another network without the proper identification and authentification.

By incorporating FIPS 140-2 certified 256-bit AES encryption and over-the-air key exchange features, iDirect is able to mask all Layer-2 information. In addition to protecting the network infrastructure, our Network Management System and Protocol Processores are subject to the Security Content Automation Protocol (SCAP) for vulnerability management and policy compliance.

Enhancing TRANSEC and Security with 4.2 and the 9-Series

With the release of the 9-Series Satellite Routers and Defense Line Cards (DLCs) iDirect has expanded their existing FIPS 140-2



TRANSEC Features

iDirect 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 Authentification
- FIPS 140-2

iDirect

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 separate and trusted path from all other interfaces on the product. The module also features a strong physical security measure 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 of zeroization of the keys can be accomplished either over-the-air (OTA) by the hub operator or locally on the remote by authorized personnel.

One-Way Networks

iDirect has further enhanced their TRANSEC capabilities in 4.2 by securing one-way broadcast transmissions. Based on their encapsulation method, LEGS, the iDirect 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-modulator 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 authentification in eac security domain. To better maintain TRANSEC networks, 4.2 introduces an enhanced user interface for the management of both one-way and two-way networks.

iDirect has implemented a TRANSEC-compliant network architecture that exceeds the requirements outlined by the U.S. government, while still maintaining the quality and service needed to support voice, video and data over a satellite link.

iDirect
13861 Sunrise Valley Drive
Suite 300
Herndon, VA 20171
+1 703.648.8000
+1 866.345.0983
www.idirect.net