



Secure Voice, Data, and Fax

For Iridium, Thuraya, Cellular, and Landline Communications

Toll Free 800-881-9125

Fax 615-902-0028 Office 615-889-8833

www.OutfitterSatellite.com

2911 Elm Hill Pike Nashville, TN 37214

Why Choose Hardware-Based Encryption?

- Hardware solutions protect keys
- Hardware based algorithms are tamper proof
- Hardware is immune to Internet based attacks
- Passwords and log-ins are not necessary, usually the weakest link
- Hardware insures implementation of the algorithm
- Hardware solutions contain random noise generation
- Hardware-based number generators are truly random
- The key generation process can not be altered by software hackers



The Citadel™ Advantage

Citadel™ developed by *Harris Corporation* is a very high-grade algorithm used to secure the communications of military and government operations. The following lists some of the advantages of the Citadel™ over commercial algorithms such as DES and 3DES.

- The Citadel™ algorithm is not publicly released; therefore it is not available for organized attacks such as those that have been performed on DES and 3DES.
- The Citadel™ algorithm does not run efficiently in software, therefore it does not lend itself to parallel, networked computer brute force attacks that search the key space. It is well known that these types of attacks have been successfully used against DES and 3DES.
- The Citadel™ algorithm is used by military organizations throughout the world in the Harris Secure Voice and Data Unit (SVDU).
- In military applications, cryptographic algorithms are changed or updated regularly. There are a number of reasons for this. These include, network separation (security autonomy), interoperability requirements or to prevent system compromise due to lost/captured equipment. The Citadel™ provides a means to update or customize the algorithm without modifying the equipment. The Citadel™ algorithm can interoperate with all Citadel™ based equipment or it can be customized to provide autonomy.
- The Citadel™ algorithm has no weak keys and DES does. A weak key is a key that has a lower number of effective key bits than the physical length of the key.
- DES and 3DES are vulnerable to Linear and Differential Cryptanalysis.
- 3DES achieves its key length through multiple passes through a DES stage. It is therefore vulnerable to the "meet in the middle attack". Citadel™ achieves its key length in a single algorithm pass and in a single iteration. It is therefore not vulnerable to the meet in the middle attack or any variant of the attack.
- DES and 3DES are commercial algorithms and are designed against a commercial threat model. The Citadel™ family of algorithms is designed against a national intelligence agency

level threat model (the highest existing threat level). The algorithms are specifically designed for securing military communications. As such, the algorithms are completely secure against all published cryptanalysis attacks regardless of the adversary's resources. This means that the algorithm is verified to have no vulnerabilities to all known cracking techniques. Commercial algorithms such as DES and 3DES are fielded with known vulnerabilities as long as the typical commercial adversary would not have the resource to exploit the vulnerability. Commercial algorithms are completely inappropriate for military applications where the adversary is a national intelligence agency. This adversary will have the resources and the motivation to exploit any vulnerability. As previously stated, DES and 3DES have been compromised by what is generally regarded as a low level, commercial adversary.

Brief Description of Key Exchange and Encryption Procedures

The Harris Corporation's Citadel™ CCX (or optional Triple DES or AES encryption algorithms) used in the USS-900, DCS-1200, and DCS-1400 are known as "symmetric" algorithms as they require the same "encryption key" on both the encryption and decryption sides. The key cannot be transmitted in the clear, as it could be intercepted and the message or conversation compromised.



The Citadel™ CCX and the AES algorithm utilize 128-bit keys and the Triple DES algorithm is utilizing 3 unique 56-bit keys totaling 168-bits. The USS-900, DCS-1200, and DCS-1400 encryption products are designed so that two and only two devices can create a successful encryption handshake during the telephone conversation ensuring that the voice, fax and data communication can not be eavesdropped by a third party.

The **Diffie-Hellman Key Agreement** procedure is used to allow two users to create and share a secret "encryption key" as follows:

At the start of each call, each user generates a private, random number, which is kept secret within the encryption device. Part of the Diffie-Hellman procedure uses a mathematical process known as a "one-way function". The one-way function has as its input the random number, called a **private key**, and as its output, a second number, which is called a **public key**. The one-way function is like a coffee grinder. You put coffee beans in and get grind out, but with the grind, you can never get the beans back. Once you have the public key, you cannot go backwards and get the private key. The two users then exchange their public keys.

Anyone eavesdropping can intercept the public keys with no problem. The original random private keys are kept secret within the original USS-900, DCS-1200, or DCS-1400 devices and are not transmitted. Once the public keys are exchanged, a second mathematical process is done on each side. Each side combines its own private key with the other side's public key and creates a third number known as the **session key**. The mathematical process is such that the session key generated on both sides is the same number, and that number is used as the encryption key for the encryption algorithm. An eavesdropper only has access to the public keys being exchanged, not the private keys held within CopyTele's units. Therefore the eavesdropper cannot create the session key used in the encryption algorithm and cannot decrypt the conversation or message. New private, public and session keys are created at the start of every encryption session – ensuring confidentiality.