



## **VME Cell combines three layers of security in order to provide a completely secured Connection:**

- Symmetric block cipher AES to encrypt the data. The message transferred from the transmitter to the receiver is “locked” with a secret AES key, and thus can be “unlocked” only with the same key.
- Authentication methods to avert man-in-the-middle attacks and avoid unauthorized usage.
- Diffie-Hellman public key agreement algorithm for creating, for each session, secret random numbers, equal in both sides, without exposing secret information on unprotected channel. These random numbers used for the authentication and as secret key for the data encryption.

### **1. AES: Advanced Encryption Standard**

The AES algorithm is advanced and strong encryption algorithm.  
The guidelines in designing it were:

- Supply a very high level security.
- The security is in the key – up to 2<sup>256</sup> possibilities (256 bits key).
- Coherent and completely closed algorithm.
- The algorithm is in the public domain (which guarantees the best security testing).
- Not a MIPS consuming algorithm.
- Can be implemented in reasonable circuits.
- Efficient algorithm.

### **2. Diffie-Hellman Public Key Agreement Algorithm**

- Diffie-Hellman algorithm is based on the mathematical difficulty in calculating discrete logarithm in finite fields.
- In order to create a common secret number M in two sides of the conversation, without transferring secret information between them, we select a prime number P and a random number G smaller than P. P and G are the public key.  
The public key may be common to many users. Knowing the public key cannot help to an eavesdropper to reveal the secret key.
- Each side selects a random number X, which is the private key.
- Each side calculates the following expression:  $Y = G^x \text{ mod } P$ .



- The sides exchange the Y numbers over the unsecured channel. Knowledge of the Y does not help the eavesdropper to discover the secret key
- Each side calculates  $M = Y \times \text{mod } P$ . The secret number M is equal in both sides.
- M is used as the key of the AES and for the authentication.

### 3. Authentication in VME Cell

Authentication in VME Cell two objectives: to ensure that the other side is an authorized member of the VME Cell user group and to avoid man-in-the-middle attacks. To achieve these goals two methods are used:

#### 3.1 Group Number

All VME Cell are loaded in advanced with a common secret group number. At the beginning of each conversation each side sends to the other side its group number. To avert revealing the group number, it is not sent openly, but it is scrambled together with bits of the common secret number M that was created using Diffie-Hellman method. The caller and the answerer scramble different parts of the secret number, to prevent the sophisticated eavesdropper to reply with the original message. If VME Cell gets a message that fails to correspond to its own group number the call is dropped.

#### 3.2 Session Identification Number

In case of the man-in-the-middle attack, the eavesdropper creates a separate secured session with each side. However, the secret numbers M that created in each session are different, and the eavesdropper cannot make them to be the same. Part of the M number is used as a Session Identification Number, which is shown on VME Cell connected phone screen. At the beginning of the conversation, both sides must compare orally these numbers. If the numbers are not the same, the call must be dropped.

### 4. VME Cell Implementation of the Security Algorithms

- Diffie-Hellman public key (P and G) are common to all VME Cell products
- The public key is programmed in each device.
- Diffie-Hellman private key (X) is randomly drawn for each session.
- For each session the Diffie-Hellman public key agreement is used to create the AES key.

## VME Cell™



- Therefore, for each session there is a new AES key.
- Diffie-Hellman keys length: P and G are 1024-bit numbers. The exponent X is 192-bit number.
- AES key length: 256 bits.
- AES block size: 128 bits.
- Scramble function for group number: SHA-1 (Secure Hash Algorithm).
- Group number possibilities: 126.