



Sectera In-Line Network Encryptor (KG-235) Bulletin

Universal Changeover To Occur March 2003

The following describes how the Sectera INE (KG-235) and the NES (Network Encryption System) handle the Universal Changeover.

Universal Changeover Description: During the year prior to the universal changeover, the FIREFLY keys are issued in “Supersession”, which means that there are actually two universals on the physical key material – the current and the next material. Prior to the supersession period, there is only one universal on the key – the current. After the supersession period, there is only one universal on the key – the next (which now becomes the current one). This is done to make the transition from one universal to the other as seamless as possible.

Changeover Date: The changeover date is only specified by a month and a year. This means that the day is a matter of interpretation. The NES chose to use the beginning day of the month as the changeover date (the key expiration date is also handled the same way). The HAIPIS specification defined the last day of the month as the changeover date (the key expiration date is also defined this way). Because of this interpretation difference, there is a difference in the way the NES and Sectera INE handle Universal Changeover.

NES Only: In networks where there are only NES units (i.e. no Sectera INE’s), the NES will switch from one universal to the other on the first day of the month. The NES will not change from the current universal to the next universal while it is operational. The NES must either reboot or go through a TEK expiration (24 hour self-test). Remember that this TEK expiration time is configurable and can be set for duration or for an absolute time of the day. Therefore, if two NES units are communicating and the Universal changeover date occurs (first day of the month), the units will continue to communicate on the current key until one of the units (or both) go through the TEK expiration reboot. At this time, the unit that reboots will recognize that the current universal has expired and it will load the “next” universal. After the unit reboots, it will try to resume communications with the other units. They will not communicate until each unit goes through the TEK expiration and reboots and loads in the “next” universal.

If all units were to reboot at the same time, all units would come up and communicate on the “next” universal. The caution here is that if the TEK expiration is set for somewhere just before midnight, if a unit should reboot quickly and load the key before midnight, it would get the current key. The next unit might take just a little longer and it might load its key just after midnight. It would get the “next” key. In this case, the units would not communicate. The remedy for this is to reboot the unit that is still on the current key and it will solve the problem. A better solution is to make sure that the TEK expiration time is not set for “close to midnight.” If units are on a staggered TEK expiration, they will lose communication as one unit reboots and will not regain it until the next unit reboots. A good way to solve all of this would be to plan to reboot all units just after midnight of the day of universal changeover (on the first day of the expiration month, not the last day).

Sectera INE Only: In networks where there are only Sectera INE units (i.e. no NES’s), the Sectera INE will switch from one universal to another on the last day of the expiration month (not the first day as is the case with the NES). The Sectera INE will not change from one universal to another until a TEK expires. In the Sectera INE, the unit does not reboot, but each TEK expires one at a time as a function of time from when it was created. Once the TEK expires in either Sectera INE, it will not be recreated until communication is requested. At this time, the changeover date will be evaluated. If the time on both units is after midnight on the last day of the changeover month, the “next” universal is used to create the new TEK. If the time is before midnight on both units, the current universal is used to create the new TEK. If one unit is before midnight and one is after, the TEK will not be created. Attempts will continue to establish the TEK until both clocks are after midnight, when the TEK will be created using the “next” universal. This process will occur TEK by TEK until all TEK’s have been replaced (having been created using the “next” universal).

Mixed Networks: In a network where there are both Sectera INE units and NES units, the process is a combination of the above conditions, with one exception. Since the NES will actually change from the current universal to the next universal at the beginning of the expiration month and the Sectera INE will not change to the next universal until the end of the month, the two units will be configured with the incorrect universals during that month. There are several ways to mitigate this situation.

1. Replace the keys in the Sectera INE on the first day of the universal changeover month with single edition keys (these will have only the next universal on them). Note that these keys will not be available for order until March 1, 2003.
2. Set the clock on the NES to be one month earlier so the two expiration dates will line up with each other.
3. Set the time on the Sectera INE to one month later so the two expiration dates will line up with each other. This currently can only be done with a CM6000.

The EKMS 322 specification actually allows a grace period on key expiration, which makes it acceptable to extend the life of a key for a short period of time. NSA is currently defining this “grace period” to be a maximum of 6 months.

Key Expiration Clarifications for the Sectera INE (KG-235)

When a Sectera INE determines the key expiration date for a FIREFLY key, it reads the month and year and expires the key at the end of the given month. When an NES determines the key expiration date for a FIREFLY key, it also reads the month and year and then expires the key at the beginning of the given month. If the following ground rules are observed, users will not have an issue with key expiration in their networks.

A general ground rule to follow would be to assume all keys expire at the beginning of the month instead of the end of the month and there will never be an issue with key expiration. Additional information given below may allow a user to extend this a little longer if desired.

If the network is a pure Sectera INE network (i.e. no NES units), all key material will expire at the end of the month. This means all units will be fully operational throughout the expiration month. A user with this type of network can take advantage of these extra few weeks if desired, but could just change key material as if it expired at the first of the month.

If the network is not a pure Sectera INE network (i.e. has NES units also), the NES key material will expire at the beginning of the month and the Sectera INE key material will expire at the end of the month. If a user were to just replace the NES keys and allow the Sectera INE keys to remain in the unit until the end of the month, the Sectera will operate correctly, but when it communicates with an NES, the NES will consider the key material expired and will shut itself down. For this reason, Sectera INE key material must be replaced and considered expired at the first of the month, not at the end of the month.

Therefore, if a user always considers key material expired at the beginning of the month instead of at the end, there will never be any problems. The only case where this can be ignored is in a Sectera INE only network.

Release 1.1 Certified

Software Release Version 1.1 has been certified. CD ROMS have been shipped to all KG-235 customers. This is our "Bug Fix Release" which corrects problems found from continued testing in our engineering labs and from customer's inputs. It is unfortunate that we had some problems but the good news is that this software release can be loaded into your KG-235s either locally with the CM5000 or over your network with the CM6000.

If you have not received your copies of Release Version 1.1 contact customer support at:

Phone: (480) 726-1048

DSN: (312) 282-1048

CONUS Toll Free: (877) 449-0600

E-Mail: customer.service@gd-decisionssystem.com

Next Releases Scheduled

Two more software releases are scheduled for 2003.

Release 2.0 will add the final Traffic Flow Security (TFS) mode. The current KG-235 has four modes of TFS already implemented. Other major enhancements in this release will be; Pre-Placed Keys (PPK), DS-101 key loading interface for the Data Transfer Device (DTD), and enhance front panel operation.

We quickly follow the above Release 2.0 with Release 3.0. This will implement HAIPIS Specification Version 1.3.2. Two of the major features are AutoDiscovery and the MEDLEY algorithm. Release 3.0 will also include Layer 2 Transparent Mode with Auto Discovery. With this Layer 2 mode the KG-235 will be interoperable with such protocols as 802.1Q Virtual Private Networking.

Quick Delivery Available

Although, General Dynamics Decision Systems normally quotes Direct Sales as 90-day ARO delivery, we have been filling orders in less than a week. If you have a critical delivery need please contact our order entry by calling or emailing Vicki Muller (480-441-3685 vicki.muller@gd-decisionsystems.com).

Next HAIPIS Meeting In Scottsdale

The next HAIPIS meeting is scheduled for March 11,12 & 13 at General Dynamics Decision Systems in Scottsdale, Arizona. Contact Kristen Heisig (619-553-8273 heisigk@spawar.navy.mil) for details. Average temperatures for March are High 74°F and Low 51°F.

GENERAL DYNAMICS

Decision Systems

8220 East Roosevelt Street
Post Office Box 9040
Scottsdale, AZ 85252-9040

Email: customer.service@gd-decisionsystems.com

Toll Free: 1-877-449-0600

Phone: 1-480-726-1048

Fax: 1-480-726-2971