NANC 157

**Key exchange interval default value**

**Origination Date :**09/10/1997

**Originator:**Lockheed Martin Team

**Description:**

Per requirement R7-111.4 the NPAC SMS shall change the key used between the NPAC and the Service Provider after one year of usage. The default value for the key exchange states 7 days.  These values should be the same.

Laundry list of standards proposed:

* Service Providers may use a single keylist across multiple regions. This applies only to the keylist that the Service Provider generates.  NPAC keys to be changed once a week within the key list.
* Keylists that are exhausted prior to years-end will be replaced with newly generated keylists with keys equal in length to the keys in the exhausted keylist.
* New keylists generated once a year augmented with strengthened keys.  Starting out with an initial keylength of 600 bit and strengthening in increments of 24 bits (per year).
* Naming convention for keylists to be as follows:

   FROM   |  TO   |  REGION  |  KEYLIST #

    XX      XXX   XX        X

e.g. NP      ATT   WC        8

There was a concern that this would allow for only 9 keylists to be generated for each SP (per region).  However, what I propose that in the unlikely event that more than 9 keylists are generated for an SP (per region) we move to alphas as well (i.e. 1-9 and then a-z).  This would allow for a total of 35 keylist to be generated (if we generate more keylists than this for a region something is wrong).

**Final Resolution:**

The default value in requirement R7-111.4 should be changed to 365 days.

The key change occurring once a week is an NPAC only requirement.

The standards proposed have been accepted with the exception of the file name.   Which will be defined as indicated below.

The key file will be <from company SPID >. <to company SPID>X. A file sent from NPAC will be <NPAC Region SPID>.<SPID>X. A file sent from a service provider will be <SPID>.<NPAC Region SPID>X. Where SPID is a 4 digit number (e.g. “0715”).  The NPAC SPID will be those defined in the IIS.  X will be the KEYLIST # as described in the original proposal.

Closed for release 1.

**Related Release:**

1.6

**Status:** Implemented