**Origination Date:** 07/11/17

**Originator:** iconectiv

### Change Order Number: NANC 497

**Description:** NPAC Customer ID in CMIP Key Exchange Files

**Functional Backwards Compatible:** Y

**IMPACT/CHANGE ASSESSMENT**

|  |  |  |
| --- | --- | --- |
| DOC | FRS | IIS |
| Y | N |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CMIP | GDMO | ASN.1 | **Neustar NPAC** | iconectiv NPAC | SOA | LSMS |
| N | N | N | N | N | N |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| XML | XIS | XSD | **Neustar NPAC** | iconectiv NPAC | **NPAC** | SOA | LSMS |
| N | N | N | N | N | N | N |

**Business Need**

Documentation updates to clarify use of NPAC Customer ID in CMIP key files.

**Description of Change:**

Changes detailed below.

FRS:

NPAC SMS (changed text in yellow highlights)

***Appendix D. Encryption Key Exchange***

The CMIP interface to NPAC SMS requires an exchange of the encryption keys used to verify digital signatures. This exchange will consist of a file containing the 1000 key list, and an acknowledgment of receipt of the list will consist of a file containing the MD5 checksum value of each key in the list. This is a CMIP specific concept and applies only to the CMIP interface. The formats for these files is described here.

***Key Exchange File***

The following table shows the format of the encryption key exchange file. This file consists of some header information, followed by 1000 instances of key information. There are no separators of any kind between the individual fields, between the header and key data, or between each set of key data.

When this file is generated by the NPAC SMS, the NPAC Customer Id field contains the region identifier of the NPAC region, as defined in IIS Exhibit 13. When this file is generated by the local system, the NPAC Customer Id field should contain the identifier of the NPAC Customer, but the NPAC SMS shall accept either the NPAC Customer ID or the NPAC region identifier as defined in IIS Exhibit 13.

| **Encryption Key exchange file format** |
| --- |
| **Field Number** | **Field Name** | **Type** | **Size (bytes)** | **Format** |
| 1 | NPAC Customer Id  | ASCII | 4 | Character String |
| [snip] |  |  |  |  |

***Key Acknowledgment File***

Before a key list may be used, the sender must receive a key acknowledgment file. The key acknowledgment file serves two purposes:

1. Verify that the key list has been received by the intended recipient.
2. Verify the correctness of each key in the list.

Furthermore, the need for an acknowledgment of this kind is specified in requirement R7-108.2. Once this file has been received, the sender of the key list can put the list into active use.

Table D-1 below shows the format of the encryption key acknowledgment file. This file consists of some header information, followed by 1000 instances of key hash information. There are no separators of any kind between the individual fields, between the header and key hash data, or between each set of key hash data. The MD5 hash value will be calculated from the public modulus value of the key.

When this file is generated by the NPAC SMS, the NPAC Customer Id field contains the region identifier of the NPAC region, as defined in IIS Exhibit 13. When this file is generated by the local system, the NPAC Customer Id field should contain the identifier of the NPAC Customer, but the NPAC SMS shall accept either the NPAC Customer ID or the NPAC region identifier as defined in IIS Exhibit 13.

| **Encryption Key acknowledgement file format** |
| --- |
| **Field Number** | **Field Name** | **Type** | **Size (bytes)** | **Format** |
| 1 | NPAC Customer Id  | ASCII | 4 | Character String |
| [snip] |  |  |  |  |