

## March 4-5, 2014 LNPA WORKING GROUP ACTION ITEMS ASSIGNED:

**NOTE: FOR THE FOLLOWING ACTION ITEMS THIS NUMBERING SCHEME APPLIES:**

- **FIRST TWO DIGITS DESIGNATE THE MONTH OF THE LNPA WG MEETING/CALL**
- **SECOND TWO DIGITS DESIGNATE THE DAY OF THE LNPA WG MEETING/CALL**
- **THIRD TWO DIGITS DESIGNATE THE YEAR OF THE LNPA WG MEETING/CALL**
- **LAST TWO DIGITS DESIGNATE THE ACTION ITEM NUMBER**

## LNPA WG PARTICIPANTS ACTION ITEMS:

### Neustar Action Items

#### **030414-01 – Sunset list 3.2 – Require Query “More” SVs**

In R3.3 (Feb 2006), the NPAC implemented NANC 285, the enhanced SV Query capability. Similar to the LTI with the “more SVs” button, NANC 285 added a “more” capability to the CMIP SV Query. For SOAs/LSMSs that do not support the “more” capability, SV Query functionality is limited. This functionality is still optional in the XML interface. Sunset of this feature would make it required for both interfaces. Neustar to investigate how often this error of queries exceeding the 150 SV returned limit occurs.

#### **030414-02 – Sunset list 9.3 Remove unused Billing categories (like mass storage, audits, etc.)**

Neustar to provide a list of the billing data and billing reports.

**030414-03** – Neustar to update the Sunset list based on March discussion and resend. Remove the items that the WG has decided not to sunset and remove items that already have a change order to remove.

## ACTION ITEMS REMAINING OPEN FROM PREVIOUS LNPA WG MEETINGS:

**010714-02 REVISED** – Service Providers and Vendors should review the M&P for certificate-related activities in the NPAC XML interface. The M&P can be found on the NPAC secure web site at the following URL:

<https://www.npac.com/npac-user/access-connectivity/npac-xml-certificate-trust-authority>

Additionally, section 3.3 (NPAC Use of Certificates) in the XIS describe how this works from an application perspective.

Reviewers should consult with their information security teams to make sure these procedures are acceptable. In the current process, the User supplies basic information to the NPAC Certificate Authority (CA) via email. This basic information makes up the distinguished name of the certificate, and includes the SPID, region and system type. The NPAC CA creates a User within the system for this request, and the requestor receives the logon URL and the login credentials in separate emails. Upon login, JavaScript code is downloaded to the User's web browser. This JavaScript code calls APIs within the User's browser to generate a public/private key pair. The public portion of this key pair is then sent to the NPAC CA. The NPAC CA combines this public key with the information associated with the User to generate a signed certificate that includes the public key and the distinguished name information (the spid, the region, and the system type). This signed certificate is then downloaded to the User's machine, where it is combined with the private key. The private key is generated on the User's machine and is never transmitted to the NPAC CA.

**010714-04** – WG members are to be prepared to continue discussion of the potential sun-set list at the March 2014 LNPA WG meeting. WG will discuss benefit and need for each item on the list including level of effort for keeping or removing.