NANC 382

**“Port-Protection” System**

**Origination Date :**04/04/2003

**Originator:**Neustar

**Description:**

**Overview:**

The “Port Protection” system is a competitively neutral approach to preventing inadvertent ports that gives end-users the ability to define their portable telephone numbers as “not-portable.”  The NPAC SMS enforces the “not-portable” status of a telephone number so long as it remains in effect.  No Local Service Provider (LSP) can invoke or revoke “port protection” on a working telephone number; end-users completely control the portability of their portable telephone numbers.

**Business Need:**

Inadvertent porting of working numbers is a concern to both Local Service Providers (LSPs) and their customers.  In today’s LNP environment, an LSP cannot absolutely assure its customers that their terminating service will not be interrupted, even if it can insure that physical plant is operated without failure.  This is because any LSP by mistake may port a telephone number away from that number’s current serving switch.

The inadvertent port can occur in a number of ways, but the most common occurrences appear to be caused by two errors: (1.) when the wrong telephone number submitted to NPAC for a conventional inter-SP port, and (2.) when intra-SP ports are not done before a pooled block is created.  There is a similar inadvertent port problem for non-working numbers, but erroneous moves of non-working numbers are not directly service-affecting and are not addressed here.

NeuStar suggests the following competitively neutral method to prevent inadvertent ports of working TNs.

**System Architecture**

Changes to the NPAC SMS are required, to establish a table of “Port-Protected TNs” in which portable numbers that no longer can be ported are listed.  A step must be added to the NPAC SMS’s validation process in order to check this new table whenever an inter-SP port or pooled block create is attempted.  An interface change could be required as well if industry wishes to know when a request’s rejection is due to the involved number being on the “Port Protection” list.

Creation of an IVR system is required, to receive end-user requests for protection of their numbers from porting (or to remove this protection) and to relay the information to the NPAC SMS.  The system would automatically modify the NPAC’s “Port-Protection” tables based on the end-user requests it receives.  Access to the IVR would be through the end-user’s current LSP customer rep.  Any other LSP willing to assist the end-user could be involved.

The end-user’s telephone number is entered in the NPAC’s “Port Protection” tables whenever “port-protection” is requested.  The end-user cannot reach the “Port-Protection” IVR system directly, but instead must be connected through a local Service Provider’s customer contact system, much like what is done in the PIC selection process, where the Service Provider’s customer rep advances the call to a third-party verification service, then leaves the call to allow the third-party verifier and end-user to converse.

The IVR system must recognize the LSP as authorized to participate in the “Port Protect” process.  (The LSP need not be a facility-based provider.)

Arrangements for security handshakes must be made in advance with each participating LSP.

A telephone number may be added to or removed from the “Port Protection” list whenever and as often as the end-user wishes.

To maintain the proposal’s competitive neutrality, the process assumes any LSP may assist the end-user.  However, the possibility of end-users invoking or revoking “Port Protection” on telephone numbers other than their own would be mitigated if only an LSP with which the end-user had a contractual relationship could participate, i.e., only the current LSP or a new LSP in a pending port request situation.

**System Operation -**

The end-user’s telephone number is entered in the NPAC’s “Port Protection” tables whenever “port-protection” is requested.  The end-user cannot reach the “Port-Protection” IVR system directly, but instead must be connected through a local Service Provider’s customer contact system, much like what is done in the PIC selection process, where the Service Provider’s customer rep advances the call to a third-party verification service, then leaves the call to allow the third-party verifier and end-user to converse.

The IVR system must recognize the LSP as authorized to participate in the “Port Protect” process.  (The LSP need not be a facility-based provider.)

Arrangements for security handshakes must be made in advance with each participating LSP.

A telephone number may be added to or removed from the “Port Protection” list whenever and as often as the end-user wishes.

To maintain the proposal’s competitive neutrality, the process assumes any LSP may assist the end-user.  However, the possibility of end-users invoking or revoking “Port Protection” on telephone numbers other than their own would be mitigated if only an LSP with which the end-user had a contractual relationship could participate, i.e., only the current LSP or a new LSP in a pending port request situation.

When the NPAC attempts to create a pending SV or a pooled block, the NPAC will check the “Port Protection” list in its validation process for inter-SP port (including Port-to-Original) and “-X” create requests.

The “Port Protection” validation does not occur for intra-SP ports.  These may represent inadvertent ports, but validation necessary to determine whether override would be appropriate is not feasible.  The validation occurs for only those deletes that are “Port-to-Original” situations.

**Process Flow**

The end-user contacts an LSP (or an LSP contacts the end-user).  (It is not inherently necessary for there to be Service Provider involvement in this process, but NeuStar is not prepared to operate a system which does not involve LSP participation.)

End-user indicates desire to invoke (or revoke) “Port Protection.”

LSP customer rep places end-user on hold and calls the “Port-Protection” IVR.

LSP provides its pre-assigned ID information to IVR system.  (LSP arrange for security codes before attempting to assist end-users with the “Port-protection” process.)

LSP brings end-user on to the active line and leaves call; end-user interacts with IVR.

Using a standard script, the IVR confirms caller is authorized to make changes to the telephone number account, determines the caller’s name, and lists the telephone number(s) to be added to (or removed from) the “port-protection” table.  The customer may actually enter the TN desired.  The call is recorded.

The IVR system then enters this information into an automated ticket system.

Completion of the ticket automatically sends triggers an update of the NPAC’s “port-protection” table.

In the case of a number that has been entered in the port-protection table, but is no longer assigned to an end-user, the current Service Provider itself can ask that the number be removed from the “port-protection” table.  The provider would have to be recognized by the NPAC as the code/block owner and would have to state that the number is not assigned to an end-user.

This change order was reviewed and revised during the May through Sep ’03 LNPAWG meetings.  The final version of the open change order at the time of acceptance (for development of more detailed information) is shown below:

**Overview:**

The “Port Protection” system is a competitively neutral approach to preventing inadvertent ports.  The system makes it possible for end-users to define their portable telephone numbers as “not-portable.”  The NPAC SMS prevents the port of a “not-portable” telephone number (TN) through its automated validation processes.  A Local Service Provider (LSP) can invoke or revoke “port protection” for a working TN, but only at the end-user’s request.

**Business Need:**

Inadvertent porting of working TNs is a concern to both Local Service Providers (LSPs) and their customers.  In today’s LNP environment, an LSP cannot absolutely assure its customers that their terminating service will not be interrupted, even if it can insure that the physical plant is operated without failure.  This is because another LSP by mistake may port a TN away from that number’s current serving switch.

The inadvertent port can occur in a number of ways, but the most common occurrences appear to be caused by two errors: (1.) the wrong TN is submitted to the NPAC SMS for a conventional inter-SP port, and (2.) intra-SP ports are not done before a thousands-block is created. There are similar inadvertent port scenarios for non-working TNs, but erroneous moves of non-working TNs are not immediately service-affecting and are not addressed here.

NeuStar suggests the following competitively neutral method to prevent inadvertent ports of working TNs.

**System Operation**

A TN is added to the NPAC’s Port Protection table when an LSP requests this action.  The same process applies when an LSP requests the removal of a TN from the table.

The NPAC Help Desk accepts requests to change Port Protection table entries only from pre-authorized representatives of an LSP.  (The LSP need not be a facility-based provider.)  A TN may be added to or removed from the “Port Protection” list as often as required.

When the NPAC SMS receives the new SP’s Create request, it will check the Port Protection table during the Pending SV Create validation process for inter-SP ports (including Port-to-Original SV deletes). Optionally , the validation is performed for intra-SP ports.

The NPAC SMS also will make this validation check in connection with “-X” create requests.

The validation is not applied to Modify requests

In the disconnect scenario, the NPAC SMS will check the Port Protection list and, if the TN is found, will remove the involved disconnected ported TN from the list.  This automatic removal of a disconnected TN from the Port Protection list can occur only in the case of a disconnected TN that was ported.  A non-ported TN that is disconnected must be removed from the list by the LSP having the disconnected non-ported TN in its inventory.

**Process Flow**

**NPAC Help Desk**

•    The end-user contacts an LSP (or an LSP contacts the end-user).

•    End-user indicates to LSP his desire to invoke (or revoke) “Port Protection.”

•    LSP contacts NPAC Help Desk via e-mail to request change.

•    The NPAC Help Desk updates the Port Protection table.

**NPAC SMS**

•    NPAC SMS applies the Port Protection validation (1.) to the new-SP Create request of an inter-SP port, (2.) to a Block Creation request, and (3.) optionally at the individual SPID level, to an intra-SP port request.  If the TN is found on the Port Protection list, NPAC SMS rejects the request and indicates that a Port Protection validation failure is the reason for the request’s rejection.

•    Disconnect of a ported TN results in automatic removal of the TN from the Port Protection list; disconnect of a non-ported TN requires owning LSP to request the disconnected TN’s removal from the list.

•    An LSP’s regional NPAC SMS Profile indicates whether the Port Protection validation should be applied also to its intra-SP port requests.

**Nov ’03 LNPAWG, discussion:**

The group discussed the high-level steps.  There were a couple of updates that were requested.  These steps will be evaluated once the policy issues/questions are discussed:

1.    For intra-ports, let the port go through and keep them on the list.

2.    In steps 4.b, no need to look at the list, just allow the Old SP Create to happen.  If they are on the list, then for now, leave it on the list.

3.    For step 8, add that this does NOT apply to PTO.

**Policy issues/questions:**  (at the Jan ’04 LNPAWG, we would discuss if and how, we might Tee this up at NANC).

1.    What types/classes of numbers can be placed on the list?  What criteria?  What kind of criteria?

2.    Who can put it on the list and remove it from the list?  This is an authorization question.

3.    What is the PROCESS for getting them on and off the list?  How mechanically, do you put/remove it on the list?

4.    Who can access the list? Need a process to access the list.  What is shown when they access the list (police, other authority)?

**Other points discussed:**

1.    Want more than just the IVR way to get numbers on/off the list.

2.    Want some type of pre-validation process to “ping” the list and see if someone is on the PPL.

3.    Want the ability to audit the list.

**Final Resolution:**

Moved to closed/no-action.

**Related Release:**

N/A.

**Status:** Closed