



# **NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL**

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

## **Implementing a Simple Security System for Conversations Between the Interchange Distribution Calculator and Various Authority Servers**

### **NERC TISWG**

In light of recent discussions within the TIS Forum, the TISWG and the IDCWG have agreed that the following approach should be taken to ensure secure communications between the Interchange Distribution Calculator (IDC) and the various Authority Servers in use with E-Tag.

Essentially, each Authority Server will be assigned a password to use when communicating with the IDC. This password shall be contained in the TMP Protocol as the Tag Key used when communicating with the registered forwarding URL. Should the IDC receive any requests containing credentials other than those known to it, the IDC shall ignore these requests; otherwise, the IDC shall evaluate these requests as normal. At times, in order to facilitate the changing of keys, it may be necessary to operate with two “valid” keys; this is described in more detail in the section titled, “The Interchange Distribution Calculator.”

This method assigns the following procedures and responsibilities as detailed below:

#### ***NERC***

NERC shall, at various intervals chosen at their discretion, supply both the Interchange Distribution Calculator (IDC) and an associated Authority Server with a secret key to use in communications between the Authority Server and the IDC. This key shall be generated by a concatenation of 12 characters selected randomly from the following: the numbers 0–9, and both upper and lower cases of the English Alphabet (ASCII 48-57, 65-90, 97-122). Upon assignation of a key, NERC will mail (via secure and traceable means) the contents of the key to both the Authority Server that will utilize the key and the IDC with which the Authority Server will be communicating. When issuing these key assignments, NERC will also supply a date at which point the new key shall be effective.

#### ***Authority Servers***

An Authority Server shall have a user configurable 12-character “IDC Key.” This key shall be provided to the Authority by NERC staff and generated by a concatenation of 12 characters selected randomly from the following: the numbers 0–9, and both upper and lower cases of the English Alphabet (ASCII 48-57, 65-90, 97-122). Standard key conventions within E-Tag append this 12-character key to the acronym of the Load CA; this practice shall continue, although the IDC shall only verify the contents of the last 12 characters.

Upon sending an IMPLEMENT message to the IDC, the Authority shall use this static key (rather than a dynamically generated key) as the Tag Key. Under no circumstances shall an Authority attempt to assign a key to the IDC other than the appropriate key designated by NERC for this purpose. All communications with the IDC shall utilize this key.

Authorities must provide a mechanism with which users may change this key upon demand. Upon the changing of the key, all further communication from the Authority Server to the IDC must utilize the new key. Keys should be changed as soon as possible on the day specified (in Central Standard Time) by NERC in their letter of key assignment.

### ***The Interchange Distribution Calculator***

The Interchange Distribution Calculator (IDC) shall store, for each Authority, a maximum of two keys. These keys shall be provided to the IDC by NERC staff and generated by a concatenation of 12 characters selected randomly from the following: the numbers 0–9, and both upper and lower cases of the English Alphabet (ASCII 48-57, 65-90, 97-122). Each single key should be associated with a particular Authority.

Should a request for key assignment be made, the IDC Operator shall activate the new key prior to (but no more than 24 hours prior to) the date specified (in Central Standard Time) by NERC in their letter of key assignment.

At the end of the date specified (in Central Standard Time) by NERC in their letter of key assignment, the IDC Operator shall deactivate the old key, leaving the new key active. The time during which two distinctly different keys are active should be kept to the smallest practicable minimum while meeting the requirements described above.

The IDC, upon receipt of an IMPLEMENT message from an Authority, shall immediately verify the validity of the transmission by first using the Tag ID to determine the Authority Server for the transaction (based on the registry). Next, the IDC shall verify the string comprised of the last 12 characters of the tag key presented in the transaction is indeed identical to the key registered to the previously identified Authority. Should the key appear to be invalid or not match one of the two potentially (as described above) active keys, the transaction shall immediately be considered invalid and no further processing of the message shall occur. If, on the other hand, the key is valid, the message should be processed as normal and then accepted as legitimate.

Under no circumstances should key validation exceed these requirements. It is not necessary, and indeed forbidden, for the IDC to require that modifications to an existing tag (i.e., cancellations) share the same key; it is validation enough that the Authority Server has presented credentials identifying itself as a legitimate Authority.