Bank Audi

Annex: Security Best Practices & Measures

1- Creating/Validating an MD5 Signature for e-Payment Transactions

The merchant creates the MD5 Secure Hash value on the Transaction Request data. The e-Payment gateway creates another MD5 Secure Hash value and sends it back to the merchant in the Transaction Response.

The Secure Hash is a Hex encoded MD5 output of a concatenation of all the data parameters. The order that the data parameters are hashed in is extremely important as different transactions contain different data fields so rather than giving the explicit order for each parameter, the order that parameters are hashed in should follow the following rules:

- The Secure Hash Secret is always first.
- Then all parameters are concatenated to the secret in alphabetical order of the parameter name. More specifically, the data sort should be in ascending order of the ASCII value of each parameter's name, for example, '**Card**' comes before '**card**'. Where one string is an exact substring of another, the smaller string should be ordered before the longer, for example, '**Card**' should come before '**CardNum**'.
- Fields must not have any separators between them and must not include any null terminating characters or the like.

The e-Payment gateway also includes the vpc_SecureHash in the Transaction Response so the merchant can check the security of the receipt data. This is performed by first stripping off the vpc_SecureHash, and then performing the same steps as creating an MD5 Secure Hash for the Transaction Request, but using the received Transaction Response data fields instead.

The received vpc_SecureHash should be compared by the merchant with the MD5 Secure Hash calculated from the Transaction Response data. **If both MD5 signatures are the same, the data has not been changed in transit. If they are different then you cannot trust the response as it has been manipulated and the transaction should be considered as declined even if the response code is 0 (accepted).**
Accordingly the first thing to be done when a response is received is the hash validation and if it's correct then the merchant can proceed and check other fields in the response.

2- Store Secure Hash Secret Key Securely

You must keep your Secure Hash Secret stored securely. Do not store your Secure Hash Secret key within the source code, or other website page as it is common for web server vulnerabilities to be discovered where source code of such pages can be viewed. You should store your Secure Hash Secret in a secured database, or in a file that is not directly accessible by your web server and has suitable system security permissions. Secure Hash Secret can be changed at any time you believe that its security may have been compromised. Please contact the bank when there's a need to change the Secure Hash Secret key.