KTA Encryption-Decryption algorithm

307446

Question / Problem:

What is (or are) the encryption algorithms used for passwords and secure variables in KTA? I need to know the used encryption level by KTA to make sure that our security departments accept them for storage of password.

Answer / Solution:

There are several encryption algorithm such as:

DES/3DES or TripleDES

Blowfish

AES

Twofish

IDEA

MD5

SHA1

HMAC

RSA Security

In terms of KTA, protecting all the data in transit (apart from Secure variables) can be done using HTTPS with more secure encryption ciphers. We don’t do anything specific in KTA for that.

In terms of protecting secure variables, this functionality is to protect sensitive data that is being passed between client/server. In order to protect this data, we encrypt these variables if the user wishes to do so. This encryption/decryption is done on the server to avoid any storage of the cryptographic key on the client. This is done using APIs Encrypt() and Decrypt() methods in CryptoHelper using 3DES algorithm.

In other words, 3DES algorithm is currently been used but would be changed to AES.
**Applies to:**

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>KTA</td>
<td>7.3</td>
<td>Encryption/Decryption</td>
</tr>
<tr>
<td>KTA</td>
<td>7.4</td>
<td>Encryption/Decryption</td>
</tr>
<tr>
<td>KTA</td>
<td>7.5</td>
<td>Encryption/Decryption</td>
</tr>
</tbody>
</table>

Author: Tunji Akanni