How can I decrypt encrypted data?

Scope: This Solution applies to data encrypted with TDES or AES algorithms using either the Data Key Variant or a PIN Key variant. Therefore it applies to all encrypting readers.

Answer:

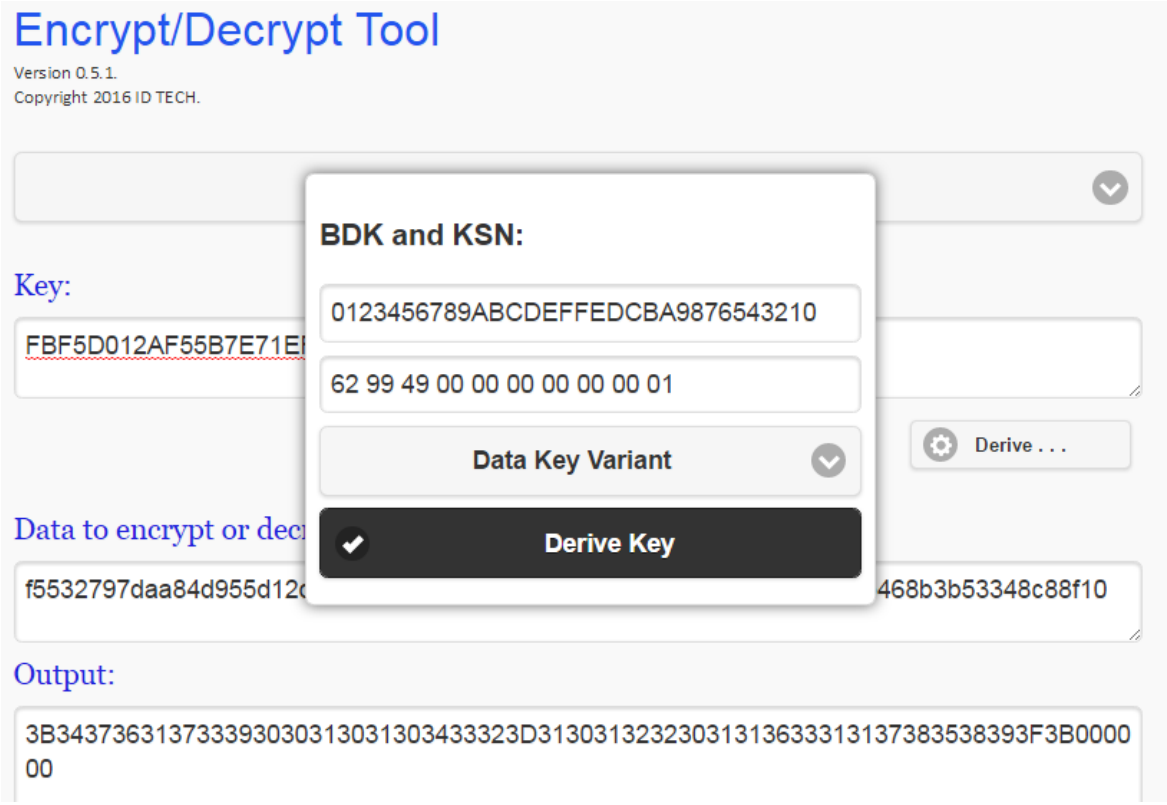
To decrypt encrypted data, you will need the the BDK (Base Derivation Key) and the KSN (Key Serial Number) with which the data was encrypted. Generally speaking, the BDK is "super-secret." You will only have the BDK when using a reader that is injected with a demo key. The BDK for a reader with a demo key injected should be 0123456789ABCDEFFEDCBA9876543210 (this is the so-called ANSI standard test key). The KSN will always be sent in plain text (unencrypted) along with the encrypted data and will change slightly with every transaction. The BDK for a production key is only "known" by the key injection facility (ID TECH) and the decrypting party (gateway or acquirer).

> ⚠ A production BDK is, by design, never exposed outside an HSM (Hardware Security Module). Even when transferred or backed up it is broken into parts and obscured mathematically. So, to say that a production BDK is "known" by anyone is inaccurate. The point to understand is that the payments industry has gone to great lengths to ensure that BDKs are kept secret. The only exception is the demo BDK. It is knowable. (known)

For low-level information on the decryption process, see How to Decrypt Credit Card Data. This two-part article goes into detail about how DUKPT keys are derived and how those keys can be used to decrypt data that was previously encrypted using TDES or AES algorithms.

For a tool you can use right now to decrypt data: Navigate to the ID TECH Encrypt/Decrypt Tool. Select "Encrypt or decrypt data" option, then use the Derive button to enter your KSN and derive a session key. In the main window, enter your encrypted data in the Data pane, put the derived (session) key in the Key pane, and click Decrypt.

> ⚠ TDES is the default (and, by far, the most common) encryption/decryption algorithm. However, if the data was encrypted using AES instead of TDES, Check the "use AES" checkbox.



Related articles

Content by label

There is no content with the specified labels