Derived unique key per transaction

From Wikipedia, the free encyclopedia

This is the current revision of Derived unique key per transaction as edited by CitizenB (Talk | contribs) at 18:41, 5 November 2007. This URL is a permanent link to this version of this page.

(diff) ← Previous revision | current version (diff) | Newer revision → (diff)
Jump to: navigation, search

In cryptography, **Derived Unique Key Per Transaction (DUKPT)** is a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key. Therefore, if a derived key is compromised, future and past transaction data is still protected since the next or prior keys cannot be determined easily. [1] **DUKPT** is specified in ANSI X9.24 part 1.

DUKPT allows the processing of the encryption to be moved away from the devices that hold the shared secret. The encryption is done with a *derived* key, which is not re-used after the transaction. DUKPT is used to encrypt electronic commerce transactions. While it can be used to protect information between two companies or banks, it is typically used to encrypt PIN information acquired by Point-Of-Sale (POS) devices.

DUKPT is not itself an encryption standard; rather it is a standard method for generating matching cryptographic keys at each end of an encrypted transaction. There is no public key, nor is there any key negotiation between the two parties. At no time is the shared secret, or any subsequent key derived from the shared secret, exposed to possible interception. Only a few bytes of terminal identification, followed by the cryptogram itself, are transmitted. With each successive mutually and independently derived unique key, each party plugs the key into an encryption algorithm and uses the key to encrypt and decrypt the cryptogram. Once each transaction is complete, the two parties generate a new key derived from the key just used, and discard the old key. This key is used in the next transaction, and so forth.

The system relies on a base derivation key (BDK), which is the shared secret used to start the chain of keys. In a host-client topology, before the client is deployed, the host initializes the client device with a base derivation key and an initial transaction key (ITK). The client, once deployed, uses the ITK to initiate contact with the host. When contact is established, the chain of discarded and recalculated keys begins.

The system provides excellent security because even if one transmission is successfully intercepted and decrypted, no useful information is provided to facilitate decryption of subsequent or previous transactions. Further, when coupled with strong encryption, the time required to decrypt a transmission makes man-in-the-middle attacks virtually impossible.

This cryptography-related article is a stub. You can help Wikipedia by expanding it.

Go Search

Toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link
- Cite this page

- This version of the page has been revised.
  Besides normal editing, the reason for revision may have been that this version contains factual inaccuracies, vandalism, or material not compatible with the GNU Free Documentation License.
- Privacy policy
- About Wikipedia
- Disclaimers