A B C D E F G H I
J K L M N O P Q R
S T U V W X Y Z

search Go

Forward
Introduction
Normative References
Using the T1 Telecom Glossary
Annex A: Informative References

ITS Development Site

<< Back

derived unique key per transaction (DUKPT)
In cryptography, a key-management technique that uses a unique key for each separate transaction to prevent the disclosure of any past key used by the transaction-originating tamper-resistant security mode (TRSM). *Note:* The unique transaction keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction. [After X9.24]

These definitions were prepared by ATIS Committee PRQC

For more information on the work related to these definitions,
please visit the ATIS website and the ATIS Document Center