RFC6979 - Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)

return to the IETF Standards

Table 1: Data sheet for Transmission Control Protocol (TCP)

Title	Transmission Control Protocol
Acronym	ECDSA
Version	2013
Document Number	RFC6979
Release Date	August 2013
Reference	https://tools.ietf.org/html/rfc6979

Note: The following is an excerpt from the official IETF RFC. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Abstract

This document defines a deterministic digital signature generation procedure. Such signatures are compatible with standard Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures and can be processed with unmodified verifiers, which need not be aware of the procedure described therein. Deterministic signatures retain the cryptographic security features associated with digital signatures but can be more easily implemented in various environments, since they do not need access to a source of high-quality randomness.