Entrust Technologies White Paper

Standards Supported by Entrust®

Author: Dr. Paul Van Oorschot

Date: December 1996
Version: 2.0

Motivation for use of Standards in Entrust

Entrust Technologies is committed to the use of open standards throughout the Entrust® product family. This facilitates interworking of Entrust products with other vendors' products and simplifies the incorporation of Entrust into the existing networks of customer organizations. The goal of Entrust is to provide the world's best Public Key Infrastructure (PKI), and to maximize interoperability between PKIs. In order to achieve this, Entrust will continue to evolve and support open security standards as they emerge. Specific standards implemented in the Entrust product line are listed in this document.

Entrust: Standard Cryptographic Algorithms and Techniques

Encryption

- DES (U.S. Data Encryption Standard) in accordance with U.S. FIPS PUB 46-2 and ANSI X3.92.
- CAST block cipher (from Entrust Technologies, see white paper on http://www.entrust.com/).
- DES and CAST encryption using CBC mode of operation in accordance with U.S. FIPS PUB 81, ANSI X3.106 and ISO/IEC 10116.

Digital signatures

- RSA digital signature in accordance with RSA Data Security Inc. Public Key Cryptographic Standards (PKCS) specification PKCS#1.
- DSA in accordance with the Digital Signature Standard, U.S. FIPS PUB 186 and ANSI X9.30 (Part 1)

Hash functions

- SHA-1 in accordance to U.S. FIPS PUB 180-1 and ANSI X9.30 (Part 2).
- MD5 Message-Digest algorithm in accordance with Internet RFC 1321.
- MD2 Message-Digest algorithm in accordance with Internet RFC 1319.

Key management

- RSA key transfer in accordance with RFC 1421 and 1423 (PEM), and PKCS#1.
- (EntrustSession Toolkit) Diffie-Hellman key agreement in accordance with PKCS#3.

Integrity by symmetric techniques

- Message Authentication Code (MAC) in accordance with U.S. FIPS PUB 113, ANSI X9.9, and X9.19.

Pseudo-random number generation

- As per ANSI X9.17 Appendix C

Entrust: Standard Data Formats and Protocols

Certificate formats

- Certificates specified by ITU-T Rec. X.509 (1993), including X.509 version 3 (v3) certificates and CRL extensions per Amendment 1 and Technical Corrigendum 1. (Common standard, amendments and corrigendum with ISO/IEC 9594-8 (1994).)
- Support for X.509 version 1 (v1) certificates per Internet RFC 1422 (PEM).
- RSA algorithm identifiers and public key formats in accordance with Internet RFC 1422 and 1423 (PEM), and PKCS#1.
- (Entrust/WebCA™) generation of certificates suitable for use in SSL.

File envelope format

- Standard file envelope format based on Internet RFC 1421 (PEM).
- PKCS#7 and S/MIME supported by Entrust toolkits currently in beta testing.
- PKCS#10 certificate requests supported by Entrust toolkits currently in beta testing.

Directory protocols

- LDAP (Lightweight Directory Access Protocol) in accordance with RFC 1777.
- (Entrust/Server™, optional) support for Directory Access Protocol (DAP) in accordance with ITU-T X.500 (1993) Series of Recommendations. (Common standard with ISO/IEC 9594 multipart standard.)
- (Entrust/X.500 Directory™, optional) support for Directory Access Protocol (DAP) and Directory System Protocol (DSP) in accordance with ITU-T X.500 (1993) and ISO/IEC 9594.

Key storage

- private key storage based on PKCS#5 and PKCS#8.

Client management protocol

- Entrust Technologies' Secure Exchange Protocol (SEP), built using Generic Upper Layers Security (GULS) standards ITU-T Recs. X.830, X.831, X.832 and ISO/IEC 11586-1, 11586-2, 11586-3.

Entrust: Software and Application Program Interfaces (APIs)

- On-line mode high-level security API in accordance with Internet Generic Security Services API (GSS-API) per RFCs 1508 and 1509.
- On-line GSS-API public-key implementation mechanism using Simple Public Key Mechanism (SPKM) per Internet RFC 2025, and SPKM entity authentication as given in FIPS 196.
- Store-and-forward high-level security API based on Independent Data Unit Protection GSS-API (IDUP-GSS-API) Internet Draft, draft-ietf-cat-idup-gss-05.txt.
- PKCS#11 (CRYPTOKI) hardware cryptographic interface supporting hardware tokens from any vendor, to allow FIPS 140-1 Level 2 and higher security.

Government Endorsement

- Cryptographic module validation under U.S. FIPS PUB 140-1: cryptographic software module validated to Level 1.
- Canadian Government Cryptographic Endorsement and Assessment Program (CEAP) evaluation in progress.

Entrust Technologies' Role in Standards Development

Entrust Technologies participates directly in standards activities/forums including:

- OpenGroup (formerly OSF and X/Open)
- ISO/IEC JTC1/SC21/WG4 and ITU-T SG7 Directory
- ISO/IEC JTC1/SC27/WG2 Information Technology Security Techniques
- ANSI X9F1 Cryptographic Techniques for the Financial Services Industry
- IEEE P1363
- NIST CRADA group MISPC (Minimum Interoperability Spec for PKI Components)
- PKCS#11 Technical Working Group
- U.K. Ministry of Defense Technology Demonstrator Program
- Electronic Messaging Association (EMA)
- CommerceNet
- Internet Engineering Task Force (IETF) working groups including: PKIX group (Public-Key Infrastructure, X.509-based), CAT group (Common Authentication Technologies), S/MIME group, ASID group, and others.

Recognizing that many aspects of network security are not currently standardized, Entrust Technologies is working actively in many forums to ensure that Entrust and emerging standards align, such as progressing the Entrust Technologies CMS-API within the OpenGroup's Certificate Management API (CM-API) project. Entrust Technologies is committed to following industry standards when they achieve maturity, including IETF's PKIX, NIST's MISPC, Microsoft's CryptoAPI, and others.