Return to Security home page

Current work:

- Managers Guides
- MGIS
- Data Privacy
- PKI
- Guide to PKI
- Identity Mgt
- Access Control
- Security Patterns
- Secure Messaging

Strategy/Roadmap

Useful links:

Security topics

Info sources

Liaisons

How we work

Open Group Security Standards/Guides

CDSA

The ***Common Data Security Architecture (CDSA)*** is a set of layered security services and cryptographic framework that provide an infrastructure for creating cross-platform, interoperable, security-enabled applications for client-server environments. CDSA covers all the essential components of security capability, to equip applications for electronic commerce and other business applications with security services that provide facilities for cryptography, certificate management, trust policy management, and key recovery.

CDSAv2 is scalable such that it can provide security services for any device, ranging from Personal Digital Assistants (PDAs) to Mainframes, and any operating platform from Windows to UNIX / LINUX. Incorporating the CDSA solution into enterprise environments effectively decouples any single security solution from the infrastructure, and integrates a mechanism (EMM) that allows you to plug and unplug security solutions as required.

A CDSA Explained Guide provides an introduction to the security issues addessed by CDSA and a high-level description of the main components in the CDSA architecture, how they interrelate, and how the CDSA provides interfaces to service provider modules and to applications software.

Download the CDSA Version 2 Technical Standard, May 2000 - FREE!

CDSA is available from Sourceforge as open source. Sourceforge supports this CDSA open source with 5 email lists on the open source home page, set up to handle support-related queries.

The Open Group currently does not have an active working group on support for CDSA. Having now published the CDSA Standard, and also the associated Human Recognition Service (HRS) Standard, and worked with Intel to support their making CDSA available as open source from Sourceforge, our activities are limited to responding to market stimulus and email queries.

Further Information

The Intel CDSA site at http://www.intel.com/ial/security/ provides comprehensive information on support for CDSA. It organizes this information under the following categories:

- Download - CDSA open source from the Sourceforge site.
- Press - key articles and other press coverage.
- Documentation - supporting white papers, presentations, tutorials, and technical publications.
- FAQs - answers to ferquently asked questions.
- Technical Information - a very brief technical overview of the functionality and infrastructure that CDSA provides.
- Adopters - deployment of CDSA in products, and from which vendors.
- Specifications - Intel's references to The Open Group's CDSA Standard and HRS Standard, plus the Intel Simple PKI (SPKI) certificate documentation, which consists of two RFCs:
  - RFC2692: Requirements giving the requirements gathered by the working group at the start of the process.
  - RFC2693: Theory giving the theory of authorization certificates, as opposed to name or ID certificates that most people (e.g., X.509) discuss. This document points out some of the flawed assumptions in ID certificate theory and shows how SPKI's certificates (both authorization and ID) attempt to correct those flaws.

Brief Overview of CDSA Standard

CDSA defines a horizontal, four-layer architecture:

1. Applications
2. Layered services and middleware
3. Common Security Services Manager (CSSM) infrastructure
4. Security Service Provider Modules

The CDSAv2.3 Technical Standard is organized into 15 parts, each addressing specific aspects of the architecture, and catering for the needs Application Developers, CSSM Infrastructure Providers, and Security Service Module Providers

The Parts are:

1. The CDSA architecture
2. Common Security Services Manager (CSSM) APIs for core services
3. Cryptographic Service Providers (CSP)
4. Trust Policy Services (TP)
5. Authorization Computation Services (AC)
6. Certificate Library Services (CL)

7. Data Storage Library Services (DL)
8. Module Directory Service (MDS)
9. Key Recovery Services (KR)
10. Embedded Integrity Services Library (EISL)
11. Signed Manifest
12. Object Identifiers for Certficate Library Modules
13. Elective Module Manager (EMM)
14. Add-in Module Structure and Administration
15. Appendices, Glossary, and Index

© The Open Group 1995-2020