



Intel's Common Data Security Architecture

**George Cox
Intel Corporation**

Why A

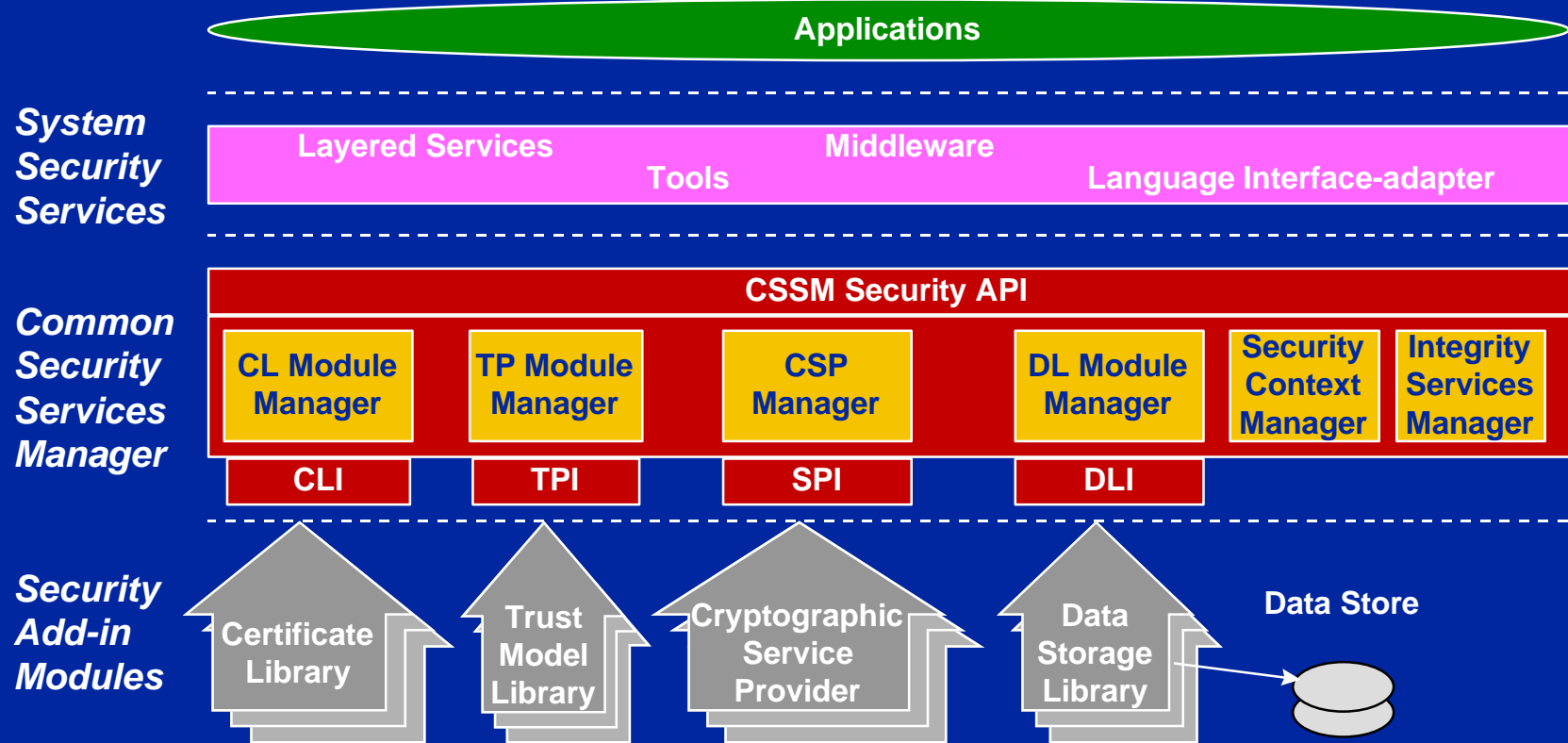
Common Data Security Architecture?

- In early 1995, we recognized the need/opportunity for an open, interoperable, cross platform, security infrastructure
- Our idea was to provide PCs a basic infrastructure so that the primary ingredients of any security solution are “just there”
 - interface specs designed to remove interoperability hurdles
 - lower TTM hurdles for incorporating security features into legacy and new products
 - openly reviewed to ensure robustness
- We published
 - an early version of the specifications at the 1996 RSA Conference
 - and evolutionary versions of the specifications on the Intel Web site (<http://www.intel.com/ial/security/>) for review/comment
- Intel has developed this functionality for use in its own products (e.g., LANDesk Management)

CDSA Design Goals

- Create an open, cross platform, interoperable, core security infrastructure
- Support use and management of the fundamental elements of security:
 - certificates
 - trust
 - cryptography
 - integrity
- Support multiple programming environments (e.g., C and JAVA)
- Make extensible above and below
- Build outside any Operating System

Common Data Security Architecture

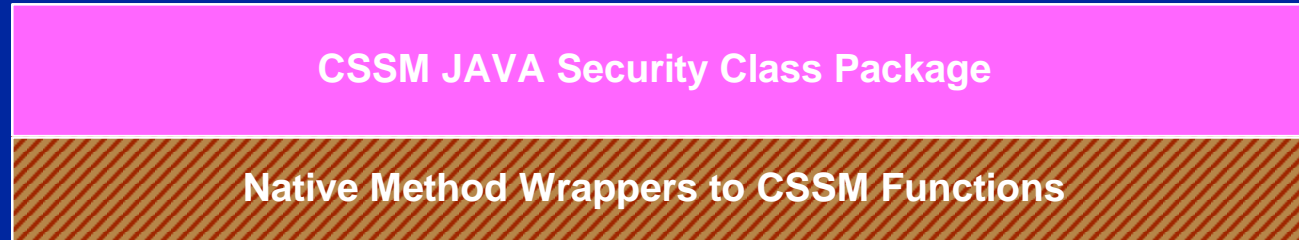


JAVA Support

Applications



Java to CSSM Wrapper



CSSM Security Services



  Implemented in JAVA

   Implemented in C