Common Data Security Architecture

David Aucsmith

Security Architect

Intel Corporation

Agenda

- Overview
- System Security Services
- Common Data Security Services
- Crypto Service Providers
- Reference Applications

Common Data Security Architecture

- A set of layered security services that address common communications and data security problems in the emerging PC business space
- Each layer is defined by a set of services and an API
- Not just a crypto API
  - Provides management framework for tokens and digital certificates
  - Provides tight integration of individual services while allowing those services to be provided by interoperable modules
- Key component is the Common Security Services Manager

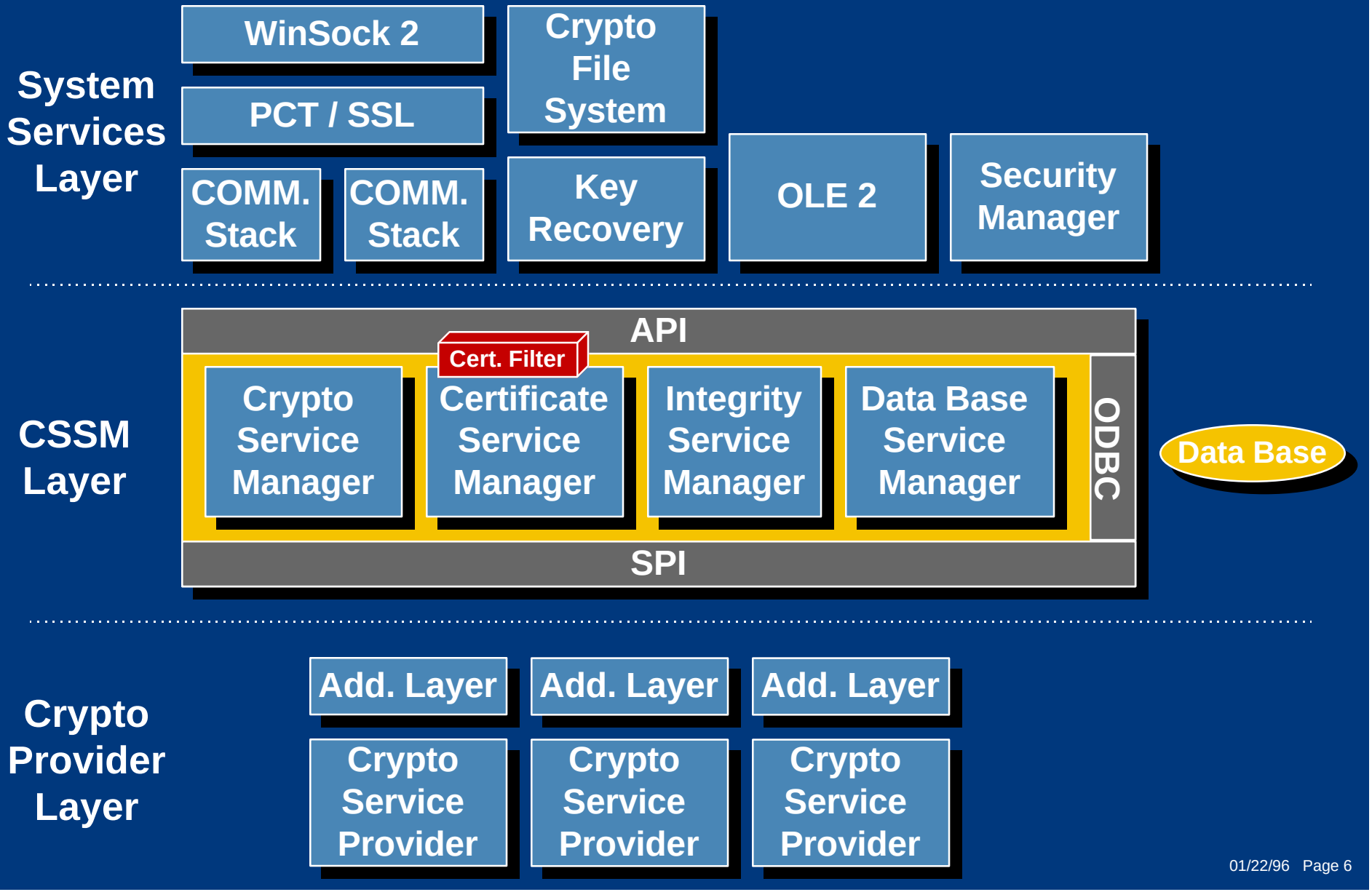
Objectives

- Remove security / safety as a barrier to new businesses using the PC
- Encourage open interoperable horizontal interfaces
- Provide key components of security capability to industry

Two Fundamental Premises

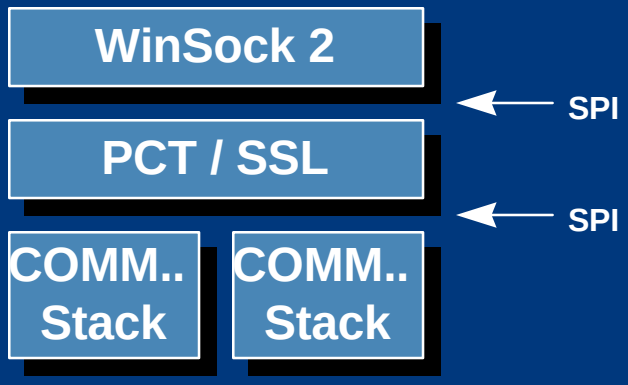
- Portable digital tokens will be used as a person's "digital persona" for commerce and communications
  - Many form factors (smart cards, PCMCIA cards, floppy disks)
  - Hardware or software (depending on the application)
  - "Crypto Service Provider," "Digital wallet" and "Encryption Module"
- Digital Certificates will be used to represent trust
  - There are no alternative (X.509 V3, endorsed by many different parties)
  - Electronic equivalents of current trust models

Common Data Security Architecture



System Services Layer

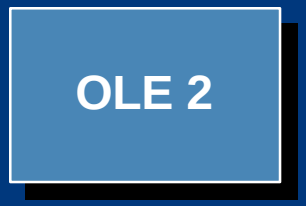
- **Secure WinSock 2**
  - Layered Service Provider
    - » Registers services with IOCTLs
    - » SPI on top and bottom
    - » Supports both PCT and SSL
  - Supports multiple comm. stacks (TCP/IP, SPX/IPX)



- **Cryptographic File System**
  - Uses Windows Installable File System (IFS) hooks
  - Transparent block encryption and decryption
  - File specific symmetric key encrypted by public-key of session certificate
  - Key recovery module

System Services Layer

- OLE 2 Security Client \ Server
  - Provides “drag and drop” interface to all of the CSSM services
    - » e.g., drag a facsimile of a signature onto a document to sign it
  - Uses CSSM default parameters
- Security Manager
  - GUI user interface to CSSM
  - Set default parameters
  - Query CSSM state and settings



Common Security Services Manager Layer

- Crypto Services Manager
  - Manages crypto interface
    - Low-level interface for fine control
    - High-level interface for ease of use (uses defaults)
    - Manages *crypto session*
  - Manages Crypto Service Providers
    - CSPs register with CSSM
      - ID, level of trust, and capabilities
      - Capabilities passed as *Identification Structures*
    - Handles reentrancy

Common Security Services Manager Layer

- Certificate Services Manager
  - Certificates stored in canonical format
    - » X.509 V1 information as record, V3 extensions as blobs
  - APIs revectored to certificate filters that have functions to:
    - » Import, export, create, display, and verify
  - Complete certificate chain stored
  - Root certificate includes information on on-line verification
  - Certificates include rich media (e.g., .bmp and .wav)
- Any CSSM can be a Certificate Authority
  - Hierarchical or introducer trust models
  - Revocation lists can be cached in optimized Bloom-vector
- Manages certificate sessions
  - Maps certificate public-key to CSP private-key

Common Security Services Manager Layer

- Integrity Services Manager
  - Audit
    - All security relevant events are auditable
    - Union of user and application audit masks
    - Audit record recorded in either data base of OS audit log
  - Integrity Verification Kernel
    - Verifies digital signature of executable images (on disk or in memory)
    - Verifies correct execution of other Integrity Verification Kernels
    - Distributed trust model
    - Kernels are tamper resistant
      - Self-modifying, encrypted modules
      - All parameters passed as challenge/response

Common Security Services Manager Layer

- **Data Base Services**
  - **ODBC interface to data base**
  - **Digitally signs and verifies all records as written and read**

Crypto Provider Layer

- **Adaptation Layer**
  - **Maps SPI to common token interfaces**
    - » **PKCS #11, Forteza, …**
    - » **Performs registration for CSPs that do not have ability**
    - » **Performs other CSP functions for non-fully compliant CSPs (e.g., key index)**
    - » **Can be combined with driver for hardware CSP**

Crypto Provider Layer

- Crypto Service Provider
  - Hardware or software
  - All crypto functions
    - » Bulk cipher, Key exchange, Signature, Cryptographic hash,
  - Secure storage
    - » One or more symmetric or asymmetric keys
    - » Hash of public-key stored with private-key as index
  - Identification
    - » Type, manufacturer, and trust level
  - Other functions
    - » Random number generation

Reference Applications

- System Security Applets
  - Secure WinSock 2.0
  - Cryptographic File System
  - OLE 2 Server / Client
  - Security Control Panel
- Vertical reference applications to demonstrate architecture and implementation
  - Such as a certificate-based PGP

Status

- Experimental implementation exists
  - Fully functioning
  - Default software CSP with most capabilities
  - Documentation
  - Reference applications
- Planning underway for evolution and diffusion
  - For further information visit our Web site on:

    http://www.intel.com