

HSPD-12 & SafeNet



THE FOUNDATION OF INFORMATION SECURITY

© 2004 SafeNet, Inc. All rights reserved.

About SafeNet

- 20+ years of focus on the information security space
 - Highly profitable, well-managed
 - Most profitable EPS, pure play information security company (EPS CAGR: 251%)
 - Fastest Growing Networking Company *NetWork World 2005*
 - Global operations, sales, and support capability
 - Offices in 25 countries
 - Sales and distribution in over 100 countries
- #1 Provider of high assurance T1 & satellite link encryption (*75% market share*)
 - #1 Provider worldwide of external Frame Relay, ATM & Link encryptors
 - #1 Provider worldwide provider of USB Tokens (*IDC*)
 - 66% of the market for secure Web acceleration (*IDC*)
 - 84% of the PKI Root Key market (*Salomon Smith Barney*)



Smart ID Card Experience

Complete FIPS 201 Solution

- Card Management System
- Middleware
- Smart card
- PKI Root key protection/secure key generation

US State Department

- Match-on-card finger biometric
- GSC-IS compliant middleware, Entrust certified

FDIC

US Treasury FMS

Canadian DND

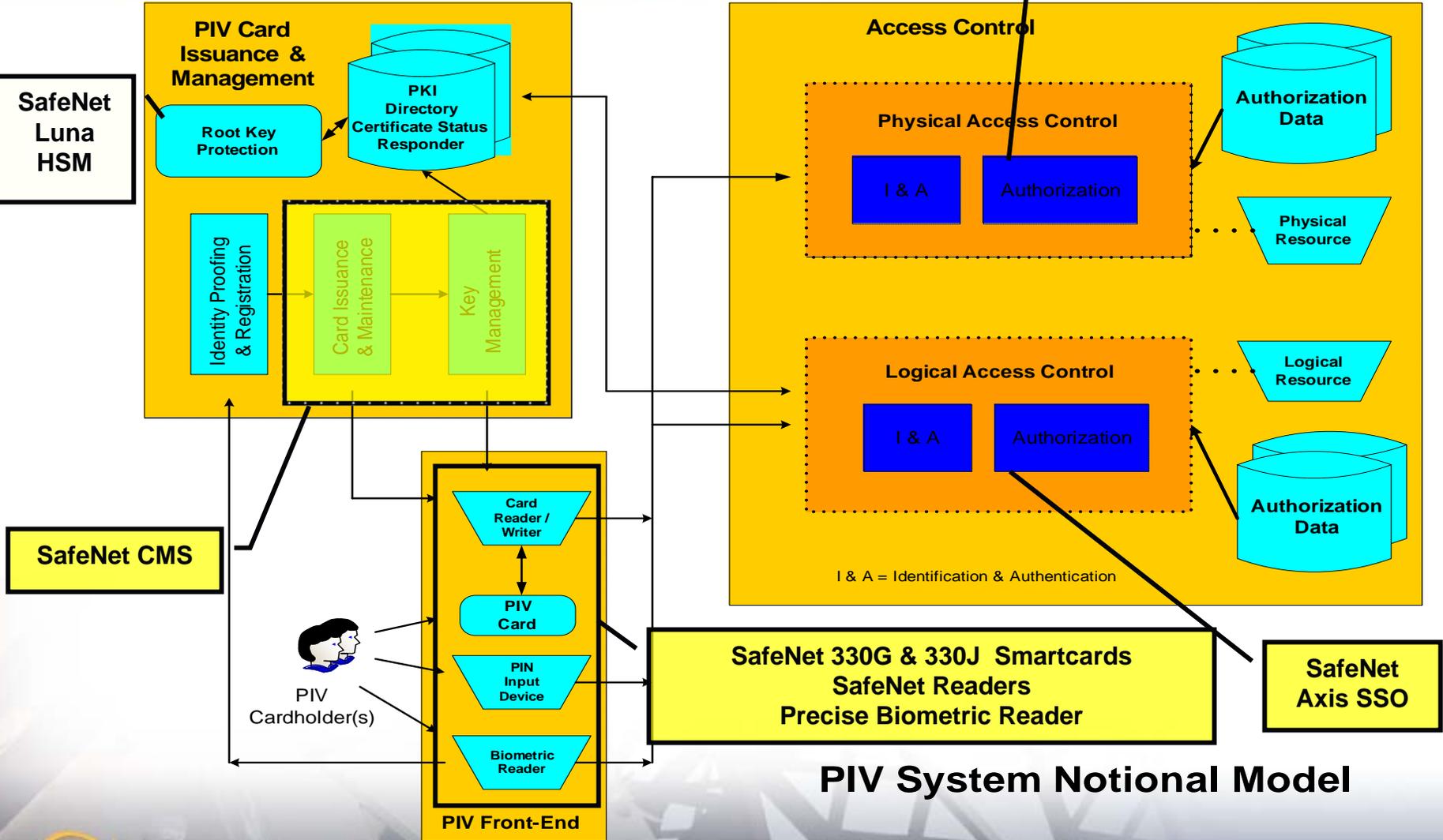
- 90,000 card deployment

Large US Financial Services Organization

- Remote access authentication
- Customer financial transaction signatures

Personal Identity Verification (PIV) Architecture Components (with SafeNet Products)

SafeNet Smartcards With Second Chip added



PIV System Notional Model

SafeNet's Luna Line of HSMs

Embedded HSMs



PCMCIA HSM token

- FIPS 140-1 Level 2
- Secure digital signing



Replacement PCMCIA

- FIPS 140-1 Level 2
- Secure authentication
- Digital signing



Embedded PCI HSM

- FIPS Level 3 & CC EAL4+
- Asymmetric and Symmetric encryption
- High performance

Appliances & Systems



Network HSM Server

- FIPS 140-2 Level 3
- Network shareable
- Multi-application partitions



PKI root key management

- FIPS 140-1 Level 3
- Common Criteria EAL4+



Application Security Module

- FIPS 140-2 Level 3
- Provides secure Java (J2SE) programmable appliance
- Supports XML & web services

SafeNet Card Management System (CMS)

Web Based

- Easy to use interface
- Support for centralized, distributed, or Hybrid issuance methods

Directory Support

Work Flow Centric

- Central control of security policies and business rules
- Full Lifecycle management of digital credentials and cards
- Role and Group based access

PKI Oriented

- Multiple CAs support simultaneously
- Uses CA policies
- Multiple Keys and Certificates supported

Physical Access integrated

- Support for ISO 14443-A – MiFARE Standard today

Tracking and reporting on card and certificate status

Full auditing of administrator actions

Support for multiple smart cards

Applet deployment and management

PIV 2 compliance upgrade available in Q4 2005



SafeNet Smartcards

- PIV 1 compliant now
- Match-on-card finger biometrics (FIPS certified)
- Java and file system options
- Cryptographic API
 - PKCS#11, MS CAPI, ISO-7816, PC/SC
 - FIPS 140-1 level 2 certification
 - GSC-IS v2.1 Compliant
- Cryptographic Functions
 - Symmetric Key Generation – on Token
 - RSA – RC2, RC4, DES, 3DES up to 2048 bits
 - Asymmetric Key Generation – on Token
 - RSA – up to 2048 bits
 - DSA – up to 1024 bits
 - AES – available in Oct. '05
 - Hash Digest Functions
 - SHA-1, MD5
- PIV 2 compliant card available in October 2005
- Card and USB token (iKey) options



SafeNet's Axis

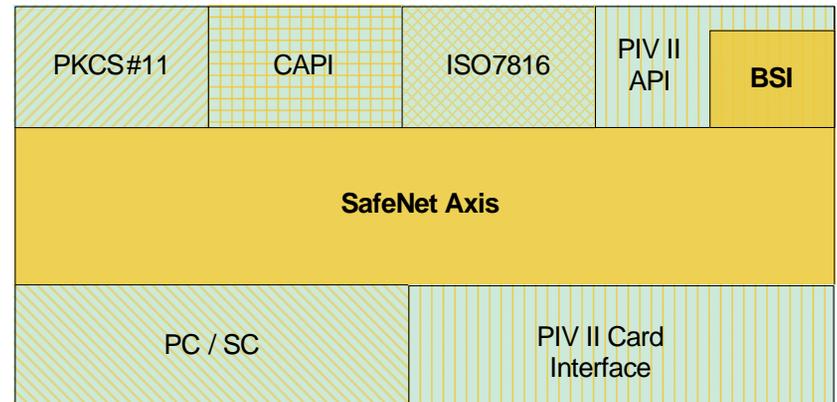
Axis Middleware manages readers, tokens and applications

Central administrator controlled configuration

Rapid deployment and update via .msi distribution

Small footprint

Broad worldwide deployments



SafeNet Benefits

Single source for integrated FIPS 201 compliant solution

Strong reputation for delivery performance

US Government security expertise

Established smart ID card expertise

Flexible deployment and implementation options

Interoperable with broad range of complementary technologies

Questions?

John Barrett (410) 626-8695

Chuck Screen (703) 647-8414