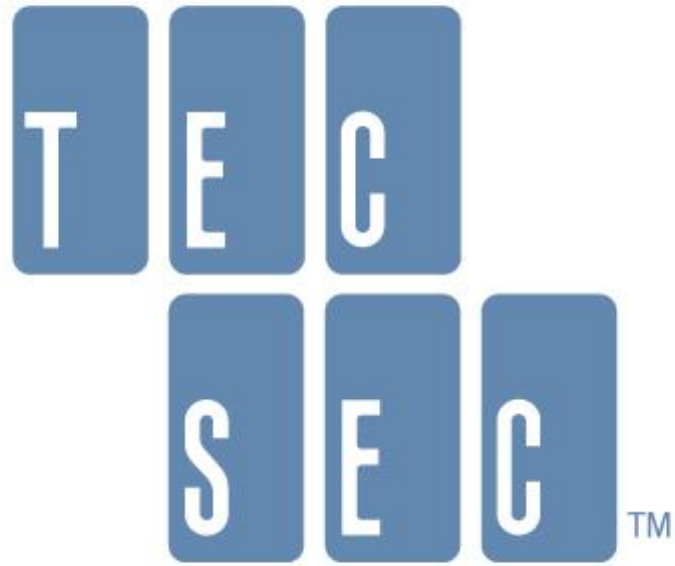


ADVANCED INFORMATION SECURITY & PRIVACY

Presentation to HHS on HCFA Adoption & Use of CKM®

www.tecsec.com

The Need

New Privacy Laws of Great Consequence

- Health Insurance Portability and Accountability Act of 1996
  - Law was “finished” on 12/28/00 with Presidential approval of Privacy Rules
  - Rules ratified 4/14/01 by President Bush, despite strong lobbying efforts; Compliance mandatory 4/03
  - Sweeping changes, including civil and criminal penalties for non-compliance
  - Being treated like Y2K in the medical community

- Gramm Leach Bliley Act of 1999
  - Outlines future structure of financial community, how it will be regulated and supervised, and promulgates customer privacy and protection
  - Compliance Mandatory 7/01
  - Sweeping implications to financial and non-financial institutions
  - Provisions allow for customers to Opt-Out, preventing the sharing of personal financial information with third parties

In the Greater Healthcare Ecosystem…

"How does one protect selective electronic information that has been released without having a chance of knowing who may see it or come into possession of it downstream?"

For example…

1. Healthcare payment claims
2. Healthcare claims attachments
3. Enrollment and disenrollment in a health plan
4. Eligibility for a health plan
5. Healthcare payment and remittance advice
6. Health plan premium payments
7. Reports of injury/disability
8. Healthcare claim status
9. Referral certification and authorization
10. etc.

Fiducial Responsibility and Liability

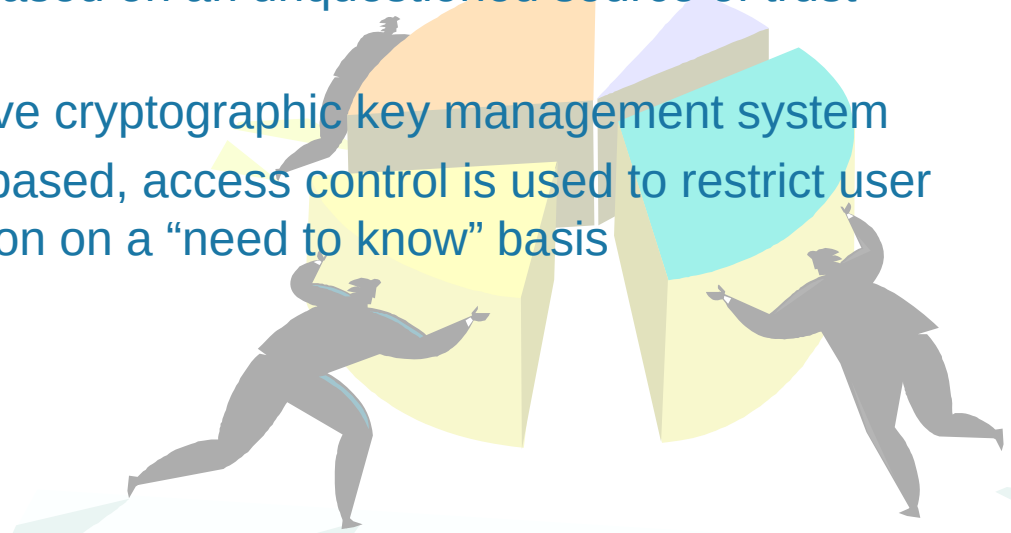
Reasonable man standard:

"The standard which one must observe to avoid liability for negligence is the standard of the reasonable man under all the circumstances, including the foreseeability of harm to one, such as the plaintiff."

Black's Law Dictionary, 5th Edition, page 1138.

National Research Council Recommendations *

- *In its book, "For the Record," the National Research Council delineates the Key Components of a System that provides Data Privacy, Confidentiality and Security*
  - ✓ Smart, token-based cryptographic authentication and authorization systems
  - ✓ Information access based on rules and roles
  - ✓ Digital signatures based on an unquestioned source of trust and legal liability
  - ✓ Trusted and effective cryptographic key management system
  - ✓ Fine-grained, role-based, access control is used to restrict user access to information on a "need to know" basis



**** Source: For the Record, Protecting Electronic Healthcare Information, Computer Science and Telecommunications Board, National Research Council, 1997.***

The Solution

- ✓ Protect the data and information in transit & at rest
- ✓ Control who has access to what using Role Based Access Control (RBAC) & Granular Encryption
- ✓ Provide physical & logical access control through Smart Tokens and Cryptography
- ✓ Integrate the solution into existing business systems and processes

What is Constructive Key Management® (CKM®)?

- CKM is a technology and methodology used to securely transfer, store and access information
  - Access privileges to information based upon an individual's role
  - Access privileges are assigned at the object level
  - Information security access adjudication moved away from a central, on-line server to a user's Smart Token
- TecSec uses CKM in its Privity™ product line
  - End-to-End Solutions (Custom and Turn-key)
  - Component technology
  - Integration Tools and API for existing processes and systems

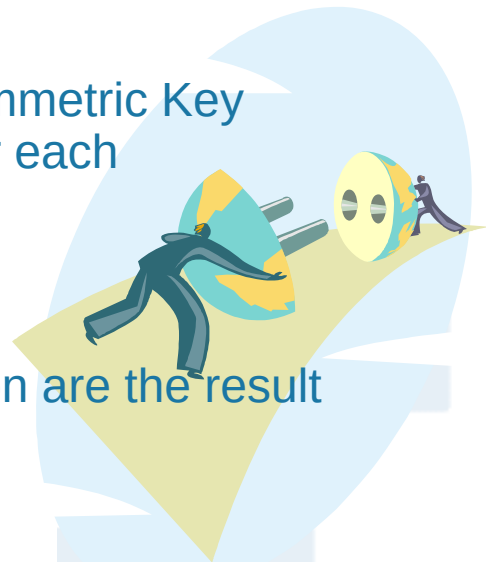
CKM Features

- Integrated enterprise information security & information management software with four major features:
  - Cryptographically Enforced Access* Management (CEAM™)
  - Object Management and Data Separation
  - Built-In Key Recovery
  - Scalability
- Award winning 5th generation security technology
- Deployment – Separate or integrated
- Architecture – Permits use and encryption/decryption while disconnected from network/intranet/Internet
  - Central Key Management, centralized/decentralized user credentialing, tokens can provide additional revocation (e.g., sunrise/sunset) and access control features while disconnected
- Operating system agnostic, standards-based, patented
- While CKM builds upon and enhances PKI infrastructure, it may be deployed without it

* Note: Access = role based, rule based, policy based, vendor-based, etc.

CKM & PKI

- CKM extends the capabilities of Public Key Infrastructure
  - PKI is an excellent technology for digital signature and I&A
  - PKI as an encryption method presents architects and implementers significant scalability and access management problems
- Cryptographic Key Management
  - Symmetric
  - Asymmetric
  - Constructive
- CKM combines the benefits of Symmetric and Asymmetric Key Management while offering significant benefits over each
  - Inherent key recovery (Asymmetric)
  - Role Based Access Control
  - Scalability
- Patented data separation and object level encryption are the result



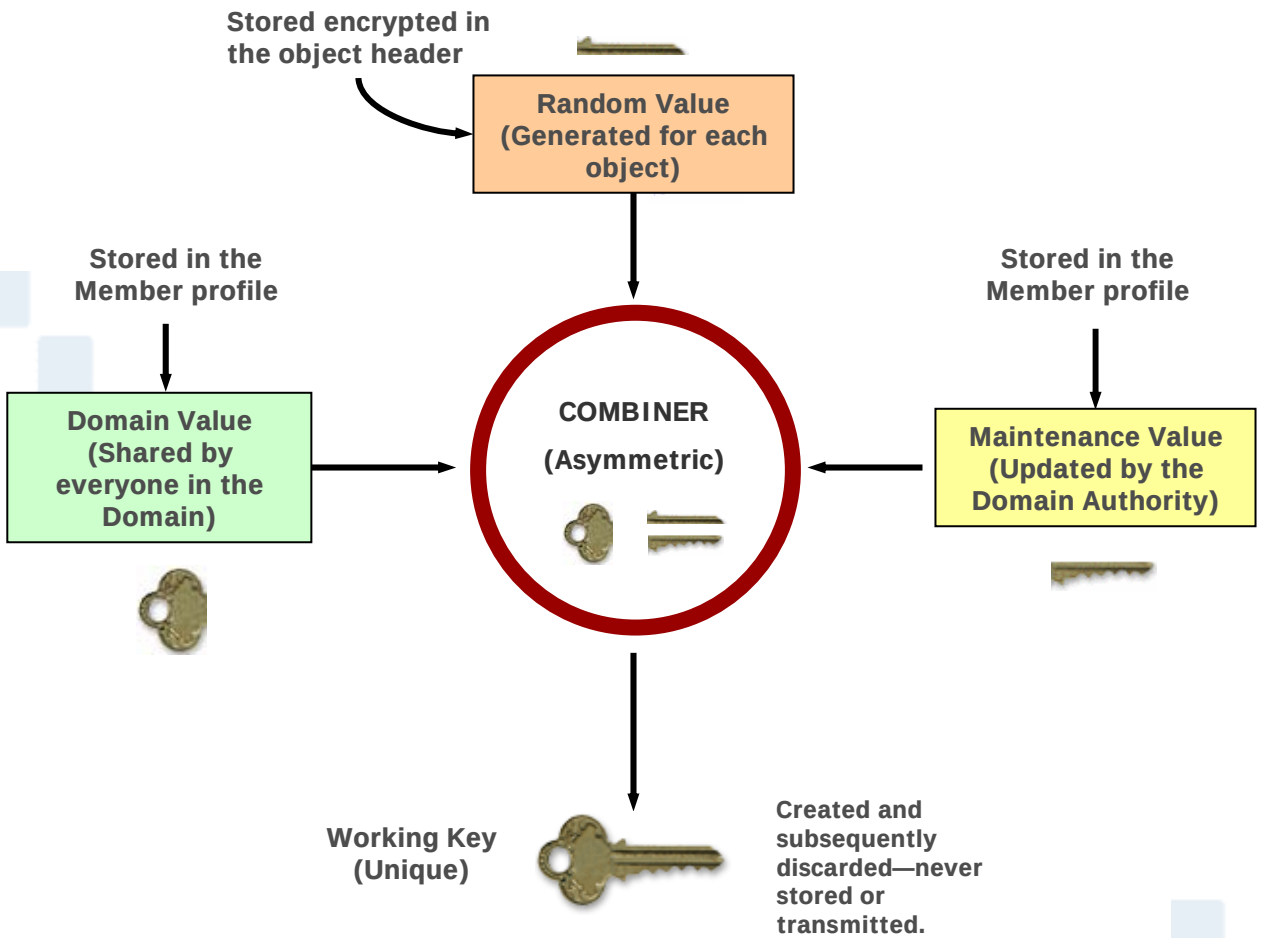
CKM Enhances PKI

Public Key Infrastructure	Constructive Key Management
➔Developed in 1960's – point-to-point technology – ID & authentication	➔Developed in 1990's – access control to information in a distributed environment
➔Limited scalability	➔Vast scalability
➔Key recovery not assured - typically via escrow	➔Key recovery – Key & data recovery solely by system owner
➔Central server enrollment	➔Distributed enrollment
➔Not designed for role-based or object-level granularity	➔Inherent Role-based & object-level granularity

STANDARDS BASED TECHNOLOGY

Standard	Description
ANSI X9.30-2, X.942; FIPS 180-1, 186-2	Public Key Functions
ANSI X9.31	Digital Signature Authentication
ANSI X9.52, X9.65; FIPS 46-3,81	3XDES
ANSI X9.69	Framework for key management extensions
ANSI X9.73	Cryptographic message syntax
ANSI X9.84	Biometric Identification/Authentication
ISO 7816	Smart Card Specification
PKCS#11	Cryptographic Token Interface Standard (Cryptoki)
FIPS 140-1	Security requirements for cryptographic modules

CKM's ANSI X9.69 Combiner



HCFA's Adoption and Involvement

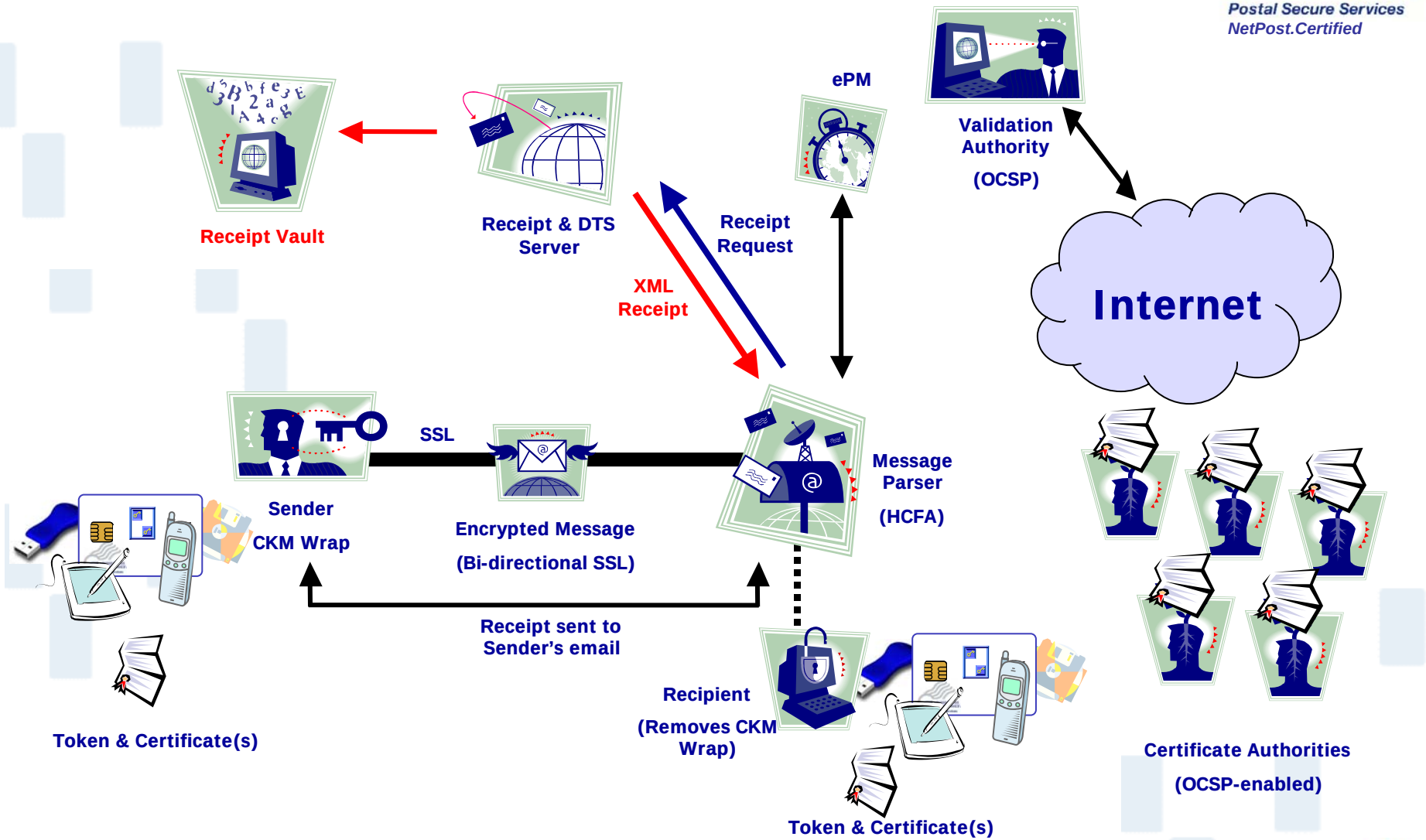
- The HCFA adopted solution:
  - USPS as the foundation of trust via the smart card and in-person identity proofing (required by HHS Document HHS-IRM-2000-0011, dated 1/8/01)
  - Internal Certificate Authority, hosted at HCFA
  - "Granular" confidentiality/privacy layer provided by CKM
  - The use of Postal PK to start the process and the use of the CKM credentials under HCFA control to evoke roles and rules
- Key Players:
  - CIO (Dr. Gary Christoph)
  - Director, IT Architecture Staff (Ms. Susan McConnell)
  - Senior Security Advisor (Ms. Victoria Quigley)
  - Director, Division of HCFA Enterprise Standards (Ms. Julie Boughn)
  - System Security Group/OIS (Mr. Don Bartley)
- CKM soon expected to be ratified as HCFA's Emerging Technology (Electronic Signatures) by the IT Security Architecture Working Group

NetPost.Certified™ / PrivityPlus™

HCFA Health Care Financing Administration

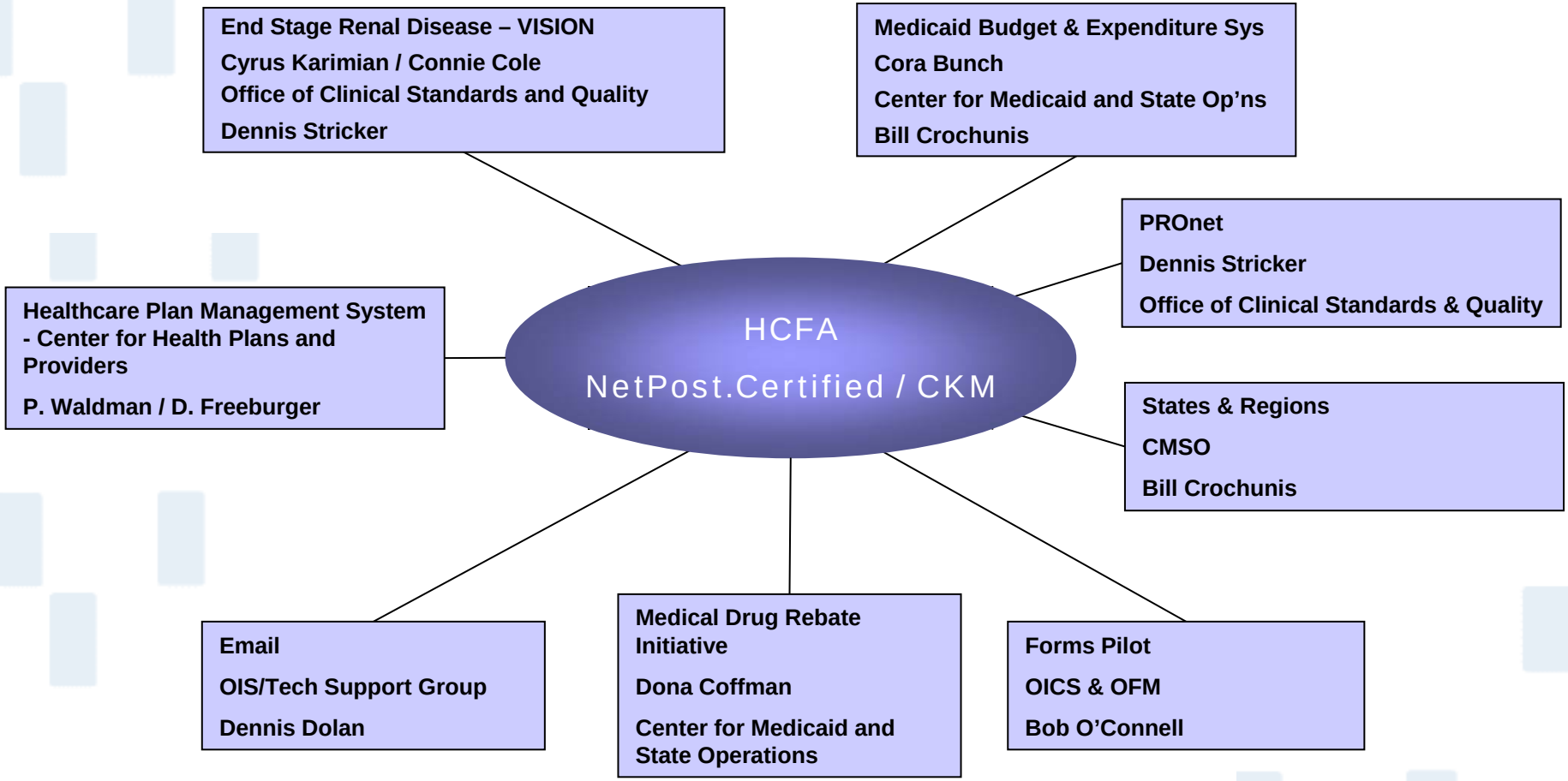
UNITED STATES POSTAL SERVICE

Postal Secure Services
NetPost.Certified



CKM TECSEC

HFCA Pilot Groups



Peer Review Organization Network (PROnet)

"Providing e-business to the PRO community and their customers to promote sharing of information/ideas, quality improvement tools, data exchange, provider data inquires, and data collection in a secured environment"

PROnet Design

- Secured at the network, hardware, and data access levels
- Use the TecSec “HCFA approved” encrypted data transfer and login methodologies for access through the Internet or AGNS dial-up
- Build upon the proven Minimum Data Set (MDS)/Outcome Assessment Information Set (OASIS) collection and reporting system model used by the 30,000 long term care and Home Health Agencies in each of the 50 states, VI, DC, and PR
- Delegated authority of login and passwords administration to PRO’s for access to PROnet from the PRO and their provider community
- Management tools for PRO’s to administer home page, PRO links, data inquiry reports, data exchange directories, provider profiles, quality improvement tools, PRO quality improvement marketing (e.g. newsletters, calendars, events information)
- Integrated PROvantage functionality (e.g. automatically push provider record request lists to PROnet provider directories)

PROnet Provider Inquiries

- Reporting system that provides for a queuing system, query with parameters, view online, submit and come back later to retrieve and download

- Reports and queries for providers to inquire and report on record status (1st and 2nd request), technical denials, adjustments, case review results, and trends of case review and record tracking overtime

Related Initiatives

- State of North Dakota/SSA/USPS
- SSA & HHS Interface
- Boeing Aircraft Company
- DoD/Intel
- International Data Poste

Background Product Charts

Privity™ & CKM® Product Overview

Privity™ - priv´-i-tē:

1. *n.* Knowledge of something private or secret shared among individuals, especially with the implication of approval or consent.
2. *Law.* A successive or mutual interest in or relationship to the same information or property.

Product Groups

Core Technology

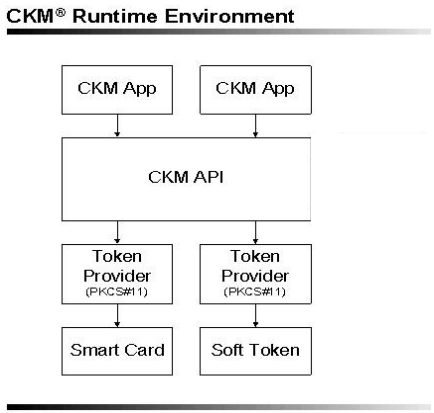
SmartTokens™

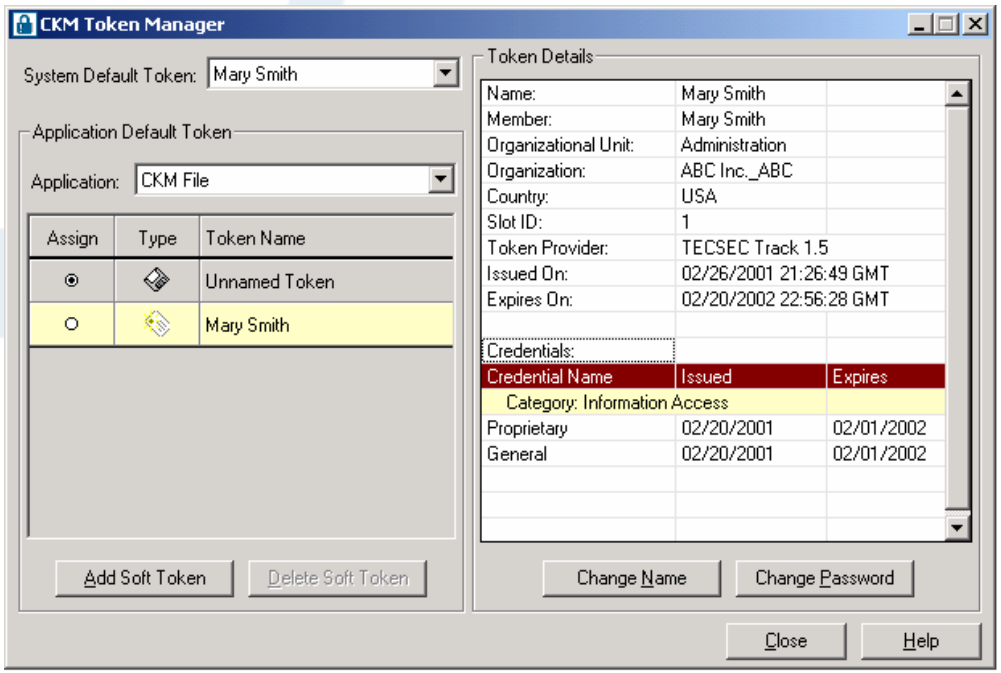
Administration Tools

Desktop Products

Core Technology

- **CKM Runtime Environment (RTE)**





- **CKM Token Manager**

Core Technology, cont'd

- CKM SDK Version 1.02
  - The CKM Software Developer's Kit (CKM SDK)
    - Designed to simplify the process of integrating CKM technology into custom and third party applications
  - The product consists of a number of components
    - Some are part of the CKM RTE
    - Others are exclusive to the SDK
  - CKM API provides programmatic interface to the RTE

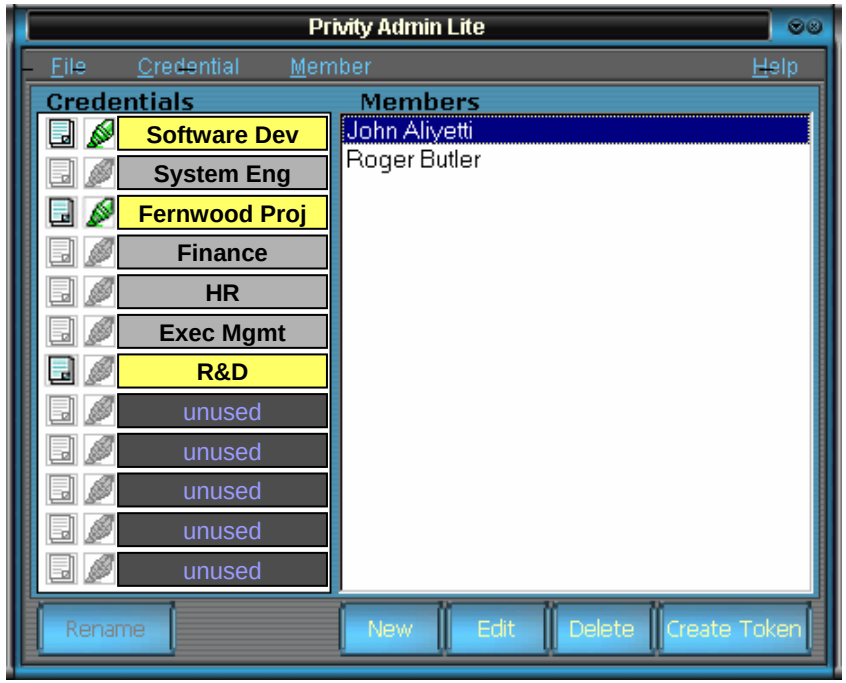
SmartTokens™

- Track 1.5
  - Supports the storage of ANSI X.509 v3 Certificates
  - RSA Signing on the Token
  - Storage of CKM Credentials
  - Key Pair Generation (KeyGen) (Optional)
  - FIPS 140-1 L2 (Optional)
  - Soft Token, ISO 7816 card, USB Fob

- Track 2.0 (Available Fall 2001)
  - Track 1.5, plus
  - KeyGen on Card (Standard)
  - CKM Operations Performed on the Card/SmartToken
  - FIPS 140-1 L2 (Optional)
  - Soft Token, ISO 7816 card, USB Fob
  - Purse, Procurement, Debit Capabilities (Planned)
  - Future Alternative Tokens (PDA, Wireless Devices, iPAQ™ Holster, etc.)

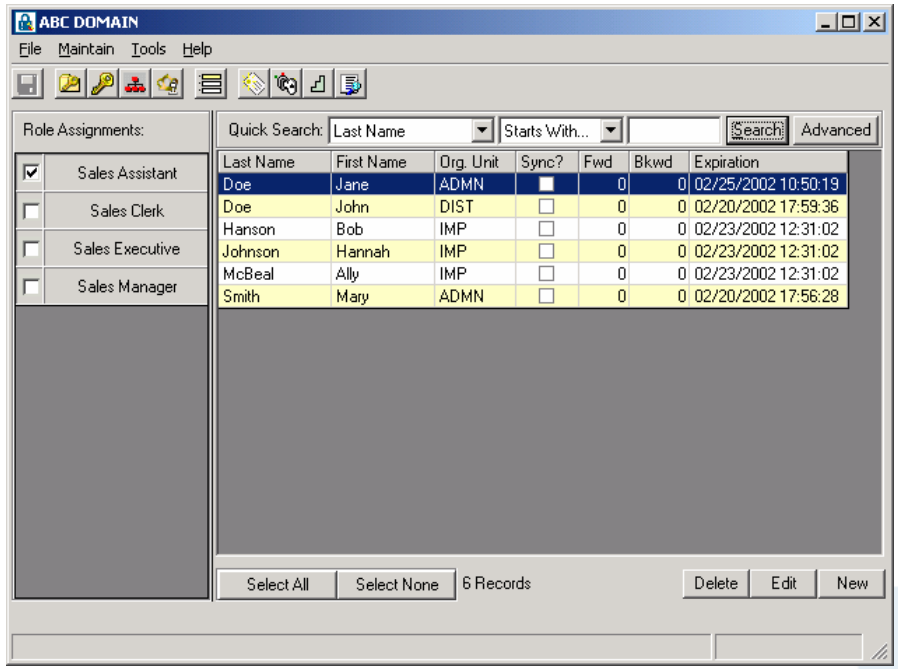
Administration Tools – *Privity Admin Lite*

- Designed for Small Office/-Home Office (SOHO) Applications & Pilots
  - Very few dependencies
  - Supports up to 50 members
  - Lightweight Database and Ultra-Light Footprint
- "Out of the Box" CKM Admin
  - Ease of Use, Minimal Member Data Entry
  - Single-Click Assignment of Pre-Defined Credentials
- Secure Access and Secure Data-at-Rest
- Multiple Token Support
- ActiveSkin USI Support



Administration Tools – *CKM Admin Tool*

- **Designed for Large, Single Domain Enterprise**
- **Flexible, Scalable**
- **Provides Role Based Access Control**
- **Allows the Domain Authority to…**
  - **Create Customized Categories, Credentials, and Roles that mirror existing organizational structures**
  - **Enroll Members (Indiv. & Bulk Load features)**
  - **Assign Roles to Members**
  - **Create Tokens for Members**



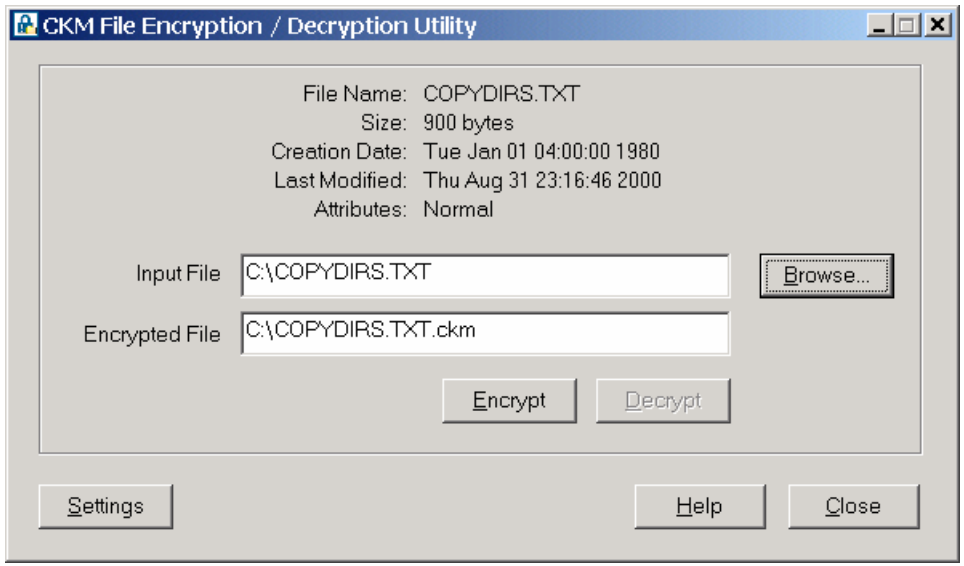
Administration Tools – *Privity Enterprise Builder*

E-1 - Summer 2001

- Remote Token Updating
  - Revocation (zeroizing or disabling)
  - Add/Remove Credentials, Categories, Policies
  - Adjust Maintenance Values
- Tiered Administration Architecture
  - N-tiered hierarchy supports large enterprises
  - Members assigned admin rights via X.509 cert
- Web-based Member Enrollment Process
  - SSL based browser security
- Enhanced Token Creation Process
  - Outsourced Token Creation/Production
- Multiple Domain/Workgroup Support

Desktop Products – *CKM File*

- **File Encryption/-Decryption Utility**
- **Encrypts, decrypts one file at a time**
- **Easy to Use, Simple to Learn**
- **Flexible Settings**
- **What We Use Internally**



Desktop Products – *Privity File 2.0*

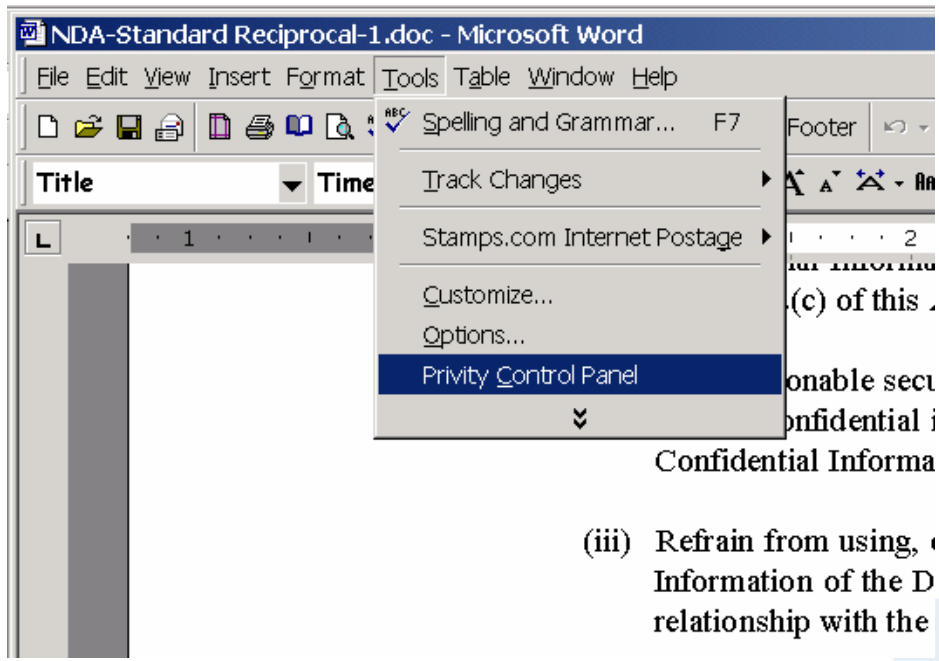
E-1 - August 2001

- **Next Generation of CKM File**
- **Digital Signature Support**
- **Multiple File Encryption/Decryption**
- **Directory Based Encryption**
- **ActiveSkin USI Support**
- **Privity File Safe Integration**

Product Groups – Desktop Products – *Privity Office*

E-1 - Summer 2001

- Privity Word
  - Integrated “Redactor” Plug-In for Microsoft Word
  - Role based access to objects (word, paragraph, graphic, etc) enforced using CKM
  - “Nested” or “Embedded” objects of any type can be protected using CKM
  - ActiveSkin USI Support
- Privity Outlook
  - Same feature set as Word



Q&A, Discussion and Action Items

POC Information

TecSec, Incorporated
1953 Gallows Road, Suite 220
Vienna, VA 22182
703-506-9069
http://www.tecsec.com

Brice Zimmerman, President & COO (x147) – bricez@tecsec.com
Mike Cummins, Director, Health Care Practice Area (x156) – mikec@tecsec.com
John Von Kadich, Director, HCFA Program Development (410-786-6513) – jvonkadich@hcfa.gov