aSuretee SM

FIRST DATA

Advances in Digital Identity Management

Steve Howard, VP
Global Development
First Data Corp.

February 27, 2003

Identity Management: Migration

- Where we started
- What's available today
- What to consider for future systems

Migration: Passwords to SSO

- Passwords
  - PRO: Easy, Scaleable
  - CON: Hackers focus on UID/Password attacks to gain access to records: Identity Theft
- Token
  - PRO: Portable,
  - CON: One application per token, inconsistent in how the “what you know” is managed
- SSO/AAA
  - PRO: Enable enterprise to focus on internal business management issues and efficiency
    - fewer password resets, resolves multiple identity issues
  - CON: Internal integration, attack one UID/password pair - gain access to all authorized applications

Back to the Basics

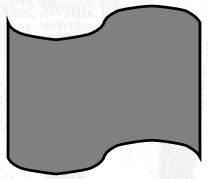
- Identity
- Authenticator
- Identification and Authentication
- Authorization
- Audit
- Confidentiality
- Supported by
  - Something you have, know and are

Identity vs. Authentication

- **Identity:** process of validating a claim of identity through background checks, verification of out-of-wallet information, the historical record, and establishing an identifier that represents that verified claim (e.g., driver's license, a digital certificate, a distinguished name, user-id, or biometric on a system)
- **Authenticator:** technologies and process that enable validation of an identity for access to a system (e.g., a password, PIN code, digital signature, message authentication code)

Biometrics & Certs NOT Enough

- Cannot make a secret from a non-secret
- Biometrics
  - Useful in determining identity presence during transaction
  - Often requires additional factor to support authentication of principal
- Certificates
  - Certificate is NOT an authenticator
    - Just a bag of bits = magstripe
  - Need the digital signature to authenticate



Time to Move On

- Risk of the password as the authenticator is now being highlighted – risk no longer acceptable
  - Large internet enterprises are experiencing higher Identity Theft rates
- Most PKI and SSO/AAA solutions focus on an enterprise
  - Installations can only support hundreds of thousands - NOT *millions* or *hundreds of millions*
  - Introduce *systemic risks:* Root keys or centralized passwords

Need to focus on replacing Passwords with Public Keys – strong YET scalable authentication

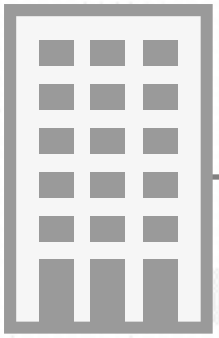
Flexible Identity Solutions

- Support industry initiatives that recognize privacy and enterprise business needs
  - Liberty Project
  - RSA's Nightingale (we hope)
- Recognize risk of large scale solutions enabling Identity Theft
  - Passport
  - Magic Carpet
  - eBay/PayPal
  - Financial access solutions (online statementing, credit app, trading)
- Focus on solutions using existing applications infrastructure as the base that resolve authentication risk issues
  - Support established identity between consenting parties
  - Support established processes (Federal Trust Bridge), if necessary
  - Provide scalability for large deployments
  - Stop paying the *lawyers*

Application IS the Infrastructure

- Business applications already integrate identity verification/validation to support access and authorization
  - PKI requires external source = outsourcing key management
    - Accepts that Identity and Authenticator must be explicitly *unified*
    - Accepts requirements to integrate outside identity authority and management processes into business applications
- Business applications in open networks are experiencing new risks
  - Password attacks
  - Scaling to hundreds of millions
- The Account Based Digital Signature (ABDS℠) uses a business's existing account information (identity included) to authenticate users and transactions
  - Account based solutions already *work* in industry today
    - >1 billion V/MC accounts successful every day

Account Based Digital Signature



User ID	Public Key	Authorization Level
Smith, J	AXBCY	> $50 PIN present; $1500 max.
Smith, S	CYDFW	> $50 PIN present ; > $1000 PIN Active; $10,000 max
Thomas, W	QUNME	> $100 PIN present ; > $2000 PIN Active; $100,000 max

- Business employs one-step process of adding public key from user's token/smart card to business account
- Each organization controls identity and user permissions through established business processes
- Business application dictates levels of authorization based on value of transaction

Federal Credential Life Cycle