Achieving online trust through Mutual Authentication
Agenda

- Where do we need trust online?
  - who are the affected parties?

- Authenticating the site to a consumer
  - V by V and SecureCode, next generation browsers

- Authenticating the consumer to a site
  - strong authentication options
Where do we need trust online?

“For it is mutual trust, even more than mutual interest that holds human associations together.”

H. L. Mencken (1880 - 1956)
Where do we need trust online?

For any online interaction where consumer confidence would be eroded if a fraudster could gain value from intercepting or changing data such as....
Authenticating the consumer to a site

- For financial payments
  - CVV2
  - Address verification

- For bank account management
  - Almost always user name and ID
  - Some pioneers (Lloyds TSB, Alliance & Leicester)

- For online service providers account management
  - Almost always User Name and ID
  - Some pioneers (eBay, PayPal, MicroSoft, Yahoo)
Authenticating the site to a consumer

“Trust in Allah, but tie your camel”
Old Muslim Proverb
Authenticating the site to a consumer - Today

Address: https://www.playsecureserver1.com/order.asp

Privacy Policy
Authenticating the site to a consumer – Future

- SSL and browser providers working together
  - to help fight fraud

- Display security and site authenticity
  - method depends on browser

- Standards (nearly) complete for IE7, vary by browser
  - based on authentication procedures for “High Assurance” certificates

- Higher security browsers are available today
  - Netscape / Firefox available, IE7 (85% share) late 2006
Internet Explorer 7 user experience
Internet Explorer 7 user experience
Authenticating the consumer to a site

“All men are frauds. The only difference between them is that some admit it. I myself deny it.”

H. L. Mencken (1880 - 1956)
Authenticating for financial payments – CVV2 & AVS
Authenticating the consumer to a site – future

- Two factor or strong authentication, many form factors
  - token, phone, application on PC, “bingo card”

- Many models for authentication
  - must reflect security requirements AND consumer acceptance

- Shared token makes financial sense, helps acceptance
  - Financial Payments
  - Bank Account Management
  - AND Online Service Provider Account Management
Many form factors

**HARD**
- OTP Token
- Smart Cards
- Multi-Function Devices

**SOFT**
- Digital Certificate
- Desktop Soft Token
- Mobile Phone
- Fixed Phone (voice)

VIP Two-Factor Authentication
Many models for authentication

- VeriSign have identified 5 models for the UK banking and retail community
  - Traditional
  - EMV CAP
  - Closed user group trusted 3rd Party
  - Open user group trusted 3rd Party (VIP)
  - Hybrid (EMV CAP and VIP)

- 1st draft of White Paper available
  - Will be distributed to contacts within banking and retail community
Open group trusted 3rd party

End User

ONLINE BANK USER ID, PASSWORD, OTP

APPLICATION USER ID, PASSWORD, OTP

Online Bank

User Store

VIP Validation Service

Online Merchant

User Store

VIP Validation Service

Online Auction

User Store

VIP Validation Service

VeriSign

VIP OTP Validation Engine

VeriSign Identity Protection
VeriSign Identity Protection Network (VIP)

- Invisible or Web Lifestyle Friendly Security for Consumers
- Comprehensive & Turn-Key Solution for Online Services

Intelligent Infrastructure for ID Protection
From the Leading Internet Infrastructure Operator
Inspired by the offline world

✓ An ATM card works across all the Banks on the Cirrus Network
✓ A VIP Device Works Across all the Web sites on the VIP Network
Achieving online trust through Mutual Authentication