Knowledge-Based Authentication
Challenge Response System

Kevin Trilli
Director, Product Management
VeriSign, Inc.

Bill Andrews
Sr. Manager, Product Management
Lightbridge, Inc.
Purpose and Agenda

▶ Purpose
  – Explain deployment example for KBA
  – Cover challenges of quantifying Challenge/Response (C/R)

▶ Agenda
  – Overview of VeriSign Authentication Service Bureau
  – Challenge/Response in Action: On-Line Auction Site
  – Challenge/Response System Configuration
VeriSign Security Services

Provide Critical Security and Payment Infrastructures that Maximize Efficiency, Remove Complexity, and Reduce Risk

- 380,000+ secure sites & servers
- 90,000 merchants
- 4,000+ enterprise customers
- 90,000 consumers verified
- 30,000+ certificates issued
- ~25% of N. America E-Commerce
- ~5M payment transactions
- $500M-$700M processed
VeriSign Intelligence and Control℠ Solutions

Provide targeted Solutions to business needs

With flexibly deployed Offerings

Leveraging World-Class Assets

Delivered from Solid Infrastructure

---

**Business Continuity**
- Network Infrastructure Continuity

**Regulatory Compliance**
- HIPAA, FDA

**Business Partner Integration**
- Secure Extranets

**Commerce Enablement**
- Security, Payments

- Strong Authentication
- Secure Access To Networks

- Network Security
- Intelligent Monitoring & Management

- Application Security
- Secure Web Services

- Commerce Security
- Fraud Protection

---

**Technology**
(Managed Security Services, DNS, PKI, Trust Gateway, SSL, Payment Gateway)

**Data**
(enterprise event data, 9 billion DNS transactions, 25% N. American payment volume, SSL certificate validation)

**Intelligence/Expertise**
(Internet health monitoring, event correlation, fraud detection engine)

Atlas, 24*7 redundancy, secure operations, PKI roots
VeriSign set of Offerings: Credentialing and ID Proofing Services

- **Credentialing Systems**
  - Managed Strong Authentication Service Platform
  - PKI, Strong Authentication
  - Commercial and Public Sector Offerings
    - FIPS-140
    - Federal Bridge Compliant
    - Mortgage Banker’s Association

- **ID Proofing Services**
  - Physician Authentication using VeriSign’s AMA Database
  - Consumer Authentication using Lightbridge Services
  - Business Authentication using D&B Database
  - In-Person Proofing Services
    - Notary
    - Postal Service
Various levels of customer authentication

Non intrusive

- Tier 1: Identity Verification
  - Based on application data
  - Name, Address, Phone
  - Optional: email, date of birth, drivers license
  - Custom Risk Score

- Tier 2: Interactive Query
  - Based on credit report
  - Dynamic “out of wallet” questionnaire

- Manual Review
  - For exception handling and support
  - 24x7 live person in call center

Interactive

- Physical Proof
  - Faxing in passport, drivers license, utility billing
A consumer initiates a transaction online. Before completing the transaction the merchant or institution submits the consumer data to VeriSign/Lightbridge for validation, verification and authentication.

CAS Tier 1 validates and verifies consumer data using a unique online fraud model and returns a numeric score indicating the consumer’s relative level of risk.

CAS Tier 2 compares the consumer data to multiple consumer databases, creates a customer profile, and formulates a unique set of “out of wallet” questions which are sent back to the consumer through the merchant web server.

After receiving the consumer’s answers, the CAS decision engine scores the answers and returns an authentication decision to the merchant web server.
eBay Deployment Example
Deployment example

End Users

Consumer Portal / Application

VeriSign CAS

Credit Bureaus
Name & Address
Public Records
DMV and SSN
Higher Risk Data
Proprietary Blacklists

Real time Transaction
XML Interface
24x7x365 support
Guaranteed SLA
Audit Trail Reporting
Custom Configuration

XML

VeriSign®
Case Study: Online Marketplace

Business Challenge

- Provide a safe and secure marketplace for both buyers and sellers
- Track and screen out fraudulent users
- Non-intrusive process that is private and confidential

VeriSign Solution

- Identity verification methods that cross verify identity information using 50+ data sources
- 24x7 call support to handle exceptions
- Leverage VeriSign brand to build consumer confidence

Results

- **Instant account verification** of all users
- **Custom risk score** to flag accounts requiring additional monitoring
- **Tier based authentication** approach to managing risks
Be prepared to provide specific information about your financial data.
CAS gathers data about the individual and creates a challenge only the user should know.

Credit Card Account Number
Enter the next 2 digits in the Account Number for the Discover Credit Card whose account number begins with the digits 601100.

If you don't have a credit card that begins with those digits, please leave the answer blank.

Account Number 601100

Previous Street Name
Enter the Street Name of your Previous Address in HERNDON.

For example, if you lived at 567 North Santa Cruz Avenue, you would enter "Santa Cruz" or if you lived on 2400 5th Street, you'd enter "5th". If you lived at more than one address in the city, enter just one street name. If you have never lived in this city, please leave the answer blank.

Street Name

Credit Card Limit
Enter the Credit Limit for the Discover Credit Card whose account number begins with the digits 601100.

If you don't have a credit card that begins with those digits, please leave the answer blank.

Credit Limit $00
Successful registration!
Feedback Summary
117 positives. 114 are from unique users.
1 neutrals.
0 negatives. 0 are from unique users.

Ebay User is now ID Verified!
C/ R - Authentication Questions (Automated)

- Credit Card Questions
- Previous Address
- Payment Questions
- Account Number Questions
Unanswered Automated Questions

Bank/Institution Questions

Employment Questions
C/ R - Configuration Settings

- Allowable Visits: Number of allowable authentication attempts per user in a specified period of time.
- Allowable Visits Counter: Period by which authentication attempts counter is reset.
- Question Sets: Number of potential automated question sets in a given session.
- Min./Max: Questions per set: Minimum and Maximum number of automated authentication questions per question set.
- Passing Score – Questions Correct: Number of correct answers required for passing automated process.
- Passing Score – Percentage Correct: Percentage of correct answers required for passing automated process.
- Borderline Score – Questions Correct: Number of correct questions required for Borderline Score.
- Borderline Score – Percentage Correct: Percentage of correct questions required for Borderline Score.
C/ R- Configuration Settings

- Question Variances – Payment Amount Questions: Difference between answer provided and information in consumer profile on a per question basis.

- Manual Review: Offline Authentication Process handled by the Lightbridge Call Center whereby consumers verbally answer authentication questions.
Challenges in Quantifying C/R

- Requires merchant/agency involvement
- Time lag between fraudulent event and knowledge of event
- Fraud data
  - Sensitive to customers
  - Inaccurate/lack of reporting

Requires macro view of multiple systems and direct involvement of customer