Scorecard for Authentication
Technologies

Dow A. Williamson
Market Development Manager - Government Operations
dwilliamson@rsasecurity.com
Authentication Scorecard

• Why Focus on Authentication?
• What are the Requirements for Authentication?
• What is the State of Authentication Technology?
• What is the Authentication Scorecard?
Understanding The Problem
No Single Technology Solves ALL The Problems

United States Nuclear TRIAD

Intercontinental Ballistic Missile (Peacekeeper)

Bomber (B2)

Ballistic Missile Submarine (USS Maine)

“The Most Trusted Name in e-Security”
E-Security requires solutions in three key areas:

- **Authentication** for binding the user to the digital identity
- **Encryption** for binding the digital identity to the data and transactions
- **PKI** to provide a managed service to reduce operational costs
Why Focus on Authentication?

- Authentication is the essential foundation for e-government
  - Establishes trust by proving identities of the participants in a transaction
- Authentication is the foundation for other important security services
  - Authorization
  - Audit

“On the Internet, no one knows you’re a dog!”

“The Most Trusted Name in e-Security”
### e-Security for e-Government …

#### Authentication: A Piece of the Puzzle

<table>
<thead>
<tr>
<th>e-Government Requirements</th>
<th>e-Security Services</th>
<th>e-Security Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prove identities (establish trust)</td>
<td>• Authentication, Strong Authentication</td>
<td>• UserID/Password, Kerberos/DCE, Hardware Tokens, Software Tokens, Digital Certificates (PKI), Biometrics</td>
</tr>
<tr>
<td>• Protect communications</td>
<td>• Data Privacy, Data Integrity</td>
<td>• Encryption</td>
</tr>
<tr>
<td>• Sign transactions</td>
<td>• Non-Repudiation</td>
<td>• Digital Signatures (e.g.,PKI, Encryption)</td>
</tr>
</tbody>
</table>
Authentication Market

Drivers

• Expanding access
  • Increasing numbers of mobile workers
  • Increasing numbers of telecommuters
  • Extension of the enterprise network to third parties
  • Increasing network size and complexity
  • Need for portable credentials

• “Willy Sutton effect”
  • Increase in sensitive information on intranets
  • High levels of internal compromise/theft
  • Growing security awareness in enterprise accounts

• The problem w/ passwords
  • Passwords provide weak security
  • Unmanageability of multiple passwords

Source: RSAS, adapted from Frost & Sullivan “US Network Authentication Markets”

“The Most Trusted Name in e-Security”
Authentication Market
Inhibitors

- **Costs**
  - Perception of high deployment costs
  - Perception of additional administrative burden
  - Lack of installed base of smart card readers
  - Concern over lost / forgotten / broken tokens or smart cards

- **Deployability**
  - Concern over scalability
  - Interoperability with current systems
  - Short-term focus on Y2K initiatives

- **Business Justification**
  - Lack of security awareness
  - Difficulty in quantifying ROI

Source: RSAS, adapted from Frost & Sullivan “US Network Authentication Markets”

“The Most Trusted Name in e-Security”
Market Forecast: Authentication Technologies

Source: Frost and Sullivan, US Authentication Market

“The Most Trusted Name in e-Security”
Authentication Scorecard

- Why Focus on Authentication?
- *What are the Requirements for Authentication?*
- What is the State of Authentication Technology?
- What is the Authentication Scorecard?
IATF Authentication Requirements

• IATF Chapter 6 - “Defend the Enclave Boundary/External Connections”
  • Focus on “effective control”
    • Firewalls
    • Guards
    • Virtual Private Networks (VPNs)
    • Identification & Authentication
  • Focus on “effective monitoring”
    • Intrusion Detection Systems (IDS)
    • Vulnerability Scanners
    • Virus Detection
Authentication Maps to the “Defense in Depth Overview”

Defense in Depth Overview, Figure 2, “Technical Elements of the Defense-in-Depth Strategy”
What Our Government and Commercial Customers Require

“The Most Trusted Name in e-Security”

“Protection for Network Access (PNA) addresses the requirement for authorized Local Area Network (LAN) users and administrators, and individual workstation/personal-computer users, to be able to safely-access and to be-safely-accessed-by untrusted (potentially hostile) network connections.”

Source: IATF, Section 6.1

• The ability to **strongly authenticate**…
  • e-Government/e-Business
    • Protect mission-critical applications, databases, files or web sites, while enabling the sharing of highly valuable information
  • Local Networks
    • Provide local network login protection and authenticate users to critical network operating systems (e.g., Mainframe, workstation, and PC)
  • Remote Access
    • Ensure only authorized remote users can access information resources via direct dial-in systems or Internet-based connections via VPN/Firewalls

“The Most Trusted Name in e-Security”
**Strong Authentication:**

**“Two or More Factors”**

- **Something you know**
  - Password
  - PIN
  - “Mother’s maiden name”

- **Something you have**
  - Physical key
  - Token
  - Magnetic card
  - Smart card

- **Something you are**
  - Fingerprint
  - Voice
  - Retina
  - Iris

“The Most Trusted Name in e-Security”
Defense Information Infrastructure-wide (DII-wide) Strong Authentication

- Internet Access
- Web Application
- RSA Agent
- VPN or Firewall
- Web Server
- RSA ACE/Server
- Mainframe
- Wintel
- Unix
- Dial-Up Access
- DII Access

“The Most Trusted Name in e-Security”
Authentication Scorecard

- Why Focus on Authentication?
- What are the Requirements for Authentication?
- What is the State of Authentication Technology?
- What is the Authentication Scorecard?
Most significant authentication issues

- Password maintenance
  - 20%-50% of Help Desk calls
- Password security
- Password cost
  - Average $80 per Help Desk call

"What applications are causing you to re-evaluate your authentication strategy?"

- e-Commerce: 78%
- Partner Extranet: 58%
- Employee Remote Access: 48%
- Internal Network/Application Login: 38%

Source: Forrester Research, “A Digital Certificate Road Map”

“The Most Trusted Name in e-Security”
Authentication Status Quo

Employees

Source: Forrester Research, “A Digital Certificate Road Map”

“The Most Trusted Name in e-Security”
Authentication Status Quo
Partners

Source: Forrester Research, “A Digital Certificate Road Map”

“The Most Trusted Name in e-Security”
Authentication Status Quo
Customers

Source: Forrester Research, “A Digital Certificate Road Map”

“The Most Trusted Name in e-Security”
The Problem with Passwords (I)

- Shoulder-surfing coworkers
- Finding written passwords
  - Post-It notes
  - Day-Timer
- Guessing passwords
  - “password”, “secret”
  - Spouse/dog/kid’s name
  - Username
The Problem with Passwords (II)

- “Social engineering”
- Password cracking tools
  - “Crack”
  - “L0phtCrack”
  - “Cracker Jack”
- Network sniffing
- All of the “casual” approaches
The Problem with Passwords (III)

- Passwords are *surprisingly* expensive
  - 20 - 50% of Help Desk calls are password related
  - Help Desk calls cost an average of $80 each
  - Lost user productivity from lack of network access

- Exposure to loss from password breaches far greater than Help Desk costs

- Security fears keep organizations from pursuing new e-government opportunities
Strong Authentication In Use Today with DII Components

- 7+ million users at 4500+ companies
- 150+ strong authentication-ready COTS products from 100+ vendors
  - Firewalls/RAS
  - VPNs
  - Operating Systems
- Scalable to 100,000s of users
- Broad range of form factors

IATF, Figure 6-1, “Defend the Enclave Boundary/External Connections”

“The Most Trusted Name in e-Security”
# U.S. Government

## Strong Authentication Users

<table>
<thead>
<tr>
<th>Executive</th>
<th>Legislative</th>
<th>Judicial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the President of the United States</td>
<td>United States House of Representatives</td>
<td>United States Supreme Court</td>
</tr>
<tr>
<td>Every Cabinet Department</td>
<td>United States Senate</td>
<td>United States Court of Appeals</td>
</tr>
<tr>
<td>Several Independent Agencies and Commissions</td>
<td></td>
<td>United States Federal Courts</td>
</tr>
</tbody>
</table>

**“The Most Trusted Name in e-Security”**
State-Of-The-Art
Time-Synchronous Tokens

Hardware or Software Token

Access Server

Same Seed

Same Time

“The Most Trusted Name in e-Security”
State-Of-The-Art
Digital Certificates

Serial Number: 6cb0dad0137a5fa7988f
Validity: Nov.08,1997 - Nov.08,1998
Subject / Name / Organization
Locality = Internet
Organization = VeriSign, Inc.
Organizational Unit = VeriSign Class 2 CA - Individual
Subscriber
Organizational Unit = www.verisign.com/repository/CPS
Incorp. by Ref.,LIAB.LTD(c)96
Organizational Unit = Digital ID Class 2 - Netscape
Common Name = Keith H Erskine
Email Address = kerskine@ne.mediaone.net
Unstructured Address = 160 Boston Rd Chelmsford
Public Key: ie86502hhd009dkias736ed55ewfk98dszbc
vcqm85k309nviidwtooifkk2834kl
Signed By: VeriSign, Inc.
kdiowurei495729hshsgo925h309fhw09721h
481903207akndnznkjaoeru10591328y5

Status: Valid

Public Key
Private Key
Certificate Authority

“The Most Trusted Name in e-Security”
Digital Certificates
How Secure is the Private Key?

<table>
<thead>
<tr>
<th>Where is it stored?</th>
<th>How is the store protected?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Drive</td>
<td>Nothing, or Password</td>
</tr>
<tr>
<td>Software</td>
<td>Authenticator of Choice</td>
</tr>
<tr>
<td>Smart Card</td>
<td>PIN</td>
</tr>
</tbody>
</table>

"The Most Trusted Name in e-Security"
State-Of-The-Art
Multi-Application Smart Cards

- Highest security
  - On-card digital signatures
- Supports latest application features
  - Dual keys and certificates
- Mobility
  - Credential store on-card with keys, certificates, network login information, and software token seed record
- Versatile
  - Supports PKI applications and traditional token-protected systems
  - Magnetic stripe for physical access
  - Personalization for employee identification

The Most Trusted Name in e-Security
Biometric authentication depends on something unique about you personally:
- Fingerprints
- Iris pattern
- Voiceprint
- Faceprint
- Retinal Pattern

A pattern of the physical characteristic is recorded in advance:
- The physical characteristic is re-read at the time of authentication
- The read characteristic is compared with the stored version
- If the match is good enough, the access is granted
Confusing Market Messages

• Industry Analyst
  • “Use proprietary random PIN tokens only where they are already deployed or are urgently needed in the next 6-9 months.”
  • “Expensive.”
  • “Smart cards … can do more at a lower cost.”

• Industry Analyst (4 months later)
  • “Implementing certificate-based solutions is complex and costly at this time, and will take 12 - 24 months to be widely deployed. Consider other mechanisms for authentication such as ... proprietary tokens in the interim”.

A consistent framework for comparison is needed!

“The Most Trusted Name in e-Security”
Authentication Scorecard

- Why Focus on Authentication?
- What are the Requirements for Authentication?
- What is the State of Authentication Technology?
- What is the Authentication Scorecard?

“The Most Trusted Name in e-Security”
Authentication Scorecard

Why??

- Companies are reevaluating authentication strategies
- Several authentication technologies are available
  - How to objectively position alternatives?
  - How to objectively choose most appropriate?
  - How to objectively allocate investments?
- Market buzz ≠ Market reality, e.g.,
  - Biometrics gets hugely disproportionate share of press coverage relative to actual deployment
  - “Year of the PKI”: 1997 1998 1999 2000
  - “Tokens are Dead” vs “Long Live Tokens”
Authentication Scorecard
Methodology

• Select key authentication technologies for evaluation
• Establish consistent evaluation criteria
• For each authentication technology, assign values (scale of 1-10) for each evaluation criteria
• Weight evaluation criteria according to relative importance for a particular application or environment
• Compare results
Authentication Scorecard
Technologies Considered

- UserID / Password (baseline)
  - Near-universal use
  - Growing awareness of inadequacy
  - Growing problems with scale
- Two-factor authentication (Time-Synchronous Tokens)
  - Hardware (multiple form factors)
  - Software (multiple platforms)
- Digital certificates (standalone)
  - PKI
- Two-factor authentication (use with certificates)
  - Smart cards
  - Biometrics
  - Tokens

“The Most Trusted Name in e-Security”
## Authentication Scorecard
### Evaluation Criteria (I)

- **Interoperability**
  - Does the authentication method work natively with multiple products, or does it work only if all parties install additional software on their desktops or servers?

- **Back-end integration**
  - How easy is it to integrate into the access control mechanisms of the back-end resources or applications?

- **Portability**
  - How portable is the authentication method?
    - Can it be used to gain access from multiple systems?

- **Scale/Robustness**
  - Does the authentication solution scale to the degree required now? Three years from now?

Source: RSAS, adapted from Giga Information Group, “The Hows and Whys of Online Authentication”

"The Most Trusted Name in e-Security"
Authentication Scorecard
Evaluation Criteria (II)

• Ease of deployment
  • How easy is it to deploy the technology? This includes the distribution of any necessary hardware or software; ease of installation; ease of configuration; etc.

• Ease of adoption / Ease of use
  • How easy is it for end-users to learn how to use the authentication method? How convenient is it for end-users to use the authentication method, day in and day out?

• Multi-Purpose
  • Can the authentication method be used for more than one purpose? E.g., physical access, network access, application access, digital signature, etc.

Source: RSAS, adapted from Giga Information Group, “The Hows and Whys of Online Authentication”
Authentication Scorecard

Evaluation Criteria (III)

- Initial costs
  - What are the initial acquisition and deployment costs? This may include additional hardware, software, servers, readers, services, etc. associated with acquiring and deploying the authentication solution.

- Operating costs
  - What are the ongoing operating costs? This may include costs for replacement (e.g., expired / lost / stolen / broken) authentication mechanisms; ongoing management; upgrades; support; help desk; etc.

- Relative strength
  - How strong is the authentication? Is it adequate for the information being protected? Does it meet regulatory requirements (if any) for the protection of information?

Source: RSAS, adapted from Giga Information Group, “The Hows and Whys of Online Authentication”

“The Most Trusted Name in e-Security”
Authentication Scorecard Example

Source: RSAS, adapted from Giga Information Group, “The Hows and Whys of Online Authentication”
# Authentication Scorecard

**Example**

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weight</th>
<th>UserID/Password</th>
<th>Hardware Tokens</th>
<th>Software Tokens</th>
<th>Digital Certificates</th>
<th>Smart Cards + Certificates</th>
<th>Biometrics + Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interoperability</td>
<td>10.0%</td>
<td>8</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Back-end Integration</td>
<td>10.0%</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>5</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Portability</td>
<td>5.0%</td>
<td>9</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Multi-Purpose</td>
<td>5.0%</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>Scale/Robustness</td>
<td>10.0%</td>
<td>4</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>Ease of Use</td>
<td>10.0%</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Ease of Deployment</td>
<td>10.0%</td>
<td>9</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Initial Costs</td>
<td>10.0%</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Operating Costs</td>
<td>15.0%</td>
<td>3</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Relative Strength</td>
<td>15.0%</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>5</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Weighted Score</td>
<td>100.0%</td>
<td>5.60</td>
<td>6.75</td>
<td>6.30</td>
<td>5.70</td>
<td>5.90</td>
<td>4.90</td>
</tr>
</tbody>
</table>

**SUMMARY**

<table>
<thead>
<tr>
<th>Weighted Score</th>
<th>UserID/Password</th>
<th>Hardware Tokens</th>
<th>Software Tokens</th>
<th>Digital Certificates</th>
<th>Smart Cards + Certificates</th>
<th>Biometrics + Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.60</td>
<td>6.75</td>
<td>6.30</td>
<td>5.70</td>
<td>5.90</td>
<td>4.90</td>
</tr>
</tbody>
</table>

- Make your own evaluation - Interactive Authentication Scorecard
- Visit the RSA booth at the Conference
- Visit the RSA Web site

Source: RSAS, adapted from Giga Information Group, “The Hows and Whys of Online Authentication”
**Scorecard**

**UserID/Password**

- **Pros**
  - Easy to use
  - Platform/hardware independent
  - No acquisition cost
  - Interoperable
  - Minimal end-user training

- **Cons**
  - Weak security
    - Static value - can be intercepted, guessed, spoofed, cracked
    - Most are poorly chosen
  - High operating costs
    - Help Desk for forgotten passwords
  - End-user aggravation
    - Inconsistent formats between applications
    - Hard to remember if frequently changed

---

"The Most Trusted Name in e-Security"
Scorecard
Hardware Tokens

• Pros
  • Strong security
    • Two-factor
    • Dynamic value; difficult to hack or predict; negates replay attacks
  • Platform-independent
  • Portable
  • No desktop software required
  • High interoperability
  • No password administration

• Cons
  • End-user training required
  • Acquisition and deployment cost
  • Replacement cost for lost, stolen or expired tokens
  • Single-purpose device
    • Cannot be used as ID badge or physical access

“The Most Trusted Name in e-Security”
**Scorecard**

**Software Tokens**

**Pros**
- Low acquisition cost
- Strong security
  - Mechanisms to bind token to specific machine
- High interoperability
- End-user does not have to carry separate device

**Cons**
- Need to install software on desktop
- Platform-dependent
- Not portable

“*The Most Trusted Name in e-Security*”
Scorecard
Digital Certificates

**Pros**
- Low acquisition cost
- Support for Web-based applications
- Multiple use
  - SSL, S/MIME, IPSec
- Digital signature
- Scaleability

**Cons**
- Medium security
  - Private key often unprotected, or protected by password
  - No copy protection
- Limited certificate-enabled applications
- High administrative costs
- Complex to deploy

“The Most Trusted Name in e-Security”
Scorecard
Smart Cards + Certificates

**Pros**
- Multi-purpose
  - ID badge
  - Physical security
- Strong security
  - Two-factor
- Easy end-user adoption

**Cons**
- High acquisition cost
- Limited certificate-enabled applications
- Need to deploy hardware and software to each user
- Limited interoperability
  - Standards emerging

“The Most Trusted Name in e-Security”
Scorecard
Biometrics + Certificates

• Pros
  • Perceived ease-of-use
    • Minimal end-user training
  • Always have it with you
  • Strong security
    • Two-factor

• Cons
  • Maturity of technology
  • End-user acceptance
  • Very high acquisition and deployment cost
  • Hard to scale
  • Limited interoperability
**Conclusions**

- Authentication is the essential foundation for e-government
  - Establish trust
- Organizations should understand tradeoffs between authentication alternatives
  - Balance tradeoffs with security requirements
  - Avoid evaluation based on a single criteria (price, scale, etc.)
- Markets and technologies will continue to evolve
  - Near-term: tokens
  - Longer-term: digital certificates and smart cards

“The Most Trusted Name in e-Security”
Dow Williamson
RSA Security, Inc
36 Crosby Drive, Bedford, MA 01730
Telephone: 781-301-5381
Fax: 781-301-5310
E-Mail: dwilliamson@rsasecurity.com
Web Site: www.rsasecurity.com