KBA Applicability to e-Government

Mindy Rudell
Dick Stewart
Robin Medlock
Angel Rivera

February 10, 2004
KBA Working Definition

- **KBA has the following characteristics:**
  - Claimant does not need previously established relationship with the relying party
  - Verification of an identity is based on information associated with and provided by the identity claimant
  - Result depends on an acceptable level of consistency with information held by the authentication verifier

- **Knowledge-based techniques may be used for additional purposes, e.g.,**
  - Register for a reusable authenticator
  - Reclaim a lost authenticator
Why KBA?

- **New challenges posed by e-Government**
  - Large numbers of prospective users, up to entire U.S. population
  - Prospective users might have no previous connection with a given agency
  - Infrequent interactions can be expected

- **Result:** Impractical for systems to incorporate advance user-specific information for authentication or access control

- In addition, OMB/GSA propose that agencies accept credentials issued by Credential Services
Generic KBA Model

- Claimant
- Questionnaire
- Claimed identity
- Question(s)
- Responses to Questions
- Context
- Authentication Reference Data
- Commercial data
  - Agency data
- Selected data items
  - Retrieval time limits
  - Scoring thresholds
- Decision Maker
  - Identity Proofing (Scoring)
- Decision
Generic KBA Model: Scoring

Claimant

Claimed identity

Question(s)

Responses to Questions

Authentication Verifier (CSP)

Authentication Reference Data

Context

Decision Maker

Identity Proofing (Scoring)

Decision

Relying Party
Scoring Characteristics for Successful KBA

- **Use of information that is**
  - Clearly bound to a claimant
  - Invisible or not readily available to others

- **Unpredictability of attributes requested of claimants**
  - Use of changeable parameters (e.g., previous payment amounts) where appropriate
  - Constraints on claimant guessing attribute values

- **Ability to compensate for alternate spellings, abbreviations, estimates, etc.**
Generic KBA Model: Information Sources

Claimant

Claimed identity

Question(s)

Responses to Questions

Authentication Reference Data

Commercial data
Agency data

Context

Authentication Verifier (CSP)

Decision

Relying Party
Information Characteristics for Successful KBA

- Scope of coverage comparable to likely population of users
- Use of quality sources (e.g., primary sources preferred to secondary sources)
- Attributes that are not generally known or publicly accessible (e.g., account numbers)
- Currency of volatile information, such as last payment
- Information elements of length and structure that resist guessing
Generic KBA Model: Decision

Claimant

Claimed identity

Question(s)

Responses to Questions

Authentication Reference Data

Context

Authentication Verifier (CSP)

Decision

Relying Party
Decision Characteristics for Successful KBA

- Acceptable interactive response time
- Measures of quality within constraints suitable to relying parties’ use and assurance level
  - Accuracy of authentication decision
  - Acceptable penetration and insult rates
Operational Characteristics for Successful KBA

- **Compliance with law**
  - Privacy
  - Consumer credit
  - Others as appropriate

- **Adaptability of KBA rules to test outcomes and operational experience suitable to relying parties’ needs**

- **Use of reliable information sources**

- **Protection, e.g.,**
  - Communications
  - Source information
  - Against spoofing of Credential Service
  - Audit information
Authentication Metrics

Accuracy of Authentication Decision

Penetration Rate

Insult Rate
## Authentication Metrics: Penetration Rate

### OMB Assurance Levels

<table>
<thead>
<tr>
<th>Level 1:</th>
<th>Level 2:</th>
<th>Level 3:</th>
<th>Level 4:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Little or None</td>
<td>Some</td>
<td>High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

**Goal**
- Not an appropriate measure at Level 1
- Acceptably low, as determined by relying parties
- Acceptably low as determined by relying parties
- Generally lower than Level 2
- No penetrations

**Potential Effect of Erroneous Authentication**
- Little to no effect
- Unauthorized use of relatively low-risk transactions
- Unauthorized transactions with potentially serious security consequences
- Serious consequences

**Expectation**
- Insignificant concern for no-risk and low-risk transactions
- Relatively low penetration
- Acceptability and ability to limit effect determined case-by-case
- Lower penetration than at Level 2, based on more stringent identity proofing. Penetrations may cause serious consequences
- Serious consequences
## OMB Assurance Levels

<table>
<thead>
<tr>
<th>Level 1: Little or None</th>
<th>Level 2: Some</th>
<th>Level 3: High</th>
<th>Level 4: Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal</strong></td>
<td>Very low</td>
<td>Low enough for public acceptance</td>
<td>Low enough for public acceptance of more stringent identity proofing</td>
</tr>
<tr>
<td><strong>Potential Effect of Turning Away Legitimate Users</strong></td>
<td>Disuse of e-government resources, public dissatisfaction</td>
<td>Depends on business owner’s mission</td>
<td>Depends on business owner’s mission</td>
</tr>
<tr>
<td><strong>Expectation</strong></td>
<td>Insult rate will be insignificant since identity is unverified</td>
<td>Moderate</td>
<td>Higher than for Level 2, due to more stringent identity proofing</td>
</tr>
</tbody>
</table>
### Suitability of Knowledge Based Techniques

#### OMB Assurance Levels

<table>
<thead>
<tr>
<th></th>
<th>Level 1: Little or None</th>
<th>Level 2: Some</th>
<th>Level 3: High</th>
<th>Level 4: Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate Authentication</td>
<td>Suitable</td>
<td>Generally suitable</td>
<td>Generally unsuitable</td>
<td>Unsuitable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acceptability depends on the potential relying party’s judgment</td>
<td>KBA cannot meet high identity proofing standards</td>
<td>Level 4 identity assurance standards cannot be met</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adjustment to relying party requirements may be needed</td>
<td>May be acceptable for access to certain special-case transactions if high accuracy can be demonstrated</td>
<td></td>
</tr>
<tr>
<td>Knowledge Based Registration</td>
<td>Suitable for obtaining a reusable credential</td>
<td>Suitable for obtaining a reusable credential</td>
<td>Suitable for obtaining a reusable credential (consistent with NIST guidance) in combination with another separate mechanism</td>
<td>Unsuitable</td>
</tr>
<tr>
<td>Reclaiming Lost Authenticator</td>
<td>Suitable for Level 1 authenticators</td>
<td>Suitable for Level 1 and Level 2 authenticators</td>
<td>Suitable at least for Level 1 and 2 authenticators (consistent with NIST guidance)</td>
<td>Unsuitable</td>
</tr>
</tbody>
</table>
Other Considerations

- Implications of relying party amplification of a CS’s KBA decision
- Tradeoff between KBA effectiveness and intrusiveness
- Handling abuses detected post-authentication (e.g., fraud)
- Use of do-not-authenticate and fraud lists
- Business authentication
- Attribute authentication
- Need for real test data as basis for establishing confidence in CSPs
- Relationship between KBA and Credential Assessment Framework concepts of operation