KBA Applicability to e-Government

Mindy Rudell
Dick Stewart
Robin Medlock
Angel Rivera

February 10, 2004

CENTER FOR ENTERPRISE MODERNIZATION

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

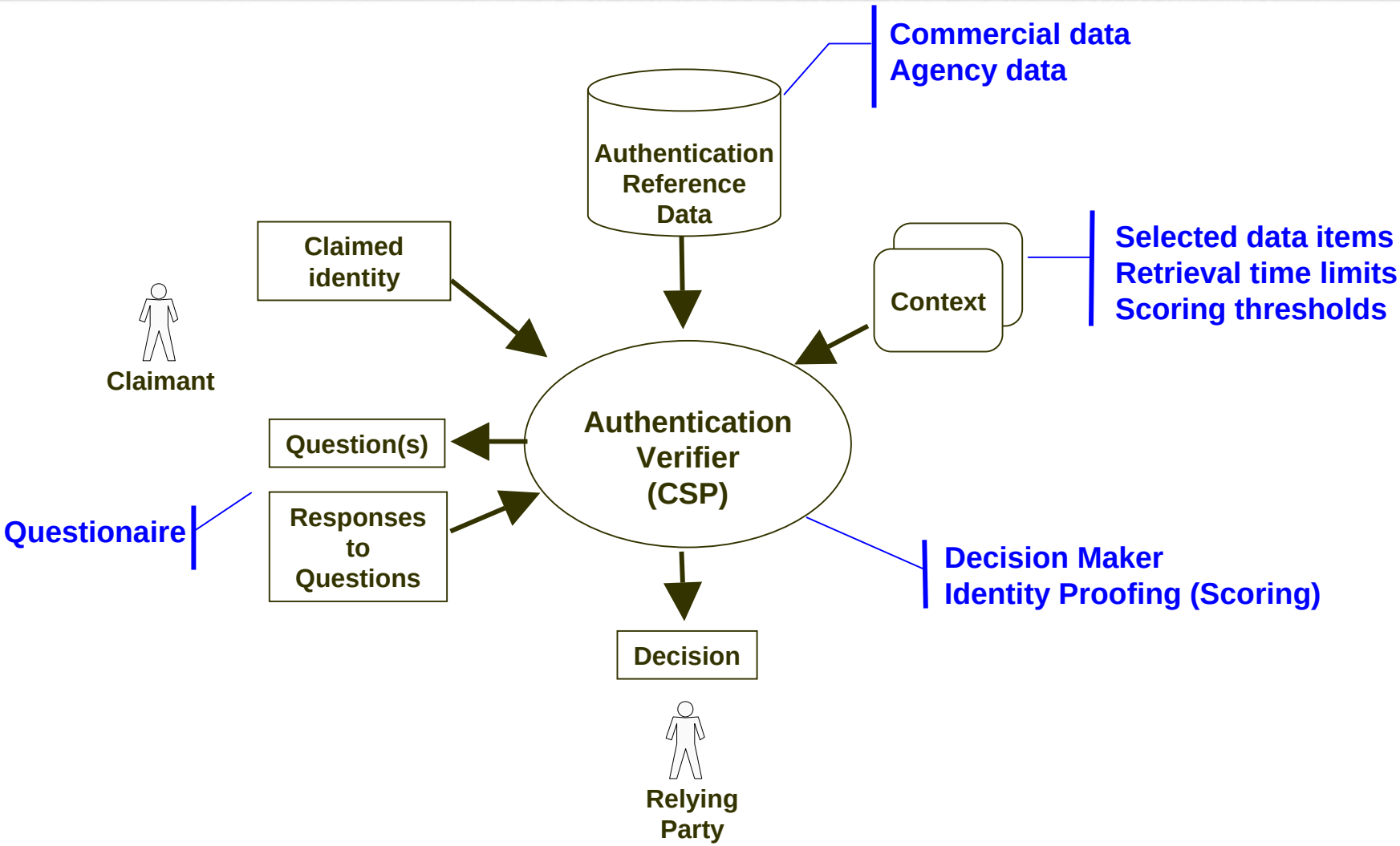
CENTER FOR ENTERPRISE MODERNIZATION

Why KBA?

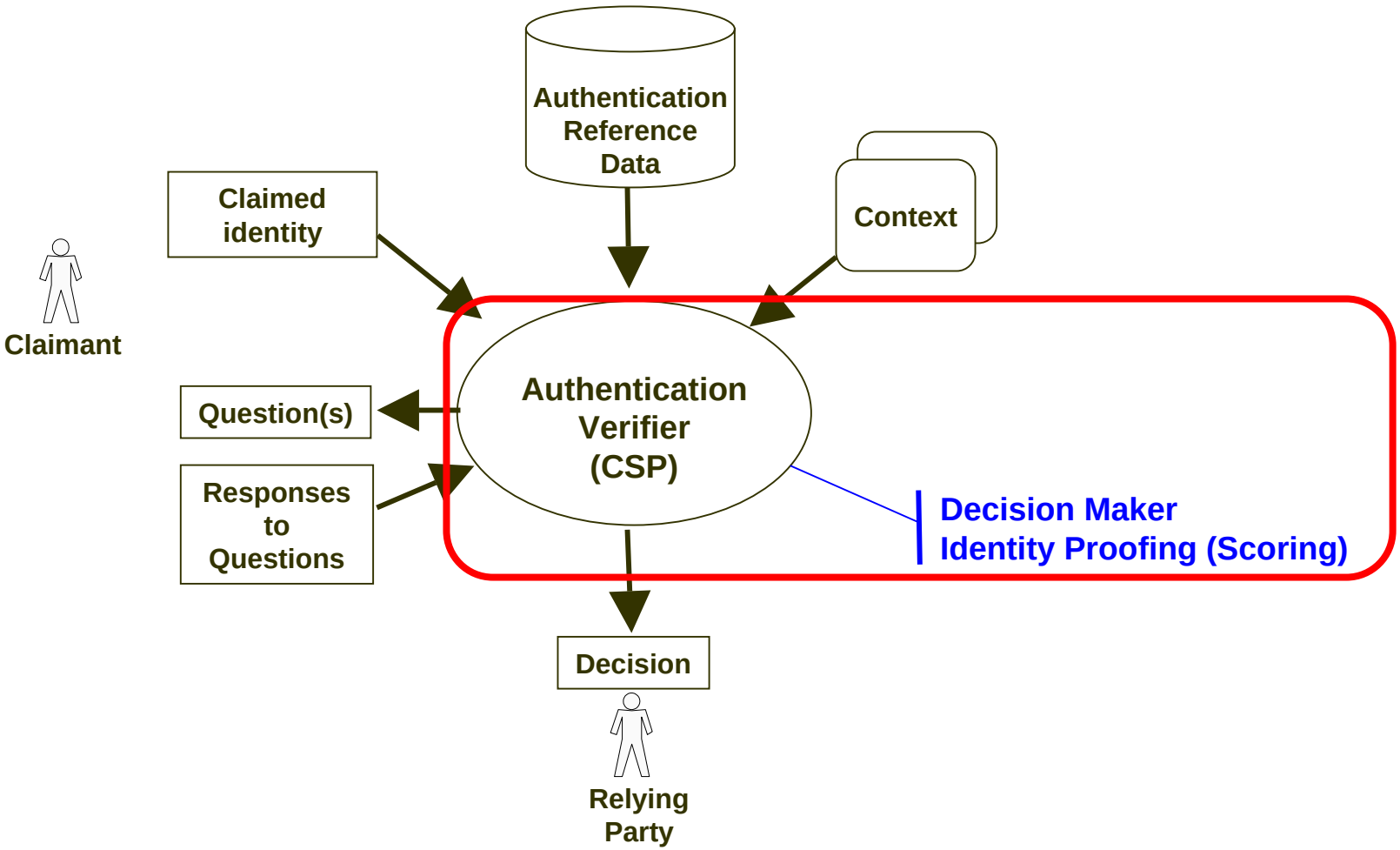
- **New challenges posed by e-Government**
  - Large numbers of prospective users, up to entire U.S. population
  - Prospective users might have no previous connection with a given agency
  - Infrequent interactions can be expected
- **Result: Impractical for systems to incorporate advance user-specific information for authentication or access control**
- **In addition, OMB/GSA propose that agencies accept credentials issued by Credential Services**

CENTER FOR ENTERPRISE MODERNIZATION

Generic KBA Model



Generic KBA Model: Scoring

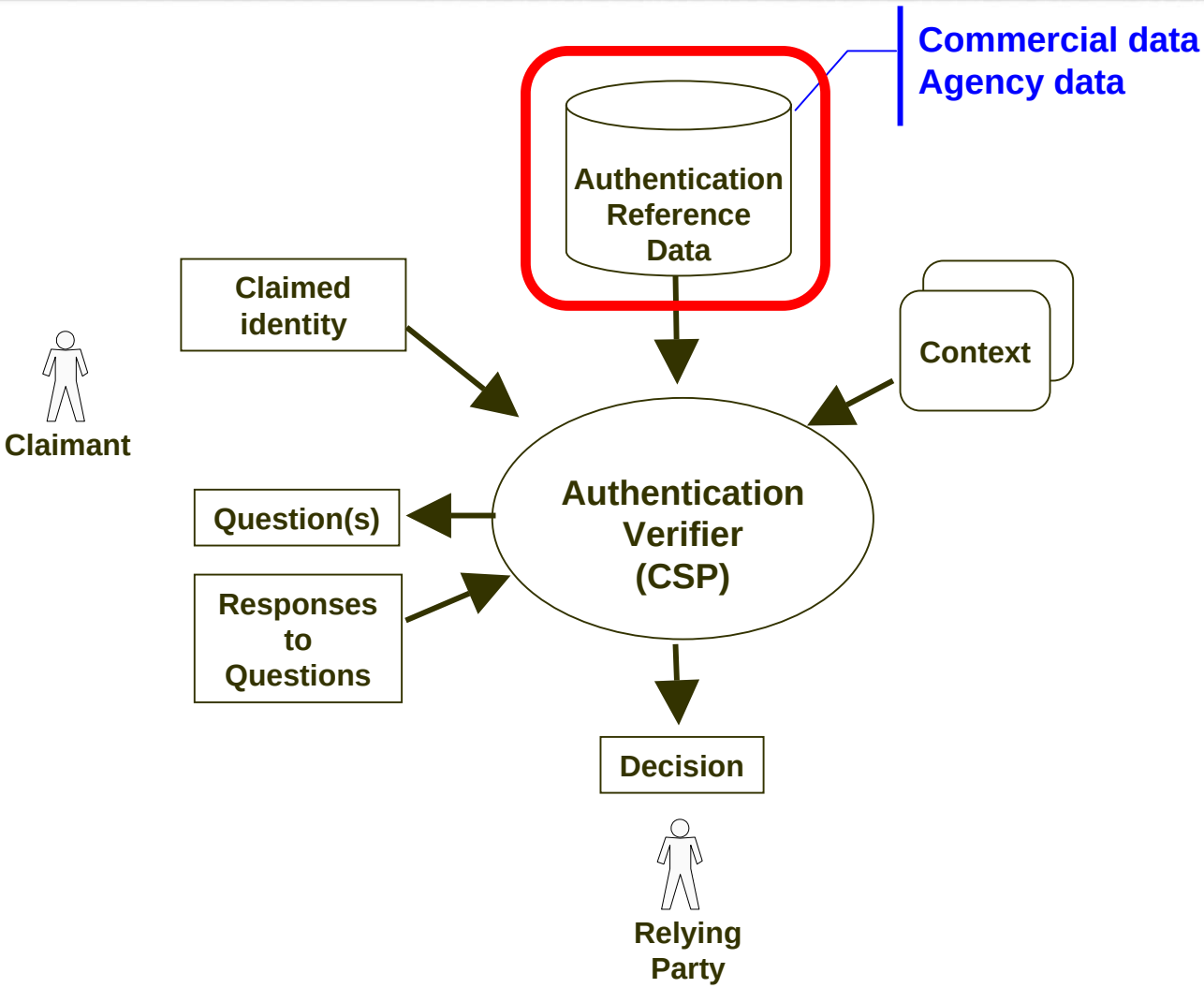


Scoring Characteristics for Successful KBA

- **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.**

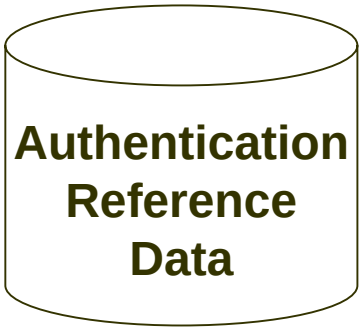
CENTER FOR ENTERPRISE MODERNIZATION

Generic KBA Model: Information Sources



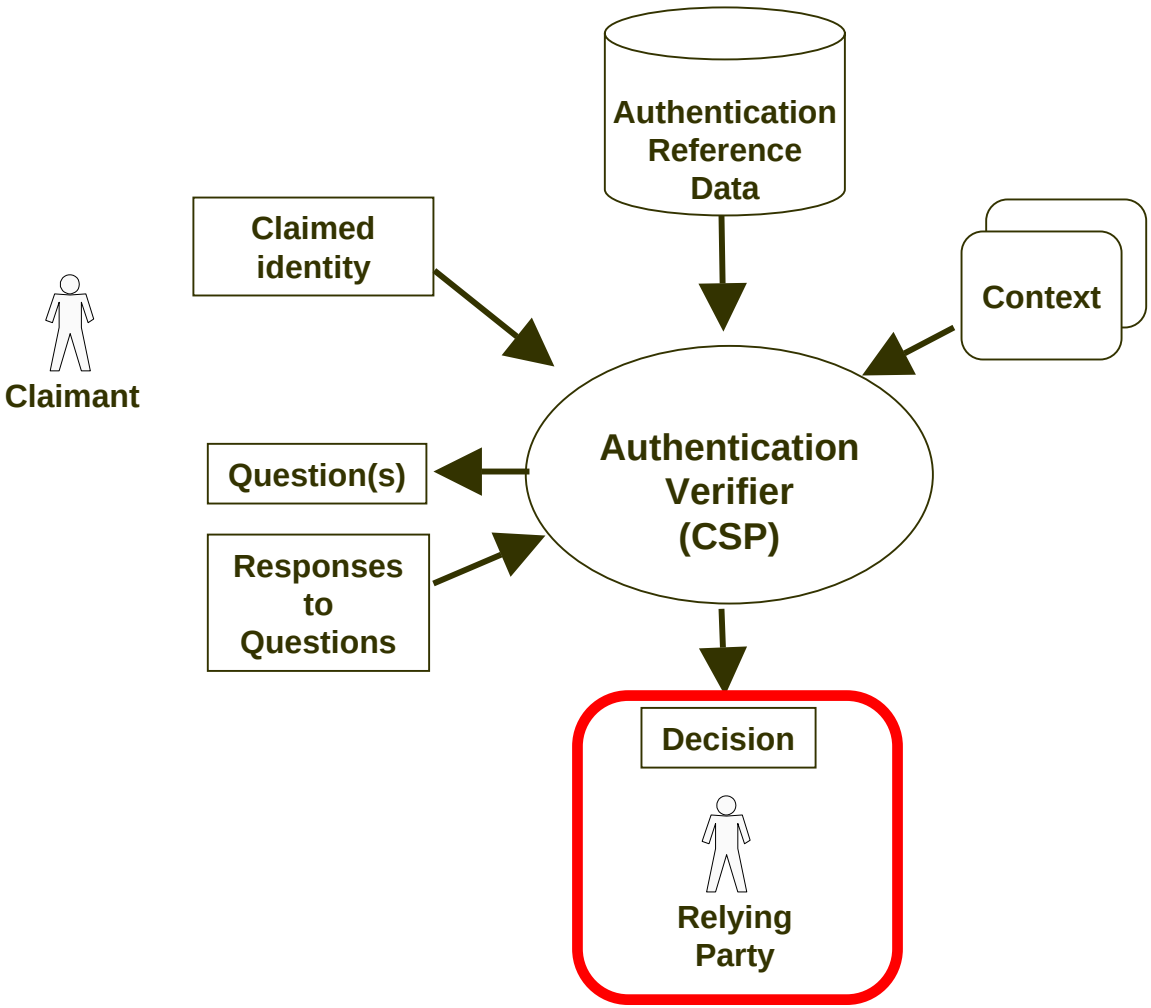
CENTER FOR ENTERPRISE MODERNIZATION

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



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

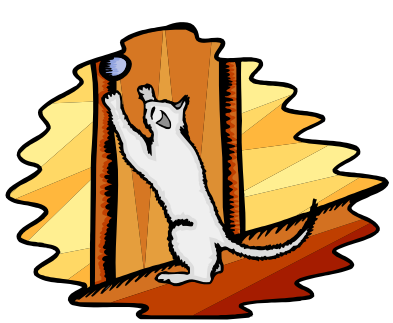
CENTER FOR ENTERPRISE MODERNIZATION

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

CENTER FOR ENTERPRISE MODERNIZATION

Authentication Metrics: Penetration Rate

OMB Assurance Levels

	Level 1: Little or None	Level 2: Some	Level 3: High	Level 4: Very High
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

CENTER FOR ENTERPRISE MODERNIZATION

Authentication Metrics: Insult Rate

OMB Assurance Levels

	Level 1: Little or None	Level 2: Some	Level 3: High	Level 4: Very High
Goal	Very low	Low enough for public acceptance	Low enough for public acceptance of more stringent identity proofing	As low as possible
Potential Effect of Turning Away Legitimate Users	Disuse of e-government resources, public dissatisfaction	Depends on business owner's mission	Depends on business owner's mission	Protection of extremely sensitive transactions may require tolerating a significant insult rate
Expectation	Insult rate will be insignificant since identity is unverified	Moderate	Higher than for Level 2, due to more stringent identity proofing	May be relatively high due to extremely sensitive transactions

CENTER FOR ENTERPRISE MODERNIZATION

Suitability of Knowledge Based Techniques

OMB Assurance Levels

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

CENTER FOR ENTERPRISE MODERNIZATION

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