

Standard Metrics for Knowledge-Based Authentication

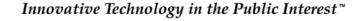
George H. Datesman, Ph.D. February 10, 2004

Topics

• Purpose

- Goal of Knowledge-Based Authentication
- Possible Outcomes of Knowledge-Based Authentication
- Standardized Error Measurement Techniques
- Qualifications Based on Measured Error Rates
- Advantages
- Disadvantages









 To Propose Standardized, Outcome-Focused Metrics for Evaluation of Knowledge-Based Authentication Methodologies





Goal of Knowledge-Based Authentication

 Error-Free Authentication; 100% Assurance that a User is Who He/She Claims to be



Innovative Technology in the Public Interest™



Possible Outcomes of Knowledge-Based Authentication

- Error Free
- Type 1 Error False Rejection of a Claimed Identity
- Type 2 Error False Acceptance of a Claimed Identity

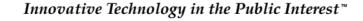




Standardized Error Measurement Techniques

- Periodic Field Follow-Up Investigations Conducted on a Representative Sample
- Periodic Penetration Testing







6

Qualifications Based on Measured Error Rates

- Standardization of Error Measurement Techniques as Opposed to Identity Authentication Methods
- Minimum Acceptable Error Rates and Confidence Intervals Established for Each Assurance Level



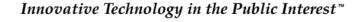


7

Advantages

- Higher Confidence in Claimed Error Rates
- Provides Realistic Basis for Comparison
- Provides Protection for Proprietary Business Information
- Encourages and Rewards Innovation





8

Disadvantages

- Expensive
- Ongoing
- Increased Oversight Responsibilities
- Ongoing Research to Improve Measurement Techniques



