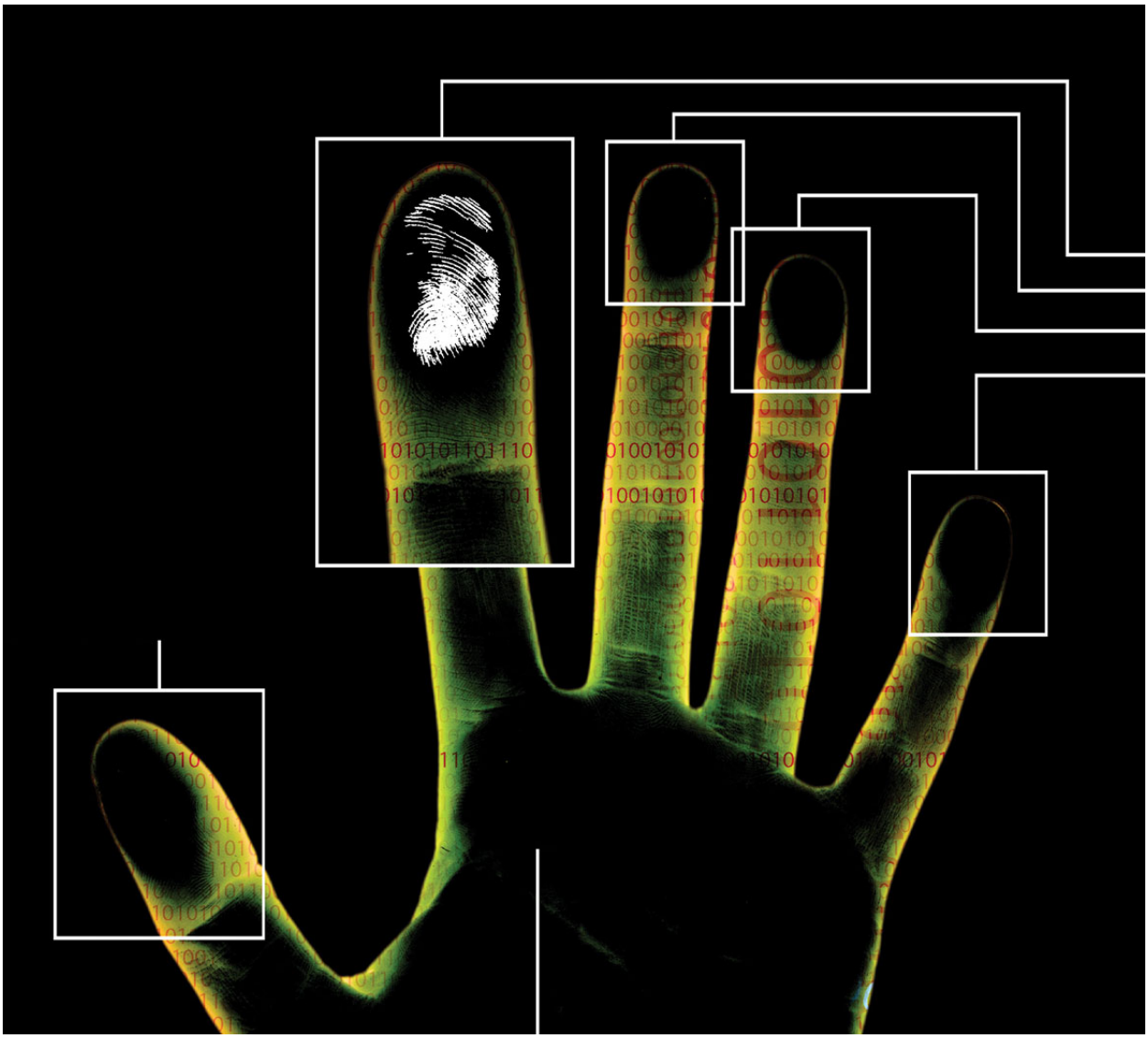
E-Authentication Best Practices for Government

Keir Breitenfeld | June 29, 2011



Every year in the United States, more than 40 million people move and approximately 3 million women change their last name. More than 13 million Americans share one of 10 common surnames, tens of millions of consumers use nicknames or initials, and 57 million males have one of 10 first names.

These realities pose complex challenges to the electronic authentication (e-authentication) process, which establishes confidence in user identities presented to an information system, for both the public and private sectors. The private sector spends more than $2 billion per year on fraud detection and prevention efforts, and government agencies must work to keep pace to ensure that their constituents and customers are protected against cyber-security threats.

Despite e-authentication challenges, government agencies must offer a variety of online services based on e-government directives, public demand and the need for greater operational efficiencies. Given the growing threat of fraud against government agencies — and the wide array of sensitive information in play — e-government is potentially a data supermarket for fraud. This means government agencies must be best-in-class in identity proofing and fraud prevention.

While the private sector faces compliance-oriented pressures, such as the Patriot Act and the Fair and Accurate Credit Transactions Act (FACTA) Red Flags Rule requirements, it has done a good job of adopting risk-mitigation capabilities and implementing processes that strike the right balance between regulatory checks, customer experience, fraud risk mitigation and cost. Given the need for citizen confidence in the security of highly sensitive information, the public sector also has the opportunity to adopt a risk-based and proportional approach to authentication — an approach which is clearly articulated in the National Institute of Standards and Technology levels of assurance and the Office of Management and Budget's (OMB) E-Authentication Guidance for Federal Agencies.

The business drivers differ substantially between industry and government, but one can argue that public agencies benefit from adopting the private-sector's bottom-line driven approach to identity authentication and fraud prevention. That's simply because these institutions — and specifically fraud managers — are in the business of adopting the most risk-predictive and cost-effective capabilities and technologies.

The OMB's E-Authentication Guidance for Federal Agencies promotes risk-based authentication by defining four authentication levels tied to consequences of authentication errors and misuse of credentials. More simply, the guidance asks, "What's the worst that can happen if a bad guy gains credentialed access?" In combining two perspectives of risk — "What's the worst that can happen?" and " What's the likelihood this individual is who he or she claims to be?" — a tiered authentication approach emerges:

Level 1 — Little or no confidence in the asserted identity's validity

- Identity proofing is not required at this level, but the authentication tool should provide some assurance that the same person is accessing protected transactions or data.
- Relevant industry tools include the use of a user identification, personal identification number, password or secret questions.

Level 2 — Requires confidence that the asserted identity is accurate

- Provides for single-factor remote network authentication, including identity-proofing requirements.
- Relevant industry tools include the use of more formal identity proofing: identity element verification, authentication and fraud risk scores.

Level 3 — Provides multifactor remote network authentication

- At this level, identity proofing procedures require verification of identifying materials and information, ideally online.
- Relevant industry tools include out-of-wallet questions, financial instrument verification and one-time passwords.

Level 4 — Provides the highest practical assurance of remote network authentication

- Authentication is based on an individual proving possession of a key through a cryptographic protocol and requires personal presence.
- Relevant industry tools include the use of public key infrastructure, digital signature, biometrics and multifactor identity elements.

These guidelines require that agencies review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. So how do you determine what level of identity authentication assurance your agency needs?

1. Conduct a risk assessment of the e-government system.

2. Map identified risks to the applicable assurance level.

3. Select technology based on e-authentication technical guidance.

4. Verify that the implemented system has achieved the required assurance level.

5. Periodically reassess the system to determine technology refresh requirements.

To illustrate the potential complexities of e-authentication, consider the following scenario:

Mary Smith takes out a student loan using her Social Security number and college address under the name Mary J. Smith. Then, using her father's Social Security number and her parent's address, Mary takes out a credit card loan under Mary Smith. Mary gets married and takes her husband's last name, Johnson, and uses his Social Security number to take out a mortgage using their new home address. She then takes out a second mortgage under her maiden name and a different home address while using her Social Security number. Later she files for bankruptcy under a new first name, Margaret, while using a different address.

Given these life events, how can an online government site verify that Mary Smith is really who she asserts to be? Many compliance-oriented authentication requirements (e.g., the Patriot Act and FACTA Red Flags Rule) and their processes hinge upon verification checks and validating identity elements, such as name, address, Social Security number and phone number.

While address verification, for example, is an important element in identity proofing, it should also be taken in context from a fraud risk perspective. Credit information company Experian has shown in recent data validations that the fraud rate associated with non-address-verified identities is less than 1 percent higher than the fraud rate associated with address-verified identities. So while such verification is important, binary conditional checks like this are not the best way to accurately predict identity and fraud risk.

Without minimizing the importance of performing such checks, there are more robust authentication tools that strengthen the process and validate identities. As you assess your organization's risk and the level of protection needed, consider the following best practices that have been proven to boost protection and prevent fraud during e-authentication:

Identity proofing — Use accurate and comprehensive public and private data sources to validate identity elements, such as name, address, date of birth, phone number and Social Security number. Employ these validated elements to verify individual identities.

Risk-based authentication — Incorporate analytics in the form of identity risk scores and a holistic assessment of a subject and transaction with the goal of applying effective but not overly intrusive or costly authentication treatments.

Out-of-wallet data — Provide consumers and constituents dynamically generated questions that are designed to segment true name individuals from fraudulent ones. This process incorporates knowledge-based authentication with an overall authentication strategy to provide an additional layer of verification.

Risk-Based Authentication

The purpose of a risk-based approach to authentication is to leverage a wide breadth of accurate data sources and quantitative techniques to further assess the probability of fraudulent behavior. The ever-changing nature of identity fraud warrants a risk-based and flexible approach to combating it. Assuming the finite pool of financial and human resources available to government agencies, a risk-based approach to managing identity fraud and citizen access allows institutions to focus on those identities and access points that pose the greatest threat to their application and citizen customers.

More institutions are implementing this type of holistic approach, rather than a rules-based program (one in which particular individual conditions are identified, detected and used in isolation or near isolation in decision-making). This risk-based approach assumes that no single rule or set of rules provides a comprehensive view of a client's identity and associated fraud risk. Instead, an appropriately comprehensive set of customer data sources can provide the foundation for very effective fraud prediction models in combination with detailed customer authentication conditions.

The inherent value of risk-based authentication can be summarized as delivering a holistic assessment of a customer and/or transaction with the end goal of applying the best authentication and decision-making treatment at the right time. Benefits include:

Reduced fraud exposure — Use of analytics and a more comprehensive view of a client identity (the good and bad) combined with consistent decision-making over time will outperform simple binary rules and more subjective decision-making from a fraud-detection perspective.

Improved customer experience — By applying the right authentication and decision-making treatment, customers are subjected to processes that are proportional to the risk associated with their identity profile. This means that lower-risk customers are less likely to be put through a more arduous course of action, preserving a streamlined and often purely behind-the-scenes authentication process for the majority of customers and potential customers.

Operational efficiencies — With the implementation of a well designed program, much of the decision-making can be done without human intervention and subjective human contemplation. Score-driven policies enable an institution to use automated authentication processes for the majority of its applicants or account management cases. This translates into the requirement of fewer human resources, which usually means lower cost. Conversely it can mean that human resources staff are more appropriately focused on the applications or transactions that warrant such manual attention and treatment.

Measurable performance — It's critical to understand past and current performance of risk-based authentication policies to allow for their adjustment over time. These adjustments can be made based on evolving fraud risks, resource constraints, approval rate pressures or demands and compliance requirements. This is why ongoing performance monitoring using authentication tools is recommended.

Best Practices

Below are some best practices to consider in the implementation and ongoing assessment of a comprehensive risk-based authentication policy:

Analytics — An authentication score is probably a primary decision-making element in any risk-based authentication strategy, so choosing and validating a best-in-class scoring model is critical in establishing performance expectations. This initial analysis will allow for decision-making thresholds to be established, acceptance and referral volumes to be planned for operationally, and benchmarks to be established against which performance monitoring results can be compared.

Targeted decision-making strategies — Applying unique and tailored decision-making strategies (incorporating scores and other high-risk or positive authentication results) to various access channels and levels of assurance that are related simply makes sense. Each access channel (call center, Web, face-to-face, etc.) comes with unique risks — recall the OMB's definition of risk as " the consequences of the authentication errors and misuse of credentials" — available data and varied opportunity to apply an authentication strategy that balances risk management, operational effectiveness, efficiency, cost and customer experience. Champion/Challenger strategies also may be a safe way to test newly devised strategies within a single channel or subsegment population without risk to an entire addressable population.

Performance monitoring — It's critical that key metrics are established early in the risk-based authentication implementation process. Key metrics may include, but should not be limited to:

- actual versus expected score distribution;
- actual versus expected characteristic distributions;
- actual versus expected out-of-wallet question performance;
- volumes, exclusions, customer velocities and mean scores;
- actual versus expected pass rates;
- accept versus referral score distribution; and
- trends in decision and result-code distributions.

Performance monitoring allows for managing referral volumes, decision threshold changes, strategy configuration changes, auto decision-making criteria and pricing.

Reporting — To apply the three best practices, accurate, timely and detailed reporting must be established around authentication tools and results. Regardless of frequency, institutions should work with internal resources and third-party service providers early in the implementation process to ensure that relevant reports are established and delivered.

As e-government customer demand and opportunity increase, regulatory requirements and relevant guidelines will become more standardized and uniformly adopted.

Regardless of credentialing techniques and ongoing access management, all enrollment processes must continue to be accurate and, most importantly, predictive of fraud risk and compliant with regulatory checks. Such authentication tools must be able to evolve as new technologies and data assets become available, as compliance requirements and guidance become more defined, and as specific fraud threats align with various access channels and unique customer segments.

A risk-based fraud detection system lets institutions make customer relationship and transactional decisions based on a holistic view of a customer's identity and predicted likelihood of associated fraud risk. To implement efficient and appropriate risk-based authentication procedures, institutions must combine comprehensive and broadly categorized data assets with targeted analytics and consistent decision-making policies to achieve a measurably effective balance between fraud detection and positive identity proofing results. The inherent value of a risk-based approach to authentication lies in the ability to strike such a balance — not only in a current environment, but also as that environment shifts in response to external factors.

Keir Breitenfeld is a senior director of product management and marketing for Experian's Decision Analytics business unit. His responsibilities include stewardship of

Experian's comprehensive suite of consumer and commercial authentication and fraud management products and services.

http://www.govtech.com/pcio/articles/E-Authentification-Best-Practices-for-Government.html