Creating an Authentication Framework: The Future of Authentication Strategy

MARCH 2017

Prepared for: Nok Nok LABS
TABLE OF CONTENTS

EXECUTIVE SUMMARY........................................................................................................... 3
INTRODUCTION .......................................................................................................................... 4
  METHODOLOGY ....................................................................................................................... 4
AUTHENTICATION CHALLENGES............................................................................................... 5
WHAT DOES AN AUTHENTICATION FRAMEWORK LOOK LIKE?.............................................. 7
CONCLUSION ............................................................................................................................ 10
ABOUT AITE GROUP ................................................................................................................ 11
  AUTHOR INFORMATION ........................................................................................................ 11
  CONTACT ............................................................................................................................... 11

LIST OF FIGURES

FIGURE 1: TYPICAL SILOED AUTHENTICATION PROCESS...................................................... 7
FIGURE 2: AUTHENTICATION FRAMEWORK APPROACH....................................................... 8
EXECUTIVE SUMMARY


Key takeaways from the analysis include the following:

- In the last three to five years, the number of authentication options for consumer-facing applications has grown exponentially. New biometrics are being added to more traditional authentication options, such as one-time passcodes (OTPs), which have also evolved to be delivered through smartphones and SMS rather than a token.

- The triad of “something you have, something you know, and something you are” continues to be the best model for multifactor authentication.

- Many financial institutions (FIs) are adopting multiple modes of authentication for different customer experiences and risk levels. Technologies such as biometrics enable FIs to combine an improved customer experience with better security. To enhance customer experience and security, FIs must ensure authentication methods are integrated and usable for customers.

- As these new authentication methods are integrated, FIs need to ensure they are improving their security stance while they improve the user experience. Implementing biometrics the wrong way can maintain reliance on server-side secrets, which are prime targets for criminals. Instead, passwords need to be replaced. If biometric data remains distributed on users’ devices, FIs can largely sidestep the patchwork of regulation springing up around biometrics.

- As threats continue to advance and biometric technologies evolve, FIs need the agility to quickly support new authentication options. FIs also need to take advantage of new hardware and software as it becomes available yet avoid massive and expensive technology projects to support and maintain these new options.

- One emerging trend is the concept of the standards-based authentication framework. This technology allows an FI to weave new authentication methods into its existing framework, test and optimize them quickly, and remove suboptimal solutions—with lower project costs and minimal operational disruption.
INTRODUCTION

Since the Federal Financial Institution Examination Council (FFIEC) first released online banking authentication guidance in August 2001, authentication technologies have been evolving rapidly. The principles laid out in the 2001 guidance (which are focused on the “something you have, something you know, and something you are” factors of authentication) still apply, yet there are now many more options for each of the three factors. The FFIEC released updates to the 2001 guidance in 2005, 2011, and 2016, but still is not keeping pace with technology and criminal tactics.1 Similar regulatory requirements exist in many countries across the globe and are often modeled on, or improve upon, U.S. regulatory requirements.

As the environment has evolved, some authentication methods have also evolved. For example, much of the personal data associated with knowledge-based authentication (KBA) questions has been compromised or posted online by the individual, severely impacting the KBA questions’ efficacy. Similarly, while OTPs were deployed by some institutions as either hard tokens or transmitted via SMS, man-in-the-browser attacks, SIM swaps, and the added friction to the user experience undermined these approaches’ effectiveness. Recently, the National Institute for Standards and Technology unveiled plans to deprecate both SMS OTP and emailed OTP tokens.2

Authentication capabilities and use cases have been further expanded with the spread of smartphones, tablets, and laptops that include multiple sensors, such as fingerprint readers, cameras, GPS, gyroscopes, and accelerometers; wearable devices have added new biorhythm options as well. Many technologies already in consumers’ hands offer a variety of authentication options; the challenge for FIs is to evaluate and incorporate them in an integrated manner that provides improved customer experience and security, enhanced privacy, and lower costs.

This white paper describes strategies that improve customer experience and security. It focuses on the technology and integration required to create an authentication strategy that supports flexibility, agility, and reduced costs.

METHODOLOGY

Aite Group interviewed a number of executives from Tier-1 and Tier-2 U.S. financial institutions in Q2 and Q3 2016 to better understand their strategies for authentication across channels and how they currently coordinate their authentication efforts or plan to do so. This white paper also contains analysis from ongoing, in-depth Aite Group interviews with senior fraud executives at U.S. and European banks.


AUTHENTICATION CHALLENGES

Authentication has become a key component in remote channel experiences, including contact center, ATM, mobile, and web interactions. Every channel has unique authentication constraints and assets to enable authentication. So much personal information is exposed on the Internet voluntarily or through data breaches that methods used in the past, such as usernames and passwords, are crumbling and ineffective.

FIs face a number of questions when it comes to determining authentication approaches and strategies:

- What authentication methods in use are effective—and at what scale?
- What new authentication methods might prove easier to use, more effective, and more appealing to customers?
- How would these new methods impact the online and mobile customer experience?
- How would the introduction of a new authentication method impact operations?
- How much does the authentication method cost to acquire, deploy, integrate, maintain, support, and operate?
- What criminal techniques are already available to circumvent the authentication method, and what are potential future threats?
- Where are potential security gaps that have not been exploited yet?
- How can the risk of an activity select the appropriate type(s) of authentication?
- How can the firm agilely test or implement new authentication options with minimal additional investment and disruption?

These are just a few of the strategic questions FIs should be asking themselves, and each organization will have a different perspective. But there is also a larger strategic question FIs should be asking: When supporting multiple interaction channels with differing capabilities and different risks, how can an institution create the optimal user experience? Considering that user experience and customer adoption are the main drivers for authentication effectiveness, firms must look for ways to make enrollment and day-to-day use as simple as possible across every channel.

As an example, a large European bank sought to improve security through stronger authentication. Customers were issued chip card readers that would create an OTP when the debit card chip is inserted. The user experience was very cumbersome, especially on mobile. As a result, customers started using online banking less and used higher-cost channels, especially the call center, for day-to-day needs. In this case, the poor user experience led to low adoption and higher costs.

Additionally, when implementing a new authentication system, FIs must keep in mind the security profile they are implementing and whether it is truly achieving the objective or merely
adding some window dressing that criminals can ultimately compromise. For example, some biometrics implementations do nothing more than copy a password from a cache and paste it into the receptive field. While this satisfies the demand for a better user experience, it does nothing to improve the security stance vis-a-vis authentication.

To address these challenges—user experience, cost, and security—FIs need to be flexible and address three key topics:

- Technology and integration
- Process changes and improvements
- Staff and customer education and training

Without a flexible and standards-based authentication framework, institutions will continue to face high costs in testing and adding new authentication tools as well as long implementation timelines. To solve this, industry standards can enable institutions to move more quickly and cost-effectively.

One growing and flexible standard is the FIDO® specification. By conforming to such a standard, vendors can create solutions that are easier to deploy, weaving new capabilities into the authentication framework and putting less onus on financial institutions to change internal code. FIs benefit from being able to plug in solutions based on the standard, significantly reducing time to market as well as testing and deployment costs.

It is important today to view authentication as a journey rather than a destination. What might be an appropriate authentication for one part of a user interaction may not be appropriate for other interactions, and additional authentication methods or procedures may be required. This process must be adaptive to new risks, devices, and device capabilities as well as changing expectations for customer experience.

---

WHAT DOES AN AUTHENTICATION FRAMEWORK LOOK LIKE?

Speaking to a number of large U.S. financial institutions, there was a clear theme: Many are working toward an authentication framework that can incorporate and coordinate authentication options based on a number of inputs, such as transaction or session risk monitoring, access channel, and customer experience impact. The core idea behind a framework is the creation of a flexible platform whereby multiple different features of authentication can be integrated seamlessly together.

Some FIs have been building their own internal frameworks to coordinate and orchestrate various authentication options, risk profiles, and user preferences. This approach enables total control, but with that comes very high implementation and maintenance costs. Other FIs are implementing new authentication methods, such as biometrics, piece by piece with little interoperability and integration, leading to a mishmash of authentication methods in different channels and a confusing customer experience. This approach also limits the ability to measure the authentication program’s performance and make improvements (Figure 1).

Figure 1: Typical Siloed Authentication Process

Source: Aite Group
An alternative approach is to leverage standards, such as the FIDO® specification, combined with an integration framework that can coordinate authentication methods. FIs can more easily incorporate new methods and include reporting and monitoring tools. This approach provides agility and lowers project and maintenance costs, and can help improve the customer experience. Leveraging authentication standards can help avoid vendor lock-in as well as simplify proofs of concept or pilot projects and allows institutions to rapidly adopt new authentication technologies as they become available (Figure 2).

**Figure 2: Authentication Framework Approach**

![Authentication Framework Approach Diagram]

This approach attempts to address key concerns for financial institutions.

- **Enrollment and identity binding:** This process is one of the most challenging and is one of the most important steps in the authentication life cycle.

- **Compliance with current and future regulatory guidance:** While the guidance provides minimum standards for authentication, compliance is still important. For example, the recent update to the U.S. FFIEC Payments Services Handbook contains the new Appendix E, which highlights the need for strong authentication in the mobile environment.  

• **Minimized fraud losses:** Losses due to account takeovers, social engineering, and scalable attacks against traditional user name/password and shared secrets infrastructure can be prevented.

• **Minimized costs and vendor lock-in:** There is a significant amount of innovation in authentication and biometrics in particular. Institutions need to become more agile and able to embrace new technologies quickly and with low costs. Standards such as FIDO® specifications can help maximize flexibility and minimize the chance of being locked into aging technology.

• **Customer experience:** Improve and simplify the customer experience by minimizing inconvenience while maximizing security.

Until recently, most institutions leveraged native vendor application programming interfaces (APIs) for biometrics authentication, which are often incompatible. Substantial technical expertise is needed to effectively leverage various proprietary APIs securely. This approach increases integration costs, maintenance costs, and time to market to add new authentication methods, and it limits flexibility as new modalities emerge.

Many FIs are now looking at a more strategic and integrated approach to authentication by leveraging an authentication framework. This approach enables risk-based authentication with the flexibility to quickly integrate new technologies and avoid vendor lock-in. This strategic approach can help institutions prepare for inevitable technological evolution and future regulatory changes.

Around the world there is a great amount of authentication activity, particularly in the mobile channel. Mobile offers a great range of sensor inputs and interaction modalities, and as such, many authentication options in one device. This has driven many institutions to rethink biometrics, starting in the mobile space. Institutions are at various stages of evaluating and testing a variety of solutions as well as deploying at least some biometrics capabilities.

Anecdotally, institutions that enable biometrics (often Apple’s Touch ID) are seeing increased customer engagement, especially in mobile, which means even more opportunities to cross-sell and up-sell while providing convenience to the customer. Most institutions report that they see strong initial adoption that then tails off—continued communication, especially with new account holders, helps improve overall adoption.

It becomes important to support a variety of biometrics authentication options across a number of devices with varying capabilities. The best way to manage this is through a flexible authentication framework that can support these current challenges and looks forward to what might come in the future.

---

CONCLUSION

An authentication framework approach offers advantages such as improved agility, reduced costs, and improved customer experience.

- Authentication provides a key component of fraud prevention; emerging biometrics solutions, especially with mobile, can be key drivers of customer experience.

- Financial institutions that view authentication holistically, incorporating all customer interaction channels and all authentication methods, have the best chances for success today and going forward.

- A standards-based authentication framework can enable agility to support new types of authentication in the future with lower technology acquisition, integration, and maintenance costs.

- An authentication framework can also set an institution up for success as regulations and technologies evolve.

- Institutions can more easily manage and evolve the customer experience, across channels, with an effective authentication framework.

Key recommendations for FIs follow:

- Evaluate and map how different authentication methods are used within the organization, in different channels, and in lines of business.

- Map these against security and customer experience goals to identify gaps and opportunities.

- Consider that there is not going to be a one-size-fits-all approach to authentication, particularly with mobile. It is critical to evaluate a number of modalities and potentially choose more than one.

- Leverage a standards-based authentication framework such as FIDO® specifications to improve agility, lower costs, and enable positive customer experiences.
ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com