Building the Business Case for Strong Authentication

The importance of strong authentication

To ensure customers are able to conduct financial transactions whenever they need, from wherever they are located, financial institutions have increased access they provide to critical internal banking applications. Supporting and protecting this anytime, anywhere access, however, is increasingly difficult using traditional security measures. Not only are access requirements growing, but the threat landscape continues to evolve, with attacks increasing in frequency and sophistication.

Any financial institution or business that offers Internet and mobile banking, online financial services, alternative payment solutions or an e-commerce website is a big target, due to the sensitive and potentially lucrative nature of their information and transactions. They are likely to face targeted man-in-the-browser (MitB) trojans, viruses, key-loggers, rootkits, browser redirections and other malware, as attackers try to execute fraudulent transactions that often result in millions of dollars in losses. Businesses must maintain the integrity of their online platform and ensure that every user interaction is trustworthy and legitimate.

While there are existing authentication methods in place, these methods are considered dated and should no longer be the standard for protecting a customer’s assets. For example, the European Union Payment Service Directive II (EU PSD2) mandates that starting from 2018 all banks in EU will need to have strong 2-factor authentication. Currently several worldwide banks use only a password to protect their customer account. Besides a password (something you know), users will need to have a second factor—either something you have or something you are. Although the technical standards driven by EU PSD2 will be specified by the end of 2017, we already see that in a lot of EU countries tan lists (code cards) will not be allowed to be used anymore. The reasoning behind this is that tan lists (and most likely also SMS) are considered 2-step verification instead of two-factor—people need to know the code they apply.

New regulations (like PSD2) are also aiming to set out a harmonized framework that is to ensure an appropriate level of security for consumers and Payment Service Providers (PSP), for performing transactions effectively, allowing for the development of user-friendly, risk-based, accessible and innovative means of payment for their customers. Today’s accelerated provisions for access-to-account cause financial organization interest in Open APIs and Open Banking initiatives which could pave the way to enhanced innovation and customer relevance, industrial partnerships with the larger ecosystem of Fintech market participants.

While financial institutions know they need to add security, they can’t afford to add time or complexity; they need a way to support all the access requirements of their customers, while appropriately balancing the costs and security requirements of their business.

The Problem

If you notice the evolution, you are able to understand the dynamics of the rapidly changing digital commerce space and identify opportunities and threats that digital businesses face. The growing number of threats and attacks creates a constant arms race during which financial institutions have to learn about those threats, detect them, analyze and protect against them.
As an increasing number of customers use their smartphones or mobile devices to conduct transactions (Juniper estimated more than 1 billion mobile banking users by end of 2015¹), financial institutions must be able to support and protect them. This is an ever-growing problem, as the number and sophistication of malware that can infect an end-user's device only continues to grow. An obvious challenge for financial organizations is how to keep their services convenient and secure. On top of this the cost of the implementation and maintenance is not negligible.

What to Look for in an Online Banking Security Solution

Banks benefit economically not only when they sign on more online banking customers, but also when those customers use the Internet and mobile banking services with greater frequency, especially for fee-based services. There already is considerable data identifying customer segments—typically younger, technically savvy and mobile-centric audiences—that are using mobile banking services several times a day².

In order to ensure suitable online banking security measures—without compromising on user convenience—banks should look for certain key capabilities in an Internet and mobile banking security solution:

- **Support for an integrated, multi-layered approach.** Online banking customers expect to be kept safe even if their behavior is not in line with cybersecurity best practices. Solutions that utilize a wide array of authentication methods to identify the customer and provide end-to-end protection at the device, the app, the connection, and the backend server are typically the most resilient.

- **Ability to easily assign and configure multiple authentication methods to different audiences.** Look for a solution that is highly configurable, supports multi-tenancy, and can apply any combination of multiple authentication methods across different banking channels, user populations and banking divisions according to role and policy. Such an approach will allow the bank to lower its cost of operations by managing all of its authentication needs from a single centralized platform—even if it operates through numerous banking divisions and entities located globally. It will also allow customers who have multiple accounts with the bank to log on to these accounts with single credentials, thereby improving user experience.

- **Threat intelligence gathering to spot potential problems based on risk analysis before and after they infect the system and users' devices.** The best online security solutions anticipate and recognize potential threats—both known and emerging—and can use contextual information to correlate the threat surface against expected user behavior, device configurations and the threat profile.

- **Strengthened compliance frameworks.** Compliance regulations are far more than a prescribed method for passing an annual audit. Being in compliance with requirements such as PSD2, FFIEC, SAMA and other mandates strengthens the entire security chain for mobile banking, reducing risk for the banks and increasing consumers’ confidence. Your online banking solutions should support compliance frameworks as integrated functions, not as add-ons.

- **Strong authentication without impacting user experience.** While it makes sense to use two-factor (or more) authentication for mobile banking security, users don’t want to spend a lot of time validating their identity and user privileges in order to check balances or pay bills. Customers’ efforts can be minimized without compromising on security by running

---

¹ Juniper: "Worldwide Digital Banking: Mobile, Online & Wearable 2015-2020"
² Mobile Banking, Mobile Payments: What Consumers Value," RateWatch (The Street, Inc.) April 2015
most authentication methods “behind the scenes” so that user involvement via a step—up authentication is only required when absolutely necessary according to policy settings and risk profile.

The need for Mobile Security Solution

While banks may already have had some security frameworks in place for online banking for some time, those defenses are not adequate for the unique challenges of mobile banking. As a result, banks that attempt to leverage existing online banking security infrastructure and tools will find their risk profile much higher than if they adopt more mobile oriented solutions.

Some of already existing authentication methods, like SMS, have become unsecure and not compliant with the regulations of financial organizations. The costs associated with those methods are also becoming a challenge when defining and maintaining the service targeting a wide audience. FFIEC in its last Mobile Security Guidance document deprecates SMS 2FA since it introduces risks, including someone simply reading the 2FA code from a lock-screen notification.

HID Global recommends financial institutions to take into consideration new regulations (like European Union Payment Security directive II, PSD2) when designing and choosing their authentication platform so requirements of their security and legal teams are duly accomplished. The PSD2 requires users to authenticate with a minimum of 2 out of the following 3 authentication methods: knowledge (e.g. security questions), possession (such as a mobile device) and inherence (such as fingerprint or retina data). Additionally there are certain requirements for these authenticators defined in the PSD2 mandate have led some analysts to consider SMS OTPs as not being compliant to PSD2, due to lack of confidentiality of the authentication material.

Other factors that are driving Mobile banking:

- Mobile devices, along with your house keys and wallet, have become one of the three must-have items when leaving the home, and they may eventually become the only must-have item. Because of their ubiquitous nature, and the wide array of sensors that they contain such as GPS, pressure sensors and biometrics, mobile devices themselves can become part of a user authentication strategy.
- The mobile experience is all about convenience, and users expect a seamless experience when accessing apps, services and content, without having to think too hard, if at all, about security. They expect the bank to ensure that mobile banking is secure.
- Mobile devices support “always-on” email, SMS, browsing and a gesture-based approach to using mobile apps which makes mobile devices more vulnerable to an increasing array of security threats, such as phishing, social engineering, malware, malvertising, advanced targeted attacks and zero-day attacks.
- Reliance on Wi-Fi and other mobile network technology, instead of wired networks running over carrier-class wide-area networks.

In order to safely deliver mobile banking services, and to make consumers more confident in the safety of banking on their mobile devices, banks must provide multi-layered security. Their solutions must address potential challenges at both the front end (consumer devices) and the back end (banking systems that recognize and facilitate legitimate user requests through mobile devices).

Consider Solutions From HID Global

One of the leading and most experienced suppliers of security tools for mobile banking is HID Global. The company is a reliable and trusted supplier of solutions for the banking industry, with a wide range of products and services targeting classical online services, but also aimed specifically
at mobile banking use cases. HID Global’s solutions protect against banking fraud and data breaches that often are initiated through PC or mobile devices, as well as ensuring the safety, privacy and accuracy of customers’ data when accessing online banking services. The company’s strong authentication and network security technology is designed to detect and defeat attempts to clone or forge identities and perform account takeovers through PC or mobile devices. HID Global’s solutions are based on a multi-layered security architecture that verifies identities and creates a trusted environment for online banking users.

At the heart of these solutions is the ActivID® Authentication Server, which provides an effective, multi-layered protection against account takeovers resulting from phishing attacks. With the ActivID Authentication Server, organizations can tailor their authentication methods for specific groups of users, based on their business objectives and police/regulatory compliance needs. The ActivID Threat Detection Service can protect consumers against cybercrime, automatically guarding customer data and helping to defend against fraudulent access, malware and breaches. With no impact on the user, it protects online transactions from a wide range of threats; including Trojan and man-in-the-browser (MITB) attacks where consumers are directed to infected versions of what seems to be a legitimate banking website. ActivID Threat Detection Service relies on contextual information to help banks detect and prevent fraud from compromised PC and mobile devices or accounts.

The ActivID Trusted Transaction SDK for mobile banking applications relies on a unique concept of a secure channel established between the bank and the customer’s mobile device and uses push technology to send a real-time out of band notifications, thereby providing a turnkey 2FA solution. Coupled with the ActivID Threat Detection Service, step-up authentication can be triggered in the event of a transaction looking unusual or corresponding to a high-risk request such as setting up a new payee or initiating a high-value transfer. On receiving the alert the customer can approve the transaction by pressing a button or typing an optional PIN. Thanks to ActivID Trusted Transaction, the user knows exactly what data transaction is to be validated; they are in full control of their eBanking customer journey. This reinforces their trust in the service. In the same time, the solution protects against unsecure behavior from the end-users.

ActivID Authentication Server supports the broadest range of authentication methods, from strong passwords to certificate-based authentication, including KBA (Knowledge Based Authentication), two-factor hardware tokens, soft tokens, device forensics, and SMS Out-of-Band One-Time Password (OTP) options. Different authentication algorithms are supported: proprietary to provide additional functionalities, or OATH and PKI to be able to use standard tokens.

To ease the deployment, HID Global’s solutions are built on open standards that promote interoperability, scalability and reduce implementation time and cost of ownership. The solutions also come with integrated analytics and reporting tools that spot problems before they become widespread, while alerting key decision-makers about potential threats and steps to take in ensuring data privacy and integrity.

The result is a full online banking security framework that creates trust for users and ensures adherence to compliance and governance requirements for IT organizations. This drives greater use of online banking services and products, resulting in incremental revenue for banks without creating undue risk. The end-user is secured and in-control without additional hassle.

Integration of HID Solutions

HID Global's ActivID Authentication Server provides corporate, financial and government organizations with risk-appropriate, cost-effective user authentication. The solution enables end
users to have convenient anytime, anywhere access to sensitive data from their smartphones, tablets, computers and virtually any other device.

Deployment is simplified, too, through the platform’s pre-integration with major cloud apps, VPN systems, application servers, banking applications and other third-party systems.

Available on-premise, ActivID Authentication Server can also be delivered either as a hardware appliance or as a virtual appliance, which helps to reduce costs with easy installation, eight years token lifetime, and simple integration into an organization’s existing network infrastructure. As banks enhance online and mobile channels in response to competition and user demand, they must successfully address risks associated with authenticating their customers and employees, and integrate their respective front-end and back-end systems with a central ActivID Authentication Server.

ActivID Authentication Server implementation consists of integration the ActivID API into the Front-End/Back-End systems existing in the Bank. The main functions to be accomplished are the following: authentication and transaction validation, user management, help-desk, audit. As an example to accomplish those needs HID Global delivers an ActivID Appliance pre-configured for Temenos - one of the Front-End/Back-End vendors. Appliance is ready to work with Temenos T24 Core Banking (T24), Temenos Connect Internet Banking (TCIB), Temenos Connect Mobile Banking (TCMB), as a versatile authentication server all in one cost-effective solution.

The following diagram outlines the high-level architecture of the ActivID Appliance integration with Temenos components.

ActivID Appliance is pre-configured for banks using T24 and Temenos Connect Digital Channels platforms. In addition, HID Global can assist with deployment related to any of the bank’s unique system environments, and ensures a secure key generation process. This allows the appliance to be easily restored or replaced in case of hardware faults or disaster recovery.

At time of deployment, the implementation services team assures proper integration into the bank's ecosystem. Customers may opt for additional services, such as customizations and projects related to Connect Internet online banking security, including support for PIN mailers and other associated projects.

The ActivID Appliance can be deployed in a redundant configuration to ensure fault tolerance and high-availability for their mission-critical authentication systems.

The ActivID API is exposed though SOAP service defined Web Services Description Language (WSDL) using a defined Web services interface that can be used to create client implementations.
that are on different technology stacks. Other Front-End/Back-End banking systems are integrated with ActivID Authentication Server in a similar way to Temenos as depicted on the following figure:

ActivID Authentication Server can work concurrently with legacy authentication servers for graceful and efficient migration or it can accommodate new authentication methods as they become available. This is achieved thanks to an extensible framework into which organization can add additional authentication methods using custom adapters.

For user repositories ActivID Authentication Server can rely on its internal database or additionally it can integrate with Active Directory and most standard LDAP. This allows it to address internal security needs with a strong segregation between different user populations with enhanced Security Domains.

Integration of HID Mobile solutions

ActivID Trusted Transaction is a push-based validation solution whereby transactions, for example banking transactions, can be digitally signed using cryptographic keys stored on a user’s mobile device (smartphone or tablet). The following is a common scenario representing a secured banking transaction using the push-based validation solution. This scenario could apply to any ‘Logon request’ validation or ‘Action’ validation, making this solution highly adaptable to a dynamic market. It offers varied possibilities of seamless pushed-based feature integration within a complex business environment.

1. A user initiates a transaction (making a purchase or transferring money) on a commercial or banking web site.
2. The web site initiates secure transaction verification which results in sending the push notification to user mobile device. The user receives a notification on their device and opens it to review the details. For privacy and security reasons, the push notification networks are not used to send transaction details or the response to the transaction. Instead, the mobile application uses its own secure communication channel.
3. A Secure Channel is established between the mobile application and the ActivID Authentication Server so the transaction details are transferred and displayed on the mobile device for review, for example, “buy a DVD from your debit account for $10” or “transfer $25,000 from your company bank account to company XYZ bank account”.
4. The user validates (or declines) the transaction on their device.
5. The response is sent from the user’s device to ActivID Authentication Server and next to the Internet Banking Server, with information that the transaction is approved (or declined).
6. The web site receives the response and replies to user’s validation (or decline).

The following picture presents the workflow of transaction signing using ActivID Trusted Transaction SDK in a mobile application. Other scenarios, like logon or secure code generation are also available.

The authentication and signing functions of ActivID Trusted Transaction can be made available to the existing mobile banking application via ActivID Mobile API integration.

The current version of ActivID Authentication Server is delivered with code samples for Bank mobile application based on Android, iOS, Windows Phone.

ActivID Trusted Transaction API relies on highly secure cryptographic standards (AES 256, RSA 2048, ECC-DH). ActivID Trusted Transaction mobile application leverages PKI technology for the push-based validation. The private key is protected (preventing extraction or cloning or access from another application). The same device can run multiple Services that call the ActivID Mobile Signing SDK, but each Service is separate and does not share credentials. For example, a user with two bank accounts (in two different banks) can register for a service from each bank using the same mobile device.

The solution supports Trusted Execution Environment (TEE) on Android, that is, devices with “Hardware-backed credential storage”. Alternatively, devices with no TEE present will use “Software credential storage”.
Benefits of HID Solutions

1. User Convenience
   a. Easy to use: Mobile Push technology with straightforward approval process
   b. No need to type one-time passwords
   c. Frictionless Threat Detection

2. Cost-effective
   a. Single platform consolidating all authentication methods
   b. Expandable to support new authentication methods
   c. Mobile Push techniques eliminating costly SMS, requires no additional hardware token
   d. Pre-built integration with Temenos T24/TCIB/TMIB

3. Flexibility
   a. Multi-Tenancy on back-end site and on client site
   b. Support for multiple authentication devices
   c. New authentication methods can be added as they arise
   d. Rich API’s available for in-house development and for sharing banks’ services in the Fintech ecosystems.

4. Compliance
   a. National regulations, e.g. FFIEC in US, SAMA
   b. Multinational regulations, e.g. PSD2 European Directive

5. Security
   a. Broad security scenarios supported, i.g. authentication, challenge/response, transaction signing
   b. ActivID Trusted Transactions Mobile Push:
      i. PKI-based digital signature
      ii. Secure channel for data replacing unsecure SMS
      iii. Secured provisionning protocol
      iv. Mobile application security (RASP, jailbreak and rootkit detection, debugger and emulator detection, code obfuscation, tamper detection, …)
      v. Key protection (anti-cloning, Device ID, …)
   c. Hardware tokens with customer managed secrets
   d. Legally binding Tamper-Evident audit log
   e. Works optionally with FIPS 140-2 HSM to secure an organization’s keys.
   f. Support for TEE (Trusted Execution Environment)
   g. The mobile application and the server application follow the OWASP best practices
   h. The mobile application and the server application have been audited by independent laboratories.