Security as a Bridge for New Financial Services

Edward Scheidt

20 November 2018

Introduction

Decisions are being requested that will impact future financial services. Missing are new roles for security to establish trust and acceptance as digital architectures impact the way business can be done within financial services. There is a quest for faster payments and related real-time interbank settlement while from a security perspective the subjects of three main security criteria found in Identity, Authentication, and Authorization are viewed as disparate use cases. On the scene is digital currencies which are bringing new digital technologies to the existing financial ecosystems and requesting international direction, and they, too, will need security to bridge the potential assortment of what the financial market is defining for future digital currencies. The result from this potpourri of request and actions will lead to a review of the roles for security. In the balance will be whether trust and acceptance can be extended to cross-border financial transactions, and the goal of faster payment architecture can be secured within the US borders and extended beyond the US borders.

Background

The Financial Digital Ecosystem and real-time interbank settlement: The Federal Reserve published an October 3, 2018 network press release requesting the financial community and the public to comment on improving the overall safety of the faster payments market in the United States (US). The Federal Reserve is considering whether to develop a service for real time gross settlement (RTGS) of faster payments. To expand the RTGS service usage, a liquidity service capability could support funding needs as a real time action and take advantage of digital technologies. A further goal would be to take advantage of existing private settlement rails for internal financial entry's processing with connectivity to a new real time interbank settlement. Timing of a new RTGS service may be aligned with the integration of ISO 20022 payment messaging. How and when, as a global process would result in an architecture that is beyond the scope of this document. There would be a dependency relationship between security functionality and a global settlement process which could include ISO 20022 messaging.

Payment needs: The banks or financial institutions involved in a payment must have a way to receive and exchange payment messages. To complete a payment between two banks or equivalent virtual entities, three key levels of the payment process are necessary: end-user services, clearing services, and interbank settlement services (RTGS). A payment message typically contains information related to the payment, such as Identity of the parties involved, relevant account information, and the payment amount. Without a payment message and a method to exchange it, the banks involved in a payment would not know the details of a payment. In practice other information may also be included. Clearing activities may also include screening for fraudulent payments and other risk management measures. The roles for security extend into abstract considerations associated with identity and its various available digital access management capabilities, authentication and new variants of party validation processes, and authorization leverage access and protection at the object content level. Today, *security may travel with a payment and be executed independent of the network supporting the communication channels for the content. Security can also be packaged to result in a multiple step process contained in a single secure object coded message.* And, let's not forget that a financial ecosystem can support itself, but it needs to be able to also support the end user: the consumer, with assurances for trust, privacy, and confidentiality.

A Security Snapshot

Introduction: The mechanics of security must lead to trust and other assurances in which the financial ecosystem can support while it adapts to the changing digital world. The paradigms associated with security have been threatened in conjunction with a static-like financial infrastructure which is seeking dynamic needs to accommodate financial services wants.

We can think of security in various abstract terms such as Identity, Authentication, or Authorization and have built the current financial security ecosystem in these terms to accommodate an understanding of a dynamic threat which appears to include excessive resources.

The Security Balance Sheet: The security balance sheet for the financial ecosystem continues to shift to-and-for protection and compromise. However, a crystal-ball view of the future must also include another dimension for security which could be significant for the security balance sheet. - The digital models that are used by the financial community have been shifting to putting emphasis on the end financial actions and less focus on the middle supporting processes. – The supporting communications, linking rails, and digital paths are providing the state-of-art for the financial community, but its security is left to linkage protection of an older era. The need for persistent protection at the end financial actions is available as a digital

container or a digital object. A visualization of succinct objects representing new digital representation being aligned with the mechanics of security can result in a stronger bridge between digital representations and security support.

Moving Object Related Security into a New Financial Services Landscape: The Federal Reserve is asking for concurrence to establish a new financial service which advances faster payments and related real-time interbank settlement processes. These processes will be represented as digital applications. To be affective as a faster implementation, the newest digital technologies as object forms will be included, yet, the makers of security services may not take advantage of an opportunity to shift efforts for an object support . The financial community could be forced to morph security services with capabilities that the threat has access for many years and has demonstrated a neutralizing- understanding. Another dimension for security also must consider interoperability within the digital environment which can lead to security issues associated with implementing security into their support digital applications. – The point is that security considerations must include various operational perspectives and potential implementation errors. Having security closer to a digital application and its supporting functionality objects calls for a parallel supporting role for security as objects. Security objects can be modules that do defined protection capabilities such a privacy while taking advantage of a security tool that performs a cryptographic assurance capability. An example is an object oriented cryptographic key management that supports using cryptography exists as ANSI x9 standards; X9.69, x9.73 supported by an ISO standard, ISO 11568. Of course, these security tools include other capabilities which can be aligned with financial object models. Standards are important to security to ensure a common acceptance among national and international entities.

An Opportunity to Leverage Selected Security Techniques as a Policy Enforcer: A benefit with security with object functionality is that security technology exists that can bridge the analog actions found with policy and digital actions to execute desired financial services action. In additional to the faster payment and settlement wants, another financial action is pending; to add ISO 20022 messaging with its complimentary business defining messaging as another financial service which will seek efficient coupling to the existing US financial infrastructure(s). Policy can be exhibited through the business defining messaging and enforced through security tool(s). However, to ensure efficiency through a security thrust into the US financial ecosystem and a future ISO 20022, object level security offers a new opportunity to couple security and financial service visions.

A Fundamental Question of How to Bridge Security Among New Financial Services: Aligning security modules into the vast financial services can be complex when a big picture is addressed. And, dealing with details can add to the complexity. It is possible to begin by examining security in the context of Identity, Authentication, and Authorization wants, and then align the security wants with the financial digital applications themselves. Further defining the How will lead to specific security technologies which can be put into a business use case. We must not forget that security technologies are also evolving and can be impacted with technology advances such as quantum computing. Object modeling for security can break down the complexity within digital usages, to handle subjects like privacy and confidentiality, with a modular security design that can bring to bear enforcement. Kits are available now, a support such a future reality.

All the Payment needs, identified earlier, can be realized once object-oriented security is implemented. With a dynamic view of security, the Federal Reserve would have one potential obstacle removed and proceed to a new definition for a faster payment capability.