Harvard University Extension School ISMT E-599
05/04/2017 Spring 2017

Team 5

Dynamic Multi-Factor Authentication For Securing Banking Transactions

Capstone Final Paper

By:

Christopher Martinez Servin

Merrill Raman

Nick Wright

Kamran Zameer

Table of Contents

Executive Summary

Client Introduction

Bank of Cambria is a U.S. based consumer bank with assets of 100B under management. It has a large retail footprint with many offices in all 50 states. The bank offers standard banking services which include checking and savings accounts, loan and credit facilities. In order to compete with the vast number of internet-only banks and embrace digital banking, Bank of Cambria has created an online client portal that allows clients to manage their banking accounts and conduct various banking transactions via an online interface.

Consulting Firm

Sigma Tech is the creator and provider of a security platform that can be used to enable multi-factor authentication services. It's platform augments the existing authentication systems of organizations and protects against unauthorized access to data and applications. Bank of Cambria has contracted Sigma Tech to augment the current authentication system to protect client data and improve transaction security for the bank.

Problem Statement

In 2012 Bank of Cambria launched a customer portal that allows banking customers to perform a variety of banking transactions electronically. This portal was well received by its customers with over 50% of them conducting transactions via the portal. In 2014, the bank followed up with publishing an app in the iOS and Android marketplace. In 2016 Bank of Cambria reported that over 75% of its customers used its portal or app to conduct banking transactions.

This increased electronic transaction volume has come at the expense of increased fraud. In 2012 the number of fraudulent transactions increased by 50% and the bank reported fraud related losses of $50M. In 2014 the bank reported losses of $100M. An investigation of the vectors associated with the fraudulent transaction reveals the primary cause to be impersonation through the use of stolen credentials.

Solution

Sigma Tech has identified the primary problem to be weak authentication methods. The current methodology which comprises of a username and password to gain access is inadequate and lends itself to easy impersonation. As a solution, Sigma Tech recommends that the Bank of Cambria implement a secure Dynamic Multi-factor Authentication (DMFA) system to bolster the security of clients and transaction and minimize impersonation.

Multi-factor Authentication (MFA) is an authentication scheme that requires more than one type (factor) of information to verify the authenticity of a user. Typically, the factors fit within the information categories of knowledge (something the user knows), possession (something the user has) and inherence (something the user is). Examples of factors can include:

- Knowledge Factors: Username & password, pin number, pattern & image recognition etc.
- Possession Factors: Cell phone, tokens, keys etc.
- Inherence Factors: Fingerprint, voice, retinal information etc.

By employing such a scheme, the risks associated with unauthorized access are greatly minimized as a fraudulent agent will need to possess multiple pieces of disparate authentication information to successfully navigate the authentication process.

DMFA takes this concept of multi-factor authentication and builds upon it by allowing the different factor groups mentioned above to be mixed in various ways to meet different risk levels.

For example, let us consider two scenarios:

- Scenario A: User prints out his bank statement.
- Scenario B: User sends a wire transfer for $5,000 USD to an account number.

Scenario B requires more scrutiny than A and therefore under a DMFA scheme, to conduct the transaction defined in Scenario B, the user will need to verify identify more conclusively (using more factors or factors with higher credibility) as when compared to the verification process to conduct the transaction in Scenario A.

Part 1: Business Requirements

“As-is” Business Process: Username & Password

The current state of authentication at Bank of Cambria utilizes a standard username and password mechanism for securing access. The client sends an access request to the server and the security agent verifies that the provided combination of username and password matches in the Bank’s credential database before granting access. This mechanism incorporates strong password measures to offer protection against brute force attacks and data leakage. This mechanism, however, does not protect against stolen credentials and anyone with a stolen username and password is able to conduct transactions in the customer portal.

“To-be” Business Process: Dynamic Multi-factor authentication (DMFA)

The to-be business process involves the implementation of an authentication system that supports multiple factors. Each factor will have an authentication score set by Bank of Cambria. Depending on the type of transaction performed, the risk engine in the authentication system will require an authentication factor or a mix of factors to meet the minimum authentication score before the transaction is allowed. For example: To log in to the customer portal (a low-risk transaction), the required authentication score need not be high and therefore may be satisfied with a single factor (username and password). However, to initiate a wire transfer (a high-risk transaction), a higher overall authentication score is necessary and therefore a confluence of factors to meet the minimum authentication score. Hence, when a customer who has logged in with a username and password (carrying a low auth score) attempts to perform a high-risk transaction, the system will automatically invoke an additional authentication process with a list of available registered factors for the user to use to meet the minimum auth score for the transaction to complete. Development of authentication factors will be provided by external vendors. Also, the development of the Risk Engine is outside the scope of this project as there is already an existing system (Bank of Cambria) used to block user transactions based on historical data.

Functional User Stories

1. *As a customer of Bank of Cambria, I want to login to my online portal easily and securely.*

- The online portal can be accessed via the web or mobile applications.
- The user shall be able to authenticate identity using an authorized single factor

2. *As a customer of Bank of Cambria, I need to be able to perform my banking transactions online.*

- Once logged into the portal, the user will have the ability to perform banking transactions like wire transfers, bill pay, address change etc.
- All transactions have a required authentication score associated with them. The system will ask for additional factor based authentication if the transaction to be performed requires an authentication score which is not met by the factor used to log in.

3. *As a customer of Bank of Cambria, I need to prevent fraudulent transactions on my account.*

- An authenticator agent will verify the factors used by the customer for authentication. If the factors provided do not reach the score required, the transaction will be denied.
- A risk analysis method performed by risk engine will determine the authentication score required to process a transaction. The risk engine will make use of the customer's historic transactions to identify unusual activity.

4. *As Bank of Cambria CISO, I need to challenge the identity of fraudsters.*

- The system will use many methods to challenge the identity of fraudsters
- It will compare any incoming request from web server and deny access which are not coming from whitelist IPs.
- Risk engine that will invoke a secondary authentication process and request a different factor for identity verification and meeting the authentication score requirements.

5. *As Bank of Cambria VP of Customer Service, I want to provide my customers a seamless and frictionless experience*

- The authentication system will provide scalability; low latency, availability, and integration with multiple mobile and desktop devices (see non-functional requirements).
- It gives customers flexibility in the type of factors they want to use for authentication.

6. *As Bank of Cambria risk analyst, I want to block weak authentication methods for high-risk transactions.*

- In the context of DMFA system, transactions like wire transfer, ACH transfers, address changes, etc. are considered high-risk transactions. These transactions coupled with the other parameters like dollar amount, transaction history etc. will generate a risk score and an authentication score requirement for the transaction. The DMFA system will require that the authentication score is met or exceeded by the confluence of authentication factors for the transaction to proceed.

Non-functional Requirements

<u>Scalability</u>: Bank of Cambria currently has 500,000 active customers, with only 10% of those customers utilizing its customer portal. It is expected that by 2018 the number of customers using its customer portal will increase to be about 75% of the total active users. To support this growth the Bank of Cambria will leverage the use of its private cloud infrastructure to allow scaling up or down to adjust the demand of incoming transactions.

<u>Privacy</u>: Sigma Tech is tasked with providing the orchestration layer and authentication framework only. The authentication factors and mechanisms are the responsibility of the third party factor providers. In the same vein, the privacy and security of factor data is the responsibility of the third party factor providers and managed by the Bank of Cambria.

<u>Security:</u> The proposed solution framework should keep all data such as customer data, transaction data and URL repository encrypted at rest. All data in transit is also expected to travel encrypted using SSL.

Availability: To ensure high customer satisfaction, this authentication service needs to be available 99.99% of the time. Additionally, if a failure occurs, the systems should be able to fall back to the traditional method of username and password for authentication.

Interoperability: System should be extensible and compatible with new authentication factors that become available.

Business Justification

The Bank of Cambria is currently losing 200M to authentication fraud. With this DMFA system implemented, an 80% reduction in authentication related fraud loss is expected. Also, the new authentication system will improve and streamline the customer experience, necessitate additional verification only when necessary and give users the flexibility of choosing their preferred method of authentication.

Cost Estimate

Sigma Tech estimates a cost of $13M in 2017 to architect the DMFA. Contractual costs are estimated at $7M for 2017. This cost accounts for the man hours required for implementing the Orchestration Layer and integrating it into the Bank of Cambria Customer portal. The $2M yearly fee in 2018 onwards is expected to cover software updates and ongoing support. A $3M fee is assessed annually to support third-party authentication factor providers that Bank of Cambria has selected as participants in the DMFA platform. The table below outlines the proposed cost structure in greater detail.

	2017	**2018+**
Internal IT Work	$3M	$1M
Orchestration Layer	$7M	$2M
Additional Brokers	$3M	$3M
Total	**$13M**	**$6M**
Capital	$6M	$1M
Expense	$7M	$5M

Return on Investment

Implementing DMFA through Sigma Tech will yield an estimated savings of $53.5M annually for Bank of Cambria. These savings are calculated with a high level of confidence given current industry trends in account attacks, social engineering breaches, and current mitigation efforts. The majority of the financial savings for Bank of Cambria are through decreased fraud transactions. DMFA is expected to save $50M that Bank of Cambria is currently losing annually. In addition to transaction fraud, DMFA will drive additional savings through reduced calls to the bank helpdesk for authentication issues.

Furthermore Significant Account Change (SAC) notification letter costs and Breach Notification costs will be reduced by a total of $1.5M as a result of reduced fraud mitigation. Additional Return on Investment specifics are listed in the table below along with their estimated percentage improvement with the implementation of DMFA solution.

Hard Savings	**12 Month Impact**	**% Improvement**
Transaction Fraud - Existing Customers	$50,000,000	80%
Password Reset Calls to Bank Location	$2,000,000	25%
Confirmed EBITDA Improvement	**$52,000,000**	

Soft Savings	**12 Month Savings**
SAC Notification Letter Cost	$500,000
Breach Notification Letters	$1,000,000
Total Confirmed Savings	**$53,500,000**

Success Metrics

The success of the DFMA system will be measured primarily through the Reduction in Fraud per Subscriber KPM (Key Performance Metric). This metric is a standardized metric used across the banking industry. A secondary success metric will be the impact to the customer experience and measured by customer effort and satisfaction scores. A more detailed description of the success metrics methodology for analysis can be found in the success metrics section on page 30.

Part 2: Technical Specification

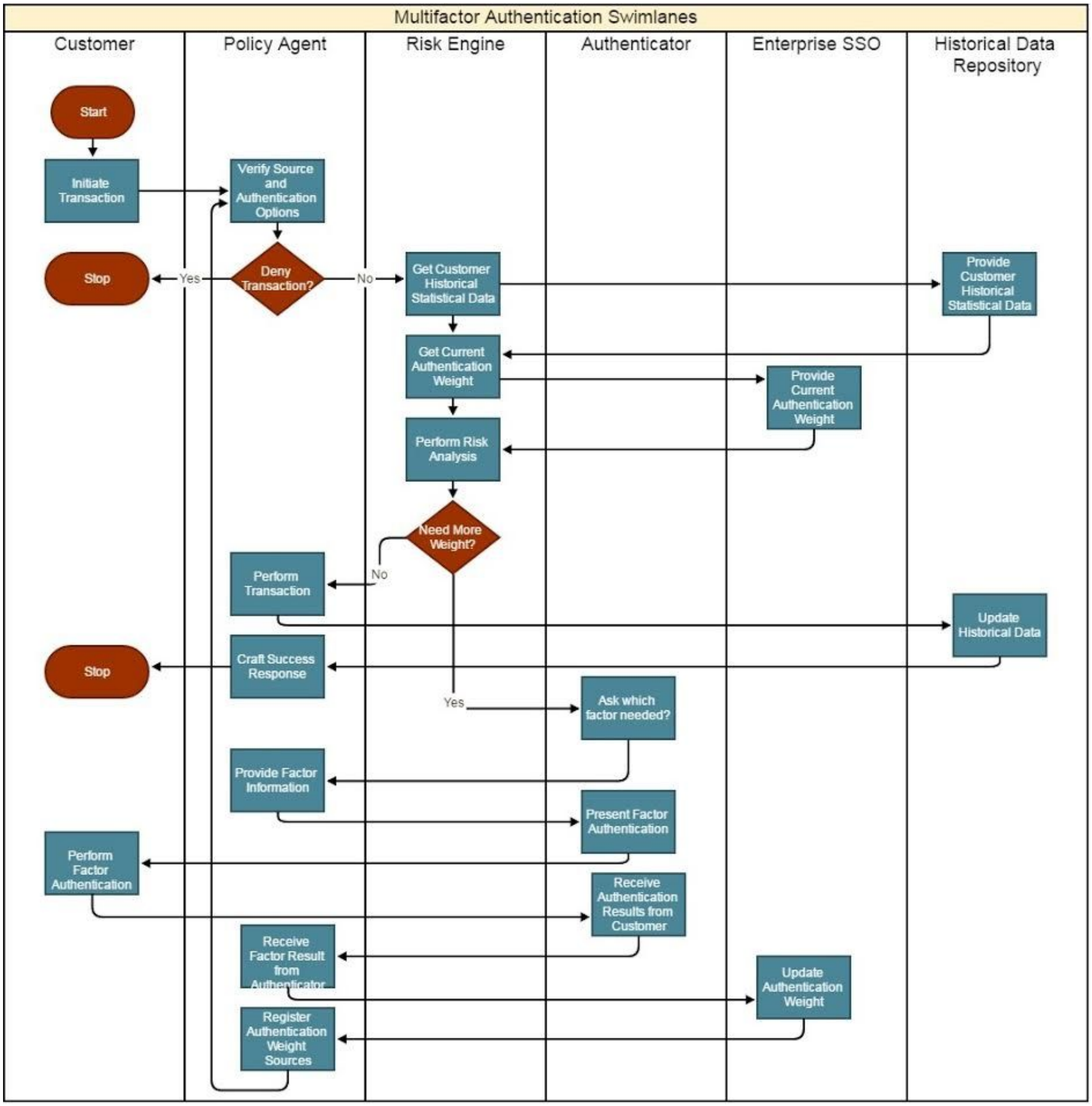
Software Solution Overview

The components comprising the software solution are the policy agent, the risk engine, the authenticator, the enterprise SSO/ID Provider and the historical data repository modules. The system allows or denies the transaction based on the factor authentication outcome, its weight defined in the system and the rules defined in risk engine. Additionally, the system provides an admin console that allows Bank of Cambria to manage factors available for authentication.

It is important to note that development of factors and their data management is not within the scope of this project. This factors will be provided by external vendors. Sigma Tech will provide software with the ability to integrate external authentication factor providers who have expertise in factor design and development. The management of factors and the storage of customer authentication information will be managed by Bank of Cambria and the external vendors that the bank has authorized as factor providers.

Architectural Data Flow

The proposed solution is divided into six main high-level components. The following swimlane diagram shows how the component interact.


Multifactor Authentication Swimlanes
Customer
Policy Agent
Risk Engine
Authenticator
Enterprise SSO
Historical Data Repository
Start
Initiate Transaction
Verify Source and Authentication Options
Stop
Yes
Deny Transaction?
No
Get Customer Historical Statistical Data
Provide Customer Historical Statistical Data
Get Current Authentication Weight
Provide Current Authentication Weight
Perform Risk Analysis
Need More Weight?
No
Perform Transaction
Update Historical Data
Stop
Craft Success Response
Yes
Ask which factor needed?
Provide Factor Information
Present Factor Authentication
Perform Factor Authentication
Receive Authentication Results from Customer
Receive Factor Result from Authenticator
Update Authentication Weight
Register Authentication Weight Sources

Applications, Components, Sites and Services

The dynamic multi-factor authentication solution consists of systems interacting with each other securely by establishing a circle of trust. A detailed list of systems and components that will be owned and hosted by the Bank of Cambria are described below:

Web Server

The server serves the public-facing website of Bank of Cambria which provides the ability for customers to perform online banking. It receives and replies to the HTTPS requests from customers. It interacts with the decision making Policy Manager and serves the appropriate responses to customer requests. This is the only public-facing component of the solution.

Policy Agent

The Policy Agent's main duties include collaboration, orchestration, and interaction with other components to make a decision on whether to allow or deny a transaction. It takes requests from the Web Server, gathers authentication and authorization data of the current user from the enterprise SSO and forwards that information to the Risk Engine. Based on the response from the Risk Engine, it decides if the customer needs to be presented with a request for additional authentication via other factors or allow the current request without additional authentication. It also periodically polls for information from the enterprise message queue and consumes the messages that factor providers have sent to the queue.

Risk Engine

The Risk Engine takes customer identification information, current transaction details, and authentication weight of the current transaction and analyzes it to calculate risk. It uses data mining and machine learning algorithms on customer's historical data to perform predictive analysis and inform the Policy Manager the results. The development of Risk Engine is not in the scope of this project. This system already exists at Bank of Cambria and can be used to block user transactions based on predictive analytics. Sigma Tech will leverage this existing system and will provide an integration layer to communicate to it. The Policy agent will use the decision provided by Risk Engine to determine if the user needs a higher authentication score to perform additional transactions.

Identity Provider/SSO Server

The identity provider (IDP) or enterprise SSO provides centralized authentication services. Bank of Cambria already has a license for Microsoft ADFS which implements OASIS SAML 2.0 specification to provide single sign-on. The solution will utilize ADFS to provide seamless identity services and build a circle of trust among customers, policy agent and factors providers. The SSO server will also be used by customers to login into the Bank of Cambria portal. The Policy Agent will use the SSO server to get and set current authentication weight of logged in users. Factor providers will be registered with this IDP server to establish a circle of trust and allow customers to use their interfaces by gaining access with customer's current credentials. All communication to and from the IDP server, customers, and the Policy Agent will be fully encrypted using SSL and all message encryption will be based on PKI and digital certificates using SAML specification.

Firewalls, IPS/IDS system

In order to keep a strict control on all requests coming into to the public subnet, an enterprise firewall will be installed. The firewall will allow incoming and outgoing requests at specific ports while denying all further requests. Additionally, an IDS/IPS device will be placed after the firewall with explicit deny rules for traffic monitoring and DoS mitigation tools.

Databases

The solution will have two main databases installed: the Application Data Storage and Customer Historical Data. The application data storage will contain current transactional data and will be used for BOC online transaction processing. It will also contain data for factors registration and customers. It will be used by the Policy Manager to execute transactions. It will keep the last 6 months of customer transaction data.

The Customer Historical Data database will periodically pull the information from the Application Data Storage as a batch process and will keep all historical customer data. This database will be used by risk manager for data analysis, data mining, analyzing usage pattern and predictive analysis to calculate risk.

We are keeping transactional and analysis databases separately for efficiency reasons as data mining tasks on historical data by the Risk Engine could have a big performance impact on overall system. OLTP can be used to efficiently serve customer requests and data mining and predictive analysis can be done in parallel without affecting other parts of the system.

Database Backups and Snapshots

Bank of Cambria, as a financial service provider, has strict requirements on data security and disaster recovery. To meet these requirements, the system will take automatic periodic secure backups, logs, and snapshots of both databases to provide disaster recovery and failover capabilities. Additionally, backups will be granular in nature so as to allow the restoration of databases to any specified point in the past.

Administrator Console

The Administration Console is an existing web portal of Bank of Cambria which is used to manage groups, roles, users and single sign-on server. The ability to manage authentication factors has been introduced into this application so that Bank of Cambria IT Staff or Administrators can use the same interface to manage authentication factors. The management of factors will include registering of new factors into the system, view & modification of existing factors and the activation or deactivation of existing factors. Once a factor is registered in the admin console, it will be available for the customer to sign up for.

Customer Portal

This is existing customer facing website of Bank of Cambria used by customers to perform account management and day to day banking transactions. We have introduced new screens to give customers ability to register for new available factors. Using new screens customers can activate or deactivate or re-register the factors they have registered. We also modified the funds transfer screens of the portal and injected calls to policy manager so that fund transfer policy can be enforced.

Authentication Factor Providers

Authentication factor providers are external entities which provide products that support authentication factors. Examples of such providers are Duo (Fingerprint), Eyelock (Retina). The technical details how they implement the factors is out of the scope of this project. The factors will be integrated into our solution using the Administration Console. Once registered with our system, customers can sign up for factors using the Customer Portal. During the registration process, factor providers will collect customer specific information that is required for authentication of the customer for the particular factor. When the policy manager redirects the customer to the factor provider for further authentication, it will try to authenticate the customer against registered information and will send the response back to policy manager if the authentication is successful or not.

The factor providers will authenticate the customer using SAML-based SSO implementation against IDP server for which they established a circle of trust as service providers. Factor providers can communicate with the policy manager by sending RESTful messages to message queue (consumed by policy manager). These messages may include successful registration customer with a factor or other communication.

Message Queue

The Message Queue will be used to establish a direct communication channel between the BOC Policy Agent and Service Providers. The Policy Manager will continuously poll new messages from the message queue and process them to get in sync with the factor state. It only makes RESTful HTTPS GET requests to the service providers and expects an HTTPS response with the authentication status.

System Architecture of Dynamic MFA

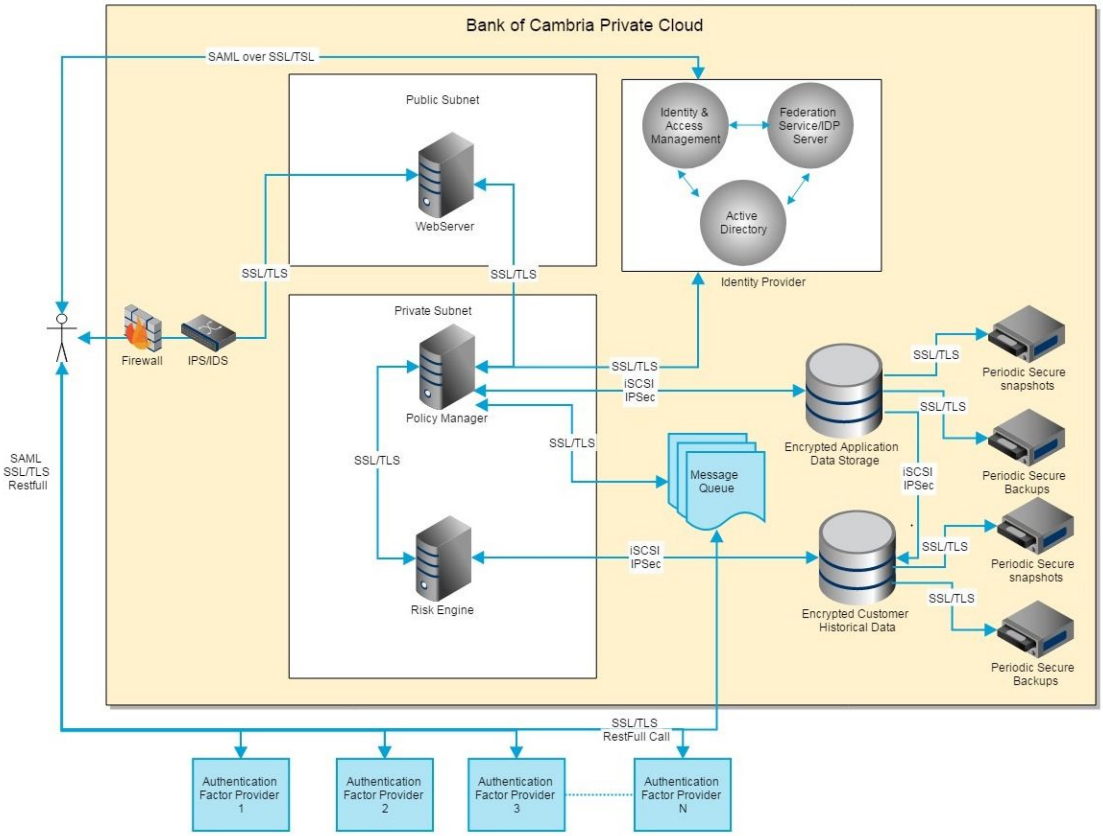

Bank of Cambria Private Cloud
SAML over SSL/TSL
Public Subnet
WebServer
Identity & Access Management
Federation Service/IDP Server
Active Directory
Identity Provider
SSL/TLS
SSL/TLS
Private Subnet
Firewall
IPS/IDS
Policy Manager
SSL/TLS
iSCSI IPSec
SSL/TLS
SSL/TLS
Message Queue
Encrypted Application Data Storage
SSL/TLS
Periodic Secure snapshots
SSL/TLS
Periodic Secure Backups
iSCSI IPSec
SAML SSL/TLS Restfull
Risk Engine
iSCSI IPSec
Encrypted Customer Historical Data
SSL/TLS
Periodic Secure snapshots
SSL/TLS
Periodic Secure Backups
SSL/TLS RestFull Call
Authentication Factor Provider 1
Authentication Factor Provider 2
Authentication Factor Provider 3
Authentication Factor Provider N

Figure 1: System Architecture diagram of Dynamic Multi-factor Authentication

Architecture Diagram Description

Factor Registration

1. A customer sends an HTTPS request to the web server to establish a connection.
2. The web server checks if the incoming request is coming from an authenticated user or not. If not then it redirects the user to IDP server for authentication The IDP server presents the login page to the user and once authenticated it redirects the user back to web server
3. The web server forwards the request to policy manager using HTTPS
4. The policy manager sends a query to the application database using iSCSI over IPsec to obtain the list of factors customers can register for.
5. The policy manager sends an HTTPS response to the web server.
6. The web server provides the list of factors to the customer
7. The customer selects the factor to register for
8. The user is redirected to the service provider's website to provide authentication data
9. The authentication provider redirects the user to IDP server to check if the customer is already authenticated with it or not
10. If the customer is already authenticated by the IDP server and it is a first customer request for a factor provider, the provider will create a blanket account using customer unique id received by IDP's SAML response. The service provider gathers data needed for authentication from user
11. The user registers successfully and the service provider sends a success message to the message queue to let policy manager know that customer is registered.
12. The policy manager reads the message from the message queue and updates Customer_Factors table to reflect the newly registered factor.

Banking Transaction

1. A customer sends an HTTPS request to the web server to establish a connection.
2. The web server checks if the incoming request is coming from an authenticated user or not. If not then it redirect the user to IDP server for authentication
3. The IDP server presents the login page to the user and once authenticated it redirects the user back to web server
4. The web server forwards the request to policy manager using HTTPS

5. The policy manager receives the transaction request and opens a secure channel with the risk engine.
6. The policy manager sends customer id, type of transaction, transaction amount, and current and authentication weight to the risk engine
7. The risk engine connects to the customer historical data repository using iSCSI over IPsec and sends a SCSI command to query the customer information
8. The risk engine performs predictive analysis of provided data with historical data and informs the policy manager either to allow transaction or not
9. If the policy manager receives deny decision from the risk engine then
    a. It queries the application database to obtain the registered factors for the customer
    b. If policy manager has already tried to authenticate the customer using all factors for which the customer is registered for, then the request is denied.
    c. Otherwise, it determines the next factor to authenticate using the current user authentication weight basis. The policy manager redirects the user to the factor provider
    d. The factor provider asks for authentication information from the customer
    e. Based on the response from the customer, the service provider redirects the user back to the policy manager along with authentication success or failure
    f. If the policy manager receives the success message it will again try to execute the transaction (step 5)
    g. If the policy manager receives the failure message from authentication service provider, GOTO step 8a.
    h. If the policy manager receives an allow response from the risk engine then, the policy manager will execute the transaction and send the success message to customer via web server using HTTPS

Ecosystem Map

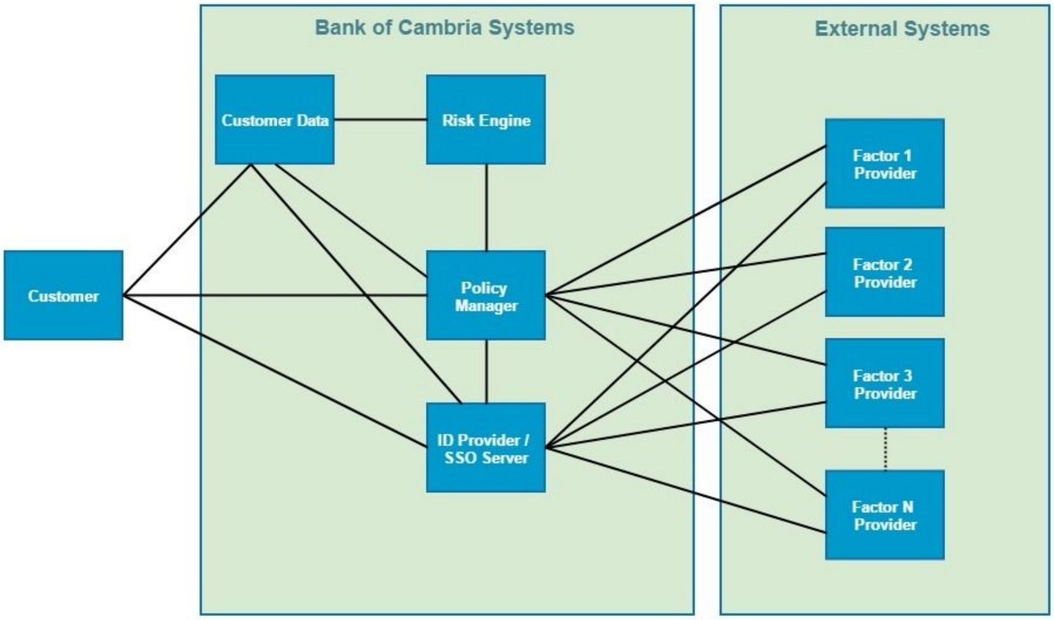


Figure 2: Ecosystem map for Dynamic Multi-factor Authentication solution

Software Solution

Software Development Platform and Approach

The platform selected for this solution is JEE. The reasons for selecting JEE as the platform for development are:

1. Multi-tiered Architecture: Separate functions for processing and data management allow for greater flexibility. Additionally, individual layers can be modified without having to rework the entire application
2. Cross Platform: The application can be hosted on a variety of environments including Linux and Windows. Bank of Cambria's private cloud environment comprises of a mix of Windows and Linux servers.
3. Caching System: Given that risk engine will need to perform risk analysis repeatedly with authentication data and historical transaction records, the robust and effective caching system of the JEE platform can be leveraged.

4. The recommended approach for this development is the Waterfall approach. This approach ensures that Sigma Tech and the Bank of Cambria agree on the software deliverables. It allows for easy and accurate measurements of progress.
5. Since the specifications of the application are agreed upon, it allows for the parallel development of modules and a shorter development timeline.

Deployment Model

The deployment of this software will occur on Bank of Cambria's private cloud which is managed by Rackspace. Bank of Cambria has 500,000 active customers and it is expected that 75% of them will be active users of the online portal by 2018. Considering this, the minimum baseline environment to support this volume of transactions and throughput comprises of

- 25 x General Purpose Cloud Servers (32GB RAM, CloudBlock Storage, 35,000 IOPS) in a clustered configuration to provide web tier functionality for the authenticator and enterprise SSO.
- 75 x Memory Optimized Cloud Servers (120GB RAM, CloudBlock Storage, 35,000 IOPS) in a load balanced configuration with auto scaling features enabled to house the policy agent and risk engine.
- 75 x I/O Optimized Cloud Servers in a load balanced configuration with auto scaling features enabled to house the historical data repository and perform the read / write operations on the database.

System Metrics

The dynamic multi-factor authentication system is designed to meet the volumes expected from the Bank of Cambria's customers. It will be designed to maintain an uptime of 99.99% or higher. The following metrics will be captured and analyzed for performance optimization.

Transaction Type	Volume Per Day	Concurrent Requests	Average Execution Time
Login	100,000	10,000	1.5 Seconds
Post changes to account	50,000	5000	2 Seconds
Transfer of Funds	10,000	1000	2 Seconds

Table 1: System Metrics for Dynamic Multi-Factor Authentication Solution

Integration

Integration with Other Bank of Cambria Applications

In order to allow the dynamic multi-factor authentication system across all applications created by Bank of Cambria, Sigma Tech will provide two components to enable the standard username/password authentication replacement:

1. Sigma Tech Software Development Kit (SDK)
2. Sigma Tech Server.

The Sigma Tech Software Development Kit (SDK) will allow Bank of Cambria developers to granularly control how multi-factor authentication is handled within their application. Using this SDK, Bank of Cambria will be able to define factor specific authentication weights, specify transaction-based authentication requirements and connect the specify the location of historical data transaction repository. The SDK is also crafted for iOS and Android devices and will allow Bank of Cambria to extend this capability across all modalities of its application. The Sigma Tech Server is a standalone server which can be placed on-premise or in the cloud (i.e. Amazon Web Services).

Integration Process

With the use of the SDK and the Sigma Tech Server, any Bank of Cambria application can quickly and easily integrate with the dynamic multi-factor authentication system. After placing the SDK files in your application project, the application implements two calls to the Sigma Tech Server: Authentication and Configuration.

Authentication: Each time the application needs to authenticate a user, it calls authenticate.

- Through the Sigma Tech Server, the application calls the authenticate function with a specific authenticator such as voice recognition or fingerprint biometrics.
- Additionally, the application will also have the ability to call the authenticate function for a menu option where the server presents a menu of available authenticators from which the user can choose.

Through this process, the Sigma Tech SDK and Server take care of the entire authentication process and return the appropriate result back to the application.

Configuration: Through the SDK any Bank of Cambria applications can also manage different types of authenticators. Using the configure function, the application can, for example, allow the user to enroll for face recognition.

Through the use of this SDK and Server, this solution works alongside authenticators that may have already been implemented. Thus the dynamic multi-factor authentication platform can evolve as per the bespoke needs of any existing or future Bank of Cambria application.

SDK & Server Updates

When a product update is available, Bank of Cambria will be contacted via email with specific information on accessing the update along with all release notes and installation instructions. Patches are typically released in the form of self-extracting binaries that can be applied as a package. The update process will typically require a server process restart, which usually takes less than one minute from start to completion. Since Sigma Tech servers are stateless and typically deployed behind a load balancer, these updates can be applied in a staggered fashion, across servers without causing any application downtime.

Data Design and Management

BOC’s existing Enterprise Systems will continue to serve as the Systems of Record for all customer information and historical transaction data. Existing relational schemas like Password(userID,password) and AllCustomerData(data,...,...) will be kept in service. The proposed solution will introduce new entities to the existing databases, primarily for data-in-use interactions between the Policy Manager, Customers, the Risk Engine, ID Provider and service providers.

Business Data Diagram

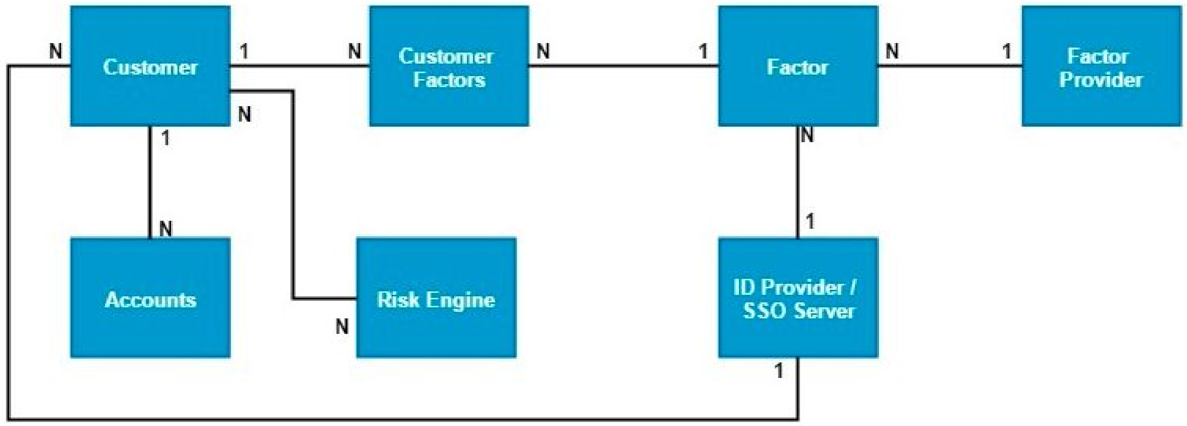


Figure 3: Business data diagram for Dynamic Multi-factor Authentication solution

- A customer can have multiple accounts with BOC but each account will be associated with a unique customer
- A customer can be registered to multiple factors however a customer can be associated to a particular factor at most once
- A factor can be associated with multiple customers
- A factor must belong to a unique factor provider, however, a factor provider can provide multiple factors
- Each factor can have at most one circle of trust with IDP server, however, IDP server can register multiple factors as service provider
- A customer can have many data elements shared to risk engine, and risk engine can have data elements of many customers at a time
- A customer can have at most 1 account with IDP, and IDP can have accounts of multiple customers

Entities

Factor Entity: The factors entity contains details for existing authentication methods registered for customer use. The table includes the following attributes.

Factors(factor_id (PK), factor_name (FK - Factor_Provider[factor_provider_id]) , provider, authentication_weight, public_key, attr_name, auth_attr, case_sensitive, logout_url, logout_success_url, logout_success_url, encoding, signing_algorithm_url, signing_algorithm_name, signing_algorithm_name)

Factor Provider Entity: It contains information regarding the service providers of authentication factors.

Factor_Provider(factor_provider_id (PK), provider_name, email, address, phone)

Customer Factors Entity: It captures the relationship of all the factors registered by each customer.

Customer_Factors(factor_id (PK & FK Factor[factor_id]) , userID (PK & FK Customer[userID])

Customer Entity: This entity captures the relationship between customers and their accounts.

Customer(userID (PK), account_number (FK Accounts[accID]), Idp_account (FK IDP_Provider [idp_id])

Accounts Entity: This entity captures information for each account.

Accounts(accID (PK), account_type, balance)

Risk Engine Entity: This entity captures the relationship between the risk engine data and the customer transaction.

Risk_Engine(risk_session_id (PK), userID (FK Customer[userID]), type_of_transaction, transaction_amount, current_auth_weight)

ID Provider entity: This entity captures the relationship between customers, authentication factors, and the IDP server.

ID_Provider(idp_id (PK), userID (FK Customer[userID], factor_id (FK Factor[factor_id])

Monitoring Authenticators

In order to keep track of each authentication request and performance metrics, the administrative interface can be used for measuring:

- how many users are using each authenticator
- success and failure ratios for each authenticator
- the time it takes users to complete an authentication process with each authenticator
- Following and examining the authentication path for each user

Sigma Tech monitoring serves two purposes: First, it allows product managers to measure the impact of the authenticators and rules they publish as well as identify user experience issues. Second, it allows customer support to understand the detailed authentication flow for each user in order to provide the best support possible.

Managing Failed Logins

The solution can be configured to set a threshold on how many failures are allowed for each authenticator and what action to take in case of failure. For example, when a customer exceeds the threshold of login attempts, the authenticator locks and the user is not able to log in with that authenticator again. The user needs to authenticate with a different authenticator and then they can choose to reset the locked authenticator.

Part 3: Implementation Plan

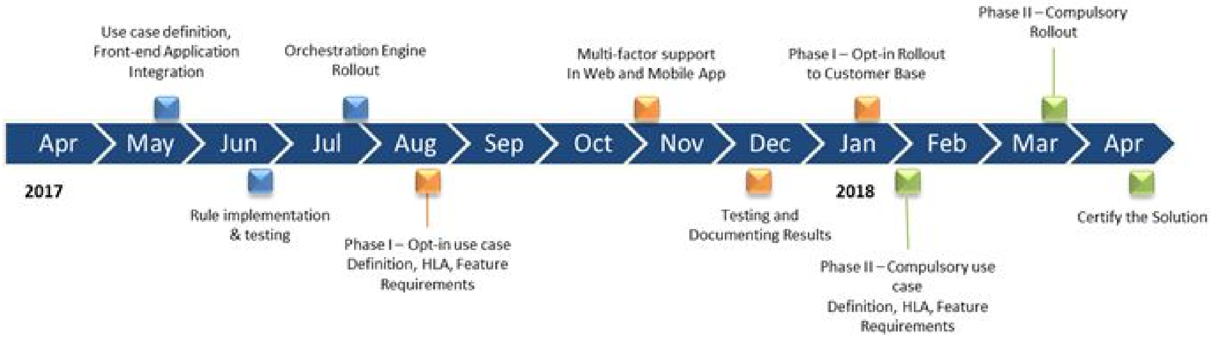
Solution Delivery Roadmap

Sigma Tech will follow an agile build, with two 2-week iterations comprising of monthly enterprise releases. Sigma Tech will deploy software enhancement with three main milestones: 1) Orchestration Engine, 2) Phase I Deployment – User Opt-in, and 3) Phase II Deployment – Compulsory Multi-factor. Each milestone will contain multiple iterations to successful completion. (An overview of the main phases of deployment are listed as appendix item 1.1.)

The Orchestration Engine will provide the solidified, back-end plumbing to the Multi-factor Authentication Engine. During this phase, all front-end applications will be programmed into the orchestration layer for seamless multi-factor implementation. All third-party authentication sources must be fully vetted, programmed, and tested before moving on to the second phase. Phase I will focus on a purely optional opt-in experience. All authentication methods will be deployed and used as Bank of Cambria's customers enroll. Sigma Tech will monitor these adoption rates for analysis on acceptance and success before deploying the third, compulsory phase. Phase II will require all Bank of Cambria customers to enroll in a form of multi-factor authentication in order to proceed with any level of heightened authentication. Without enrollment, single-form authentication will only allow the customer view-only attributes of account access.

Sigma Tech will migrate Bank of Cambria's old authentication to the new, multi-factor authentication engine by running both systems in parallel. In fact, the old authentication engine, containing username and password, will still remain an option for secondary verification in the new, multi-factor engine. Further, maintaining both systems in parallel will enable multi-factor to use the old authentication engine as a very low-level authentication for generic, view-only transactions in the new multi-factor engine.

The timeline below helps to visualize the critical path from development, through each phase to final deployment:


Use case definition, Front-end Application Integration
Orchestration Engine Rollout
Multi-factor support In Web and Mobile App
Phase I – Opt-in Rollout to Customer Base
Phase II – Compulsory Rollout
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
2017
2018
Rule implementation & testing
Phase I – Opt-in use case Definition, HLA, Feature Requirements
Testing and Documenting Results
Phase II – Compulsory use case Definition, HLA, Feature Requirements
Certify the Solution

Project dependencies are the main, foreseeable hurdle to a delay in implementation. The Orchestration Engine must be fully vetted to ensure all customer touch-points have been considered and accounted for, and that all third-party development efforts meet the Phase I timeline of Jan 2018 enterprise release. Deployment for our customer-facing milestones will not proceed until testing for all third party authentication factors has been concluded as successful. Further, the success of the customer Opt-in phase will lend itself to an even speedier deployment of Compulsory phase. Sigma Tech suggests that Bank of Cambria market the Opt-in experience as possible to gain attention, and migrate as many voluntary customers as possible.

Operationalization

Business Operations Around the Dynamic MFA System

Bank of Cambria administrators will be able to access the admin console to manage their new authentication factors. The admin console is an existing dashboard page where administrators can manage groups, roles, and users. A new section will be provided for managing factors where administrators will have a list of authentication factors registered in the system.

The ‘Manage Factors’ page in the admin console will allow administrators to view the details of authentication factors, modifying factor information, deactivate existing factors, and register new factors.

Incident Management

The existing Bank of Cambria IT Customer Service Desk will be responsible for incident management. The service desk manager will provide and manage all training for the service desk. The goals of the incident management team are to restore a normal service operation (defined in the SLA) quickly and to minimize the impact on banking transactions.

The first process of the incident management plan consists of trying to match the reported incident with existing problems registered in the known error database (keDB). If a workaround has been developed, the service desk can provide the existing fix. If the incident is not present in the keDB, or it cannot be resolved quickly by the help desk, it will be assigned to specialist technical support groups. The technical support groups will create a problem record and the problem management process will become involved, resulting in registration of the new incident in the keDB for future reference.

Change Management

Changes to the system will be handled by the DMFA service manager at Bank of Cambria. Any change to the DMFA system will start with a request for change. Once an RFC has been submitted, the manager will assess the impact, cost, benefit and risk of proposed changes, develop business justification and obtain approval. Proposed changes must be approved by the Change Advisory Board.

If the change is approved, the DMFA manager will be responsible for managing and coordinating change implementation, monitoring and reporting on implementation, and closing the change request. Change management is responsible for managing change process involving MFA hardware, system software, documentation and procedures associated with the running, support and maintenance of live systems.

Release Management

This management process will oversee managing, planning, scheduling and control new software builds for the DMFA system. The process will follow agile development principles.

Performance Requirements and Service Level Agreement

The performance standards that the DMFA system is obligated to meet are:

- 99.99% availability and uptime
- An application response time of fewer than 2 seconds
- A three-week advance notification of system changes that may affect customers.
- Help desk response time of at least 24 hours
- Usage statistics that will include a number of logins per authentication factor, registered factors, authentication wait time, and number and type of transactions that required a high (>5) authentication score.

Customer Satisfaction Data Collection

Customer satisfaction will be measured by using three strategic surveys to collect information at different periods of the customer experience process.

- Post DMFA registration survey to assess the ease of the registration process.
- In-app survey after use of the DMFA to assess the satisfaction of the DMFA process.
- Monthly email surveys to assess overall satisfaction.

User Enablement

There are two types of users of our application: Bank of Cambria IT employees, and Bank of Cambria customers. The approaches for user enablement are:

User Enablement: Bank's IT Employees

For IT employees of Bank of Cambria, in-person training sessions will be conducted. There will be three, two-hour sections conducted on Monday, Wednesday and Friday of training week followed by on-demand video recording. For the first six months of post-application deployment, Sigma Tech will have a 24/7 customer helpline dedicated to IT employees. The focus of the training will be how to use the new application from an administration perspective, i.e:

- How to register new factor with system
- How to deregister/deactivate existing factors in system

- How to activate already deactivated factors
- What are configuration parameters to set in order to factor work correctly within the system?

User Enablement: Customers

User enablement for customers of Bank of Cambria is a challenge as the user base consists of hundreds of thousands of customers. Therefore an encouragement based strategy will be implemented to politely engage customers and persuade them to use the new application. The goal of this strategy will be to educate the customer to adopt this higher form of security practice.

The six high-level steps that we have decided to follow in order to persuade customers for multi-factor authentication are:

1. The highly visible registration process with clear articulation of benefits.
2. Automated emails to customers describing the change and benefits
3. Incentives for customer sign-up
4. Offer additional guarantees to keep customer personal data secure
5. Simplify the DMFA registration process
6. Use of modal popups

Highly Visible Registration Process

Making the registration process obvious and intuitive for the customer is the single most important element to persuade them. We will make sure that initiation of the registration process is differentiated from the rest of the pages by using contrasting colors, a larger font and prominent positioning for best chances to grab customer's attention. The goal will be to retain the customer's focus on DMFA and effect a registration on login.

Automated Emails to Customers

As part of user enablement process, we recommend that Bank of Cambria send periodic automated emails to customers describing the new authentication process. These emails will be targeted to only those customers who haven't registered for DMFA. The goal of this activity will be to educate customers about security and convenience features of this upgraded authentication system and invite them to invite them to register via a call to action in the email.

Incentives for Customer Sign-up

Offering incentives to sign up increases the chances that customer will register and use the DMFA. Sigma Tech recommends the offering of gift cards and sweepstake entries as means of incentivizing customers to enroll in this program. When customers login into Bank of Cambria using his/her username and password, the application will show a splash screen or pop over with the offer along with potential security benefits that they will get if they opt in for dynamic multifactor authentication. The application will ask them to avail of the offer by registering for the multi-factor authentication system. Customers at that point can opt to avail the offer and be incentivized in the process.

Offer Additional Guarantees

Security breaches and transaction fraud are the main issues for customers. It is extremely important to offer the guarantees to the customer that the information that they provide will be solely used for authentication purposes and authentication providers will not sell or share customer information like phone numbers, emails or address information to any other entity. Additionally, if customers are enrolled in DMFA, the bank should provide additional insurance against fraudulent wire and ACH transactions.

Simplify Registration Forms

As the application will be supporting multiple authentication factors and give customers ability to subscribe for multiple factors, the registration process should be as short and simple as possible. There will be clear instructions and profile information will not be re-entered during the multi-factor registration process.

Modal Popups

In order to give the customer a cohesive user experience, the application will use modal popups for DMFA registration. The usage of modal popups will simplify the user experience and give users the ability to access their regular site by closing the modal popup.

Success Metrics

As a part of the project plan and in order to measure the performance of the solution after the go-live date, detailed operational and process metrics will be captured. The metrics will consist of two categories that comprise the primary business benefits of the program. The two categories are Fraud Reduction and Improved Customer Experience.

Fraud Reduction

- A real-time tally of transactions that did not meet the minimum authentication requirements to execute will be captured and analyzed on a regular basis.
- This information will be aggregated to calculate the Fraud per Subscriber Key Performance Metric.
- A quarterly comparison of fraud claims against the prior years' claims will be performed.
- A user adoption report will also be captured and analyzed to assess the percentage of online users that are registered with the DMFA system

Date	Time	Transaction Type	Transaction Amount	AuthScore	Required AuthScore	Disposition
4/20/2017	5:00 AM ET	Wire Transfer	$ 50,000	2	7	Blocked
4/20/2017	5:53 AM ET	ACH Transfer	$750,000	3	8	Blocked

Improved Customer Experience

An improved customer experience is a secondary goal of the program and will be measured by:

- Application Performance: Page loads and transaction times will be closely monitored. We have set a goal of two seconds for all interactions. Any time the site or a transaction takes more than two seconds for a user, a log of the interaction will be stored for analysis and remediation.

Code	Metric	Resource	Value	Breach Value	State	Details
12120	Response Time (MS)	Registration Page	2500	2000	Critical	Link
1200	Availability	DMFA Link	1	0	Critical	Link

- Customer Effort & Satisfaction Scores: To ensure that all users are able to access all features and functions of the application with minimum effort, a customer effort score that is a composite of all actions and the time to perform then will be calculated. In addition, a customer satisfaction survey will be administered monthly to assess overall satisfaction with the different modules of the application.

Task	Learnability	Efficiency	Usability	Satisfaction	Composite Score
MFA Registration	100%	3:00	99%	95%	95
Invoke DMFA	99%	1:25	95%	94%	94

Appendix

Figure 1.1 - Key phases and time-frames for responsible parties

Phase	Key Tasks	Time-frame	Entities Responsible
Discovery	Customer Use Cases, Mapping Cases to Multi-factor Solution, Application Flow	1-2 Weeks	Sigma Tech and Bank of Cambria
Data Collection	Application Architecture, Integration Elements, User Store, Connecting to Pre-built Risk Engines	1-2 Weeks	Sigma Tech and Bank of Cambria
Design Workshop	Application Flow and Architecture for Authentication Factors and Third-party Integration	1-3 Weeks	Sigma Tech and Bank of Cambria
Orchestration Engine	Design Orchestration Engine to Encompass all Front-end, User Entrance Programming into a Solitary Source for Authentication	6-8 Weeks	Sigma Tech and Bank of Cambria
Phase I – Customer Opt-in	Deploy to Early Adopter Customers, Provide Incentives to Migrate Existing Customer Base at an Opt-in Level	20-24 Weeks	Sigma Tech
Testing and Documenting Results	Test Cases, End-to-End Testing, Expected Results and Captured Output	3-4 Weeks	Sigma Tech and Bank of Cambria
Phase II – Compulsory Multi-factor	Migrate Remaining Customer Base to Multi-factor Authentication, Additional Heightened Level Transactions Cannot Be Performed Unless Enrolled in Multi-factor	8-12 Weeks	Sigma Tech
Certifying the Solution	End-to-end Solution	2-4 Weeks	Bank of Cambria

References

- Loonkar, Rakesh. "Keep Pace with Biometrics." Transmit Security. Retrieved February 28, 2017 from http://www.transmitsecurity.com/use_case/keep-pace-with-biometrics/
- Mahdi, D. A., Ant A., & Singh A. (2016, November 23). *Market Guide for User Authentication* (ID: G00301822). Retrieved from Gartner database.
- Moyer, Mallory. "Forget Passwords: How Biometrics Are Transforming the Security of Mobile Payments." TechCrunch. Retrieved April 7, 2017 from https://techcrunch.com/sponsored/forget-passwords-how-biometrics-are-transforming-the-security-of-mobile-payments/.
- Ping Identity (2013). *Multi-Factor Authentication: Best Practices For Securing The Modern Digital Enterprise* [White Paper]. Retrieved March 1, 2017 from https://www.pingidentity.com/content/dam/pic/downloads/resources/white-papers/en/mfa-best-practices-securing-modern-digital-enterprise-3001.pdf?id=b6322a80-f285-11e3-ac10-0800200c9a66
- SafeNet (2015). *Multi-Factor Authentication: Current Usage and Trends* [White Paper]. Retrieved March 1, 2017 from http://www2.gemalto.com/email/pdf/Multi_Factor_Authentication_WP_EN_A4_v3_3Apr2013_web.pdf
- Strom, David. "Introduction to Multifactor Authentication Methods in the Enterprise." SearchSecurity. TechTarget. Retrieved March 5, 2017 from http://searchsecurity.techtarget.com/feature/The-fundamentals-of-MFA-Multifactor-authentication-in-the-enterprise.
- Blake Ross, “Firefox and the Worry-Free Web”, from Security and Usability, ed. Cranor and Garfinkel. (O’Reilly 2005)
- Cameron Chapman “5 Simple Tips To Help You Increase User Sign Ups”, https://blog.kissmetrics.com/increase-user-sign-ups/
- Sarah Kuranda, “The 10 Biggest Data Breaches Of 2016”, http://www.crn.com/slide-shows/security/300083246/the-10-biggest-data-breaches-of-2016.htm
- Jenii Lowe, “Using Pop-Ups on Your Website: The Advantages”, https://business.yell.com/knowledge/using-pop-ups-on-your-website-advantages/

- Humayun Khan, 8 Ways Pop-Up Stores Can Boost Revenue and Build Buzz for Your Brand, https://www.shopify.com/retail/120059907-8-ways-pop-up-stores-can-boost-revenue-and-build-buzz-for-your-brand