CU*Answers Best Practices

Standards and Guidelines for Clients and Third-Party Vendors

Single Sign On (SSO) Integrations with CU*Answers Tools

Revised September 27, 2011

Introduction

The ability for **It's Me 247** Online Banking (and even CU*BASE GOLD) to be the central authority for user access to third-party systems is an increasingly popular technique for supporting member interactions in the world of interconnected systems.

CU*Answers is committed to projects that add these integrations for our credit unions' members. We want to help you. We want to support these relationships. And we value these new connections to strengthen and expand our network for the benefit of members. At the same time, based on our experience and our responsibility to maintain a secure network, a strong tool set, and a sustainable organization for our owners and clients, we must exercise due diligence and appropriate caution when evaluating every new project request.

Purpose

With the number of vendors and SSO designs expanding every day, this Best Practices strategy was developed to allow us to support rapid development while still maintaining our high standards for securing member data and network resources.

It is not intended as a technical document, but rather to describe, in layman's terms, the business logic behind why CU*Answers might or might not choose to pursue a particular integration project.

General Guidelines

As the name implies, Single Sign On (SSO) integrations allow a member (or CU employee) to authenticate once, and from there click a simple link to access separate websites and tools without the need to remember or type user names and passwords over and over again. The link might be a simple one-time request for some information to be displayed (like a check image), or could initiate a jump to a separate website (like an online PFM tool), or other techniques with varying degrees of complexity.

For the purposes of this discussion there are three main types:

- **Data Retrieval:** A basic server-to-server communication mechanism to retrieve data on behalf of the member and pull it back to the authenticated system. *Example: cleared check images.*
- **SSO Handoff to Another Website:** A more complicated process than data retrieval, the SSO handoff to a 3rd party website can involve multiple server-to-server communication steps to establish authentication before the final redirect of the member to another website. *Example: online bill payment.*
- **Integration:** A customized, full-featured integration with a vendor that includes data exchange even beyond that which is needed for the SSO. As many variations as there are vendors, with expanded rules of engagement and end-user access techniques. *Example: eDOC Innovations Photo ID vault, which includes an SSO to scan and store IDs as well as SSO links to retrieve stored images.*

Many of the interfaces we've developed over the years are hybrids of more than one of these types, and the specific techniques to accomplish them have almost as many variations as there are vendors and CUs who need them.

Sample Online Banking Integration Techniques

The following table groups similar types of online banking interfaces. This list is not exhaustive, nor intended to limit the types of integrations we will do, but rather is presented to describe how our experience will be applied to requests for new projects, and adapted to new technologies as they come along.

	SSO Type	Example	Description	End-user Access Point	Other Integration Features
1	Data Retrieval	▪ Cleared Check Images	Simple request for data element (image); no session maintained	Account History page, in line with associated transaction	
2	SSO Handoff	▪ Secure Document Storage (e.g., eDOC Member Portal)	Simple link to initiate an authenticated session with 3rd party vendor	CU-configured Related Links page *(other access points planned for the future)*	
3	SSO Handoff (independent integration techniques)	▪ OTB[1] Loans, Credit Cards, and Investment Savings Products	SSO link that supplements corresponding data from CU*BASE (data populated via data upload and/or manual input, independent of the SSO)	Link on the Account Info page, one click away from the Account Summary	Basic account data is displayed from CU*BASE OTB database; click initiates SSO to vendor website for more details
4	Hybrid SSO Handoff w/ Limited Integration	▪ Personal Financial Management tools (e.g., MoneyDesktop) ▪ Investment Services (e.g., CFS eVision)	Link to initiate an authenticated session with 3rd party vendor but no known member enrollment status; limited server-to-server communication	Global navigation, easily accessible from any location	No data stored in CU*BASE except activation flag Vendor initiates periodic requests to pull member data from CU*BASE
5	Hybrid SSO Handoff w/ Integration	▪ e-Statements ▪ Bill Payment[2] ▪ Mobile App ▪ Investment Services (e.g., CFS My Portfolio View)	Link to initiate an authenticated session with 3rd party vendor, based on known member enrollment status; varying degrees of server-to-server communication	Global navigation, easily accessible from any location	Synchronization of enrollment records from vendor to CU*BASE database; periodic data exchange for database maintenance, billing, etc. (independent of SSO)
6	Integration	▪ Bill Payment Apps (e.g., iPay QuickPay and P2P Wizards) ▪ Bill Pay Status Messaging ▪ Investment Services (e.g., CFS DataVISION)	Server-to-server authentication process presents data and tools to directly to members in online banking	Various	Seamless to member, no need to leave **It's Me 247** to jump to another website

[1] OTB = Off Trial Balance, our term for member savings and loan products that are not retained on the CU*BASE member database but rather exchanged via a third party. CU*BASE maintains a basic database record, typically updated via independent data exchange with the vendor (separate from the SSO), to document the presence of the account for CU staff and members online.

[2] We currently have two interfaces for online bill pay services; more are anticipated in the future. Both are essentially hybrid SSO links with varying degrees of integration, using different techniques for database synchronization and maintenance according to our relationship and long-term strategies with each vendor.

Rules of Engagement

General Requirements to Move Your Project Along

As stated above, this document is not intended to provide technical specifications for integrations, but the rules and checklists below are an important first hurdle to cross in moving your project forward with our development teams.

As our discussions about your project progress, more detailed technical specifications will be provided, and those, along with the business rules defined here, will become the standards against which the final integration specifications will be measured.

Remember that although our teams will be as flexible and innovative as possible, they will not compromise when it comes to basic requirements to protect your member data and the integrity of our network, your credit union included. Credit unions or vendors that wish to circumvent any of our guidelines, outlined here or published elsewhere, will be requested to agree to formal indemnification agreements, to be determined upon advice of legal counsel.

Analyses to be Completed

The decision-making process involves several separate evaluations that will be completed by various experts here at CU*Answers, based on consultations with and information received from both your credit union and your chosen vendor. (See also "Decision Checklist for New Projects" below.)

1. **Business Analysis**

   As described throughout this document, our team looks at each integration project from a big-picture standpoint to evaluate how it fits with current and future corporate goals and direction. We consider whether the CUSO will be investing its own funds to produce an end-product that will ultimately become a standard product offering to all network participants, or if it's just a simple custom connection to facilitate your credit union's desire to do business with a certain vendor. This analysis will not only determine whether we move forward and how, but also whether CU*Answers will help fund the project.

2. **Risk Assessment**

   Our compliance and security experts will perform a risk assessment that will evaluate, from our perspective, any potential risks to your credit union, as well as to the CUSO and other network participants.

3. **Data Security Evaluation**

   Among other things, projects will be considered according to the vendor's ability to adhere to standards like these:

   - **Data Retrieval SSO:** Server-to-server request establishes authentication and authorization, member data and response is sent over the wire fully encrypted. HTTPS and IPSec is used to secure transmission of data.
   - **3rd Party Website SSO:** Server-to-server request establishes authentication and authorization, returning a session token and URL to the client server. HTTPS and IPSec is used to secure transmission of data. Session token is used to direct the member to the requested web resource. Flexible XML delivery of required member data is established per vendor.

   *NOTE: CU*Answers does not maintain OFX servers.*

4. Code Review

This evaluation includes a more detailed analysis of the workflow, user interface, database structure, and other elements to look for overall compatibility with our current infrastructure. In a nutshell, this evaluation is to determine whether the project is even *possible* within our existing hardware and software framework.

Decision Checklist for New Projects

Following are factors that will be needed for evaluation of your project:

☐ What will the **end-user interface** look like? Where does the jump happen (in other words, what do members/staff see and what do they click on)?

☐ Will **enrollments** or other status information need to be kept synchronized between the vendor and CU*BASE? Does the system need to evaluate **member eligibility** even to sign up to use the service? *(Such as if you wanted to offer an SSO only for your business accounts or members with certain types of checking accounts.)* What database infrastructure and end-user tools will need to be added to CU*BASE to support this synchronization or rule set? *This will affect implementation windows based on the need to coordinate with CU*BASE software release schedules.*

☐ Will **activation** be controlled by a CU*BASE database element? (This is our preference is most cases, at least to facilitate our analysis of credit union participation.) Will statistical data be needed to allow for CU*BASE dashboards or other end-user tools for CU employees?

> *For example, when we developed our initial bill pay interfaces, tools were created in parallel for both CU*BASE and **It's Me 247**. Enrollment could be done by a CU employee in CU*BASE or online by the member. Bill pay activity stats were retained for use by various CU*BASE dashboard analysis tools. On the other end of the spectrum, MoneyDesktop is activated by a simple on/off flag but no enrollment or other status details are maintained on CU*BASE. An interface like the former significantly increases the project timeline to allow for CU*BASE development program efforts, in addition to the SSO work itself.*

☐ Does there need to be a **member fee posting** structure in place for members who use the service? Will it need to include relationship waivers (like age/aggregate balance, or even Tiered Service/Marketing Club waivers)?

☐ How much of the data needs to be **encrypted**? This is an critical, required security measure but does place greater strain on resources as encryption is CPU intensive. An evaluation will need to be done as to whether it will be necessary to encrypt all data elements, or just specific fields such as account base, Social Security number, etc. Likewise, to ensure that the data being shared is reasonable and does not exceed the bounds of the specific project requirements, the vendor will need to provide a comprehensive list of all data elements to be exchanged for review by our development and internal auditing teams.

☐ Do we need to enforce a **key cycle process** with the vendor (for regular exchange and rotation of encryption keys)? *Requires significant overhead to develop and manage; currently done only for the Fiserv bill pay integration.*

☐ What **activity logging and exception handling** processes will be needed?

☐ We'll also want to get a general sense of the nature of **your relationship with this vendor**: how long they've been in business, long-term prospects for ongoing development and evolution of the interface, etc. Although no one can predict the future, for everyone's sake we want to do everything we can to avoid getting into a vendor relationship that goes sour.

Related Materials

Following are related Best Practices that should also be reviewed in conjunction with your SSO project request. All are available via www.cuanswers.com (click I am a Client, then Best Practices).

- Secure Document Exchange with **It's Me 247**
- Secure Data Exchange with CU*Answers' CU*CheckViewer
- Integrating Third Party Applications with CU*BASE GOLD
- Online Banking Check Images Project Management Site

Project Steps

Procedures

To initiate a formal request, use the procedures outlined in the separate "Initiating a Special Project Request" document, or simply contact any Client Service Representative to get the ball rolling.

Typical Development Timelines

Every integration project is unique. The exact development timeline will depend heavily on specific project requirements, similarities to existing interfaces, vendor responsiveness, and many other factors. Something as simple as activating an existing data retrieval interface might require only a few weeks, while a full-blown integration with data synchronization or exchange elements might require a minimum of six months or more to complete, plus time for beta testing, documentation, and other implementation rollout tasks. Therefore, as described previously, a timeline will be estimated for you after the initial evaluations have been completed.