Technical Specification

Conflict Notification Tool

5-Oct-2017

Document Version v0.1

Document No: TBD



Author(s): Edward Martini / Marc Johnson

This document and any attachments, supplements, or references contains Bracket information that is privileged, confidential or otherwise exempt from disclosure under applicable law and is intended solely for the use of the individual(s) to whom it was intended to be addressed. If you are in possession of this document by mistake, or you are not the intended reader, any disclosure, dissemination, distribution, copying or other use or retention of this document or its substance is prohibited. If you have received this document in error, please immediately notify Bracket in writing that you received this document by mistake and also permanently delete the original and all electronic or physical copies of this document and any attachments and supplements.

Document Details

**PRODUCT NAME**: Conflict Notification Tool

**DOCUMENT TYPE:** Technical Specifications Document

**DOCUMENT ISSUE DATE:** 5OCT2017(v 0.1)

**DOCUMENT NO.:**  TBD

Authorized Document Approvals

| Name and Title/Organization | Signature | Date |
| --- | --- | --- |
| Ed Martini,  **TBD** | As author, my electronic signature on this document indicates that I acknowledge that this document is accurate, complete and contains the necessary degree of detail to accomplish the intended purpose. | See electronic signature |
| Stan Chow  **Manager, Product Analysis, Product Innovation** | My electronic signature on this document indicates that I have inspected the content and format of this document and have found no errors or omissions that are substantive enough to prohibit its use. | See electronic signature |
| Steve Battisti  **Product Manager, Product Management, Product Innovation** | My electronic signature on this document indicates that I have inspected the content and format of this document and have found no errors or omissions that are substantive enough to prohibit its use. | See electronic signature |
| Dorean Downing  **Associate Director, Product Development, Product Innovation** | My electronic signature on this document indicates that I have inspected the content and format of this document and have found no errors or omissions that are substantive enough to prohibit its use. | See electronic signature |
| Mansour Shamsai  **Manager, Product Testing, Product Innovation** | My electronic signature on this document indicates that I have inspected the content and format of this document and have found no errors or omissions that are substantive enough to prohibit its use. | See electronic signature |
| Samuel Whitaker  **Chief Technology Officer** | My electronic signature on this document indicates that I have inspected the content and format of this document and have found no errors or omissions that are substantive enough to prohibit its use. | See electronic signature |
| Thomas Barlow  **Associate VP, Total Quality Management** | My electronic signature on this document indicates that I have inspected the content and format of this document and have found no errors or omissions that are substantive enough to prohibit its use. | See electronic signature |

Document Revision History

| **Version** | **Date** | **Reason for Changes** |
| --- | --- | --- |
| 0.1 | 5OCT2017 | Draft document created. |
|  |  |  |
|  |  |  |

Table of Contents

[1. Introduction 5](#_Toc494805721)

[1.1 Document Purpose 5](#_Toc494805722)

[1.2 Audience 5](#_Toc494805723)

[1.3 Document Conventions 5](#_Toc494805724)

[1.4 Document Scope 5](#_Toc494805725)

[1.5 References 5](#_Toc494805726)

[1.6 Glossary and Acronyms 6](#_Toc494805727)

[2. Executive Summary 7](#_Toc494805728)

[2.1 System Architecture Solution 7](#_Toc494805729)

[2.2 Operating Environment 7](#_Toc494805730)

[2.3 System Architecture Impact 7](#_Toc494805731)

[3. Current System Summary 8](#_Toc494805732)

[3.1 Summary of Functions 8](#_Toc494805733)

[3.2 Application Flow 9](#_Toc494805734)

[4. Proposed System Enhancements 10](#_Toc494805735)

[4.1 Summary of Functions 10](#_Toc494805736)

[4.2 Application Flow 11](#_Toc494805737)

[Appendix A SSO Operational Flowchart 12](#_Toc494805738)

# Introduction

The Conflict Notification Tool gives users the ability to view packages that have been processed with conflicts. The user also has the option to resolve conflicts if applicable.

## Document Purpose

This Technical Specification Document contains the technical specifications for enhancements to the Conflict Notification Tool.

The purpose of this document is to provide the technical details and methodologies that would be necessary to enhance the Conflict Notification Tool from a security compliance perspective.

## Audience

This document is intended for Project Managers, Product Test Engineers, and Product Developers. Each team member or role uses the information in the following way:

| Project Team Member/Role | Use |
| --- | --- |
| Project Managers | Determine requirement needs to manage the project. |
| Product Test Engineers | Review recommendations for developing test plans and test cases. |
| Product Developers | Review recommendations for security and compliance enhancements for the product. |

## Document Conventions

The following conventions are contained in this section:document standards.

### Document Standards

The following typographical standards are used in this document:

| Font Convention | Type of Information |
| --- | --- |
| **Bold** type | Important terms and literals |
| Italic type | Variables and document names |
| Courier type | Commands that are typed and samples |

## Document Scope

The technical specifications define how the required enhancements to the Conflict Notification Tool will be met. The scope of this document is limited to the enhancements to the Conflict Notification Tool. Whenever necessary, this document refers to other design specifications that cover already-existing or standard functionality.

## References

The following is a list of references that apply to this project. All documents in this list reside in the document management system (SOPs, STDs, etc.) or in the designated development collaboration environment (SDKs, other PRDs, etc.), unless otherwise specified.

* *SOP-RD-001—Software Development Lifecycle*
* *SOP-RD-002—Product Testing*
* *SOP-RD-005—Software Development*
* *SOP-RD-006—Product and Functional Requirements*
* *SOP-RD-007—Design Specifications*
* *STD-RD-001—Software Development Standards and Lifecycle*
* *Bracket Scientific Services Dictionary of Terms*
* *Your Partner Application User Requirements Document*

## Glossary and Acronyms

The following is a list of common terminology and acronyms used throughout this document.

| Term | Definition |
| --- | --- |
| Framework | Foundation |
| ADO.NET | Framework |
| SOA | Service-Oriented Architecture |
| UDF | User-Defined Functions (typically name/value pair) |
| UI | User Interface |

# Executive Summary

The contents of this section fulfill the following requirements:

Overview here

## System Architecture Solution

***Technology stack***

1. Microsoft .Net Framework, version 2.0
2. VB.NET
3. SQL Server 2005/SQL Server 2008

## Operating Environment

The Your Partner SSO system is a Bracket built website developed using:

* Microsoft .NET Framework 2.0,
* VB.NET,
* SQL Server 2005/SQL Server 2008
* The application is a web .NET application.

The transactional data is stored in a SQL Server 2008 database (UBCUserAuthentication).  Each table in the database will have a parallel audit table in a comparably named\_audit database (UBCUserAuthentication\_Audit).  Triggers will be implemented on all transactional tables which will insert a row into the corresponding audit table whenever a row is inserted, updated or deleted.  The rows in the audit table contain the action (insert, update or delete) and the date time of the action.  The transactional tables capture the user and date time each row is created and the last modification was made.

The minimum hardware and software requirements for the Your Partner SSO application are as follows:

**Hardware Configuration**

* 4GB RAM
* Intel Core 2 Duo CPU, 2.53 GHz or faster processor
* 40 GB hard drive

**Software Configuration**

* Windows 2003 Server or higher

**System Architecture Solution**

The application is a web Forms application. The application makes use of Infragistics Web, UltraWebGrid, UltraWebTab, WebDataInput and WebDateChooser components. UBC components are used for common tasks such as group and user authentication, database access, logging, and other utility tasks.

## System Architecture Impact

There are no significant architectural changes from previous versions.

# Current System Summary

## 3.1 Summary of Functions

The Bracket Your Partner Web Single Sign On application is a web-based application that has been implemented to provide a single location for user login validation and authentication for Bracket's other web-based applications.

**Login and User Authentication**

**State**

**Application Access and Availability**

### Login and Authentication

User account authentication is performed via a DLL developed to authenticate user supplied credentials against Active Directory. The Active Directory domain used for authentication is determined by both application configuration and user attributes. The YourPartner web.config file contains keys that designate the Active Directory designation for Internal and External accounts. The key "ADDomainInternal" contains the name of the Active Directory to be accessed. Typically this is "UBCMAIN.com", although a "Dev.Pharmastar.local" domain was implemented for development purposes . The key "ADDomainExternal" contains the name of the Active Directory to be accessed. Typically this is "CP.UBCMAIN.com."

Currently there are several concerns regarding the "Forgot your password" and "Forgot your username" features that are addressed in a separate document.

**Internal vs. External Users**

User accounts are designated as Internal or External by a bit field in the is\_employee column in the Users table in the UBCUserAuthentication database. A value of 1 indicates an internal user, a value of 0 indicates an external user. Internal users login using their UBCMain login and password and are authenticated against the UBCMain Active Directory. External users are authenticated against the CP.UBCMain Active Directory.

**Electronic Signature Acceptance**

After successful authentication, the user is directed to an "Electronic Signature Acknowledgement" acceptance form. Without accepting this declaration, the user is not logged in and is returned to the login page.

### State

### Upon acceptance of the "Electronic Signature Acknowledgement," the YourPartner website writes an in-memory, automatically expiring cookie to the web browser. Currently, this cookie contains the following pieces of data in plain text:

* IsAuthenticatedWithAD: a true/false value that designates that the user has been authenticated
* Username: the user's username in the UBCUserAuthentication database and the Active Directory username.
* UserType: internal vs external?
* UserFirstName: from the UBCUserAuthentication database.
* UserLastName: from the UBCUserAuthentication database.
* MasterRaterId: from the RaterQualificationProd database, if applicable.
* CandidateId: the user's userID from the LZ-RTS database (LearningZone)
* LegacyCandidateId: left over from an older version of LearningZone. No longer supported.
* ShowTasksFilterOption: internal LearningZone filtering option.
* FromUM: bit to indicate the user arrived from UserManagement to bypass login requirement for linked accounts
* FromUMCandidateID: the LearningZone account ID linked to an RDA Master account

It is this cookie that is referenced by Bracket's other Web-based applications to determine whether or not the user is logged in and authenticated, or whether bypass the login for linked accounts.

### Application Access and Availability

A user who successfully logs in to YourPartner and receives the cookie is redirected to the YourPartner LandingPage.aspx. This page displays tabs and hyperlinks allowing the user to be redirected to the web-based Bracket applications that they have been authorized to access. This authorization is configured via Bracket's User Management web application. The access link provided by YourPartner only provides the hyperlink to the individual application and does not necessarily convey any specific access role.

The UBCUserAuthentication database contains the data relevant to user and application access . Tables relevant to access and availability are as follows. The **application\_lkup** table contains the list of integrated applications, the related Active Directory security group, the application URL (for REACT and portal applications), sequencing information (although it appears that this is not used), internal vs. external bits and relevant audit data. The **users** table contains the Active Directory username of each user, the RDA, LMS and Legacy LMS User IDs, a bit field indicating whether or not the user is a Bracket employee, the Active Directory domain that the user authenticates against, "Forgot Password" security question and answer data, a field for user language (although it appears that this is not used) and relevant audit data.

The links that are provided for user access are currently hard-coded in the YourPartner application. In order to provide an additional application link (or tab) in YourPartner, the solution must be updated, recompiled and redeployed.

**Application Security and Access Roles**

Bracket's User Management web application provides users the ability to grant or remove base access to an SSO-integrated application. User account access, roles and permissions for each user must be configured within each individual application internally.

## Application Flow

See Appendix A for flowchart

# Proposed System Enhancements

## 4.1 Summary of Functions

Security enhancements

### Login and Authentication

### No changes to Login and Authentication methodology are currently proposed, however, there are several concerns regarding the "Forgot your password," "Forgot your username" and password reset features that are addressed in a separate document.

### State

The browser cookie used by YourPartner will be encrypted. Having the browser cookie stored in plain text makes its contents vulnerable and exposes the application to being hijacked. For example: is easy to view and modify the cookie contents in the web browser. In order to spoof someone else's credentials, in RaterStation, all someone needs to do is know the username of a valid user, update the "UserName" cookie value in the web browser to reflect someone else's username and proceed to RaterStation. This will force RaterStation to use the spoofed username for security and data access, allowing any user to view data (but not necessarily save data) as the spoofed user.

This allows RaterStation users to see data that they otherwise might not be able to see.

### Application Access and Availability

The application hyperlinks presented by YourPartner will be stored in the database and dynamically built rather than being hard-coded. This will involve dynamically generating tabs using the Infragistics controls.

### Functional Requirements

**Cookie Encryption - More Secure Statement Maintenance**

In an effort to make the cookie storage of local data more secure, the data contained in the cookie should not be stored (or transmitted) in plain text. SSL provides an encryption process for the transmission but not the storage. The process for encrypting this information is straightforward and should consist of encrypting the cookie attributes and their respective values. The encryption process will need to use a key shared by each application and be reversible so that the data can be encrypted prior to creating the cookie and decrypted on post-back in the applications. This will allow the data to be stored safely and still be usable by the applications. Alternatively, if a key shared amongst all applications isn't recommended, the data can be stored in such a way that will allow for multiple data sets, each keyed and encrypted for individual applications, each with their application-specific key.

**More Secure But Not Hijack-Proof**

Encrypting the cookie data above will help secure the data in the browser and make it more difficult to hijack an authenticated session or spoof a different user's access. This encryption will, however, not help if someone copies the encrypted cookie from one machine (or browser session) and inserts the encrypted values into another. Making the cookie-stored data harder to swap between users and/or machines, another encryption approach can be taken. In addition to the above recommendation or a shared encryption key (or application-specific keys, if desired), the encryption key should be augmented using some other piece of data. To maintain machine-specific recognition, the encryption key should be encrypted using a combination or a shared (or application-specific) key and the requesting machine's IP address (in whole or in part). This would make the process of copying valid encrypted cookie data from one machine to another, making it significantly more difficult to replace effectively or to spoof.

**Caveat - Proxy Server**

Adding the additional layer of a machine-specific combination key work well, in theory, for all cases with the exception of environments that use a proxy server for YourPartner access. After multiple inquiries to IT and TD, it is not currently known which clients (if any) use a proxy server to access Bracket's YourPartner and other applications. The concern with proxy server access is that the machine-specific cookie combination will not be exactly machine-specific. I t would still be possible to copy encrypted cookie information between multiple machines effectively under this scenario. Whereas the encryption would certainly make the cookie significantly more secure than plain text, it would not have the extra added benefit of the machine-specific encryption .

**Effected Applications**

Both of these require security augmentations to each of the SSO consuming applications currently used by YourPartner. These include, but are not limited to) Rater Station, UBC Document Upload (if still used), VERIFIED (if still used), Learning Zone, Device Management, Conflict Management Tool. Most of these should be relatively minor updates to the application's security class, however, each will need to be looked at individually.

Bracket's User Management carries one additional caveat. User Management contains a built-in SSO bypass mechanism to access RDA Linked accounts. This access bypass would be encrypted as well but because it is used on a regular basis, it would also need to remain in place.

**Dynamically display application links - Enhanced Application Access and Availability**

While not a security update, while Bracket is making modifications and enhancements to YourPartner, the methodology YourPartner uses to generate and display hyperlinks should be updated. Currently the hyperlinks and organization tabs are hard-coded in the YourPartner application. Since the application was designed this way, each time a new application is integrated into SSO, YourPartner needs to be rebuilt and re-deployed. This means downtime, additional testing and the possible introduction of environmental, build or other software integration issues.

The UBCUserAuthentication database already contains a column in the application\_lkup table to hold the URL for the application. For the most part, this column is unused. An enhancement should be made to the YourPartner code base to take advantage of this column and have the data populated for integrated applications. After that point, the application can be updated to generate these hyperlinks (along with their related 'grouping' tabs) dynamically. This would remove the need to rebuild and re-deploy the YourPartner website each time a new application is integrated.

**Forgot Username and Forgot Password Enhancements - Login and Authentication Security**

The current mechanisms through which YourPartner allows users to both retrieve their username and reset their password create certain security issues that should be addressed in the application. Further explanation and recommendations are detailed in a supplemental document.

**Code and Technology usage**

Code samples and specific technologies to be used have been intentionally left out of this document so that the approach and implementation details can be discussed and agreed upon prior to implenentation.

## Application Flow

* No changes to the application flow are proposed.

1. SSO Operational Flowchart

