# xpedx.com Next generation

# *B2B Security Design Document*

**Authors: Sterling Commerce**

**Date Created:** 5/9/2010

**Last Updated:** 8/26/2010 8:14 AM

**File Name:** C:\Documents and Settings\bfurman\My Documents\Temp\Methodology v1.1\Project Management\TEMPLATE - DOCUMENT - Use Case Definition.docxpedx Security Detail Design Doc V1.3.docx

Approval Signatures (Mandatory)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Title** | **Name** | **Signature** | **Date** | **Comments / Issues / Concerns** |
| **xpedx Owner(s)** | Steve Bugher |  |  |  |
| Cheryl Tullis |  |  |  |
| **Sterling Commerce Owner(s)** | Guy Read |  |  |  |
|  |  |  |  |

**Note**: The sign off indicates approval of all sections of the document.

Document Revision History

This chart tracks the changes introduced by the revisions to the document as the project progresses through the stages of the System Development Life Cycle (SDLC).

| Version | **Date** | **Description (Changes Made)** | **Author(s)** |
| --- | --- | --- | --- |
| 0.1 | 05/09/2010 | Initial Draft | Sterling |
| 1.0 | 05/13/2010 | Ready to deliver | Sterling |
| 1.1 | 7/30/2010 | Updated with feedback | Sterling |
| 1.2 | 8/18/2010 | Updated with feedback from meeting 8/18 | Sterling |
| 1.3 | 8/26/2010 | Updated with feedback 8/26/2010 | Sterling |

Related or Reference Documents

| Document Name | Description | Owner | Location |
| --- | --- | --- | --- |
| SCI\_Xpedx Solution Definition Document v1.5 | Solution Definition document | Sterling Commerce |  |
|  |  |  |  |
|  |  |  |  |

TABLE OF CONTENTS

1. Introduction 4

1.1 Document Purpose 4

1.2 Document Audience 4

2 Security 5

2.1 Functions & Solution 5

2.1.1 xpedx users 5

2.1.1.1 Security Admin 5

2.1.1.2 Internal Users 5

2.1.2 Customer Users 6

2.1.2.1 Regular Customer User 6

2.1.2.2 B2B Customer User 6

2.1.3 Anonymous Users 6

2.1.4 Other functionality changes 6

2.1.4.1 Data Security Policies 6

2.1.4.2 Security Logging 7

2.1.4.3 Password Policies 7

2.2 Master System 9

2.3 Implementation Details 9

2.3.1 Entity objects. 9

2.3.2 Actions involved and Functions 9

2.4 Process Flow 9

2.5 Field Mapping 10

2.5.1 Check Valid UserId Mapping 10

2.5.2 Login Mapping 10

2.6 Schema 10

2.7 Screen Shot 11

2.8 Open Questions 13

2.9 Assumptions 13

3 Connectivity Diagram 15

3.1 Sterling to Active Directory Connectivity Diagram 15

3.2 Connectivity Process 15

4 Glossary of Terms 16

# Introduction

## Document Purpose

This document is the governing functional design document for the overall Security functionality. It presents significant decisions and constructs used in developing the functionality. Testing, builds, configuration management are not covered in this document.

The document will also serve the purpose of keeping a list of assumptions that were made during design discussions.

## Document Audience

This document is intended for management and technical staff working on this project, xpedx IT and Business, webMethods, Legacy(MAX and ACCESS), HP, IW, xpedx/IP Network Team. Sterling will use the document during design and configuration for design consideration.

# Security

## Functions & Solution

Security in the context of xpedx.com NG refers to the setup of various types of users within the system along with the ways by which they can login into Sterling.

What a user sees and is able to access once they login is controlled by Roles and permissions that are not in scope of this document.

The basic types of users in the system are

1. xpedx users
   1. Security Admin
   2. Internal users (CSRs, Division Admins, eBusiness Managers, etc.)
2. Customer users
   1. Regular dotcom customer user
   2. B2B transactions customer user
3. Anonymous users

## xpedx users

## Security Admin

Created using the Application manager. These users will not have any other role than to create internal users in the system.

## Internal Users

They are created by Security Admins in Call Center. At the time of user creation, the Security Admins also assign the relevant roles to the Internal Users.

The roles that have been identified so far are

1. Sales Reps
2. CSRs
3. Division Admins
4. Credit
5. Sales Manager
6. eBusiness Admins

Internal user passwords are managed via a separate internal system, that is not linked to Sterling. However authentication is done by Sterling via LDAP. The following use cases are to be supported.

1. When internal users are created in Sterling, there is a validation step. Once the user ID (xpedx network ID) is entered, Sterling makes a call to LDAP to verify if the user exists. Only if this check passes, the user is created in Sterling.
2. During internal user creation, after the network ID has been verified in LDAP, we fetch the first name/last name/email address and employee ID fields from LDAP and pre-populate this information into the relevant fields.
3. All internal users login using their userid (xpedx networked) and password. The userid/password are validated against LDAP to allow login into Sterling. This is for all applications through which internal users can login. The process of Sales Reps logging into Web Channel is being tracked in JIRA 209.

## Customer Users

Customer users – The first customer user (with an admin role) will be created by an Internal User like a CSR using Call Center. The subsequent customer users may be created by the customer admins themselves using the web channel.

## Regular Customer User

Created by either customer admins or internal users with appropriate roles (e.g. Sales Reps). These users will log into the Web channel for their entire shopping experience. Customer users will be able to manage their passwords through the web channel.

The password reset mechanism sends an email to the email address on file for the user. Customer admins should be able to request password resets for regular customer users. Once a password reset is requested by a customer admin, the email is sent to the customer user to rest the password themselves.

## B2B Customer User

These user are created by Customer admins or by Internal users with the appropriate roles. For the B2B Stock Check webservice and the B2B Punchout interfaces that are exposed to the customer, the user is authenticated against the passwords stored in the Sterling database.

Since B2B users can’t login through the web channel directly, their passwords are managed by customer users that have the admin role or are eBusiness managers.

There are two types – B2B Stock Check Webservice users and B2B Punchout users. B2B Order Place, Order Place ACK and Invoice do not require specific users to be setup.

George – 5/21 - If the purpose is for integration (to validate account credentials), then it needs to be restricted to Customer Solutions.

## Anonymous Users

For users to anonymously access the catalog at the various storefronts, Sterling has the Anonymous User construct. An anonymous user will need to be setup for each storefront through the Application Manager. All users that land on the storefront will behind the scenes be logged in using this generic login.

## Other functionality changes

## Data Security Policies

The xpedx.com site will have a footer element that links to xpedxs’ data security policies.

## Security Logging

xpedx needs to be able to track the login activity of users. This will be done through the logs that will capture these events.

xpedx needs to track role changes for a user. These are also tracked through the logs.

Based on latest reporting/data warehouse discussions, these are no longer reported as events.

## Password Policies

Xpedx has defined standards for passwords that may be used to access systems. These are applied only to external users. All internal users are tied to their networked and their passwords follow the policies defined for Active Directory.

Managing system access, like controlling physical access, is a critical part of an organization's Information Security program.  System users must have a unique user account and a password. The password must meet the following standard requirements for complexity. The standard requirements must be implemented and enforced at the system level.

|  |  |
| --- | --- |
| **Requirements** | **Baseline Standards** |
|  | Authentication Systems must implement complex passwords that meet the standards defined in RQ 2-18 |
|  | Password minimum length = 8. |
|  | Password maximum length = 14. |
|  | Password must contain at least two (2) alphabetical characters = Yes |
|  | Password must require at least one (1) numeric character = Yes |
|  | Password must require at least one (1) Upper Case character = Yes |
|  | Password must require at least one punctuation character or special character (!# @ % ^ & \* ) = Yes  This requirement does not apply to any passwords. |
|  | Password must not contain the characters ‘!’, ‘$’, ‘?” |
|  | Maximum repeated characters = 2 |
|  | The password must not allow the user’s first name  Steve – 5/20 - Not a requirement at xpedx |
|  | The password must not allow the user’s last name  Steve – 5/20 - Not a requirement at xpedx |
|  | The password must not allow the user’s Login Name |
|  | Maximum password age in days = 90  No Limit based on policy exemption. |
|  | Minimum password age in days =  1  Can’t change password (within the same day). Jasmine to check if this applies to External Users. [ Jasmine – 5/19 - When the password is reset the user will be forced to change the password when he logs on next time.] Not a requirement at xpedx. |
|  | Disallow the last five (5) passwords when creating a new password |
|  | Present a warning message of password expiration beginning fourteen (14) days prior to expiration  Jasmine to check if this applies to External Users. [Jasmine 5/19 - This doesnot apply to Next Gen confirmed from our Audit Remediation project. The password never expires] |
|  | After ten (10) failed attempts to log in with a valid user ID and an incorrect password, the user ID must be locked  Current site is 5 attempts. No time limit.  Username is locked and CSR must be contacted to unlock. [Steve B. – 5/20 - Bugher: process is that once the ID is locked the user must use the ‘Forgot Password’ feature to request a temporary password be emailed to them, or call the eBusiness Support Desk and they will enter a temporary password for the user]. [Prashant 7/30 – The last part does not work together with the requirement from George that a CSR should not be able to login into a customer account.] |
|  | Locked user ID **must not** be configured to automatically unlock after a specific time period |
| **Guidelines** |  |
|  | Where temporary or first time passwords are assigned to a user, that password should be complex.   [Steve B – 5/20 - .   Bugher: to clarify, the password rules should apply consistently to a new or changed password] |

Additional Requirements for System Security (Jasmine – 5/19)

|  |  |  |
| --- | --- | --- |
| **Forced Change of All Passwords after System Compromise** | | |
|  |  |  |
|  | http://swnapps03.ipaper.com/icons/ecblank.gif | http://swnapps03.ipaper.com/icons/ecblank.gif |
| Whenever a system has been compromised, system managers must immediately change the password of every account on the involved system. Even suspicion of a compromise requires that all passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded. Similarly, under either of these circumstances, all recent changes to user and system privileges must be reviewed for unauthorized modifications. See policy 1.1.3 for requirements on reporting compromised systems. | | |

This will be achieved using a cron job that will be initiated by IT to reset all user passwords on demand.

|  |  |  |
| --- | --- | --- |
| **Forced Change of Passwords after System Administrator Leaves** | | |
|  |  |  |
|  | http://swnapps03.ipaper.com/icons/ecblank.gif | http://swnapps03.ipaper.com/icons/ecblank.gif |
| Whenever an administrator with a privileged account leaves the company, and the privileged account cannot be removed, system managers must immediately change passwords for the account. | | |

An account in Sterling can be deactivated. Hence there is no need to reset password of the system administrator that leaves. Just deactivate his/her account.

|  |  |  |
| --- | --- | --- |
| **Password Disclosure by Security Administrators** | | |
|  |  |  |
|  | http://swnapps03.ipaper.com/icons/ecblank.gif | http://swnapps03.ipaper.com/icons/ecblank.gif |
| Security administrators must only disclose passwords if a new user-ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of his or her user-ID. Security administrators must not reveal a password unless the involved user has first provided definitive evidence substantiating his or her identity. | | |

In Sterling the security administrators do not enter any user passwords. Passwords are generated automatically and sent to the email id on file. The admin does not see the password being sent.

|  |  |  |
| --- | --- | --- |
| **All Accounts must Have an Owner** | | |
|  |  |  |
|  | http://swnapps03.ipaper.com/icons/ecblank.gif | http://swnapps03.ipaper.com/icons/ecblank.gif |
| All accounts must be assigned to one owner, responsible for its use. [Steve B – 5/19 - who is the owner for an account that has no users assigned to it?] [Prashant – 7/30 – Not sure what this requirement means. Could you please clarify. What account is being referred to here?] | | |

|  |  |  |
| --- | --- | --- |
| **Disclosure of Incorrect Log-In Information** | | |
|  |  |  |
|  | http://swnapps03.ipaper.com/icons/ecblank.gif | http://swnapps03.ipaper.com/icons/ecblank.gif |
| When logging into an International Paper system, if any part of the log-in sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the log-in process was incorrect. | | |

This is the standard behavior in Sterling.

## Master System

N/A

## Implementation Details

## Entity objects.

## Actions involved and Functions

## Process Flow

## Field Mapping

The following mapping contains the fields that are received from Active Directory so that a user can be created in Sterling.

## Check Valid UserId Mapping

## Login Mapping

Use standard LDAP protocol to verify that the networkID/password entered by user is authenticated by Active Directory.

## Schema

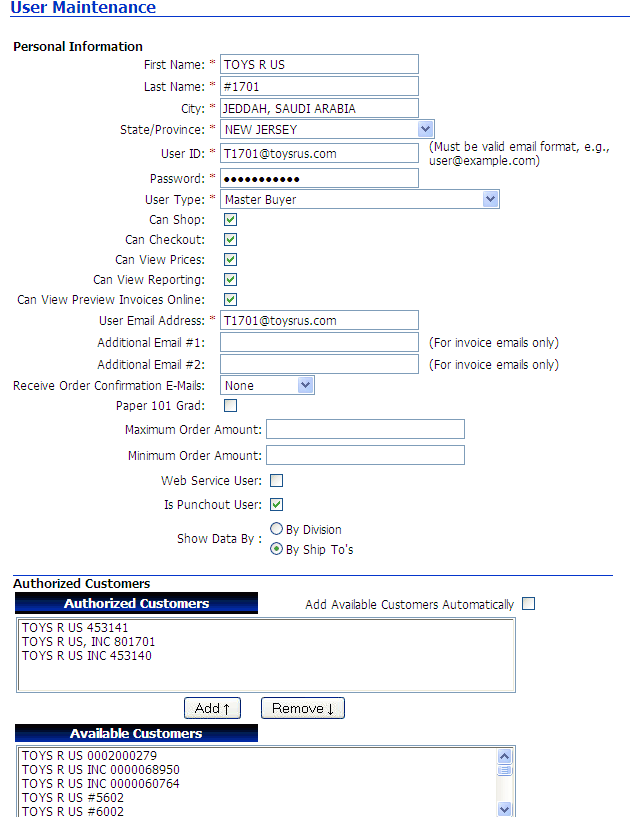
The fields that are present and relevant to Sterling in Active Directory are -

|  |  |
| --- | --- |
| **Field Name** | **xpedx Active Directory Attribute/Property Name** |
| Network ID | sAMAccountName |
| First Name | givenName |
| Last Name | sn |
| Employee Id | employeeNumber |
| User Email Address | mail |

## Screen Shot

***Security Admin/Internal User Setup Page***

***Customer User Setup Page***

******

## Open Questions

1. Are security admins also created/authenticated against LDAP? [George T. – 5/21 - Yes, they will be authenticated against LDAP.] [Jasmine – 5/19 - They will be created directly in the database.] [ Prashant 7/30 – Creating users directly in the DB is not supported in Sterling.]
2. Need LDAP tree structure to see what data is stored and what the gaps maybe. [Jasmine – 5/19 - . Will schedule a meeting next week.] [Prashant – 8/11 – received information from Active Directory team]
3. Need to define process of creating internal users – do we need to check id against LDAP at creation time or is it enough to do so at login time ? [Jasmine – 5/19 - ? Check at creation time. If the internal user doesn’t exist in Active Directory, user won’t be created.]
4. Need to define the field mapping to create internal/external users. [Jasmine – 5/19 - This will be covered under user and customer profile.] [ George T – 5/21 - Jasmine, I think it should be in this document. Customer profile DDD should focus on functionality of each field.]
5. How to enable Sales Reps access into the dotcom via Web Channel. [Jasmine – 5/19 - . This was already discussed. The customer selection screen should have these selctions: Division, legacy system, customer name, customer number, city, state and postal code.] [George T – 5/21 - . Customer batch will contain Sales Reps employee ID. Sales rep can access only if their employee ID is associated with the customer account. I probably answered a slightly different question. But, hope the information helps.][Jasmine – 8/18 – Tracked via JIRA 209]
6. Can CSRs have access to the Sterling Business Center via the same login credentials ? [George T – 5/21 - ? Not sure what CSR functionality is in Business Center. Internal user will have only one user ID (network ID) and one authentication process (LDAP). So, the answer is if the user needs access to Web Channel and/or Business Center and/or Call Center, it will be the same user ID and password.]
7. Where do we authenticate punchout user? I don’t recall that the punchout request had a user-password. [Jasmine – 5/19 - Will schedule a meeting next week] [ Prashant - 7/30 – Covered in the B2B document. There is no password verification for b2b users. They work based on the shared secret and not the user’s password.]
8. Is there a way in Sterling to re-activate a user? [ Prashant – 7/30 – Yes]. . [George – 8/3 – Reference ootb documentation on how to activate/deactivate the user]
9. Need to investigate Sterling’s ability to report on the login activity of a user. [ Prashant – 7/30 – being handled by webtrends]
10. For password reset, xpedx would like a one-time randomly generated temporary password to be sent to the user’s email address. Is this possible in Sterling? [Prashant – 7/30 – Yes]
11. Verify that all the password standards specified in the Password Policies section can be supported in Sterling.
12. Xpedx will need to ensure that all the user passwords being migrated meet the criteria, else the migration will fail.
13. Communication between Sterling and Liaison will need to be authenticated, else anyone could potentially place orders using an XML tool. Need to work out some process for this.
14. [ Jasmine – 5/19 - Can we validate e-mail address at user creation?] [Prashant – 7/30 – How would you like the process to work? Typically email verification happens in self-registration systems. If we are talking about just making the admin enter the user’s email address two times, that could be done with some customization]. [George – 8/3 – The ootb create new user functionality that sends an email to the user’s email address fulfills this requirement.]
15. [Jasmine – 5/19 - Forgot User Id process? If the user forgets the user Id, user will be asked to enter e-mail address, if this matches the e-mail address on the system then send the user id to this e-mail address]. [Prashant – 7/30 – This is not supported ootb in Sterling. If this is a requirement will need to custom code]. [Steve – 8/3 – Not required as long as the user name can be searched in Call Center using email address.]
16. [Prashant – 7/30 – Since we are not allowed access to the AD/LDAP from Sterling, we are unable to test connectivity or get a feel for the fields that are stored in LDAP. Please provide mapping of fields as well as real data samples of the kind of data we can expect from AD] [ Prashant 8/11 – done.]

## Assumptions

1. Internal Users are created manually by the Security Admin. They are setup using the Sterling Call Center Application.
2. Internal Users do not have access to the Application Manager.
3. Customer users are created by Internal Users, based upon the role that they are assigned to (e.g. Sales Reps can create customer users, but Credit users cannot). [George T – 5/21 - Has this been defined anywhere?] [ Prashant – 7/30 – In the User roles document]
4. External users are allowed a email id like LoginId.
5. Internal users are to use their Network Id are the LoginId.
6. For BR1 Anonymous users only have access to the catalog browsing functionality.
7. Internal users will not be deleted from the database, they will only be deactivated. [George T – 5/21 - What is the process to activate them?] [ Prashant – 7/30 – This is done by the active checkbox in Call Center]
8. User data will be reported on from Data Warehouse.
9. Sterling stores the user passwords in encrypted form.
10. Only 4 fields are retrieved from LDAP to populate user information. These are rarely changing fields and hence will be kept in sync with between Sterling/LDAP using a manual IT process.

# Connectivity Diagram

## Sterling to Active Directory Connectivity Diagram

The Active Directory system is available on the internal network to all machine. Since we are no longer developing web services to fetch user data from AD/LDAP, there is no need to specify a connectivity diargram/process.

## Connectivity Process

N/A

# Glossary of Terms

|  |  |  |
| --- | --- | --- |
| S. No. | Term | Definition |
| 1. | WSDL | Web Services Definition Language |
| 2. | UE (User Exit) | Hooks to write custom code in Sterling |
| 3. | MQ | Message Queue |
| 4. | BR1 | Business Release 1 |
| 5. | IW | Industrial Wisdom – UI firm engaged on the project. |
| 6. | AD | Active Directory – Miscorsofts’ implementation of LDAP |
| 7. | LDAP | Lightweight Directory Access Protocol |