**SAML v2 Authentication**

**Project name:**

**Application name:**

**SB991 number:**

**(If applicable)**

**Customer:**

Version: 0.0

Date: mm/dd/yyyy

Status: Unapproved

**For more information**

|  |  |
| --- | --- |
| **ITS contact** | **Customer contact** |
| Name: | Name: |
| Title: | Title: |
| Phone: | Phone: |
| Email: | Email: |

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change Description** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**NOTE:**

In answering the following questions, keep in mind that the intention of this document is to provide information relevant to the integration of the system with NCID. The major integration points would revolve around identity management, authentication, high level authorization and auditing of these services. This document is NOT intended to collect all application requirements. To save you time, please limit your answers to requirements needed for integration with the NCID service.

Not all applications will require entries in all sections or tables. Below is a list of required sections.

* Management Summary
* Architectural Overview Diagram
* Functional Requirements with repeating necessary requirement/test cases
* Web Server Information
* Acceptance Criteria
* User Training Information
* [Acceptance Criteria Approved](#_Toc318803838)
* [Application Contact Information](#_Toc318803839)
* [Customer Application Contact Information](#_Toc318803840)
* User Profiles

If you have questions or need additional guidance, please let us know.

**Table of Contents**

[1 Introduction 4](#_Toc383521855)

[1.1 Management Summary 4](#_Toc383521856)

[1.2 Assumptions 4](#_Toc383521857)

[1.3 Architectural Overview Diagram 4](#_Toc383521858)

[1.4 Definitions 4](#_Toc383521859)

[Table 1 - Definitions 4](#_Toc383521860)

[2 Requirements 4](#_Toc383521861)

[2.1 Functional Requirements 4](#_Toc383521862)

[2.1.1 Functional Requirement 1 - <Title> 4](#_Toc383521863)

[2.1.2 Functional Requirement 2 - <Title> 5](#_Toc383521864)

[2.1.3 NCID Variables Available to Be Transmitted to Service Provider 5](#_Toc383521865)

[2.1.4 Web Server Information 6](#_Toc383521866)

[2.2 Non-functional Requirements 6](#_Toc383521867)

[2.3 Priority of Requirements 7](#_Toc383521868)

[2.4 Acceptance Criteria 7](#_Toc383521869)

[3 Production Readiness Requirements 7](#_Toc383521870)

[3.1 User Training Information 7](#_Toc383521871)

[3.2 Acceptance Criteria Approved 7](#_Toc383521872)

[3.3 Application Contact Information 8](#_Toc383521873)

[Table 4 - Application contact information to assist the NCID team 8](#_Toc383521874)

[3.4 Customer Application Contact information 8](#_Toc383521875)

[Table – 5 Application support contact information to assist ITS Service Desk 8](#_Toc383521876)

[4 User Profiles 9](#_Toc383521877)

[5 Appendices 9](#_Toc383521878)

[5.1 Appendix A – Requirements assistance 9](#_Toc383521879)

[5.2 Example Functional Test Cases 10](#_Toc383521880)

[5.2.1 User Login 10](#_Toc383521881)

[5.2.2 User has valid NCID but is not in the application database 11](#_Toc383521882)

[5.2.3 User needs access to application but never registered in NCID 12](#_Toc383521883)

[5.2.4 User has an inactive state/local employee type NCID Account 12](#_Toc383521884)

[5.2.5 User Logs in with an Incorrect NCID User ID 13](#_Toc383521885)

[5.2.6 User Logs in with an incorrect NCID Password 14](#_Toc383521886)

[5.2.7 User Password has expired 14](#_Toc383521887)

[5.2.8 User Account is locked after Three Unsuccessful User Login Attempts 15](#_Toc383521888)

[5.2.9 User Logs out of the Application 16](#_Toc383521889)

[5.2.10 Session Timeout Logout 17](#_Toc383521890)

# Introduction

## Management Summary

*In this section, summarize the project’s scope.*  *This is usually extracted from the scope or project definition document. Describe the customer's needs / opportunities for the project and provide a high level overview of the project.*

## Assumptions

*Include a brief narrative of assumptions or constraints impacting the project. It may also be appropriate to include issues and rename this section accordingly.*

## Architectural Overview Diagram

* *Application Architecture: Attach a diagram which should contain the following*
* *Network links*
* *Database server and OS*
* *Application server and OS*
* *Presentation (GUI) server and OS*
* *Are any of the servers hosted by some other entity, if so show which one(s) and indicate where*
* *Any other architecture information*

*(Create the Application Architecture Diagram and insert it here)*

Figure 1 Application Architecture Diagram

## Definitions

### Table 1 - Definitions

Provide any project-specific definitions.

|  |  |
| --- | --- |
| Term | Definition |
|  |  |
|  |  |

# Requirements

This section specifies the requirements, which are the characteristics of the integration that are conditions for its acceptance.

See appendix 5.1 Appendix A – Requirements assistance for additional information.

## Functional Requirements

This section identifies the integration functional requirements. A functional requirement is a business function or capability to be included in the solution to be developed.

See Appendix A – Requirements assistance 5.1 and 5.2 for example requirements and test cases.

### Functional Requirement 1 - <Title>

***This should be either a written functional requirement or a use case.***

*For a functional requirement, it shall itemize the system/component requirements associated with the capability. If one functional requirement can be more clearly specified by dividing it into constituent functional requirements or capabilities, specify these in subparagraphs.*

*If use cases are to be documented separately, this document should, at a minimum, specify the use case name, high-level description and actors for each use case*

*Use Case Model - You may substitute your own model for use cases below.*

|  |  |
| --- | --- |
| Brief Description |  |
| Actors |  |
| Pre-conditions |  |
| Post-conditions |  |
| Basic Flow |  |
| Alternate Flows |  |
| Special Requirements |  |
| Open Issues |  |
| References  (content in other docs) |  |

### Functional Requirement 2 - <Title>

*Repeat for each functional requirement.*

### NCID Variables Available to Be Transmitted to Service Provider

Below is a list of information that can be passed to SPs if requested. Please refer to it for showing NCID requested information as noted in this document.

The table is examples of information available.

| **NCID Attribute** | **Notes** |
| --- | --- |
| Prefix | Mr., Ms., etc - Not always present |
| First Name |  |
| Middle Initial | Not always present |
| Last Name |  |
| Suffix | Jr., Sr., etc - Not always present |
| Full Name | First + Last Name |
| User ID | Can change |
| Business Phone | Not always present |
| Extension | Not always present |
| Address Line 1 | Not always present |
| Address Line 2 | Not always present |
| City | Not always present |
| State | Not always present |
| Zip Code | Not always present |
| E-mail Address | Not always present **and not unique for all users** |
| Employee Type | Full Time, Part Time, Contractor -  Not always present |
| User Type | **S** - State employee  **L** - Local employee  **B** - Business  **I** - Individual |
| GUID | Unique and does not change |
| Organization | Passed as a CN reference - Not always present |
| Division | Passed as a CN reference - Not always present |
| Section | Passed as a CN reference - Not always present |

### Web Server Information

Complete the table below for server(s) that the SAML calls will be communicated to/from for NCID.

(Please add additional rows if needed.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server Operating System** | **Version** | **Web Server** | **Version** | **Proxy**  **(Y/N)** |  |
|  |  |  |  |  |  |
| **SP Initiated SAML Integration:** | | | | | |
| **Public Published URL:** | | | | | |
| **META Data URL:** | | | | | |
| **SP SAML software manufacture and version:** | | | | | |

## 

## Non-functional Requirements

This section identifies the integration non-functional requirements which address aspects of the system/component that may not directly affect the functionality of the system/component as seen by the users. They can, however, have a profound effect on how that business system/component is accepted by both the users and the people responsible for supporting that system/component.

*The non-functional aspects of a business system/component cover a broad range of themes. The major non-functional themes identified are:*

* *Performance (including Capacity)*
* *Scalability*
* *Availability (including Recoverability and Reliability)*
* *Maintainability (including Flexibility and Portability)*
* *Security*
* *Manageability*
* *Environmental (including Safety)*
* *Data Integrity (including Currency, Locality of Updating, Data Retention)*

*In summary, non functional requirements shall specify required behavior of the system/component and shall include applicable parameters, such as response times, throughput times, other timing constraints, sequencing, accuracy, capabilities (how much/how many), continuous operation requirements, and allowable deviations based on operating conditions.*

## Priority of Requirements

Unless otherwise stated all requirements are equal in weight and should be developed at the same time and in place for the integration to move forward. Any requirements that have a less significant need (nice to have) should be listed below and noted that they will not be required to move forward, but might be developed at a later time.

## Acceptance Criteria

Unless otherwise stated all requirements are equal and must pass for acceptance of this integration. The criterion for acceptance is that the test cases listed above pass with the expected results. Additionally the integration must pass load testing as defined by the application sponsor.

# Production Readiness Requirements

The information in this section will need to be completed before moving the integration into the NCID production environment.

## User Training Information

*The User Training Information is specifications of the content, structure, audience, media, and format, of the documentation of the system/component to be used by the users. What are the tools that will be used to train users on the system and on how to gain access to the system?*

*The NCID team can assist with review of documentation the service will use to assist customers with obtaining NCID accounts and application access.*

*The User Training Information**work product consists of all documentation, on-line help, and other materials that support users in learning and using the system/component. Different User Training Information may be delivered on different media, for example: printed manuals, on-line help, computer files, reference cards, hypertext, web sites, multimedia presentations, videos, etc.*

## Acceptance Criteria Approved

The NCID team needs documentation indicating that the Acceptance Criteria has been met in the pre production (Q/A test) environment. The project sponsor, project manager or a designee may send an email indicating all functional **and** load testing passed in the pre production NCID environment.

Load testing requirements are based on your application’s needs and are defined by the agency supporting the application. ITS offers load testing services if required. Please let the NCID team know in advance that load testing assistance is needed so there is time to engage the needed resources.

## Application Contact Information

The NCID team needs the following information to assist with support of the integration between the application and NCID.

**Important Note:**

ITS provides a list on the ITS Communications Hub (<https://communications.its.state.nc.us>) to assist agencies in keeping up-to-date with changes planned for the NCID service. The list is called “NCID – Application Administrators”.

To subscribe to the list you will need an active NCID account. You may click on the link above for access to the hub. There are links to assist you with subscribing and managing your information. If you need assistance please let your NCID integrator know or open a request with the ITS Service Desk.

### Table 4 - Application contact information to assist the NCID team

|  |  |
| --- | --- |
| **Technical contact** | **Service contact** |
| Name: | Name: |
| Title: | Title: |
| Phone: | Phone: |
| Email: | Email: |

## Customer Application Contact information

The information in this section will be used to assist with handoffs between your support staff and the ITS Service Desk staff. The ITS Service Desk will use the information to help customers that call for support of NCID or your application.

The ITS Service Desk is a 24 X 7 operation. They may receive calls about the integrated application after normal business hours. The information below will assist them in providing the customer with needed information when they call in. You may enter information for a service desk, support group, or individuals. Please add any additional information you feel will assist in these communications.

Type of contact refers to the kind of support the customer will be referred to. It could be a support group (a service desk), an individual, a team, etc.

### Table – 5 Application support contact information to assist ITS Service Desk

|  |
| --- |
| **Type of contact:**  *(Service Desk, Group, Individual, etc.)* |
| **Name:** |
| **Hours of operation:** |
| **Phone numbers:** |
| **Email:** |
| **Names customer may use in reference to the application:** |
| **How to direct customer application inquires that are received after hours:** |

# User Profiles

This section identifies a set of user profiles that define the different types of user groups for the planned solution, and the key characteristics of each group.

* Identify types of users that will need access to the system (Ex: State Employees; Local Government Employees; Business Users; Individual/Citizens)
* Identify the number of expected users of each type from above
* State any peak load that the system will be designed to handle
* Show an expected 5 year growth in user base, per year

|  |  |  |  |
| --- | --- | --- | --- |
| **PRODUCTION ROLLOUT DATE: mm/dd/yyyy** | | | |
| **Year** | **User Type** | **Initial number of Users** | **Peak times of use** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |

* Depict the different levels of authorization that are required

# Appendices

## Appendix A – Requirements assistance

Functional requirements should be summarized as "verbs" that specify a required behavior of the system/component. A good functional requirement should be testable, unambiguous, understandable, concise, traceable, unique, complete, consistent, comparable, modifiable, attainable and design independent.

The degree of detail to be provided shall be guided by the following rules:

* Concentration of the requirements should be towards user account administration, authentication, authorization, and auditing needs.
* Lower level application processes that do not require additional (past the initial “login”) authorization are not required to be detailed.
* Include those characteristics of authentication, authorization, account administration and auditing for the system/component that are a condition for system acceptance.
* Defer characteristics that the customer is willing to leave up to the application developer, to design descriptions.
* If there are no requirements in a given paragraph, the paragraph shall so state.
* If a given requirement fits into more than one paragraph, it may be stated once and referenced from the other paragraphs.

Requirements are identified by the following categories:

* Functional
* Usability
* Non-functional
* External Interface
* Other

For each requirement, the following information is documented:

* Unique identifier, for traceability
* Description, stated in a way that an objective test can be defined for it
* Priority of essential, conditional or optional (see definitions in the note below); stated with each requirement
* Acceptance criteria, including acceptance method (inspection, testing, analysis, etc.); stated with each requirement
* For system requirements, a reference to its uniquely identified customer requirement
* For component requirements, a reference to its uniquely identified system requirement

**Note:** Acceptance criteria and cross-references should be documented on the Requirements Traceability Matrix, which may be referenced here to avoid duplication of information.

**Note:** The following definitions (sourced from the IEEE Standards Collection, Std 830-1998\*) may be used for priority:

* Essential - This implies that the software will not be acceptable unless these requirements are provided in an agreed manner.
* Conditional - This implies that these are requirements that would enhance the software product, but would not make the product unacceptable if they were absent.
* Optional - This implies a class of functions that may or may not be worthwhile.

\* Reprinted with permission IEEE Std. 830-1998, "Recommended Practice for Software Requirements Specifications", Copyright 1998 IEEE.

The IEEE disclaims any responsibility or liability resulting from the placement and use in the described manner.

From IEEE Std 830-1998, Copyright 1998 IEEE. All rights reserved.

## Example Functional Test Cases

These are example test cases to assist the author in creating relevant test cases for this specific integration. This is not a definitive list; other test cases will be needed.

**NOTE: For these test cases the following is assumed:**

**No application group needs to be created in NCID; anyone with a valid NCID can gain access to the application; unique email address is not required**.

### User Login

|  |  |
| --- | --- |
| Brief Description | **User Successfully Logs in to application** |
| Login users | All login Users |
| Pre-conditions | Users must have an active connection to the Internet  Users must have an NCID User ID and password  The NCID account is active and the password has not expired  The application site must be running correctly and available to Internet users |
| Post-conditions | Users must be authenticated in to the application, or must be prompted for correct action |
| Basic Flow | User opens web browser on local machine  User navigates to application home page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User enters **correct** User ID and password  Authentication is confirmed and browser redirected to SP  Application receives a positive authentication from NCID  If there are required attributes, these are passed to the SP  Based on returned information user is allowed into the application  Login user can gain access to suitable application information base on the user roll type in the application database |
| Alternate Flows | None |
| Special Requirements | None |
| Open Issues | None |
| References  (content in other docs) | N/A |

### User has valid NCID but is not in the application database

|  |  |
| --- | --- |
| Brief Description | **User needs access to application but does not have an account with the application database** |
| Login user | All login Users |
| Pre-conditions | Users must have an active connection to the Internet  Users must have an NCID User ID and password  The NCID account is active and the password has not expired  The application site must be running correctly and available to Internet users |
| Post-conditions | User logged in to NCID  User is informed that he or she has no authority to access the application  User is given information about how to gain authorization to the application |
| Basic Flow | User opens web browser on local machine  User navigates to application home page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User enters **correct** User ID and password  Authentication is confirmed and browser redirected to SP  Application receives a positive authentication from NCID  User is allowed into the application  User is informed that he or she has no authority to access the application |
| Special Requirements | None |
| Open Issues | None |
| References  (content in other docs) | N/A |

### User needs access to application but never registered in NCID

|  |  |
| --- | --- |
| Brief Description | **User needs access to application but does not have an account with the NCID system** |
| Login user | All login Users |
| Pre-conditions | Users must have an active connection to the Internet  The application site must be running correctly and available to Internet users |
| Post-conditions | An NCID account is created for the User  Government employee user is informed that his / her registration has been approved |
| Basic Flow | User opens web browser on local machine  User navigates to application home page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User enters **unknown** User ID and password  Authentication is not confirmed  User receives an error message from NCID login page  User is given on screen instructions or link on how to obtain an NCID account |
| Special Requirements | None |
| Open Issues | User will need guidance from the application owner about how to obtain an account in NCID and access to the application |
| References  (content in other docs) | N/A |

### User has an inactive state/local employee type NCID Account

|  |  |
| --- | --- |
| Brief Description | **User has registered with NCID before but the ID is disabled** |
| Login user | All login Users |
| Pre-conditions | User has registered with NCID before as a state employee type account  Users must have an active connection to the Internet  The application site must be running correctly and available to Internet users |
| Post-conditions | An inactive NCID account is enabled by the correct DA  User is informed that his / her id is active now  User can attempt login again |
| Basic Flow | User opens web browser on local machine  User navigates to application home page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User enters **correct** User ID and password  Authentication is **not** confirmed  User is presented with an error message from the NCID login page  User is **not** allowed into the application  User is informed that he or she has no authority to access the application |
| Special Requirements | None |
| Open Issues | User must have instructions on how to get the account reactivated |
| References  (content in other docs) | N/A |

### User Logs in with an Incorrect NCID User ID

|  |  |
| --- | --- |
| Brief Description | **User logs in with an incorrect user ID** |
| Login user | All login users |
| Pre-conditions | Users must have an active connection to the Internet  Users must have an NCID User ID and password  The NCID account is active and the password has not expired  The application site must be running correctly and available to Internet users |
| Post-conditions | User notified that the User ID or password entered is incorrect |
| Basic Flow | User opens web browser on local machine  User navigates to application protected folder page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User enters an incorrect User ID and Password  Authentication is **not** confirmed  User is presented with an error message from the NCID login page  User is **not** allowed into the application |
| Alternate Flows | None |
| Special Requirements | None |
| Open Issues | None |
| References (in other docs) | N/A |

### User Logs in with an incorrect NCID Password

|  |  |
| --- | --- |
| Brief Description | **User logs in with incorrect password** |
| Login user | All login users |
| Pre-conditions | Users must have an active connection to the Internet  Users must have an NCID User ID and password  The NCID account is active and the password has not expired  The application site must be running correctly and available to Internet users |
| Post-conditions | User notified that the Password or UID entered is incorrect |
| Basic Flow | User opens web browser on local machine  User navigates to application protected folder page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User enters a correct User ID and incorrect Password  Authentication is **not** confirmed  User is presented with an error message from the NCID login page  User is **not** allowed into the application  User re-enters correct user-id and password  Authentication is confirmed and browser redirected to SP  Application receives a positive authentication from NCID  User is allowed into the application  Login user can gain access to suitable application information base on the user roll type in the application database |
| Alternate Flows | If the password is determined incorrect twice in one session, the user may not be granted access and will be provided the link to the NCID security questions and answers |
| Special Requirements | None |
| Open Issues | None |
| References  (content in other docs) | N/A |

### User Password has expired

|  |  |
| --- | --- |
| Brief Description | **User logs in and is notified that their password has expired** |
| Login user | All login users |
| Pre-conditions | Users must have an active connection to the Internet  Users must have an NCID User ID and password  The NCID account is active and the password has expired  The application site must be running correctly and available to Internet users |
| Post-conditions | User changes expired password |
| Basic Flow | User opens web browser on local machine  User navigates to application protected folder page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User enters a valid User ID and Password  Authentication is **not** confirmed  NCID validates account and determines the password has expired  NCID notifies user that password has expired, and prompts user on how to change password  Once the password is successfully change on the NCID login page User re-enters correct user-id and password  Authentication is confirmed and browser redirected to SP  Application receives a positive authentication from NCID  User is allowed into the application  If the user ID is in the application database user is allowed access  Login user can gain access to suitable application information base on the user roll type in the application database |
| Alternate Flows | User ends session without changing password and is not allowed to the application during this or other sessions until the password is changed |
| Special Requirements | None |
| Open Issues | None |
| References  (content in other docs) | N/A |

### User Account is locked after Three Unsuccessful User Login Attempts

|  |  |
| --- | --- |
| Brief Description | **A user supplies incorrect password during NCID Login three times and account is locked** |
| Login user | All login users |
| Pre-conditions | Users must have an active connection to the Internet  Users must have an NCID User ID and password  The NCID account is active and the password has not expired  The application site must be running correctly and available to Internet users |
| Post-conditions | User is presented with ‘Account is Locked’ error message  User’s account object shows lockout reset time  User’s account object shows login tries set to the number of attempts  Nothing is passed to the application  User is not allowed to the protected site |
| Basic Flow | User opens web browser on local machine  User navigates to application protected folder page  SAML determines no valid security toke present  Browser is redirected to NCID IDP  User is shown NCID login page  User supplies correct User ID and incorrect Password combination (1st attempt)  User is presented with an invalid login error message and prompted to re-enter credentials  User supplies correct User ID and incorrect Password combination (2nd attempt)  User is presented with invalid login error  NCID redirects user to security questions and answers  User navigates to the NCID password recovery screen  User cannot recover password  User supplies correct User ID and incorrect Password combination (3rd attempt)  User’s account is locked out  User receives message from NCID indicating account is locked  User is not allowed to access the application |
| Alternate Flows | If password recovery successful, user can attempt login again if done before lockout |
| Special Requirements | None |
| Open Issues | None |
| References  (content in other docs) | N/A |

### User Logs out of the Application

|  |  |
| --- | --- |
| Brief Description | **User ends their session with the web site** |
| Login User | All login users |
| Pre-conditions | User is logged into the application web site |
| Post-conditions | Browser session is closed after user clicks on ‘Close Browser’ (session cache may or may not be cleared depending on browser version) |
| Basic Flow | A logged-in user clicks on ‘Log Out’ button of the application  User session is terminated  Application and local cookies are removed in including SAML token  User is redirected to ‘Log Out’ screen with confirmation message  User clicks on ‘Close Browser’ button  User attempts to access application and is required to login again |
| Alternate Flows | None |
| Special Requirements | None |
| Open Issues | None |
| References  (content in other docs) | N/A |

### Session Timeout Logout

|  |  |
| --- | --- |
| Brief Description | **A logged-in user is automatically logged out after session idle or maximum limit is reached** |
| Login user | All login users |
| Pre-conditions | An application web site user is logged into the system |
| Post-conditions | User is redirected to login form page |
| Basic Flow | User is logged-in  User waits until session maximum limit has been reached  User attempts to access a protected resource  User’s session has expired  User re-directed to the NCID login page for authentication |
| Alternate Flows | None |
| Special Requirements | None |
| Open Issues | None |
| References  (content in other docs) | N/A |

End of document–