

NCIP Basic Patron Authentication Profile

An Application Profile to support ANSI/NISO Z39.83-2002

Abstract:

This application profile is designed to provide one coherent, agreed-upon set of behaviors, options, and parameters that support the exchange of messages for verifying the identity of a patron.

Draft: March 2005

Prepared by Steve Gregory, Colorado State Library

Table of Contents

1.	Introduction	3
1.1	Profile Constraints.....	3
2.	Description of Application Area	3
3.	Scope	3
3.1	Dependencies	4
4.	References.....	4
5.	Definitions	4
6.	Conformance.....	5
6.1	Introduction to Conformance and Support.....	5
6.1.1	Roles	5
6.1.2	Statements of Conformance	5
6.1.3	Requirements of Conformance	5
6.2	Optional Features.....	6
7.	Profile Specification.....	6
7.1	Profile Description	6
7.2	Participating Applications	6
7.3	Business Rules	6
7.4	Management of User and Staff User Interaction	6
7.5	Required Components	6
7.5.1	Required and Optional Services	7
7.5.2	Required and Conditionally Required Data Elements	7
7.5.3	Enumerated Types.....	7
7.6	Event Table	7
7.7	Lookup Service Table	8
8.	Transport Protocol.....	8
9.	Security and Privacy	8
10.	Registration of Schemes Used in this Profile.....	8
11.	Guidelines for Implementers	9
11.1	Use Cases.....	9
11.2	Example Messages.....	10

1. Introduction

This application profile is designed to provide one coherent, agreed-upon set of behaviors, options, and parameters that support the exchange of messages for verifying the identity of a patron.

The base standard that enables this communication is NCIP. This profile is based on that protocol, as well as the supporting NCIP Implementation Profile 1.

1.1 Purpose

This profile defines the use of NCIP by a group of libraries to determine whether the credentials of a user can be authenticated.

The behavior described in this profile is based on the assumption that a successful response to the “Authenticate User” NCIP service indicates a positive answer to the question, “Is this user listed in the Authentication Target’s Patron database?”

2. Description of Application Area

This application profile is designed to support the exchange of messages for verifying the identity of a patron.

Example uses of NCIP Patron Authentication may include:

- (1) Licensed Databases: Patron approaches a library gateway web site and requests access to a database that is available only to citizens of Utopia. The Authentication Client will exchange messages with its business partner(s) who have the authority to authenticate citizens of Utopia.

3. Scope

This profile discusses the use of NCIP messages for retrieving information about Agencies and about Patrons.

The NCIP “Lookup Version” service is used by the Authentication Client to dynamically determine whether the Authentication Target supports one or more versions of NCIP that are also supported by the Authentication Client. If no such common version exists, authentication cannot be performed.

The “Lookup Agency” service is used to obtain the Authentication Target agency’s Authentication Prompt.

The “Authenticate User” service is used to verify that the Patron is listed in the Authentication Target’s patron database. No other information about the Patron is exchanged.

This profile does not discuss the exchange of any information about the Patron other than basic authentication.

NCIP messages that relate to the lookup and/or manipulation of circulation information, such as loans, requests, or fiscal transactions, are not within the scope of this profile.

This profile is intended for groups of libraries or other institutions that require sharing user information, and are willing and able to share and maintain policy and configuration information to attain that goal.

This profile does not address what policy and configuration information must be shared, nor how it is maintained. It is assumed that conforming applications will have different requirements and will provide

appropriate mechanisms to achieve them. For example, applications must be able to transmit NCIP initiation messages to the applications associated with other agencies. Because there is no facility in NCIP to determine a network address for an agency's NCIP application, each application must be able, outside the scope of this profile, to determine such addresses.

This profile defines the employment of NCIP services by conforming applications; other activities, while in many cases necessary to the employment of those services (e.g., database updates, display of information to the user) are out of the scope of this profile.

3.1 Dependencies

This application profile does not require the use of any other NCIP application profile.

It is expected that other NCIP application profiles which describe circulation activities but omit discussion of the details of patron authentication may refer to this profile as a required component.

4. References

- NISO Z39.83-2002, NISO Circulation Interchange Protocol
- Implementation Profile 1, a Profile of the NISO Circulation Interchange Protocol

5. Definitions

Authentication The process of verifying an identity claimed by or for a Patron.

Patron A person by or for whom authentication is requested.

Home Institution An organization of which the Patron is a member. This organization maintains a list of its valid Patrons and their authentication Credentials, which is consulted whenever anyone requests authentication.

Authentication Client A computer system requesting authentication of a Patron. The Authentication Client always acts as the initiator of NCIP messages.

Authentication Target A computer system that contains a database of valid Patrons for the Patron's Home Institution and will respond to authentication requests initiated by the Authentication Client. The Authentication Target always acts as the responder in NCIP message transactions.

Credential(s) Data that is transferred or presented to establish the identity of a Patron. This is the basic information that the Authentication Target needs in order to authenticate a patron. For example, a public library might require the Patron's last name and visible library card number.

6. Conformance

6.1 Introduction to Conformance and Support

This section defines rules for determining whether an application's claim of conformance to this profile and any statement of support for optional features are valid. Throughout this section references to the Event Table are to Section 7.6 and to the Lookup Service Table are to Section 7.7 in this document.

6.1.1 Roles

This profile defines two roles to which an application may claim conformance:

- Authentication Client
- Authentication Target

These roles are defined in Section 5 above.

6.1.2 Statements of Conformance

A statement of conformance to this profile shall be made in the following form:

"X conforms to the Y role(s)."

"X" specifies the application claiming conformance and "Y" identifies one or more of the roles listed above.

6.1.3 Requirements of Conformance

An application that claims conformance to a role SHALL, while operating according to this profile:

1. Conform to the NISO Circulation Interchange Protocol and the Implementation Profile 1.
2. Be able to recognize every Required Event in those rows where its role is listed in the Initiating Application column of the Event Table.
3. Invoke each Required Service in those rows where its role is listed in the Initiating Application column of the Event Table whenever it recognizes an Event.
4. Be able to respond successfully to every Required Service in those rows where its role is listed in the Responding Application column of the Event Table.
5. Meet the Message Constraints as defined in the Event Table for all messages it transmits.
6. Include all required and conditionally required elements in all messages as defined in the Lookup Service Table.
7. Meet all restrictions on enumerated types as stated in Section 7.5.3.

6.2 Optional Features

This profile does not define any optional features.

7. Profile Specification

7.1 Profile Description

This document profiles a way for an application or institution having no direct knowledge of a patron to request that the patron be authenticated by another application or institution.

7.2 Participating Applications

Two application roles are described in this profile: the Authentication Client and the Authentication Target (see section 5, Definitions). The Authentication Client always acts as the initiator in NCIP message transactions, and the Authentication Target always acts as the responder.

7.3 Business Rules

The Patron will voluntarily provide Credential(s) to the Authentication Client. The Authentication Client relays this data to the appropriate Authentication Target via an NCIP initiation message. The Authentication Target checks that the message has come from a trusted source, and then compares the Credential(s) against the database of existing Patrons. The Authentication Target prepares an NCIP response message indicating the results and returns the message to the Authentication Client. If the Patron is found in the Authentication Target's database of existing Patrons, then the authentication is said to have been successful. If the Patron is not found in the Authentication Target's database, then the authentication is said to have been unsuccessful, and the appropriate NCIP "Problem" message is returned (See Appendix A of ANSI/NISO Z39.83-2002 for definitions of "Problem" data elements).

The Authentication Target determines whether the User's Credential(s) are valid for a patron in their database. There is no presumption that a successful response by the Authentication Target authorizes the patron for any further services.

7.4 Management of User and Staff Interaction

It is assumed that the Authentication Target organization's staff will be responsible for maintaining their patron database, but this activity is not within the scope of this profile.

7.5 Required Components

7.5.1 Required and Optional Services

The following table lists required and optional services, messages, and responses required for this profile. NCIP services not listed are not used by this profile.

Authentication Client – NCIP Initiator:

Service	Required (R) or Optional (O)
Lookup Version	O
Lookup Agency	O
Authenticate User	R

Authentication Target – NCIP Responder:

Service	Required (R) or Optional (O)
Lookup Version Response	R
Lookup Agency Response	R
Authenticate User Response	R

7.5.2 Required and Conditionally Required Data Elements

The following table defines the Message/Data Elements that are Optional in the NCIP Protocol or the Implementation Profile 1, but are Mandatory or Conditional in this Profile.

Message	Profile Required Elements	Conditions
Lookup Agency	Authentication Prompt	

7.5.3 Enumerated Types

These Enumerated Types which are listed as “Open” in the NCIP document and/or the Implementation Profile 1, are required by this application profile:

Open Enumerated Types:

Scheme	Applies to Element
http://www.iana.org/assignments/media-types	Authentication Data Format Type
http://www.iana.org/assignments/media-types	Authentication Prompt Type
http://www.niso.org/ncip/v1_0/imp1/schemes/authenticationinputtype/authenticationinputtype.scm	Authentication Input Type

7.6 Event Table

Triggering Event and Event Location	Initiating Application	Service Initiated	Responding Application	Message Constraints
Authentication Client initiates contact with Authentication Target	Authentication Client	Lookup Version	Authentication Target	
User of Authentication Client selects an available Authentication Target	Authentication Client	Lookup Agency	Authentication Target	Required: Authentication Prompt
User of Authentication Client supplies information requested via Authentication Prompt	Authentication Client	Authenticate User	Authentication Target	

7.7 Lookup Service Table

Responding Application	Lookup Service	Required Unique Ids	Required Response Data Elements
Authentication Target	Authenticate User	Authentication Input	
Authentication Target	Lookup Agency	Unique Agency ID	Authentication Prompt
Authentication Target	Lookup Version	From Agency ID, To Agency ID	

8. Transport Protocol

The Authentication Client SHALL support the HTTPS transport protocol.

The Authentication Target SHALL support the HTTPS transport protocol.

This Application Profile is concerned with sending potentially sensitive personal information about patrons across domains. Thus it is necessary to employ a secure connection protocol. HTTPS is the only protocol available in the Implementation Profile 1 that meets this requirement.

9. Security and Privacy

An excellent trust relationship must be in place between the organization operating the Authentication Client and the organization operating the Authentication Target. Prior to exchanging any NCIP messages, the two organizations must agree on the Target's hostname, port, and protocol for NCIP messaging, as well as the UniqueAgencyId's (scheme and value) by which they will recognize each other. Authentication MUST be denied (by indicating a Problem condition) if the Target fails to recognize either the FromAgencyId or the ToAgencyId in any AuthenticateUser message.

The HTTPS transport protocol is required for all message transactions related to Patron Authentication.

10. Registration of Schemes Used in the Profile

For information about maintenance and registration activities, see Appendix G, "Designation of Maintenance and Registration Agency", in the NCIP standard.

11. Guidelines for Implementers

The guidelines listed below are intended to assist vendors in implementing this profile. As guidelines, they are non-normative and represent non-protocol assumptions or options that might be employed by a well-designed application that is conformant to this profile.

- The nature and type of user Credential(s) that the Authentication Client will send with the Authenticate User message are normally discovered by first exchanging Lookup Agency messages. In this case the Lookup Agency message includes an Agency Element Type element with a value of “Authentication Prompt”, and the Lookup Agency Response will include one or more instances of the Authentication Prompt element.
- If the Authentication Prompt for a given responder is expected to change infrequently or never, it may be deemed unnecessary to use Lookup Agency to obtain the prompt every time a Patron is authenticated. In this case, it may be sufficient to use Lookup Agency to obtain the prompt occasionally, storing the results and reusing the prompt on subsequent authentication attempts.
- If the Authentication Client and the Authentication Target have a clear and durable agreement as to the Credential(s) required for authentication, the Authentication Client may configure the prompt information in advance and forego the use of Lookup Agency altogether.
- If, having received the Authentication Prompt from the Authentication Target via a Lookup Agency Response, the Authentication Client finds that it cannot construct the requested Authentication Input element(s) because the specified data types and/or data elements are not supported by the Client, the Authentication Client should terminate the NCIP authentication dialog and consider the authentication attempt unsuccessful.

The Use Cases and Example Messages below do not cover all possible cases and are intended to be illustrative but not exhaustive.

11.1 Use Cases (Non-normative)

Use Case: Patron Authentication
Primary Actor: Patron
Other Actors: Authentication Client (NCIP Initiator)
 Patron’s Home Institution (NCIP Responder)
Scope: Patron Authentication via NCIP Messaging
Level: User Goal

Main Success Scenario:

- Patron approaches Authentication Client’s user interface.
- Authentication Client prompts Patron to select Home Institution from a list of participating libraries.
- Patron Selects Home Institution
- Gateway Institution sends NCIP “*Lookup Version*” message to Home Institution.
- Home Institution responds with “*Lookup Version Response*”.
- Authentication Client chooses highest NCIP version supported by both parties and uses that version for subsequent transactions.
- Authentication Client sends NCIP “*Lookup Agency*” message to Home Institution, requesting *Organization Name Information*, *Agency Address Information*, and *Authentication Prompt*.
- Home Institution replies with “*Lookup Agency Response*” message, including requested elements.
- Authentication Client displays *Organization Name Information* and *Agency Address Information* to Patron on a welcome screen and prompts Patron to enter *Authentication data* (using *Authentication Prompt*).
- Patron enters *Credential(s)*.
- Authentication Client sends NCIP “*Authenticate User*” message to Home Institution, supplying *Credential(s)* and requesting *Name Information* and *Visible User ID*.
- Home Institution replies with *Authenticate User Response* message including requested information.
- Authentication Client parses the *Authenticate User Response* message and verifies that the Patron was authenticated.

Extensions

Exception	Response
<ul style="list-style-type: none"> Authentication Client fails to establish NCIP connection with Authentication Target NCIP Connection terminates before transaction is complete Authentication Client fails to parse any NCIP response message Authentication Client does not support any NCIP version supported by Authentication Target Authentication Client does not support Authentication Input Data requested by Authentication Target 	<ul style="list-style-type: none"> Authentication Client closes all open NCIP connections Authentication Client displays "Technical Difficulties" screen to Patron Authentication Client writes problem report to log and emails problem report to Authentication Client's system administrator
<ul style="list-style-type: none"> Authentication Client does not recognize Home Institution indicated by Patron Authentication Target returns "Problem" in <i>Lookup Agency Response</i> 	<ul style="list-style-type: none"> Patron is not authenticated Authentication Client displays "Please try again" screen to Patron
<ul style="list-style-type: none"> Authentication Target returns "Problem" in <i>Authenticate User Response</i> 	<ul style="list-style-type: none"> Patron is not authenticated Authentication Client displays "Please try again" screen to Patron

11.2 Example Messages (Non-normative)

Example Message 1a: Lookup Version

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCIPMessage PUBLIC "-//NISO//NCIP DTD Version 1//EN"
"http://www.niso.org/ncip/v1_0/impl/dtd/ncip_version.dtd">

<NCIPVersionMessage
  version="http://www.niso.org/ncip/v1_0/impl/dtd/ncip_version.dtd">
  <LookupVersion>
    <FromAgencyId>
      <UniqueAgencyId>
        <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
        </Scheme>
        <Value>Example Initiator</Value>
      </UniqueAgencyId>
    </FromAgencyId>
    <ToAgencyId>
      <UniqueAgencyId>
        <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
        </Scheme>
        <Value>Example Responder</Value>
      </UniqueAgencyId>
    </ToAgencyId>
  </LookupVersion>
</NCIPVersionMessage>
```

- This is a Lookup Version message from the "Example Initiator" to the "Example Responder".
- In this example, the names of both agencies in *FromAgencyId* and *ToAgencyId* are found in a scheme controlled by the responder at [example_responder.org](http://www.example_responder.org).

Example Message 1b: Lookup Version Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCIPVersionMessage PUBLIC "-//NISO//NCIP DTD Version 1//EN"
"http://www.niso.org/ncip/v1_0/impl/dtd/ncip_version.dtd">

<NCIPVersionMessage version="http://www.niso.org/ncip/v1_0/impl/dtd/ncip_version.dtd">

<LookupVersionResponse>

  <FromAgencyId>
    <UniqueAgencyId>
      <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
      </Scheme>
      <Value>Example Responder</Value>
    </UniqueAgencyId>
  </FromAgencyId>

  <ToAgencyId>
    <UniqueAgencyId>
      <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
      </Scheme>
      <Value>Example Initiator</Value>
    </UniqueAgencyId>
  </ToAgencyId>

  <VersionSupported>
http://www.niso.org/ncip/v1\_0/impl/dtd/ncip\_v1\_0.dtd
  </VersionSupported>

</LookupVersionResponse>
</NCIPVersionMessage>
```

- In this response message, the “Example Responder” declares that it understands only version 1.0 of NCIP. The Initiator will use version 1.0 for all subsequent transactions in this session.

Example Message 2a: Lookup Agency

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCIPMessage PUBLIC "-//NISO//NCIP DTD Version 1//EN"
"http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">

<NCIPMessage version="http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">
  <LookupAgency>
    <InitiationHeader>
      <FromAgencyId>
        <UniqueAgencyId>
          <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
          </Scheme>
          <Value>Example Initiator</Value>
        </UniqueAgencyId>
      </FromAgencyId>
      <ToAgencyId>
        <UniqueAgencyId>
          <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
          </Scheme>
          <Value>Example Responder</Value>
        </UniqueAgencyId>
      </ToAgencyId>
    </InitiationHeader>
    <UniqueAgencyId>
      <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
      </Scheme>
```

```

    <Value>Example Responder</Value>
  </UniqueAgencyId>

  <AgencyElementType>
    <Scheme>
http://www.niso.org/ncip/v1\_0/schemes/agencyelementtype/agencyelementtype.scm
    </Scheme>
    <Value>Authentication Prompt</Value>
  </AgencyElementType>
</LookupAgency>
</NCIPMessage>

```

- In this *Lookup Agency* message, the Example Initiator asks the Example Responder for its *Authentication Prompt*

Example Message 2b: Lookup Agency Response

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCIPMessage PUBLIC "-//NISO//NCIP DTD Version 1//EN"
"http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">

<NCIPMessage version="http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">
  <LookupAgencyResponse>
    <ResponseHeader>

      <FromAgencyId>
        <UniqueAgencyId>
          <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
          </Scheme>
          <Value>Example Responder</Value>
        </UniqueAgencyId>
      </FromAgencyId>

      <ToAgencyId>
        <UniqueAgencyId>
          <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
          </Scheme>
          <Value>Example Initiator</Value>
        </UniqueAgencyId>
      </ToAgencyId>

    </ResponseHeader>

    <UniqueAgencyId>
      <Scheme>
http://www.example\_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm
      </Scheme>
      <Value>Example Responder</Value>
    </UniqueAgencyId>

    <AuthenticationPrompt>
      <PromptOutput>
        <AuthenticationPromptData>Enter your Barcode</AuthenticationPromptData>
        <AuthenticationPromptType>
          <Scheme>http://www.iana.org/assignments/media-types</Scheme>
          <Value>text/plain</Value>
        </AuthenticationPromptType>
      </PromptOutput>

      <PromptInput>
        <AuthenticationInputType>
          <Scheme>
http://www.niso.org/ncip/v1\_0/impl/schemes/authenticationinputtype/authenticationinputtype.scm
          </Scheme>
          <Value>Barcode Id</Value>
        </AuthenticationInputType>
        <AuthenticationDataFormatType>
          <Scheme>http://www.iana.org/assignments/media-types</Scheme>
          <Value>text/plain</Value>

```

```

    </AuthenticationDataFormatType>
  </PromptInput>
</AuthenticationPrompt>

<AuthenticationPrompt>
  <PromptOutput>
    <AuthenticationPromptData>Enter your Pin</AuthenticationPromptData>
    <AuthenticationPromptType>
      <Scheme>http://www.iana.org/assignments/media-types</Scheme>
      <Value>text/plain</Value>
    </AuthenticationPromptType>
  </PromptOutput>

  <PromptInput>
    <AuthenticationInputType>
      <Scheme>
http://www.niso.org/ncip/v1\_0/impl/schemes/authenticationinputtype/authenticationinputtype.scm
      </Scheme>
      <Value>PIN</Value>
    </AuthenticationInputType>
    <AuthenticationDataFormatType>
      <Scheme>http://www.iana.org/assignments/media-types</Scheme>
      <Value>text/plain</Value>
    </AuthenticationDataFormatType>
    <SensitiveDataFlag/>
  </PromptInput>
</AuthenticationPrompt>

</LookupAgencyResponse>

</NCIPMessage>

```

- The response to Lookup Agency includes the Authentication Prompt information.
- The prompt labels that the Authentication Client will display to the Patron are “Enter your Barcode” and “Enter your Pin”.
- The Authentication Input Data elements (Credentials) that should be used in the subsequent Lookup User message are “Barcode Id” and “PIN”, as enumerated in the scheme authenticationinputtype.scm.
- The media type for all Authentication Prompt elements in this example is “text/plain”, as enumerated in the IANA Media Types scheme.

Example Message 3a: Authenticate User

```

<?xml version = "1.0"?>
<!DOCTYPE NCIPMessage PUBLIC "-//NISO//NCIP DTD Version 1//EN"
"http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">
<NCIPMessage version="http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">
  <AuthenticateUser>
    <InitiationHeader>
      <FromAgencyId>
        <UniqueAgencyId>
          <Scheme>http://www.example_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm</Scheme>
          <Value>Example Initiator</Value>
        </UniqueAgencyId>
      </FromAgencyId>
      <ToAgencyId>
        <UniqueAgencyId>
          <Scheme>http://www.example_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm</Scheme>
          <Value>Example Responder</Value>
        </UniqueAgencyId>
      </ToAgencyId>
    </InitiationHeader>
    <AuthenticationInput>
      <AuthenticationInputData>EXAMPLEUSER1</AuthenticationInputData>
      <AuthenticationDataFormatType>
        <Scheme>http://www.isi.edu/in-notes/iana/assignments/media-types/media-types</Scheme>
        <Value>Text</Value>
      </AuthenticationDataFormatType>
    </AuthenticationInput>
  </AuthenticateUser>
</NCIPMessage>

```

```

        </AuthenticationDataFormatType>
        <AuthenticationInputType>
            <Scheme>http://www.example_responder.org/ncip/schemes/AuthenticationInputType.scm</Scheme>
            <Value>Barcode Id</Value>
        </AuthenticationInputType>
    </AuthenticationInput>
    <AuthenticationInput>
        <AuthenticationInputData>1234-567-890</AuthenticationInputData>
        <AuthenticationDataFormatType>
            <Scheme>http://www.isi.edu/in-notes/iana/assignments/media-types/media-types</Scheme>
            <Value>Text</Value>
        </AuthenticationDataFormatType>
        <AuthenticationInputType>
            <Scheme>http://www.example_responder.org/ncip/schemes/AuthenticationInputType.scm</Scheme>
            <Value>Pin</Value>
        </AuthenticationInputType>
    </AuthenticationInput>
</AuthenticateUser>
</NCIPMessage>

```

- In this example of *Lookup User*, the Authentication Client provides the Patron's Authentication Input: (Barcode Id = "EXAMPLEUSER1", PIN="1234-567-890").

Example Message 3b: Authenticate User Response

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NCIPMessage PUBLIC "-//NISO//NCIP DTD Version 1//EN"
"http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">
<NCIPMessage version="http://www.niso.org/ncip/v1_0/impl/dtd/ncip_v1_0.dtd">

    <AuthenticateUserResponse>

        <ResponseHeader>
            <FromAgencyId>
                <UniqueAgencyId>

<Scheme>http://www.example_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm</Scheme>
                <Value>Example Responder</Value>
            </UniqueAgencyId>
        </FromAgencyId>
        <ToAgencyId>
            <UniqueAgencyId>

<Scheme>http://www.example_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm</Scheme>
            <Value>Example Initiator</Value>
        </UniqueAgencyId>
        </ToAgencyId>
    </ResponseHeader>

    <UniqueUserId>
        <UniqueAgencyId>

<Scheme>http://www.example_responder.org/ncip/schemes/uniqueagencyid/agencynames.scm</Scheme>
        <Value>Example Responder</Value>
        </UniqueAgencyId>
        <UserIdentifierValue>EXAMPLEUSER1</UserIdentifierValue>
    </UniqueUserId>

    </AuthenticateUserResponse>
</NCIPMessage>

```

- In the response to *Lookup User*, the Home Institution has provided a *Unique User Id* featuring a *User Identifier Value*.
- The fact that a Unique User Id was included in the response (rather than a Problem element) indicates that the Patron is indeed listed in the Home Institution's Patron database.

