Community Care Information Management (CCIM)

Data Submission and Technical Specifications

INTEGRATED ASSESSMENT RECORD (IAR)

IAR RELEASE 7

VERSION 1.3

March 2017

Security Classification: Low Security
Copyright

This document is the property of Community Care Information Management and is copyrighted, and all rights are reserved by Community Care Information Management. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of Community Care Information Management.

Disclaimer

This document is current as of March 2017 and any changes to all related applications after that date will be incorporated into the next version of this document.

Security Notice

This material and the information contained herein are proprietary to Community Care Information Management and may not be used, reproduced, stored in electronic retrieval systems, or disclosed to others, in any form or by any means, except as specifically permitted in writing by creator of the document.

The recipient of this information, by its retention and use, agrees to protect it from any loss, theft or compromise. Please contact the IAR Service Desk (iar@ccim.on.ca) if you wish to share this document with organizations outside of Community Care Information Management.

This document has a Low Sensitivity Classification.
### Document Details

#### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Comments</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial release</td>
<td>June 4, 2010</td>
</tr>
<tr>
<td>1.1</td>
<td>IAR Release 4 updates</td>
<td>Sept. 4, 2012</td>
</tr>
<tr>
<td>1.2</td>
<td>IAR Release 5 updates</td>
<td>May 24, 2013</td>
</tr>
<tr>
<td>1.3</td>
<td>IAR Release 7.1 updates, including:</td>
<td>Mar. 15, 2017</td>
</tr>
<tr>
<td></td>
<td>- Updated documentation section</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Incorporated IAR and consent schemas (section 2.4.3) into one document</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Added ‘assessmentTypeOther’ to IAR and consent schemas (sections 2.4.2.3 and 2.4.3.5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Removed ‘unsupported’ consent value (section 2.4.3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Removed support for SSL and added requirement for TLS (section 2.4.5.1, Operation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Updated IAR submission security header details due to stricter validation of the security handler (section 2.4.5.1, SOAP header)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Corrected error in security header in web service call message (section 2.4.5.1, sample SOAP header)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Added Appendix C to address new elements in the security header handling for SOAP messages, and a list of minor changes to the web service responses</td>
<td></td>
</tr>
</tbody>
</table>
Intended Audience

**Vendors** will use this document along with all of the supporting documents to develop a data feed for submitting assessment data to the Integrated Assessment Record (IAR) solution. Clarifications and questions about these requirements can be sent to the IAR Service Desk at iar@ccim.on.ca.

**Organizations** should read and understand this document and all the supporting documents that make up the data submission requirements. Organizations are responsible for ensuring that their vendor delivers a solution that meets these requirements.

Organizations and vendors should understand that this requirement package is designed for the purpose of submitting assessment data to the IAR application. Requirements for automating and supporting the individual assessment model are provided by the corresponding assessment standard.

Documentation

The following documents represent the data submission requirements for the IAR solution, and are available from the Vendor section on the CCIM website – www.ccim.on.ca:

1. IAR Release 7 Toolkit:
   a. IAR Data Submission and Technical Specifications (PDF – this document)
   b. IAR Submission Schema (XSD, IARSubmissionDefinitions _2.0.2.xsd)
   c. PHI Submission Schema – RAI-MH (XSD, CCIMSubmissionPHI-1.0.3.xsd)
   d. PHI Submission Schema – all other assessment types (XSD, CCIMCommonClient-1.2.xsd)
   e. Consent Record Submission Schema (XSD, IAR_ConsentSubmission-1.0.3.xsd)
   f. Web Service Definition (WSDL, IAR_Submission_2.0.2.wsdl)

2. Assessment specific data supplements to these specifications.

The CCIM website also provides additional documentation related to vendor testing.
# Table of contents

1. IAR overview .......................................................................................................................... 6  
1.1. What is the IAR? .................................................................................................................. 6  
1.2. What the IAR is not ............................................................................................................. 6  
1.3. What is stored in the IAR? .................................................................................................. 6  
1.4. Benefits of the IAR ............................................................................................................ 6  
2. Data submission requirements ............................................................................................... 7  
2.1. General information .......................................................................................................... 7  
2.2. Submission process .......................................................................................................... 7  
2.3. Rejections, corrections and resubmissions ........................................................................ 8  
2.4. Technical requirements .................................................................................................... 9  
2.4.1. Technical requirements ................................................................................................ 9  
2.4.2. IAR submission schema 2.0.2 ..................................................................................... 11  
2.4.2.1. IAR submission – description of the major elements ............................................. 12  
2.4.2.2. Transmission header record .................................................................................... 13  
2.4.2.3. Submission header elements ................................................................................... 14  
2.4.2.4. Submission content record ..................................................................................... 15  
2.4.2.5. Submission content elements .................................................................................. 16  
2.4.3. Consent submission schema 1.0.3 ................................................................................. 17  
2.4.3.1. IAR and HSP consent model .................................................................................... 17  
2.4.3.2. IAR consent schema ................................................................................................. 18  
2.4.3.3. Consent directive record .......................................................................................... 19  
2.4.3.4. Consent directive – person information section ..................................................... 20  
2.4.3.5. Consent directive – apply to element ....................................................................... 21  
2.4.3.6. Consent directive – directive element ..................................................................... 22  
2.4.3.7. Consent directive – recorded by element ................................................................. 23  
2.4.3.8. Sample consent XML ............................................................................................... 24  
2.4.4. Encoding ....................................................................................................................... 26  
2.4.5. Submission methods ..................................................................................................... 27  
2.4.5.1. Automated submission – web service ..................................................................... 27  
2.4.5.2. Manual submission .................................................................................................. 29  
2.4.6. File naming convention ................................................................................................ 30  
2.5. Submission rules ................................................................................................................. 31  
2.6. Testing process ................................................................................................................... 32  
Appendix A – Assessment specific requirements ....................................................................... 33  
OCAN assessment requirements ............................................................................................... 33  
RAH-MH assessment requirements .......................................................................................... 33  
Appendix B – IARSUBMISSIONService-client-side ................................................................ 34  
Technology document ............................................................................................................. 34  
Creating the client stub code .................................................................................................. 34  
Customization to client stub code ............................................................................................ 34  
Testing ....................................................................................................................................... 36  
Summary ................................................................................................................................... 37  
Appendix C – IAR submission security header ......................................................................... 38
1. **IAR overview**

1.1. **What is the IAR?**

The Integrated Assessment Record (IAR) is an initiative within Community Care Information Management (CCIM) to allow assessment information to be viewed by health service providers (HSPs) within a client’s circle of care in a secure manner.

As an application, it can be used to access and view assessment information that is centrally housed at a Health Information Network Provider (HINP).

As a central repository for collected data it is a means to share assessments across community mental health organizations, hospital emergency departments, community support service organizations, primary care, and hospital mental health in-patient teams to provide improved quality care.

1.2. **What the IAR is not**

The IAR is not a clinical system of record. This means that the source systems feeding the IAR with assessment data will always be relied upon as the integral source for person information. In its design, no provisions have been made to permit data changes to occur from the IAR application; meaning it has been specifically designed to be a “Read Only” system to view client assessments.

1.3. **What is stored in the IAR?**

The IAR currently captures common assessment information pertaining to interRAI CA, interRAI Preliminary Screener, interRAI CHA, OCAN, RAI-HC, RAI-MH, and RAI-MDS 2.0, as well as Coordinated Care Plans (CCPs).

1.4. **Benefits of the IAR**

The IAR facilitates a common understanding of a client’s needs and helps to improve the continuity of care across community and hospital settings. Benefits of the IAR for clients, health service providers and the health care system include:

- Identifying other providers within the client’s circle of care and providing access to their most recent assessment
- Improving the quality and reliability of information sharing
- Ensuring a secure exchange of personal health information
- Providing data for health service planning to healthcare providers and LHINs
- Supporting networks and learning opportunities across organizations
- Providing the basis for coordinated community-based care planning, and assisting organizations to identify service overlaps and gaps
2. Data submission requirements

2.1. General information

The IAR is an initiative within CCIM to allow assessment information to be viewed by health service providers within a client’s circle of care in a secure manner.

This section provides data and technical specifications for use by organizations and their assessment tools vendors in the development of interfaces for data transmission to the IAR.

A data transmission to the IAR is defined in this and subsequent sections as a “submission”. A submission contains extracted assessment records, and these records may or may not be stored in a file.

This document includes the following sections:

- Submission Process
- Rejections, Corrections and Resubmissions
- Technical Requirements
- IAR Submission Schema
- Consent Submission Schema
- Encoding
- Submission Rules
- Testing Process

2.2. Submission process

Organizations have independent control of submission tracking and are responsible for ensuring that all assessment records are accounted for and available in their source systems. It is expected that organizations will use due diligence to ensure that an accurate and complete account of assessment records are successfully transmitted to the IAR repository as regularly as daily.

The IAR maintains an organization profile for the purpose of receiving submissions and communicating with the organization. Figure 1 - Overview of Assessment Submission Process presents a high-level view of the process for submitting assessment records for an organization. The IAR handles received submissions in two steps as follows:

Step 1 - Once a submission is sent to the IAR, the submitting organization receives a status indicating if the submission was successfully received and queued for further processing in the IAR. The IAR processes submissions in the order they are received and the processing may not happen immediately following the successful transmission.

Step 2 - Schema validations such as XML structure, mandatory fields and values, expected values and referential integrity validations are performed on the queued submissions at the time of processing. These validations could lead to a rejection of a submission or individual assessment records in a submission for which the submitting organization received a status in step 1 indicating that the transmission to the IAR was successful.
Assessment records in a submission must meet data quality edit checks and adhere to the predefined business rules required by the source system. The IAR assumes that these requirements are met and does not duplicate any content validations.

2.3. **Rejections, corrections and resubmissions**

Organizations have independent control of submission tracking and are responsible for ensuring that all assessment records are accounted for and available in their source systems. It is expected that organizations will use due diligence to ensure that an accurate and complete account of assessment records are successfully transmitted to the IAR repository as regularly as daily.

The IAR will reject an entire submission or individual records in a submission if the entire submission or the individual records do not pass validations at the time of processing. No records in the submission will be processed if the entire submission is rejected.

In the event that submission rejection or individual record rejection occurs, the submitting organization will be contacted by the IAR Service Desk with details on the nature of the error(s) and the actions to be taken for the record(s) to be accepted by the IAR.

The IAR requires that rejected records be corrected at source given that source systems are considered the systems of record for the IAR. This requirement has the added benefit of ensuring that source systems and the IAR hold consistent data, with all elements completed and records submitted in the correct format.

The submitting organization is not contacted if the IAR does not generate an error during the submission processing.

In cases where submissions are not successful due to technical issues (transmission, network or connectivity failure) extracted records need to be resubmitted with no change by the submitting organization.

Resubmission of records that were previously rejected or that were not successfully received (the submitting organization received a status indicating that the transmission was not successful or the submission failed due to technical issues) is the responsibility of the submitting organization.
2.4. Technical requirements

2.4.1. Technical requirements

Organizations have independent control of submission tracking and are responsible for ensuring that all assessment records are accounted for and available in their source systems. It is expected that organizations will use due diligence to ensure that an accurate and complete account of assessment records are successfully transmitted to the IAR repository as regularly as daily.

The IAR will only accept assessment data in formats that conform to standards specified by the corresponding assessment. Formats specified by the Canadian Institute for Health Information (CIHI) for RAI-MH assessment data for example will be accepted as will be formats specified in OCAN. Assessment data in the original format must be enclosed in envelope – see section Documentation, [2] IAR Submission Schema - to be accepted by the IAR.

The following diagram illustrates the structure of the submission envelope where assessment data contains personal health information (PHI), e.g., OCAN 2.0.

In cases where assessment data does not contain PHI (e.g., RAI-MH), the IAR requires corresponding PHI data to be provided in addition to the assessment data and consent directive, and the assessment data, PHI record and consent record must be included in the same submission envelope. Each set of the PHI record and consent record is linked to assessment record by the corresponding assessment ID, and there must be a PHI and consent records to accompany each assessment record. The structure of the submission envelope containing assessment and PHI data is shown in the following diagram.
The XML structure (XSD) for the submission envelope is defined in section Documentation, [2] Submission Schema, the XML structure (XSD) for personal health information is defined in section Documentation, [3, 4] – PHI submission Schema, and the XML structure (XSD) for the consent record in section Documentation, [5] Consent Record Submission Schema. Sample XML files are included in the requirements package.

The content of the IAR submission envelope is described in subsequent sections of this document.
2.4.2. IAR submission schema 2.0.2

The IAR submission schema is a universal xml envelope that is used to submit information to the IAR. It allows for various types of content to be submitted that conform to external schema definitions. This content can consist of assessment records covering various sectors, consent directives regarding the viewing of the assessment data, and PHI (personal health information).

![Diagram of IAR submission schema 2.0.2]

**FIGURE 2 – IAR SUBMISSION ENVELOPE 2.0.2**

*Note: Changes to this version of the schema (2.0.2) do not impact submission of assessments using the previous schema version (2.0.1).*
2.4.2.1. IAR submission – description of the major elements

An IAR submission envelope consists of 2 main records: the transmission header and the submission content. The transmission header describes the content. The submission content contains embedded xml records that can be of 3 types – assessments (RAI-MH, OCAN, interRAI CHA, etc.); consent directive information; and personal health information (PHI). As a general rule, all assessment content must be submitted with accompanying consent directive content.

A PHI record is required only for assessment information that is not IAR/CCIM designed and does not contain PHI, such as schemas developed by the Canadian Institute for Health Information (CIHI). A sample of a RAI-MH submission using all possible records is shown below.

```xml
<iar:IARSubmission version="2.0" xsi:schemaLocation="http://iar.on.ca/types IARSubmissionDefinitions_v2.0.2.xsd" xmlns:iar="http://iar.on.ca/types" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <iar:TransmissionHeader>
  </iar:TransmissionHeader>
  <iar:SubmissionContent>
    <Record mimeType="text/xml" recordType="Assessment" version="2016">
      <text><![CDATA[<OMHRSSubmission ....</OMHRSSubmission>]]></text>
    </Record>
    <Record mimeType="text/xml" recordType="PersonalInformation" version="1.0.3">
      <text><![CDATA[<CCIMSubmissionPHI version="1.0.3"/>]]></text>
    </Record>
    <Record mimeType="text/xml" recordType="Consent" version="1.0.3">
      <text><![CDATA[<ConsentSubmission ....</ConsentSubmission>]]></text>
    </Record>
  </iar:SubmissionContent>
</iar:IARSubmission>
```

Figure 4 – Sample RAI-MH Submission
2.4.2.2. Transmission header record

This record contains information regarding the source of the submission – the HSP and vendor system as well as the type of assessment content contained.
2.4.2.3. Submission header elements

<table>
<thead>
<tr>
<th>#</th>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IARSubmission@version (mandatory)</td>
<td>enumeration</td>
<td>Defines the version of the IAR submission. Must be 2.0</td>
</tr>
<tr>
<td>2</td>
<td>submissionId (mandatory)</td>
<td>string (40)</td>
<td>A unique identifier from the submitting system used to identify each individual submission. This could be a filename or an incremental counter. This value is used ensure duplicate submissions are not received and as a reference for diagnostics purposes.</td>
</tr>
<tr>
<td>3</td>
<td>organization@id (mandatory)</td>
<td>string</td>
<td>This is the MOHLTC assigned number (usually 3-4 digits) that identifies the source health service provider of the submission. The ID must be a value known to the IAR in order for the submission to be accepted.</td>
</tr>
<tr>
<td>4</td>
<td>organization@name (mandatory)</td>
<td>string</td>
<td>Full name of the submitting organization. This value appears within the IAR submission history log to help identify submissions.</td>
</tr>
<tr>
<td>5</td>
<td>exportTimestamp (mandatory)</td>
<td>dateTime</td>
<td>Date and time of the submission. This value is part of duplicate detection and must be different for each submission.</td>
</tr>
<tr>
<td>6</td>
<td>assessmentType (mandatory)</td>
<td>enumeration</td>
<td>Assessment type of submission. Must be one of the following supported assessment types: OCAN, RAI-HC, interRAI-PS, RAI-CA, RAI-MH, CCP, RAI-CHA, RAI_MDS_2.0, OTHER. Assessment version is indicated in the version attribute of the record element of the submission content element.</td>
</tr>
<tr>
<td>7</td>
<td>application@id</td>
<td>string</td>
<td>Source point used to differentiate instances of applications where an HSP may submit using more than one system.</td>
</tr>
<tr>
<td>8</td>
<td>application@name</td>
<td>string</td>
<td>Assessment software product name</td>
</tr>
<tr>
<td>9</td>
<td>application@vendor</td>
<td>string</td>
<td>Assessment software vendor</td>
</tr>
<tr>
<td>10</td>
<td>application@version</td>
<td>string</td>
<td>Assessment software version</td>
</tr>
<tr>
<td>11</td>
<td>assessmentTypeOther (mandatory)</td>
<td>string</td>
<td>Description of the assessment if type is ‘OTHER’</td>
</tr>
</tbody>
</table>

The value of the submitting organization id is dependent upon the assessment type and/or version:

- In the case of **OCAN 2.0** this value is represented by the submitting organization number field.
- In the case of **RAI-MH** it represents the 3 to 4-digit facility code from the Ministry of Health and Long-Term Care (MOHLTC) master numbering system, not the 5-digit master number that is transferred in the facility number field of a **RAI-MH** assessment record.
2.4.2.4. Submission content record

This record contains the actual assessment, consent and PHI xml data from the source system. The xml content is formatted to an external schema. This can be contained within a “text” record as unchanged “CDATA” or XML Entity encoded data. Optionally, xml content can be contained within a “binary” element encoded in Base64 or in compressed (zipped) format. Up to 3 “Record” elements may be contained within a single submission: one of assessments, consent or PHI.
### 2.4.2.5. Submission content elements

<table>
<thead>
<tr>
<th>#</th>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Record (Mandatory)</td>
<td>complex</td>
<td>The external xml content can be XML entity encoded, encapsulated within a CDATA segment or zip compressed.</td>
</tr>
<tr>
<td>2</td>
<td>Record@recordType (Mandatory)</td>
<td>enumeration</td>
<td>Indicates what kind of content is stored in the record. Assessment indicates an element containing assessment data as specified by the corresponding assessment standard. The assessment record may or may not contain PI. PersonallInformation type indicates a separate PI/PHI element that comes with some assessment types, e.g. RAI-MH. Consent Indicates that content of the element is consent data.</td>
</tr>
<tr>
<td>3</td>
<td>Record@version (Mandatory)</td>
<td>string</td>
<td>Contains the version number of the external schema to use to validate the xml content, e.g., 2.0.7 for OCAN assessments. In the case of RAI-MH the value is the year of CIHI schema edition, e.g., 2016 for the 2016-2017 fiscal year.</td>
</tr>
<tr>
<td>4</td>
<td>Record@mimeType (Mandatory)</td>
<td>enumeration</td>
<td>Defines the data format of the external xml. Set to text/xml.</td>
</tr>
<tr>
<td>5</td>
<td>Record@delimiter</td>
<td>string</td>
<td>Future use. Defines the character to use for delimited data.</td>
</tr>
<tr>
<td></td>
<td><strong>EITHER</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Text (Mandatory if Binary element not used)</td>
<td>string</td>
<td>Used to hold the external xml that is encapsulated within a CDATA section or XML entity encoded.</td>
</tr>
<tr>
<td></td>
<td><strong>OR</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Binary (Mandatory if Text element not used)</td>
<td>string</td>
<td>Used to hold the external xml that is Base64Encoded or in zipped format.</td>
</tr>
<tr>
<td>8</td>
<td>Binary@compressionType (Mandatory)</td>
<td>enumeration</td>
<td>Defines the method used to encapsulate external xml – set to “none” for Base64 or “application/zip” for compressed.</td>
</tr>
</tbody>
</table>
2.4.3. Consent submission schema 1.0.3

2.4.3.1. IAR and HSP consent model

The IAR consent model supports two levels of consent directives:

1. IAR Level Consent
2. HSP Level Consent

The IAR consent directive is obtained directly from the client/patient through the IAR Consent Centre. This is applied to all assessments relating to an individual client/patient regardless of the HSP that uploaded the assessment.

The HSP consent directive is collected by the HSP staff members from the client/patient while conducting the assessment.

The purpose of the consent schema is to define the data structure for consent directive information to be submitted to the IAR within an IAR submission envelope. Consent xml content can be placed within a Record@text or a Record@binary element of the IAR submission content record.

Consent records must always be submitted along with their associated assessments as a single submission. Consent is associated by assessment within the IAR and matching of the records is accomplished by the assessment ID and the client ID values.

The IAR has 2 states of consent directives regarding submissions – Grant or Deny.

The ability of the HSP to both submit Grant/Deny consent directives and administrate within the IAR is mutually exclusive. In the case where the Grant/Deny directives are to be submitted, consent management is to be handled by the source assessment system at the HSP. Any changes to a client’s consent (Grant/Deny) will require the re-submission of the assessments involved to the IAR following the existing New, Change, Delete re-submission rules.

All assessments are expected to be submitted to the IAR, regardless of the consent directive. Assessments that are “Granted” are viewable within the IAR.

Assessments that have “Deny” as the directive will reside within the IAR but will not be accessible or listed within the IAR. They will remain hidden and cannot be viewed.
2.4.3.2. IAR consent schema

The IAR consent schema allows for the inclusion of individual consent directive records that reference a single assessment that is part of a submission. The primary record element is the ConsentSubmission element allowing the inclusion of one-to-many ConsentDirective records. The schema is contained within a single schema file named IAR_ConsentSubmission-1.0.3xsd. Since the consent records are to be part of every IAR submission, the schema is included within the IAR submission and sample files toolkit that can be obtained through the Vendor section of the CCIM website – www.ccim.on.ca.

**FIGURE 7 – CONSENT SUBMISSION 1.0.3 - BASIC**

**FIGURE 8 – CONSENT SUBMISSION – DIRECTIVE RECORD**
2.4.3.3. Consent directive record

The consent directive record contains the actual consent information – one record per assessment.

![Figure 9 - Consent Directive Record]

Each consent directive record has the following mandatory fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>This field contains a unique record identifier. This is used to isolate all consent directives sent by an HSP and for reference purposes. Value to be generated and supplied by the source system.</td>
</tr>
<tr>
<td>type</td>
<td>Defines the type of directive contained – assessment or personal information. The IAR Release 4.0 (or higher) only supports assessment-based directives. Set to assessment.</td>
</tr>
</tbody>
</table>

Each consent directive record contains the following primary elements:

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Information</td>
<td>Identifies the person the consent applies to. (Mandatory)</td>
</tr>
<tr>
<td>Apply To</td>
<td>Contains the necessary information to match to a single assessment record contained within the IAR submission. (Mandatory)</td>
</tr>
<tr>
<td>Directive</td>
<td>Defines the type of directive received – Grant, Deny in submission. (Mandatory)</td>
</tr>
<tr>
<td>Record By Info</td>
<td>Name or user ID and date the consent was received. (Optional)</td>
</tr>
</tbody>
</table>
2.4.3.4. Consent directive – person information section

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization (Mandatory)</td>
<td>Contains submitting organization information.</td>
</tr>
<tr>
<td>Organization@id (Mandatory)</td>
<td>This is the MOHLTC assigned number (usually 3-4 digits) that identifies the source health service provider of the submission. The ID must be a value known to the IAR in order for the submission to be accepted. The value must match the organization@id field within the transmission header of the IAR submission envelope.</td>
</tr>
<tr>
<td>organization@name</td>
<td>Full name of the submitting organization. This value appears within the IAR submission history log to help identify submissions.</td>
</tr>
<tr>
<td>Source System</td>
<td>Contains information regarding the source of the submission.</td>
</tr>
<tr>
<td>SourceSystem@id (Mandatory)</td>
<td>Source point, used to further define the source of the assessment. This can be a 5 digit facility number (if used by the assessment schema itself such as RAI-MH), or a unique number to identify the instance of an application. When used as an instance identifier, the value must match that of the application@id field within the transmission header of the IAR submission envelope.</td>
</tr>
<tr>
<td>SourceSystem@type (Mandatory)</td>
<td>Specifies what type of identifier is being used, either a facility ID or an instance ID of a particular assessment system.</td>
</tr>
<tr>
<td>Person Id (Mandatory)</td>
<td>Client identifying number. Must match that of the assessment the consent relates to within the submission.</td>
</tr>
</tbody>
</table>
2.4.3.5. Consent directive – apply to element

Defines which assessment is affected by the consent directive.

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>Mandatory</td>
</tr>
<tr>
<td>AssessmentId (Mandatory)</td>
<td>The assessment number which the consent information applies to. The person ID from the personal information section and the assessment number must match an accompanying assessment within the IAR submission envelope.</td>
</tr>
<tr>
<td>assessmentType (Mandatory)</td>
<td>Specifies the type of assessment involved. Values are contained within its enumeration and must match that of the assessmentType field within the transmission header of the IAR submission envelope. Allowable values are RAI-CA, RAI-CHA, RAI-HC, RAI-MH, RAI_MDS_2.0, interRAI-PS, CCP and OTHER.</td>
</tr>
<tr>
<td>assessmentTypeOther</td>
<td>Description of the assessment if type is 'OTHER'.</td>
</tr>
<tr>
<td>PersonalInformation</td>
<td>Currently not used. Placeholder for future development.</td>
</tr>
</tbody>
</table>
2.4.3.6. Consent directive – directive element

This element contains the actual consent setting to be applied to the assessment.

![Diagram of Consent Directive - Directive]

### FIGURE 12 – CONSENT DIRECTIVE – DIRECTIVE

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessLevel (Mandatory)</td>
<td>Can be 1 of 2 values:</td>
</tr>
<tr>
<td></td>
<td>Grant – Assessment will be viewable within the IAR</td>
</tr>
<tr>
<td></td>
<td>Deny – Assessment will not be viewable within the IAR</td>
</tr>
<tr>
<td>Effective Date</td>
<td>Date the directive (if any) is to take effect.</td>
</tr>
<tr>
<td>Requested Time</td>
<td>Date and time the consent directive was received.</td>
</tr>
</tbody>
</table>
2.4.3.7. **Consent directive – recorded by element**

The recorded by element is optional and will contain the name or user identifier of the clinician who entered the information obtained from the client.

![Figure 13 – Consent Directive – Recorded By](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name or User ID</td>
<td>User name or full name of the individual entering the information.</td>
</tr>
<tr>
<td>Time Recorded</td>
<td>Date and time information was entered.</td>
</tr>
</tbody>
</table>
2.4.3.8. Sample consent XML

These samples demonstrate the 2 types of consent directives – Grant and Deny. It also highlights the difference between the use of the SourceSystem@type attribute.

**Consent directive – Grant – RAI-MH assessment type – using Facility ID**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ConsentSubmission
 xsi:schemaLocation="http://www.ehealthontario.ca/CCIM/ConsentSubmission.1.0.3.xsd"
xmns="http://www.ehealthontario.ca/CCIM"
xmns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ConsentDirective type="Assessment" id="13568953">
    <PersonIdentification>
      <organization name="Name of Organization" id="123"/>
      <SourceSystem type="Facility" id="52143"/>
      <PersonId>client215</PersonId>
    </PersonIdentification>
    <ApplyTo>
      <Assessment>
        <AssessmentId>12669658</AssessmentId>
        <assessmentType>RAI-MH</assessmentType>
      </Assessment>
      <ApplyTo>
        <Directive>
          <AccessLevel>Grant</AccessLevel>
          <EffectiveDate>2016-01-07</EffectiveDate>
          <RequestedTime>2016-01-07T09:30:47Z</RequestedTime>
        </Directive>
        <RecordedByInfo>
          <NameOrUserID>Clinician1</NameOrUserID>
          <TimeRecorded>2016-01-07T09:30:47Z</TimeRecorded>
        </RecordedByInfo>
      </ApplyTo>
    </ApplyTo>
  </ConsentDirective>
</ConsentSubmission>
```
Consent directive – Deny – OCAN assessment type – using Application ID

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ConsentSubmission
  xsi:schemaLocation="http://www.ehealthontario.ca/CCIM IAR_ConsentSubmission-1.0.3.xsd"
  xmlns="http://www.ehealthontario.ca/CCIM"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ConsentDirective type="Assessment" id="1534647416">
    <PersonIdentification>
      <organization name="Name of Organization" id="456"/>
      <!-- Facility type submission - affects the assessment id and client id's
      stored in the IAR -->
      <SourceSystem type="ApplicationId" id="1"/>
      <PersonId>client299a</PersonId>
    </PersonIdentification>
    <ApplyTo>
      <Assessment>
        <AssessmentId>703996489</AssessmentId>
        <assessmentType>OCAN</assessmentType>
      </Assessment>
    </ApplyTo>
    <Directive>
      <AccessLevel>DENY</AccessLevel>
      <EffectiveDate>2016-01-07</EffectiveDate>
      <RequestedTime>2016-01-07T09:30:47Z</RequestedTime>
    </Directive>
    <RecordedByInfo>
      <NameOrUserID>Clinician1</NameOrUserID>
      <TimeRecorded>2016-01-07T09:30:47Z</TimeRecorded>
    </RecordedByInfo>
  </ConsentDirective>
</ConsentSubmission>
```
2.4.4. Encoding

Submission envelope

The submission envelope format must use UTF-8 encoding.

Assessment data

The assessment data can be either UTF-8 or UTF-16 encoded, in accordance with assessment standard. For example, OCAN 2.0 must be UTF-8 encoded. UTF-8 encoded data can be stored in either <text>[CDATA] element or base64<binary>. However, UTF-16 encoded data can only be stored within <binary> content element. Note that according to XML W3C standard the stream encoded in UTF-16 should contain byte order mark (BOM). For more information about byte order mark please visit:

http://www.w3.org/TR/REC-xml/#charencoding and http://www.opentag.com/xfaq_enc.htm

PHI and consent data

The PHI and consent data must be UTF-8 encoded

Please refer to the XSD of the submission envelope for additional information.
2.4.5. Submission methods

The IAR offers two secure methods for transmission of electronic assessment records to its repository as illustrated in figure 1. An organization must have the ability to connect to the internet.

The solution supports an automated method using a web service and a manual transmission method using Microsoft Internet Explorer or Mozilla Firefox.

2.4.5.1. Automated submission – web service

The automated submission method supported by the IAR exposes a web service provider interface that is available to any participating organization over the internet through HTTPS protocol.

Clients must adhere to the following description in order to consume this web service.

Endpoint

The IAR assessment submission web service endpoint URLs for each HINP are as follows:

HSN: https://ia.hsnsudbury.ca/iarws-2.0/services/SubmissionService

TSSO: https://iarweb.ontariohealthapps.ca/iarws-2.0/services/SubmissionService

WOHS: https://iar.williamoslerhs.ca/iarws-2.0/services/SubmissionService

Operation

The IAR assessment submission web service defines a single SubmitAssessment operation with the following parameters:

- input: SubmissionInput
- output: SubmissionResponse

SubmissionInput is defined by the XML schema – see Documentation [2] - IAR Submission Schema – and described in the “Submission file structure definition” section.

SubmissionResponse is defined in WSDL – see Documentation [6], Web Service Definition – as complex type SubmissionResultType that has three elements:

- Result – of type Boolean that indicates if the operation executed successfully (value TRUE) or with errors (value FALSE)
- TransactionId – an attribute of result element, this is the internal IAR tracking Id that will be used for support purposes
- ErrorCode – optional, used when result = FALSE, contains error code defined by the IAR
- ErrorMessage – optional, used when result = FALSE, contains error description returned by the IAR
The IAR handles HTTP specific status codes in the way prescribed in WS-I Basic Profile 1.1 Second Edition (http://www.ws-i.org/Profiles/BasicProfile-1.1.html#SOAPHTTP), section 3.4. The following http response status codes can be returned by the IAR to a web service client:

- 200 OK
- 202 Accepted
- 400 Bad Request
- 405 Method Not Allowed
- 415 Unsupported Media Type
- 500 Internal Server Error

Security requirements are supported by transport level encryption TLS v1.0 and higher through HTTPS protocol.

**SOAP header**

The IAR submission web service is WS-Security compliant. The security header is added to the SOAP Header and adheres to the WS-Security schema http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd with the following features:

1. The user name and password is provided in the UsernameToken element with a plain text password. These user credentials are used to validate the submission uploader user (WS-user) associated with every organization’s assessment software. The WS-user is setup in the IAR clinical portal. The IAR submission web service uses UsernameToken to perform the following validations:
   a. User authentication (WS-user must exist in the IAR, the account is not locked, and the user password must match the password set-up in the IAR)
   b. User authorization (WS-user must have Uploader role, and the organization id in the user account must match the organization id from the IARSUBmission header)

2. Two additional **OPTIONAL** security header elements are available:
   a. **Nonce** – used to prevent denial of service attack. The same value of the nonce should be submitted again for the same Username, otherwise the submission will fail. **Note:** This element is **OPTIONAL** and is neither required nor recommended; however, if it is included, it must comply with the requirements as per Appendix C.
   b. **Created timestamp** – allows checking for message validity period (300 seconds). If the Created timestamp element is used the message will be accepted if the value of this element is within validity period range of current server time. **IMPORTANT:** Although this element is **OPTIONAL**, CCIM recommends that this element be removed as it requires clock synchronization between the organization and IAR servers.

**Note:** Details on the use of nonce and created timestamp elements are provided in Appendix C.
Following is an example of a SOAP header that contains user credentials in WS-Security compliant format:

```xml
<soapenv:Header>
  <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">
    <wsse:Username>uploader</wsse:Username>
    <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-password-token-profile-1.0#PasswordText">uploadpass</wsse:Password>
  </wsse:Security>
</soapenv:Header>
```

**Note:** Please refer to Appendix C for more details on the Password Type attribute.

Appendix B describes how the web service client can be implemented in Java.

### 2.4.5.2. Manual submission

The manual submission method allows users who have been authorized and authenticated to upload submission files that meet the specifications described in this document through the IAR secure web application. The user receives a message indicating if the file transmission was successful.

Transmission of data can occur 24 hours a day, seven days a week. Once the initial set-up for an organization has been put into place, authorized and authenticated users of this organization can submit data to the IAR at their convenience.
2.4.6. File naming convention

For submissions that are delivered in files, names must be standardized to facilitate the tracking of the assessment submission. The file-naming convention must be followed to ensure that the file is accepted by the IAR application.

The assessment submission file will be in the format:

\[\text{[Assessment Type]}<\text{YYYYMMDD}><\text{HHMM}><\text{OOOO}><\text{ZZ}>.<\text{999}>.\text{xml}\]

Where:

- **[Assessment Type]**, possible values are 'OCAN', 'RAI-MH'
- **YYYYMMDD** – the date when the export process started;
- **HHMM** - time when the export process started (note 24 hour clock is used);
- **OOOO** – organization ID, or parent organization id used in assessment application in multi-site environments (in case of OCAN);
- **ZZ** - target system suffix, 'IA' for Integrated Assessment;
- **999** - file sequence number, a sequence number of extracted file if export is broken into multiple parts, default value 001.

For example, if Organization 1234 is submitting a single part OCAN assessment file on the 1st of July 2016, at 5:05 PM the file name will look like this:

OCAN2016070117051234IA.001.xml

For example, if organization 5067 is submitting a single part RAI-MH assessment file on the 21st of July 2016, at 6:15 PM the file names will look like this:

RAI-MH2016072118155067IA.001.xml
2.5. Submission rules

Organizations have independent control of submission tracking and are responsible for ensuring that all assessment records are accounted for and available in their source systems. It is expected that organizations will use due diligence to ensure that an accurate and complete account of assessment records are successfully transmitted to the IAR repository as regularly as daily.

1. Each submission must contain at least one assessment record.

2. As assessments are completed, updated or deleted in the source systems, they must be submitted to the IAR as regularly as nightly.

3. The source system must ensure that a submission does not include duplicate records. Duplicate is defined as two identical records.

4. Each submission must have a unique organization ID and can only contain assessment record(s) for this organization.

5. Each assessment record must have a unique assessment/record ID; and record IDs must be unique across the submitting organization.

6. A maximum number of 500 assessment records will be accepted per submission.

7. Each submission must conform to the submission schema [2] and be able to pass validation against the XSD files provided as part of the requirements without any errors.

8. Assessment records in each submission must conform to specifications provided by the corresponding assessment standard.

9. The source system must provide the ability to resubmit individual assessment records or complete submissions.

10. The source system must track successful and failed submissions as well as web service communications (attempts and responses) and store the logs for at least 30 days.

11. Each web service client should be configured to make at least two additional attempts in 15 minutes intervals to consume the web service if the first attempt fails due to connectivity errors such as connection failure or timeout. If these attempts are not successful, the submission must be transmitted by the next possible submission cycle.
2.6. Testing process

The IAR’s policy is to only accept submissions that conform to specifications provided to vendors and organizations. The IAR will not accept live data until organizations’ vendors have successfully completed the standard testing process. A successful test is a submission that conforms to the specified schemas.

The primary objectives of the standard testing process are to validate:

- XML structure to ensure that it adheres to the specified XSD
- All mandatory fields/values to ensure that they are populated
- All expected values to ensure that they validate against expected value lists
- Network Connectivity / ability to establish access to the IAR environment

CCIM provides the IAR implementation validation guides that include test scenarios for each assessment type. Using the implementation validation guides, testing will be conducted in 2 phases (vendor testing and user acceptance testing) for each organization that uses a vendor external to the organization. If an organization uses an in-house built source system, the vendor will be considered part of the organization and testing will be conducted in a single phase.

Organizations using automated submission method:

1. Once the interface is completed and tested by the vendor, vendors will generate and submit XML test file(s) to be validated by the IAR team.

2. Once the web service client is completed by the vendor and the XML structure (XSD) is validated, vendors will transmit test submissions in the IAR test environment using the web service client.

3. Once the solution is delivered to the organization, a user acceptance testing (UAT) phase will be conducted to ensure that business requirements are met and assessment data can be sent to the IAR data repository.

Organizations using manual submission method:

1. Once the interface is completed and tested by the vendor, vendors will generate and submit XML test file(s) to be validated by the IAR team

2. Once the solution is delivered to the organization, a user acceptance testing (UAT) phase will be conducted to ensure that business requirements are met and assessment data can be sent to the IAR data repository.
Appendix A – Assessment specific requirements

OCAN assessment requirements

The IAR supports OCAN version 2.0. Detailed structure of submissions was provided by the OCAN project team. The schema version is stored in schema_version attribute of root element of OCAN submission XML file. This attribute allows the IAR to validate the content of submitted record based on the XML schema.

The IAR requires corresponding client’s personal health information in addition to assessment data. The PHI data must conform to the schema defined in Documentation [4] – PHI submission schema and both PHI and assessment data must be included in the submission envelope as illustrated in submission structure 1.

RAH-MH assessment requirements

RAI-MH assessment data layout is based on existing Ontario Mental Health Reporting System (OMHRS) technical specifications. This specification defines XML that conforms to OMHRS Submission XML Schema and single ASCII file containing variable record length as approved formats. The IAR supports the following versions of the Canadian Institute for Health Information (CIHI) submission specifications: 2008-2011 and higher.

In addition to assessment data the IAR requires corresponding client’s demographic information. The PI/PHI data must conform to the schema defined in section Documentation, [3] PHI Submission Schema and both PHI and assessment data must be included in the submission envelope as illustrated in submission structure 2.

The version attribute (iar:SubmissionContent/Record[1]/@version) will indicate the schema version of the assessments contained in the submissions file (e.g., 2016).

The values contained in the submission header fields – FiscalYearOfSubmission, FiscalQuarterForThisSubmission and DateOfSubmission should correspond to the schema version of assessments in the file as described in the chart below.

<table>
<thead>
<tr>
<th>Date of Submission (not current date)</th>
<th>Fiscal Year for which data is being submitted</th>
<th>Schema Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>April – May 31</td>
<td>Previous fiscal year</td>
<td>Previous fiscal year schema</td>
</tr>
<tr>
<td></td>
<td>Current fiscal year</td>
<td>Current fiscal year schema</td>
</tr>
<tr>
<td>June 1 – March 31</td>
<td>Previous or current fiscal year</td>
<td>Current fiscal year schema</td>
</tr>
</tbody>
</table>
Appendix B – IARSSubmissionService-client-side

Technology document

This appendix is intended for vendors' developers and should be used for information purposes only. It provides an example of how web service clients can be generated using Java. Vendors are free to choose their implementation as long as it meets the specifications.

The SubmissionService client web service stub was built and tested with the following technologies:

4. Apache Axis2-1.4.1 ([http://ws.apache.org/axis2/download/1_4_1/download.cgi](http://ws.apache.org/axis2/download/1_4_1/download.cgi))
5. WSDL file ([IAR_Submission_v2.0.2.wsdl](http://ws.apache.org/axis2/download/1_4_1/download.cgi))

Note: The versions of software indicated above do not reflect the current versions at the time of the publication of this specification. Vendors should use the latest versions available.

Creating the client stub code

The following web service Eclipse-Axis2 tutorial was used to auto-generate the client stub code:


Customization to client stub code

Customization was necessary in the client code to incorporate the WS-Security requirement. Since the autogeneration by Eclipse does not incorporate WS-Security features out-of-the-box, Rampart is the WS-Security module that is made to plug into Axis2. A pre-defined WS-Security client policy is needed in order for the client stub code to make a proper request. At this time the credentials (username and password) are being sent as plain text only. A different security policy will have to be used if these requirements were to change, i.e. if the password is digested (encrypted). The following is the current security policy used by Axis2:
The following Java snippet shows how the security policy is loaded into the client and a request being initiated:

```java
public SubmissionServiceStub() throws org.apache.axis2.AxisFault, XMLStreamException {

    //Web Service end point
    this ( "http://localhost:8181/IAR_Webservice5/services/SubmissionService"
    );

    Options options = _serviceClient.getOptions();

    //loading client-plain-text-security-policy
    options.setProperty (RampartMessageData.KEY_RAMPART_POLICY,Policy.loadPolicy("plain-policy-client.xml"));

    //setting credentials
    options.setUserName ( "libuser" );
    options.setPassword ( "books" );

    //engaging Rampart WS-Security engine
    _serviceClient engageModule ( "rampart" );
}
```
Testing

In order to confirm that the client side stub code has been configured correctly, the actual endpoint i.e. the web service needs to be deployed on a server that is accessible to the client stub. For local testing, an application server like Tomcat is suitable. The server side web service needs to be deployed as a standard Java web application archive file (*.WAR). Once the WAR file has been deployed, the web service will be active and be listening for incoming client requests.

A typical request will look like this:

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:typ="http://iar.on.ca/types">
  <soapenv:Header>
      <wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="UsernameToken-1">
        <wsse:Username>libuser</wsse:Username>
        <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">books</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
    <typ:ARSubmission version="1.0">
      <typ:TransmissionHeader>
        <submissionId>8899</submissionId>
        <organization name="www" id="111">my organization</organization>
        <exportTimestamp>2009-10-10T12:00:00-05:00</exportTimestamp>
      </typ:TransmissionHeader>
      <typ:SubmissionContent>
        <Record recordType="Assessment" version="1.0">
          mimeType="text/xml" delimiter=";">
            <!--You have a CHOICE of the next 2 items at this level-->
            <text/>
          </Record>
        </typ:SubmissionContent>
      </typ:ARSubmission>
    </soapenv:Body>
</soapenv:Envelope>
```
A sample response when the user is authenticated is:

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <ns1:SubmissionResult xmlns:ns1="http://iar.on.ca/types">
      <Result transactionId="TX-177234">true</Result>
    </ns1:SubmissionResult>
  </soapenv:Body>
</soapenv:Envelope>
```

A sample response when the user is not authenticated is:

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <soapenv:Fault xmlns:ns2Xvpe="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <faultcode>ns2Xvpe:FailedAuthentication</faultcode>
      <faultstring>The security token could not be authenticated or authorized</faultstring>
      <detail/>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

Summary

The above technologies outlined how a client stub can be configured to access a web service defined through a WSDL file. The use of auto-generation in Eclipse aid in producing client code quickly that is reliable and testable. Please refer to the technology links outlined in the start of this document for further information on the respective technologies. Additionally, the web service Eclipse-Axis2 tutorial (link above) was helpful in implementing client and server side code for the web service.
Appendix C – IAR submission security header

The IAR submission web service was updated (IAR Release 7.1) to use the newer versions of Apache Rampart software. As a result some behaviour of the security header handling has changed. With the IAR Release 7.1 the validation of the security handler is stricter, and this might require an update in the organization’s submission process. This section provides details of the implementation of the security header in the submission message.

Password type attribute value correction:

This version of the specification has updated previously incorrect spelling, where a “-“ was omitted in the “wss-username” part of attribute value. Currently, submissions to the IAR with the incorrect value will result in a warning in the IAR submission web service log. For organizations that currently submit assessments with the incorrect spelling of the password type attribute, it is strongly recommended that the organization’s submission code be modified to fix the spelling.

<table>
<thead>
<tr>
<th>#</th>
<th>Case</th>
<th>SOAP Request</th>
<th>SOAP Response</th>
<th>Notes</th>
</tr>
</thead>
</table>
Use of Nonce and Created Timestamp in SOAP header:

<table>
<thead>
<tr>
<th>#</th>
<th>Case</th>
<th>SOAP Request</th>
<th>SOAP Response</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Case</td>
<td>SOAP Request</td>
<td>SOAP Response</td>
<td>Notes</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>Correct Created Timestamp (time is within certain time interval of current time on the IAR server)</td>
<td><code>&lt;soapenv:Header&gt;</code></td>
<td>Successful processing of security header</td>
<td>IMPORTANT: CCIM recommends that this element be removed as it requires clock synchronization between the organization and the IAR servers.&lt;br&gt;Note: This is compatible with previous versions of the web service implementation.</td>
</tr>
<tr>
<td>#</td>
<td>Case</td>
<td>SOAP Request</td>
<td>SOAP Response</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>------</td>
<td>--------------</td>
<td>---------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
  <wsse:UsernameToken wsu:Id="UsernameToken-50BD538EF67E1A8F7C1484345809621">  
    <wsse:Username>uploaduser</wsse:Username>  
    <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-username-token-profile-1.0#PasswordText">uploadpasswd</wsse:Password>  
    <wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary">HAwHWVWedGF3PrkR1K+Igw==</wsse:Nonce>  
    <wsu:Created>2016-01-13T22:17:40.096Z</wsu:Created>  
  </wsse:UsernameToken>  
  <soapenv:Header/>  
  <soapenv:Body>  
    <soapenv:Fault xmlns:ns2Xvpn="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">  
      <faultcode>ns2Xvpn:MessageExpired</faultcode>  
      <faultstring>The message has expired</faultstring>  
      <detail/>  
    </soapenv:Fault>  
  </soapenv:Body>  
</soapenv:Envelope>` | **ERROR in log: the message has expired (WSSecurityEngine: Invalid timestamp The security semantics of the message have expired)**

**Note:** Previous versions of the web service implementation will not issue an error.
Minor differences between the IAR submission web service responses in the IAR Release 7.1 and previous release of the IAR:

<table>
<thead>
<tr>
<th>#</th>
<th>Case</th>
<th>IAR Release 6</th>
<th>IAR Release 7.1</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><code>&lt;soapenv:Body&gt;</code></td>
<td><code>&lt;soapenv:Body&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;ns1:SubmissionResult xmlns:ns1=&quot;http://iar.on.ca/types&quot;&gt;</code></td>
<td><code>&lt;ns1:SubmissionResult xmlns:ns1=&quot;http://iar.on.ca/types&quot;&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Result transactionId=&quot;TX-290254&quot;&gt;true&lt;/Result&gt;</code></td>
<td><code>&lt;Result transactionId=&quot;TX-177234&quot;&gt;true&lt;/Result&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/ns1:SubmissionResult&gt;</code></td>
<td><code>&lt;/ns1:SubmissionResult&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/soapenv:Body&gt;</code></td>
<td><code>&lt;/soapenv:Body&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/soapenv:Envelope&gt;</code></td>
<td><code>&lt;/soapenv:Envelope&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>password</td>
<td><code>&lt;soapenv:Body&gt;</code></td>
<td><code>&lt;soapenv:Body&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;faultcode&gt;wsse:InvalidSecurity&lt;/faultcode&gt;</code></td>
<td><code>&lt;faultcode&gt;ns2Xvpn:FailedAuthentication&lt;/faultcode&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;faultstring&gt;The security token could not be authenticated or authorized; nested exception is: java.security.auth.callback.UnsupportedCallbackException: authentication failed, please contact support&lt;/faultstring&gt;</code></td>
<td><code>&lt;faultstring&gt;The security token could not be authenticated or authorized&lt;/faultstring&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;detail/&gt;</code></td>
<td><code>&lt;detail/&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/soapenv:Fault&gt;</code></td>
<td><code>&lt;/soapenv:Fault&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/soapenv:Body&gt;</code></td>
<td><code>&lt;/soapenv:Body&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/soapenv:Envelope&gt;</code></td>
<td><code>&lt;/soapenv:Envelope&gt;</code></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Case</td>
<td>IAR Release 6</td>
<td>IAR Release 7.1</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="">soapenv:Body</a> &lt;ns1:SubmissionResult xmlns:ns1=&quot;<a href="http://iar.on.ca/types%22%3E">http://iar.on.ca/types&quot;&gt;</a></td>
<td><a href="">soapenv:Body</a> &lt;ns1:SubmissionResult xmlns:ns1=&quot;<a href="http://iar.on.ca/types%22%3E">http://iar.on.ca/types&quot;&gt;</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;Result transactionId=&quot;-1&quot;&gt;false&lt;/Result&gt;</td>
<td>&lt;Result transactionId=&quot;-1&quot;&gt;false&lt;/Result&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;DetailMessage&gt;Assessment organization 345Q is not valid for this user, please</td>
<td>&lt;DetailMessage&gt;Assessment organization 345Q is not valid for this user, please</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>contact support.&lt;/DetailMessage&gt;</td>
<td>contact support.&lt;/DetailMessage&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/ns1:SubmissionResult&gt;</td>
<td>&lt;/ns1:SubmissionResult&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/soapenv:Body&gt;</td>
<td>&lt;/soapenv:Body&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/soapenv:Envelope&gt;</td>
<td>&lt;/soapenv:Envelope&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="">soapenv:Body</a> &lt;ns1:SubmissionResult xmlns:ns1=&quot;<a href="http://iar.on.ca/types%22%3E">http://iar.on.ca/types&quot;&gt;</a></td>
<td><a href="">soapenv:Body</a> &lt;ns1:SubmissionResult xmlns:ns1=&quot;<a href="http://iar.on.ca/types%22%3E">http://iar.on.ca/types&quot;&gt;</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;Result transactionId=&quot;-1&quot;&gt;false&lt;/Result&gt;</td>
<td>&lt;Result transactionId=&quot;-1&quot;&gt;false&lt;/Result&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;DetailMessage&gt;information upload not authorized for user: yhradowy , please</td>
<td>&lt;DetailMessage&gt;information upload not authorized for user: Slava , please</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>contact support&lt;/DetailMessage&gt;</td>
<td>contact support&lt;/DetailMessage&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/ns1:SubmissionResult&gt;</td>
<td>&lt;/ns1:SubmissionResult&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/soapenv:Body&gt;</td>
<td>&lt;/soapenv:Body&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/soapenv:Envelope&gt;</td>
<td>&lt;/soapenv:Envelope&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system (Rhapsody)</td>
<td><a href="">soapenv:Body</a> &lt;ns1:SubmissionResult xmlns:ns1=&quot;<a href="http://iar.on.ca/types%22%3E">http://iar.on.ca/types&quot;&gt;</a></td>
<td><a href="">soapenv:Body</a> &lt;ns1:SubmissionResult xmlns:ns1=&quot;<a href="http://iar.on.ca/types%22%3E">http://iar.on.ca/types&quot;&gt;</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;Result transactionId=&quot;-1&quot;&gt;false&lt;/Result&gt;</td>
<td>&lt;Result transactionId=&quot;-1&quot;&gt;false&lt;/Result&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;DetailMessage&gt;web service could not complete transmission, please contact</td>
<td>&lt;DetailMessage&gt;web service could not complete transmission, please contact</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>support&lt;/DetailMessage&gt;</td>
<td>support&lt;/DetailMessage&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/ns1:SubmissionResult&gt;</td>
<td>&lt;/ns1:SubmissionResult&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/soapenv:Body&gt;</td>
<td>&lt;/soapenv:Body&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;/soapenv:Envelope&gt;</td>
<td>&lt;/soapenv:Envelope&gt;</td>
<td></td>
</tr>
</tbody>
</table>