Implementation Guide

Washington State Patrol

Regional System XML Interface

DMPP-2020, OFML and DSEO

Implementation Guide

Version 1.0

Datamaxx® APPLIED TECHNOLOGIES

www.Datamaxx.com

This document, or any portion thereof, may not be modified, reproduced, sold, or redistributed without the express written permission of Datamaxx Group, Inc.

This document is provided to you "AS IS" and Datamaxx Group, Inc. d/b/a/ Datamaxx Applied Technologies, Inc. provides no warranty as to the results you may obtain from using it.

Datamaxx™, the Datamaxx logo, Datamaxx Message Processing Protocol®, DMPP-2020®, Datamaxx Standard Embedded Object®, DSEO-2020® and Datamaxx Applied Technologies, Inc. Leading Law Enforcement Technology® are trademarks of Datamaxx Applied Technologies, Inc. Any other product names used within this document are the trademarks of their respective holders.

Published by:

Datamaxx Group, Inc. d/b/a
Datamaxx Applied Technologies, Inc.
2001 Drayton Drive
Tallahassee, FL 32311-7854
(850) 558-8000
www.Datamaxx.com

Revision History:

Version	Date	Notes
Version 1.0	03/31/2015	Initial Release

TABLE OF CONTENTS

1.0 INTRODUCTION

The purpose of this document is to define the complete interface that must be used by a regional system to access the Washington State Patrol ("WSP") ACCESS message switch for all messaging functions.

This interface implements the new technology using Internet standards to replace the old legacy interface. It does, though, retain the concepts of the legacy interface with regards to message addressing and routing at the regional interface

This interface uses the following technologies.

- Datamaxx Message Processing Protocol ("DMPP-2020"). This is the specification for the communications interface
- Datamaxx Omni*xx* Force Markup Language ("OFML 2015") This is the specification for the Data streams
- Datamaxx Standard Embedded Object ("DSEO"). This is the specification for the Image data encapsulation.

The documentation for these technologies is attached by reference. Also, an online resource center is being provided so that documentation is immediately available, including access to all the functions (queries, entries, modified, etc.) that are available to a regional system.

This interface provides not only additional functionality, but simplifies many of the transactions, eliminating data fields that are redundant or unnecessary.

The terminology used should be familiar to any practitioner familiar with creating interfaces in the Law Enforcement and Criminal Justice environment.

2.0 COMMUNICATIONS INTERFACE

This section provides the considerations for implementing the communication interface. The regional system is defined as being the “Client” system, and the ACCESS message switch as the “Server”.

The communications interface has the following characteristics:

- All messages to and from the client system and the server at WSP will use the Datamaxx Message Processing Protocol (“DMPP-2020”) protocol framing specification.
- All messages will be encrypted using the FIPS 140-2 standard. This is DMPP-2020 encryption header type code "n".
- A key book containing a series of keys will be provided via WSP staff, password protected, under separate cover.
- The client system will initiate the connection to the server located at WSP.
- The client system will identify itself using a “Validation String”, as described below.
- All messages from the client to the server should be sent requesting an acknowledgement, to ensure proper flow control.
- All messages received from the server and sent to the client will be sent requesting an acknowledgement from the client system, in order to prevent overloading the client system.
- There will be no fixed length for the messages. However, it can be reasonably assumed that a response message containing an image will not exceed 256Kbytes in size, and that the average size will rarely exceed 32 Kbytes.
- The server will require an idle time (also known as a “keep alive”) to ensure that the client interface is indeed active. The client interface should send a “Keep alive” every 45 seconds, as a minimum, when idle. Any traffic causes this interval to be reset, so that with continual message flow at a minimum of every 45 seconds, there is no need for a “Keep alive” request to be sent.
- The actual IP address and the port number to which the connection is made should be implemented as to be soft configurable, to allow for changes in the configuration.
- The IP address and port number will be provided by WSP staff.
- There will be no fixed length for the messages. However, it can be reasonably assumed that a response message containing an image will not exceed 256Kbytes in size, and that the average size will rarely exceed 32 Kbytes.

All data streams will use the Datamaxx Omni*xx* Force Markup Language (“OFML 2015”) with the required elements as described in the next sections.

All image data will be encapsulated using the Datamaxx Standard Embedded Object (”DSEO”) with the XML format, using industry standard “Base 64” encoding.

3.0 XML DATA STREAM

An OFML message consists of the following components:

- HDR Node. Always present. Contains control information for the data within the message.
- TRN Node. Provides the data elements for a request from the client to the server.
- RSP Node. Contains response information from the server to the client.
- IMAGES Node. Contains image information to be exchanged between the client and the server.

The following considerations apply:

- All nodes must be within an "<OFML>" wrapper.
- The RSP and TRN nodes are mutually exclusive
- IMAGES nodes may have multiple images, and may be used in either direction; however, transactions from the client to the server are usually limited to just one image due to the nature of the message.

3.1 OFML "HDR" ELEMENTS FROM CLIENT TO SERVER

For the WSP implementation, the following fields must be present in the "HDR" element.

- MKE. Required Message Key.
- DAC. Required. Device Address. This identifies the device that requested the transaction.
- ORI. Required. Must be a valid ORI code for the requesting device.
- USR. Required. User Identification, for audit purposes.
- REF. Optional User control field/reference field that contains context for the client system. This data will be returned to the requestor with the response. It must be 10 alpha-numeric characters. Its value is controlled by the client system, and is not processed by the server, but returned intact. For unsolicited responses this value will be set to "UNKNOWN".
- DRI. Optional. Destination State, when required by the transaction.
- DAT. Optional date and time stamp.
- SUM. Optional summary data, for documentation and audit.
- DFM. Optional. Used to request a specific format (XML or text or both) from a Data source, in cases where that data source provides such options.

3.2 OFML "TRN" ELEMENTS FROM CLIENT TO SERVER

For the WSP implementation, the TRN node will contain the fields required for the transaction. The names of the fields are provided ion the "XML Resource Center". The order of the fields is unimportant.

The following considerations apply to the “TRN” node. They are designed to simplify and reduce the number of transactions that must be implemented at the client system.

- Many functions use a “sub Function” to indicate a particular property of the transaction, instead of having a series of similar transactions. This is indicated by a “MKE1” element in the TRN node. For example the function “EA” (as noted in the “HDR” “MKE”) may have a “MKE1” value of “” to indicate properties of the “EA” function.
- For NLETS functions that have a “fixed” destination (as distinct from functions that need a defined destination, such as registration query) the destination is no longer required. This simplifies the implementation of new functions for the client system.

A sample request is provided in **Appendix A**.

3.3 OFML “HDR” ELEMENTS FROM SERVER TO CLIENT

For the WSP implementation, the following fields will be present be present in the “HDR” element sent from the server to the client.

- MKE. Message Key. This will be filled in when a data source provides such information, or the control value “ACK” for acknowledgment messages.
- SRC. The source of the message (e.g. “NCIC”). For messages generated by the ACCESS system, this will be set to “OSW”.
- DAC. The device to which the message is to be routed.
- REF. The reference information as provided in the origin request, unless an unsolicited response.
- SUM. The Summary data as provided in the original request, unless an unsolicited response.
- DAT. Date and Time stamp.

3.4 OFML “RSP” ELEMENTS FROM SERVER TO CLIENT

For the WSP implementation, the following fields may be present in the “RSP” element sent from the server to the client.

- TXT. Textual (human readable) response data
- XML_DATA. Optional. If the Data Source provided structured XML data and the original function included a request for data in that format, it will be present in this node. The format will be the responsibility of that Data Source and will follow its published specification.
- TRACKING. Information relating to the transaction, for accounting reasons. May be discarded as it does not contain any information relevant to the transaction data
- IMAGES. (optional) Images, in DSEO XML Base64 format, if requested by the client and available from the Data Source.

A sample response is provided in **Appendix B**.

APPENDIX A – SAMPLE REQUEST DATA STREAM

The following is a sample of a data stream to make a request to the ACCESS system.

The entire stream must be encapsulated as an “<OFML>” document, as follows:

```
<OFML>
<HDR> --- Header Elements --- </HDR>
<TRN> --- Transaction Data Elements --- </TRN>
</OFML>
```

Sample HDR element for an xxx query.

```
<HDR>
<DAC>DEVA</DAC>
<USR>MYUSERID</USR>
<DAT>20100915073119</DAT>
<CTL>REF1234567</CTL>
<MKE>DQ</MKE>
<ORI>WA1234567</ORI>
<SUM>:SMITH,GEORGE</SUM>
</HDR>
```

TRN element for that query.

```
<TRN>
<OLN>SMITH*1234567</OLN>
<IND>Y</IND>
</TRN>
```

APPENDIX B – SAMPLE RESPONSE DATA STREAM

The entire stream must be encapsulated as an “<OFML>” document, as follows:

```
<OFML>
<HDR> --- Header Elements --- </HDR>
<RSP> --- Response Elements --- </RSP>
</OFML>
```

HDR, as provided in the response.

```
<HDR>
<DAC>DEVA</DAC>
<DAT>20100915073119</DAT>
<CTL>12345ABCDE</CTL>
<SRC>DOL</SRC>
<ORI>WA1234567</ORI>
<MKE>DR</MKE>
<SUM>DQ:SMITH,GEORGE</SUM>
</HDR>

<RSP>
<TXT>
-------     Text Portion of DL Response -------
</TXT>

<DSEO>
------ Photo Image Portion of DL Response -----
------ Image is in Base64 Format -----
</DSEO>
            </RSP>
```