



## **LEADRS Integrations Overview**

Version 1.0. September 2008.

# Table of Contents

LEADRS Integrations Overview.....	1
Introduction.....	3
Overview.....	3
Security Considerations.....	3
Integration Processes Available.....	4
Import Case Into LEADRS.....	4
Export Case From LEADRS.....	6
Auto Login Feature.....	7
Advanced Integrations.....	8
Technical Information.....	9
XML Schemas.....	9
URLs.....	9
FAQ/Support.....	9

## Introduction

This document describes the various integrations options for the LEADRS system. The target audience of this document are IT vendors interested in integrating with the LEADRS System or Police Agencies interested in using LEADRS in conjunction with other IT systems who desire electronic data transfer between the various systems.

## Overview

The main components of the LEADRS integrations are as follows:

- LEADRS Communicates with Third Party systems using XML over secure Internet channels (https).
- LEADRS uses a validation/authentication system to provide a secure communications channel and pre-processing to maintain data integrity and security.
- LEADRS can import a new case from provided case data. The XML schema is fairly open to allow you to import only what data you have available, with additional case information optionally omitted for direct data entry from within the LEADRS system later.
- LEADRS can export a case document in XML format.
- LEADRS can provide an auto-login interface to allow seamless screen integrations with other third party systems.
- Using Advanced Integrations LEADRS can translate and work with almost any electronic case document format.

## Security Considerations

Security is a very important aspect of the LEADRS system. All online transactions and activity are performed over the https (encrypted) Internet protocol. The LEADRS system is a web based application and any integrations require a connection to the Internet from the Third Party System.

Many third party systems are hosted and managed on secure networks with strict firewall control of Internet traffic. With this in mind, the LEADRS integrations were designed to be initiated from within the firewall of the third party system. This provides more control for your local network administration, and minimal network configuration to setup a LEADRS integration.

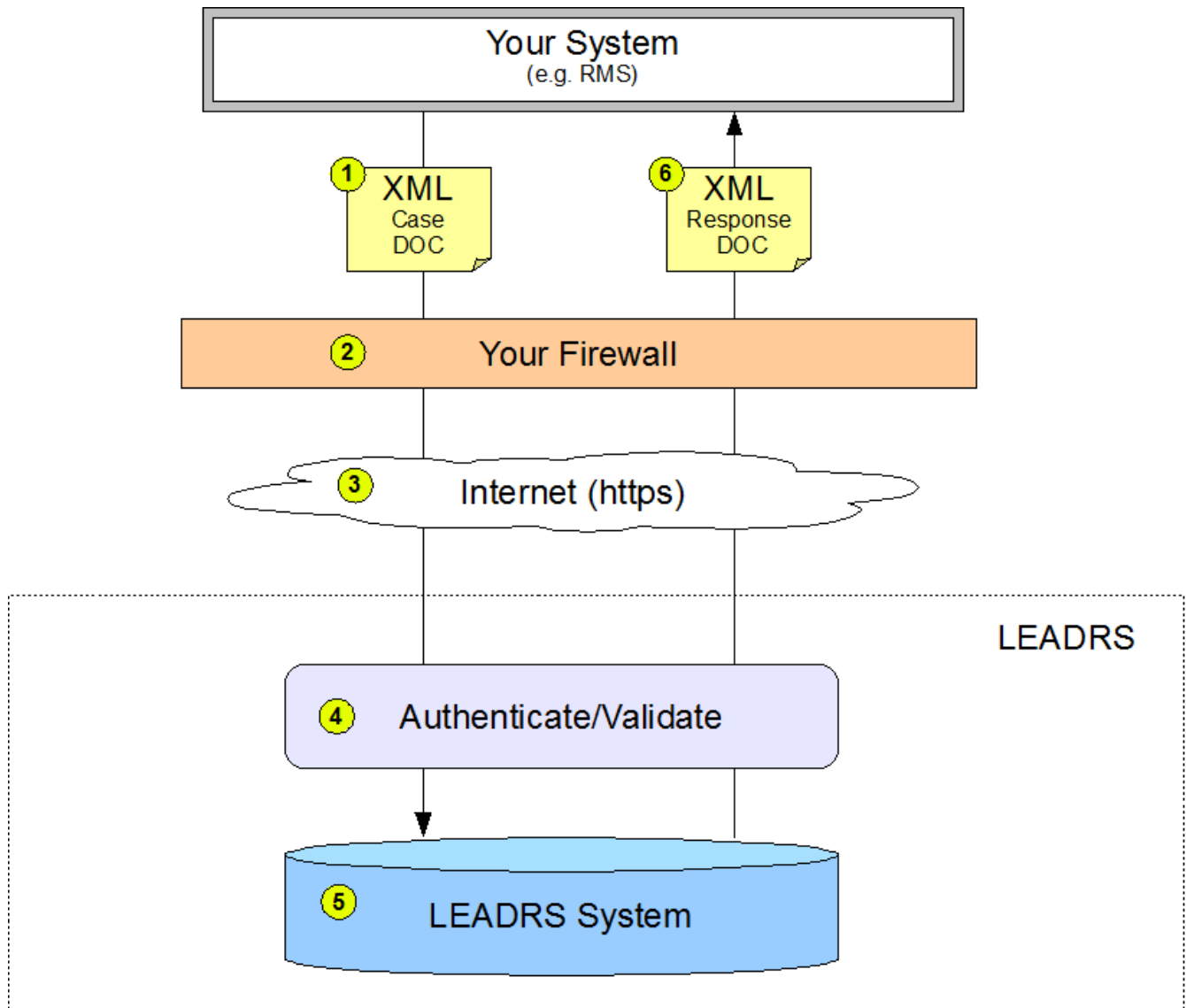
With requests arriving at the LEADRS system, an authentication is performed prior to any data analysis (see Technical Details Section for more information on authentication). Once authentication is accepted, the data/document is reviewed for compliance with the latest document specifications. Any errors are returned to the third party system in an XML response document. Successful authentication and data validation then engages the actual LEADRS system for processing. See the processes section for diagrams and more information.

Not all cases are available to third party systems. Existing case data exports are restricted to only data that was original imported via a specific LEADRS Integration Channel. This prevents any third party security system by-passing the LEADRS security model.

## **Integration Processes Available**

The following flow charts detail the available Integration Options for LEADRS.

## Import Case Into LEADRS



*Illustration 1: Import Case Flowchart*

1. Your System (Third Party System) generates an XML Document containing Case Data plus your authentication information. This is send via a HTTPS post to a LEADRS URL.
2. Because the request was initiated from within your network, there should be little or no work required at your firewall to integrate with LEADRS.
3. All Internet traffic is through HTTPS secure protocol channel.
4. LEADRS authenticates the document. This allows us to log the system where the request is coming from, plus check the username and password. The document is validated at this stage. Any validation errors are returned in the response document (See step 6)
5. The actual LEADRS system imports the case data associating the case with the supplied officer

information contained within the document (Note – Officer has to already exist as a valid LEADRS user for successful automated case import). A case ID is generated.

6. The Response document sent back to the client (Your System) contains either: A) Error Document, containing reason for error. OR B) Case ID and success notification.

At this point the case now exists as a full LEADRS case. In most instances this is not a complete case, and an officer would either login to the LEADRS system manually (at a later stage or immediately) to complete the rest of the case. Any information provided in the import will be already populated. Or the officer could use the Auto-Login feature to automatically jump to the LEADRS case directly from within the Third Party System (Your System).

## Export Case From LEADRS

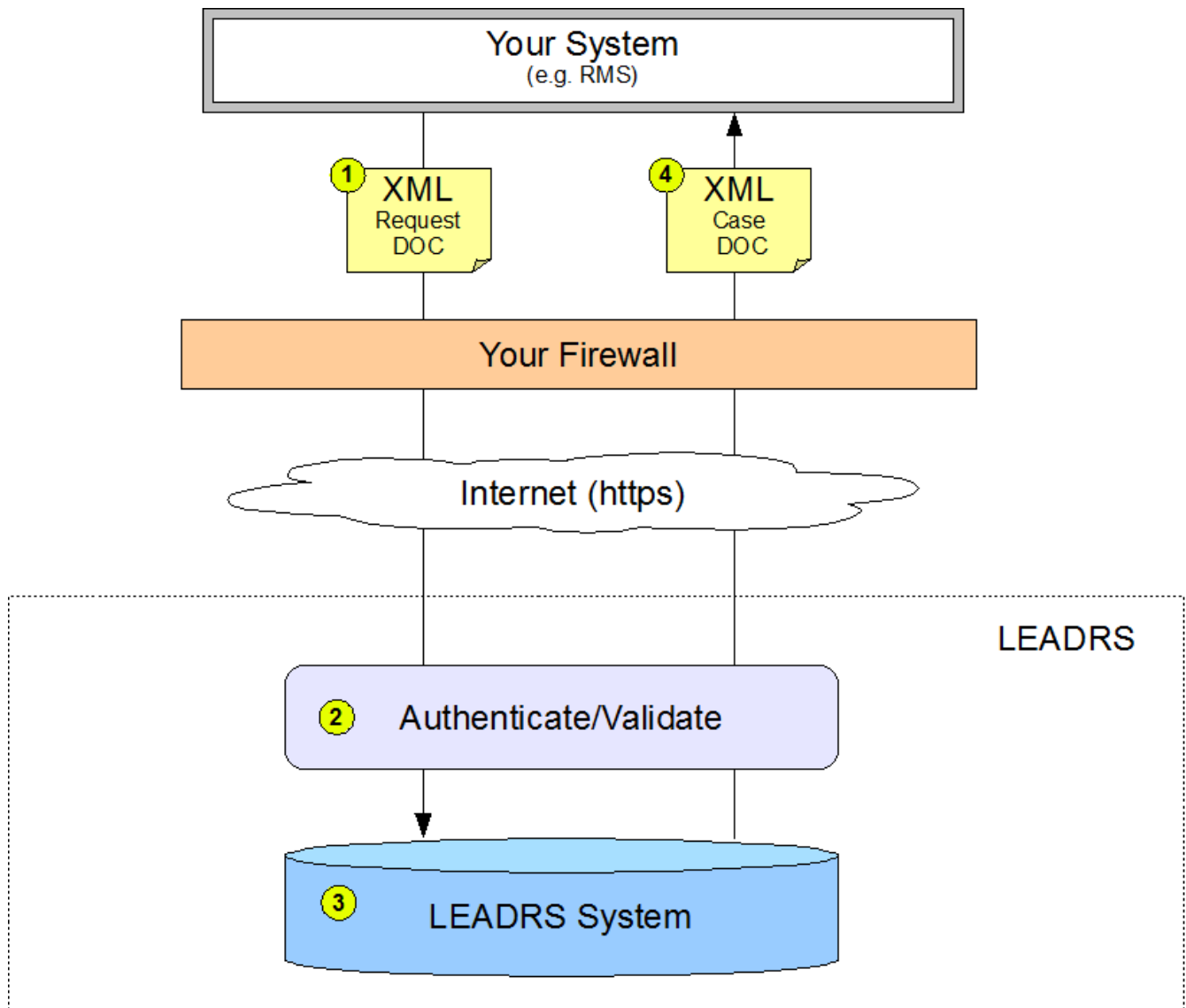


Illustration 2: Export Case from LEADRS

1. Your System submits a case request document containing authentication information and a CASE ID to the LEADRS system via HTTPS secure Internet Channel.
2. The authentication/validation process checks the user credentials of the incoming request. Only cases that were originally imported through this particular channel are accepted. Any case requests entered manually into LEADRS or from other departments or agencies are rejected. (Note – if an export channel were required for a non-agency entity such as a court system, an advanced integration with additional security validation would be required).
3. Upon successful validation the case is converted to the LEADRS XML specification.
4. The XML document is sent back to the Third Party System (Your System). If any errors occurred, and Error Document would be transmitted instead.

## Auto Login Feature

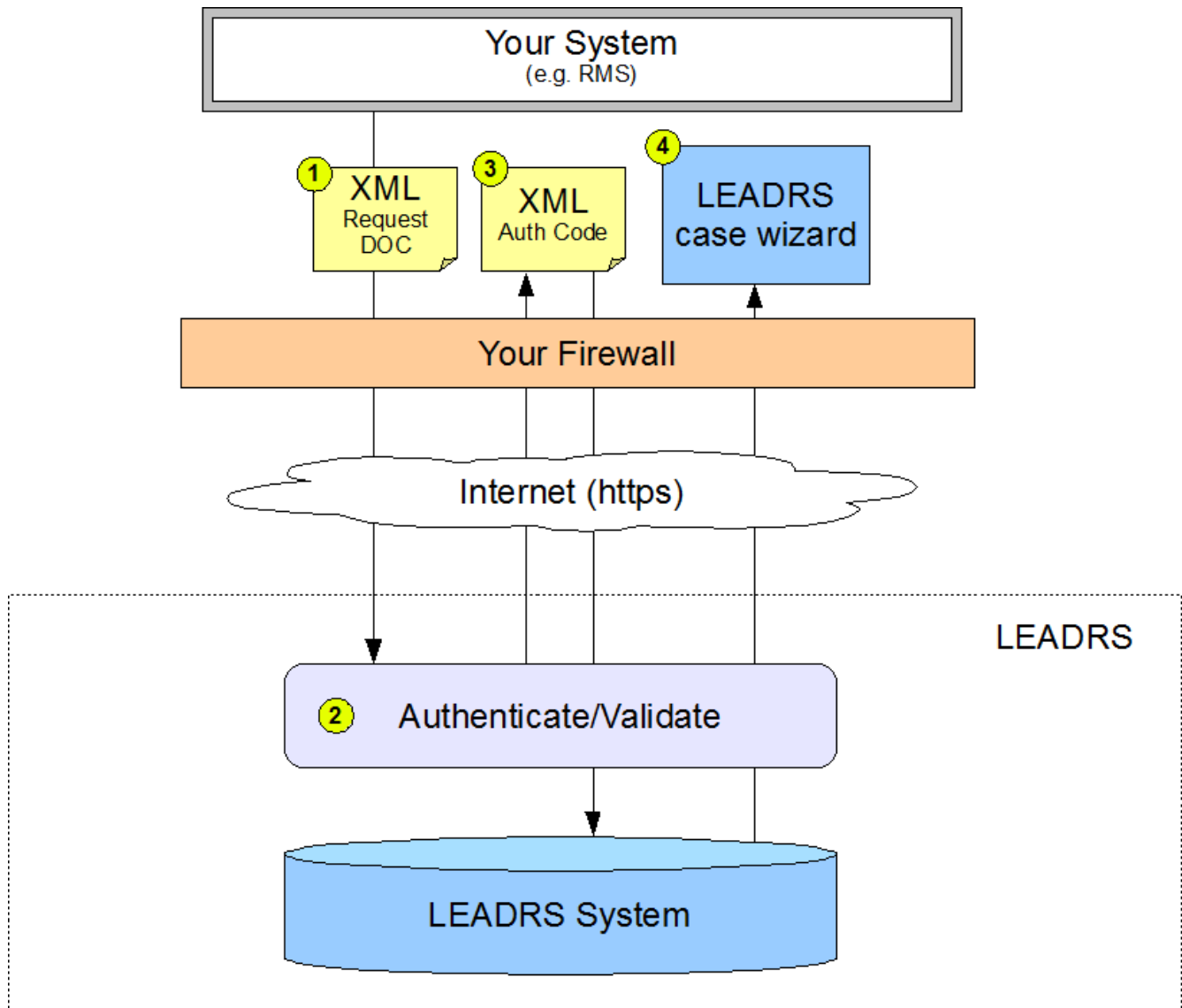


Illustration 3: Auto login Process

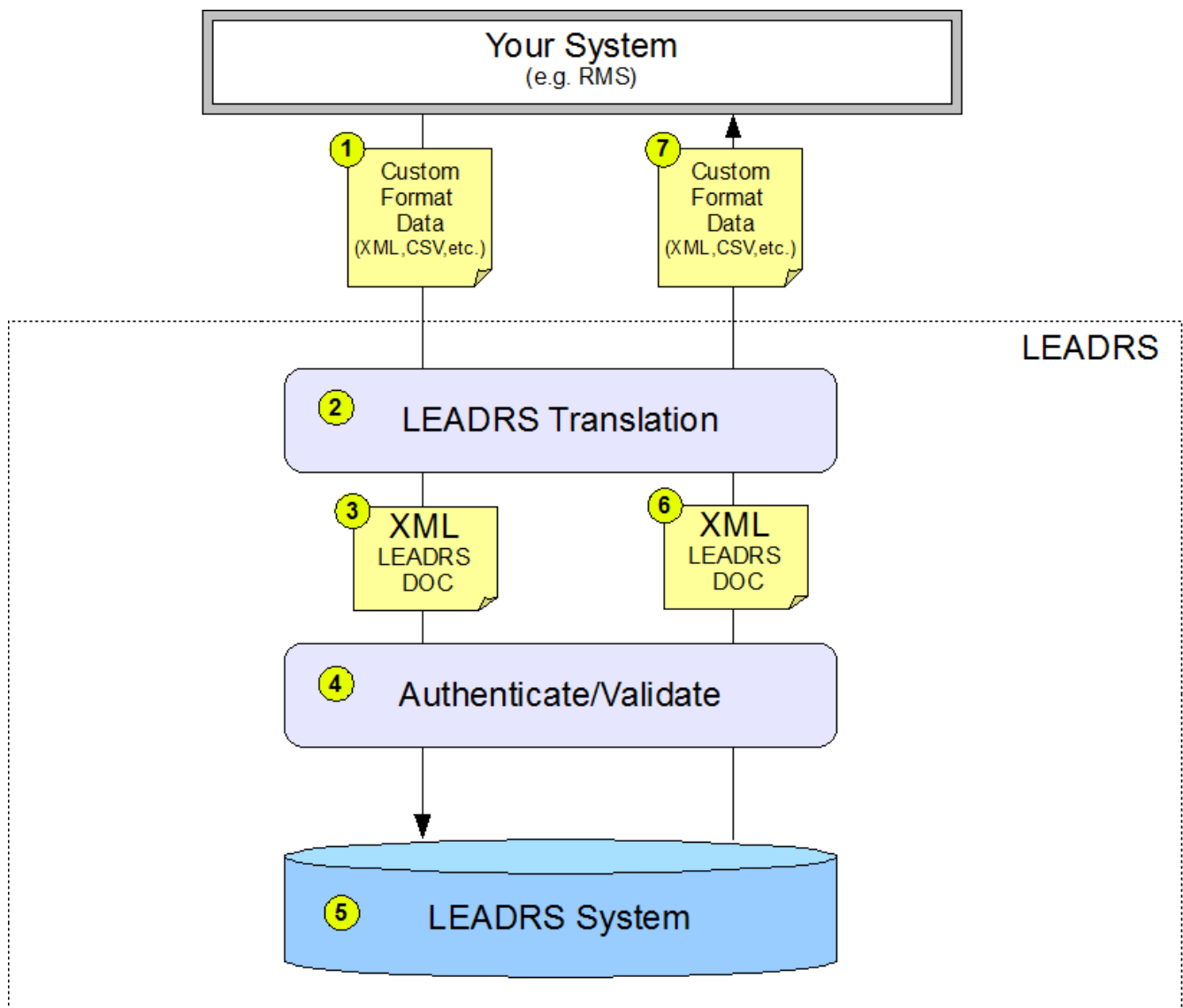
This process is useful for systems that already have screens open to an officer and want to provide a seamless “single login” type integration into LEADRS but still allow the officer to use the LEADRS system to capture extended DUI information about a case that may not be available in their own system.

1. The Third Party System (Your System) sends via HTTPS an authentication document with CASE ID.
2. The document is authenticated and validated. Note – this silent post is not visible to the actual officer, it is built into the Third Party System code. On successful authentication a temporary Access Code is returned to the Third Party System.

3. This Access code is then submitted as a URL parameter to a second page that performs the actual auto-login. The access code is then immediately destroyed so that at no time during the Auto Login is there anything visible to the end user (officer) that they could use to later compromise the security model of the system.
4. The LEADRS system is opened to the requested case in Wizard Mode.

This process would be performed real time with the intended experience for the end user (officer) being that they would click a button from within the Third Party System, and their LEADRS case information would immediately pop-up and be available.

### Advanced Integrations



This type of integration allows LEADRS to integrate as a fully customized channel. This is useful when the simple integrations above don't work, or the Third Party System already has an import/export format that is different from the LEADRS specifications.

1. The Third Party System (Your System) exports a case in its native format.
2. LEADRS translates the native format into LEADRS XML. This step is channel specific and requires custom data mapping.
3. The translation exports a LEADRS XML document.
4. The same authentication and validation process is performed like in the simple integrations.
5. The LEADRS System imports the data, or exports the data in LEADRS XML depending upon the type of request.
6. The LEADRS XML document is sent through the LEADRS Translation to be converted back into the Third Party Native format.
7. The Third Party System receives a document in its expected native format.

This type of integration is project specific and may vary slightly based on the requirements and restrictions of the Third Party System.

## **Technical Information**

This section is for IT and Programmers developing LEADRS Integrations.

### ***XML Schemas***

The latest LEADRS XML Schema can be found at the following address:

<https://texas.leadrs.org/support/integrations>

The LEADRS system is constantly under development and improvement and therefore please check the website for the latest schema. Existing Integrations Channels receive advanced notification of major schema changes. Typical changes are field changes (adding new fields), or drop down list updates for NCIC codes etc.

### ***URLs***

Test and Live URL's are provided to developers at the beginning of an Integration Project. Please contact us directly if you want to use or test Integrations.

The URL's and authentication system use a combination of Channel Key (Authentication key) plus a username/password. This information will be provided prior to any testing.

### ***FAQ/Support***

Please visit <https://texas.leadrs.org/support/integrations> for the latest support/FAQ information.

