Integrated User Verification
Customer Implementation Guide

2018-04-18
Confidential
Version 4.1
TABLE OF CONTENTS

Introduction .................................................................................................................. 2
  Purpose and Target Audience .................................................................................. 2
  Commonly Used Terms ............................................................................................ 2
  Implementation Time ............................................................................................... 3
Overview: Integrated User Verification (IUV) ............................................................ 4
  Single Sign-On Verification and IUV ........................................................................ 4
    Benefits .................................................................................................................. 4
    Challenges ............................................................................................................ 5
  How Does IUV Work? .............................................................................................. 5
Building Your Integration Application .......................................................................... 7
  Registering an Authenticated Shopper with a WebStore ......................................... 7
    User Authentication Data ...................................................................................... 7
    Response Codes and Error Messages ..................................................................... 11
    Redirecting the Shopper to the WebStore ............................................................ 12
Configuring ELMS to Talk to Your Application ........................................................... 14
  Accessing ELMS Administration ............................................................................. 14
  Finding Your ELMS Account Number ..................................................................... 14
  Adding IUV as a Verification Type .......................................................................... 15
  Configuring IUV .................................................................................................. 15
    Determining Customer Server IP Addresses ......................................................... 17
Testing IUV .................................................................................................................. 19
  Changing IUV’s Status to Testing .......................................................................... 19
  Testing Through the Test WebStore URL ............................................................... 19
Activating IUV ........................................................................................................... 21
Restoring Administrative Roles ................................................................................... 21
Appendix A – Sample Code ....................................................................................... 23
Appendix B – Support Information .......................................................................... 23
Introduction

This section covers the following areas:

- Purpose and target audience
- Commonly used terms
- Implementation time

PURPOSE AND TARGET AUDIENCE

This document provides detailed instructions for establishing a single sign-on mechanism between your organization’s existing authentication system (such as an LDAP directory) and a Kivuto ELMS WebStore. This process is called Integrated User Verification (IUV).

This document is aimed primarily at ELMS Administrators or web developers who have been assigned to the User Verification Administrator role in ELMS. It is intended to be used in conjunction with the online help available in the ELMS Administration site.

COMMONLY USED TERMS

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>A Kivuto customer (such as a company or educational institution) that is using IUV to authenticate shoppers to use an ELMS WebStore. In the ELMS Administration website, a customer is defined as an organization.</td>
</tr>
<tr>
<td>ELMS</td>
<td>Electronic License Management System. The ELMS platform includes both ELMS WebStores and the ELMS Administration site.</td>
</tr>
<tr>
<td>ELMS Administration</td>
<td>The secure administration module in ELMS that contains functions to manage a WebStore as well as set up IUV. This module is accessible by authorized users only.</td>
</tr>
<tr>
<td>IUV</td>
<td>Integrated User Verification. A single sign-on mechanism between a customer’s system and ELMS.</td>
</tr>
<tr>
<td>Shopper</td>
<td>A user that is being signed in to an ELMS WebStore.</td>
</tr>
<tr>
<td>WebStore</td>
<td>A Kivuto ELMS e-commerce website that provides products for distribution to members of a customer organization.</td>
</tr>
</tbody>
</table>
IMPLEMENTATION TIME

The time required to set up IUV for your WebStore varies with the type of authentication mechanism your organization currently uses and the technical abilities of your developers.

An average implementation time for most experienced software developers is a couple of hours.
Overview: Integrated User Verification (IUV)

This section covers the following areas:

- Single Sign-On Verification and IUV
  - Benefits
  - Challenges
- How does IUV work?

SINGLE SIGN-ON VERIFICATION AND IUV

Only authenticated users can order software through your WebStore. The mechanisms by which a user can be authenticated while signing in to a WebStore are called user verification methods.

Single Sign-On (SSO) verification methods allow users to sign in once, using a single ID and password, to gain access to multiple related but independent sites and software systems (e.g. a school’s WebStore and a school email account).

IUV is one of several SSO verification methods supported by ELMS.

BENEFITS

The benefits of IUV, and of SSO verification in general, are listed below.

- Reduces password fatigue from different username and password combinations
- Supports conventional authentication such as Windows credentials (i.e. username/password)
- Reduces support costs due to lower number of help desk calls about passwords
- Promotes security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users
- Reduces administrative costs since user administrators only have to manage user databases/lists in the parent organization. All SSO systems are fed from that system.
CHALLENGES

SSO provides access to many resources once the user is initially authenticated. As a result, it increases the negative impact if the credentials are accessed by other people and misused. Therefore, SSO requires an increased focus on the protection of user credentials and should ideally be combined with strong authentication methods.

SSO also makes the authentication systems highly critical. Failure or an inability to reach the authentication system (such as network failure) can result in denying access to any system unified under the SSO.

When using ELMS with IUV, it is imperative that the customer’s SSO implementation be available or else shoppers will not be able to access the WebStore and order software.

HOW DOES IUV WORK?

The following is an overview of the steps involved when a shopper signs in to a WebStore with IUV.

1. **Shopper arrives at customer site:** If the shopper browses directly to the WebStore, they will be redirected to the customer’s site when they click the link to sign in. Alternatively, the shopper could start from the customer’s site.

2. **Customer site authenticates shopper:** The customer’s site prompts the shopper for his or her credentials and authenticates the user using its authentication mechanism (e.g. an LDAP directory).

3. **Shopper initiates switch to WebStore:** The shopper indicates that he or she would like to go to the WebStore by clicking a link or button on the customer’s site.

4. **Customer site registers authenticated shopper with WebStore:** The customer’s site retrieves any additional information required about the shopper from its own data store and makes an HTTP POST call over Transport Layer Security (TLS) to a Kivuto URL passing relevant information about the shopper and a security key to identify the customer. See Building Your Integration Application for more information.

5. **Customer site redirects shopper to the WebStore:** If the HTTP POST call is successful – based on a specific return code – the customer’s site redirects the shopper to the return URL. This action completes the verification process, signs the shopper in to the WebStore and takes them to the WebStore’s home page.
See the diagram below for an illustration of this process.

**ELMS**

- Shopper clicks Sign In link

**Customer Integration Application**

- Shopper enters username and password
  - Customer system authenticates shopper and gets required attributes
  - Make HTTP POST call to ELMS

  **Read/Validate Response Code**

  - **200 SUCCESS**
    - Redirect shopper to ELMS
    - Shopper begins shopping!
  - **500 FAILURE (Kivuto Issue)**
    - 1. Display message to user
    - 2. Inform customer of issue via email.
    - Kivuto will automatically be informed of the issue and will resolve.
  - **400 FAILURE (Customer Issue)**
    - 1. Display message to user
    - 2. Send email to Customer Development Team
    - Customer Development Team must fix the problem and RE-TEST!
Building Your Integration Application

Build your integration application using whatever web technology is common to your organization.

Code samples written in PHP and in VB.NET 2.0, which include an aspx page used for testing the IUV process, are provided in Appendix A – Sample Code.

This section covers the following areas:

- Registering an Authenticated Shopper with a WebStore
- Response Codes and Error Messages
- Redirecting the Shopper to the WebStore

REGISTERING AN AUTHENTICATED SHOPPER WITH A WEBSTORE

To register an authenticated shopper with a WebStore, the customer site must do an HTTP POST over TLS to the URL: https://e5.onthehub.com/WebStore/Security/AuthenticateUser.ashx.

Note: This is not a redirect; this step must be performed on a customer server.

USER AUTHENTICATION DATA

The message body of the HTTP POST request over TLS has several required and optional attributes in JSON text format. The call is made over TLS so the data are automatically encrypted. The following is an example of a call to register an authenticated shopper with the attributes supplied:

```plaintext
POST
https://e5.onthehub.com/WebStore/Security/AuthenticateUser.ashx
Content-Type: application/json
Host: e5.onthehub.com HTTPS/1.1
{
    "account": "100001111",
    "username": "jsmith",
    "key": "f734ea97",
    "academic_statuses": [ "students" ]
}
```

The required and optional attributes are outlined in Table 1.
Some WebStores have a unique setup with more than one member organization to which shoppers may belong, and some IUV implementations support more than one WebStore. Refer to the data defined for Table 2 and in the section Single IUV Implementation Serving More Than One WebStore for more details.

Table 1 – Base IUV Implementation Data

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>account</td>
<td>Yes</td>
<td>The account number assigned to your organization within ELMS.</td>
</tr>
<tr>
<td>username</td>
<td>Yes</td>
<td>A unique identifier that describes each user. Maximum 100 characters.</td>
</tr>
<tr>
<td>key</td>
<td>Yes</td>
<td>“Shared secret” generated within ELMS Administration. This key should be kept as secure as possible.</td>
</tr>
</tbody>
</table>
| academic_statuses    | Yes (for academic organizations) | Important: This attribute and the default values available are intended to be passed by academic organizations. Corporate organizations may need to pass different attributes to indicate the eligibility of their users. Consult your account manager for details.  
A comma-delimited list of “user groups” to which the shopper belongs. These groups influence the shopper’s eligibility to order software. 
Each value listed must exactly match a valid user group code (e.g. do not send “student”; it must be “students”). 
Default user groups are listed below. Additional user groups can be configured (in ELMS Administration) and then passed as necessary. 
**The default user groups are:**  
- students  
- faculty  
- staff |
<p>| email                | No        | Shopper’s email address. Maximum 100 characters.                                                                                           |</p>
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_name</td>
<td>No</td>
<td>The last name of the shopper. Maximum 50 characters.</td>
</tr>
<tr>
<td>first_name</td>
<td>No</td>
<td>The first name of the shopper. Maximum 50 characters.</td>
</tr>
</tbody>
</table>
| shopper_ip     | No        | The IP address of the shopper’s computer. This is used to verify the identity of the shopper when they are redirected to the WebStore. Do not send this attribute when  
• The shopper’s IP cannot be guaranteed, or  
• The “Verify shopper’s IP address” is disabled on IUV’s Verification Settings section in ELMS Administration. |

Table 2 – Single WebStore With More Than One Organization Using the Store

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
</table>
| member_org     | Yes**     | Organization Code(s) of the specific member organization(s) that the user will be placed into.  
** Note: These codes must be defined in ELMS. Make sure to work with your account manager to set up this data.  
Example:  
“My Organization” is the parent organization. It has two satellite organizations (e.g. School Of Nursing and School of Management). If you want to have only one WebStore for the entire organization and to track which user belongs to which organization, then Kivuto will set up an organization for each entity.  
My Organization = "OrgA"  
School of Nursing = "OrgB"  
School of Management = "OrgC"  
Each of these organizations has their own member_org value, but the HTTP POST call will share a common key and account.  
What follows are the sample HTTP POST calls where 100001111 is the fictitious account number of OrgA: |
Single IUV Implementation Serving More Than One WebStore

You can create one IUV implementation that points to multiple WebStores. Each WebStore is tied to an organization.

The account number and key attributes of the HTTP POST call determine which WebStore the shopper is redirected to.
RESPONSE CODES AND ERROR MESSAGES

Success Codes

An HTTP status code of 200 (OK) is returned to the customer integration application if the HTTP POST call to register the authenticated user succeeds. The body of the response contains a URL to which the shopper can be redirected. See Redirecting the Shopper to the WebStore.

Failure Codes

- **HTTP status code 500**: If this code is returned to the customer integration application, Kivuto recommends that your application code do the following:
  - Send an email to the web development team informing them of the error.
  - Display a message to the user that access to the WebStore is currently unavailable and that someone is working on the issue.
  - Have the web development team contact Kivuto for support at tac@kivuto.com.

- **HTTP status code 400**: This code is returned to the customer integration application if there was a problem with the attributes passed. It will be accompanied by one of the messages listed in the Error Messages section below. In the event that this code is returned, Kivuto recommends that your application code do the following:
  - Send an email to the web development team informing them of the error.
  - Display a message to the user that access to the WebStore is currently offline and someone is working on the issue.
  - Have the web development team fix the issue.

Error Messages

If you need assistance from Kivuto Support to resolve any errors, be sure to provide them with the specific error message you received. Error messages that may be encountered are listed and defined below.
Table 3 – Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The required attribute [attribute name] was missing or was present more than one with different values.</td>
<td>Indicates that the attribute indicated by [attribute name] was missing or duplicated. If more than one attribute is missing, there will be more than one message delimited with the pipe (&quot;</td>
</tr>
<tr>
<td>WebStore not found. Check caller IP address and WebStore system name (if passed).</td>
<td>A WebStore was not found that was configured with the IP address of the calling server. This error message may also indicate that the account attribute is missing from the JSON data.</td>
</tr>
<tr>
<td>Submitted key does not match the one configured for the WebStore.</td>
<td>The key passed does not match the key assigned to the customer.</td>
</tr>
<tr>
<td>One or more of the user groups specified does not exist.</td>
<td>One or more of the user groups passed for the shopper does not match a valid user group code.</td>
</tr>
<tr>
<td>One or more of the user group classes specified does not exist.</td>
<td>One or more of the user group classes passed for the shopper does not match a valid user group class code. For future use, extra attributes are presumed to be user group classes.</td>
</tr>
</tbody>
</table>

**REDIRECTING THE SHOPPER TO THE WEBSTORE**

If the HTTP POST call succeeds, the shopper must be redirected to the WebStore URL returned in the response.

The following is an example of a URL returned in a response:

https://e5.onthehub.com/WebStore/Security/IntegratedSignIn.aspx?token=Q0FFThapS%2beRmWsiG40nDSzDPFs%2fpwpWjM0jzrIbfyF3JzrLzX6mg%3d%3d&ws=2fb0a48a-350a-dc11-bb1f-001372747fc5

If there is an error completing the user verification at the WebStore after being redirected, the following error will be displayed to the shopper:

*We were unable to sign you in to the store. Please try again.*
Possible reasons for this error are:

- The time between registering the authenticated user via the HTTP POST call and the redirection to the WebStore exceeded 60 seconds.

- The shopper’s IP address is being verified and it does not match the shopper IP address passed by the customer server when registering the authenticated user. See User Authentication Data for details.
Configuring ELMS to Talk to Your Application

This section covers the following areas:

- Accessing ELMS Administration
- Finding your ELMS Account Number
- Adding IUV as a Verification Type
- Configuring IUV

**Note:** To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS.

**ACCESSING ELMS ADMINISTRATION**

To access the ELMS Administration website:

1. Sign in to your ELMS WebStore.
2. Click on your ELMS username in the top-right corner of the page, and then click Administration in the menu that opens. The ELMS Administration site opens in a new browser tab or window.

**Note:** You can also access the ELMS Administration site through the central sign-in portal at e5.onthehub.com/admin. Signing in this way requires your organization’s account number as well as your username and password (see: Finding Your ELMS Account Number).

**FINDING YOUR ELMS ACCOUNT NUMBER**

Your ELMS account number is required to set up IUV.

To find your ELMS account number:

Sign in to the ELMS Administration site (see: **Note:** To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS).

1. Accessing ELMS Administration).
2. From the Main menu, click **Organization**. The Organization Details page is displayed.
3. Make note of your account number. It is found in the **Account Number** field.
ADDING IUV AS A VERIFICATION TYPE

To add IUV as a verification type:

Sign in to the ELMS Administration site (see: Note: To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS.

1. Accessing ELMS Administration).
2. On the left side-menu, click WebStore. The WebStore Details page is displayed.
3. Click the Verification tab. The WebStore Verification page is displayed, showing the list of currently configured verification types.

   **Note:** By default, “User Import” has been configured for new WebStores. If any additional verification types have already been configured, they will be listed here too.

4. Click the Add button. The User Verification Types page is displayed.
5. Click the check box beside **Standard Integrated User Verification**.
6. Click **OK**.

For the purpose of testing, you can add more than one Standard Integrated User Verification (IUV) verification method. When a new verification type is added, its status is set to “Testing” by default.

CONFIGURING IUV

Once IUV has been defined for your organization, you must configure it in the ELMS Administration site.

To configure IUV for your organization:

Sign in to the ELMS Administration site (see: Note: To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS.

1. Accessing ELMS Administration).
2. On the left side-menu, click WebStore. The WebStore Details page is displayed.
3. Click the Verification tab.
4. Click the **Standard Integrated User Verification** link. The User Verification Type page for IUV is displayed.
Note: On the Details tab, be sure not to change the values for “Sector” and “Verifications Expire In.” Changing these values could break your IUV, preventing your shoppers from being able to sign in to the WebStore.

5. On the Settings tab, provide all information required to implement IUV. See Table 4 for a description of all fields on this page and the appropriate values for each.

Table 4 – IUV Settings

<table>
<thead>
<tr>
<th>Information</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
</table>
| External Sign-in URL            | Yes       | URL of customer site page that will authenticate the shopper prior to redirecting to the Webstore, or URL of a page with a link that will direct the shopper to the Webstore.  
The WebStore will redirect the shopper to this URL when a user performs an action for which authentication is required (e.g. adding a product to a Shopping Cart), or when a user elects to sign out of the WebStore.  
To allow the customer site page to distinguish between these cases, a parameter is added to the URL’s query string. The name of the parameter is “action” and its possible values are “signin” and “signout”.  
Appropriate coding must be developed to handle each case above. |
| Key                             | Yes       | “Shared secret” used to verify the identity of the calling server.  
Generate the key by clicking the Generate button.  
The key will not be saved until you click OK or Apply. |
| Organization Account Number     | Yes       | The account number assigned to your organization within ELMS. This number is displayed here for use in the integration application. |
Verify shopper’s IP address (check box) | No |
---|---
In some cases, the shopper’s IP address as seen by the customer’s server may not remain the same after the shopper is redirected to the WebStore. This may happen due to a firewall dynamically assigning external IP addresses.
By default this is disabled.
If the check box is checked, the WebStore verifies that the IP of the shopper is the same as the shopper’s IP as determined by the customer server.

Calling Server IP Address List | No |
---|---
List of IP addresses of customer servers that will make HTTP POST calls to register authenticated shoppers with a WebStore.
The WebStore will verify that the IP of a calling server matches an IP address in this list. For assistance in determining what these addresses should be, see Determining Customer Server IP Addresses.

IUV Administrator Email Address | Yes |
---|---
Email address of individuals or a distribution list who will receive error messages from ELMS.

**DETERMINING CUSTOMER SERVER IP ADDRESSES**

In some cases, it may be difficult to determine the correct values for the customer server IP address list. This may be caused by:

- **Multiple IP Addresses**
- **Load Balancing**
- **Testing IP Address**

**Multiple IP Addresses**

If the customer server registering authenticated shoppers is configured with multiple IP addresses, typically the correct IP address is one of the following:

- Server base IP address
- Web server IP address under which the HTTP POST call is being made

If you are unable to determine the correct IP address, contact your Kivuto technical account representative. We can determine the IP address by analyzing web log data.
Load Balancing
If there are several load balanced or clustered customer servers that will be registering authenticated shoppers, you can provide a list of IP addresses for all of them.

Testing IP Address
For developers or testers testing IUV, you can supply the IP addresses of developer and/or tester workstations. When development and testing is complete, you can provide the production server IP addresses.

Changes to Customer Information
If any of the customer information discussed above changes, it is imperative that the IUV settings be updated immediately (or, if the WebStore is managed by Kivuto, that Kivuto is notified immediately).

Failure to make these changes could cause IUV to cease functioning and prevent shoppers from accessing the WebStore.
Testing IUV

Once IUV has been set up in ELMS, it should be tested before it is activated.

This section covers the following areas:

- Changing IUV’s Status to Testing
- Testing Through a Test WebStore URL

CHANGING IUV’S STATUS TO TESTING

Each verification method added to your WebStore is assigned one of the following statuses.

- **Inactive**: Verification type is not in use on the WebStore and is not being tested.
- **Active**: Verification type is not in use on the WebStore. Only one Single Sign-On verification can be active at a time.
- **Testing**: Verification type can be tested but is not visible to shoppers on your WebStore. Only one of each Single Sign-On verification type can be in Testing at a time.

The status of IUV must be set to Testing before the verification method can be tested.

To change the status of IUV to Testing:

Sign in to the ELMS Administration site (see: **Note**: To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS.

1. Accessing ELMS Administration).
2. Go to the WebStore Verification page (WebStore » Verification).
3. Click the **Change to Testing** link next to Integrated User Verification in the Actions column of the WebStore Verification page.

**Note**: If another verification method of the Single Sign-On class was already in Testing status, its status will automatically change to Inactive when IUV’s status is changed to Testing.

TESTING THROUGH THE TEST WEBSTORE URL

Once the status of IUV is set to Testing, the verification method is ready to be tested. This is done using
the Test WebStore URL found at the bottom of the WebStore Verification page.

**To test IUV:**

Sign in to the ELMS Administration site (see: **Note:** To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS.

1. Accessing ELMS Administration).
2. Go to the WebStore Verification page (**WebStore » Verification**).
3. Copy the URL found in the Testing Options section of the page.
4. Paste the copied URL into a *different web browser* than the one you are currently using.
5. Test to ensure that IUV was properly configured on the test WebStore to which you are directed.

**Note:** All orders placed using the Test WebStore URL will be test orders. This means that the Order Details page will display “Test Order” and no product keys will be issued.
Activating IUV

Once IUV has been configured and successfully tested, you are ready to activate it and begin using it on your WebStore.

To activate IUV:

Sign in to the ELMS Administration site (see: Note: To configure IUV in ELMS, you must be a registered and active ELMS Administrator or a web developer who has been assigned to the IUV Administrator role in ELMS.

1. Accessing ELMS Administration).
2. Go to the WebStore Verification page (WebStore » Verification).
3. If there are any non-SSO verification methods active on your WebStore (e.g. User Import), deactivate or delete them.

Note: If a non-SSO IUV is active at the same time as a non-SSO verification method, then shoppers who try to sign in to your WebStore will be given a choice of sign-in methods. For a more seamless user experience, it is recommended that you make IUV your WebStore’s only active verification method.

4. Click the Activate link in the Actions column next to Integrated User Verification. IUV is activated on your WebStore and can be used to verify and sign in users.

Note: If you wish to stop using IUV on your WebStore, click the Deactivate link beside it on the WebStore Verification page. It is possible to have more than one verification method active at the same time, providing the verification methods belong to a different class.

Restoring Administrative Roles

IUV implementation creates a new account for each user of your WebStore. When a user’s new username does not match their old username, administrative roles are not passed from the old account to the new. As a result, some of your WebStore’s administrators may find that they cannot access the ELMS administration site when they sign in with their new IUV account.

Affected administrators have two options if they wish to continue acting in their previous administrative role(s).

1. Contact Kivuto’s Support Team and request that the administrative roles associated with their old account be assigned to their new account.
Note: Depending on the role being requested, the request may have to come from the primary administrator of your WebStore (i.e. the individual under whose name your organization’s subscription was issued).

2. Continue to sign in using their old account credentials rather than through IUV. This can be done through the Administration sign-in portal at: e5.onthehub.com/admin.
Appendix A – Sample Code

Samples of the code required by a customer server to register an authenticated shopper and redirect the shopper to the WebStore are available in C#, VB.NET 2.0 and PHP can be found at: https://software.onthehub.com/documentation/ELMS_IUV_Sample_Code.zip.

Appendix B – Support Information

If you have any difficulties with configuring IUV for ELMS or require technical assistance, send an email to tac@kivuto.com.

Please include the following:

- Customer name
- Contact name
- Contact email
- Contact phone
- ELMS account number
- Any failure codes or error messages encountered (see: Response Codes and Error Messages)
- Detailed description of the problem or request for information