

# 

SAML2.0 Request & Response Companion Guide

# Confidentiality

© Copyright 2016 Softheon, Inc. All rights reserved.

**Trademarks**

Softheon, the Softheon logo, and Softheon’s products and services are trademarks or registered trademarks of Softheon. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or the names of their products. Softheon disclaims proprietary interest in the marks and names of others. Softheon grants no license, express or implied to any Softheon intellectual property by virtue of this document.

**Our Relationship**

Softheon takes care to review and verify the information provided in this document. However, we cannot be responsible for errors or omissions that may occur in the production of this document or as a result of the passage of time. In addition, Softheon may improve or change this presentation or improve or change its products and service offerings from time to time, without updating this document

**Confidentiality**

All information supplied in this document is to be considered Softheon confidential. This document shall not be copied, disclosed, or distributed without a written consent from Softheon.

Contents

[Confidentiality 1](#_Toc456686124)

[1.1 Overview 3](#_Toc456686125)

[1.2 Technical Implementation 3](#_Toc456686126)

[1.2.1 Security 3](#_Toc456686127)

[1.2.2 SAML2.0 Outbound Redirect 3](#_Toc456686128)

[1.2.3 SAML2.0 Inbound Redirect 4](#_Toc456686129)

# 1.1 Overview

This document is intended to provide technical specifications on how to pass the necessary data elements from the Exchange to the Carrier for payment redirects. The Exchange will generate a SAML2.0 assertion and send it to the Carrier using HTTP POST. The SAML2.0 assertion will be located in the POST body under the key value “SAMLResponse”. After validating the signature on the SAML2.0 assertion, the Carrier will be able to extract the member and payment info from the assertion. Once the member completes the payment on the Carrier’s portal, the payment results will be posted to the Exchange using SAML2.0.

This section and following subsections describe in detail how the following two transfers will be conducted:

* 1.2.2 Secure Outbound Redirect from Exchange to Carrier
* 1.2.3 Secure Inbound Redirect from Carrier to Exchange

# 1.2 Technical Implementation

# 1.2.1 Security

Since sensitive data is being passed between the Exchange and Carrier, security considerations must be taken into account. The redirect from the Exchange to the Carrier and from Carrier to Exchange will both leverage the HTTPS protocol. The SAML2.0 assertion will also be signed from the requestor’s certificate so the receiver of the SAML2.0 assertion can authenticate the message.

# 1.2.2 SAML2.0 Outbound Redirect

The table below provides the SAML2.0 assertions for the request from the Exchange to the Carrier for payment redirects.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Data Element Group | Data Element | Required(R),  Optional(O),  Conditional(C) | Description | Data Type | Min  Length | Max  Length |
| **SAML**  **Protocol Response** |  |  |  |  |  |  |
|  | saml2p:Response format | R | urn:oasis:names:tc:SAML:2.0:protocol SAML Protocol Response for HTTP post binding | String | saml2p: Respons e format |  |
|  | saml2p:StatusCode format | R | urn:oasis:names:tc:SAML:2.0:status:S  uccess  Contains Success or Failure | String | saml2p: StatusC ode format |  |
| **SAML**  **Core**  **Attributes** |  |  |  |  |  |  |
|  | SAML2:NameID format urn:oasis:names:tc:SAML:1.1:na meid-format:unspecified | R | This should be the Information Exchange System ID issued to the Carrier during the Data Services Hub onboarding process | String |  |  |
|  | SAML2: SubjectConfirmation Method | R | urn:oasis:names:tc:SAML:2.0:cm:sender-vouches | String |  |  |
|  | ds:Signature | R | Digital Signature of the SAML Assertion that includes the Partner’s Public Key | XML Digital Signature |  |  |
| SAML Extend Attributes | | | | | | | |
| **Consumer**  **Identifiers** |  |  |  |  |  |  |
|  | Partner Assigned Consumer ID | R | Unique Identifier assigned by Carrier for the consumer for  interactions with the Exchange. | String | 1 | 32 |
|  | Subscriber Identifier | R | Identifier for the Subscriber | String | 1 | 13 |
| **Transfer Information** |  |  |  |  |  |  |
|  | User Type | R | Type of the user logged on to the partner website  Consumer  Partner Call Center Rep  Agent  Broker | String | 1 | 18 |
|  | Return URL | R | Exchange’s Website URL to which the current user will be securely transferred back after their interaction with Carrier’s Portal. | String | 1 | 100 |
| **Payment Information** | | | | | | | |
|  | Payment Transaction ID | R | Transaction ID for the payment | String | 13 | 13 |
|  | Market Indicator | R |  | String | 1 | 50 |
|  | Assigned QHP Identifier | R |  | String | 1 | 50 |
|  | Total Amount Owed | R |  | Decimal |  |  |
|  | Premium Amount Total | R |  | Decimal |  |  |
|  | APTC Amount | R |  | Decimal |  |  |
|  | Proposed Coverage Effective Date | R |  | Date | yyyy-MM-dd |  |
| **User Information** | | | | | | |
|  | First Name | R | First name of the subscriber | String | 1 | 50 |
|  | Middle Name | O | Middle name of the subscriber | String | 1 | 50 |
|  | Last Name | R | Last name of the subscriber | String | 1 | 50 |
|  | Suffix Name | O | Subscriber’s suffix | String | 1 | 50 |
|  | Street Name 1 | R | Street address | String | 5 | 75 |
|  | Street Name 2 | O | Apt/suite/etc. number | String | 5 | 75 |
|  | State | R | State Code | String | 2 | 2 |
|  | Zip Code | R | Zip Code | String | 5 | 9 |
|  | Contact Email Address | R | Email address of the subscriber | String | 1 | 100 |
|  | TIN Identification | R | Subscriber’s Social Security Number | String | 9 | 9 |

# 1.2.3 SAML2.0 Inbound Redirect

Once the Carrier receives and authenticates the SAML2.0 response they can extract the member’s details and payment details from the SAML2.0 assertions. Once the Member completes the payment the Carrier can redirect them back to the Exchange using HTTP SAML2.0 POST. The SAML2.0 assertions will retain the member’s details along with the payment results. The table below provides the SAML2.0 assertions for the redirect from the Carrier to the Exchange.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Data Element Group | Data Element | Required(R),  Optional(O),  Conditional(C) | Description | Data Type | Min  Length | Max  Length |
| **SAML**  **Protocol Response** |  |  |  |  |  |  |
|  | saml2p:Response format | R | urn:oasis:names:tc:SAML:2.0:protocol SAML Protocol Response for HTTP post binding | String | saml2p: Respons e format |  |
|  | saml2p:StatusCode format | R | urn:oasis:names:tc:SAML:2.0:status:S  uccess  Contains Success or Failure | String | saml2p: StatusC ode format |  |
| **SAML**  **Core**  **Attributes** |  |  |  |  |  |  |
|  | SAML2:NameID format urn:oasis:names:tc:SAML:1.1:na meid-format:unspecified | R | This should be the Information Exchange System ID issued to the Carrier during the Data Services Hub onboarding process | String |  |  |
|  | SAML2: SubjectConfirmation Method | R | urn:oasis:names:tc:SAML:2.0:cm:sender-vouches | String |  |  |
|  | ds:Signature | R | Digital Signature of the SAML Assertion that includes the Partner’s Public Key | XML Digital Signature |  |  |
| SAML Extend Attributes | | | | | | | |
| **Consumer**  **Identifiers** |  |  |  |  |  |  |
|  | Partner Assigned Consumer ID | R | Unique Identifier assigned by Carrier for the consumer for  interactions with the Exchange. | String | 1 | 32 |
|  | Subscriber Identifier | R | Identifier for the Subscriber | String |  |  |
| **Transfer Information** |  |  |  |  |  |  |
|  | User Type | R | Type of the user logged on to the partner website  Consumer  Partner Call Center Rep  Agent  Broker | String | 1 | 18 |
| **Payment Information** | | | | | | | |
|  | Payment Transaction ID | R | Transaction ID for the payment | String | 13 | 13 |
|  | Total Amount Paid | R |  | Decimal |  |  |
|  | Payment Status | R |  | String | 1 | 100 |