

## United eWay Single Sign On via SAML

Companies using United eWay for Online Pledge Capture can tightly integrate employee accounts from the corporate intranet with online campaigns. United eWay's Online Pledge Capture System (OPCS) provides a full, standards-based implementation of Single Sign On (SSO) using SAML. This document is not intended to present the SAML specification, just the supported implementation within the OPCS. Documentation defining the SAML specification can be found at: <http://www.oasis-open.org>.

### How does it work? Four easy steps:

1. Employees log on to the company intranet
2. Employees click on a link taking them to a special launching page on the intranet
3. This launching page collects the employee information into an XML document, encrypts the data, and submits it to the United eWay donor site.
4. United eWay decrypts the data, creates the employee account if necessary, and logs that employee into the donor site

### Terminology

OPCS – United eWay's online pledge capture system, commonly referred to as the "donor site".

OPPS – United eWay's online pledge processing system, commonly referred to as the "admin site".

Integrator – the company or organization implementing SSO using SAML with OPCS.

Donor – a person that is associated with the company or organization that intends to use OPCS.

Asserting Party – the integrator's system that asserts information about a donor.

Target URL – URL for OPCS SSO:

Testing environment: <http://opcssso-test.United-e-Way.org>

Production environment: <https://opcssso.United-e-Way.org>

Campaign Code – The campaign code specified for the campaign to which the donor is associated. This code uniquely identifies your online campaign and is used to look up preferences that you have configured for your online pledge site.

SAML fragment – The XML fragment containing authentication and information specific to the integrator and donor.

Encrypted Data – The Triple DES encrypted SAML fragment.

Donor Attribute – Information specific to the donor. The OPCS implementation of SAML supports the full list of attributes available in the Donor Import file specifications (<https://docs.UnitedeWay.org/specs/opps-import/DonorImport.pdf>) with the following changes:

- Donor Identifier (within the SAML fragment, this is used as the value for the NameIdentifier attribute)
- The field "username" is always ignored
- The field "password" is always ignored

## Implementation

United eWay supports the SAML implementation commonly referred to as the Browser/POST profile in which the following processing occurs:

1. The donor has an authenticated session on the integrator's system.
2. An HTML form, which includes an encrypted SAML fragment in a hidden form element, is provided back to the donor's browser from the integrated system.
3. The donor's browser posts the form to the target URL.
4. OPCS requests the Triple DES public key from OPPS for the campaign specified by the campaign query string parameter value.
5. OPCS decrypts the SAML fragment using the obtained public key.
6. The donor is authenticated within OPCS using the campaign specified by the campaign query string parameter value and the donor identifier within the decrypted SAML fragment.
7. If the donor's account does not currently exist, the account is created and populated with information from the SAML fragment.
8. The donor is logged into and redirected to the donor site.

## Sample Case

ACME is an organization that has implemented SSO with OPCS. The ACME campaign has been assigned a campaign code of "ACME\_Campaign" within OPPS. Bob and Joe are donors employed by ACME who wish to make a donation through OPCS. Bob is a salaried person who makes \$60,000 per year and has been assigned a Donor Identifier of "Bob\_1". Joe is an hourly worker, who makes \$50,000 per year at an hourly rate of \$30. Joe has been assigned a Donor Identifier of "Joe\_1".

## SAML Fragment

The SAML fragment uses the supported extensions of the SAML specification, in which extrinsics can be included using the Attribute element. The Attribute element contains a single attribute named `AttributeName` and a single element named `AttributeValue`.

### Bob's SAML fragment:

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
  <saml:AuthenticationStatement AuthenticationMethod="password"
    AuthenticationInstant="2004-12-10T10:32:00Z">
    <saml:Subject>
      <saml:NameIdentifier SecurityDomain="acme.com" Name="Bob_1" />
    </saml:Subject>
  </saml:AuthenticationStatement>
  <saml:AttributeStatement>
    <saml:Attribute AttributeName="First Name">
      <saml:AttributeValue>Bob</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="Last Name">
      <saml:AttributeValue>Smith</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="Donor Group Name">
      <saml:AttributeValue>Finance</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="AnnualSalary">
      <saml:AttributeValue>60000</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

### Joe's SAML fragment:

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
  <saml:AuthenticationStatement AuthenticationMethod="password"
    AuthenticationInstant="2004-12-10T10:32:00Z">
    <saml:Subject>
      <saml:NameIdentifier SecurityDomain="acme.com" Name="Joe_1" />
    </saml:Subject>
  </saml:AuthenticationStatement>
  <saml:AttributeStatement>
    <saml:Attribute AttributeName="First Name">
      <saml:AttributeValue>Joe</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="Last Name">
      <saml:AttributeValue>Carlson</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="Donor Group Name">
      <saml:AttributeValue>Marketing</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="AnnualSalary">
      <saml:AttributeValue>50000</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="HourlyPayRate">
      <saml:AttributeValue>30.00</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

## HTML Form

The HTML form (at a minimum) contains the following:

- A form with a method of post. The action attribute of the form contains the target URL and a query string parameter with the name "campaign".
- A form element named "data" which includes the encrypted data.

DRAFT

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
.
.
.
<body onload="document.forms[0].submit();">
  <form name="ExampleForm"
    method="post"
    action="http://opcssso-test.United eWay.org?campaign=ACME_Campaign">
    <input type="hidden" name="data">epqnbashaqabalzav==</input>
  </form>
</body>
</html>
```

DRAFT