SAML message examples

Requesting authentication at a specific LoA

A SP can request authentication at a specific LoA by specifying that LoA in the `AuthnRequest`. Note that an SP can send an `AuthnRequest` to the gateway at any time, also when a user is already logged in at the SP. This allows an SP to raise the LoA depending on the context.

The requested LoA is seen as a minimum LoA. The SURFsecureID gateway can perform authentication at a higher LoA, in which case the higher level will be expressed in the returned SAML `Assertion`.

The requested LoA is passed to the SURFsecureID gateway in an `AuthnContextClassRef` element in a `RequestedAuthnContext` element in the SAML `AuthnRequest`:

RequestedAuthncontext

```
<samlp:RequestedAuthnContext>
    <saml:AuthnContextClassRef>http://surfconext.nl/assurance/loa2</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

AuthnRequest with a request for authentication at LoA 2

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ID="_ace040cdf97c2efba5aa4d973a32318217b9aaae09"
                    Version="2.0"
                    IssueInstant="2014-05-26T06:47:27Z"
                    Destination="https://sa-gw.surfconext.nl/authentication/single-sign-on"
                    >
    <saml:Issuer>http://test-sp.example.com</saml:Issuer>
    <samlp:RequestedAuthnContext>
        <saml:AuthnContextClassRef>http://surfconext.nl/assurance/loa2</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

All AuthnRequest messages must be signed by the SP using SHA-2. The `HTTP-REDIRECT` binding must be used to submit the request: the signature is put in HTTP request parameters (no XML-Signature is used).

Authentication failure

When authentication fails, it is generally because the user:

1. cancels authentication during verification of the second factor or
2. does not have a suitable second factor identification.

User cancels authentication

```
 <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                ID="_Yasz/Kubip05bTwe7hIWOc5As+NxwmEliPJ88nUQ"
                Version="2.0"
                IssueInstant="2015-05-12T12:17:38Z"
                Destination="https://your-sp.example.com/acs-location"
                InResponseTo="_6d93f735ccfb8d98454999b4016d515834211b0dde"
                >
    <saml:Issuer>https://sa-gw.surfconext.nl/authentication/metadata</saml:Issuer>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:AuthnFailed" />
        </samlp:StatusCode>
                <samlp:StatusMessage>Authentication cancelled by user</samlp:StatusMessage>
        </samlp:Status>
</samlp:Response>
```

User does not have suitable second factor identification

```
 <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                ID="_Yasz/Kubip05bTwe7hIWOc5As+NxwmEliPJ88nUQ"
                Version="2.0"
                IssueInstant="2015-05-12T12:17:38Z"
                Destination="https://your-sp.example.com/acs-location"
                InResponseTo="_6d93f735ccfb8d98454999b4016d515834211b0dde"
                >
    <saml:Issuer>https://sa-gw.surfconext.nl/authentication/metadata</saml:Issuer>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext" />
        </samlp:StatusCode>
        </samlp:Status>
</samlp:Response>
```