

# FEEIDE

Bridging OpenID and SAML 2.0



Andreas Åkre Solberg  
andreas@uninett.no

# FEIDE Terminology

## OpenID Terminology

OpenID  
Consumer

OpenID  
Identity

OpenID  
Provider

## SAML 2.0 Terminology

SAML 2.0  
Service Provider

SAML 2.0  
Identity Provider



# What is your OpenID?

Your identity - is your web site URL!

<http://rnd.feide.no> is my OpenID identity.

- You can control over what you put on that URL.
- The URL is globally unique.
- It is one aspect of your identity.



# User centric

OpenID is centric around the user, not centric around a specific IdP or federation.

OpenID consumers works with all possible OpenID providers - no need for trust relationship in advance - basically consumers does not have to trust the provider, they trust **the user!**

The user can switch to another IdP at any time...

# FEIDE No trust?

There is no trust in OpenID.

A site can never really know **who you are** - instead the site can know that you are the very same person that registered an account.



# Target group: services

World wide services where everyone can create "anonymous" accounts, but there is a need to protect the account with credentials:

as yahoo, aim, flickr, facebook, digg, technorati ++  
(world wide and too large to possibly join every possible federation out there)

Lightweight accounts: comments on blogs, public wikis, polls etc.

(too small to join a complex SAML2.0 federation)

# FEIDE The open in OpenID

*OpenID is "open".*

- No federation
- Anyone can become an OpenID consumer (Service)
- Anyone can become an OpenID provider (IdP)
- All OpenID providers can authenticate users for all consumers (no groups/federations/circles of trust) - just one big network where everyone is connected...

# FEIDE Why?

Why introduce OpenID in our closed but happy federated environment?

- Convenient for users! Many more services increases the usefulness of federated SSO.
- These services would never be SPs.
- It is not a competing technology - it will be an extension to our federations. We don't replace SAML with OpenID, we extend with OpenID.

# FEIDE Why OpenID?

## Independent

Not bound to specific vendor.

## Simple

The spec is only a few pages.



# How does it work

On the OpenID address web site, you add some meta headers about your OpenID provider:

A screenshot of a web browser window. The title bar reads "Feide RnD". The address bar shows "http://rnd.feide.no/". Below the address bar, the browser's developer tools are open, showing the source code of the page. The code includes a comment and two link tags for OpenID metadata.

```
<!-- OpenID -->  
<link rel="openid.server" href="https://uninett2.bridge.feide.no/simplesaml/openid/provider" />  
<link rel="openid.delegate" href="https://openid.feide.no/andreas@uninett.no" />
```


This is an abstraction layer that allows you to switch Identity Provider re-using the same OpenID identifier.



# How does it work

When you visit an OpenID consumer, you are asked about your OpenID URL:

Sign in with OpenID [What is OpenID?](#)



Sign in

Then the consumer contacts that URL, extract the openid meta headers, and now have the address of the OpenID provider.

# FEIDE Two modes

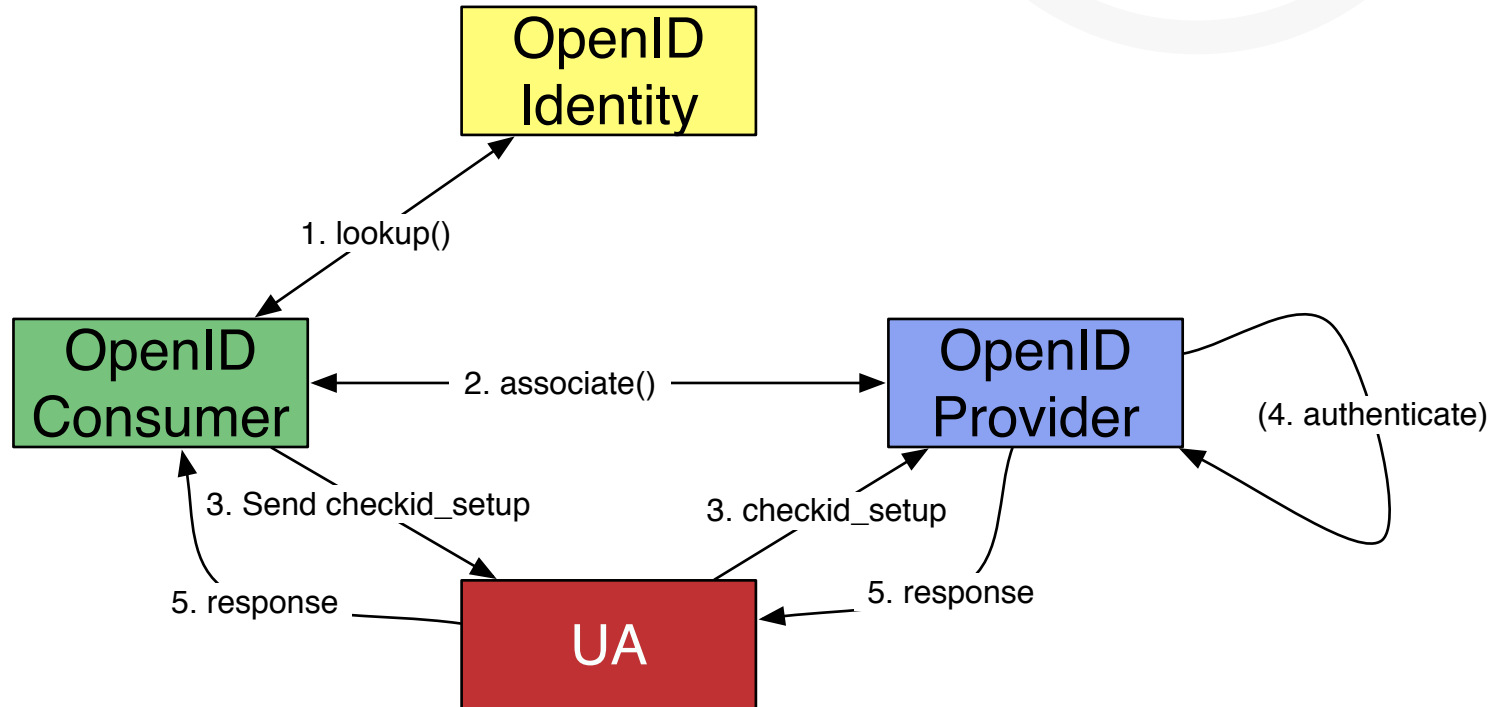
There is two modes:

**smart mode** and **dumb mode**

Smart mode is for consumers that can keep state.

Dumb mode is for consumers that are stateless.

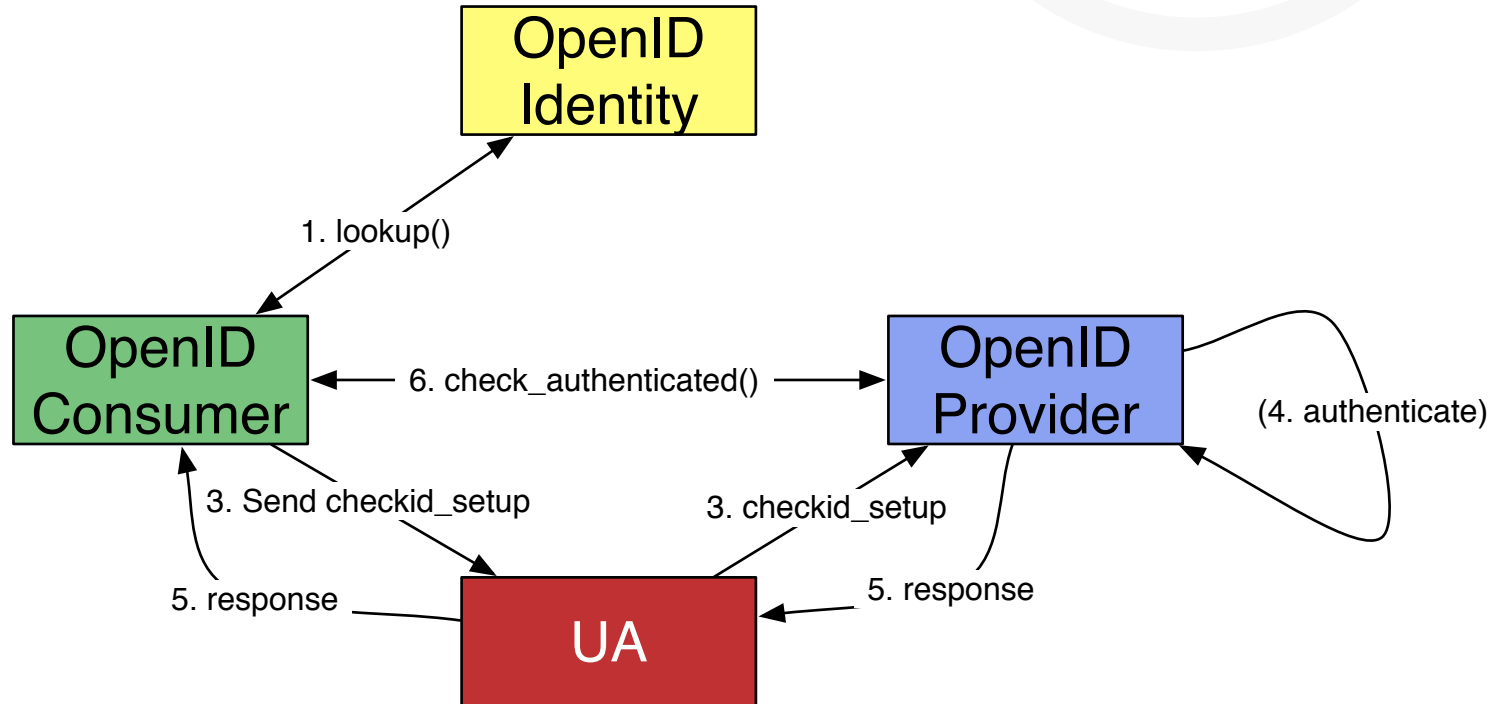
## Smart mode



Shared key is exchanged in advance using DH in the `associate()` call.



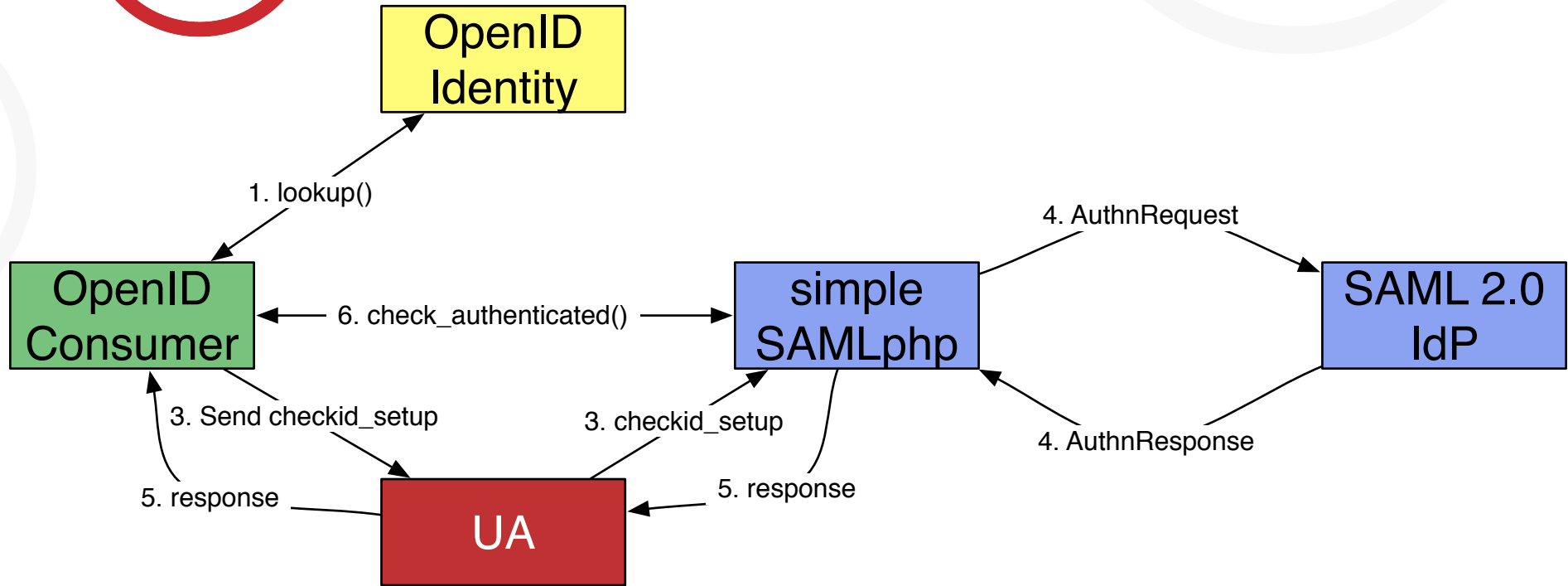
# Dumb mode



Shared key is exchanged in advance using DH in the associate() call.



# OpenID <-> SAML 2.0



Shared key is exchanged in advance using DH in the `associate()` call.



# Security considerations

## Phishing?

Not different from other web sec mechs. Some counter attacks: native browser support, infocard++.

## No trust?

We don't need it, we have SAML too ;)

## DNS attack on consumer

If you care much about securing your accounts, your OpenID identity + OpenID server should be on HTTPS.