

Migration Guide 1.1

New Features

Fediz IDP

- Core relies on Spring Web Flow and Spring Security
- supports publishing WS-Federation Metadata document
- can act as Resource IDP besides Requestor IDP
- supports Home Realm Discovery Service
- Form based Login support
- SAML Holder-Of-Key support
- Encrypted token support
- Auditing

Fediz Plugins

- Support for Jetty 7 and 8
- Support for IBM Websphere 7 and 8
- Support for Spring Security 3.1 and 2.0
- Support for CXF JAX-WS
- Support for PEM format signer certificate
- SAML Holder-Of-Key support
- Encrypted token support
- Extension points to customize SignIn request

Major Changes

- Configuration file for Relying Parties in the IDP moved from `RPClaims.xml` to `idp-config-realm.xml`
- IDP Federation URL changed to `https://<hostname>:<port>/fediz-idp/federation`
- IDP supports two realms A and B out-of-the-box which impacts the certificates used. The `stsstore.jks` has been replaced by `stsrealm_a.jks` and `stsrealm_b.jks`
- Relying Parties use the `ststrust.jks` which only contains the public key of the two signer certificates and the 1.0 signer certificate for backwards compatibility (Fediz 1.1. RP and Fediz 1.0 IDP)

API Changes

- None

Deprecated API

- None

Examples

- Signer certificate changed to support more than one realm. All examples trust the Realm A by default whereas Realm B is used for authentication only.
Configure the following issuer in `<trustedIssuers>` in the fediz configuration file:

```
<issuer certificateValidation="PeerTrust" />
```