

# Signicat Documentation

## Connectis Identity Broker Release Notes

Historical release notes for the Connectis Identity Broker.

### 18 March 2022

#### Security patch

We have patched a security vulnerability in one of our systems (Old Gen). We have also thoroughly investigated the scope, impact and consequences of this potential risk and we have taken mitigating actions. The system has immediately been patched.

---

### 20.02

#### MyConnectis

MyConnectis has been extended so that Service Providers can now use MyConnectis for configuring their SP applications that are using OpenID Connect to connect to the Connectis Identity Broker.

MyConnectis now also offers the opportunity for customers using eHerkenning or eIDAS via de Connectis Identity Broker to manage their service catalogs. This is available under Configure eH/eIDAS -> Configure Service Catalog. This functionality is only available for customers connecting to eHerkenning and eIDAS through the Connectis Identity Broker. Customers connecting directly to eHerkenning should still contact Connectis Technical Support for service catalog changes.

For insight into certificates, MyConnectis now provides an overview of all available certificates of the Connectis Identity Broker. This includes Signing certificates, TLS certificates and Client certificates. It is also possible to generate a new, or download an existing, CSR for requesting new certificates.

#### Decryption functionality for mobile adapters

The mobile adapters in the Connectis SDK support encryption of app data. This has now become more secure, since the decryption key is not generated on the phone, but by the Connectis Identity Broker. This means that the decryption of attributes can always only be done when the user is logged in into the app.

The account linking feature is simplified for the mobile adapters, since the account linking can now be done via the Connectis Identity Broker. Two user tokens can be send to an endpoint on the broker, which will validate the tokens and store them.

#### Mobile-Web SSO

Service Providers can easily implement the sharing of a user session over their mobile app (created with the Connectis SDK) and their website when redirecting users from the app to a browser. This means that users being redirected from the app to the website do not need to authenticate themselves again.

## **eHerkenning chain authorization update**

With this release an intermediary is able to perform chain authorizations on behalf of sole proprietaries registered with BSN.

---

## **19.11**

Contains various bugfixes, security improvements and performance improvements

### **QR code login**

The Mobile adapters in the Connectis SDK, together with the Connectis Identity Broker support QR code login functionality. After being authenticated in the mobile app, the user can select QR code authentication on the Connectis Identity Broker and scan the QR code on the website with the QR code scanner from the mobile app. The authentication of the user from the app will then be shared with the website.

---

## **19.10**

(We have switched to a new version numbering scheme starting with this version.)

### **MyConnectis available**

MyConnectis, the self service environment for the Connectis Identity Broker, is now available on request for all customers. For more information about MyConnectis, see <https://connectis.com/en/connectis-identity-broker/myconnectis/>

### **Chain authorizations eH**

Updates to the chain authorization functionality from eHerkenning have been made. Chain authorization accounts are now available from every eHerkenning supplier.

---

## **9.6**

### **2FA TOTP (Authenticator app with Time-based One-time Password)**

We now support TOTP (like Google authenticator) as a multi factor authentication (MFA) option on top of any other supported IdP on the Connectis Identity Broker.

After MFA with TOTP has been enabled, users are required to enter a Temporary One-Time-Password (TOTP) code generated by an Authenticator App for the application, which they need to enter in the MFA screen to authenticate themselves.

The TOTP code is only valid for a limited amount of time and cannot be used for another authentication.

From MyConnectis, the SP can configure the Issuer information. The implementation includes both adding extra devices and changing the shared secret during the login flow.

### Single Log Out (SLO)

The Connectis Identity Broker supports single logout according to the SAML specifications. The Connectis Identity Broker will actively log out the user at the different Service Providers that made use of the SSO session of this user.

---

## 9.4

### OpenID Connect

Optimised the OpenID Connect implementation on the Connectis Identity Broker, specifically related to connections from mobile apps.

---

## 9.0

### 2FA SMS

Support SMS verification as a multi factor authentication (MFA) option on top of any other supported IdP has been added to the Connectis Identity Broker. Service Providers can provision the phone numbers and account identifiers directly to the Connectis Attribute Provider during onboarding, or later when activating the MFA option. Self-registration by the user during the login flow is also possible. After 2FA with SMS has been enabled, users are send a One-Time-Password (OTP) code via SMS, which they need to enter in the 2FA screen to authenticate themselves. The OTP code is only valid for a limited amount of time and cannot be used for another authentication.

---

## 8.10

### SSO

The Connectis Identity Broker supports Single Sign On (SSO). Besides the SSO functionality that the different IdPs support, the Connectis Identity broker can now take care of SSO regardless of the IdP. The Connectis Identity Broker places a (session) token in the browser of the user to identify the user when it returns for a new authentication request. This token does not contain any personal identifiable information. Based on the token and the authentication request (LoA, attributes, etc), the broker checks if SSO is applicable and handles the authentication appropriately.

---

## 8.8

### Account linking

All linking activities are logged, a history of the profile is retrievable and upon deletion of the profile, the history is also deleted.

---

## 8.6

### iDIN

The Connectis Identity Broker now supports iDIN connections. You can connect to iDIN via different banks.