FREJA eID

RELEASE NOTES

March 2018

Mobile application version 1.4.0

Relying Party API – Documentation version 4.0

TABLE OF CONTENTS

Freja eID Release Notes

These Release notes describe all the changes made in the Freja eID system in the previous period, This includes:

- changes in the Freja eID mobile application from version 1.3.0 to 1.4.0,
- changes made to the My Pages web portal
- changes in the Relying Party API, covered in the Relying Party Developers' Documentation from version 3.0 to 4.0

Summary

- **Support for custom attributes in the API** – Relying parties can now connect a custom ID to end user's account, specific for their organisation, thus identifying users more easily within their system while users can keep using their favourite Freja eID username(s) for logging into their services.
- **Simpler integration with Freja eID for Integrators** - The relying parties that act on behalf of their own customer organisations can now integrate more easily with Freja eID services.
- **Support for cancelling authentication or signature** has been added to the Relying party API.
- **Adding more email addresses to Freja eID account** - End users can now add up to five email addresses to their Freja eID account via My Pages and use all of them as their username.
- **Tax Agency ID card available for Freja eID+ registration** - Swedish Tax Agency ID card is now supported.
- **Automatic switch from native app to Freja eID app** – Relying party's app can now open Freja eID app automatically and get the control back once the action is completed.
- **Contact support info when the upgrade fails** - Support contact information is now clearly visible in the Freja eID application to those end users who are having trouble with upgrading to Freja eiD+.
- **Improved QR code visibility**

Support for custom attributes in the API

Freja eID now allows Relying parties (RP) to manage a single, RP-specific attribute, through the Custom identifier management service in the Freja eID Relying Party API.

A typical use of this option would be to allow for login identifiers specific to RP organisation to be returned within the result of authentication. In other words, the end user can use their preferred identifier at login, e.g. email address and Freja eID will perform the translation to the custom identifier, previously configured by the RP, e.g. employee number or domain login. In such a way, it is straightforward for RPs to map user identifiers to those known within their internal systems, without the need to store this mapping in an internal database or LDAP.

A custom identifier must be unique within the requesting relying party system inside the Freja eID service. In other words, Freja eID does not allow two identical custom attributes to be set by the same RP.

Procedure

Relying parties

In order to set a custom identifier for a user, the RP needs to obtain the existing user information for that user in the Freja eID system (e.g. the email address the user has connected to Freja eID or the social security number, if the user is on the Freja eID+ level) and pass it as a parameter in the call to Freja eID services. The RP can delete the custom ID for a specific user at any time (e.g. when an employee leaves the organisation).

Consequently, changes have been made in the Authentication services as well. In the authentication request, the relying party should pass a list of attribute types which wants to be returned in the response. The `askForBasicUserInfo` parameter has now been replaced with the `attributesToReturn` parameter, so the `initAuthRequest` now looks like this:

```
{
    "userInfoType":"User info type",
    "userInfo":"User information corresponding to user info type",
    "attributesToReturn":
      [
         {
             "attribute":"Type of attribute to be returned"
         }
      ],
    "restrict":"Restricts the login request to a specific mobile device",
    "minRegistrationLevel":"Minimum required registration level of a user"
}
```

The `attributesToReturn` is an optional parameter which should be a list of objects, with each object containing one attribute type. Currently supported attribute types are BASIC_USER_INFO (name and surname; if requested, `userInfoType` must be SSN) and CUSTOM_IDENTIFIER (a unique, RP-specific, user identifier, set by the RP through).

The response body of methods for retrieving authentication results has also been adjusted to reflect this change.

> For detailed information about the Custom identifier management in our API, please refer to the following sections in Freja eID Relying party Developers' documentation:
>
> - Custom identifier management
> - Authentication services

End users

End users currently cannot choose whether they want this custom identifier to be connected to their Freja eID account or not. However, they can disable a service in My Pages if they do not wish to be referred to with this attribute. Freja eID informs end users via email that a custom ID has been added to their account, specifying exactly which ID has been added and which RP has added it.
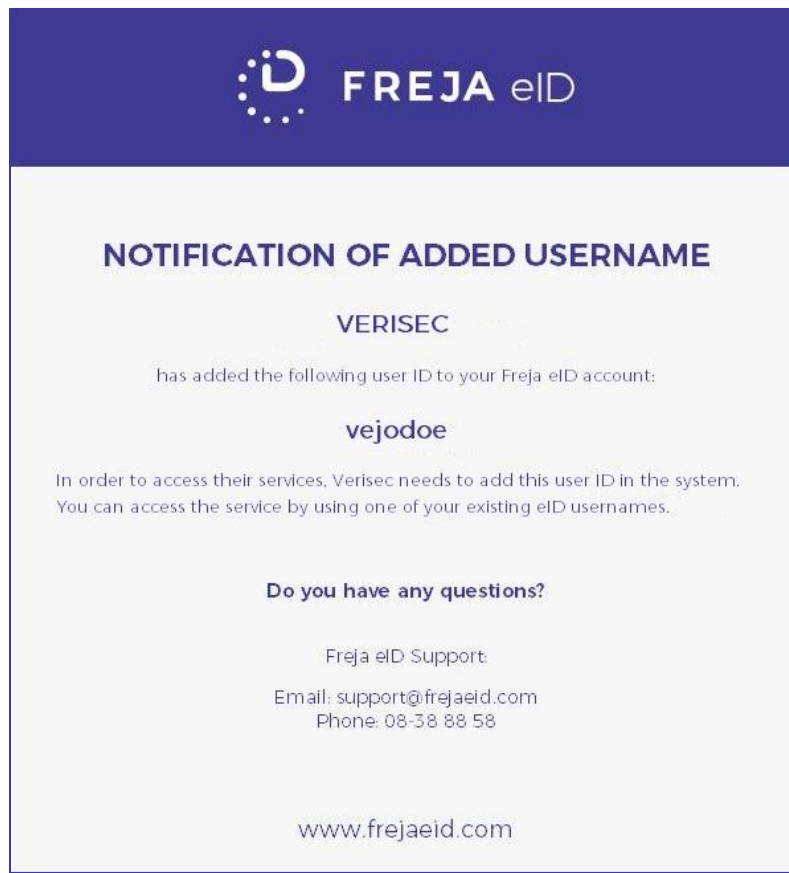
Simpler integration with Freja eID for Integrators

Identification of relying parties towards Freja eID services is achieved through SSL with client authentication. This, however, may present an issue for relying parties that act on behalf of their own customers, i.e. other organisations, which most likely have their own branding and the requirement that the end user, consuming their services, is aware of the organisation they are interacting with.

In order to avoid the complexities of having such relying parties manage multiple SSL certificates, one per customer organisation, Freja eID annotates those relying parties as "Integrators". **Integrator RPs are allowed to act on behalf of their customer organisations by utilizing a single SSL client certificate while passing the identity of a customer organisation as a parameter to API calls.**

Consequently, given the branding and presentation requirements towards end users within Freja eID, organisations on whose behalf Integrator RPs act on must be registered with Freja eID as "Integrated RPs". They cannot make use of Freja eID services directly but rather through the Integrator RP they are associated with.

Procedure

When sending an authentication or a signature request to Freja eID services, acting on behalf of an "integrated" relying party, the Integrator RP needs to pass an additional parameter to the call – the `relyingPartyId.`

> For detailed information about the Integrator relying party management in our API, please refer to the following section in Freja eID Relying party Developers' documentation:
>
> - Integrator relying party management

Support for cancelling authentication or signature

Freja eID Relying party API now supports methods for cancelling authentication and signature requests. Methods `cancelAuthRequest` and `cancelSignRequest` are added to the Authentication and Signature services respectively.

This feature is already applied to the Freja eID My Pages web portal, where users can now cancel a login or approval request, upon which the previously initiated action disappears from the action list in the mobile application.

> For detailed information, please refer to the following sections in Freja eID Relying party Developers' documentation:
>
> - Authentication services
> - Signature services

Adding more email addresses to Freja eID account

End users can now add additional email addresses to their Freja eID account and use any of them as a username when accessing services via Freja eID.

Up to five email address can be connected to one's account. The email address a user has used during the registration will be set as their primary email address by default. Users can remove email addresses and change their primary at any time.

Procedure

Additional email addresses are added via the <u>My pages</u> web portal. The user navigates to *User details* page, clicks on the **Add email address** link, enters the correct email address and then confirms the action, first in the Freja eID app and then in the confirmation email sent to the new email address.
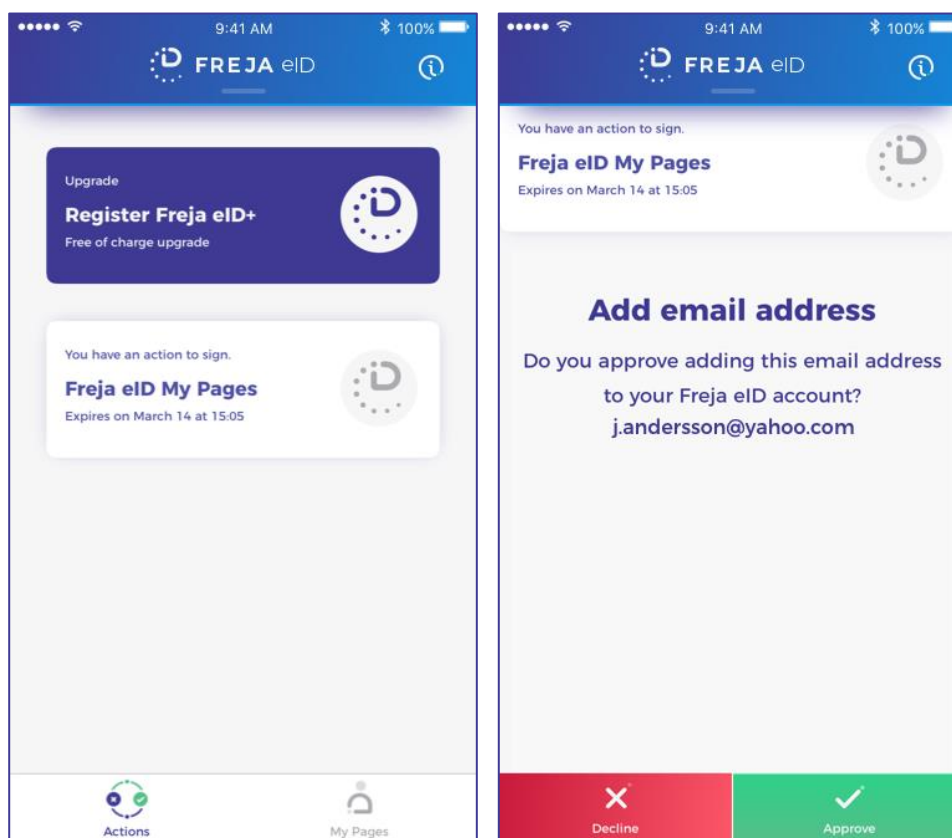
To **change the primary email address**, the user clicks the **Change primary address** link on the same page, selects an address from the list and confirms the action in the Freja eID app.

Steps for **removal of an email address** are practically the same as for changing the primary. The user cannot remove an email address previously set as their primary address.

Tax Agency ID card available for Freja eID+ registration

We have added support for the Tax Agency ID card - Svenska Skatteverkets ID-kort - which now can be used by end users for registering Freja eID+.

Automatic switch from native app to Freja eID app

Relying party's native app can now open Freja eID app automatically and vice-versa.

When end users access a service through the service provider's app installed on their device, they will be automatically transferred to the Freja eID app to confirm the action (login or signing) and then back to the desired service once the action has been confirmed. For Android users, this functionality is also supported when they try to access the service from the mobile browser, while on iOS devices, this depends on the service.

Contact support info when the upgrade fails

When there is a problem with upgrade to Freja eID+, whether with the user's ID document or during the vetting process, the **end user will be informed that the upgrade has failed and prompted to call our customer support team**. This information will be displayed In the Freja eID app, first in a pop-up and then in the "Contact Support" status header.
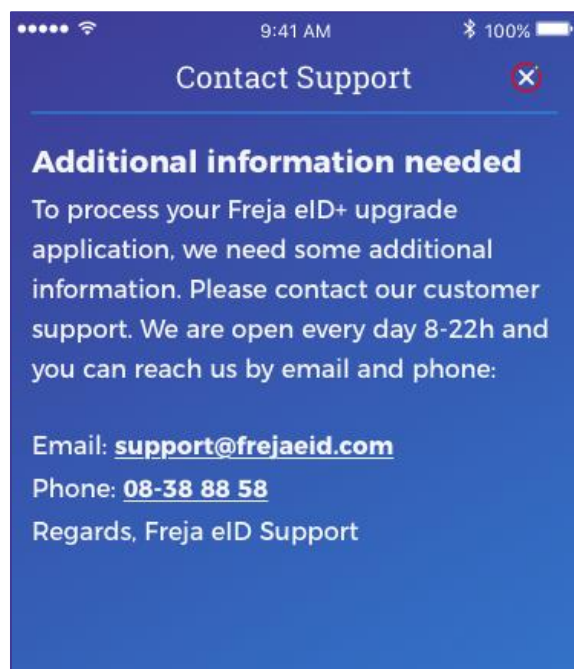
Improved QR code visibility

The new version of the mobile application contains fixes related to the QR code visibility. The QR code is displayed in the mobile application at the end of the Freja eID+ registration process. To complete the upgrade, the user needs to visit the official Freja eID vetting agent and show the QR code together with the physical ID document used for registration. The cashier then scans the QR code and compares the data received from the server with the ones on the ID document. In previous versions of the app, the QR code on some iOS and Android devices was not visible enough and therefore, hard to scan.

Any questions?

If you have any questions regarding this release, please get in touch with your contact at Verisec or send an email to partnersupport@frejaeid.com. You can also find more useful information about Freja eID on our website [www.frejaeid.com.](http://www.frejaeid.com)