Best practices

In this document we offer some tips and considerations to optimise your login flow.

1. Show value first

When deciding where in the user experience to prompt people to log in with xID and what login hints to use, think about at what point xID will provide the necessary value to make people choose this login alternative.

xID consists of three different login hints, and each will give the user a different experience on your website. We recommend that you truly understand the value of each login hint before implementing them, so you can present the user with the best login experience. One of our recommendations (also described here: User experience design) is to use the login hint XID:unsolicited:nodialog on the front page, instead of XID:unsolicited. Using XID:unsolicited on the front page will display a dialogue every time the user enters your website, even before experiencing the real value of your website.

This implicates that you need to convert the user to use xID, using the login hints XID:userintent or XID:unsolicited, at your website in a situation where the user understands the value of your website and what xID can add to this experience. If you convert the user to use xID every time on your website, this enables the possibility of knowing the users identity already on the front page and enables you to give him a warm welcome with the login hint XID:unsolicited:nodialog.

2. Using cookies to remember xID between sessions is not a good idea

We do not recommend that you use a cookie to remember xID for a longer period of time. This will weaken one of the strengths of xID; the link to the identity which is the foundation of a persons xID, and it also compromises the safety mechanisms that is used to verify the user. You will not know if the user changes xID user on the device, deletes his xID on another device or if his BankID is revoked.

We recommend that you keep the user logged in with xID for the whole user session, so the user dont have to log in with xID several times through the session. After the session is ended, you should do a new xID transaction for the next session. We also recommend to set an end time to the cookie, to limit the possibility to refresh the cookie for a longer period of time. Otherwise the safety in xID is compromised as described above.

If you still choose to save a cookie for a longer periode of time instead of doing a new xID transaction, you will need to inform the user and get his consent for this. Do not mislead the user to thinking that he is using xID and thus, relies on the safety of xID, when he is really exposed to a cookie set by the merchant himself.

To keep the value of the safety mechanisms in xID for both you as merchant and the user, we recommend to make new xID transactions for new user sessions.

3. Connect the user to already registered data

Users signing up with xID

For users signing up at your website with xID, you can save the PID (personal identifier) in your user database, and use this to match the users identity and display the correct user data later on.

Existing users starting to use xID

Does your corporation have statutory authority to get the national identity number from BankID? Then you are also entitled to use the national identity number saved in xID to match with the one you already have stored on your users, and this way present the correct user data to the user recognised with xID.

Connecting existing users

If your corporation is not entitled to use the national identity number from xID to match xID users with your own user data, and you want to connect existing users in your user base to the identity you get from xID, there are several ways to do this:

1. Make a match using the name and birth date retrieved from xID

2. Ask the user if he wants to use xID after he has logged in with regular user name and password - either through XID:unsolicited or XID:userintent. By using the login hint XID:unsolicited, you can lead the user to connect his accounts, as an xID dialogue automatically is shown to the user after logging in.
3. Ask the user if he wants to use xID after he has logged out, using XID:unsolicited
4. Ask the user to enter his username and password after initiating and accepting xID as an option, explaining that he needs to go through this to access his history at your website, and then the login experience will be simplified with xID from this time on

You need to consider what gives you the greatest probability of a match, and also what gives the best user experience and understanding of xID and how it works.

4. You dont have data on the user?

If you don't have any prior user information, you can retrieve user data from both xID and Additional Information (TINFO)**.**

How does this work?

Many companies already have prior user information. If you already have data registered on the user, you can use the data retrieved from xID to make the match and use your own information to prefill forms and customise your website for the user (as described in section #3 above). If you dont have any data registered on the user, you can use Additional Information (TINFO) to supply the customer profile with the data you need by adding some extra scope parameters. Get more information about this in the technical documentation.

What user data can you get from xID?

When an xID transaction occurs, the website will receive the following information about the customer:

- Full name
- Date of birth
- A unique user number (same for BankID and xID)
- The users Norwegian national identity number (if the merchant already has statutory authority to retrieve this information)

This information is coming directly from BankID and cannot be changed by the user himself. Please see the section on ID token in technical documentation for further information. You should consider whether or not you want to store the data retrieved from the service as described above. To get more detailed personal information, go here: Additional Information (TINFO).

Should you prefill or lock the user data i forms?

When using xID to complete forms for signing up or buying items and services online, you should consider:

1. How should the data be presented to the user after finishing the xID dialogues
2. At what point do you want to store the data in your user data base

There are a few alternatives for this, with different implications for the quality of the data.

- Prefill forms, enabling the user to edit the data before locking the form. This implies that the data source is the user himself, and not xID (BankID).
- Lock the user data coming from xID. This way you are able to store the information directly. In this case you can offer the user a button for editing his data.

You should consider the experience you want to give the user, and what purpose the user data serves. Maybe the user dont even need to see the actual data, enabling the form to be submitted directly for him through the dialogues of xID. Or maybe you want him to see the prefilled fields in the form and submit the form himself. Imagine how xID enables you to change and simplify the user experience, only using the dialogues that the service provides itself - for expamle making insurance offers with just a few clicks.

This information applies to data retrieved from Additional Information (TINFO) as well.

5. Change the users existing passwords to make xID safer

When the user is an existing customer starting to use xID at your website, he will have a user account with an associated password. If you make a connection between the user accounts, to make xID the safer option, please consider removing the existing password connected to the user account. You could instead generate a password that is complicated and unique, which the user never gets to know. This way he is still able to access his account without xID, using functions like "Forgotten password" etc.

6. Restrictions for age on your webpage?

Since xID contains the users date of birth, you can handle age restrictions at your website using xID. BankID is used by people from the age of thirteen and xID will work with the same age group. Its up to you how you want to use this information, but we recommend that you get an understanding of the age restrictions for your online content and use the information from xID to handle this.