SwissSign

SwissID Customer Experience Guideline (CEG)

SwissSign

Table of contents

SwissSign

1. SwissID Customer Experience Guideline

SwissID can be used in different use cases. This document will provide examples of some of the most common customer journeys.

The first part, 'The role of the RP and overview of the end-to-end login and onboarding processes', defines which aspects must be taken into consideration when implementing SwissID.

In the second part, 'Best practices', exemplary use cases are illustrated. We recommend that the relying party (RP) refers to how other existing RPs have implemented SwissID. You can find links to existing RPs at www.swissid.ch.

1.1 Scope

- This document focuses on the perspective of the identity owner (IdO). The technical procedures are described in the 'Integration guidelines for relying parties'.
- An online shop and an insurance company are used to illustrate the use cases. These are fictitious RPs of SwissSign Group AG.
- Wireframes[1] are used to illustrate the best practices. The text, colours, aspect ratios, etc., are hypothetical and do not correspond to CI or CD guidelines. These guidelines are described in the SwissID button manual.
- This guide only covers happy paths. Exception paths[2] will not be discussed. The SwissSign Group manages exceptions and errors if they occur within the SwissSign environment. The RP is responsible for managing any exceptions and errors that occur within their environment.
- Because this is a product that is being continually developed, the procedures may change over time.

[1] As opposed to mock-ups, wireframes do not include accurate colours or aspect ratios. They are primarily intended as illustrations and establish a conceptual framework that will then be further developed.
[2] Exception paths are scenarios in which things go wrong (unlike the happy path). They are used to catch errors and/or prepare alternative paths to ensure that the user can reach their intended destination.

2. The role of the RP and overview of the end-to-end login and onboarding processes[3]

This chapter offers an overview of the entire process.

RPs can

- send a request[4]

and, based on the answer, can

- check whether the IdO is already registered in their system
- open an account for an IdO whose UUID from SwissID is not saved or link the SwissID to an existing account as a means of authentication
- initialise step-up authentication with SwissID or switch to an alternative process independent of SwissID.

2.1 Redirection to SwissID

The RP controls the redirection to SwissID (the moment when an IdO switches from the 'world of the RP' to the 'world of SwissID'). Afterwards, the SwissID standard processes begin. This ensures that the IdO is offered a uniform user experience across different RPs.

- The RP has to position the SwissID button on their website as specified in the style guide.
- The SwissID button always redirects the user to the 'world of SwissID'.
- The overall request is stored on the SwissID button in accordance with the Integration guidelines for relying parties (IGL).
- The processes in the 'SwissID world' are always the same.
- When the IdO clicks the SwissID button, they are on a direct path to their destination so that
    - the IdO can identify themselves for the RP with SwissID if the IdO has already onboarded at an earlier time,
    - the IdO can use this button to quickly onboard themselves. After onboarding, the IdO can use the SwissID to log in to the RP's website or platform.

2.2 Return to the RP

After authentication, the IdO is redirected back to the RP. In the event of

- Login (the IdO is already registered with the RP), the IdO is verified to the RP in accordance with identity and access management (IAM).
- Onboarding, the IdO is linked to an existing account or a new account is created.
- Insufficient quality of registration (QoR), the RP decides whether it wants to initiate step-up authentication.
    - The RP can send a step-up request to the SwissSign Group. The SwissSign Group then guides the IdO through the corresponding processes.
    - Alternatively, the RP can redirect the IdO to the RP's own processes (and, for example, start a manual internal process). In this case, the IdO was not authenticated by SwissID at the desired level.

[3] Onboarding is the process of creating a local account or linking a SwissID to a local account as a means of authentication. After onboarding, an IdO can use their SwissID with an RP for authentication purposes.
[4] An RP sends a request to SwissSign. This request includes the information that the RP wants to receive from SwissSign – for example, in addition to the UUID, the individual's first name, last name and email address as well as their date of birth at a verified level with a high level of security.

3. Best practices

This chapter illustrates customer journeys that cover the most common use cases. An RP does not have to implement all the processes. An RP can use this decision tree to check which processes should be implemented:

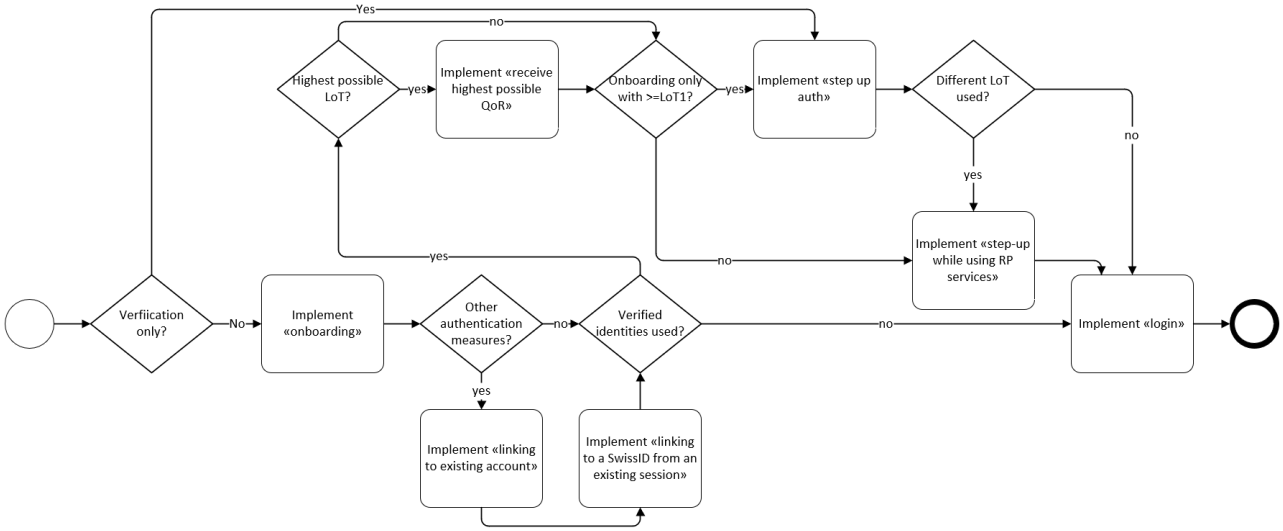

Figure 1: Decision tree

3.1 Overview of the SwissID login and onboarding process

The diagram below visualises the optimal use of SwissID. Depending on the use case, there may be deviations on the RP side.

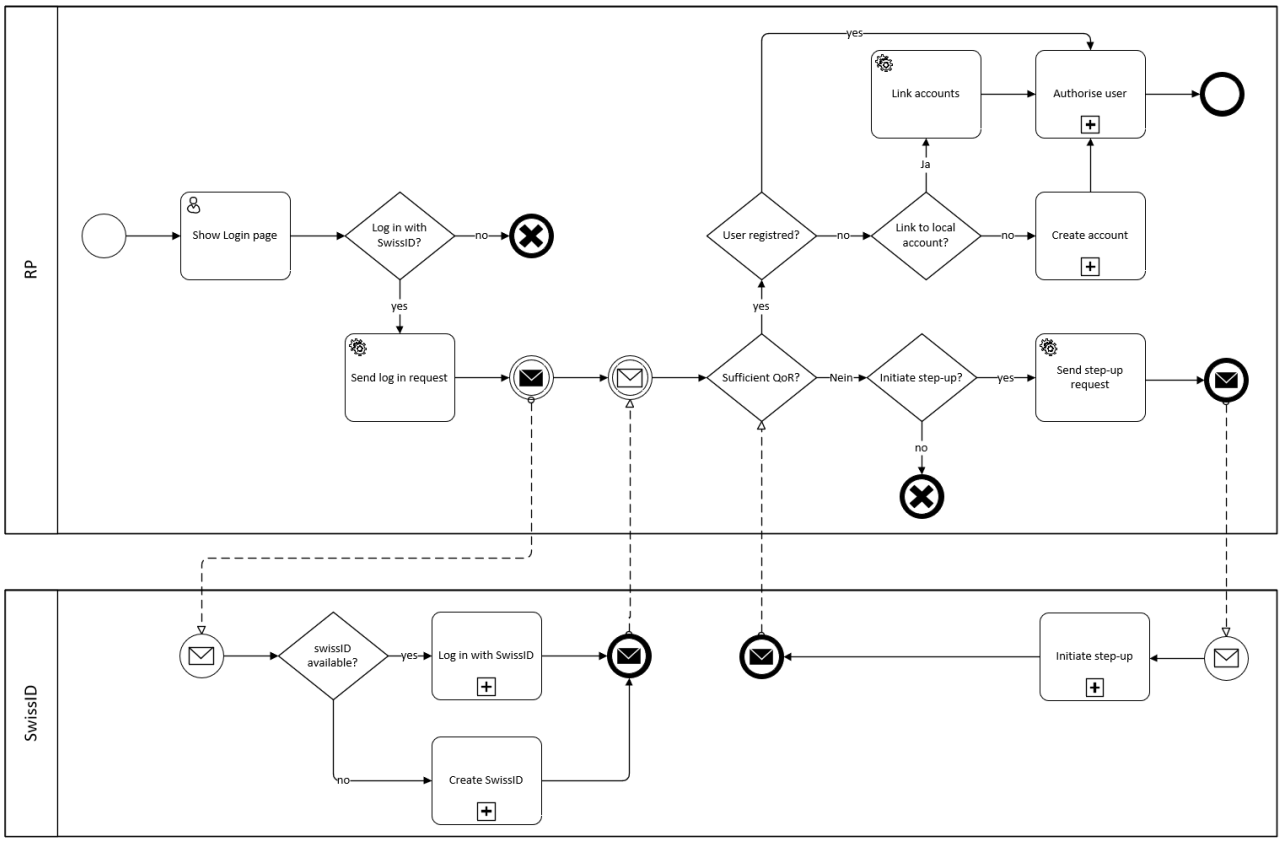

Figure 2: Overview of the onboarding and login process

Table 1: Login and onboarding

#	Process	Description	R	S
1	Show the login screen	The RP displays the login screen on their website.	X	
2	Log in with SwissID?	The IdO decides to log in with SwissID.	X	
3	Send login request	The request, the QoR, the QoA and the requested scope are sent.	X	
4	IdO has SwissID	On the login screen, the IdO enters their identifier (email address) and clicks through. Alternatively, they can create a SwissID account by selecting 'Create a SwissID account'.		X
5	Log in with SwissID	After clicking 'Log in', the IdO enters their password and completes the second factor (in the desired quality) if applicable. If no consent is stored, consent is obtained and the token is sent to the RP.		X

6	Create a SwissID	The IdO provides the necessary information to create an account, creates a password and, if asked, directly connects a second factor for authentication. Consent is obtained and the token (component for identification and authentication of the IdO) is provided to the RP.		X
7	Sufficient QoR	When the IdO is redirected back to the RP, the RP receives the token and checks whether the quality of registration is sufficient for the use case.	X	
8	User already registered	The RP uses the universal unique identifier (UUID) to check whether the user is already registered in their system.	X	
9	Authorise the user	The RP authorises the IdO using the (internally) saved permissions.	X	
10	Link to local account	The RP has the option to link the SwissID of the IdO to an existing account.	X	
11	Link account	The UUID from SwissID is linked to the local account.	X	
12	Create an account	A new account is created and the necessary steps and interactions are carried out.	X	
13	Initiate step up?	The RP decides whether they want to initiate step-up authentication or start their own internal process.	X	
14	Send a step-up request	The RP sends a step-up request to SwissID.	X	

3.2 Logging in to the RP

The IdO can use their SwissID to log in to the RP's website or platform. The RP must have already assigned the IdO (with the UUID) to an account. The RP can authorise the IdO after successful authentication.

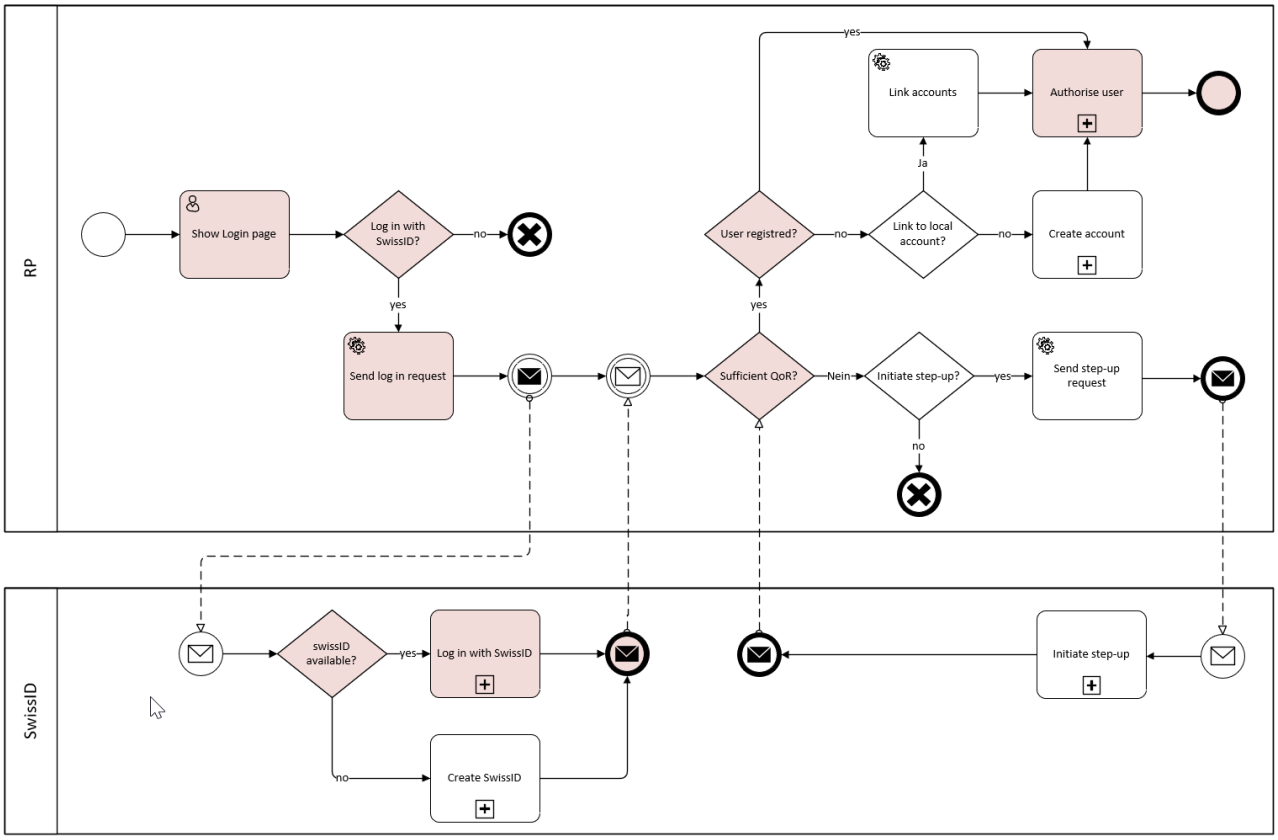

Figure 3: Login process

3.2.1 Sub-process: logging in with SwissID

The RP can include the quality of authentication (QoA) in the request. SwissID guarantees this level of quality. If the RP requires a higher QoR, SwissID can initiate step-up authentication. The RP only needs to request step-up authentication. The SwissSign Group takes care of the rest.

The IdO defines their preferred means of authentication.

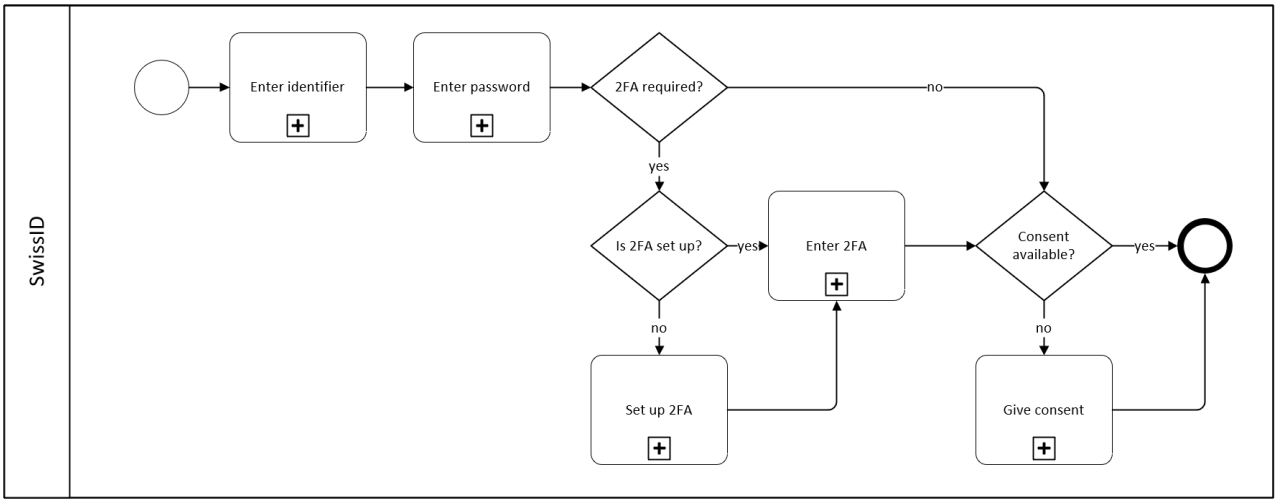

Figure 4: Logging in with SwissID

Table 2: SwissID – logging in with SwissID

#	Process	Description
1	Enter identifier	The IdO enters their identifier (email address) in the input mask and clicks 'Next'. SwissID checks whether the identifier is valid.
2	Enter password	The IdO enters their password in the password input mask. SwissID verifies the password.
3	2FA required	SwissID checks whether the • IdO • RP • applicable regulations require(s) a second factor.
4	Set up 2FA	SwissID guides the IdO through the process of activating a second factor.
5	Enter 2FA	The IdO uses the second factor and SwissID verifies its legitimacy.
6	Consent available?	SwissID checks whether persistent consent is available for this RP with this scope.
7	Give consent	SwissID shows the IdO the consent screen. The IdO gives their consent.

3.2.2 Login wireframes

You can access the clickable wireframes online (password: myShop).

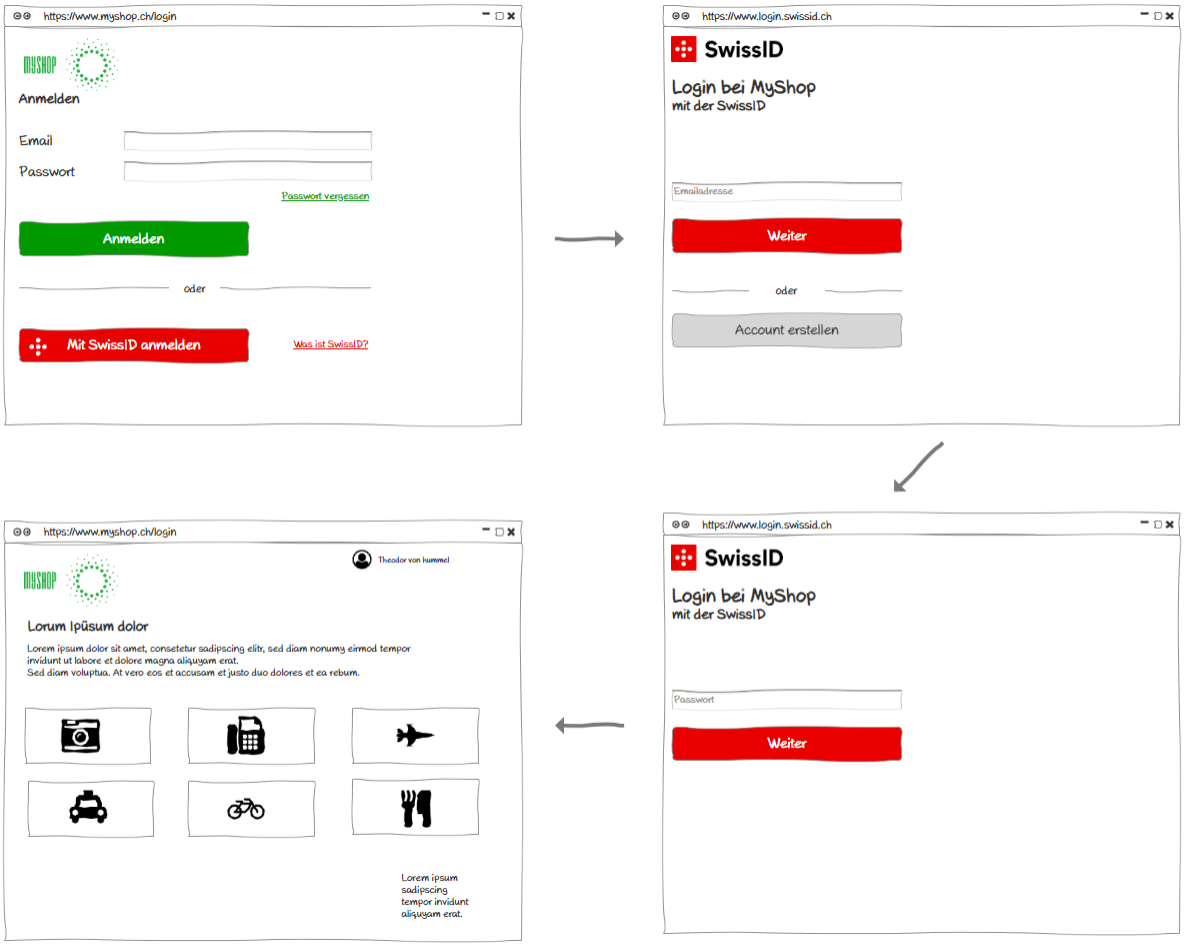

Figure 5: Login wireframes

3.2.3 Special Case: RP wants to always receive the highest possible QoR

In some cases, an RP wants to get the highest available QoR to authorise an IdO for a broader range of services. This should happen only with good reasons because SwissID holds the idea of data minimisation high. The process represents an RP, who wants to get a QoR2, but can start with a QoR0 as well. Anyway a first request could as well be for a LoT1.

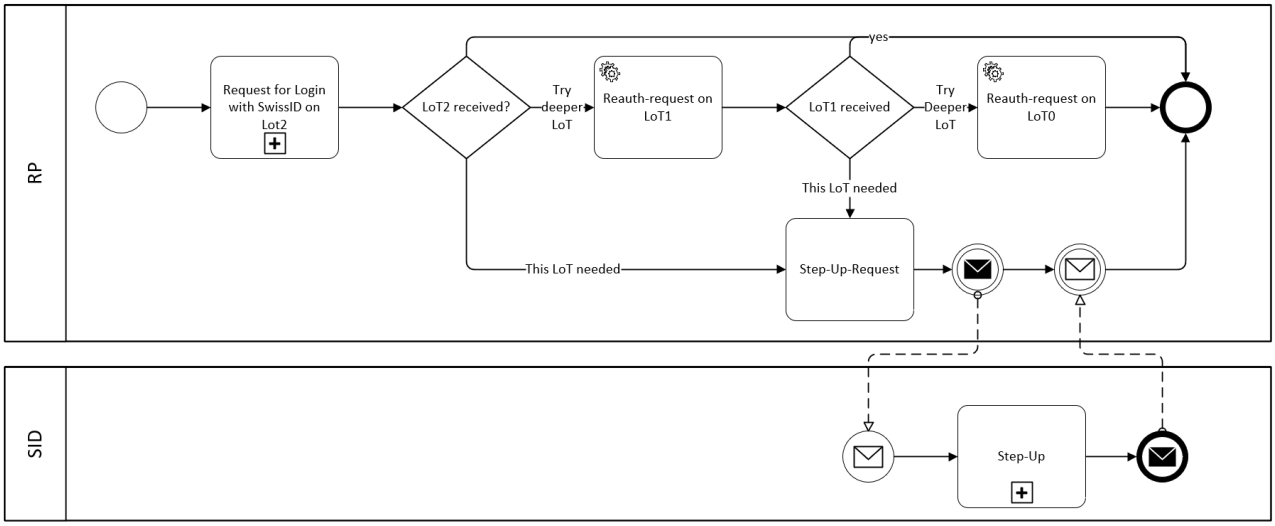

Figure 6: Request highest available QoR

3.3 Onboarding

IdOs can use their SwissIDs to onboard themselves with an RP. The RP sends the same request as for login. Based on the request, SwissID sends an answer. Once SwissID sends the UUID to the RP, the RP can determine whether a link to an account already exists. Alternatively, the RP can create a new account or link the IdO to an existing account.

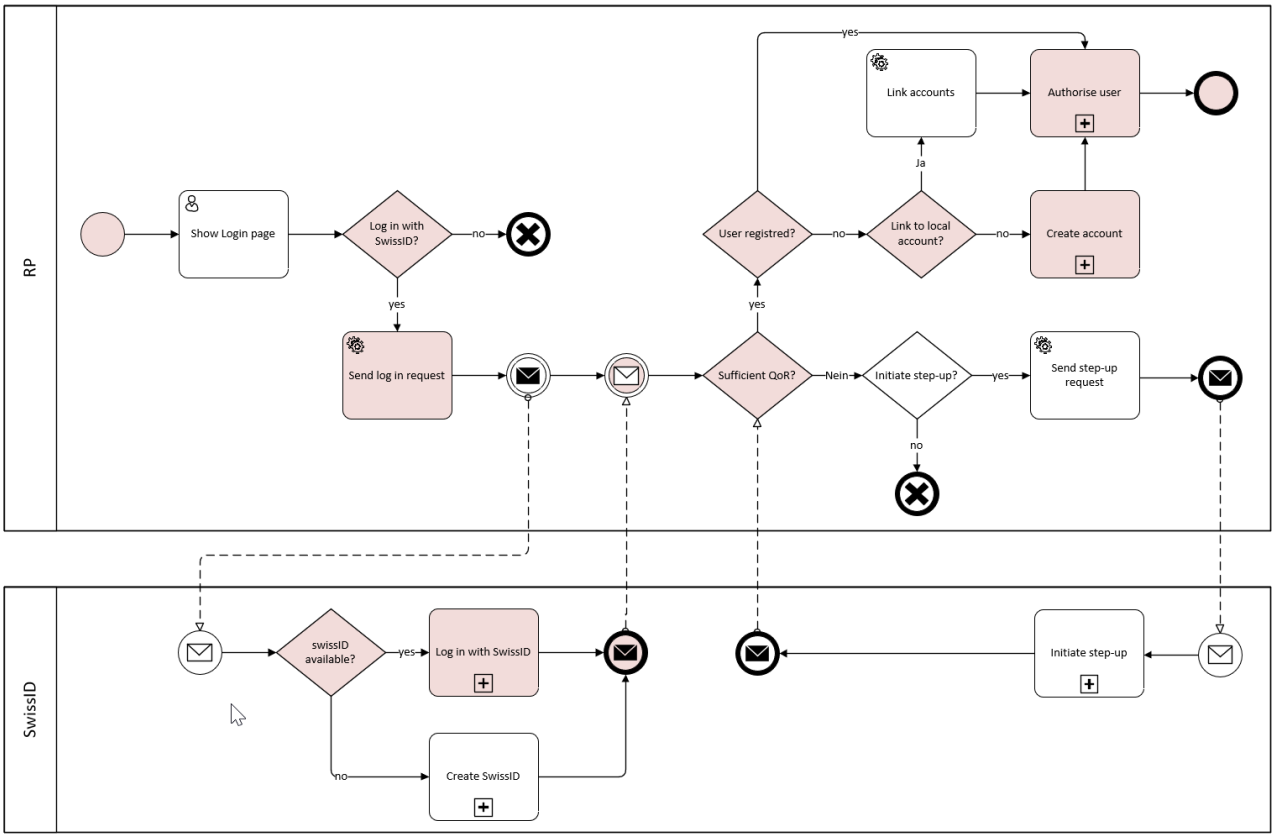

Figure 7: Onboarding with SwissID

3.3.1 Wireframes for onboarding with SwissID

You can access the clickable wireframes online (password: myShop).

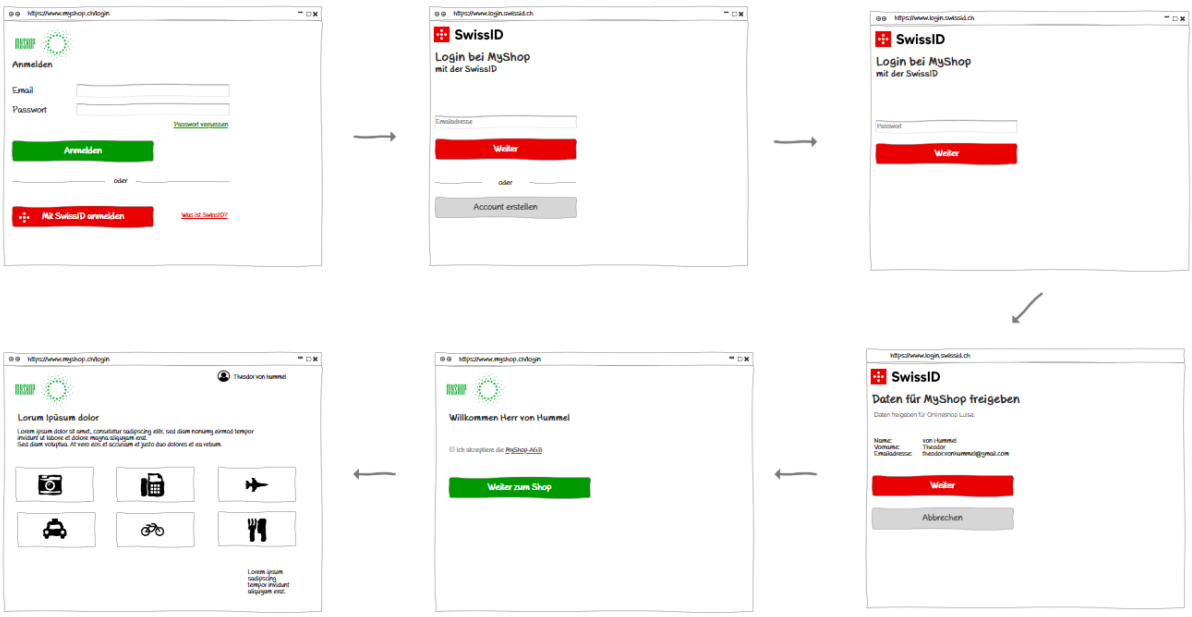

Figure 8: Onboarding with SwissID

3.3.2 Linking to an existing account

RPs can link the SwissID to an existing account as a means of authentication. The RP's Compliance department must define the reconciliation process. After authentication with SwissID and in accordance with the best practices of SwissSign Group AG, the RP authenticates the IdO with the IdO's 'old' login. This should correspond to the QoA of the request that the RP sent to SwissID. Otherwise the local login should be deactivated after linking.

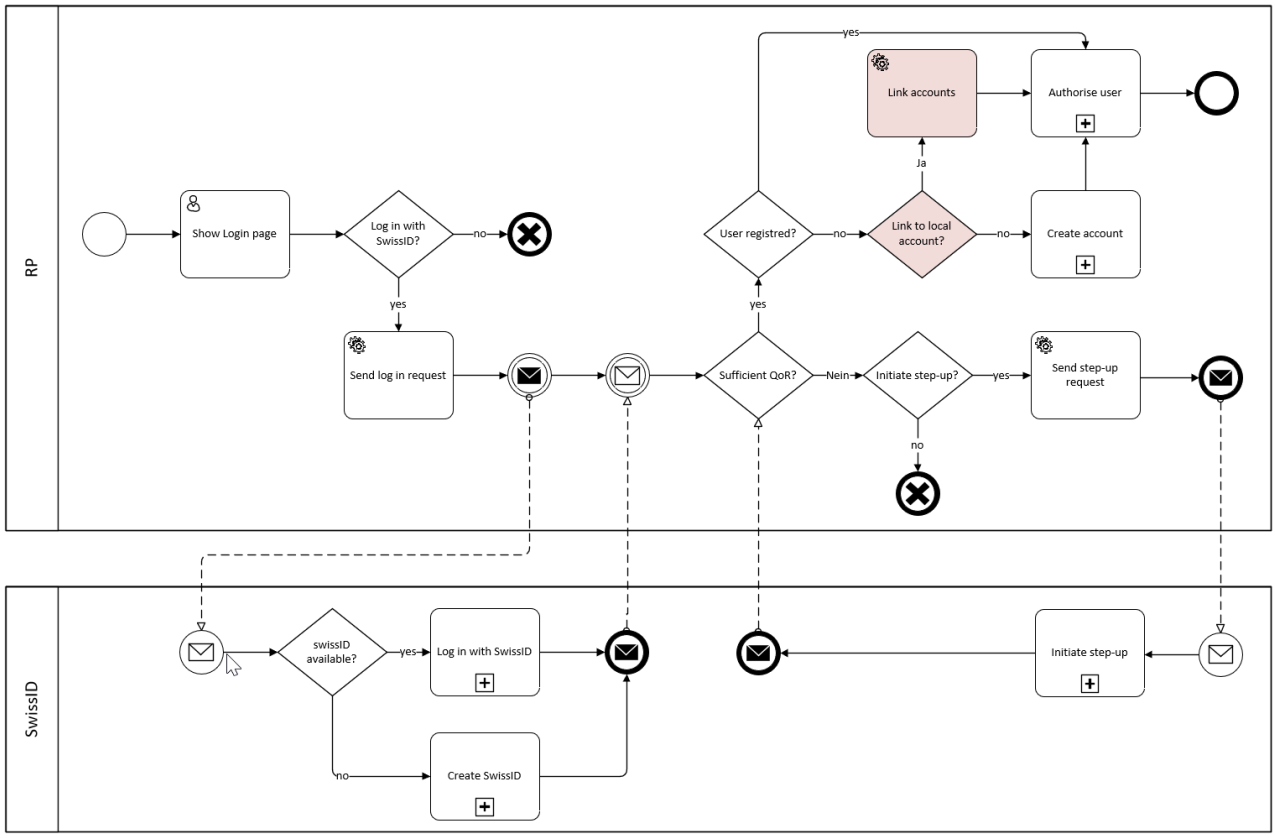

Figure 9: Linking to a local account

3.3.2.1 Wireframes for linking to a local account

You can access the clickable wireframes online (password: myShop).

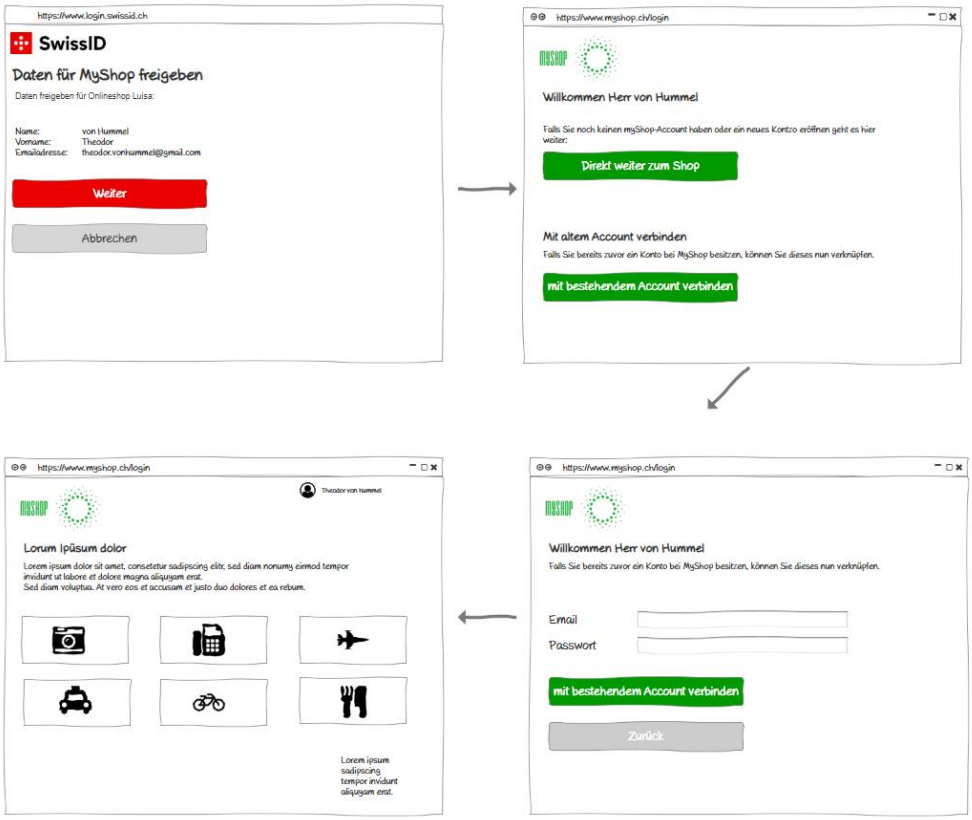

Figure 10: Linking to an existing account

3.3.3 Linking to a SwissID from an existing session

The SwissSign Group recommends that the RP make it possible to link the SwissID from an existing account also from an existing session.

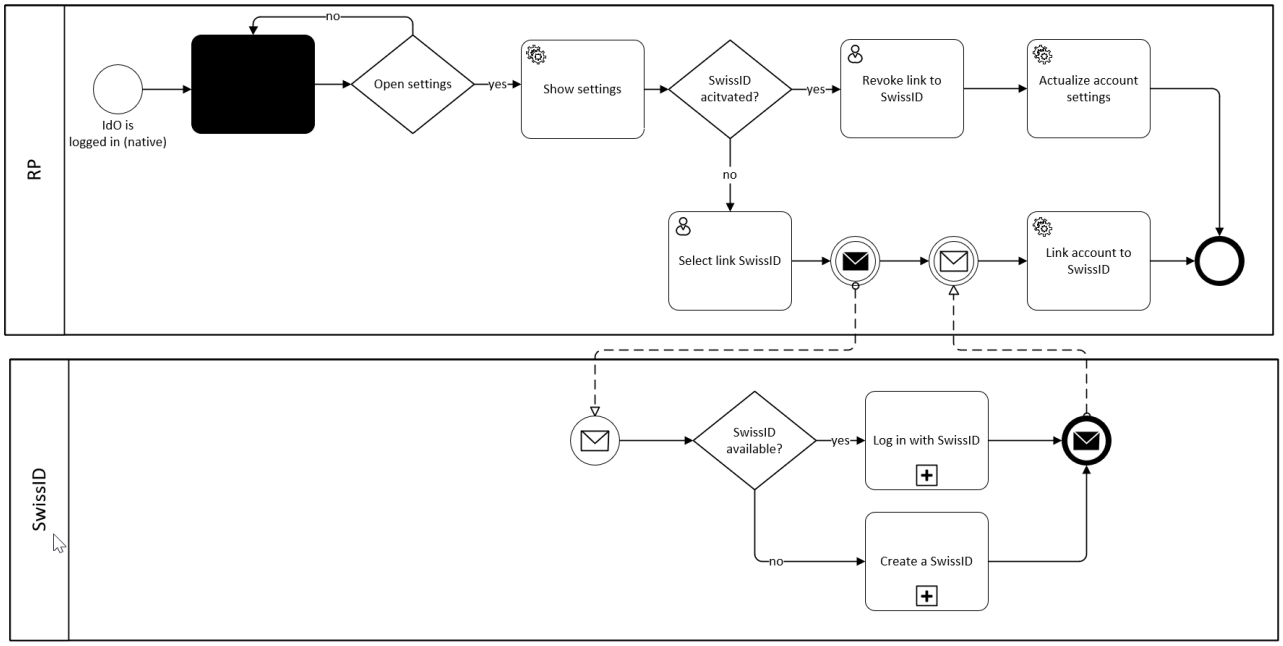

Figure 11: Linking to a SwissID from a local session

Table 3: Linking to a SwissID from an existing session

#	Process	Description	R	S
1	IdO is logged in	The RP has authorised the IdO according to his rights of the native session.	X	
2	*Blackbox*	The IdO performs actions on the RP service	X	
3	Open Settings	IF the IdO chooses “open settings” the RP presents the settings. Otherwise the IdO can continue to perform “other” actions allowed by the RP services.	X	
4	Show settings	The RP shows 'Account settings’. The RP shows the possibility to link or to decouple SwissID.	X	
5	Revoke link to SwissID	The IdO chooses to decouple the SwissID form his account	x	
6	Actualize Account settings	The RP deletes the linkage to the SwissID and adjusts user-rights.	x	
7	Select ‘Link to SwissID’	The user selects the option to link their account with SwissID	X	
8	Send login request	The RP sends the request, including the QoR, QoA and the necessary attributes.	X	

9	The IdO has SwissID	SwissID shows the login screen. The IdO enters their identifier and clicks 'Login' or selects 'Create a SwissID account'.		X
10	Logging in with SwissID	If the IdO selected 'Login', they enter their password and, if applicable, use a second factor (with the required quality) to verify their identity.		X
11	Create a SwissID	The IdO provides the necessary information to create an account, creates a password and, if asked, connects a second factor for authentication.		X
12	Sufficient QoR	The RP receives the token if the IdO is redirected.	X	
13	Link account	The SwissID is linked to the local account for which there is currently an existing session.	X	

3.3.3.1 Wireframes for linking to a SwissID from an existing session

You can access the clickable wireframes online (password: myShop).

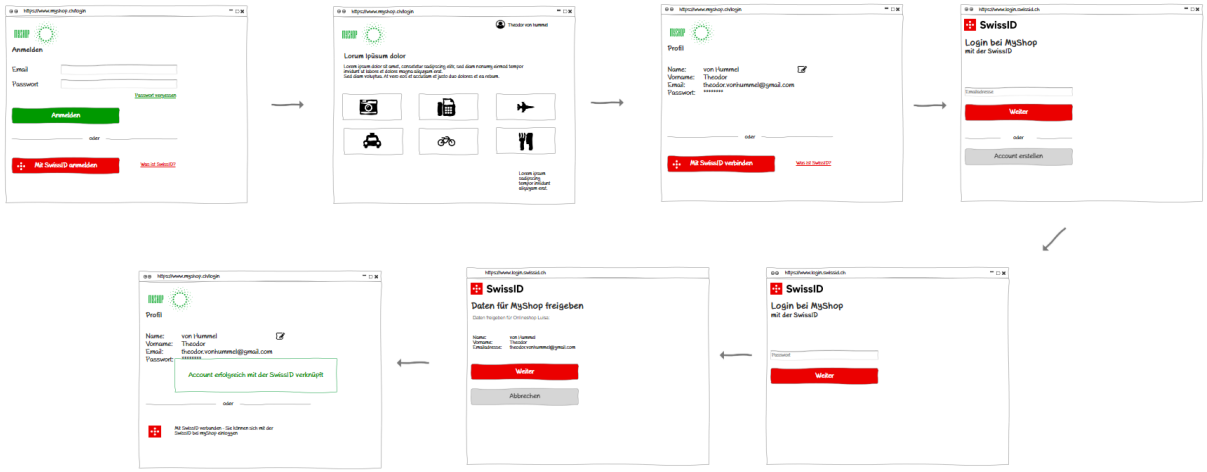

Figure 12: Wireframes for linking to a SwissID from an existing session

3.3.4 SwissID account registration

If the user does not yet have a SwissID, they can create one. This can be done directly in the authentication flow. SwissID guides them through the corresponding processes. The RP does not have to complete any additional steps.

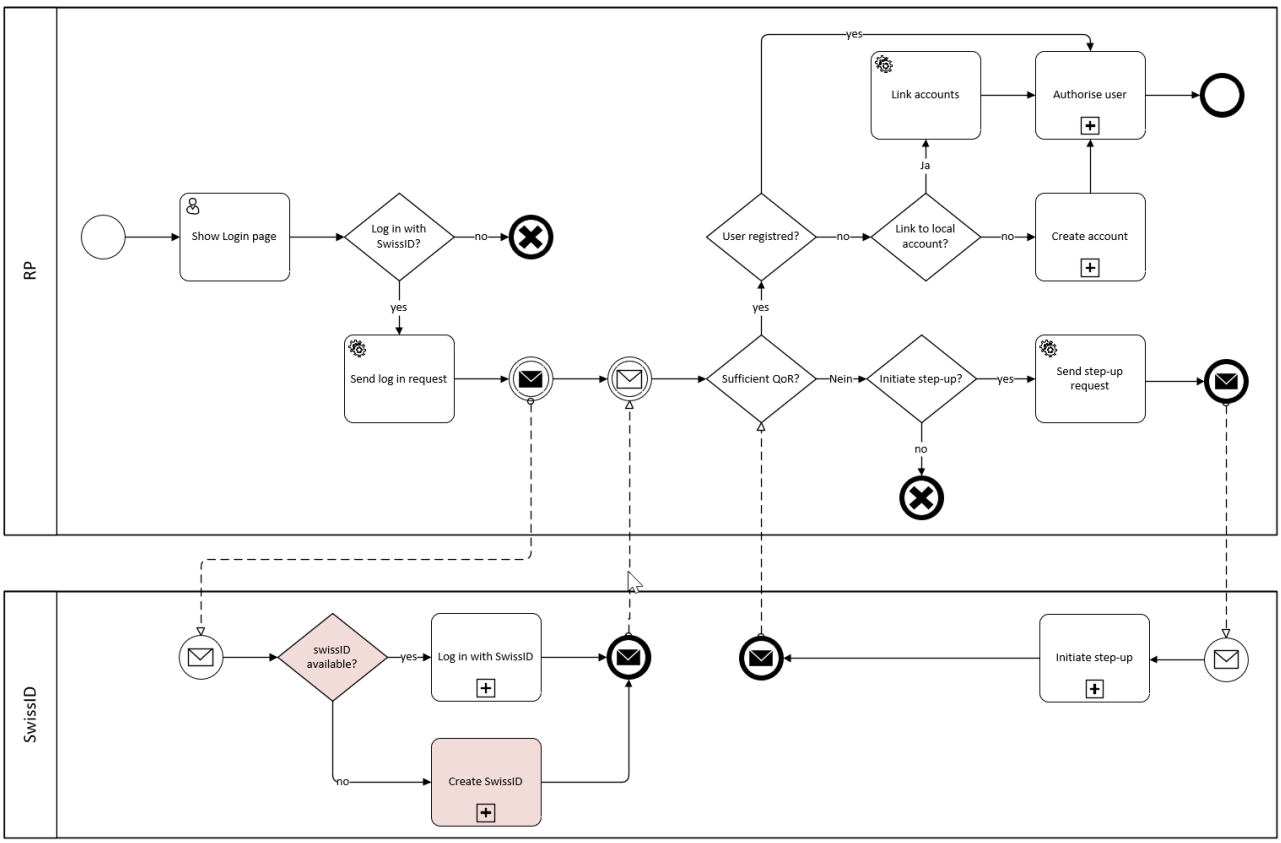

Figure 13: SwissID registration

3.3.4.1 Sub-process: create a SwissID

When an IdO creates a SwissID, they also verify their identity for the RP who sent the request.

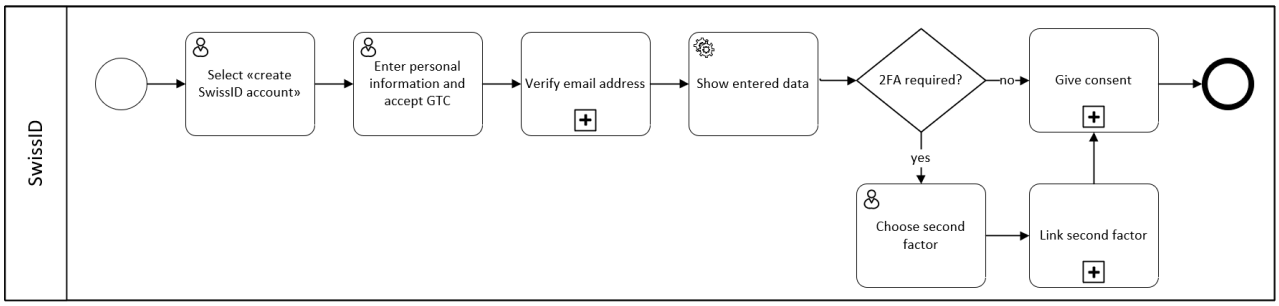

Figure 14: Create a SwissID

Table 4: SwissID – Create a SwissID

#	Process	Description
1	Select 'Create a SwissID account'	The RP or SwissID shows the option to create a SwissID account. The IdO selects 'Create a SwissID account'.
2	Enter personal information and accept the GTC	The IdO is asked to enter their personal information in order to create an account. They also need to accept the GTC. The IdO provides information about their identifiers and communication channel (email address), their identity (gender, first name, last name), creates a password and accepts the GTC.
3	Verify email address	The IdO receives an email with the verification code. The IdO enters the code to verify their email address.
4	Show entered data	SwissID shows the IdO the data they have submitted.
5	Choose second factor	The IdO is given the opportunity to add a second factor. The IdO decides which means of authentication they prefer.
6	Link second factor	The second factor selected by the IdO is linked to their account.
7	Give consent	SwissID shows the consent screen. The IdO clicks through.

3.3.4.2 SwissID registration wireframes

You can access the clickable wireframes online (password: myShop).

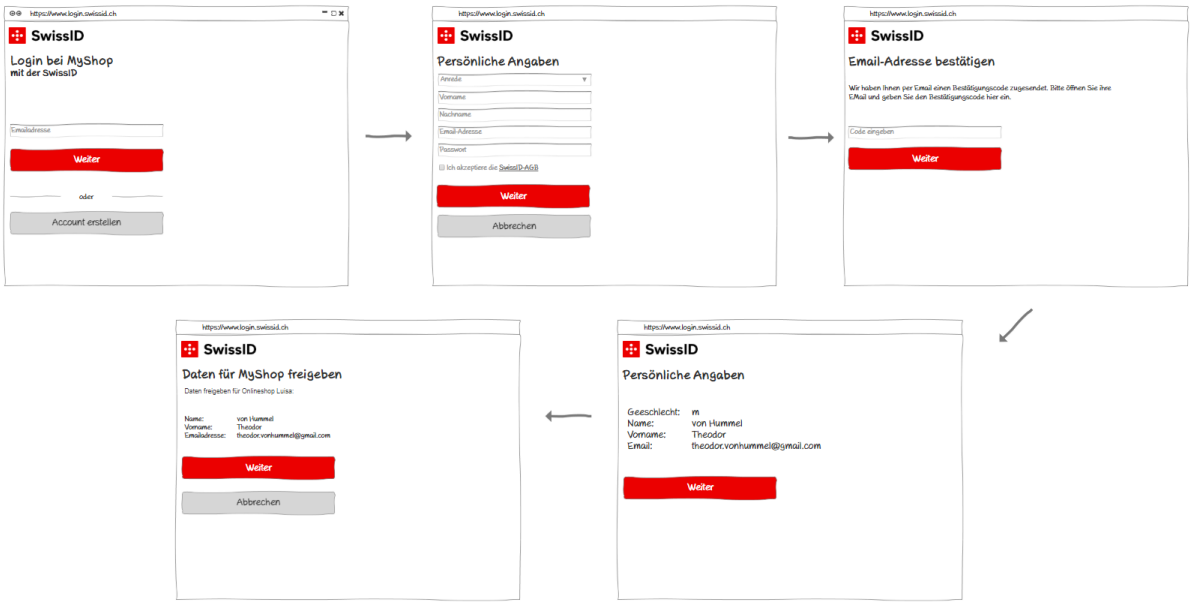

Figure 15: SwissID registration wireframes

3.4 Onboarding with step-up authentication

SwissID sends the QoR together with the token to the RP. The RP checks whether everything meets their requirements and, if the QoR is not sufficient, decides whether

- they want to move on to their own, internal process independent of SwissID or
- request step-up authentication from SwissID.
- For some step-up processes a deep link according to the IGL for RP is available
- SwissID informs the RP if a manual process (and therefore a waiting period) is needed. An RP should inform the IdO accordingly as well.

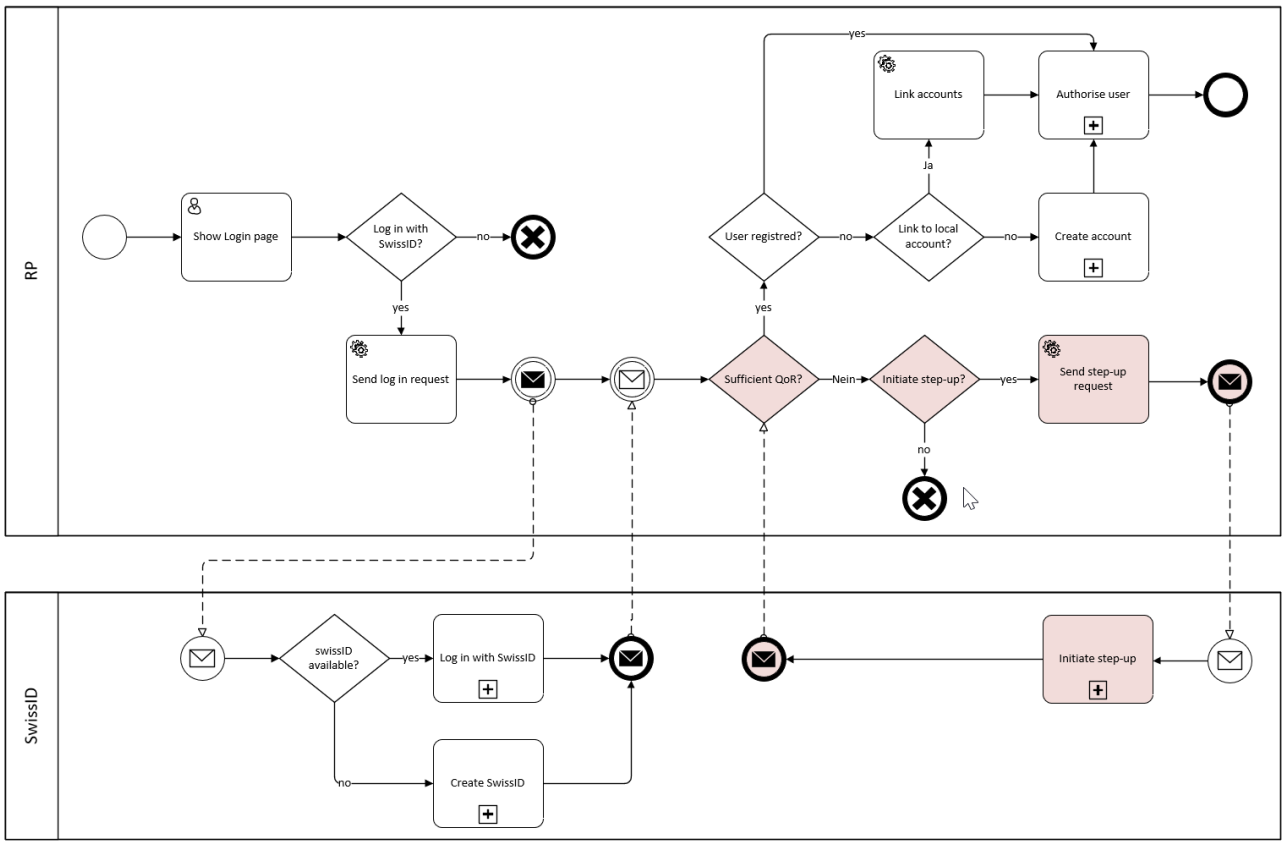

Figure 16: Onboarding with step-up authentication

3.4.1 Step-up authentication wireframes

SwissID makes sure that the IdO can upgrade to the registration level required by the RP. The photo ID process is shown here as an example.

You can access the clickable wireframes online (password: myInsurance).

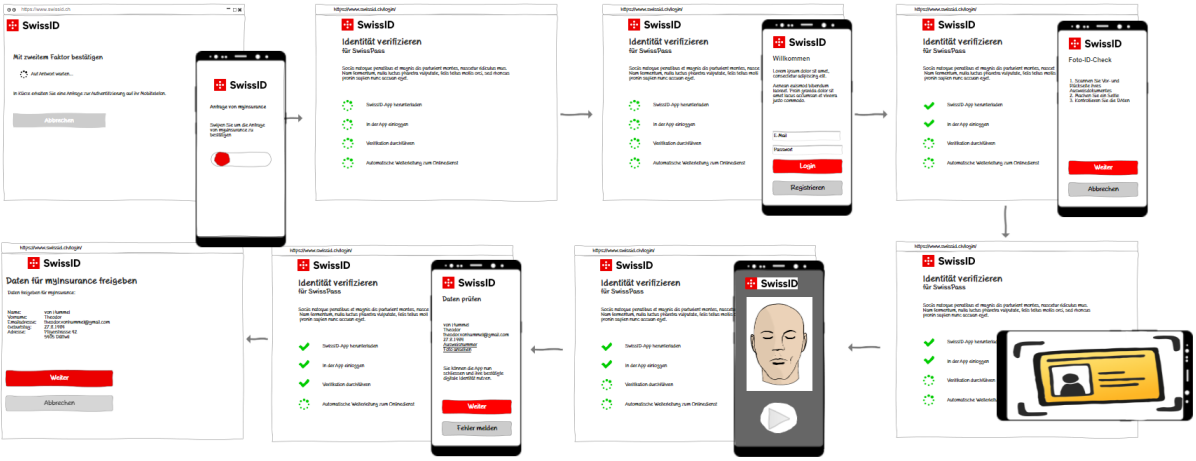

Figure 17: Wireframes for the step-up authentication example

3.4.2 Step-Up while using RP-services

Some RP have different services which need different LoT. Therefore, those RP will have to make reauthentication requests and initiate step-up processes to make certain services available to the IdO.

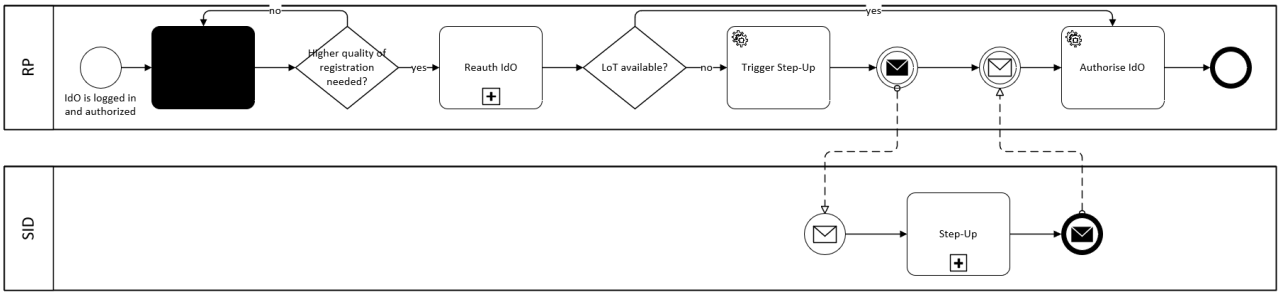

Figure 18: Step-Up while using RP-services

4. Glossary

Abbreviations	Term	Definition
IAM	Identity and access management	Identity and access management (IAM) is concerned with the management of identities and access rights to different systems and applications. The central IAM functions are user authentication and authorisation.
IdO	Identity owner	Owner of a SwissID
IdP	Identity provider	Provider of electronic identity services. Hereinafter, identity provider (IdP) will be used to refer to SwissSign Group AG as the provider of SwissID.
IGL	Integration guidelines for relying parties	The IGL serves as a manual for developers so that they can implement SwissID-specific aspects of OpenID Connect.
LoT	Level of trust	The level of trust is used to describe the corresponding security level at which a SwissID is issued. It is determined based on the quality of the identity check (QoR) and the quality of the authentication (QoA).
OIDC	OpenID Connect	OIDC is an authentication level that is based on the OAuth 2.0 authorisation protocol. The standard is monitored by the OpenID Foundation.
RP	Relying party	The relying party is the operator or provider of (online) services who is using SwissID.
Step-up authentication		The process to strengthen the quality of registration.
UUID	Universally unique identifier	The UUID is used to uniquely identify the SwissID owner to an online service. It is a number generated by SwissID that is used as a unique identifier between the IdP and the RP. When the IdO uses their SwissID with various RPs, different UUIDs are used.
QoA	Quality of authentication	The QoA defines the quality of the authentication in terms of the means of authentication used. SwissSign Group AG allows the RP to request a specific security level for the authentication. The security levels are described in Appendix A.
QoR	Quality of registration	The QoR determines the security level during registration or when collecting electronic ID (E-ID) attributes. The QoR used by SwissID is based on the current definitions in accordance with the E-ID regulations. RPs can request information on the quality of registration in accordance with Appendix A. SwissSign Group AG offers the corresponding processes and can guide the IdO through these processes. The different registration levels are described in Appendix A.

SwissSign

5. List of figures and tables

5.1 List of figures

5.2 List of tables