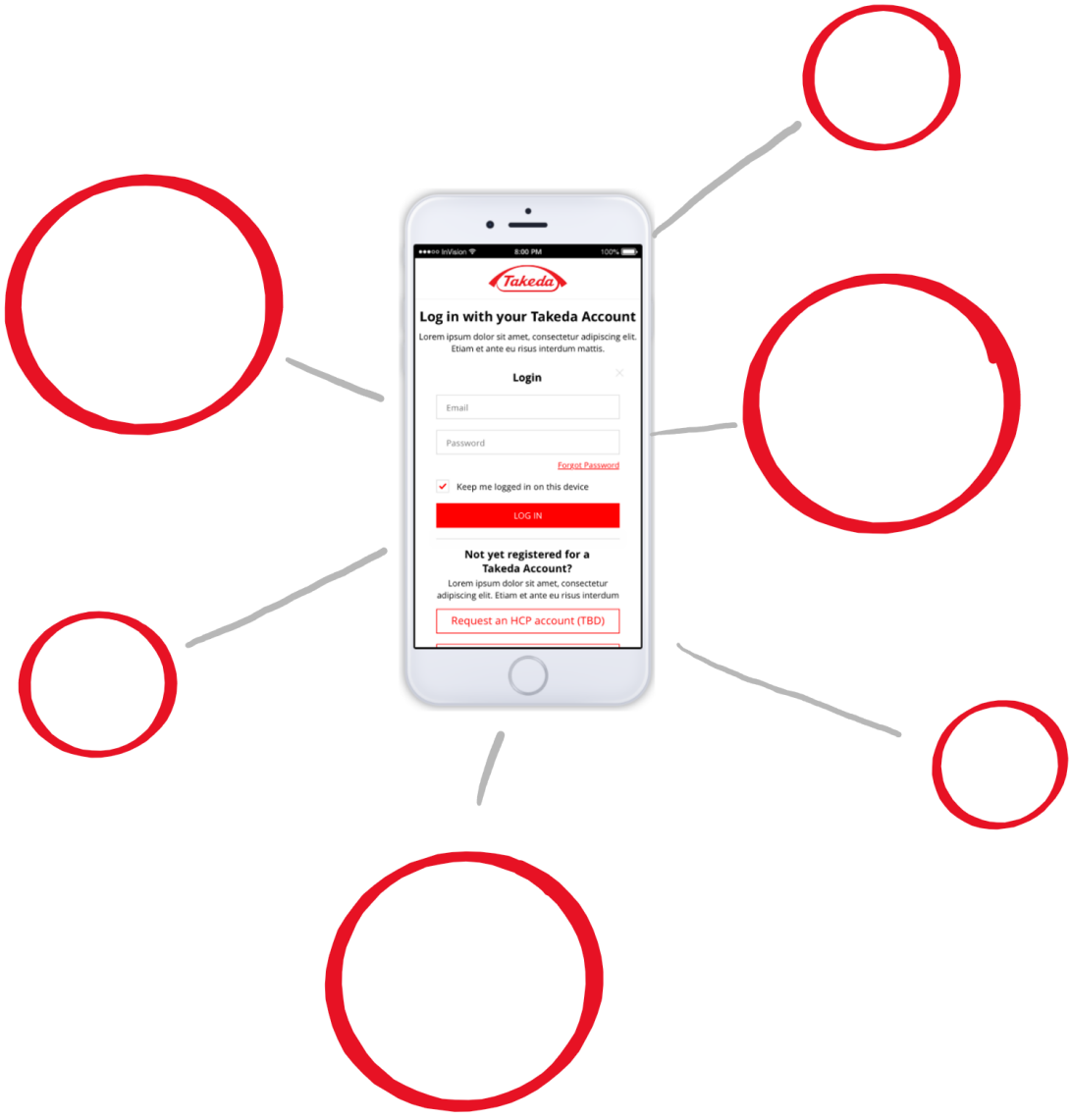
Takeda ID

Playbook



Document History

Date	*Version*	*Author/ Company*	*Description of Change*
30-07-2020	1.1	Benedikt Niepötter / Arcondis	Initial Version
08-02-2021	1.2	Isabel Alt / Arcondis	• Update Section: 3.2 How to get a Takeda ID • New Section: 3.5 Takeda ID Support Model • New Section: 4. Supporting Tools
10-10-2023	1.3	Bob Durfee / Takeda	• Updated for oxford comma. • Removal of reference to operations dashboard. • Update Section: 3.1 What kind of user information is stored, to reflect clarification of HCP group.

Table of Content

1. The Takeda ID in an overview

This playbook explains the Takeda ID by providing an overview of the following areas of interest:

- ✓ **Benefits of the Takeda ID for Takeda and for your Business Application**
- ✓ **Benefits for external stakeholders of Takeda**
- ✓ **Which Business Applications can participate?**
- ✓ **How Business Applications can utilize the Takeda ID**

1.1. What is it all about?

The Takeda ID is Takeda's global corporate external Identity & Access Management system for external stakeholders (i.e. HCPs, nurses, patients, donors, pharmacists, members of the public, etc.). It is basically Takeda's equivalent of a Google Account or an Apple ID.
The Takeda ID simplifies identity & access management for mobile apps or websites that are external-facing and require authentication. In the following we will call these mobile apps or websites "Business Applications".

Takeda has selected *Okta as the vendor for the Takeda ID infrastructure*. *Okta* is one of the best-in-class authentication services. It provides users with the opportunity to create and use a single username and password combination, for signing into any digital Takeda resource. There are two main aspects for the selection of *Okta's services:* First, we get a secure way to authenticate with Takeda's digital assets. Second, *Okta* is one of the most complete access management platforms on the market providing us with scalability, up-to-date security, and state of the art user experience.
In addition, a middleware supports the connection between your Business Application and Takeda's CRM system, which manages information about HCPs, to close the analog-digital loop for Takeda's business relationships.

The Takeda ID provides the following features for Business Applications participating:

- ✓ **Allows external stakeholders such as patients, Health Care Professionals (HCPs), nurses, caregivers and other users of Takeda's services to have a Single Sign-On (SSO) experience for many services**
- ✓ **Allows Takeda employees to authenticate with their Takeda credentials without the need of test accounts**
- ✓ **Digitally personalized and secure authentication**
- ✓ **Provides information whether the user is a confirmed HCP**
- ✓ **For HCP stakeholders there is out-of-the box integration with CRM**

1.1.1. The Benefits

External Stakeholders will only need to remember a single username and password combination. This will help to create a more streamlined, personalized, and relevant digital experience when digitally interacting with Takeda.
Internal Takeda will save time and resources by removing the need to create separate authentication service for every new digital resource.
Furthermore, it will help to manage our exposure to digital threats and strengthen adherence to Compliance and Data Privacy Standards (such as GDPR) across our online channels.

1.1.2. Why it is needed?

Takeda implements this authentication solution to keep up with the continuously increasing digitalization of the world:

In many business areas, it is nowadays standard to gain quick and easy access to the many provided online services. Whether we are booking a holiday, accessing entertainment, or doing online shopping, signing into our favorite sites quickly and easily is an important part of the overall experience.
The patients, HCPs, nurses, caregivers, and other users of Takeda's services are no different, especially when they use more than one of our digital services.

1.1.3. Who is the initiative's sponsor?

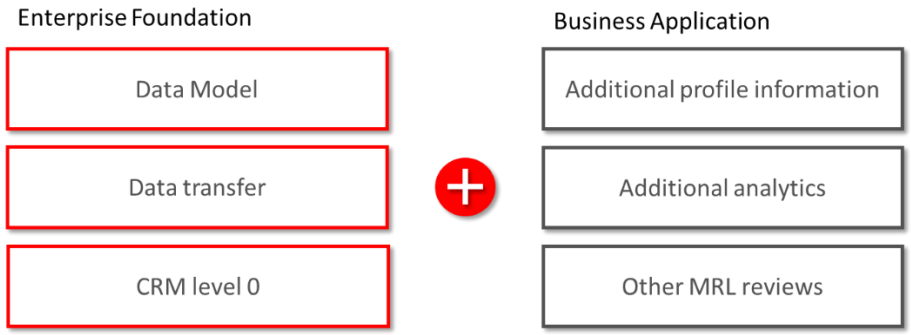
The Takeda ID initiative was initialized by Mike Towers (Chief Information Security Officers) to enhance the overall security to external-facing channels. It was built in cooperation with Commercial IT and the Data Privacy Office. The project team will continue to work on enhancements of the solution over the next month with all relevant stakeholders across the company.

1.1.4. What it is not?

This authentication service will not serve as a Master Data or Global Consent Management solution. The Takeda ID will only contain essential data required for the use of authentication such as username and password. Only a few additional attributes are collected to ensure an optimal default user experience, such as preferred communication language. Any further attributes that may be required in a Business Application (e.g. extended profile) must be stored & managed in the Business Application itself.

1.1.5. Does the Takeda ID comply with industry regulations?

The Takeda ID itself only provides identification and authentication of a user. This means Business Applications also receive the information of whether a user is a confirmed HCP. Therefore, the Takeda ID will help many Business Applications to stay compliant with the industry regulations, e.g., access to promotional websites in Europe. However, the Takeda ID will not change the accountability of the Business Application owner to complete the medical, regulatory, and legal reviews as usual.
The Takeda ID data model and the core data transfer were checked and approved by the Takeda data privacy officer and Takeda legal. All data is stored in European data centers.



*CRM Level 0 = identifies the existence of an active Takeda ID for an HCP in the CRM customer card

1.1.6. Outlook

The *Okta* Identity cloud solution is one of the most complete access management platforms on the market. The first implementation at Takeda currently enables users to sign-on using a self-defined username and password. Upcoming releases of the Takeda ID will enhance the features by enabling sign-in methods other than a password, e.g., via a fingerprint or face recognition. The so-called "social login" is also in planning. This means users will be able to sign into a Takeda service by using existing login information from a social network such as Facebook, their Google Account, or other trusted authentication sources (e.g., DocCheck or IMS OneKey account).
On top of the pure authentication, we are also working on the integration of Takeda ID into the global consent strategy – allowing all external stakeholders to manage consent for various channels in one place.
It is important to note that the Takeda ID is a forward-looking initiative and that there is currently no plan to force existing solutions with custom login solutions to retrofit their authentication process and use

Takeda ID. However, new initiatives with authentication requirements are asked to use the Takeda ID in their solutions (see 2.1).

1.2. The Takeda ID Guiding Principles

We have defined 6 Guiding Principles to summarize the Takeda ID. These are:

1. **The Takeda ID is Takeda's enterprise Identity & Access Management (I&AM) system for all external stakeholders**
   - ✓ External stakeholders can be patients, HCPs, caregivers, and other users of Takeda's services.
   - × It is not a Master Data Management solution.
   - × It is not a global consent management solution.
2. **Relevant Business Applications (= projects) can request to join the Takeda ID**
   - ✓ Every new Business Application with external stakeholder authentication should integrate.
   - × It is not planned to migrate existing solutions from other authentication providers.
3. **The Takeda ID provides authentication**
   - ✓ The Takeda ID contains the information about users being confirmed HCP
   - × "Authorization" of the user is covered by Business Application (i.e., even if a person has a valid Takeda-ID, it is up to the Business Application to verify whether this person is authorized to access the specific services or available content)
4. **The Takeda ID follows the principle of data minimization**
   - ✓ The Takeda ID only contains information required for authentication.
   - × Additional user information must be stored in the Business Application.
5. **The Takeda Digital provides flexibility to integrate as needed**
   - ✓ There will be a generic Takeda branded offering called "accounts.takeda.com".
   - ✓ Every Business Application will have the flexibility to use the accounts.takeda.com branding or integrate the Takeda-ID functionality directly and apply their own branding (skinning).
6. **The creation of a trusted/verified HCP account must be triggered by Takeda**
   - ✓ HCP = a person listed in the CRM
   - ✓ If a member of the public wants to self-register and claims to be an HCP, it will always and initially create a non-HCP account (can be changed later). We recommend for this scenario that the Business Application generates a "Lead" and pushes a request to Commercial Operations to "validate" **HCPs identity & HCP status**. Please note that this process needs to be handled locally and is essential for the integrity of the Takeda ID. For more information, please see the "Takeda ID for HCPs" Playbook on our Takeda ID SharePoint.

2. How to participate as owner of a Business Application

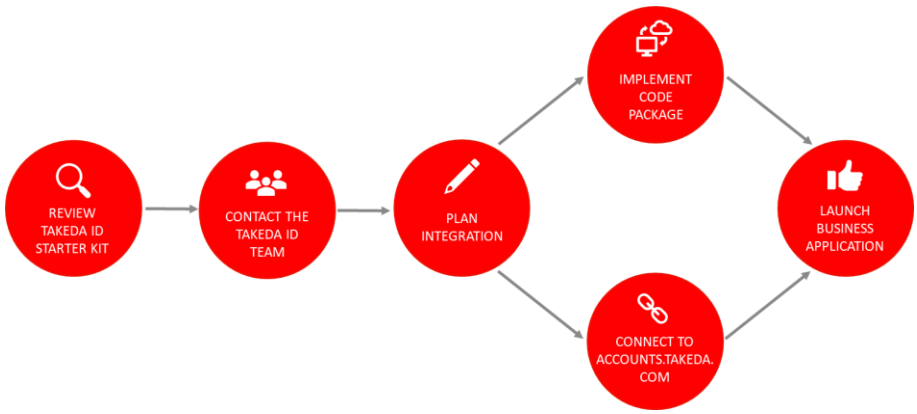
In this chapter you can find any information about the participation process for the use of the Takeda ID service. Information about service contacts, required prerequisites, and supporting material can be found here.

2.1. Who can/should participate?

The Takeda ID is a strategic initiative sponsored by the Corporate IT Security Officer and endorsed by the Digital Advisory Board. Therefore, all new initiatives that target external stakeholders and require authentication are strongly encouraged to use the Takeda ID as their authentication service.

2.2. How to get started

Integrating the Takeda ID into Business Applications is very simple and efficient. It follows the following 5 steps:



In order to get started, please review the Takeda ID Starter Kit. Once you have done so, please contact the Takeda ID team and present your Business Application via AskIT. The team will provide you with additional information and help you to plan the implementation.
There are two options during implementation of the Takeda ID. The first and preferred option is a direct interface between the Business Application and the Takeda ID APIs. The second is a link rerouting the login service to a Takeda-specific login site (accounts.takeda.com). Read more about this in section 2.3 “How to use ”.

2.2.1. Authentication process: What is covered by the Takeda ID and what by the Business Application?

External Identity & Access Management is more than just having a username and password. Currently, the full “Authentication Stack” can be divided into tasks referring to 13 topics. Usually, all these topics should be fully covered by the respective Business Application. With the implementation of the Takeda ID, the **Takeda ID will already take care of 9 of these topics** so that only the remaining **4 need to be covered in the Business Application**. The reduction of these tasks allows a faster and more effective development of Business Applications. The table below shows an overview of the full stack:

Authentication topics	Description/ Comment	Takeda-ID Foundation	Business Application
Infrastructure	Based on certified *Okta* Identity Cloud, APIs managed in MuleSoft	**X**	
Security	Protection against fraudulent "Account Take Over" and other external security threats. Eliminate blind spots by knowing exactly who has access to the Takeda digital ecosystem	**X**	
Regulatory compliance (e.g. GDPR)	*Okta* is classified as a data processor of the Takeda-Identity.	Foundation data-model & process, reviewed by Global DPO and Global legal	Specific use must be reviewed within the context of the Business Application.
Backend Integration	Integration with Takeda`s Digital Backbone architecture (e.g. CRM)	For CRM: Level 0	For CRM: Level 1 and 2
Multi-factor authentication	Enhance the security of your Business Application with contextual authentication using a broad set of second factors	Next release	The Business Application needs to create the UI to allow the user to enter their second factor.
Single Sign-on	Embed secure single sign-on for custom applications and provide access to the Takeda digital ecosystem	**X**	
Authentication	Improved login procedure to verify an account's identity and provide secure access to the Takeda digital ecosystem	**X**	
Authorization	Allowing access to specific data/ services in a specific business application		**X**
Account Life-cycle management	How to manage the account-life cycle	Activate/de-activate account (in line with Records Management & Regulatory requirements)	Business Applications might need to implement additional Records Management systems & Regulatory requirements
Centralized User-management	Centralized Access Management to the Takeda-Digital ecosystem	At the Takeda Digital-ecosystem level	At a Business Application level
Password recovery		**X**	
UX and Integration in a business application		Accounts.takeda.com offers a simple authentication experience	Customized skinning, UX requirements
Penetration Testing	Pro-active scanning for security vulnerabilities that expose Takeda & end-user	**X**	

2.2.2. Takeda ID – Starter Kit

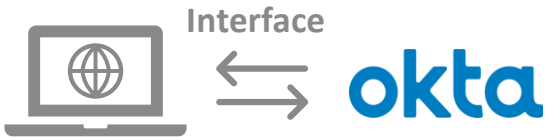
Integration of the Takeda ID is easy, and you can work with your development partner to do the integration. To aid the implementation of the Takeda ID, we have created a *Starter Kit* that provides every Business Application and their development partner with the tools and building blocks to implement the Takeda ID. The table below lists the content of the Starter Kit and the responsibilities/actions that need to be carried out by the Business Application.

Provided by Takeda ID ("Starter Kit")	**To be covered by Business Application**
Documentation and Functional specifications for the Takeda ID	Documentation of Business Application.
Standard Processes to Create, Authenticate, Update & Delete User	Authorization of user in the Business Application.
Takeda Branded Login Portal (accounts.takeda.com)	Integrate connection to Takeda Branded Login Portal (optional).
Code Packages to integrate with the Takeda ID	Integration of the Code Package in the Business Application (optional).
Takeda ID "Snippets" for T&C, Privacy & Cookie Policy	Can use the Takeda ID "Snippets" but needs to provide their own specific T&C, Privacy & Cookie Policy for Business Application.

2.3. How to use Takeda ID for authentication

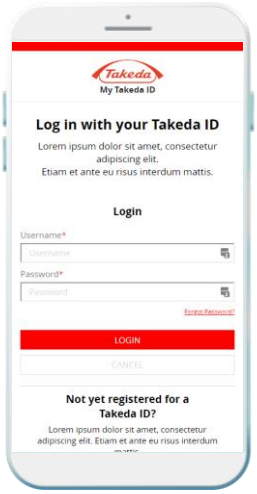
Once the Takeda ID service is implemented in the Business Application, the standard authenticating process works as follows:

- ✓ **A user enters the login authentication credentials into the Business Application**
- ✓ **The Business Application calls the Takeda ID service via a standardized interface**
- ✓ **Your Business Application receives a successful authentication information via an access token**



2.3.1. Integration flexibility

The Takeda ID has been designed to allow flexible integration to best suit the application's individual requirements. There are two options possible:



Generic offering

The Business Application is connected to a Takeda-specific user authentication site. A ready-to-go login screen is available via the link "accounts.takeda.com", which opens in a new window and afterwards automatically returns the user to your Business Application.

Pro

Your Business Application does not have to call the Takeda ID interface or create any login or user management screens.

Con

The login experience in this case is not fully integrated to your Business Application. This means after clicking on "Login" the user will see a login screen which looks different.

Customized branding

The Business Application is connected directly to the Takeda ID interface and keeps its product-specific look and feel, while maintaining the security of using a single platform for identity.

Pro

The end user login experience has a completely integrated login and registration procedure. The Takeda ID service is just in the background while the look and feel of the Business Application will be maintained.

Con

A code package needs to be integrated into your Business Application to use the Takeda ID services.

2.3.2. Backend Integration - CRM

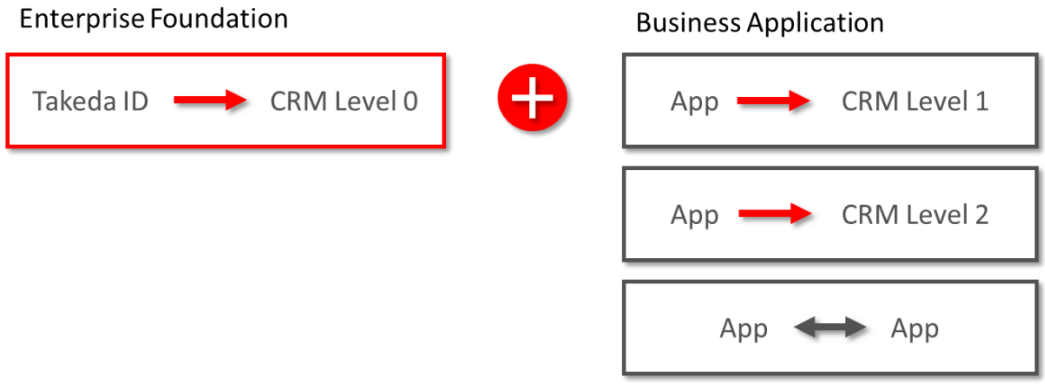
The Takeda ID service is linked to the CRM and saves in the data if an HCPs creates a Takeda ID. Thus, it can inform the Business Application whether a user is a verified HCP. We refer to this level of CRM integration as level 0 as it is the very basic integration. It is the default mode in the enterprise-wide foundation of the Takeda ID.

Further integration with CRM, for instance to report logins of HCPs to a business application (Level 1 of CRM integration) or particular actions within a Business Application (Level 2) are also possible via the Takeda ID but not part of the default in the enterprise-wide foundation. As these levels of integration are very specific to every Business Application and are dealing with personal data, they will only be added for Business Applications that require and justify the need for this information. Using level 1 or level 2, a Takeda Key Account Manager, MSL or Sales Rep can easily get additional information whether an HCP is using a digital service and if so, what an HCP is particularly interested in.

If the Business Application wants to use a deeper integration with CRM (level 1/2) it is the responsibility of the Business Application to ensure that all regulations, such as GDPR, are followed. This also means that the developers of the Business Application will need to define, which data they want to capture, how they want to use it, and how to deal with users that do not want to be tracked.

2.3.3. Additional Data Integration

The Takeda ID provides the opportunity to connect Takeda's digital assets. However, the Takeda ID service will not track any user across these assets. It will also not deliver a personalized user journey by itself because the usage of data between assets always needs to be justified in the context of a specific use case.



2.4. How long does it take to integrate the Takeda ID and what are the costs?

As described in the Authentication stack (see 2.2.1) the Takeda ID covers already many but not all authentication steps for the Identity & Access Management of external users. The remaining authentication steps as well as the integration of the Takeda ID into a Business Application need to be considered in the budget of the Business Application.

The effort and cost to integrate a Business Application into the Takeda ID service depends on the chosen integration approach (see 2.3.1) as well as on the Business Application itself. Usually, the work can be done in a few weeks. Please contact the Takeda ID team to get a better estimate for your Business Application.

In addition to the costs for the implementation, there can be fees for user licenses provided by *Okta*. A pool of available licenses is managed by the Takeda ID operations team. If the number of user licenses exceeds the pool of available licenses, the respective Business Application may need to provide funding for these additional licenses during the first year. After the first year the license costs will be taken over by the IT Security team and no further funding is needed going forward by the Business Application.

3. End User Management

The following chapter explains the flow of creating a basic user entry with Takeda ID services, the data that is stored in this entry, and how data can be updated.

3.1. What kind of user information is stored?

The following table lists all user attributes which are managed by the Takeda ID service.

Attribute	**Mandatory**	**Additional for HCP Users** (from CRM systems)	**Specifications**
Title			Dr. / Mr. / Mrs.
First Name	X		n/a
Last Name	X		n/a
Username	X		Must be in Email address format
Digital ID	X		Auto generated ID (hidden)
Country	X		Can be used to limit access
Language	X		Preferred language being used for communication
Password	X		Following the Takeda password policy
Customer ID*		X	Takeda Input (hidden)
CRM Country		X	Takeda Input(hidden)

*When Customer ID is populated, the user is automatically added to a group called HCP. This group information is returned in the ID Token provided as part of the authentication/authorization process.

3.2. How to get a Takeda ID

There are two possibilities to obtain a Takeda ID: Either via self-registration for instances asking for access while browsing the page/ Business Application, or via an invitation link provided by a trusted user. Depending on the chosen way, users can be registered in the Takeda ID as “member of the public” without any specific role or instantly as a verified HCP. The self-registration process allows only the creation of a “member of the public” account. To “upgrade” to an HCP account a verification step is required (For more information, please see the “Takeda ID for HCPs” Playbook on our Takeda ID SharePoint). This follows the Takeda ID design principles of trust in assuring HPC-accounts have been verified against CRM and ensures that the Takeda ID can be in a commercial context.

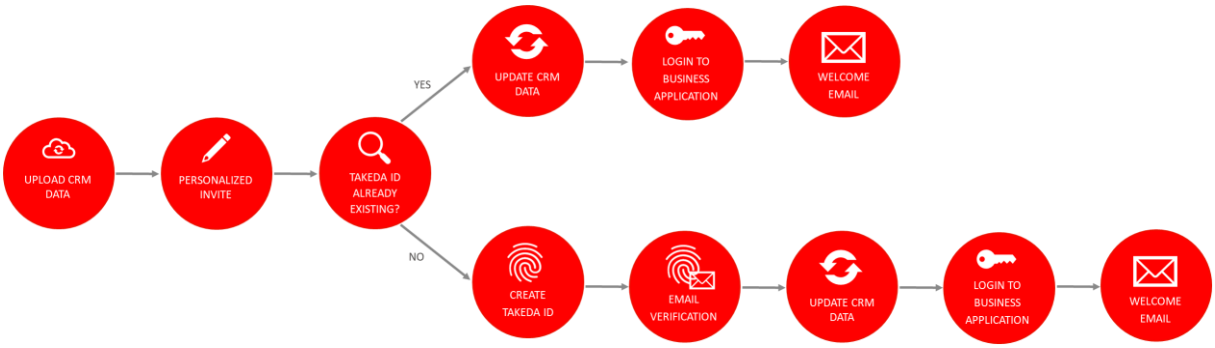
3.2.1. How to register a user

For a standard user (non-HCP) the following registration procedure shall be used.

Step No.	Description	Outcome
1a	A trusted user of the Business Application initiates an invitation, and the Business Application sends an automated email which includes either the following: ✓ link to the login screen ✓ link to download the app that can be used for login	Business Application displays a login screen.
1b	Without an invitation, a user can make a self-registration via browsing to the website or downloading the app.	
2	By clicking on "Create Takeda ID" the user is asked to enter a username, password, and give information about certain attributes. For a not fully embedded version, after clicking on "Create Takeda ID" the user is directed to the Takeda ID registration site, in which the user fills in the username, password and additional attributes (listed in chapter "3.1.3. What kind of user information are stored?")	The Takeda ID verifies whether the entered username already exists in *Okta*.
3a	If the username does not yet exist, a Takeda ID and a user profile will be created in *Okta*.	Takeda ID is added to user profile in Business Application.
3b	If the username already exists, i.e., a Takeda ID has already been created for that user, the user will be informed via a Takeda ID disclaimer.	User decides to create an ID using another username or to log into the system with existing account.
4	The Business Application sends an email to the user to validate the email address. This step is required as the new user needs to confirm that the email address is trusted. After completing the validation, the user can use the Takeda ID to authenticate.	User logs into Business Application the first time.
5	The user completes its profile, if the Business Application requires any additional data that is not part of the Takeda ID profile.	The user receives a welcome email.

3.2.2. How to register an HCP-User

For an HCP the registration process is very similar to the normal user. The main difference is the verification of the HCP status, hence there must be an invite from a trusted user to start the registration process or the update process of an existing ID. The specific steps are as follows:



Step No.	Description	Outcome
1	To invite an HCP, the relevant HCP data (CRM Country, Customer ID) from the Takeda CRM systems needs to be uploaded to the Business Application.	Takeda ID verifies whether the entered username already exists in *Okta*.
2	The Business Application sends out a personalized invitation to the HCP User. The invitation is adapted to the HCP user registration status. ✓ link to the login screen ✓ link to download the app that can be used for login	User logs into Business Application.
3a	If the HCP user has not yet created a Takeda ID, the "Takeda ID creation" screen will be displayed. For a not fully embedded version, after clicking on "Create Takeda ID" the user is directed to the Takeda ID registration site, in which the user fills in the username, password and additional attributes (listed in chapter "3.1.3.What kind of user information are stored?")	The Takeda ID verifies whether the entered username already exists in *Okta*.
3b	If the username already exists, i.e., a Takeda ID has already been created for that user, the user will be informed via a Takeda ID disclaimer.	User decides to create an ID using another username or to log into the system with existing account.
4a	A Takeda ID and a user profile will be created in *Okta*.	Digital ID is added to user profile in Business Application.
5a	The Takeda ID is saved in the CRM system.	Digital ID mapped to the CRM ID.

4b	After invitation link the username is already existing and linked to a non-HCP account: the user decides to login with the existing Takeda ID.	Update of Non-HCP to HCP account and saving of Digital ID in the CRM system.

3.2.3. What happens if an HCP user wants to do self-registration?

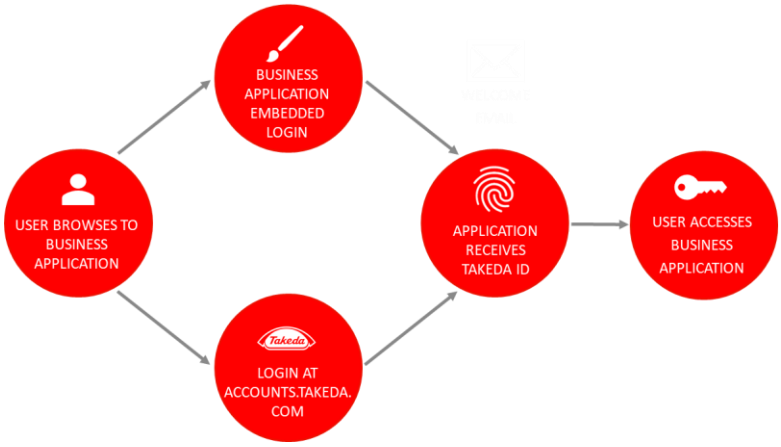
Self-registration of a verified HCP is not possible. If a member of the public wants to self-register and claims to be an HCP (usually via checkbox "I am an HCP" during the registration process for your Business Application), it will always and initially create a non-HCP account (can be changed later). For this scenario we recommend that the business application generates a "Lead" in the lead verification tool (see Chapter 4) and pushes a request to Commercial Operations to "validate" **HCPs identity & HCP status**. By "Lead" we mean that the local Commercial Operations Team should be involved for the following reasons:

1. You might want to know that an HCP is interested in Takeda Services to follow up with him/her.
2. You need to verify the HCP status.
3. You need to verify the identity of the HCP registering for your Business Application.

Only after the CRM connection is done and updated, the Takeda ID will identify the user as an HCP. Please note that this process needs to be handled locally (e.g., with a team of data steward(s) validating the leads) and is essential for the integrity of the Takeda ID. (For more information, please see the "Takeda ID for HCPs" Playbook on our Takeda ID SharePoint).

3.3. Login with the Takeda ID

Login with the Takeda ID is very simple. The login form contains only the username and a password. Depending on the chosen implementation in the Business Application, the user can either login directly via an embedded form or the user will be redirected to accounts.takeda.com where the login form is displayed. The result is the same in both: The user is authenticated to all Business Applications connected to the Takeda ID, meaning a user can switch seamlessly between services that use the Takeda ID and all these services know exactly which user is visiting the Business Application.



Step No.	Description	Outcome
1	A user browses to a Business Application to log in.	The Business Application either redirects to or opens an embedded login from accounts.takeda.com
2	User types in the Takeda ID username and password in the respective login form and click on “login”.	The login credentials are sent to the Takeda ID service for authentication and the outcome is sent back to the business application.
3	The business application receives the access token (incl. the Takeda ID profile information).	User is identified (incl. HCP yes/no)
4	The user can browse services and content based on the authorization set in the Business Application.	User is authenticated to all Business Applications that use the Takeda ID.

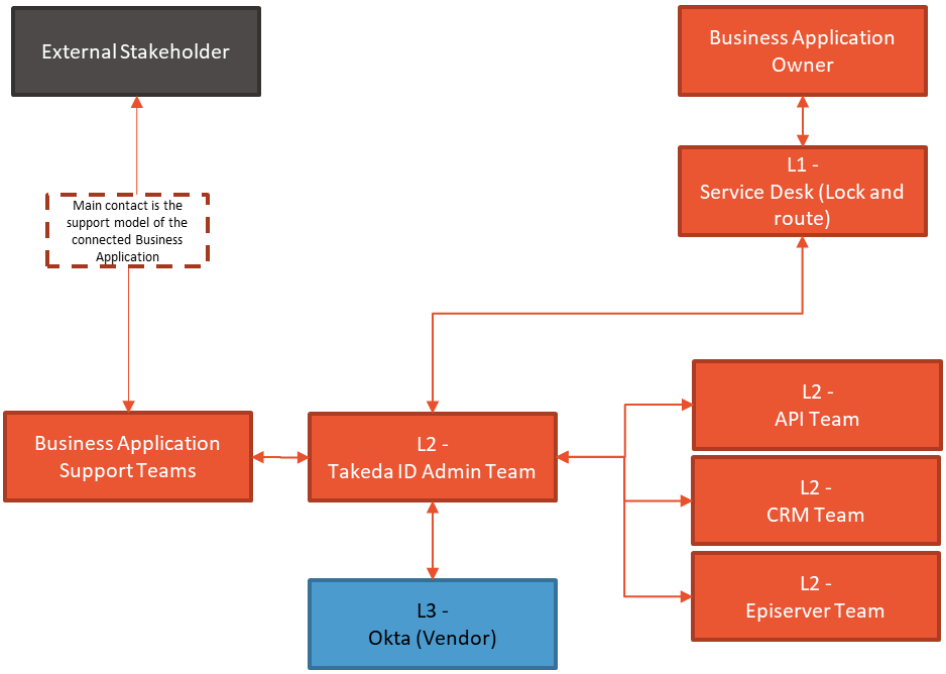
3.4. Access and Change management of a user profile

The Takeda ID provides the following functionalities to manage a user profile. Certain tasks must be managed by Takeda support whereas others can be accessed by an authenticated user or Takeda support.

Feature	Managed by User	Managed by Takeda
Change of shared user attributes	X	
Change of password	X	
Forgot password	X	
Delete User's Takeda ID		X
Review HCP status		X

3.5. Takeda ID Support Model

Please note, Takeda ID does not have an external-facing service desk solution and external users do not have direct access to Takeda Support AskIT, therefore first-level-support needs to be covered by the Business Application (e.g., user faces problems during registration etc.). In case of any issues that cannot be resolved by the Business Application Support Team, please submit a ticket via AskIT.



4. Supporting Tools

4.1. Takeda ID Lead Verification Tool

If automatic verification of the leads will not be possible due to various reasons, they must be validated manually. The lead verification tool will help you with this. This tool lists all leads that are pending verification. The lead verification tool is connected to the CRM and the leads to be verified can be compared with the references in the CRM. In addition, verification/confirmation emails can be sent to the leads. For more information on the tool and the process involved, please contact the Takeda ID team.

5. Glossary

Term	Description
Access Token	Contains the security credentials for a login session and identifies the user
Authentication	The act of proving an assertion, such as the identity of a computer system user
Authorization	The function of specifying access rights/privileges
Business Application	Project that wants to join the Takeda ID
HCP	Healthcare Professional
Okta	Cloud software that helps companies manage and secure user authentication into modern applications