UBISECURE®

Connecting Identity.
Transforming Digital Business.

Migrating your organisation's IAM system

Everything you need to know about seamlessly replacing Identity and Access Management capability in apps and services

UBISECURE®

Contents

When to migrate your IAM system

Many scenarios call for a migration from one identity and access management (IAM) system to another. But how do you know when it's time to move on?

Let's look at 8 common examples of when migration is required and the drivers behind them:

— EXAMPLE 1: YOUR IN-HOUSE DEVELOPED SOLUTION HAS BECOME UNMANAGEABLE…

…and is taking too many developer and support resources from the core business.

Many companies fall victim to developing and maintaining in-house tools, consuming untold expert resources that could be working on truly unique core business logic that differentiates your products and services from that of competitors.

Companies that recognise this issue should look for modern developer-friendly tools and components, that do all the heavy lifting and provide clear API integration points to local business processes. This moves projects forward faster, gets services to market quicker and frees up developers to add true value to your business.

TIP: Find out more about building IAM capability in-house versus buying from an IAM provider in our white paper: Build vs Buy: IAM.

— EXAMPLE 2: YOUR LEGACY SYSTEM HAS PERFORMANCE, USABILITY OR SCALABILITY ISSUES

As organisations grow - and the user accounts, roles and attributes grow with them - they may find that their once-adequate IAM system no longer performs at scale. Slower logins, painful management or simply hitting system limits may force a company to seek a replacement.

— EXAMPLE 3: YOU WANT TO SIMPLIFY ENVIRONMENTS

Complexity has a cost. Simplifying an enterprise architecture across an organisation and consolidating services can reduce costs on multiple levels: risk of failure and licencing costs can both be reduced. A highly siloed organisation may have multiple services performing the same functions in different business units that could be combined into an organisation-wide platform with a new IAM system.

— EXAMPLE 4: YOUR COSTS FOR LICENSING MODELS, HOSTING AND MAINTENANCE ARE TOO HIGH

Cost models that once seemed attractive may, quite suddenly, become unattractive or even unsustainable. Changes in policy or business models may cause product vendors or hosting services to adjust or renegotiate contracts. Or changes in your own organisation – such as expansion into new regions, or a large increase or decrease in user or transaction volume – may suddenly swing the cost structure in such a way that the company must find an alternative.

Maintenance costs of legacy systems can grow as the pool of specialists shrinks and talent moves to newer technologies. In the worst-case scenario, inability to find or attract staff to maintain and develop systems can lead to the risk of a critical business function becoming unsupportable.

— EXAMPLE 5: YOU NEED TO MAINTAIN A STANDARD OPERATING ENVIRONMENT DURING A MERGER OR ACQUISITION

When two companies combine, identity management can be an efficient way to rapidly combine the services of two organisations. This allows customers of the acquiring company to use their current credentials and accounts to access the services of the acquired company, and vice versa. However, over time, maintaining two separate systems can become a burden – especially as rebranding of one of the services occurs, causing confusion over which account is which.

Like other IT infrastructure, a desire to standardise the operating environment between both companies may involve migration of all users from one system to

the other. In some cases, it may be an opportunity to migrate away from both platforms to a new, better solution.

— EXAMPLE 6: YOU NEED BETTER SECURITY AND COMPLIANCE FROM YOUR IAM SYSTEM

As laws tighten across industries, existing IAM solutions may no longer adequately meet new requirements. We have seen this over the years with examples such as SOX, HIPAA, regional data protection regulations, financial services directives - and more recently, GDPR and PSD2.

Such standards demand tighter data management, audit trails, encryption throughout data lifecycles, specific identity proofing and authentication requirements. Other examples are accessibility requirements or laws requiring personal user data to be stored only in - or always replicated to - the home jurisdiction of the user.

— EXAMPLE 7: YOUR CURRENT SOLUTION DOESN'T OFFER CERTAIN SOFTWARE FEATURES

A system that once looked shiny and new may lose its shine if it doesn't keep up with the latest integration methods and authentication capabilities. It may become costly, or even impossible, to integrate with more modern applications or new cloud services. It may also become incompatible with the way your team deploys environments, using techniques that were used as recently as a few years ago.

— EXAMPLE 8: YOUR LEGACY SYSTEM HAS BECOME END-OF-LIFE AND IS NO LONGER SUPPORTED BY THE VENDOR

Sometimes, for commercial reasons, the software that is at the heart of your identity system becomes end-of-life and the vendor announces that support is ending as they change their own focus through restructure, merger or acquisition. Running non-supported software is an unacceptable business risk. In this case, it is important for business continuity to find a replacement solution – often preferably one that can be replaced with the least disruption possible.

Why migrate your IAM system

Throughout the examples above, there are common motives for migrating an IAM system, including:

- **Security** – ensuring user data, projects and tools remain protected by using proven best practices.
- **Compliance** – meeting requirements from industry regulators.
- **Usability** – keeping up to date with current user expectations and enabling modern technical integrations.
- **Cost** – often in the form of reducing work effort in maintaining legacy systems. Sometimes in the form of reducing hosting and licensing costs by seeking modern and optimised solutions.
- **Architecture** – simplifying technical deployment models, enabling architectures like microservice-based designed, hybrid-cloud or multi-cloud deployments.
- **Performance** – an organisation may have outgrown a solution that was never designed for the scale of users, organisations, roles or attributes that the business now has.

Migration methods

There are multiple ways to handle a migration project. What the best option is for your company depends on your business requirements but, roughly speaking, there are two main strategies: big bang migration and trickle migration. Let's run through the two approaches.

BIG BANG MIGRATION

In big bang migration, a.k.a. 'rip & replace', the main idea is to extract data from the legacy system, import it into a new one and reconfigure all related applications for all users in one go.

This means that you switch all of the system's identities to a new system during a certain maintenance window, which is usually when there is a minimal traffic flow to your applications, e.g. overnight. In many cases, after the change is done, users won't even notice the difference. If the new IAM system is API-based then the user interfaces will not need to change – functionality is simply integrated to the existing application. If the new system is not API-based, users might have to deal with new front-end screens and operating procedures, etc.

Big bang migration simplifies the planning of the project schedule, since you can do the actual data import execution of the project inside a relatively small, predefined time window.

TRICKLE MIGRATION

Trickle migration - a.k.a. 'phased migration', 'synchronised migration' or 'iterative migration' - involves running the two systems (old and new) in parallel, migrating target applications one at a time and decommissioning the old system gradually, until everything is running via the new IAM system.

This method offers a phased approach, which gives you time to monitor a successful execution of the step by step migration process, while the services are still partly relying on the old system and running simultaneously with the new one.

Choosing a method

With sufficient planning, either method will ensure success for your IAM system migration. Yet it's important to be aware of the risks of poor planning with each method, so these can be mitigated against.

Big bang migration, due to its short time window for changeover, could be stressful if something goes wrong during that time window. In comparison, trickle migration offers a smaller comparable risk by implementing at individual stages, particularly if there is a huge amount of data to be imported.

On the other hand, trickle migration can be more complicated to plan and execute since there can be several distinct components affecting the migration, meaning the project's timeframe has more potential to overrun. Also, you have to think carefully about the synchronisation between the old and the new systems which are in operation at the same time. Therefore, a lot of companies prefer the big bang method for IAM system migration at least at the application level. This means that one or a few applications would be migrated all together in the first phase. Then, later, the other applications can be migrated.

See below for how to mitigate against risk with either method.

UBISECURE®

User migration top tips

Careful planning ensures on-schedule success and minimises service downtime. In order to guarantee a successful execution of your project, consider the following steps.

- Make sure you have a **fresh back up of the data** before starting the execution phase, and that you test that the backups are functional before proceeding.

- **Transfer existing customer credentials where possible.** The chances are that you can import most of the user attributes from the legacy system to the new IAM system. However, there might be some attributes that are more challenging to transfer, such as passwords or SSNs (Social Security Numbers). This type of sensitive information is often saved in a hash format. This is not a problem if your new IAM solution supports the same cryptographic hash algorithms as the old one.

- Allow **parallel logins** during a migration period (if required). If you choose to use the trickle migration method, make sure that the old system is running and is accessible at the same time as the new one. You can conduct the import in several steps that can be phased in many ways, such as by user group, business unit, customer group, region, use case, a target application, etc.

- Always **transfer existing customer account links** where possible. Sometimes your system has a link to log in via another trusted party's service, such as a social account login or third-party persistent IDs. Another case is where, during login, another service returns one or more attributes to match the account of a local user. You should preserve these links to the new service during the migration project. (more on account linking later)

- **Thorough testing and audit of access control logic.** Both pre-testing and post-testing are essential parts of migration projects. Typically, an enterprise has a test IAM environment in addition to a production environment. Establish the test environment before the production environment and utilise it in the pre-testing stage by migrating the system to it. It is also important to test the environment after (and possibly during) the migration to see that everything is working as planned. Once the test environment is functioning you can start to migrate the production environment.

Data import

Importing the user data from your legacy system to a new one is a crucial part of the migration project. Here, the migration strategy plays a big role: should you get everything imported in one go (big bang migration) or should you run both systems simultaneously and move the data in phases (trickle migration). Here are some options you can choose from.

ONE-OFF IMPORT

In the case of big bang migration, you can use a one-off import method. A good option is to use an import tool if it is provided by your IAM provider. A ready-made tool makes the process much easier and faster. If such a tool is not available, you could create a script that utilises the APIs of the new IAM system to import the data. In both cases, everything is imported in one go.

If the passwords (and possibly other attributes) are not stored in a plain text format, find out if the new IAM system supports the same hash algorithms as the old one. If this is not the case, then you cannot do a one-off data import.

PHASED IMPORT

If you can't do a one-off import, a simple solution is to ask users to re-register their accounts to the new system. If the new IAM system facilitates it, you could send users an email invitation to a re-registration form in the application itself, importing the existing data via APIs where possible. In many cases, some of the identity attribute fields can be refilled (e.g. when the invitation is initiated from a CRM system). Thus, the user just verifies that everything is correct, accepts the terms of use and defines a new password. This is then saved to the new IAM system in a hash format.

A challenge may arise if you cannot accept re-registration, or even a password reset, as part of the new system's introduction process. 'On the fly migration' allows a secure rehashing of existing customer passwords, even if the password data is unavailable in the new IAM system. You can import all the plain text attributes to the new system and, when a user signs into it for the first time, their password validity will be checked against the user directory of the old backend service. If it is correct, the new IAM system rehashes and saves the password. On the fly migration allows a smooth registration during the login process that is transparent to the end user.

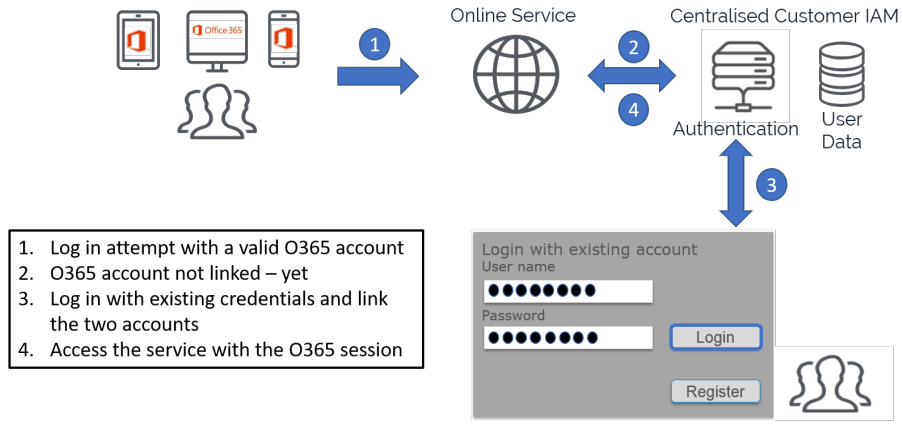
Account linking

When transferring information from the old IAM system to the new one, you should preserve account links wherever possible. Use the tools provided by your new IAM solution to facilitate the process. Let's take a look at what this involves.

USER-DRIVEN FEDERATION

The basic idea of user-driven federation is to let the end user link existing third-party system credentials to your online service. This allows users to use an authentication method they already own, instead of the traditional new username and password combination. The concept is called BYOI (Bring Your Own Identity).

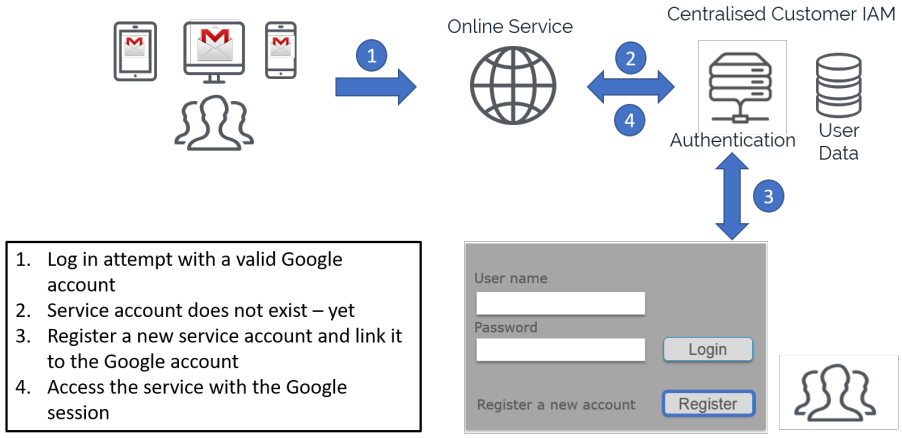
You could link, for example, social accounts such as Facebook, Google, LinkedIn, Twitter, etc. or business accounts such as Office 365. If necessary, the linking can be verified by using a strong authentication method, like a bank ID, to get a verified social identity. From the user perspective, it is a manual linking of two authentication methods provided by different sources that do not even need to have common trusted attributes. You can do the account linking either by first signing in using the existing account or by registering a new account while signed into an existing third-party account.



A simplified presentation of sign in with User-Driven Federation

In the first example, the user already has an account for a given online service and would like to link their Office 365 business account to it for smoother logins. To begin the linking they have to first visit the online service, choose O365 as an authentication method and sign in to it. Next, the user has to further sign in with the original online service credentials, after which they can set up the link between the accounts.

Next time, the user can sign in to the online service using the O365 credentials and even utilise features such as **SSO** (Single Sign-On) which allows them to step into the service without a separate login if they are already signed in to their business account.

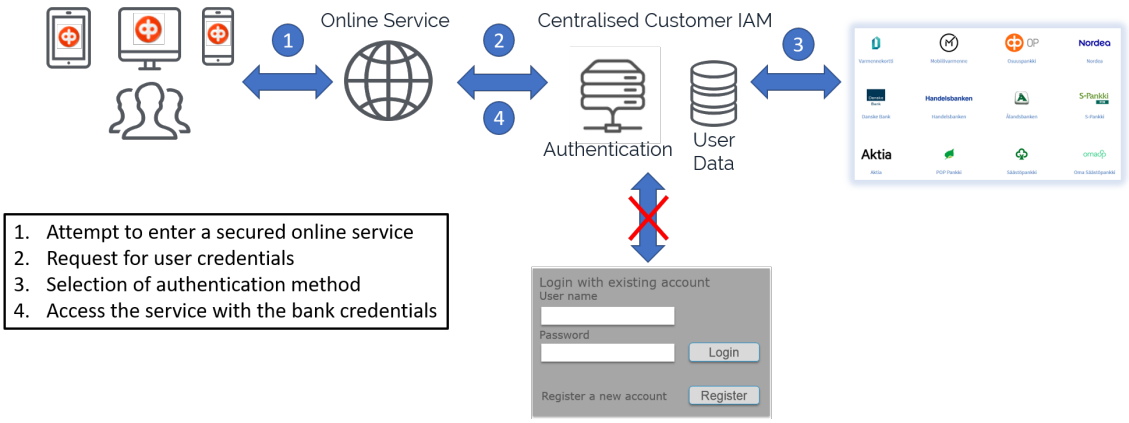


A simplified presentation of account registration with User-Driven Federation

The second option allows you to register a new account utilising your existing third-party account. In an example case a user, who is logged in to their Gmail account, enters the target service for the first time. They choose to create a new account and will get a partly pre-filled registration form with their name and email attributes automatically fetched from the Google service. After the user has finalised registration, they are able to single sign-on to the target system from the internet utilising their Google account.

DIRECTORY USER MAPPING

Directory User Mapping is quite similar to User-Driven Federation. It offers an automatic account linking based on a lookup to a third party user repository. The user can sign in to a service using their existing credentials for a different service such as Bank ID, Mobile Certificate (Mobiilivarmenne in Finnish) or using an identity card. Another common example is to use third party AD's (Active Directory) attributes to find a user's account from an online service's repository (Centralised **Customer IAM** in the picture below). During login, one or more known trusted attributes are returned from the third party service and are used to search and match the account of the local user. As a result of the successful mapping, your IAM solution can create an identity to access an online service in a single sign-on session.



A simplified presentation of sign in with Directory User Mapping.

In this third example image a user already has a registered account, thus their identity attributes are stored in the Customer IAM user repository. The online service requires that a unique attribute(s), such as SSN (Social Security Number), is used for identity verification and the attribute has to be fetched from a trusted source such as bank, telecoms operator or national population registry services. First, the user chooses an authentication source, their bank for example, from the list of authentication methods from which the IAM system receives the SSN attribute and checks it against its own data repository to find the user's attributes. From the user point of view, this is just like a typical strong authentication sign-in process. There is no need to first sign in using the original credentials.

Final tips

An IAM system migration is a relatively big project that potentially introduces a lot of new things to users. Some users can be resistant to big changes, so it is a good idea to communicate in advance that users should expect a system update on given dates. Focus on the positive side and possibilities that the new solution provides. Here are some tips and tricks on how to make the introduction of the new solution frictionless.

- **Think of it as a data cleansing.**

  This is a good time to re-validate and re-verify user attributes to maintain data quality. You could even use an incremental approach where you ask the users to, for example, check and update one attribute per week such as " Are you still at 12 High Street? Yes/No -> if not correct" or "Is your phone number +3585827756? Yes/No -> if not correct".

- **Re-attestation of user rights.**

  An IAM migration project is the perfect time for re-approval of access to services. It is important that the right persons have access to the right areas of your services. A situation where the job role of an existing user has changed, or they have left the company, often requires modifications in the access credential configurations. Here, a delegated user management facility can considerably help the task - where the customer or partner organisation's main user manages the access rights and authorisations of company employees. There are several benefits in this approach such as increased data accuracy, decreased security risks of abandoned accounts and credential sharing, and reduced operational costs for your enterprise. Find out more about Delegated Authority here.

- **Increase security and compliance with regulations.**

  There are many business-driven factors to purchase a new IAM system, such as increased security and help complying with regulations. You get better hashing and encryption algorithms for passwords and other sensitive information and you can choose from the latest and best authentication methods. Self-service portals let users view and manage their own account information which is necessary for compliance with regulations such as GDPR and saves organisations considerable amounts of time (and therefore money).

- **Add usability and convenience.**

  As mentioned before, users can be resistant to big changes. To soften the introduction of the new system, increase usability and convenience. This can be achieved, for example, by planning easy-to-use workflows provided by the new IAM system and using login with an email address instead of user ID or log in with (verified) social identities. If you choose to use trickle migration, where both the old and new systems run in parallel for a while, then consider keeping the old branding during parallel use and update the visual brand later on.

- **Maintain all things that impact browser heuristics on form fillings.**

  This includes hostnames, field names, page elements etc. Use any existing browser cookies for discovery where possible.

- **Encourage and entice users to use the new service.**

  Send user invitations such as "We would like to introduce you to our

enhanced and easy to use service. You can now assign a new convenient authentication method for your account". To further entice the users, you could arrange small competitions and incentives. Getting users to use the new system is especially important if you were not able to migrate all the attributes to the new system e.g. due to the incompatible hashing algorithms. In such a case, these attributes need to be re-created (See the next bullet).

- **Allow parallel logins via old UI in the case of "on the fly migration".** One form of trickle migration is called 'on the fly migration' (as described earlier). In this phased migration method, you retain the old login for long enough that most users would log in to the new system. The idea is to check user ID/password combination against the old backend service and, if it is correct, save it in the new IAM system. The password is rehashed with a new hashing algorithm and the old account is marked as migrated. You might not have time to wait for everyone to have logged in to the new system due to the licensing costs of the old system. In that case, the remaining users might need to re-register or at least reset their old passwords.

Conclusion

As business IT systems keep progressing with digitalisation and innovation, migration projects are a necessity. Software must cover more ground and requirements are changing frequently; data needs to be consolidated and lots of services are moving to the cloud. This is also true of IAM solutions, so make sure you select one that satisfies your business needs and is flexible enough to progress with your organisation.

Ubisecure **Identity Platform** offers a scalable and easy-to-integrate omnichannel platform for your enterprise's services whether you are looking for an on-premise solution or a cloud implementation, including the option for a quick-start deployment with **Identity-as-a-Service (IDaaS)**.

Ubisecure has tools and processes in place to simplify your migration to our Identity Platform - with minimal business interruption. Get in touch at **www.ubisecure.com/contact** and book a time with our experts to discuss your individual situation and plan your IAM migration.

About Ubisecure

Ubisecure provides feature rich customer identity management software and services to help companies reduce identity data breach risk, improve operational efficiencies, and improve user experience.

The company provides a powerful Identity Platform, deployed as IDaaS, Cloud, or on-premise software. The platform consists of productised Customer Identity & Access Management (CIAM) middleware and API tooling to enable single digital identity benefits across multiple applications. Capabilities include enabling complex authorisation and delegation workflows, single sign-on (SSO), frictionless multi-factor authentication (MFA), user identity management, and pre-established connections to dozens of third-party identity providers (social, mobile, and verified).

Ubisecure's Right to Represent is a representation governance solution offering a fast and easy way to assert and verify an individual's mandated rights to electronically represent their company, including financial, signatory, or other authority. Ubisecure's widely used Delegated Authority solution allows individuals and organisations to manage which users and organisations can act on their behalf to dramatically reduce costly, time consuming and delay-prone manual workflows.

Ubisecure is accredited by the GLEIF to issue Legal Entity Identifiers (LEI) under its RapidLEI brand. RapidLEI is a cloud-based service that automates the issuance and registration of these highly assured organisation identifiers.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com

UBISECURE UK
The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK
UK: +44 1273 957 613

UBISECURE FINLAND
Vaisalantie 2
FI- Espoo, 02130
Finland
FI: +358 9 251 77250

UBISECURE SWEDEN
Blekholmstorget 30 F
111 64 Stockholm
Sweden
SE: +46 70 603 34 83

UBISECURE DACH
Franz-Joseph-Str. 11
80801 Munich
Germany
DE: +49 89 20190980