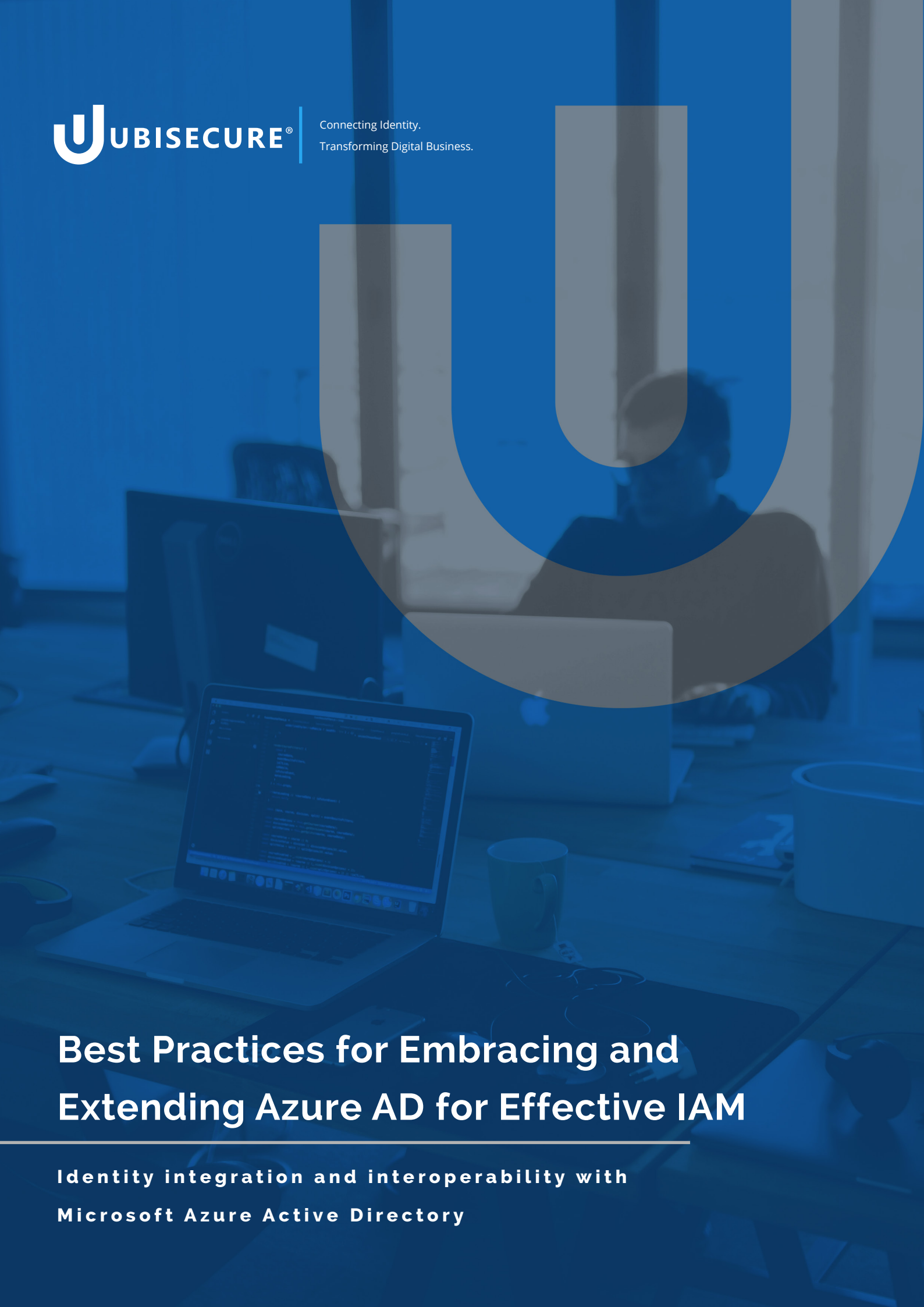
UBISECURE®

Connecting Identity.
Transforming Digital Business.



Best Practices for Embracing and Extending Azure AD for Effective IAM

Identity integration and interoperability with Microsoft Azure Active Directory

Internal vs external IAM

In the past, industry analysts kept emphasising how the 2020s would be the "decade of data", and compared data to oil, the "black gold" of the late 20th century. It is easy to agree with that claim, as the megatrend of digitalisation is taking ever larger strides forward, fuelled by the rapid change in how we work and consume after the start of the COVID-19 pandemic.

If data is the new oil, digital identities must be gold nuggets. Where to store and process digital identities carries profound choices to any growing organisation, and just like with any other valuable asset, matters should never be left to random chance.

Many organisations mix internal (employee) and external (customer, partner, citizen, remote worker) identities together. While having a single, unified identity repository is the correct choice for many situations, sometimes it is clearly better to keep internal and external users separate.

— DOWNLOAD THE DIFFERENCE BETWEEN INTERNAL IAM AND CUSTOMER IAM

Internal users are typically much lower in number than external users, but require much more fine-grained access permissions and access to many more integrated systems. In addition, internal users can be trained on the nuances of internal systems and are willing to tolerate longer delays in their workflow than external users.

Another major difference is in the authentication methods themselves. Typically, internal user identities are created and managed by the organisation's HR/IT departments, while it's much more user friendly to let external users re-use their existing identities, be it via social media providers, platform providers like Google and Apple, or strong digital identity providers like banks and telecoms.

Unlike competing solutions, Ubisecure Identity Platform does not impose any artificial limits – neither technical nor pricing – on the underlying type of users (internal vs external), or the way they authenticate themselves. This is a conscious decision. As an independent, dedicated IAM platform vendor, Ubisecure is able to remain agnostic in our support for third-party platform integrations. In this white paper, we discuss best practices for integrating Ubisecure with Azure AD, enabling you to avoid tie-in with the full Microsoft

Why standards compliance matters

identity stack.

Related to this platform neutrality is the importance of standards compliance. Platform-specific solutions (vendors who own both the cloud platform and the IAM solution running on it) tend to be point solutions, built quickly to band aid a specific departmental need, without looking at the larger picture or challenges. On the other hand, platform-neutral solutions (focused IAM providers like Ubisecure) fulfil a complete end-to-end need with seamless interoperability, often resulting in lower TCO (total cost of ownership).

> Interoperability is made possible by the implementation of standards

As the world keeps getting smaller and more networked, the resulting complexity can only be managed efficiently by increasing levels of automation. To enhance automation, interoperability enables a system or a product to work with other systems or products, without any special effort on the part of the end user (a customer or a partner - or both). Interoperability is made possible by the implementation of standards. As Ubisecure is OpenID Connect Basic certified by the OpenID Foundation, utilising Azure AD as an identity provider is straightforward. In addition, a later section in this white paper explores integration with plain OAuth 2.0 and its limitations.

Azure AD, Azure AD B2B, Azure AD B2C…what's the difference?

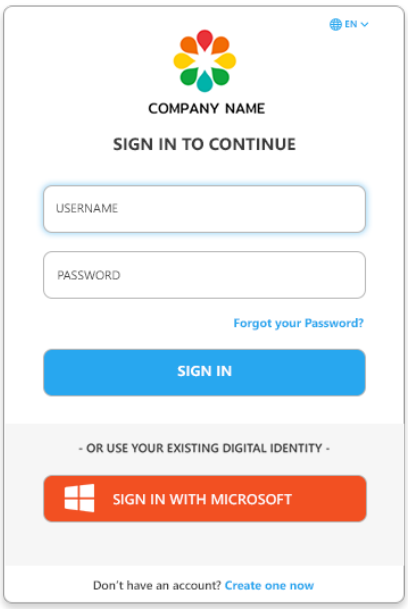
Microsoft's Azure Active Directory, or Azure AD for short, is a cloud-based directory service. Its primary purpose is to provide identity storage and an authorisation service for cloud applications. Two well-known applications relying on Azure AD are Microsoft's own Azure cloud platform and Office 365.
Azure AD B2B and B2C are additional services built on top of Azure AD. Unlocking all of their features requires a premium Azure AD subscription.

AZURE AD B2B

Azure AD B2B is built for cross-organisation collaboration. It seeks to address issues in matching different security policies, credential types and, of course, the user accounts themselves that exist between two organisations. Utilising Azure AD B2B, there is no need to create a new user account and set up new credentials when inviting a user to your application or when sharing a document with them. They sign into your app with their own (home organisation) credentials. However, you will be able to set the security policy and, for example, require multi-factor authentication.

In more technical terms, Azure AD B2B grants application access to users from another Azure AD tenant. This also highlights one of the major limitations – the

— FIND OUT MORE ABOUT HOW UBISECURE ENABLES ADVANCED DELEGATION CAPABILITIES



users already need to have accounts in Azure AD or have a Microsoft ID. The blurring of the lines between internal and external users – for example mixing remote worker and customer identities together - presents a potential security issue: unless the permissions are carefully audited, invited users can often have wider permissions than intended. For example, just seeing the names of documents and folders can reveal a lot, even if the files themselves cannot be viewed or downloaded. Another limitation is that while users can be invited, organisations cannot. With the Ubisecure Identity Platform, a whole or a subset of an organisation can be invited to the system by delegating one or more users as "main" (admin) users. Those main users can then independently invite and manage other users from their organisation (within defined parameters). This saves your team time and costs, allowing organisations to manage their own users - who, after all, know them best.

AZURE AD B2C

Azure AD B2C, on the other hand, is built to allow anyone to sign up as an application user with their email address as an identifier, or an existing digital identity from, for example, a social media provider. In a nutshell, Azure AD B2C is a cloud identity repository with several options for self-registration. However, some of the limitations of Azure AD B2C include: having no provisioning without writing a custom tool against the AAD Graph API; and no way to log into Office 365 with a social media identity. In addition, the users must finish the registration process in one go, or start again from the beginning.

Integrating with Azure AD

The Ubisecure Identity Platform can both use Azure AD as the Identity Provider (IdP), or act as the IdP itself.

With Azure AD as the IdP, the Ubisecure Identity Platform extends Azure AD by providing several strong authentication methods and wide protocol translation abilities for integrated systems, and the possibility to present different workflows for different identities.

When the Ubisecure Identity Platform is used as an IdP, it acts as a central hub for managing digital identities, offering a standards-compliant, neutral and performant repository to store identities and individual attributes across the organisation. It can integrate with Azure AD, AWS, Google, or a smaller cloud provider – or even a service or cloud provider that doesn't exist yet. Ubisecure

Identity Platform has been platform-agnostic since its beginnings almost two decades ago.

With Azure AD and the Ubisecure Identity Platform together, user authentication can be separated from authorisation, proving platform independence and helping to mitigate any configuration errors and future security vulnerabilities. In addition, you can easily combine local accounts and several external IdPs, for example choosing to use Azure AD for most important customers/partners and local accounts for others. In the Ubisecure Identity Platform, you can also access all user attributes provided by Azure and use them for access control (authorisation) decisions. This can be useful if you integrate with several Azure AD tenants that use different attributes or security groups.

For a practical example with best practices, please see how to set up the "Sign in with Microsoft" authentication method using Microsoft Azure AD as an identity provider: **https://www.ubisecure.com/identity-provider/sign-in-with-microsoft-azure-ad/**

OAuth 2.0 flows in Azure AD B2C

The OAuth 2.0 authorisation framework supports several different flows (aka grants). When third-party cookies do not present a problem, the implicit grant flow is the simplest on paper. In the implicit grant flow, the application receives access tokens directly from the Azure AD authorization endpoint, without any server-to-server messaging. This means that all authentication and session handling is done entirely on the client side, which poses serious problems if the application cannot be trusted to store shared secrets – for example, mobile apps.

Azure AD B2C offers a non-standard extension to partially mitigate these issues, but in order to avoid the remaining security issues – as well as the resulting vendor lock-in from using proprietary extensions with standard protocols - replacing implicit grant flow with Authorization Code Flow + PKCE should be a top priority. One should keep in mind that while the access tokens are cryptographically signed to protect against manipulation, they are easily decoded, revealing all claims with potentially sensitive (meta-)data.

The Proof Key for Code Exchange (or PKCE) enables public (untrusted) clients to mitigate the threat of having the authorisation code intercepted by an adversary. Native applications cannot securely store a Client Secret. Disassembly of the application will reveal the Client Secret, which is application-specific and the

same for all users and devices. In short, PKCE adds a secret created by the calling application to the Authorization Code Flow, that will be verified by the authorisation server. The full specification is available as **RFC 7636**.

When utilising the Authorization Code Flow + PKCE, two important limitations of Microsoft's Authentication Library for JavaScript (MSAL.js) are: the inability to gain authorisation to access Azure AD protected resources; and requiring administrator privileges to obtain tokens for Microsoft APIs (for example MS Graph API) using delegated permissions.

The Ubisecure Identity Platform can be used as a universal translator between applications that use different OAuth 2.0 grant types, or even completely different protocols such as SAML and OpenID Connect (OIDC). This flexibility enables the update and migration of the connected applications as needs evolve, helping to ensure that the technology stack scales with the business needs at hand.

Summary

As the digital identity landscape continues to evolve, not all IAM platforms are equal. Different vendor platforms offer different core competencies, which should be thoroughly evaluated before investing in a platform. As identity and access management (IAM) integrates with business-critical systems, it is important to ensure that appropriate functionality in all the key domains is present in the platform of choice.

> **Ubisecure's Identity Platform integrates seamlessly with Azure AD B2C and B2B as a developer-first, API-first technology stack.**

With a wealth of experience spanning two decades, including contributions to standards working groups (such as with the Kantara Initiative) and framework consultation (like the Finnish Trust Network), Ubisecure is well-placed to provide advice and guidance on the IAM solution that is best for your individual organisation.

Get in touch

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-premises 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