UBISECURE®

Connecting Identity.
Transforming Digital Business.

Digital identity and remote working

Blurring the lines between Employee IAM and Customer IAM

Introduction

2020 has seen remote working become the new norm, with many predicting that remote working will continue to prevail beyond the pandemic.

With this in mind, many businesses have had to raise urgent logistical questions around employees staying connected and maintaining access to internal systems efficiently and securely. Naturally, digital identity plays the central role in organising access to business applications, regardless of user location (in the office or remote).

Verifying user identities and managing appropriate access to various resources is a key aspect of both internally (employee) and externally (customer) focused applications. However, until now, the management of these internal and external identities has been treated differently by organisations. Let's explore why that's now changing, and how it affects you.

IAM vs CIAM: until now

Many businesses have faced the pitfalls of attempting to make employee IAM - aka traditional/legacy/enterprise/internal IAM, built for in-office, workforce identities - work for external users (customers, partners, citizens etc.).

The assumption that 'one IAM fits all' has left businesses unable to cope with external user demands for usability and scalability, alongside different necessary approaches to regulation adherence.

These issues saw the emergence of Customer IAM – a subset of IAM that is specifically designed for external identities. For example:

- Greater focus on seamless user experience, e.g. with various options for authentication
- Putting users in charge of their own data and account access delegation, to support scalability
- Regular platform updates in line with technology trends, rather than a fixed system

This infographic (on page 3) provides an overview.

The difference between IAM and CIAM

Customer Identity and Access Management

Identity and Access Management

External users (consumers, customers, partners, contractors, things, citizens)	MANAGE IDENTITIES FOR:	Internal users (employees)
Key driver to business success and differentiation	USER EXPERIENCE	Needs to meet a minimum standard – employees should have training
Normally several	IDENTITY PROVIDERS	Normally one
Needs to keep up technology trends and remain flexible	PLATFORM FLEXIBILITY	Often quite rigid, doesn't need new add-ons very often
Significantly more users than IAM, must be able to scale at a higher rate	SCALABILITY	Predictable number of users, typically significantly fewer employees than customers
Requires outsourced & tiered management	IDENTITIES MANAGED BY:	HR/IT – can be relatively manual
The external user should be in control of their own data	PRIVACY, TRUST & DATA REGULATION	The organisation owns and operates the data of a user
May bring in revenue through new digital services, or at least saved support costs	REVENUE	Not designed to bring in revenue

UBISECURE®

IAM and CIAM in 2020: new 'blurred lines'

When it comes to remote working, however, the typical internal user starts to look and behave a lot like an external user, increasing the importance of CIAM-specific capabilities. The lines between IAM and CIAM have started to blur.

ONBOARDING

Many employees may now be recruited and onboarded without ever meeting their colleagues in person, which throws up needs that are better met by CIAM – for example, remote identity verification with international identities as opposed to a manual process with HR.

TRAINING

Employee IAM is traditionally something that new starters are trained to use face to face. Any nuances of the system become familiar over time, with the ability to ask colleagues sat nearby for assistance when needed. Customer IAM removes any user experiences obstacles for external users, who don't have training or the patience for clunky identity workflows. Similarly, remote workers will not be able to receive face to face training – a scenario that would be better served by the accessibility of CIAM.

SECURITY

Further, while every interaction now needs to be digital, hacking and phishing incidents are on the rise. This means that secure access, to only the right resources, from any location, is more important than ever. Again, something that's facilitated by CIAM's ease of use – think identity providers (IdPs), delegated authority, risk-based authentication (RBA) and options for multi-factor authentication (MFA).

- Let's take RBA as an example. In an office environment, staff are typically asked for a password in order to gain access to applications. The location of the device, the browser, the time of day etc. are unlikely to change. If a hacker is sat at an employee's desk trying to gain access to the systems, other staff members will notice. However, in a remote situation, the employee's device IP address, the time zone, the device itself, may all be unpredictable. In this case, RBA workflows would recognise where additional, stronger authentication factors are needed, until the device and other situational factors are authorised and trusted.

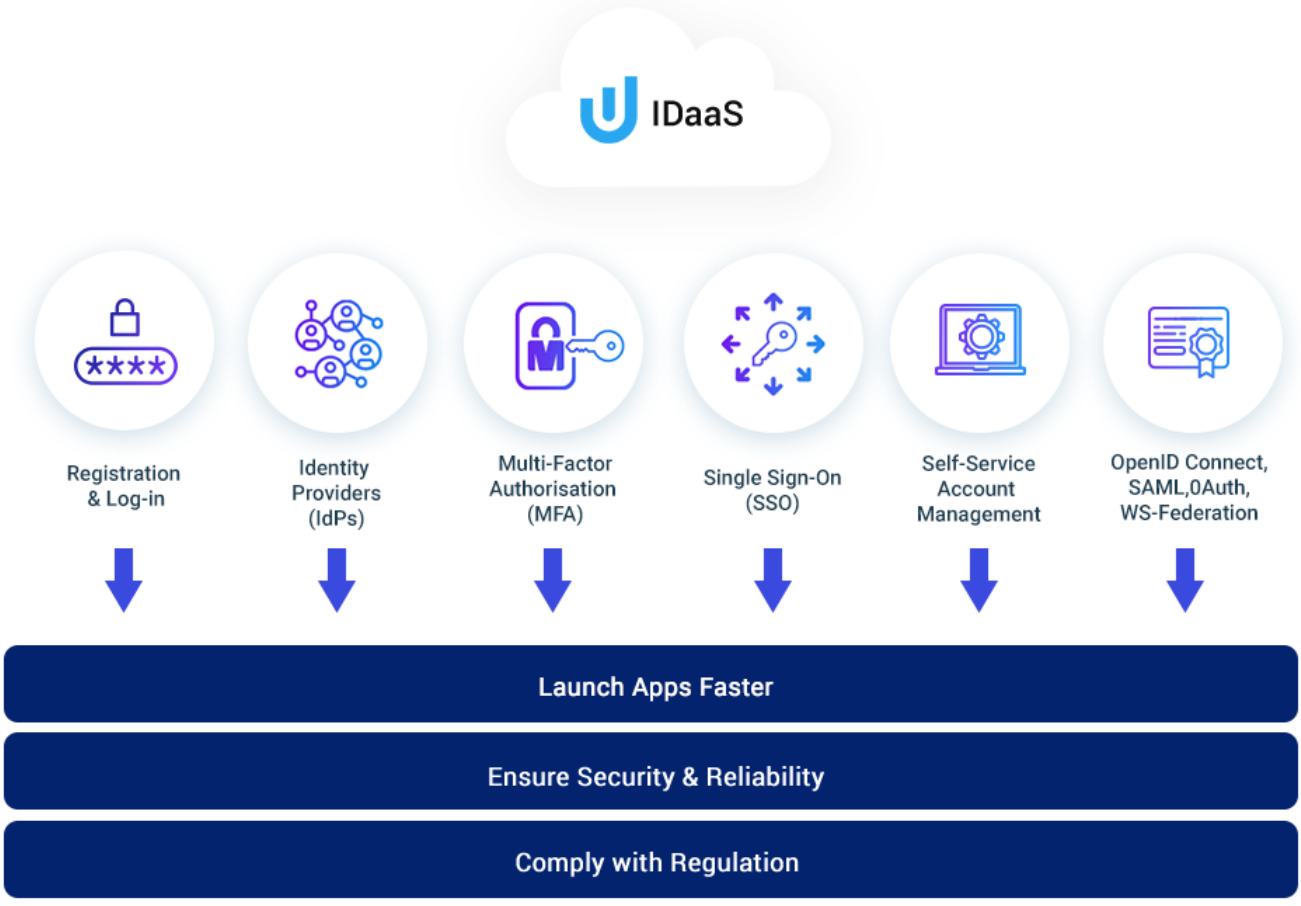
> To take the earlier incorrect assumption that 'one IAM fits all', the shift to remote working has shown us that, in fact, 'one CIAM fits all'.

What does this mean for organisations?

If your employees have been asked to work from home this year, you'll already know if your internal systems have stood up to the challenge of remote identity and access management.

If they have, operational efficiency will not have changed since employees were office-based. For example, there will be no increase in IT Support having to sort out login issues, or employees wasting time trying to gain access to necessary services.

If not, this paper may explain why. For these businesses, you'll need to implement a solution to help you deal with these now-external identities – fast. Try Identity-as-a-Service (IDaaS).



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