ProofID
Managing Identity

Is IDaaS the best fit for your enterprise?

2018 | Whitepaper | v2.0

ProofID.com

Contents

Executive summary

As with most technologies, Identity and Access Management (IAM) is rapidly transitioning towards a cloud first delivery model, with many focusing mainly on Identity-as-a-Service (IDaaS) platforms. IDaaS, in common with all Software-as-a-Service (SaaS) platforms, is an attractive proposition in many ways, providing core identity management functionality such as single sign-on (SSO) and authentication with limited or no on-premise technology.

However, the SaaS business model necessarily reduces the ability for vendors to support complex, custom or bespoke configurations; Gartner describes IDaaS as "bundling software and operations into a commoditised service". Such a commoditised service is often unable to support the complex identity management requirements which large, global enterprises frequently need.

An alternative approach exists, in the form of IAM Managed Service. This approach is distinct from IDaaS in that it offers a hosted and fully-managed, customer specific instance of enterprise identity management technology. This enables enterprises to benefit from the 'cloud experience' without needing to compromise the commoditised functionality available in IDaaS platforms.

This white paper describes the differences between the IDaaS and IAM Managed Service approaches and explores the relative value propositions. In addition, the white paper provides guidance to enterprises to assist in determining which approach will most effectively fulfil their identity management requirements.

Gartner describes IDaaS as:

> *"Bundling software and operations into a commoditised service."*[1]
>
> Gartner

[1] Gartner 2016 IDaaS Magic Quadrant

Overview of IDaaS

IDaaS has for many vendors now become the primary method of delivering identity management services. In this section, we will take a look at the functionality typically provided by IDaaS platforms and compare this against the functionality typically required by large enterprises.

What is IDaaS?

Traditionally, identity management was very much an 'on-premise' technology, with often complex, full-stack vendor solutions running in customers' data centres, managing identities across predominantly on-premise application estates.

However, with the advent of mass cloud adoption around 2010, it made sense to also move identity management services to the cloud. The proposition was essentially 'manage the cloud from the cloud'. This saw the advent of IDaaS, with initial products providing SSO to major SaaS applications such as Office365.

Since then, the IDaaS market has developed significantly, with many vendors now offering mature IDaaS platforms, with increasingly broad functionality and integration capabilities. The leading vendors in the IDaaS space include: Ping Identity with its PingOne platform, Microsoft and Okta, with a number of other vendors such as Centrify and One Login following close behind. Initially, take up of IDaaS solutions was predominantly by SMEs. However, in recent years larger enterprises have started to look more closely at IDaaS as a means of providing enterprise wide identity services.

Typical IDaaS functionality

At their core, modern IDaaS solutions offer authentication services to provide federated SS0 into applications. IDaaS platforms have a core strength in delivering SSO into cloud applications, and typically offer a catalogue of pre-defined SSO templates for thousands of cloud applications, allowing administrators to very quickly configure SSO to cloud applications.

In addition to this core SSO functionality, IDaaS platforms offer other identity management features such as directory services, links to on- premise directories such as Active Directory, user provisioning, reporting and analytics. Many IDaaS platforms are increasingly looking to offer integration with on-premise applications, however this typically involves deployment of on-premise components such as software agents or servers.

IDaaS capability gap

Reaching the limits of IDaaS capability

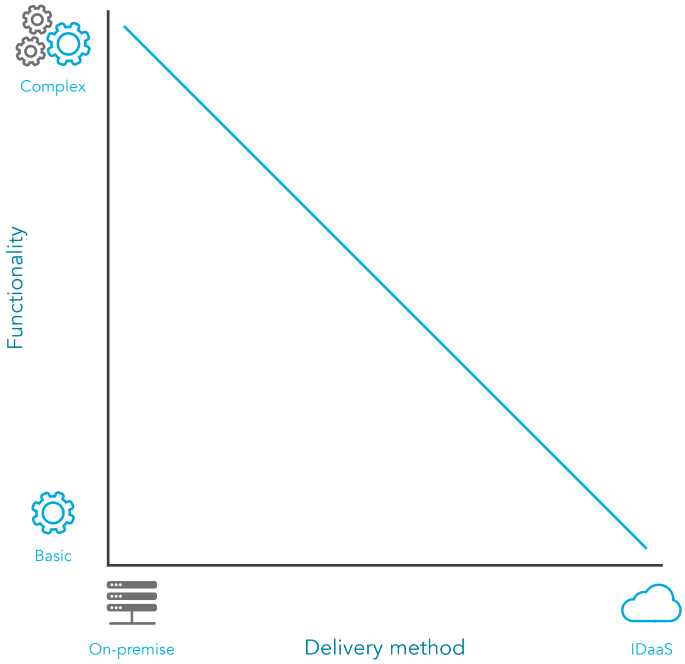
Whilst IDaaS offers an increasingly broad range of identity management capabilities, there is a limit to the depth of features that they can offer from a shared platform. In all SaaS platforms, there is a compromise between the convenience of a cloud-based platform, and the configurability and customisation available. Put simply, SaaS platforms must be 'all things to all people'.

The SaaS business model is based around scale and repeatability – it is simply not viable for SaaS vendors to support and maintain custom or bespoke solutions within individual customer's tenancies. This is equally true for IDaaS. The compromise can be visualised in the diagram.

The diagram below shows that the greatest depth of features is available in traditional on-premise software. Ultimately, for on-premise, individually managed implementations of identity management technology, complex custom solutions are viable. In contrast, in a SaaS environment the vendor's business model is based on offering the same service to all its tenants, leading to a 'lowest common denominator' approach which reduces the ability for customers to fit the solution into complex enterprise requirements.

Of course, IDaaS vendors are working hard to reduce the angle of the slope, however the imperatives of the SaaS business model means that the gap between on-premise and SaaS capability will always be present.

Fig1



Enterprise needs vs. IDaaS capabilities

As an organisation grows in size and complexity, typically its identity management requirements become significantly more complex. Larger organisations have more users, applications and territories to manage. Additionally, they have more complex business processes and security requirements, and crucially they lack the agility to change their operating model to fit the cloud-centric approach to identity management offered by IDaaS vendors.

> "Replacing customised, on-premise IAM (especially identity governance and administration) software to support legacy application architectures with IDaaS can be costly and difficult." [1]
>
> Gartner

Examples of areas where IDaaS platforms lack the depth of on-premise alternatives include:

Support for standards

While all IDaaS platforms support SAML2 (Security Assertion Mark-up Language 2), many do not offer full support for older versions of SAML, or other standards such as WS-Fed, WS-Trust or OpenID Connect. These variations can limit optionsfor integration.

Identity, governance and administration Gartner identified in its 2016 IDaaS Magic

Quadrant that many IDaaS vendors currently lack deep identity, governance and administration features. This includes workflow-driven approval processes for user and application provisioning, and certification workflows to ensure users have the appropriate access.

Legacy/On-premise application integration

Being cloud based, many IDaaS platforms require the implementation of on-premise components (agents or servers) in order to integrate with on-premise or legacy applications. This can significantly increase the complexity of managing the environment and can diminish one of the core benefits of the IDaaS proposition.

This is recognised in Gartner's research:

"Replacing customised, on-premise IAM (especially identity governance and administration) software to support legacy application architectures with IDaaS can be costly and difficult." [1]

[1] Gartner 2016 IDaaS Magic Quadrant

Custom integration

Many large enterprises need to be able to integrate custom APIs (application programming interfaces) into their authentication or provisioning flows – a commonly seen example of this is to call a bespoke web service to determine access permissions for a user. Inflexibility amongst large enterprises means that in many cases it is not possible for the enterprise to change its processes to fit an identity management platform's capability. Thismeans that the only viable approach is to implement customisations bespoke to the customer. As previously mentioned, such customisations are not viable in an IDaaS environment.

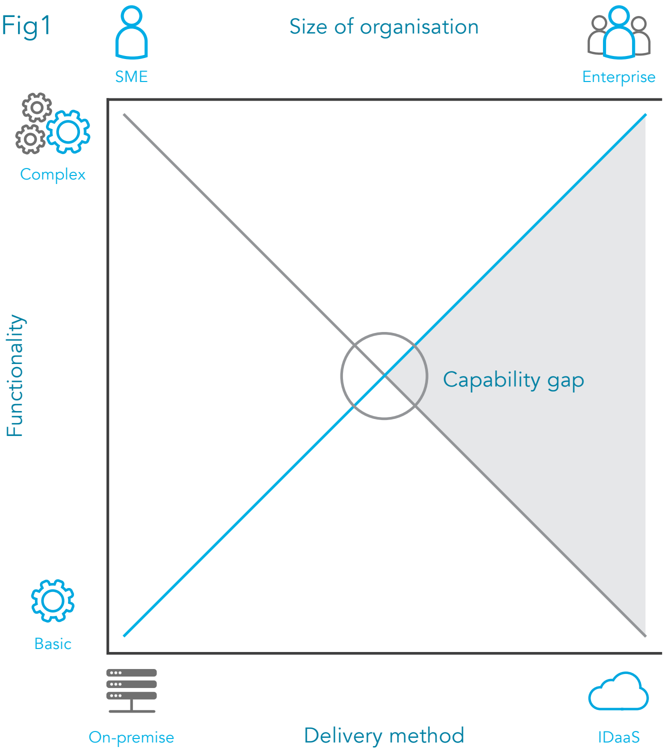
Security requirements

Large enterprises may have enhanced security requirements, which may not be supportableon an IDaaS platform. For example, issues over data sovereignty may require hosting in a certain location, or perhaps corporate guidelines mandate that all service providers are IS27001 accredited. Furthermore, security conscious organisations may feel that delegating control of a core security function such as identification and authentication of users to a commodity IDaaS vendor could present a risk.

The following diagram visualises the mismatch between enterprise requirements and typical IDaaS provision.

The highlighted area capability gap represents the gap between the functionality which a large enterprise requires, and the functionality which is provided by an IDaaS platform.

Fig1



IAM Managed Service aka IDaaS for the enterprise

Having seen how current IDaaS offerings are often unsuitable for enterprise customers due to their necessarily rigid and limited feature sets, the question arises – is there an alternative approach?

What really is SaaS?

The challenge that enterprises face is the mismatch between the drive towards a cloud-first approach to IT, and the need to support enterprise use cases. However, under scrutiny, the first part – the drive towards the cloud – often boils down to a desire for the service to be hosted outside of the organisation. Therefore, the 'cloud experience', and the benefits of removing the need for on-premise hardware and skills, outweighs any need for the service to be truly 'SaaS'.

> "IAM managed services are distinct from identity as a service (IDaaS): managed services provide only management and operation of customer-owned IAM software and infrastructure, while IDaaS bundles the software and operation intoa commoditised service that is provided on a subscription basis."[2]
>
> Gartner

In this case, an alternative approach becomes possible – IAM Managed Service. IAM Managed Service enables enterprises to achieve both aims – to benefit from the cloud experience yet still support complex use cases.

IAM Managed Service vs IDaaS

So, what are the characteristics of an IAM Managed Service platform? Essentially, IAM Managed Service is a fully-managed, customer specific example of enterprise identity management technology. Usually, an IAM Managed Service platform will be hosted by the vendor, however it is equally possible for the vendor to manage the identity management infrastructure on-premise.

Gartner describes the difference between IAM Managed Service and IDaaS as follows:

"IAM managed services are distinct from identity as a service (IDaaS): managed services provide only management and operation of customer-owned IAM software and infrastructure, while IDaaS bundles the software and operation into a commoditised service that is provided on a subscription basis."[2]

Gartner makes a further distinction between 'staff augmentation' managed service, which is essentially provision of contracted IAM consultants to operate a customer's IAM infrastructure, and 'methodology-driven' managed services – which are defined as follows:

"These services can provide round-the-clock, remote management and operation of customers' IAM infrastructure. These managed services maintain fully staffed IAM operations centres where they provide remote monitoring of IAM software installed in customer environments."[3]

IAM Managed Service falls squarely in the 'methodology- driven' camp.

[2] Market Guide for IAM Professional Services EMEA, Gartner, 31st August 2016

[3] Ibid

To elaborate on this somewhat – the key difference between IAM Managed Service and IDaaS is that the former is a fully-managed service. IDaaS is a platform which is presented to the customer 'as is' – the customer still needs to configure the platform to fulfil the organisation's identity management requirements, and to do so requires niche skills and deep knowledge of identity management technologies, standards and protocols.

Regardless of how user friendly an IDaaS UI may be, ultimately identity management is an integration technology, and without detailed domain knowledge such as understanding of standards like SAML and OpenID Connect, configuring the system will be an uphill battle. The IAM Managed Service approach does away with this problem; IAM Managed Service vendors have dedicated teams of experts who perform the configuration of the system on behalf of the customer and attend to any issues which may arise. The core benefit of this is that the customer can simply focus on the strategy and outcomes to be delivered by the platform, leaving the vendor to deal with the detail.

A further characteristic of IAM Managed Service is that because each instance is customer specific, the vendor is able to support customisations and bespoke configuration which would be beyond an IDaaS platform. Equally, seemingly simple things such as the ability to provide a dedicated VPN (Virtual Private Network) between an IAM Managed Service tenancy and the customer's data centre enables many use cases which are challenging for an IDaaS vendor. This can seamlessly accommodate tasks such as authenticating users directly against an on-premise directory service, removing the need to synchronise all corporate identities to the cloud.

Having your cake and eating it

All taken together, the IAM Managed Service approach allows the enterprise customer to 'have their cake and eat it'. The IAM infrastructure is offsite with resilience and uptime guaranteed by expert round-the-clock support. In addition, by building the service on enterprise-grade technology in a customer specific tenancy, no compromise on functionality is required – the 'capability gap' identified on page 7 is filled. Finally, because IAM Managed Service platforms are managed on behalf of the customer, there is no need to maintain niche and expensive identity management skills to maintain and develop the environment.

> "These services can provide round- the-clock, remote management and operation of customers' IAM infrastructure. These managed services maintain fully staffed IAM operations centres where they provide remote monitoring of IAM software installed in customer environments."[3]
>
> Gartner

[3] Ibid

Considerations for choosing a platform

Many supplier offerings in the IAM space share a lot of common ground, however for your B2B IAM system there are some specific requirements that can make the difference in terms of roll out and adoption. Prior to choosing a supplier or simply extending technology already in use within your organisation today we encourage you to ask the following five key questions.

IDaaS

- Cloud first strategy
- Deep identity management skills within the team
- Simple requirements with limited integration with on-premise applications
- Simple organisational structure with few distinct user communities
- No need for custom integration or bespoke configuration
- Limited end user branding requirements
- Requirement for platform availability SLAs only (i.e. vendor is not responsible for configuration errors)

IAM Managed Service

- Cloud first, on-premise or hybrid strategy
- No identity management skills within the team, or a desire to reduce headcount in this area
- Complex requirements including integration with on-premise applications
- Complex organisational structure (e.g. including multiple independent territories or group companies) with multiple distinct user communities (e.g. staff, customers, partners, suppliers)
- Custom integration or bespoke configuration
- Full branding of end user interfaces
- Both platform and service availability and fault resolution SLAs (i.e. vendor is responsible for them)

Conclusion

Many enterprises are attracted to Identity-as-a-Service offerings due to the promise of simple and quick deployment offered by cloud-based SaaS platforms. However, in common with all SaaS platforms, SaaS necessitates compromise in terms of functionality. To quote Gartner, IDaaS services "bundle software and operation into a commoditised service".

Unfortunately, enterprises rapidly discover when evaluating IDaaS platforms that the 'commoditised service' they offer is not able to deliver upon the complex use cases which are found in the modern enterprise. In particular, integration with on-premise applications, customisations and bespoke configurations are difficult for IDaaS vendors to support in a scalable and supportable way, and consequently the available functionality falls short of the enterprises' requirements and expectations. This is the IDaaS 'capability gap'.

Happily, an alternative is available which can help enterprises to have the best of both worlds. IAM Managed Service platforms are hosted and managed, customer specific instances of enterprise identity management technology, an approach known by Gartner as "methodology-driven managed service". This approach enables the enterprise to have the benefit of the cloud experience and all the cost saving and convenience which this offers, whilst not compromising on functionality and the ability to customise the environment to their needs. IAM Managed Service closes the 'capability gap' left by IDaaS, whilst offering other benefits such as round-the-clock monitoring and support.

Whilst there are no hard and fast rules as to which approach will best suit a particular organisation,

it is safe to say that enterprises which have complex user management and authentication requirements, and which are likely to require customisations would be well advised to evaluate IAM Managed Service for provision of their identity services.

With over 500,000 managed enterprise identities, ProofID's IAM Managed Service platform is trusted to process millions of user's authentication and authorisation transactions daily. Contact a representative for more information about how our IAM Managed Service platform can meet your enterprise IAM requirements.

To quote, Gartner IDaaS services:

"Bundle software and operation into a commoditised service."[1]

Gartner

Gartner describes the IAM Managed Service approach as:

"Methodology driven managed service."

Gartner

[1] Gartner 2016 IDaaS Magic Quadrant

ProofID
Managing Identity

About ProofID

ProofID is a IAM Managed Service Provider (MSP) operating globally. Our team of identity experts are trusted by many Tier-1 enterprises to design, deliver and manage their IAM services. We manage millions of identities and deliver services to over 150 countries. All successfully delivered through our methodology driven IAM Managed Service.

For more information:
email info@ProofID.com
visit ProofID.com

EMEA/APAC

Lancastrian Office Centre
Talbot Road, Manchester
M32 0FP

t. +44 (0) 161 906 1002

North and Latin America

1755 Teslar Drive,
Suite 206, Colarado Springs,
CO80920

t. +1 719 247 8473