ProofID
Managing Identity

# B2B Identity Management

The importance of Identity and Access Management to harness the potential of your partner community

**2018 | Whitepaper | v2.0**

ProofID.com

# Contents

3. Executive summary

4. The role of partners in your digital business

6. The importance of Identity and Access Management (IAM) to building a digital B2B partner platform

8. Considerations when planning a B2B IAM deployment

10. 5 key questions to ask your IAM supplier

11. Conclusion

# Executive summary

Organizations of all sizes are using technology to improve their business and achieve their goals. Many of those organizations are going through the process of converging and integrating consumers, partners, workforce and things to improve the consumer experience, reduce costs and increase speed to market. These initiatives are typically described as digital transformations or building a digital business.

This whitepaper focuses on partners as a key part of the digital business. Highlighting the specific issues that need to be addressed to provide security and access for what is typically, a large, distributed and autonomous community.

The paper puts forward the argument that to achieve security and access at scale for your partner community the adoption of Identity and Access Management (IAM) technology is essential. Furthermore, it highlights the specific differences that need to be considered by comparison to putting the same provision in place for workforce for example.

It encourages the reader to consider these differences carefully and use these requirements to drive the approach to deployment of an IAM solution and what questions suppliers need to be asked to determine whether their technology is fit for purpose.

The conclusion is that not all IAM solutions fit the partner requirement well; both from a technology perspective and in terms of costs and effort required to achieve the desired functionality. Organizations who are considering developing technology to support their partner community should seek out organizations who have the expertise and tooling to support your requirements quickly and cost effectively.

## Gartner Magic Quadrant for Identity Governance and Administration 2018

We are delighted to have received an honorable mention in the Gartner Magic Quadrant for Identity Governance and Administration 2018 report.

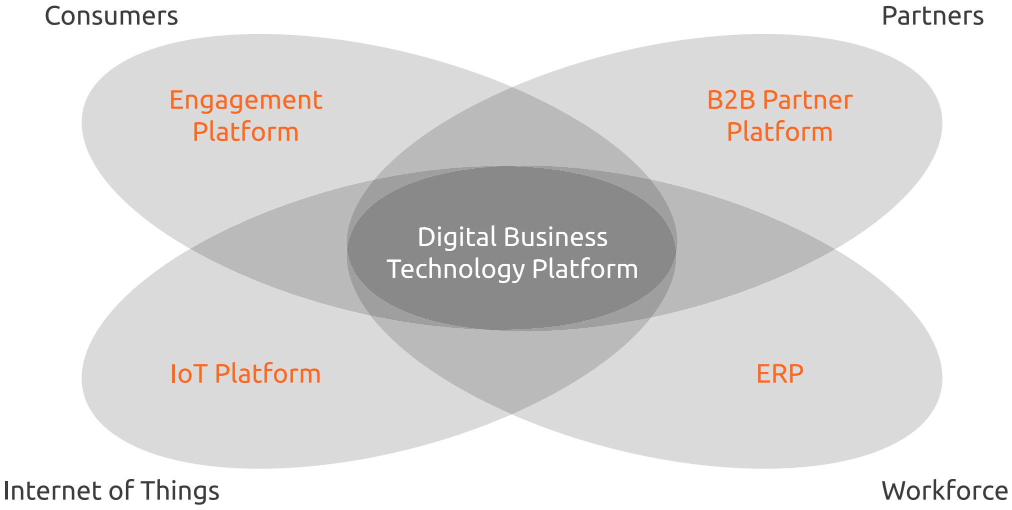
# The role of partners in your digital business

Most, if not all businesses and organizations are to some extent pursuing a digital transformation strategy – the direction of travel is towards the widespread embedding of the digital business.

Gartner defines digital business as the:

*"Creation of new business designs by blurring the boundaries between the digital and physical worlds due to the convergence of people, business and things."*[1]

This convergence of technologies and communities can be visualized as follows:



A good example of a digital business is that of the manufacturing supply chain. If we take vehicle manufacturing for example, the partner works with the consumer to specify the vehicle, arrange finance and order the vehicle via the B2B partner platform. Production is planned via the workforce ERP and progress is reported via the IoT platform. Finally, once the vehicle is delivered, the consumer engages with the engagement platform to maximize consumer satisfaction and build brand loyalty. This orchestration helps deliver three key business objectives; improve the consumer experience, speed to market and reduce costs.

[1] Building a Digital Business Technology Platform, Gartner, 8th June 2016

Whilst most attention is often given to workforce and consumers in this model, the reality of modern business is that supply chains exist across organizational and international boundaries. There is often a high level of dependency on the partner to support the fulfillment of downstream activities and goals. The importance of this area is reflected in the fact this is a rapidly growing area for many organizations. In a recent survey commissioned by Ping Identity, 79% of respondents indicated that managing ecosystems was critical to success for their digital transformation initiatives. [2]

> “Digital business is the creation of new business designs by blurring the boundaries between the digital and physical worlds due to the convergence of people, business and things.” [1]
>
> Gartner

> 79% of respondents indicated that managing partner ecosystems was critical to success for their digital transformation initiatives. [2]
>
> Ping Identity.

[1] Building a Digital Business Technology Platform, Gartner, 8th June 2016
[2] The State of Digital Transformation Report 2016, Ping Identity

# The importance of Identity and Access Management (IAM) to building a digital B2B partner platform

When we think about integrating partners into our digital businesses to achieve scale and speed up processes, we also need to consider the security implications related to this. The common thread in addressing this area is the provision of IAM services to control and govern access.

Gartner defines IAM as:

*"Identity and Access Management is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons."*[3]

Provision of IAM to support partners has many different characteristics to workforce and consumer use cases. For example, consumer and workforce systems are under your control and you have a high degree of visibility to their status. However, partners are external entities, visibility of changes in personnel, systems and processes are significantly less. Therefore, IAM to support partner deployments (B2B IAM) are different, both in terms of approach and technology and tooling decisions.

The success of B2B partner platforms is defined by how the technology allows individuals to gain access to timely, relevant information, and then collaborate on that information with the right people across a network to make better business decisions.

So, when we think about access, this is not just accessing the service you are providing but also what the individual can see and do within it. This statement may seem deceptively simple; however, a partner network can consist of 10,000s of users spread out across 100s of businesses. There may be scenarios where different businesses have visibility of different pricing agreements, there may be the ability for certain individuals who are entitled to execute commercial transactions and so on.

[3] Agenda for Identity and Access Management, 2012. Gregg Kreizman

To illustrate the importance of security for your B2B partner platform, in 2016 Deloitte reported that for the third successive year, 30% of surveyed organizations experienced supply chain fraud, where supply chain relationships were misused[4]. With this in mind, it is essential that your B2B IAM service ensures that users purporting to represent partners actually do and their entitlement remains valid. Verification and certification of partner identities becomes a vital activity. However, it is complicated by certification processes which cross organizational boundaries.

> "Identity and Access Management is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons."[3]

Put simply, this risk boils down to this: what happens if an individual leaves an organization and joins another similar organization? Will their access be revoked in a timely way? If not, what competitive information may they have access to that would put you or your partner at a disadvantage? Bearing in mind that the infamous Target breach was caused by stolen third party credentials[5], if their access is not removed and their account becomes compromised, where does the liability lie?

With the level of management that is required to manage the security and access of the B2B partner platform, the question of how this service can be scaled needs to be considered. B2B IAM also has a key role to play in achieving this. With the correct tooling and approach much of this administration can be automated and delegated. Avoiding the cost and inherent security issues related to slow, manual processes.

[3] Agenda for Identity and Access Management, 2012. Gregg Kreizman

[4] Fraud risk assessment: Escalating the battle against supply chain fraud, waste, and abuse, Deloitte, 2016

[5] Target Hackers Used Stolen Vendor Credentials- Wall Street Journal

# Considerations when planning a B2B IAM deployment

For the reasons outlined above, partner deployments of IAM have different characteristics than workforce or consumer use cases, however these differences are not always considered properly. It is often simply assumed that existing workforce focused IAM tools will be well suited to B2B IAM requirements.

Research from Quocirca found that only 20% of respondents rated their existing IAM deployment as being fit for purpose for managing external users, with Quocirca concluding that:

*"Existing IAM deployments are often legacy systems, supplied along with an IT infrastructure stack that was not designed to manage external users."*[6]

Furthermore, often new technology projects focus on the features of the platform, such as how a transaction might be executed or how information is delivered and presented. IAM is often considered late in the planning and development process, meaning that incorrect assumptions about the use of existing IAM technology can negatively impact on delivery. Planning IAM at the start of the initiative establishes the golden thread of identity that gives your development teams a reference architecture to develop against and avoids any additional costs of introducing it later in the process.

When thinking about deploying your B2B partner platform the following key points need to be recognized and planned for:

### B2B identities are different to workforce identities

The processes and tools you use to manage your workforce identities may not be appropriate for managing B2B identities. For example, workforce IAM is typically driven by events in the HR system; HR knows when staff join, leave and change roles. The IAM system can use this information as a trigger. For B2B identities, you do not have the visibility or system of record so you need to consider how you will manage this.

### B2B IAM is an asymmetric problem

Consider the example of the vehicle manufacturer again. It is very likely that they will have supplier relationships with very large firms alongside much smaller companies. Managing these different types of organizations will have very different requirements. The large manufacturer is likely to have much more significant IT infrastructure and processes, and will likely have tens or even hundreds of individuals requiring access. At the other end of the spectrum there may be just a few individuals with very limited formal IT infrastructure. Of course, there will be everything in between as well. The B2B IAM system needs to be flexible enough to cope with these different usage profiles.

[6] Getting To Know You - Building Relationships with Effective Identity and Access Management, May 2015

### Managing access to your B2B partner platform has a significant overhead

B2B partner platform users are likely to be relatively infrequent users of your service, but relatively high maintenance. The reasons they need to access your systems are almost by definition business critical, however low usage means that issues with forgotten passwords and even usernames are more likely than for staff users. It's important that your B2B IAM system can let users help themselves with common problems like recovering forgotten passwords and usernames.

### How is access approved?

Provision of access for B2B partner platform users will necessarily require some form of approval; staff users have an 'identity birth right' by virtue of having a record in the HR system – this doesn't apply for partners, so provisioning their access will always be on someone's 'say-so'. Chasing down this approval and keeping necessary documentation up to date is time consuming and not scalable. The ability to automate approval workflows is a bare minimum essential for your B2B IAM system; however, for a full solution, the management of identities should be able to be delegated to the partner organization itself, removing the overhead from your own team and assigning responsibility for management of their users to the partner itself.

### Focusing on providing access not removing it

As we liven up new platforms the goal is to provide access and drive adoption. However, what about the removal of access? It is much harder to determine whether an individual from a partner organization still works for that company, have they left? Have they joined a competitor? Introducing recertification processes to validate the entitlement to access is essential. However, with recertification processes crossing organizational boundaries, does your existing IAM solution have the delegation capabilities to be able to support this requirement?

### What are the costs of implementing your B2B IAM requirements?

As stated, many IAM platforms are designed with the workforce in mind. Design decisions for these platforms mean that more sophisticated requirements that are commonplace in a partner settings are dependent on consulting and customization. All vendors will likely be able to achieve your requirements, however at what cost and in what timeframe? Can your project timeline and budget accommodate potentially hundreds of days of consulting services to essentially build a bespoke capability within a generic IAM framework?

> "Existing IAM deployments are often legacy systems, supplied along with an IT infrastructure stack that was not designed to manage external users."[6]
>
> Quorcira

[6] Getting To Know You - Building Relationships with Effective Identity and Access Management, May 2015

# 5 key questions to ask your IAM supplier

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 organization, today we encourage you to ask the following five key questions.

### 1. What self-service capabilities can I provide to my B2B community?

For smaller organizations, the costs of implementing federated access are prohibitive. Self-service is an ideal alternative, providing capabilities not only allows individuals to request access, but also manage their ongoing access.

### 2. Will I be able to delegate administration to individuals in the business or the partner business?

Problems with usernames and passwords are not the only issue that can have a big impact on your service desk. Although requests for access can be managed by self-service capabilities, someone who is trusted and understands the business context needs to approve it.

### 3. Will it be possible for me to use a federated access approach?

For other large organizations in your B2B community federated access has many advantages. Allowing many users from the partner organization to access your services, minimizing administrative overhead and avoiding security issues related to the synchronization of identities and passwords.

### 4. How can I measure compliance with my governance policies?

As with any major system governance is a key part in measuring and controlling the access decisions that are made within your B2B community. The ability to demonstrate compliance with policy and more importantly identify where there has been non-compliance is critical to ensure that your organizations business interests are protected.

### 5. How much time and cost will I need to invest?

In the majority of cases all identity and access providers will be able to provide the above functionality. However, it can be argued that anything is possible given sufficient time and money. Most vendors provide the building blocks for these solutions; however they typically require high levels of customization by specialists in the product. This leads to substantial consulting bills, coupled with long delivery times and substantial investment from your own business resources. Look for platforms that are designed specifically for this purpose, can deliver requirements out-of-the-box and can be delivered in a measurement of days, not months or years.

# Conclusion

A key part of becoming a digital business involves developing a B2B partner platform to allow the organization to interact digitally with its supply chain, to streamline business processes and operate more efficiently.

Frequently organizations assume that existing IAM deployments can simply be extended to support this partner identity use case; however, the reality is that B2B IAM has several characteristics which make it different from the more broadly understood identity management use cases. This can lead to escalating budgets, significant delays or even failed projects when implementing B2B partner platforms. By better understanding the challenges and specific requirements of B2B IAM at an early stage in the digital transformation project, appropriate technology and process decisions can be made to ensure a successful outcome.

**The key differences for B2B IAM from workforce and consumer use cases include:**

- Low visibility of changes and state of your partner organizations
- An extremely varied community of partners to manage, from very small to very large, with varied technical capabilities
- Low usage, business critical, high maintenance usage patterns
- High risk profile around de-provisioning operations

**An effective B2B IAM solution will be optimized for these specific challenges by possessing the following characteristics:**

- Support for delegated administration to allow partner organizations to administer their own identities
- Self-service capabilities to allow partner users to recover from common problems like forgotten usernames or password
- Support for federation alongside manual administration of identities to cater for partners of all shapes and sizes
- Automated identity recertification processes which are operated in a delegated mode to cross organizational boundaries

Many traditional IAM solutions, which organizations may already have deployed, may in theory be able to support the partner use case. However, as these solutions are optimized for on-premise, workforce scenarios, 'bending' them to fit the partner use case is likely to involve a significant amount of consultancy and bespoke configuration. Before committing to a partner ecosystem project, it is highly recommended to ask the vendor in detail as to how the above characteristics will be supported, and importantly to quantify the timescales and costs involved, and the associated impact on project budgets and timelines.

ProofID IGA is an Identity Governance and Administration platform optimized to support B2B and external user scenarios. Contact ProofID to understand how IGA's optimized approach can accelerate your partner ecosystem initiative and reduce costs.

ProofID
Managing Identity

## About ProofID

ProofID is an 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

8 Exchange Quay
Manchester
M5 3EJ UK

t. +44 (0)161 906 1002

### North and Latin America

1755 Teslar Drive
Suite 206, Colorado Springs
CO80920 US

t. +1 719 247 8473