eBook

The Power of Effective B2B Identity Management:

Unlocking Success in the Modern Business Landscape

cpl.thalesgroup.com

THALES
Building a future we can all trust

Introduction

The Business-to-Business (B2B) landscape has grown significantly. For instance, the global B2B eCommerce Market[1], valued at USD 7.08 Trillion in 2022, is projected to reach a value of USD 26.59 Trillion by 2030. While this statistic refers to the eCommerce sector, the trend extends beyond eCommerce alone, emphasizing a crucial reality: Businesses increasingly rely on external partners to fuel their growth. Consequently, effective collaboration among these partners has become a pivotal component of a company's bottom line.

Even the slightest friction within a network can disrupt the broader operation and as a result, hinder productivity, output, and in the end sales. Unlocking economic growth, therefore, hinges on fostering efficient and secure collaboration and interactions between all entities.

As companies expand their business networks with an ever-widening range of external stakeholders, the significance of effective B2B Identity & Access Management (IAM) has never been more critical. Yet even though organizations recognize that a strong B2B IAM strategy has become an absolute necessity, the path to successful B2B IAM implementation remains unclear for many.

Uncertainty looms around the requirements and challenges involved in B2B identity management and how to proactively address them. This eBook aims to answer precisely that.

Read on as we conquer key challenges in B2B IAM, guided by expert Marco Venuti. With extensive knowledge in identity and B2B optimization, Venuti will guide us through the most relevant conversations involved.

These discussions can help you establish seamless collaboration and a scalable B2B ecosystem to set you on a path to growth in the digital economy.

1 https://www.vantagemarketresearch.com/industry-report/businesstobusiness-b2b-ecommerce-market-1386#:~:text=Snapshot&text=The%20global%20Business%2DTo%2DBusiness,18.00%25%20between%202023%20and%202030.

B2B Identity Management in the New Normal

The B2B landscape has transformed significantly in recent years. Several factors have contributed to this including globalization, digital transformation, increased volume of interactions, different types of partners, data security and compliance. All this is coupled with shifting working models.

Just rewind back a short five years and the operational B2B models seemed worlds apart from the current work-from-anywhere approach that has become the norm today. Digital platforms and communication tools have almost replaced physical communications.

The increasing reliance on broader networks, digital platforms, cloud services, and cross-border interactions adds layers of complexity to identity verification, access control, and data exchange: the sharing of sensitive data within any B2B network has become a daily routine. Managing identities in this complex space calls for a modernized – much more advanced and flexible– IAM approach.

> **"When it comes to identity management, B2B resides at the most complex end of the spectrum. That's because there is no one-size-fits-all solution. We are not merely discussing the lifecycle management of a single type of identity, such as customers or employees. Instead, we are faced with the challenge of effectively managing an array of diverse identities, from partners to gig workers and many more, each vital to your business, and each with its unique lifecycle and engagement requirements." Venuti explains.**

Rewriting the rulebook of traditional IAM

Traditionally, B2B IAM was primarily focused on providing access to a few external contractors or a limited number of trusted partners. Well, that's no longer the case.

With businesses now collaborating with an extensive network of external stakeholders, including suppliers, contractors, vendors and more, a new – much more complex – identity rulebook is needed.

IAM expert Marco Venuti captures the essence of this. Throughout this eBook, Venuti will guide us through the B2B identity landscape as it stands today – and outline why B2B continues to be the most difficult case of identity management.

Marco Venuti is the IAM Business Acceleration Director at Thales Group. Marco has 20+ years of direct experience in Identity & Security, having worked for multiple solution vendors in Sales and Product Management roles. Prior to Thales, he served as VP of Product Management at OneWelcome and as CTO for Identity Governance solutions at IBM. Marco joined IBM with the acquisition of CrossIdeas, an Identity Governance vendor that he co-founded in 2011. He holds a degree in Electronic Engineering from the University of Bologna, Italy.

The B2B IAM Conversations in The Age of Digital Transformation

In today's interconnected business ecosystem, companies find themselves surrounded by a network of business partners. These partners play a vital role in the success of the organization, whether they are involved in the supply chain, distribution channels, or go-to-market strategies.

Supply chain partners are the suppliers, manufacturers, logistics providers, and vendors involved in making and delivering goods or services. On the other hand, go-to-market partners are sales agents, resellers, dealers, and others who help promote and sell products or services to customers.

Enabling proper access and authorization for these diverse sets of users, potential apps, and resources is crucial for ensuring seamless collaboration and safeguarding data across the network.

And then, of course, there are consumers.

Customer Identity and Access Management (CIAM), a vital pillar in successful digital transformation, has emerged as a discipline to meet distinct consumer needs. CIAM enables seamless and secure experiences via self-registration, single sign-on, and personalized engagement on digital platforms.

So, can't we simply adopt a traditional CIAM approach and tailor it to a B2B context?

The thing is that B2B IAM goes beyond just employees and customers. It includes the 'in-betweens' too—business partners, suppliers, and other external entities that play a role in the value chain.

This means that while B2B Identity and Access Management (IAM) integrates CIAM principles, the solution at hand must be flexible enough to manage the lifecycle of not only employees or consumers but the 'in-between' organizations like partners, suppliers and more which of course have employees.

In this context, even the most advanced identity vendors must expand their offerings and be flexible enough to tackle what Venuti refers to as a 'rainbow' of identities.

"In the varied B2B identity landscape, each facet has unique engagement needs. By integrating CIAM principles, B2B IAM ensures seamless collaboration, streamlined access, and strong security throughout the business ecosystem. The key lies in the agility of the solutions." Venuti explains.

Analyst firm, Gartner[2], shares Venuti's perspective. In recent research, Gartner emphasizes that to address the increased demand for B2B identity management, IAM vendors have significantly enhanced the flexibility of their offerings by introducing more agile delegated administration, specifically tailored to address various B2B identity use cases. In response, vendors like Thales now offer comprehensive solutions, adapting to the interconnected landscape.

2 https://www.gartner.com/en/documents/3941922

Identity Governance Administration vs B2B IAM

Managing access authorization for employees is often a complex task due to the different job roles and applications involved. To address this complexity, specific solution categories like Identity Governance and Administration (IGA) have emerged.

While there are similarities between IGA and B2B IAM, Venuti stresses that it's important to understand the difference between the two identity concepts.

> "In contrast to IGA, B2B IAM presents a different access authorization landscape. Partner organizations typically have a limited number of job roles, often with only one required. Additionally, the number of applications accessible to a partner organization tends to be relatively small, usually in the range of 10."

Distinguishing IGA from B2B IAM

	Objective	Identity Lifecycle	Compliance
B2B IAM	Boosts expansion, collaboration, and efficiency by simplifying secure resource and data sharing with external entities	Focuses on external identity lifecycle, streamlining both partner Organization onboarding followed by Partner's employee onboarding, authentication, authorization, and access revocation.	Ensures compliance with terms and conditions when partnering externally, safeguarding secure and authorized data sharing.
IGA	Helps organizations achieve their internal security, compliance, and operational efficiency goals by managing user access.	Manages the identity lifecycle of internal users, from initial provisioning to role changes, access reviews, and eventual deprovisioning.	Upholds data privacy within the organization

B2B IAM User Diversity

In B2B, users are mainly categorized into three personas:

- Standard Business User
- Delegation Manager
- Partner Manager

The business users are the B2B organization employees who need tailored access levels and single sign-on for relevant applications. As the number of partners grows, it quickly becomes unmanageable for the core company to handle the volatility of business users.

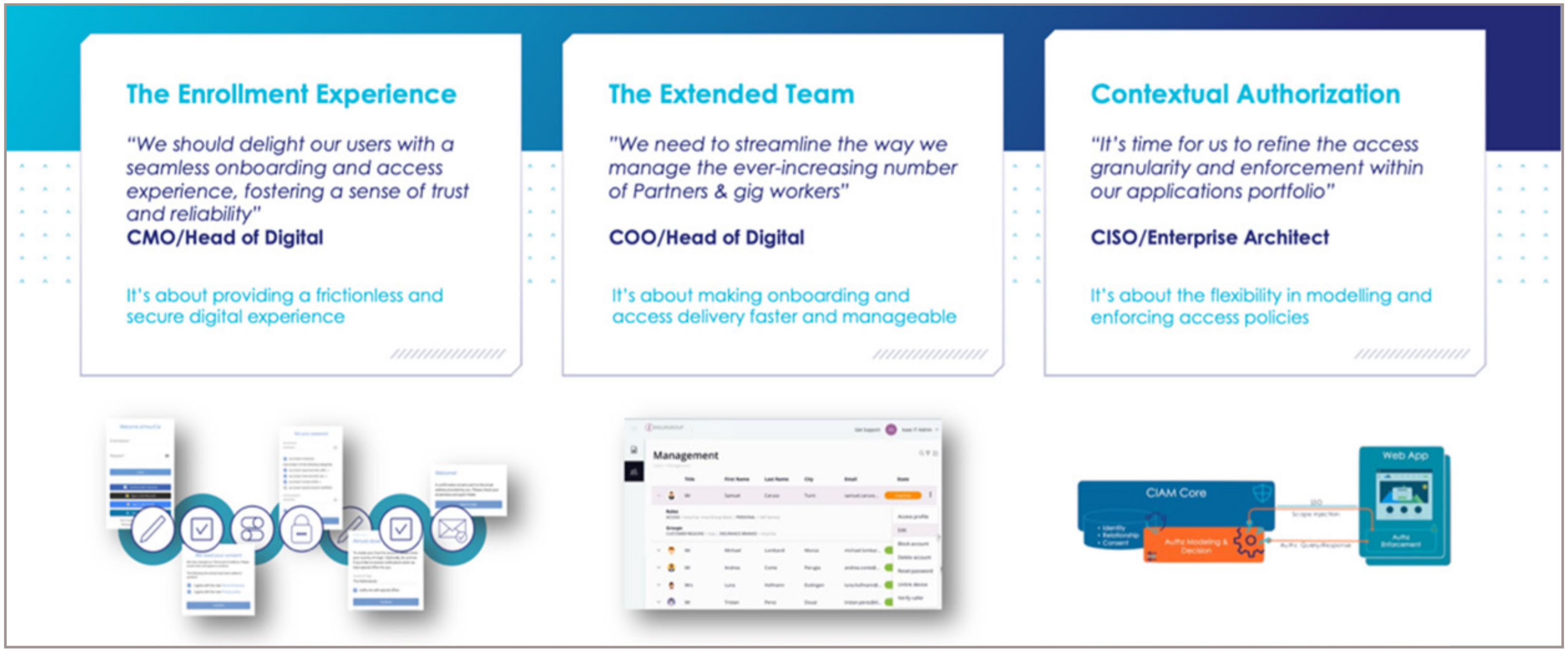
To address this, "user and access delegation" capabilities are required. The "Delegated Manager" persona, defined during organization onboarding, helps manage users effectively. They operate within their organization's boundaries managing user enrolment and access. In this context, a business user-friendly interface is essential to facilitate their tasks without requiring technical skills.

B2B features a specific extra step in the user lifecycle: "the organization onboarding" which precedes the user onboarding. Organization onboarding is required to register new business partners within a network. This is managed by what we call the "Partner Manager" persona, a business user responsible for effectively managing both the creation of the new B2B Entity and the definition of the Delegated Manager.

3 Essential Conversations in B2B IAM

B2B IAM adoption involves three crucial conversations that must be addressed collectively to ensure effective management of business relationships. Venuti, who has helped B2B enterprises around the globe, explores these conversations in detail below. He explains that each conversation brings its unique focus, triggering role and key elements.

The B2B IAM Conversations



Three conversations in B2B IAM

CONVERSATION ONE:

"The Enrollment Experience"

Objective: Create a smooth and secure onboarding and access experience that builds trust and reliability.

Key Stakeholder: Head of Digital

Key Elements: The Enrollment Experience focuses on streamlining onboarding and access, offering users a seamless and secure digital journey. It includes user journey orchestration with steps like authentication, verification, consent management, identity brokering, and attribute lookup. The aim is to design and implement an experience that balances convenience and security with the appropriate level of assurance.

CONVERSATION TWO:

"The Extended Team"

Objective: Streamline the management of access for a growing number of business partners with a focus on efficiency and scalability.

Key Stakeholder: Chief Operating Officer

Key Elements: The Extended Team conversation is focused on enhancing the efficiency and manageability of partner onboarding and access management. It involves delegation for business users, business user-friendly delegation management, and scalable approaches for flexibly managing a broad network of actors on multiple levels within your network. The goal is to establish streamlined processes and foster effective collaboration.

By creating a seamless enrolment experience, streamlining partner access management, and refining contextual authorization, businesses can establish trusted and secure relationships with their partners while ensuring efficient access controls.

CONVERSATION THREE:

"Contextual Authorization"

Objective: Refining the granularity and enforcement of access within the organization's applications portfolio, ensuring appropriate authorization levels for different user roles and contexts.

Key Stakeholder: Enterprise Architect

Key Elements: The Contextual Authorization conversation is more technically focused and involves improving the flexibility and precision of access policies. The goal is to align access policies with specific business requirements based on identity details, relationships among identities, user consent, and other security contextual aspects that are centrally managed for improved consistency for both off-the-shelf and custom applications.

Venuti highlights that the link between these three conversations is particularly important for organizations undergoing digital transformation, where two or even all three conversations may be relevant simultaneously or in a phased approach depending on the maturity and on the complexity involved.

What do these conversations look like in practice?

Let's put these conversations into practice with a real-life example. Thales recently worked with a.s.r., a leading, multi-brand insurance company with a mission to transform their B2B workarounds to optimize user experience and security.

Case Study

a.s.r.: Harmonizing fragmented B2B collaboration for seamless customer experiences

What does a.s.r. do?

As a major player in the Dutch insurance market, a.s.r. has been providing customer-friendly insurance products since 1720. Today, they offer a range of sub-brands and products.

The Challenge & How Thales Solved It

In the insurance industry, the number of business partners (brokers, resellers) can often outnumber a company's actual workforce. This is no different for a.s.r.

This creates a situation where multiple target groups need varying degrees of access, across multiple applications, through multiple channels, often across multiple brands. To increase operational efficiency, there is a need for interconnectivity to harmonize this ecosystem.

Each a.s.r. brand targets a different user group and offers a different way for customers to access their policies and systems. Working with Thales, a.s.r. took a brand-by-brand approach to re-onboarding and validating their customers brands. This helped them **unite access and registration throughout their entire B2C and B2B ecosystem, which led to a more seamless experience across their entire offering.**

The next step was to extend the unified platform to the front-end to provide customers with a better user experience by creating their own customer-friendly UI, based on business and marketing requirements. This UI functions on top of the Thales OneWelcome Identity Platform, creating a unified portal that connects through APIs to the multiple backend systems.

Results

a.s.r. can now offer a single platform that unites all brands, utilising the Thales OneWelcome Identity Platform for flexible user journey orchestration capabilities. That has led directly to less friction for customers, greater operational insight over the entire platform and a more robust approach to security and compliance challenges.

By focusing on enhancing the overall user experience, the new simplified approach provides a.s.r. with greater operational efficiencies and a more tailored offering, while at the same time with a making their customers' lives easier.

Authority Proximity: Closeness in organizational distance

Venuti highlights that B2B IAM solutions promote closer collaboration and flexibility between parties by replacing hierarchical barriers with secure, agile delegation and direct user-to-user access control. This approach ensures a seamless thread of collaboration across the ecosystem, even in situations where multiple blocks exist between the parties.

"The delegation capabilities inherent in B2B IAM enable a closer proximity between the Delegated Manager and the Business Users, facilitating a personal understanding of their specific needs. The reduced distance is ensured allowing a Delegated Manager to distribute sub-delegation when required. This is crucial for an efficient and streamlined access management process within the B2B context." Venuti notes.

This Authority Proximity benefit remains intact even as the number of managed users grows. It ensures a reasonable user-per-manager ratio, enabling personalized management while scaling effectively.

The overall result is a simplified delegated relationship that does not require IGA-like controls. In practice, this means advanced delegation introduced by B2B IAM can allow users to influence access, without depending on technical abilities.

"B2B IAM aims to strike a balance between providing sufficient access for business users to carry out their duties, while maintaining a secure environment. Effective authorization management ensures that each user has access to the necessary resources without compromising sensitive information or introducing potential security risks." Venuti explains.

Conclusion

The expansion of business networks, coupled with the integration of technology and diverse stakeholders, has amplified the challenges faced by B2B organizations.

To effectively navigate this dynamic terrain, a robust and flexible B2B IAM solution is not just an option, but a necessity. A flexible B2B IAM solution provides the foundation for secure and efficient collaboration, enabling businesses to adapt, grow, and thrive in the ever-changing B2B environment.

Want to learn more about B2B IAM?

Listen to Marco Venuti's and Martin' Kuppinger, co-founder of analyst firm KuppingerCole, recognized talk on B2B modern identity management: https://www.brighttalk.com/webcast/2037/589510

THALES
Building a future we can all trust

Contact us

For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com