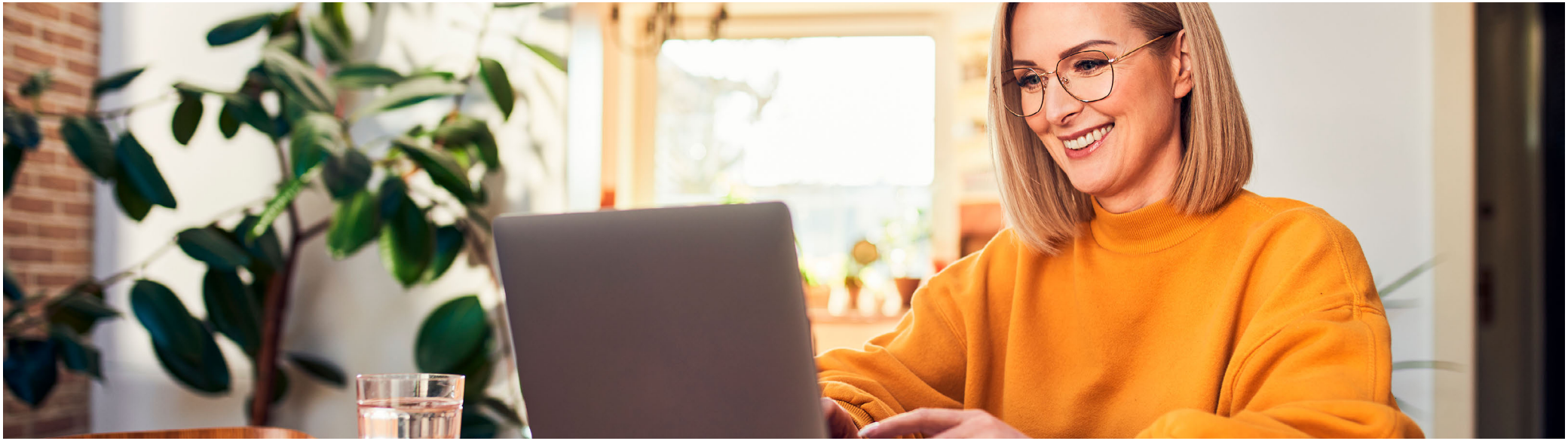
CIAM Essentials: Key Pillars for Digital Success

Demonstrating the Power of User Journey Orchestration, Externalized Authorization, and Self-Sovereign Identity

THALES
Building a future we can all trust



Introduction

With multiple options at their fingertips, consumers have little patience for obstacles at your digital front door. Research by PwC reveals that even a single bad experience can cause one in three customers to abandon a brand they previously loved, while 59% will leave after a few poor interactions.

Therefore, it is crucial to prioritize seamless user journeys and eliminate any friction that may hinder this. However, providing frictionless experiences alone are not enough.

> **1 in 3** customers will abandon a brand they love after one bad experience
>
> **59%** will leave after a few poor interactions
>
> pwc

As we progress towards a privacy-first world, brands must actively – and continually – take the right steps to earn customers' trust too. Because like with any relationship, when a person loses trust, feelings of loyalty are lost too – and can be incredibly difficult to re-establish. Regaining customer trust after a privacy breach can be a challenging, if not near impossible, task.

So, to win the battle for customer loyalty, it's essential to maintain a delicate balance. Customer Identity & Access Management (CIAM) plays a key role in this narrative. In fact, CIAM acts as a bridge between user experience, cybersecurity, privacy, and compliance: all distinct building blocks for thriving in the digital age.

In this eBook, we delve into the key identity trends and technologies that drive executives to adopt modern CIAM platforms at an accelerated pace, including:

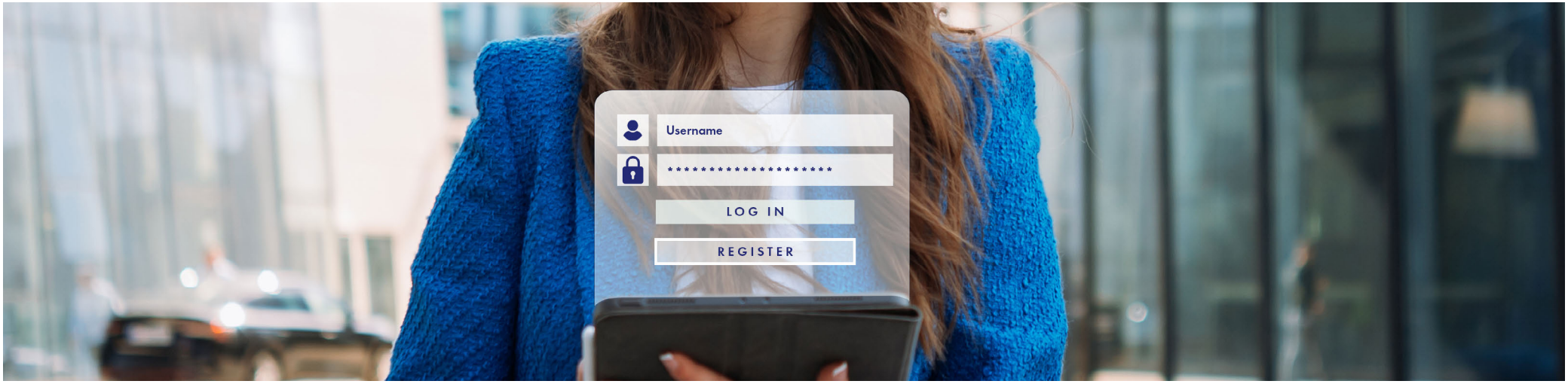
- User Journey Orchestration: streamlining customer journeys
- Externalized Authorization: simplifying and securing access control
- Self-Sovereign Identity: facilitating the shift towards a new identity model
- Technologies: to balance user experience and security

Gaining a comprehensive understanding of how these components can shape the user experience empowers you to make pivotal decisions, now and in the future.

Part 1

User Journey Orchestration

Ensuring exceptional user experiences in the moments that matter



1. User Journey Orchestration

User journey orchestration is the real-time coordination of customer experiences to encourage ongoing engagement and a positive customer experience. A robust CIAM platform will help you streamline the user journey from the point of registration to leaving.

> Customer UX is a key aspect of CIAM, as it makes or breaks the customer relationship
>
> **Gartner**

Balancing onboarding building blocks

With today's demand for fast and effortless experiences, customers must be met with easy, convenient, and relevant onboarding journeys. Anything else could result in incomplete registrations and site abandonment.

A CIAM solution simplifies the registration process, often by minimizing the information customers need to provide. User-driven features such as progressive profiling, an essential component of User Journey Orchestration, allows you ask for just enough data at the right time – and collect information based on existing customer knowledge. This eliminates the need to ask everything at once and provides a personalized experience, without turning off customers.

Giving your customers the best onboarding – no single formula

It is necessary to state that as far as onboarding goes, there is not a one-size-fits-all. The onboarding journey for a retailer may differ from that of an insurer. Ultimately, it boils down to requesting the appropriate attributes with the right level of assurance.

Figure 1: Typical retail registration flow

The figure below illustrates a widely used registration flow for a retail website:

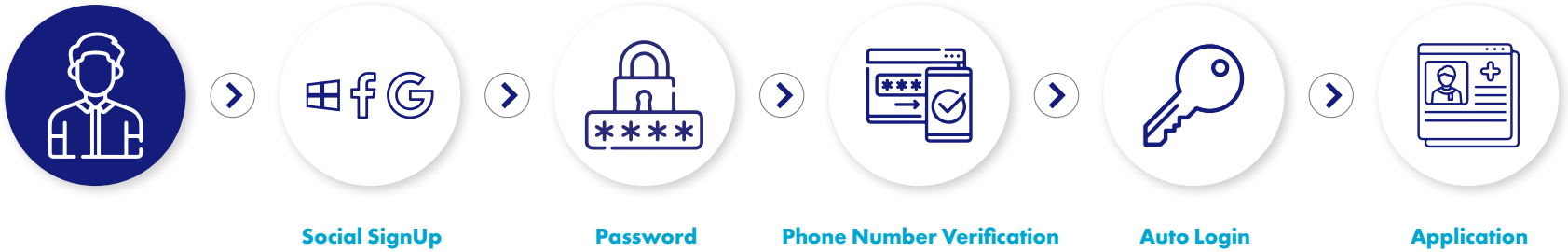
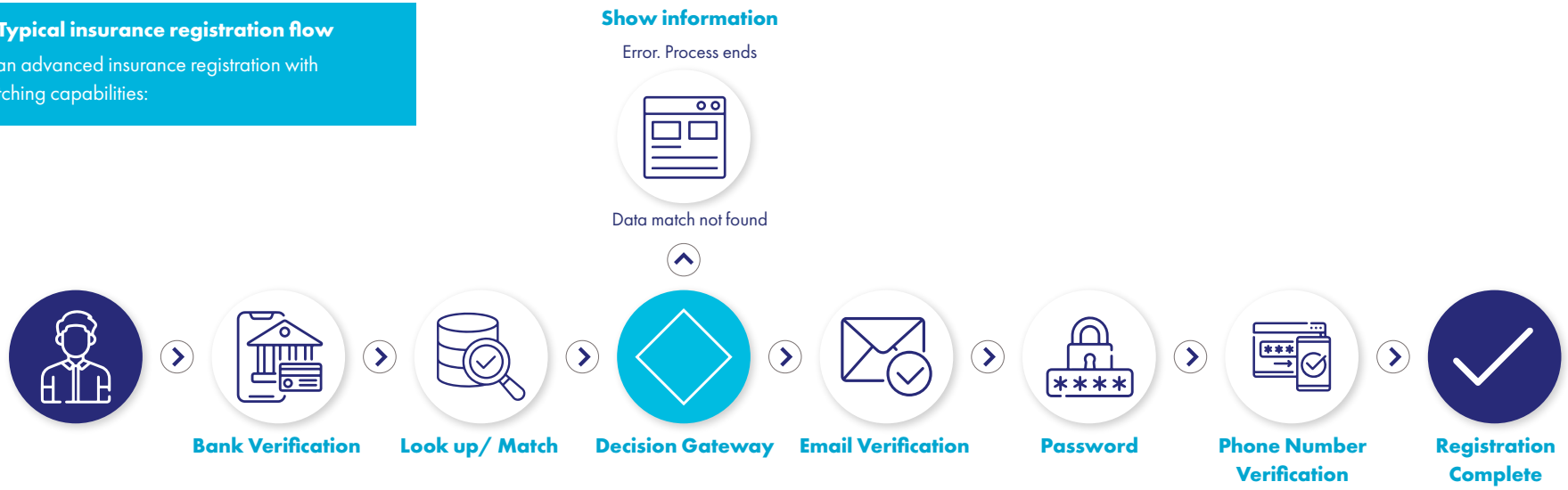


Figure 2: Typical insurance registration flow

This shows an advanced insurance registration with identity matching capabilities:



A flexible identity platform should allow brands to choose their onboarding steps so that they can orchestrate a user journey that is specifically targeted to their audience with minimum technical complexity and maintenance.

The OneWelcome Identity Platform offers an agile User Journey Orchestration application, designed to integrate diverse capabilities contributing to a fluid and secure user experience. The app gives you full control over the customer lifecycle, including onboarding, offboarding, and key moments in between. It also ensures privacy compliance throughout the customer journey.

Removing friction with single identities

The proper management of customer identities will help organizations remove friction during registration and login. This is, of course, important for brands seeking a competitive edge - that's why we listed a "frictionless customer experience" as the number one factor to include in any CIAM strategy.

> Effectively managing customer identities is the key to removing hurdles during registration and login - the gateway to the rest of your journey.
>
> **Wouter de Wit, Senior Product Manager at Thales**

On the importance of frictionless user journeys, Wouter de Wit, Senior Product Manager at Thales states "when customers have a unified identity, they can easily reuse it for multiple purchases. Achieving this level of fluidity and ease is essential for brands aiming to stand out in competition. CIAM technologies play a critical role in making this possible".

Facilitating a unified user identity across multiple brands empowers consumers to seamlessly employ their identity for repeated purchases. With features like Single Sign-On (SSO), users can access all the products they've bought from your company, regardless of brand. As a result, customers can seamlessly navigate back and forth along the buyer journey.

How can companies securely verify their customers' identities?

Identity proofing is a pivotal stage in the user journey. Moreover, identity theft is rising; an estimated fifteen million U.S. citizens had their identities stolen in 2021 alone. To combat fraudulent attempts, companies can employ a range of robust authentication technologies, such as:

Multi-Factor (MFA) or Two-Factor Authentication (2FA)

Organizations are increasingly focusing on stronger MFA adoption to protect sensitive data. MFA allows you to implement extra layers of security by asking customers for more authentication combinations, i.e., a password and a unique code sent to their mobile device or email account.

Biometric Authentication

Using biometric data, such as fingerprints or facial recognition, ensures a highly secure and easy method for identity authentication. Biometrics are hard to replicate and therefore wrap extra protection around your users' identities.

Trusted Third-Party Verification Services

One method is to use third-party digital identity verification systems. In regulated industries, such as insurance, trusted methods of authentication include leveraging verification systems like eIDAS/eID built by governments or commercially available equivalents such as FranceConnect in France, Verimi in Germany, or BankID in Sweden.

Passkey

Passkeys are cryptographic credentials that adhere to FIDO Alliance standards (an alignment developed to promote open standards for strong authentication). This method often includes scanning a user's fingerprint or utilizing facial recognition to identify them.

Document Verification

With this method you can request customers to provide scanned copies of official identity papers, such as passports. Then using recognized databases to check and verify for authenticity.

With User Journey Orchestration, you can configure authentication options specifically tailored to your security needs and user group. The important thing is to keep security, user experience, and privacy as your well-balanced north star.

Key strategies enabled by User Journey Orchestration

Extensive User Journey Orchestration solutions can help organizations improve the user experience through several strategies, including:

Progressive profiling

With third-party cookies being phased out, there is an urgent need for companies to adopt a modernized and compliant way to gather customer insights. Progressive profiling is a data collection method that lets organizations build high-quality customer profiles based on first-party data. This is key to the successful conversion from prospect to customer. While Forrester cites "one-and-done profiling" as being ineffectual and leading to lower conversion rates, progressive profiling enables incremental, user-driven data collection and transparent consent processes to build rich customer profiles – and cement trust along the way.

A single view of the customer

Choosing a CIAM system that can store identity data in a centralized place will allow you to obtain a single view of the customer, and with that, help you better understand your customer.

Increased engagement with customer insights based on tag manager input

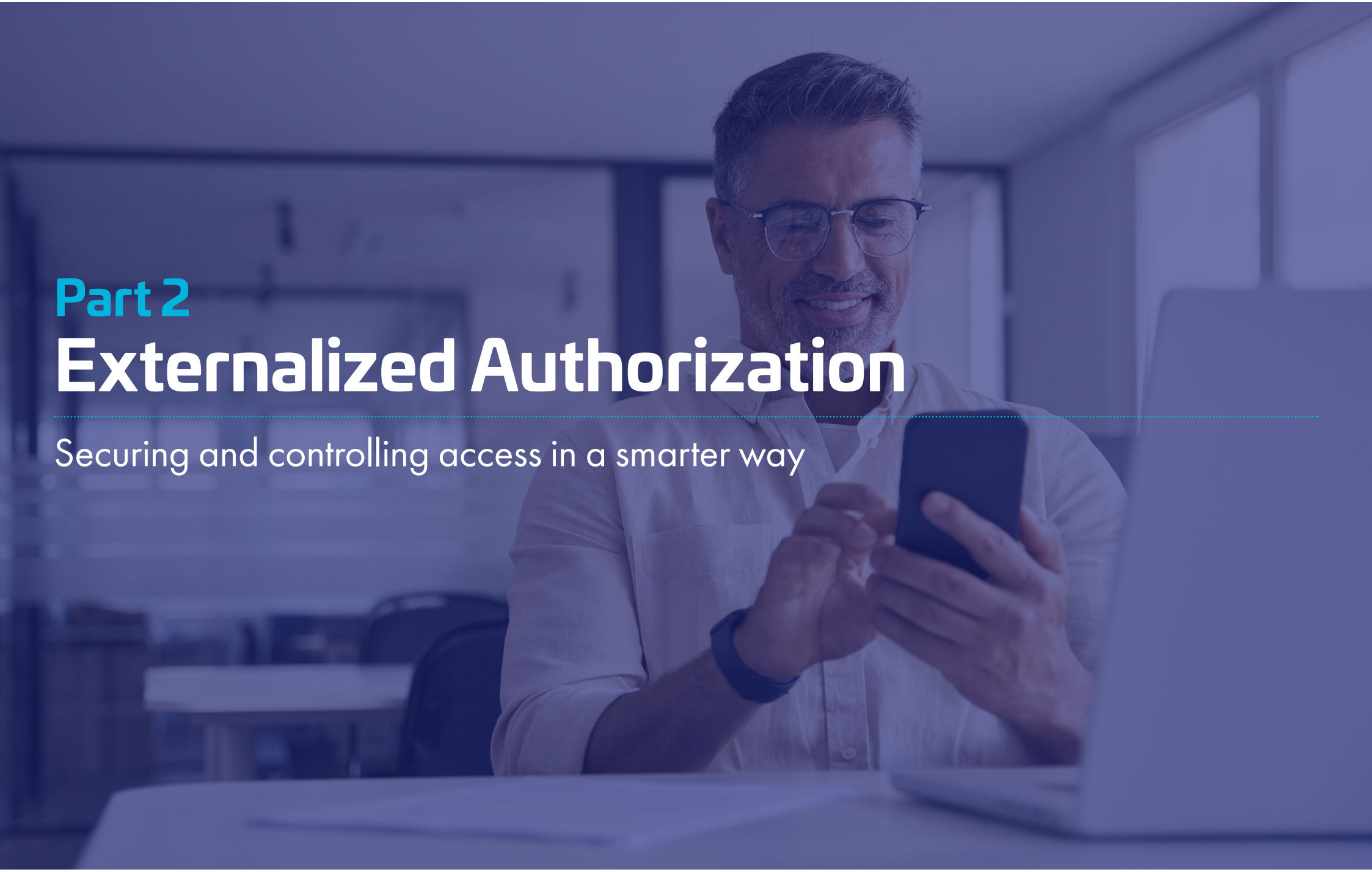
McKinsey reports that 71% of consumers expect businesses to deliver personalized digital interactions, with 76% becoming frustrated when this doesn't happen. To orchestrate a personalized user journey, near real-time insights and coordination are needed. The most comprehensive identity management solutions achieve this.

Always-On compliance

By law, organizations must often comply with a set of regulations. Non-compliance can lead to financial penalties and reputational damage. The challenge, however, is that privacy regulations undergo frequent updates, making it trickier to maintain compliance. In addition, regulations such as the General Data Protection Regulation (GDPR) in Europe, California Consumer Privacy Act (CCPA) in the U.S are getting stricter and more complex. A CIAM platform can ensure always-on compliance, safeguarding companies and individuals in parallel.

In summary

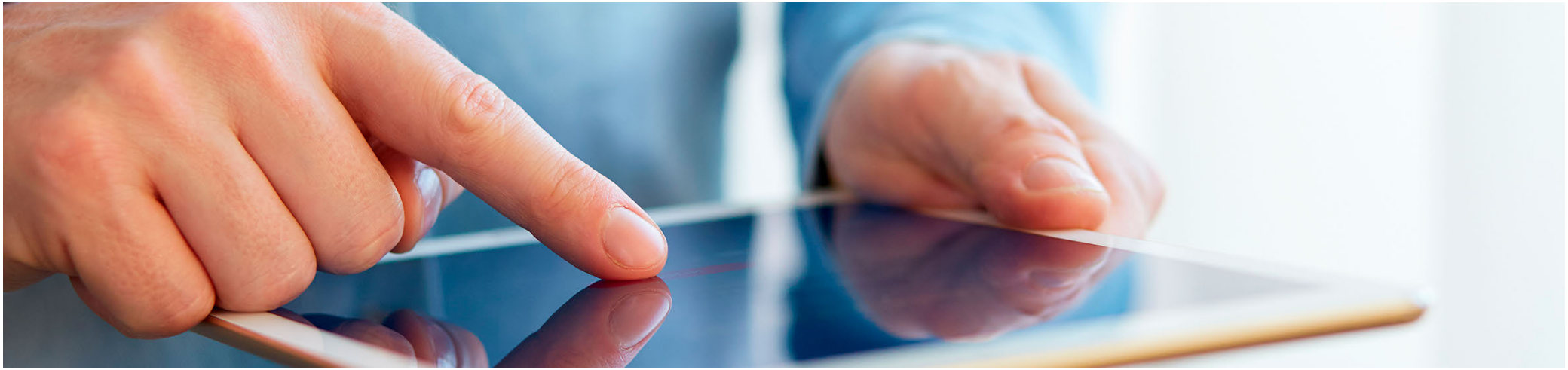
User Journey Orchestration plays a crucial role in streamlining onboarding and offboarding processes, fostering continuous engagement, and ensuring a positive overall user experience. Its ultimate goal is to deliver smooth, compliant and secure user experiences that exceeds customer expectations.



Part 2

Externalized Authorization

Securing and controlling access in a smarter way



2. Externalized Authorization

Externalized Authorization has become a critical cornerstone for successful digital transformation, and, as a result, a key driver of CIAM adoption.

And the reason is this: Fine-grained Authorization enables you to control, grant or deny access to digital services and applications on a granular level. Whether you need to control access for your partner ecosystems or for your customers directly. Fine-grained Authorization is essential for granting the right access to the right user.

> **Externalized Authorization** is a **transformative** CIAM component that unlocks multiple benefits, including enhanced user experiences and consistent security standards.
>
> **Ward Duchamps, Senior Product Strategist at Thales**

Authentication vs. Authorization

Let's start by clearing the fog about two frequently mixed-up CIAM terms: Authentication and Authorization.

Authentication validates that users are who they say they are. In most cases, systems must successfully verify many factors before granting a user access.

Authorization is the process of granting user permission on a more granular level. For instance, when a user logs into a space, Authorization determines what that user is permitted to do there. In safe environments, Authorization must always follow authentication. Customers should prove their genuine identities before being granted access to a requested resource.

Briefly stated:

- Authentication verifies identities
- Authorization grants (or denies) permissions on a granular level

Simplifying and securing access to sensitive data

Traditional access processes, especially in regulated sectors, do not fit the speed of today's world. This is where Externalized Authorization comes into play, allowing regulated sectors (and private companies) to mirror the dynamic world we live in.

Let's examine how CIAM provides seamless Authorization in a banking scenario, without compromising data security or the customer experience.

In the past, banks were dependent on lengthy, hard-coding processes, often requiring months of labor, to share access and information back and forth. Today, banks can rely on secure Authorization decisions made by a legitimate party, such as the broker.

Externalized Authorization technologies allow banks to easily, but securely, share data with trusted parties for specific operations. As a result, access and data sharing processes in banking can be faster, more user friendly and open, supported with features like strong customer authentication (SCA).

While banks are still tied to a set of strict security processes before sharing sensitive data, regulations like PSD2, a European law governing payments for both consumers and businesses, requires banks, with your consent, to grant third party access to your payment accounts.

Authorization paves the way for personalized experiences

Externalized Authorization can also drive personalization by supporting authorized stakeholder management. In a banking scenario, for instance, Authorization can help facilitate easy and legal account access to authorized third parties.

This way, banks can make it simpler for their customers to provide individuals or companies, such as relatives or accountants, with limited or full account access to manage their finances.

For instance, a user could choose to restrict access to certain accounts while providing their spouse access to a bank account to manage shared spending. Additionally, the user may choose to grant their financial advisors access to their investment accounts.

This degree of personalization has the potential to enhance the entire banking experience. Externalized Authorization has therefore become a major component of contemporary banking.

Fine-grained Authorization in other industries

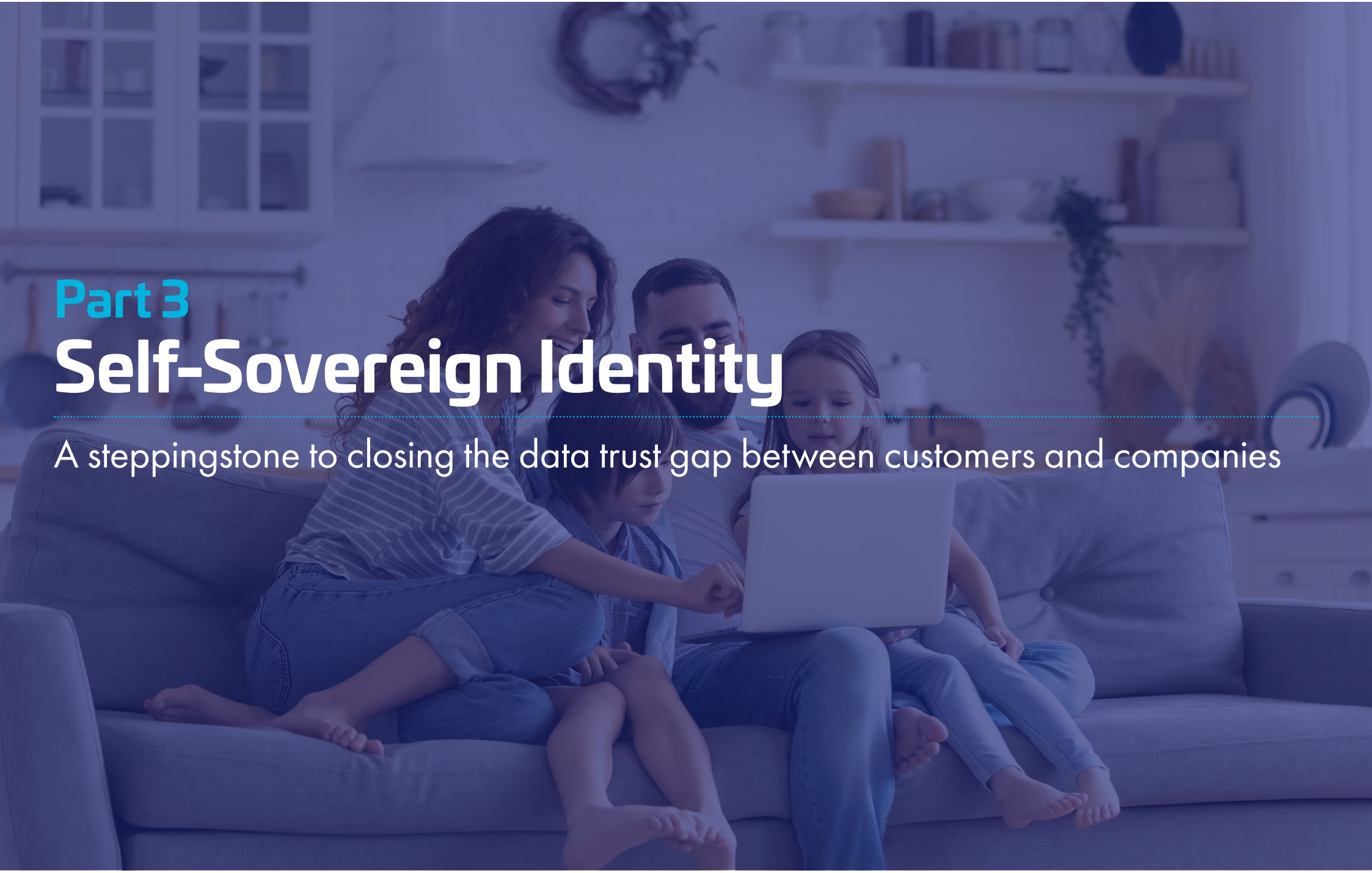
Beyond banking, fine-grained authorization is now a firmly established component of effective digital transformation. Look at health care for instance. As digital healthcare becomes the norm, patients anticipate that their information and transactions will be accessible to them and other healthcare professionals.

Whether patients are using a phone, laptop, or tablet, they want their information to be safe and private at the same time. Enabling doctors, therapists, nurses, and other practitioners to view and track their overall health over time may provide patients with higher-quality, holistic and consistent medical care.

In summary

Imagine the complex wiring needed to grant an authorized user the right access in a space where thousands – often millions – of identities operate simultaneously. Advanced Authorization tools remove the complexities in this picture, facilitating neat, simple, user-friendly and secure access to applications and digital services. It is exactly this that makes fine-grained Authorization a foundational pillar in modern business.

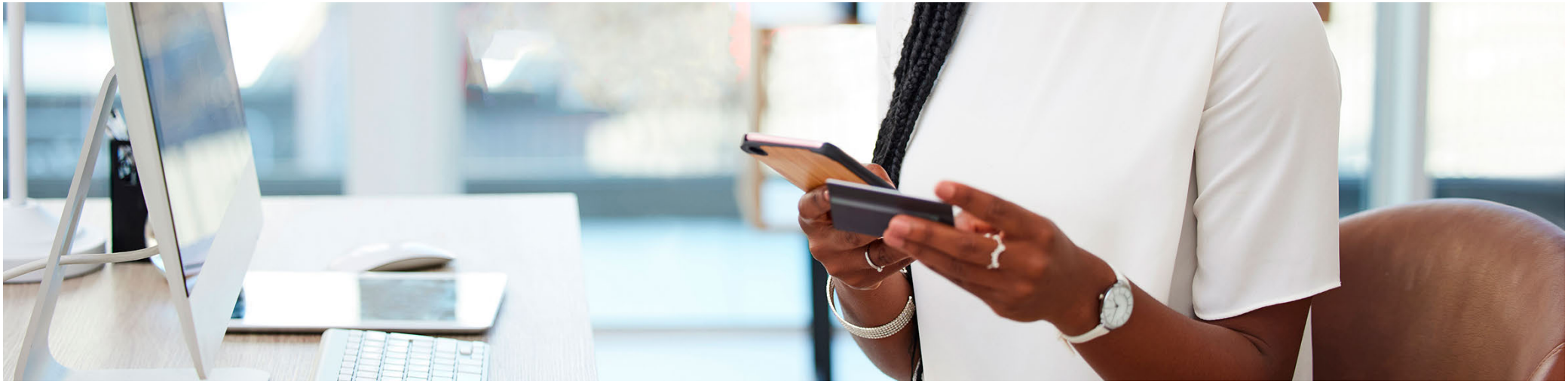
Whether you lead a financial service institution or run general medical practice, Authorization follows authentication and offers customers secure, unique and personalized experiences which can help establish trust.



Part 3

Self-Sovereign Identity

A steppingstone to closing the data trust gap between customers and companies



3. Self-Sovereign Identity

In a privacy-first era, where customers are crying out for the responsible and ethical use of their data, a new identity model is needed. Enter Self-Sovereign Identity (SSI).

What is SSI?

SSI is a privacy-first, decentralized identity model, based on the idea that individuals should have complete control of their own data.

Ward Duchamps, Senior Product Strategist at Thales, explained why the stage is set for this new identity model.

> “Customers truly care about their data – and the SSI model underpins this. Self-sovereign identity is entering the mainstream. Crucially, self-sovereign identity - and the technology underpinning it - is loved by its users. The growing focus on privacy makes SSI an essential concept in the evolving landscape of digital identities.
>
> **Ward Duchamps, Senior Product Strategist at Thales**

How does SSI work?

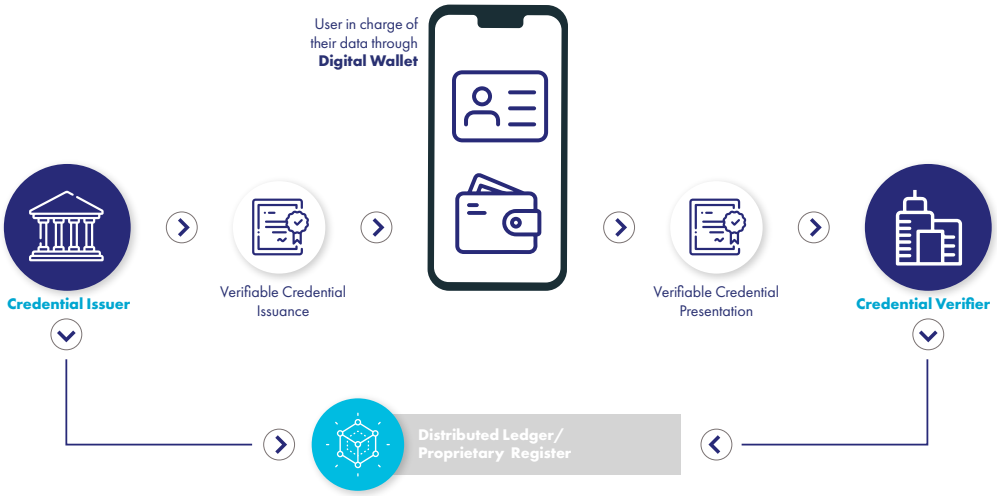
In the SSI model, citizens can store identity data in a decentralized and secure digital wallet. In general, there are three main components to the SSI skeleton:

The holder
The individual or the company that owns the digital identity. Specific information and attributes linked to this identity are stored in the form of verifiable credentials in a digital wallet app.

The issuer
The authority that issues the Verifiable Credentials.

The verifier
The party that needs to verify the credentials, this could be anything from an insurer to a retailer.

Figure 3: Components of SSI



SSI will shape identity management

Traditional consumer identity access management business cases were usually built on the following, relatively simple, equation:

Data + Consent = Personalized Journey

In the new era of identity access management, the data element is much less prominent, meaning service providers will receive less information.

People can utilize SSI to offer identity-related data in areas like school and employment records, health and insurance information, or financial data. Additionally, SSI may be applied to people, organizations, and objects (IoT).

Unlike other forms of identity verification, SSI is manipulation-proof and offers more security due to encryption and the use of decentralized Identifiers (DIDs). SSI is private and wholly owned by the user itself. And it is universal because individuals can use their SSI anywhere, anytime, even if the entity that issued it no longer exists.

What can you gain from SSI?

While SSI will require a fundamental shift in data handling, companies can harness multiple benefits from SSI, including lower risks for data breaches, reduced identity theft and simpler onboarding.

Benefits of Self-Sovereign Identity

Improved security

With SSI, companies may face lower risks for data breaches and reduced identity theft.

Stronger privacy can build customer trust

Individuals gain complete control of their own data which can generate trust.

Better UX and faster processes

With only necessary information shared, customer onboarding processes can be quicker and easier.

More inclusive

SSI can be used by people who lack conventional forms of identification. This can enhance exclusivity.

Less data = less complexities

The SSI model will reduce the amount of data you need to store and manage, making it easier to maintain compliance.

Where is the adoption of SSI currently at?

The introduction of The European Digital Identity Wallet and the updated eIDAS 2.0 regulation can accelerate the adoption of SSI in the EU as it will become mandated for public and semi-public providers.

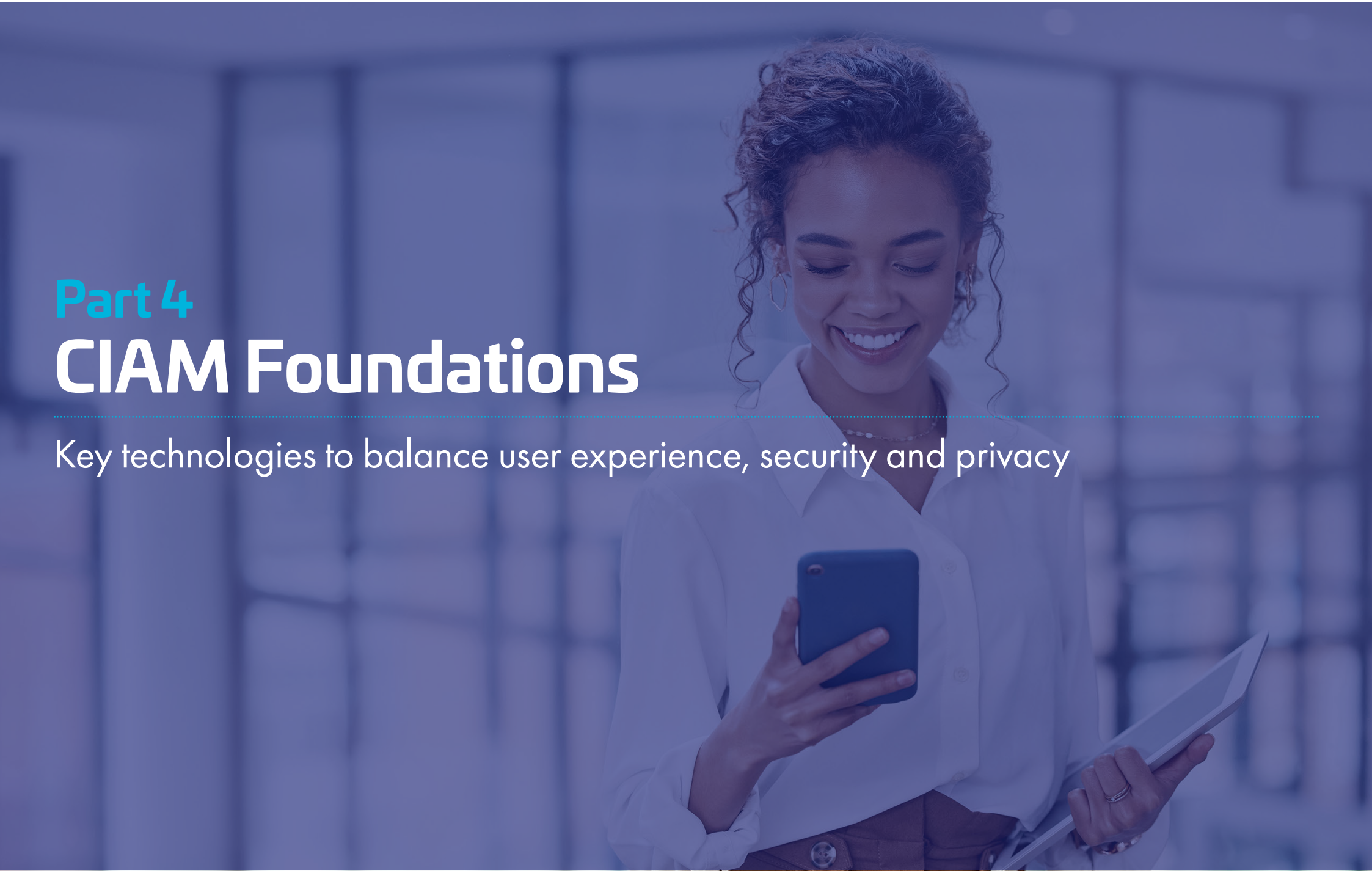
While technology is ready to accommodate this identity model, some businesses must adapt or modernize their legacy systems and in-house processes to support it. Another important question for adoption is this: Will customers trust and embrace the SSI model?

As we stride towards a privacy-first era, all signs points to a resounding 'yes!'

"We are at a tipping point in the evolution of identity access management technology where we are witnessing that SSI technology is ready, the governance landscape has paved the way for adoption and businesses are getting on board. This could trigger a fundamental change in how we deal with consumer identity. This change may, initially, at least, be disruptive." Duchamps explains.

In Summary

With SSI, customers can share personal data in a bit-for-bit fashion without having to divulge sensitive information that might be exploited fraudulently. SSI puts consumers in control of their own data – embedding privacy and security into every digital journey.



Part 4

CIAM Foundations

Key technologies to balance user experience, security and privacy

4. CIAM Foundations

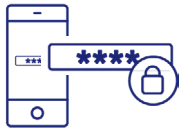
Achieving the right balance between user experience and security, starts with identifying the technologies and frameworks designed with these principles in mind, including:

Passwordless Authentication

As well as being the weakest link in the cyber security chain, passwords can be extremely frustrating for users - particularly given the volume that they must remember; more than 38 passwords on average. Passwordless authentication streamlines the user experience while bolstering security at the same time. Companies can eliminate the hassle of passwords, leveraging functionality like push-to-accept login, biometrics, or passkeys.

Single Sign-On

Single sign-on (SSO) allows customers to log in to multiple applications and websites by using just one set of credentials, requiring far less effort from users. Social logins make it easier for customers to register for a service, which can enhance conversion and reduce the number of customers who abandon their shopping carts because of the extra hassle of, say, filling out another form.



Multi-Factor Authentication

In addition to bringing extra layers of security into the authentication stage (as mentioned earlier), Multi-factor Authentication (MFA) offers customers a fast and seamless user experience. Commonly, this feature employs a combination of something a customer knows (such as a code), something that they have (often their smartphone) or something related to who they are (like their fingerprint or face).

Bring Your Own Identity

Bring Your Own Identity (BYOI) simplifies the registration process by enabling users to quickly and easily access services using credentials stored by a third-party identity provider (IdP), such as Facebook or Google. CIAM enhances the security of BYOI by providing the right infrastructure, updating attributes and deactivating accounts when necessary.

Ongoing Compliance

CIAM technologies address essential requirements for safeguarding personal information on public networks and help global enterprises comply with diverse and constantly evolving privacy laws across borders.

In summary

CIAM is the foundation of cybersecurity, but it also drives effortless, simple and fast customer experiences. Features such as passwordless authentication, single sign-on and multi-factor authentication, can help strengthen cyber defenses, while simultaneously delivering efficient, positive customer experiences that integrate seamlessly into customers' busy lives

Conclusion

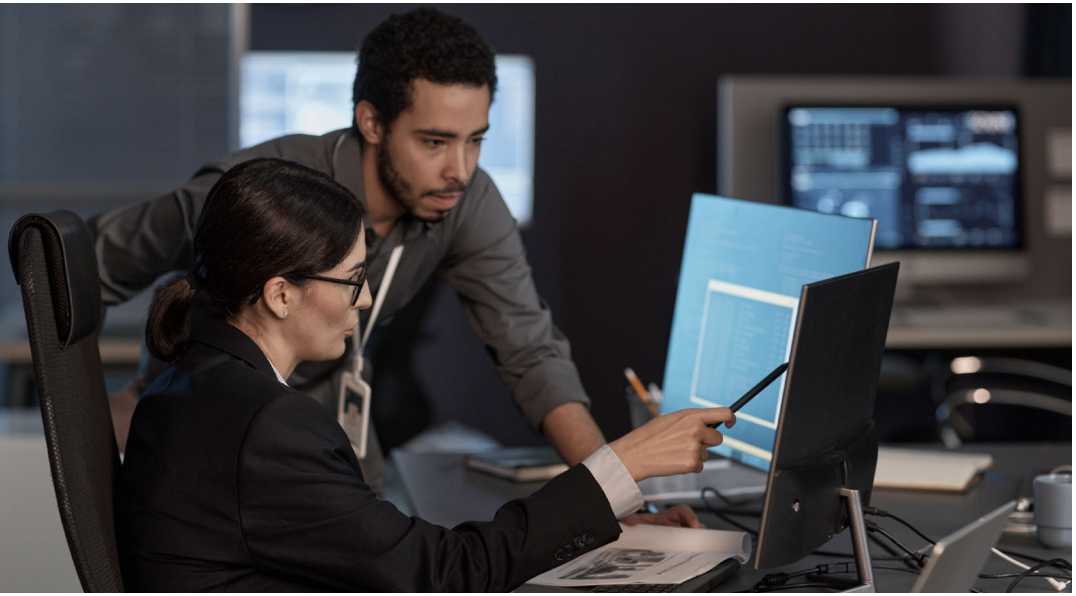
Although today's landscape poses real challenges related to user experience, security, data privacy, and compliance, companies can overcome these by implementing a robust, adaptable, and user-friendly identity platform.

Customer Identity and Access Management (CIAM) has emerged as a crucial element in striking the right balance between user experience, privacy, and security, all while requiring minimal technical maintenance.

Distinct capabilities such as strong authentication, progressive profiling, externalized authorization, and support for new identity models have made CIAM, as a product category, a key cornerstone for digital success—a fact that is increasingly recognized.

> Organizations implementing a unified CIAM solution can expect a remarkable 30% improvement in customer retention and a notable 50% reduction in customer data breaches by 2024.
>
> **Gartner**

The Thales OneWelcome Identity Platform seamlessly integrate smooth and trusted user experiences across your entire digital network. The result is a trusted, user-friendly and compliant journey that keeps customers returning.



Talk to our CIAM experts

Our team of experts is fully prepared to assist you in harnessing the complete value of CIAM. Get in touch with our experts to learn what Thales can do for your business via https://cpl.thalesgroup.com/contact-us

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centres to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

THALES

Building a future we can all trust

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

cpl.thalesgroup.com