eBook

Top 6 CIAM Deployment Pitfalls and How to Avoid Them

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

(Clickable)

Digital Business Starts with CIAM

As business models become increasingly digitalised, companies must deliver seamless, secure, and personalised experiences to customers while also reliably safeguarding sensitive data. It all starts with Customer Identity and Access Management (CIAM). By successfully deploying an effective CIAM, companies ensure their customers and other external users have secure, compliant, and convenient access to digital services. However, 52% of enterprise wide digital initiatives, including CIAM deployments, fail to meet their outcome targets[1]. This underscores the need for a more strategic approach to planning, implementing, and configuring CIAM tools.

In this eBook, we explore **six common missteps** that cause CIAM deployments to fail. We also explain the tested deployment practices developed by Thales – based on innovative technologies, proven best practices, and decades of experience – which enables us to ensure successful CIAM deployment and support companies in achieving their digital transformation goals.

[1] Gartner 2025 CIO Agenda

Why CIAM Deployments Go Wrong

Despite heavy investment and intensive implementation projects, many enterprises deploy CIAM solutions only to later discover that their chosen tools do not deliver the results they had intended. In our experience, there are six key obstacles that can seriously undermine the effectiveness and value of a CIAM system:

Lack of Business Alignment

IT and business teams often have different priorities and metrics. Without alignment, CIAM solutions fail to meet user needs, compliance requirements, or business objectives.

Scalability & Performance Issues

Quick fixes may address immediate needs but fail to support long-term growth. Poorly designed systems struggle with high user volumes, leading to slow authentication and service disruptions.

Complex, Costly Integrations

CIAM must integrate smoothly with legacy and cloud systems; otherwise, deployment becomes expensive and inefficient.

Poor User Experience

Complicated logins and slow authentication frustrate users, increasing abandonment rates and reducing engagement.

Security & Compliance Gaps

Weak authentication and poor access controls expose businesses to breaches, fraud, regulatory fines, and reputational damage.

Internal Resistance & Delays

Lack of stakeholder buy-in and poor change management slow adoption and create implementation roadblocks.

These issues often result in unforeseen security vulnerabilities, frustrated users, and wasted investment, preventing businesses from fully leveraging CIAM's potential. However, these pitfalls are avoidable. Thales offers the support and technology that businesses need to implement CIAM successfully, ensuring seamless integration, strong security, regulatory compliance, and a frictionless user experience. Below, we'll explore how Thales helps organisations overcome these challenges and achieve CIAM success.

Fail #1:
Lack of Business Alignment

A CIAM deployment can only succeed if it aligns with business objectives, user needs, and compliance requirements. Many organisations approach CIAM as just another IT project, rather than a strategic enabler. This disconnect leads to mismatched priorities, inefficiencies, and poor adoption.

Why it Fails ⊗

CIAM solutions must enhance engagement while balancing security, compliance, and operational efficiency. However, misalignment between departments often leads to delays, inefficiencies, or poor deployment outcomes. For example, an e-commerce retailer may implement CIAM to improve security, but if IT prioritises strict authentication policies while business teams focus on frictionless checkout, the result could be a complicated login process that frustrates customers and increases cart abandonment, directly impacting revenue.

Similarly, industrial and manufacturing firms rolling out supplier and distributor portals need IT, security, and operations teams to collaborate on access policies. Without alignment, IT may enforce overly restrictive controls that disrupt workflows, or business leaders may push for looser security, exposing sensitive data to risk. These conflicts slow deployment, introduce security gaps, and reduce the overall effectiveness of the CIAM solution.

Common issues

Lost Revenue	Access Mismanagement	Operational Inefficiencies	Data Exposure

How Thales Fixes It ✓

Thales ensures business and IT are aligned from the start, creating a CIAM strategy that serves both security and financial goals. Here is how we ensure CIAM deployment is built around business priorities:

Collaborate

We engage with stakeholders from IT, security, marketing, and operations to develop a CIAM strategy that enhances both security and user experience.

Adapt

We provide adaptive identity management solutions, allowing businesses to define flexible access policies based on user roles, behaviours, and risk levels.

Customise

We tailor authentication workflows to meet industry-specific needs, ensuring seamless access across multiple platforms without compromising security or compliance.

Comply

We ensure compliance-readiness with built-in support for GDPR, HIPAA, PSD2, and other industry-/region-specific regulatory frameworks, reducing legal and operational risks.

By bridging the gap between business goals and IT capabilities, Thales helps companies deploy CIAM solutions that are ready for success: secure, scalable, and aligned with real-world needs.

Fail #2: Scalability & Performance Challenges

A CIAM system must support high user volumes, peak traffic, and global accessibility without slowing down or failing. Many organisations underestimate scalability needs, leading to performance bottlenecks, authentication delays, and system outages that leave customers unhappy and damage the brand's reputation.

Why it Fails ⊗

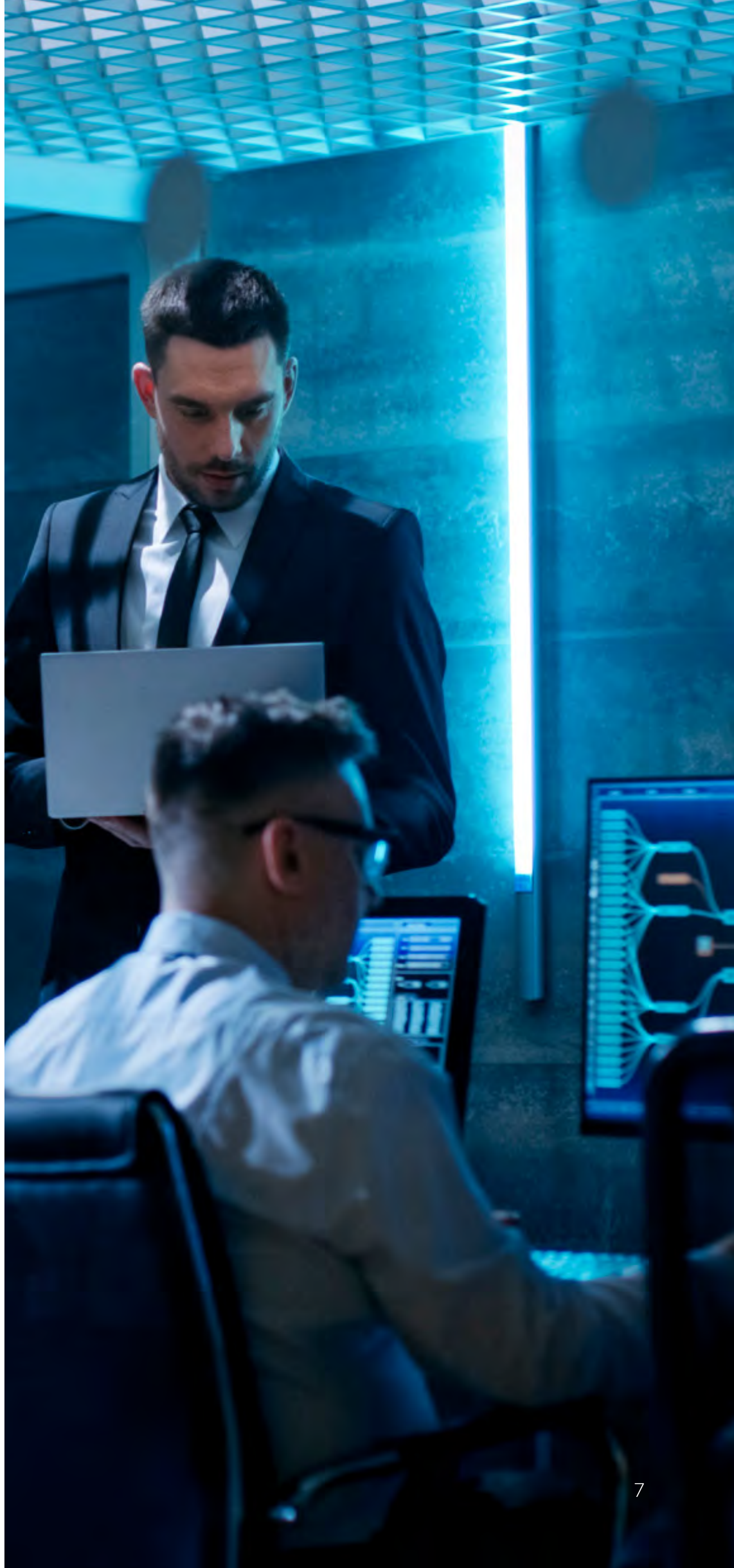
Surges in user activity can overwhelm an unprepared CIAM system. For example, during monthly payroll periods or tax season, online banking platforms may experience a dramatic spike in login attempts. If the system can't handle the load, customers may be locked out of their accounts, unable to access funds or complete urgent transactions—eroding trust and damaging the bank's reputation.

During seasonal sales like Black Friday or Singles' Day, retail companies must accommodate high volumes of logins within minutes. If their system lags or crashes under the pressure, frustrated customers may abandon their carts, leading to significant revenue loss.

Seamless authentication across multiple regions is also critical for many global companies. For example, a multinational insurance provider without cloud-based scalability may see policyholders encountering delays or login failures when trying to file claims or access documents—especially after a widespread event like a natural disaster. This can lead to dissatisfaction, regulatory risk, and customer churn.

Common issues

Login Failures	System Overload	Revenue Loss	Regional Access Issues



How Thales Fixes It

Thales delivers high-performance CIAM solutions that ensure seamless access, even under extreme load conditions. That is why our CIAM technology incorporates key capabilities to ensure scalability and performance:

Cloud-Ready

Thales' CIAM platform is built on cloud-native infrastructure, ensuring seamless scalability across global deployments.

Performance Optimisation

Smart authentication flows minimise latency, ensuring fast and frictionless logins for users worldwide.

High Availability

Advanced failover and redundancy mechanisms guarantee 99.99% uptime, even during traffic spikes.

Global Reach

Distributed identity services ensure users experience fast, reliable authentication no matter where they are.

With Thales, businesses from private enterprises to state-owned organisations can confidently scale their CIAM systems to support millions of users, high-traffic events, and international expansion, all without compromising on security or performance.

Fail #3:
Complex, Costly Integrations

For a CIAM solution to effectively add value, it must seamlessly integrate with existing applications, legacy systems, cloud environments, and third-party services – without disrupting operations that rely on these systems. However, many organisations find integration to be one of the most time-consuming and expensive aspects of CIAM deployment. Poor planning, incompatible technologies, and rigid authentication frameworks lead to delays, disrupted operations, security vulnerabilities, and excessive costs.

Why it Fails ⊗

Deployment challenges often arise when CIAM solutions must integrate with complex, multi-system environments, leading to delays, inefficiencies, and unexpected system clashes. For example, a global airline deploying CIAM for passenger logins, loyalty programs, and travel agency portals must integrate multiple legacy booking platforms. These integrations must be carefully planned, or else conflicting system requirements will stall deployment, raising the costs and extending the timeline of the project. Even after launch, authentication errors may disrupt ticket purchases and loyalty point redemptions, which damages relationships with customers and partners.

Many media and entertainment companies are facing a similar challenge now. When rolling out subscription-based streaming services, they need smooth integration with payment gateways, content delivery networks (CDNs), regional identity providers, and other systems. If deployment is rushed or mismanaged, incompatibilities between new and existing systems can create persistent login failures or payment authentication issues, delaying time to market and resulting in lost subscriptions.

Common issues

Integration Delays	High IT Costs	Legacy System Issues	Authentication Errors	Payment Failures

How Thales Fixes It ✓

Thales simplifies CIAM deployment by offering flexible, integration-ready solutions that work with both modern cloud applications and legacy infrastructure. Key benefits include:

Pre-Built Connectors

Thales provides ready-to-use integrations for CRM, ERP, HR, and e-commerce platforms, reducing the need for costly custom development.

Seamless IAM Integration

Thales ensures smooth interoperability with existing IAM and security ecosystems, enabling frictionless authentication across enterprise applications.

Multi-Cloud Compatibility

Organisations can deploy CIAM across AWS, Azure, Google Cloud, and on-premises environments without running into compatibility issues.

API-Driven Architecture

Developer-friendly APIs simplify authentication workflows and enable smooth third-party integrations with minimal effort.

Identity Federation

Integrations with external identity providers like Google, Microsoft, and regional authentication systems ensure seamless third-party authentication.

Cross-Platform Access

Thales enables Single Sign-On (SSO) across multiple applications, allowing users to move between services without reauthenticating.

With Thales, businesses accelerate CIAM deployment, minimise costs, and ensure smooth authentication experiences across all digital touchpoints, regardless of any complexity.

Fail #4:
Poor User Experience

A CIAM system must be both secure and user-friendly. Overcomplicated registration flows, slow authentication, and clunky interfaces frustrate users, leading to higher abandonment rates and lower engagement. When security measures add unnecessary friction, customers quickly lose trust.

Why it Fails ⊗

Strict password policies and frequent resets can help prevent fraud, but they can also create unnecessary friction. Nearly one third of customers (31%) rank password resets as a major source of frustration[3]. If an e-commerce brand forces customers to go through tedious login steps or repeated identity verification, for example, it may drive them to abandon purchases and switch to competitors.

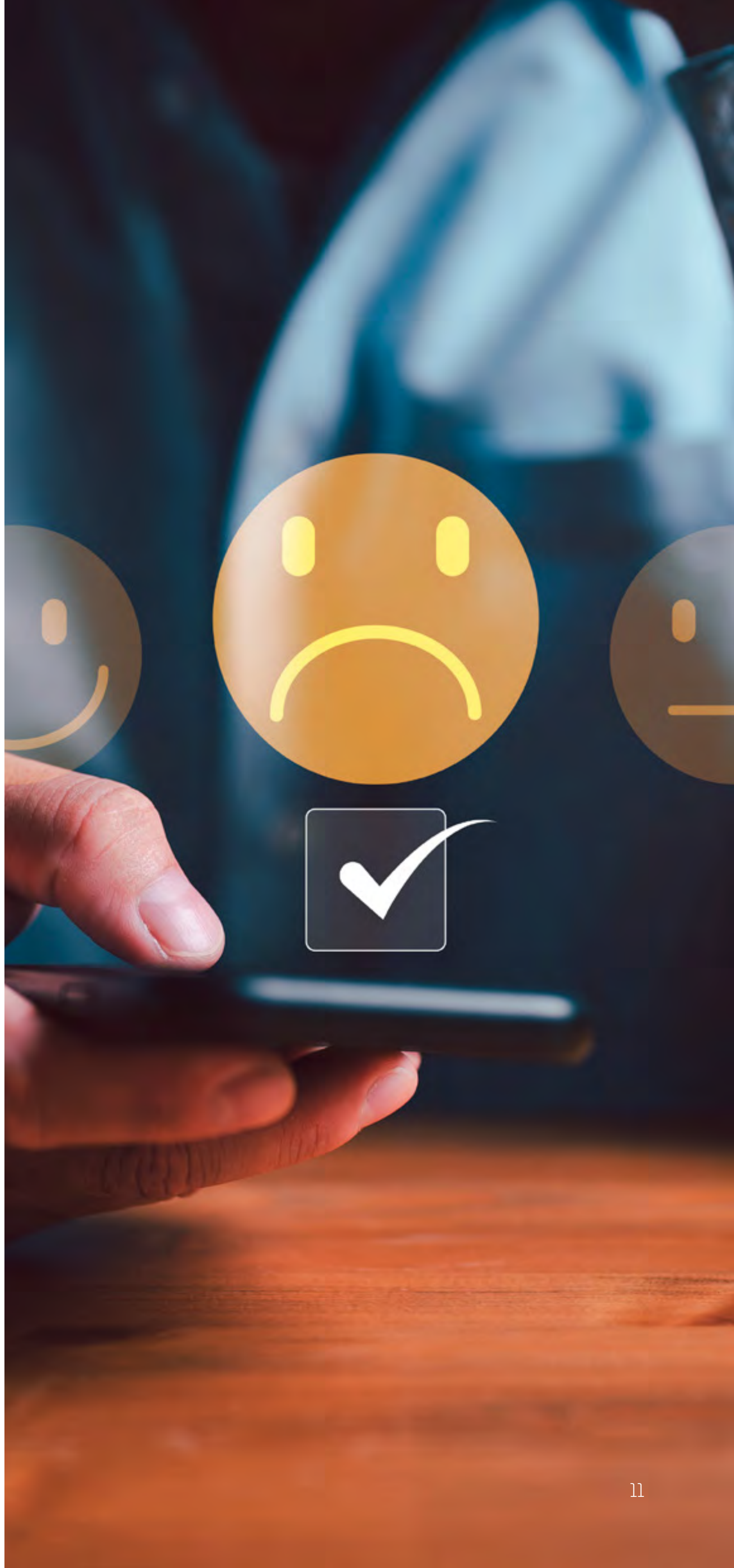
Around one third (28%) of customers also say they are frustrated by having to input the same data more than once with companies they already do business with[4]. A smart home technology company could create friction if it launches a CIAM system without Single Sign-On (SSO) across devices. If customers must log in separately for their smart thermostat, cameras, and mobile app, this fragmented experience discourages product adoption and reduces customer loyalty.

Complex identity verification steps or requests for data can push users away during onboarding. For example, a telecommunications provider requiring multiple redirects, unclear error messages, or excessive requests for personal data all at once may drive customers away from its self-service portals altogether, leading to higher call centre demand and increased operational costs.

Common issues

Lost Revenues	Account Abandonment	Damaged Trust	User Frustration	Support Overload

[3] 2025 Thales Digital Trust Index
[4] 2025 Thales Digital Trust Index



How Thales Fixes It ✓

Thales CIAM solutions are designed with user experience and engagement in mind. That is why we incorporate user-friendly capabilities, such as:

Frictionless Authentication

Thales simplifies authentication with adaptive MFA and identity verification, applying extra security only when necessary to keep access fast and seamless.

Customisable Workflows

Businesses can tailor authentication flows to balance security and convenience, ensuring compliance without frustrating users.

SSO and Social Login

Users can authenticate once and access multiple services effortlessly, reducing login fatigue and improving engagement.

Progressive Profiling

Data collection requests are dispersed throughout different stages of the user journey rather than bombarding the user with complicated data requests during the crucial onboarding stage.

By ensuring strong security and compliance in the background while delivering a seamless user experience at the front end, Thales helps businesses retain customers, enhance engagement, and reduce support costs.

Fail #5:
Security & Compliance Gaps

Weak security controls and poor regulatory compliance put businesses at risk of data breaches, legal penalties, and reputational damage. Keeping up with constantly evolving regulations adds even more complexity. Organisations must continuously monitor the regulatory landscape and ensure enforcement – without disrupting operations. If a company fails to implement strong, compliant authentication, and data protection measures, it exposes them to breaches, major penalties, and reputational damage.

Why it Fails ⊗

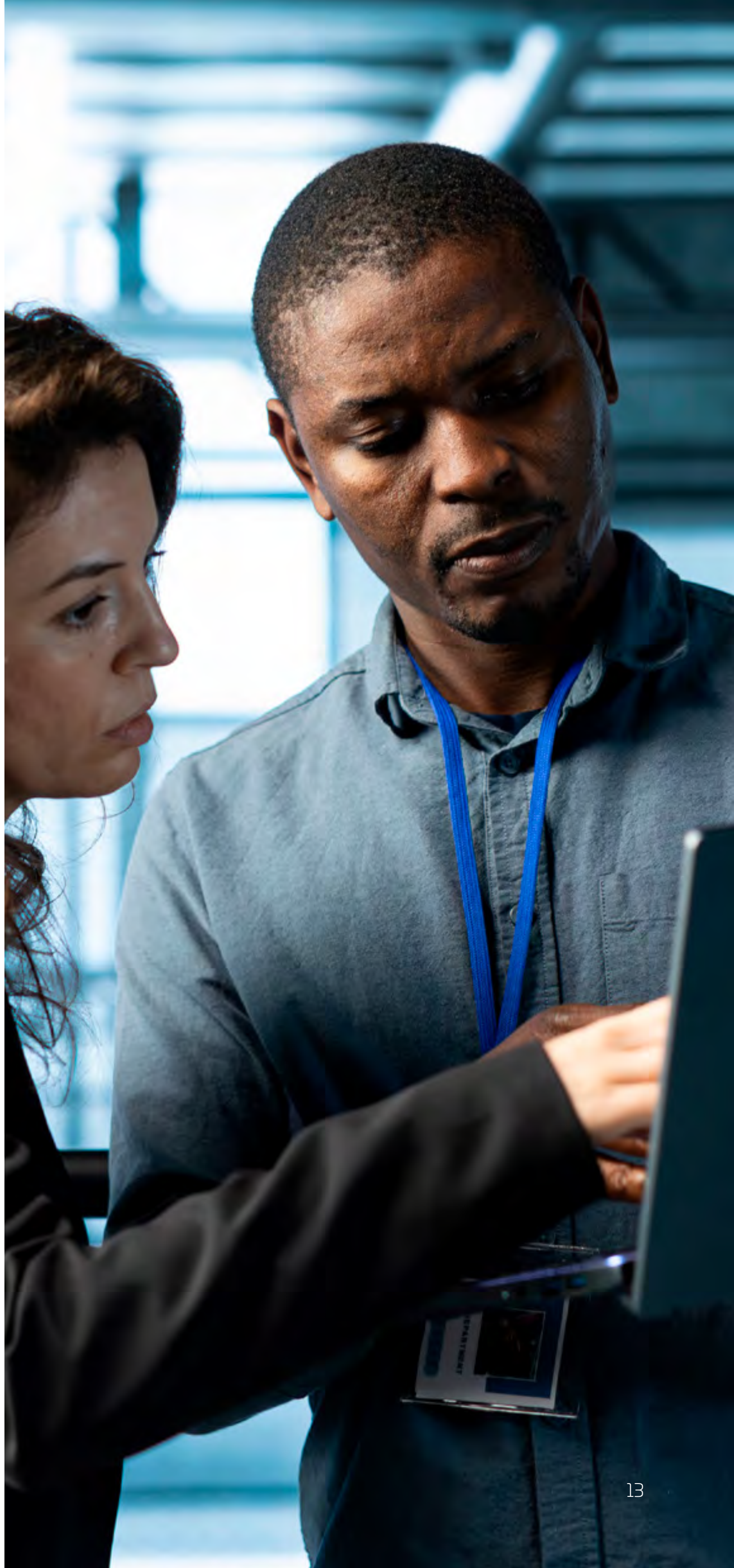
Insufficient Multi-Factor Authentication (MFA) is a common vulnerability. A healthcare provider storing patient records online may rely solely on password-based authentication, making it easier for attackers to gain unauthorised access. A data breach in this scenario could result in severe regulatory violations and damage to the organisation's reputation.

Poor password management also introduces risk. If a company allows customers to create weak, easily guessed passwords without enforcement policies, it becomes a prime target for credential-stuffing attacks. If customer accounts are compromised, the company could face fraud claims, legal action, and regulatory fines under regulations like GDPR or CCPA.

In addition, regulations are constantly evolving. This requires businesses to manually track, adopt, and enforce new compliance measures. Failure to comply with regional data protection laws can have costly consequences. A tech company expanding into the European market may not fully implement GDPR-compliant data storage and consent management. This oversight could lead to hefty fines and restrictions on doing business in the region.

Common issues

Data Breaches	Legal & Financial Risks	Higher Operational Workloads	Reputational Harm



How Thales Fixes It

Thales takes a proactive, multi-layered approach to CIAM security. Our solutions combine advanced capabilities that protect customer identities, ensure a seamless user experience, and maintain continuous compliance through automated enforcement:

Advanced Authentication

Thales enforces adaptive MFA, passwordless authentication, and biometric verification, preventing unauthorised access while keeping logins seamless.

Regulatory Compliance

Thales CIAM solutions align with GDPR, CCPA, HIPAA, and other regulations, reducing legal risks and ensuring data protection.

Strong Encryption

Built-in end-to-end encryption protects sensitive customer data, ensuring compliance with global security standards.

Risk-Based Security

Intelligent threat detection identifies suspicious login attempts, applying additional security measures only when necessary.

By combining robust security, compliance-ready solutions, and frictionless authentication, Thales helps businesses protect customer identities, avoid regulatory penalties, and build long-term digital trust.

Fail #6:
Internal Resistance & Implementation Delays

Even the most advanced CIAM solution can fail if internal teams struggle to adopt it. Resistance to change, stakeholder alignment, lack of an intuitive back end, and inadequate training slow down deployment, create inefficiencies, and reduce internal user engagement. Without a positive UX and clear implementation strategy, organisations risk delayed CIAM deployments, frustration among users, and wasted investment.

Why it Fails ⊗

Mismanaged change often leads to internal pushback. For example, a large manufacturing company transitioning to a centralised identity system for employees, contractors, and suppliers may face resistance from IT and security teams accustomed to managing separate access controls. If stakeholders are not involved early, they may view the new CIAM system as disruptive rather than beneficial.

Inadequate training can also leave employees unprepared. A multinational media company rolling out SSO and MFA for remote teams may assume users will adapt quickly. However, without proper onboarding and support, employees may struggle with new authentication flows, leading to productivity loss and increased IT support tickets.

Poor executive buy-in is also a common challenge. A healthcare organisation integrating CIAM for patient portals and medical staff might experience delays if leadership fails to see the immediate value. Unless there is support on the C-level, funding and resources may be diverted to other projects, stalling deployment indefinitely.

Common issues

Change Resistance	Skill Gaps	Poor Stakeholder Alignment	Low Adoption & Engagement

How Thales Fixes It ✓

Thales helps organisations overcome resistance and implementation challenges with a streamlined, intuitive back-end system designed for ease of integration and engagement, along with our structured, support-driven approach:

Comprehensive Change Management

Thales works closely with organisations to align stakeholders, address concerns, and ensure smooth CIAM adoption.

Executive-Level Engagement

Thales helps demonstrate CIAM's business value to leadership, ensuring strong commitment and resource allocation.

Expert Training and Support

Dedicated training programmes help IT teams, security personnel, and end-users transition seamlessly to the new system.

Ongoing Guidance

With continuous knowledge transfer and technical support, Thales ensures businesses maximise the benefits of their CIAM investment.

By focusing on tailored change management, training, and stakeholder engagement, Thales helps organisations accelerate adoption and ensure long-term CIAM success.

CIAM Deployment: Too Important to Fail

At every stage of their digital journey, customers expect smooth, secure experiences. Your company's CIAM is a vital opportunity to make a positive first impression, to gain trust, and establish a consistent user experience. Because CIAM is literally the gatekeeper to your business, it is essential to get it right.

Thales offers enterprises a strategic, technology-driven approach to CIAM deployment that aligns with your business needs and sets you on a path to further innovation. We deliver high-performance, scalable solutions that fully integrate into your existing IT ecosystem. They enhance user experience while enforcing robust security. As a full-service partner, we have the experience and expertise to guide organisations through implementation and adoption, ensuring that your CIAM solution delivers value and helps you achieve your digital transformation goals.

The future of digital business relies on two factors: trust and convenience. Achieve both with Thales as your trusted CIAM partner.

Global Enterprises Trust CIAM from Thales

Overall leader in KuppingerCole Leadership Compass for Access Management

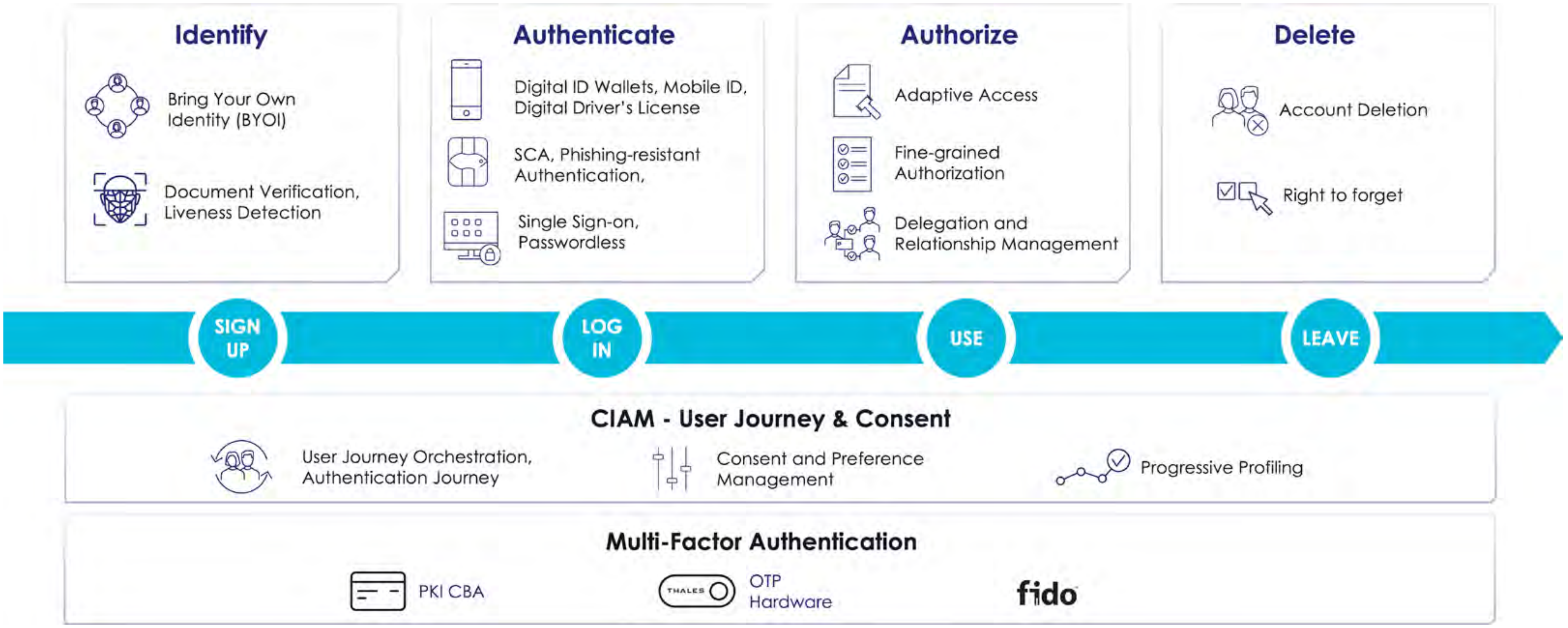
More than 35,000 Thales customers

17,500 digital identity experts worldwide

2024 Microsoft Security Excellence Award: Identity Trailblazer

Supporting the User Journey
from Start to Finish with CIAM

Thales solutions engage and protect external users, giving them secure, frictionless access to your company's digital assets at every stage of the user lifecycle.



Identify

Bring Your Own Identity (BYOI)

Document Verification, Liveness Detection

Authenticate

Digital ID Wallets, Mobile ID, Digital Driver's License

SCA, Phishing-resistant Authentication,

Single Sign-on, Passwordless

Authorize

Adaptive Access

Fine-grained Authorization

Delegation and Relationship Management

Delete

Account Deletion

Right to forget

SIGN UP

LOG IN

USE

LEAVE

CIAM - User Journey & Consent

User Journey Orchestration, Authentication Journey

Consent and Preference Management

Progressive Profiling

Multi-Factor Authentication

PKI CBA

OTP Hardware

fido

Comprehensive **CIAM Solution** from Thales

Thousands of organisations around the world trust Thales Customer Identity and Access Management (CIAM) solution every day. Our comprehensive CIAM systems balance security, user experience, and compliance. Thales offers a unified identity platform to empower organisations to manage customer identities in a way that builds trust and drives engagement.

Key capabilities

Bring Your Own Identity (BYOI) & Social Login

Enable users to authenticate using existing social or enterprise identities with OAuth 2.0 and OpenID Connect.

Multi-Factor Authentication (MFA)

Add layers of security by requiring multiple forms of verification, protecting against unauthorised access.

Identity Federation

Use OAuth 2.0 and SAML to integrate external identity providers (IDPs) like Google and Microsoft, allowing seamless cross-platform authentication.

Identity Verification

Authenticate and validate user identities to prevent fraud, ensure secure access, and comply with data protection regulations.

Strong Customer Authentication (SCA)

Enhance security and comply with regulations using passkeys and robust authentication measures.

Risk-Based Authentication (RBA)

Adapt authentication processes based on user behaviour and risk assessment to minimise fraud.

Single Sign-On (SSO)

Allow users to access multiple services with a single login, simplifying the user experience.

Passwordless and Passkeys

Eliminate the need for passwords, enabling easier and more secure user re-engagement.

Consent & Preference Management

Build trust and ensure compliance by transparently managing user consent and preferences.

Progressive Profiling

Gradually collect user data to develop rich customer profiles without overwhelming them.

Delegated User Management

Streamline access control by allowing designated users to manage roles and permissions.

Externalised Authorisation

Establish consistent access policies based on user attributes, enhancing security and compliance.

OAuth 2.0 & API Security

Secure access to applications and services with OAuth 2.0-based authorisation, protecting APIs and enabling controlled access to sensitive data.

Fraud and Risk Management

Ensure only legitimate users gain access to digital services, protecting against fraudulent activities.

User Journey Orchestration

Personalise interactions and optimise engagement by tailoring user journeys.

About Thales

As a global leader in cybersecurity, Thales safeguards sensitive data, identities, applications, and software for the most trusted brands in the world. Through advanced encryption, identity access management, application security, and software entitlement, Thales secures cloud environments, defends against cyber threats, ensures compliance, and enables trusted digital experiences.

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

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