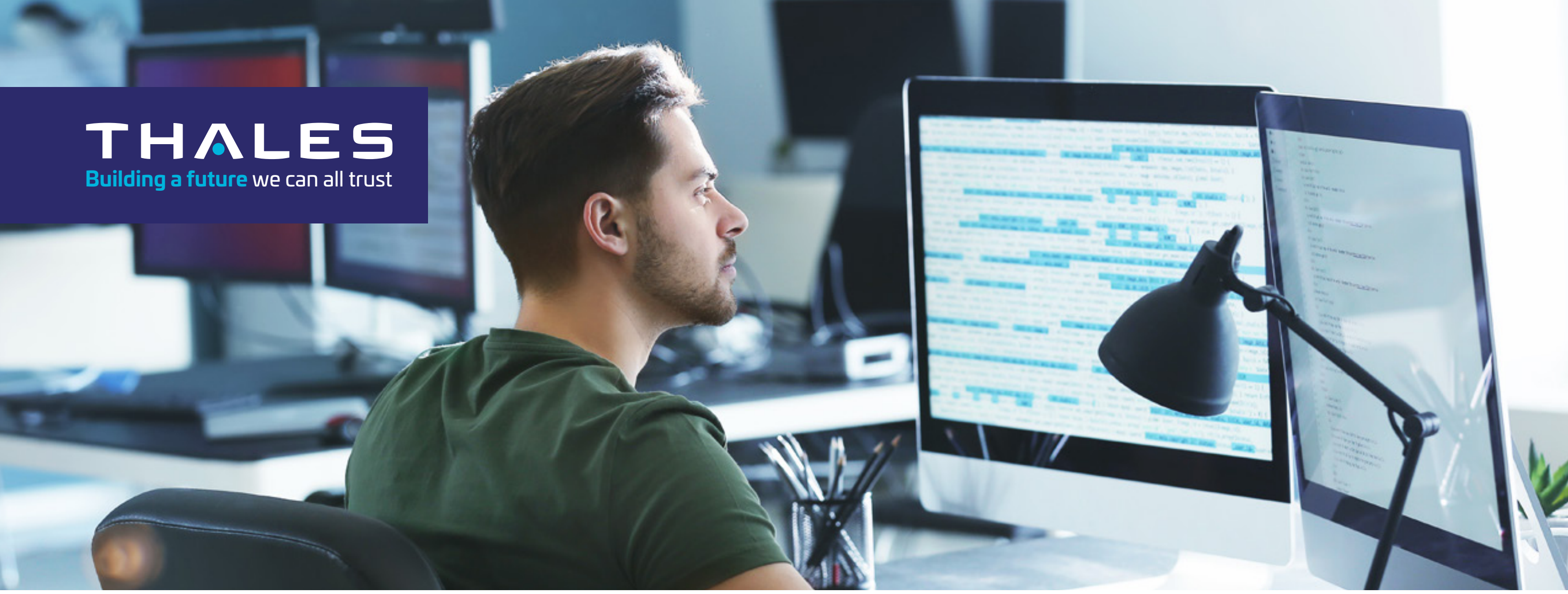
CIAM DIY vs. BUY

Making the Right Choice for Your Insurance Organization

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents



Introduction

Deciding whether to build or buy your Customer Identity and Access Management (CIAM) solution in the insurance industry requires careful evaluation of several critical factors: functionality, integration complexity, specialized expertise, regulatory compliance, always-on requirements, and time to value.

1. Understanding the Complexity of Building

Building a CIAM solution internally requires more than technical skills - it demands integration of diverse components, adaptability to customer needs, and ongoing commitment. In the insurance industry, where consumer trust can be hard to earn, a CIAM platform can play a crucial role in rebuilding confidence by offering secure, personalized experiences. As you navigate this complex process, it's essential to be aware of the specific challenges that can arise.

To better understand the potential pitfalls, let's explore the main challenges when building a DIY CIAM solution:

1. **Functional Complexity**
   CIAM has evolved beyond simply managing customer logins. Nowadays, it involves frictionless onboarding, omni-channel access, data privacy compliance, data validation, managing diverse user types, and accommodating emerging technologies.
2. **Integration Complexity**
   Standards change. SAML has been the go-to for logins for years, but standards like OpenID Connect, FIDO, and SCIM are now vital. Navigating this shifting landscape can be challenging.
3. **Specialized Expertise**
   Building a CIAM solution internally isn't just about offering functionalities. Ensuring configurability, seamless integrations, and comprehensive documentation, while also future-proofing the solution, requires a specialized, dedicated team.
4. **Always-on Requirements**
   An effective CIAM system should be constantly accessible and capable of handling traffic surges. It also needs to be resilient against cyberattacks and compliant with necessary certifications.
5. **User Lifecycle Mangement**
   Deliver a consistent user experience, reduce security risks and harbor trust is by ensuring a CIAM solution can manage the entire user journey, from onboarding to offboarding, with seamless access and consistent security.
6. **Time to Value**
   CIAM projects are complex, involving multiple stakeholders and intricate decision-making phases. This can lead to lengthy planning and infrastructure dependencies, causing delays in time-to-value.

2. Key considerations for your DIY CIAM

For companies committed to a DIY approach, it's crucial to be aware of the key risk factors that can make or break the implementation. Here are some key risk factors that insurance companies should consider ensuring that their DIY CIAM implementation remains robust and trustworthy.

1. Functional Complexity

□ **Balance security with frictionless onboarding:** Are your security protocols robust while still allowing for a smooth and easy registration process for users?

□ **Ensure omni-channel login support:** Does your solution allow users to access their accounts seamlessly across all devices and platforms, while delivering a consistent and user-friendly experience?

□ **Validate data and provide integration with external ID sources:** Does your system support integrations with trusted external IDs, like government, bank IDs, or social logins, to streamline authentication?

□ **Manage access for diverse user types:** Have you implemented role-based access controls (RBAC) and delegation capabilities to efficiently manage consumers, business users, partners, and guests?

□ **Stay compliant with data privacy regulations:** Is your solution updated regularly to meet evolving data privacy laws (e.g., GDPR, CCPA)?

2. Integration Complexity

□ **Stay current with evolving standards:** Are your systems up-to-date with important CIAM standards like OpenID Connect, FIDO, and SCIM?

□ **Navigate complex security protocols:** Do you have a clear strategy for managing and implementing Public Key Infrastructure (PKI) within your CIAM system?

□ **Handle versioning challenges as standards mature:** Is your IT team prepared to manage versioning and updates as industry standards evolve, ensuring your CIAM solution remains compatible and secure?

3. Specialized Expertise

□ **Build a dedicated team for CIAM development:**
Do you have a specialized team in place focused on the development, maintenance, and enhancement of your CIAM solution?

□ **Evaluate resource allocation for long-term commitment:**
Have you assessed and allocated sufficient resources to ensure ongoing support and development of your homegrown CIAM platform?

□ **Ensure CIAM platform has configurability, seamless integrations, and comprehensive documentation:**
Is your solution flexible enough to meet your needs, integrate smoothly with other systems, and provide thorough documentation?

□ **Handle versioning challenges as standards mature:**
Are you prepared to manage updates and changes as CIAM standards evolve and new versions are released?

4. Always-on Requirements

□ **Implement 24/7 monitoring for incident detection and resolution:**
Do you have continuous monitoring in place to quickly detect and resolve incidents, ensuring system uptime and reliability?

□ **Ensure resilience, scalability, and security for the CIAM system:**
Is your DIY solution designed to be resilient and scalable, with strong security measures to handle varying loads and potential threats?

□ **Maintain robust infrastructure:**
Are your data centers, DevOps practices, and security protocols well-established and capable of supporting a reliable CIAM environment?

□ **Regularly update and make configuration changes with minimal downtime:**
Do you have a process for applying updates and configuration changes that minimizes system downtime and disruption?

5. User Lifecycle Management

□ **Automate deprovisioning and compliance:**
Do you have the automated processes in place to regularly and efficiently remove inactive or obsolete users while ensuring compliance with privacy laws and data retention policies?

□ **Reduce security risks:**
Are you deprovisioning users immediately after their accounts become inactive to minimize security vulnerabilities?

□ **Enhance system efficiency by maintaining an up-to-date user base:**
Do you regularly review and update your use base to enhance system performance and minimize resource waste?

6. Time to Value

□ **Assess internal expertise and resources:**
Do you have the skills and capacity to build and maintain the CIAM solution?

□ **Estimate project complexity and timeline:**
Have you planned for the full scope, including potential delays?

□ **Plan for system integration:**
How will your CIAM solution integrate seamlessly with existing systems?

□ **Consider ongoing maintenance needs:**
Do you have the resources to handle post-launch support and updates?

□ **Evaluate dependencies on other initiatives:**
Are there critical projects relying on the timely delivery of your CIAM solution?

3. An Alternate Path: Pre-Built Solutions

If these challenges seem overwhelming, consider a CIAM solution that's backed by experts and prebuilt with your industry in mind. These out-of-the-box platforms offer faster time to value, reduced costs, and minimized risk. By incorporating industry best practices, such platforms not only simplify implementation but also enhance consumer confidence through secure, personalized experiences that help address the trust gap in the insurance sector. They provide ongoing vendor support, resulting in a more reliable and secure CIAM solution.

With a robust and agile solution like the Thales OneWelcome Identity platform, you can focus on your business and your customers and know that your CIAM needs are in good hands. Not only has our solution been recognized as an overall leader in CIAM by Kuppingercole, but it's also designed to be modular – mix and match what modules you need to achieve your identity objectives at your own pace.

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