The Perfect RFP Questions for CIAM

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

Introduction:

If you're looking for a CIAM vendor, it's vital you get the answers you need to make an informed decision.

Over the last decade we have seen hundreds of different RFPs, from an enormous range of different companies and in our experience, these are the most important questions that need to be addressed. Where possible, we recommend tailoring these questions to suit your specific needs.

1. Company Profile

Implementation of a complex system like CIAM usually results in long-term partnerships, so it's important that you get a general sense of the company you're dealing with – and not just focus on current functions and features. Are they an established company, or are they owned by Private Equity? Do they have a vision for the future? Can you rely on them to deliver what they promise for years to come?

1. Can you describe the business of your company in relation to the field of Cyber Security as a whole?
2. How many colleagues are working in this broader field?
3. How many colleagues are associated with IAM and how many with CIAM?
4. Are you private equity owned or listed on a stock exchange?
5. Are you profitable?
6. Where are your headquarters, product management, professional services, and support located?
7. Can you provide details about your background and experience in implementing CIAM solutions?
8. How many clients do you currently serve with your CIAM offering?
9. What are the 3 largest single deployment of these services?
10. Can you elaborate how your offering differentiates for B2C, B2B and B2E IAM?
11. Is it possible to provide 3 relevant reference cases in our industry?
12. Please provide reference to your achievements on CIAM analyst reports?
13. What consultancy partnerships do you have in place that could be beneficial to us?
14. Are you an existing partner that provides services to any part of our organization, outside of IAM?
15. Could you outline areas where your organization has made substantial contributions within the realm of CIAM?
16. Are you making continual investments in CIAM innovation, development and technology? Please provide details and examples.

2. Platform Functionality

When it comes to the platform itself, it is vital that you collect as much relevant information as possible – not only to fulfil your immediate needs, but also long-term requirements. That includes information about data storage, authentication, automation, federation and consent. Is there a delegated user management capability? How about mobile identity? Or external authorization? What about integration and infrastructure capabilities? It may seem like a lot, but world-class vendors should be able to easily answer all of the questions below.

Identity Storage

1. What system is your data model based on? And can it support multiple identity schemas?
2. Is your solution flexible enough to let us create new schemas specific to the attributes we require?
3. Will it be possible for us to also collect meta data (red to the NIST8112)? If so, what sort of meta data can be collected?
4. We need as little friction as possible for the end-user with data migration. Please explain your migration strategies, with regards to I hashed passwords?
5. How do you deal with duplicate accounts?
6. What session management capabilities do you offer?
7. Do you have a central location that stores all generated events? Can you provide a brief explanation of how it works?
8. Can you provide different information based on the specific user, or a business application the user is trying to access?
9. Can you provide details on your reporting capabilities? What are some of the metrics these reports can measure?

Registration and Onboarding

1. Please explain how your platform offers the ability to automate the customer journey from registration and beyond?
2. Can you support different onboarding journeys based on the user persona, branding or sales channel?
3. Does your solution allow us to design custom registration workflows that are tailored to the specific needs of users?
4. What are your progressive profiling capabilities?
5. Do you provide integration with tag manager to analyse and optimize the user journey?
6. Do you provide the ability to automate customer engagement workflows, such as personalized recommendations or targeted marketing campaigns, to help us build stronger relationships?
7. Is it possible for customers to manage their own profiles by updating their own data, preferences and see their event history?
8. How will we be able to quickly adapt to new innovations (i.e a new digital wallet that gains popularity) so users can register through channels they are more comfortable with?
9. As technology and consumer preference evolve, will we be able to support identity wallets, zero knowledge proof attributes and claims providers?
10. Can we integrate solutions like Know Your Customer (KYC) processes into our user onboarding process?

Authentication and Federation

1. Do you support SAML?
2. Do you support OIDC?
3. Do you Support Oauth Device flow for IoT integration?
4. Is your solution FIDO certified?
5. Can you list the other protocols that you support for authentication (e.g. Radius)?
6. How does your solution connect with external applications for identity verification?
7. What social identity providers (e.g. Google, Facebook, Apple) do you support?
8. Can customers use these Social IDs to quickly create prospect logins?
9. Which National Identity Schemes (eIDs) can you provide support for, when it comes to onboarding and authentication?
10. Does your platform allow users to login using Government IDs and/or Bank IDs?
11. Can you integrate with decentralized identities and self-sovereign identity wallets?
12. What methods do you offer for passwordless authentication?
13. Does your solution support FIDO Passkeys?
14. Does your solution support synced and device-bound Passkeys?
15. Will it be possible to request integration with additional IDPs in the future? What process do you have for this?

Consent & Preference Management

1. What is your vision for addressing and supporting GDPR and other regional privacy regulations?
2. What processes have you established for policy and document consent?
3. Do you support document consent in multiple languages?
4. Do you support different policies for different business lines?
5. Please describe how you support consent on user data and attribute level as defined in GDPR?
6. Do you support multiple processing purposes per user attributes?
7. Do you support life cycle management for processing purposes?
8. Is document and attribute consent configurable in a point and click manner?
9. How have you implemented double opt-in?
10. Do you allow users to manage their own consent and attribute preferences in a compliant manner? Can users withdraw their consent at any time?
11. In addition to providing consumers with consent confirmation, will we also be able to implement a detailed approach to the lifecycle management of that consent?
12. Do you have a model that allows us to add identity attributes and flexibly store personal preferences, interests, and profile information, regardless of the communication channel?
13. How do you support real-time synchronization of consent items across other business applications?
14. Do you provide a User Interface (UI) that we can easily apply our branding to, where users can view, change, or withdraw consent through their profile page?
15. Can users easily view, edit, download, and delete their data?
16. Is it possible for us to choose to use our own portal with the aid of your consent-API?
17. Can you describe, in detail, the process for sunsetting processing purposes?

External (B2B) User Access Management

1. What are your methods for registering and validating third party organizations in your IAM system?
2. Can you describe the processes for the onboarding of users from third party organizations?
3. What functionalities do you have for managing access of users from third party organizations?
4. Do you offer a launch pad for applications the user is entitled to use?
5. Can user management be delegated to hosts in third party organizations?
6. Do you support invitation and activation flows?
7. Does your solution provide the possibility for a single user working for more than one company to be given distinct levels of access?
8. Do you support a flexible onboarding journey depending on the persona of the business user?
9. How does your platform ensure we are giving the right access to the right people?
10. How does your solution manage offboarding when users leave the business?
11. Can your platform handle different sorts of business customers (commercial, non-profit, resellers, institutions, etc.) and offer them the right experience without requiring specific training?
12. Is your solution flexible enough to accommodate gig workers, temporary contractors and guest users?
13. Do you support multiple hierarchies in parallel, such as geo and division?
14. Does your solution offer Role Based Access Control (RBAC)?
15. Does your platform offer a clear, intuitive UI to help efficiently manage external business users, such as agents and brokers?
16. Does your platform offer an intuitive point-and-click UI for managing roles and groups?
17. How can role management, group management and role assignment be delegated?
18. Do you support both fine-grained and dynamic access, based on the Open Policy Agent?
19. In cases where users cannot manage their own account, or need intervention to regain access, do you support mandating or 'on-behalf-of' authorization? And is it possible to provide a full audit trail of the activities performed?
20. Can you provide a scalable approach to the administration of access rights, allowing application or process owners to create, manage and delegate role administration?
21. From an architectural point of view, can your delegation management system integrate with other identity stores?
22. Is there a way to automate group memberships, role assignments or change attribute values?
23. Is it possible to customize the UI with our own look and feel, using our logo and brand guidelines so that it looks and feels like an integral part of our brand identity?
24. Can we tailor the UI/UX to specific user personas, such as business users, delegated managers and power users?
25. Do you provide the ability to empower delegated managers to confer the same delegation management rights they own (also known as Delegation Chaining)?

Mobile Identity

1. Do you offer a secure mobile application that serves as both an authenticator app and an end-to-end mobile app security platform?
2. What ready-made, customizable mobile security features do you offer?
3. Is it possible to create customer mobile apps with tier-one security?
4. Do you support other forms of identity verification, such as passwordless access via passkeys? If so, where are the passkeys stored?
5. Can we apply our own branding to the mobile authenticator app?
6. Is the authenticator functionality included in the Software Development Kit (SDK)?
7. Can the SDK offer direct communication channels such as push messages?
8. What are the supported frameworks for your SDK?
9. What authentication options does your mobile application provide?
10. How does your mobile application control flows and traffic? What encryption do you offer?
11. Is it possible to exchange data without needing to share usernames or passwords?
12. How is management and control of the rules and policies configured?
13. How does your platform ensure secure web and mobile communication?
14. What are some of the different ways a user can register with the app?
15. How does mobile authentication work and what methods can be used?
16. Do you offer App2App SSO?
17. When it comes to error handling, if users are unable to fix the error on their own, what solutions do you provide?

Fine-grained Authorization Capabilities

1. What is your approach to fine-grained, externalized and dynamic authorization management?
2. Do you support both fine-grained and dynamic access, based on the Open Policy Agent?
3. Do you offer an out-of-the-box authorization service that reduces complexity and improves time-to-market?
4. Is it possible to consolidate all authorization decisions into a single component to ensure consistent enforcement of authorization policies?
5. Will there be a way for us to separate policy management from the application lifecycle?
6. Do you provide a no-code, or low-code, environment where policies can be edited?
7. Do you support complex authorization policies that are a combination of contextual elements?
8. Is it possible to integrate the externalized authorization app into your cloud platform?
9. Can you provide a clear flow chart outlining how your externalized authorization solution works?
10. How can you ensure API back-end users and devices are protected?
11. Will it be possible for policy administration to be integrated into our environment?
12. Can you provide a clear explanation of how policy validation works?
13. How does your solution define permissions?
14. What are some of the most popular mechanisms we can use to integrate with Externalized Authorization?

Infrastructure, Integration & APIs

1. When it comes to infrastructure, what are the specific design drivers your technology strategy is built around?
2. Do you have design principles that you adhere to? If so, can you provide further details about each individual principle?
3. Can you provide a high-level overview of your technical architecture, including components per client instance, generic components and connectors.
4. Is it possible to integrate your infrastructure into our existing CRMs, marketing automations and customer experience platforms?
5. Can your infrastructure solutions provide further analytics for our SIEM and business intelligence platforms?
6. What standards do you support for current protocols and schemes?
7. Can you provide a full list of the categories you support with APIs?
8. What are the native capabilities your solution provides when it comes to common identity and access-related use cases?
9. As technology and consumer preference evolve, will we be able to support identity wallets, zero knowledge proof attributes and claims providers?
10. Can we integrate solutions like Know Your Customer (KYC) processes into our user onboarding process?
11. Will we be able to integrate Adobe Analytics or Google Analytics to provide deeper understanding of user behaviour to improve metrics such as conversion rates?
12. Can you provide a list of third-party integrations supported by your platform?
13. Specifically which security standards does your solution comply with?
14. Do you offer no-code or low-code integrations?
15. How do you support inbound user synchronization?
16. How do you support outbound user synchronization (provisioning)?

3. Non-Functionals & Performance

While the technical side of things can be complex, you can also learn a lot about a company by how well they communicate the specifications and scalability of their technology. While the answers themselves are important, so is the context. If a company cannot clearly explain technical aspects in an RFP, they will likely struggle with this in the future too.

1. How does your solution address scalability and performance?
2. Is your proposed solution cloud based or on-premises?
3. What cloud service providers are you using?
4. Are you providing private tenant or multi-tenant?
5. What are the regions where the CIAM data resides?
6. From your current customers, what percentage is running in the cloud and what percentage is on-premises?
7. What browsers does your solution support?
8. Do you provide Business Continuity and/or Data Recovery services?
9. What service level options do you provide?
10. What protection do you offer from traffic floods, bot traffic and other threats?
11. What options do you offer regarding monitoring availability and performance for your customers?
12. How do you inform clients on maintenance and patch releases?
13. Please explain your possibilities regarding continuous delivery?
14. How do you provide support for developers?
15. Is it possible to change login flows ourselves?
16. What kind of authorization/enforcement do you offer on all your APIs?
17. Is it possible to host tenant specific operational components, like audit and monitoring, security services and back-end configuration capabilities?
18. Can you ensure these components will not be exposed to customers?
19. Could your solution support millions of users attempting to log in at the same time?

4. Regulations & Compliance

Compliance with data regulations is vital in today's digital economy. In recent years, we have seen a lot of changes, and with more regulatory changes expected, you need to ensure proposals clearly outline a plan for adapting to new legislation.

1. How is data portability implemented in your solution?
2. Please explain how you handle, store and protect data that falls in the category 'special categories of personal data'?
3. Can your solution support us with data minimization?
4. How will you deal with attributes that need to be stored from a legal/regulatory perspective? And how do you communicate exceptions to users?
5. How do you support data retention on all personal data collected?
6. Please explain how you have incorporated privacy by default, and privacy by design, in your solution?
7. How can your solution assist us in conducting audits for data compliance regulations?
8. How can you help us navigate the challenges arising from Schrems II?

5. Implementation & Support

Meeting your current technical and compliance needs is obviously the priority, but it's also important to have a partner that can help you adapt to future changes in your business, and can help you scale as your business grows.

1. How many implementations have you conducted in our industry sector over the past three years?
2. What is the average duration of your product deployment, commonly known as "time to market"? Could you also share evidence that showcases how your solution effectively reduces time to market?
3. Could you provide an overview of your customer onboarding procedure and describe the composition of your onboarding team?
4. Which consultancy and implementation partners do you recommend?
5. What are the prerequisites before we can start implementation?
6. Please explain your preferred delivery model considering your resources, knowledge level, input and orchestration?
7. Do you have your own CIAM consultancy practice able to guide us in digital transformation processes? If yes, please provide us with some customer cases.
8. What is your lead-time for an out-of-the-box tenant delivery and with what preconditions on our side?
9. How will ongoing support be organized?
10. What contact will we have after implementation?
11. Can you provide 24/7 support and services to our offices around the world?
12. Can you share case studies of clients using your solution to manage scalability due to business growth?
13. Can you provide an ongoing roadmap for future developments?

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 centers to devices and across networks. As the global leader in data security, identity & access management, 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.

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