Sample Selection Criteria for Customer Identity and Access Management (CIAM) Platforms

Akamai

A starting point for vendor evaluation

This document provides a list of sample questions to assist you with RFP creation for a customer identity and access management (CIAM) solution. This guide is intended as a starting point; it should help your teams and stakeholders identify your organization's specific requirements and priorities. We consider these questions basic evaluation criteria for comparing CIAM solutions and vendors.

Vendor Information

1. What is the name of your company?
2. Please list all company locations and staffing levels at each location.
3. How long has the company been in business?
4. Please provide a brief history of your company.
5. Please give an overview of the product and services portfolio.
6. Please describe the availability of your platform on a global scale.
7. Please provide information regarding commercial or technical partnership(s) with other organization(s).
8. Please provide an overview of the company's finances.

Experience and References

1. Please describe your company's experience delivering CIAM solutions.
2. How many clients do you have?
3. Please provide at least five examples of active deployments.
4. Who among your clients are similar in size and scope to our organization?
5. Please provide analyst reports or other independent studies that illustrate your leadership in the CIAM space.
6. Please describe examples of your company inventing, innovating, or spearheading CIAM-related developments.

CIAM Capabilities

1. Please describe in detail your suite of CIAM offerings.
2. What registration features are supported (CAPTCHA, in-line verification, data validation, etc.)?
3. Do you support multiple social network and identity providers for authentication (e.g., Facebook, Google, Twitter, LinkedIn, etc.)?
4. Can clients easily configure user-facing forms to match their site's look and feel, and how flexible and customizable are these screens?
5. Please describe the process of integrating user-facing forms into a client's sites.
6. Please detail the devices that integrate with your solution. Include mobile devices, tablets, and IoT/ connected devices.
7. Please provide details about responsiveness.
8. What software development kits (SDKs) are available for both standard and mobile platforms?
9. Does your system support the use of different languages in all fields (UTF-8/double-byte characters) for multilingual countries as well as to allow for special characters (e.g., ñ in Spanish, ö in German, ç in French)?
10. Is your solution Open Standards compliant?
11. Does your service provide detailed reporting capabilities?
12. Please describe the authentication capabilities of your platform.
13. Please describe your platform's capabilities for access control and access policy management.
14. Please describe your platform's administration capabilities.
15. Can clients create and manage other resources such as devices, subscriptions, or sub-profiles?
16. Please describe how delegated administration is supported for consumer use cases.
17. Can consumers create accounts for friends or family and invite them to join?
18. Do you offer a centralized authentication service for end users?
19. Can web and mobile apps easily connect to your platform using standard libraries?
20. How does the platform store consent data?
21. How long is audit history for consents maintained?
22. Are both coarse-grained and fine-grained consent supported?
23. Do end users have full visibility and control of their consent data?
24. Can consent be collected in context as needed?

25. Can end users download a copy of their data?
26. Can end-user data be deleted upon request?
27. Does your solution provide configurable authorization capabilities?
28. What level of granularity does your authorization support (RBAC, ABAC, etc.)?
29. Does your solution support dynamic lookup of policy attributes?
30. Does your solution support policies spanning multiple identity providers?
31. Can your solution provide audit logs of authorization decisions? And can sensitive data be auto-encrypted in these logs?
32. How are policies created (i.e., do you have visual tools for creating policies or are policies created via textual/coded configuration)?
33. What tools do you provide to ensure the validity, integrity, and impact analysis of your policies?
34. Does your solution have the capability to control who can create/modify/delete policies?

Integrations

1. Which browsers are your platform compatible with? Please specify:
    - 1.1 Firefox
    - 1.2 Google Chrome
    - 1.3 Apple Safari
    - 1.4 Microsoft Edge
    - 1.5 Microsoft Internet Explorer
    - 1.6 Android browser
2. Please describe how you support integrations with third-party platforms, including (but not limited to) the following categories:
    - 2.1 CRM solutions
    - 2.2 Email marketing platforms and services
    - 2.3 Other digital marketing platforms
    - 2.4 Ecommerce platforms
    - 2.5 CMS solutions
    - 2.6 BI and analytics solutions
    - 2.7 SIEM and log monitoring solutions

3. Does your platform support both batch and real-time integration patterns?
4. Please describe the available format options for profile data that is retrieved from your platform.
5. Is event data available as part of a feed? Please list all events that are available.
6. Describe the controls that are in place to ensure that only authorized and consented data is sent to downstream systems.

APIs

1. Please describe the following application program interfaces (APIs) of your platform:
    - 1.1 Registration APIs (client and server side)
    - 1.2 Authentication APIs (client and server side)
    - 1.3 Account Update APIs (client and server side)
    - 1.4 Administrative APIs
    - 1.5 Querying APIs

Platform Architecture, Data Storage, and Infrastructure

1. Please outline your platform architecture and the ways in which data can be retrieved.
2. Do you offer a real-time, queryable structured database for user profile data collected during the authentication process?
3. Please describe the flexibility of your data schema for adding and removing data fields, changing fields from optional to mandatory, and vice versa.
4. Please describe the ability to delete a data item from a user record (e.g., if requested for legal reasons). Please describe how this is achieved within your solution, subject to data access security rules.
5. Please describe what happens when a user deletes their account from your solution.
6. Please describe how your solution enables users to make changes to their profile data.
7. Please provide solution details around data replication, resilience, and availability of infrastructure.
8. Please provide technical details of your data and backup storage facilities, including the geographical location, the relevant physical and logical security framework, and backup procedures.
9. As a guide, how many user records could you accommodate at a maximum?
10. How is system availability monitored by your customers?
11. What level of system availability will be guaranteed by your organization, and what financial credits will be given if this level is not achieved?

12. Please provide a summary of your proposed business continuity procedure in the event of major technical and/or operational disruptions. This may include your disaster recovery processes.
13. Is your solution dynamically scalable on demand, e.g., able to cope with large-scale user promotions? If not, how much advance notice would you need to deal with an expected spike? Do you already have the infrastructure in place to support this?
14. Alternatively, does your solution use a large database with enough headroom to cope with this demand?
15. What independent performance benchmarking have you undertaken? Please share the results of these benchmarks.
16. Does your platform leverage a microservice architecture to independently scale components?
17. Does your platform include separate repositories for customer profiles and web events?
18. Does your infrastructure integrate customer profiles with their web activity?
19. Does your infrastructure include a data pipeline to reconcile, transform, and conform data for data warehouse reporting?

Cybersecurity and Data Protection

General Security

1. Please provide a completed, full standardized information gathering (SIG) questionnaire.
2. Please describe your security architecture. Include network-, database-, and application-layer security.
3. Do you have a security and privacy overview?

Security Programs

1. Do you have an information security management program (ISMP)? If yes, how is its effectiveness evaluated?
2. Do you have a risk program?
    - 2.1 Please describe how you track known risks and how you ensure known risks are managed.
    - 2.2 Please describe how you perform formal risk assessments. How frequently are these performed and what is the scope?
3. How do you manage anti-virus defense?

Access Control

1. How do you manage your employee access to production systems?
2. Do you use multi-factor authentication?

Change Management

1. Do you have a change management policy?
2. How do you ensure change management procedures are followed?
3. How is change management operationalized during engineering development of your core product offerings?
4. Please describe your change management process for client application configurations.
5. Please describe your change management process for client customizations.
6. How do you inform clients about maintenance and patches?
7. How do you inform clients about product releases?

Data Protections

1. Please detail if/how your stored data is encrypted.
2. Please detail if/how data is encrypted in transit.
3. Does your solution provide granular security access controls over individual data fields so that we can control which fields other systems, websites, mobile sites, and external parties can view, read, modify, and delete?
4. Does your solution provide multiple security levels for applications and people accessing stored data? Can those security levels be applied per-application or per-role?
5. What intrusion detection mechanisms do you have in place?

Key Management

1. How do you manage encryption keys?
2. Can we bring our own key?

Password Management

1. Do you hash passwords?
2. What cost factor do you use for your hashing algorithm?
3. Do you provide each end user a unique salt?
4. How are salts handled during a password reset?
5. Can clients choose their own password rules (own password regular expression)?

Durability

1. What durability do you provide to client data?

Monitoring

1. Do you provide 24/7/365 monitoring?
2. Do you inform customers in real time about your platform status?
3. Do you perform trend monitoring on client applications?
4. How do you handle advanced persistent distributed attacks?
5. How do you handle denial-of-service (DoS) attacks?
6. Can you block IPs?
7. Does your solution enable the export of security events to a security management or SIEM platform?

Network Protections

1. Please describe your firewalls.
2. Do you use security groups?
3. Do you use virtual private clouds (VPCs)?
4. Is your solution designed for Zero Trust?
5. What elements do you harden?

Business Continuity and Disaster Recovery (BCDR)

1. Do you have a business continuity policy? Please detail.
2. Do you regularly practice your BCDR plans?
3. Do you simultaneously write client data to an alternate data center?
4. How many backups do you make of client data?
5. How many backups do you make of your core platform?
6. Do you test restores from backup? If yes, how often, and is this verified by external auditors?
7. Have you ever implemented your disaster recovery or business continuity plans in a live situation? If yes, please describe.

Penetration and Vulnerability Testing

1. How often do you do a network penetration test?

Compliance

1. Which of the following compliance certifications do you have verified by an accredited external audit firm?

    1.1 SOC 2 Type 2 Security (Common Criteria) – If yes, please provide the report.

    1.2 SOC 2 Type 2 Availability – If yes, please provide the report

    1.3 SOC 2 Type 2 Confidentiality – If yes, please provide the report.

    1.4 SOC 2 Type 2 Processing Integrity

    1.5 SOC 2 Type 2 Privacy

    1.6 ISO 27001:2013 – If yes, please provide the report.

    1.7 ISO 27018:2014 – If yes, please provide the certification link.

    1.8 HIPAA – If yes, please provide the report.

    1.9 HITECH – If yes, please provide the report.

    1.10 CSA Star Level 2 Certified – If yes, please provide the certification link and attestation report.

    1.11 Privacy practices – If yes, please provide proof of assessment.

    1.12 Privacy Shield – If yes, please provide proof of assessment.

General Data Protection Regulation (GDPR)

1. Does your solution provide workflows to support data subject requests under GDPR?
2. If personal data is transferred across country borders, please identify the relevant transfer mechanisms – such as Privacy Shield certification, binding corporate rules (BCR), or standard contractual clauses – that your company can meet or provide to legitimize the transfer.
3. What GDPR training have you implemented?
4. Do you have an information security manager?
5. Do you have a VP of privacy or chief privacy officer?
6. Does your solution offer a consent management capability?

Support and Services

1. Please provide an overview of your solution's deployment process, the support functions that will be available to clients through deployment, and the average time to market.
2. Please describe your technical support services, including 24/7 options and SLAs.
3. Please describe the strategy and consulting services offered by your company.
    3.1 Does your company have expertise in third-party integrations or enterprise architecture best practices?
4. Please describe the training services or training program offered by your company.
5. What is the hiring profile for a Technical Support Engineer?
6. Where are the Technical Support teams located?
7. How are the Technical Support teams trained?
8. How are the Technical Support teams measured and coached around ticket quality?
9. How does the Technical Support team measure success?
10. What is the relationship between Technical Support and Engineering?
11. What processes are used to protect the customer from possible misconfigurations by the Technical Support team?
12. How do you protect customers from unauthorized configuration requests or changes?
13. What kinds of data does the customer receive from the Technical Support team on a monthly or quarterly basis?
14. What is the escalation process for Technical Support issues?
15. What is your SLA compliance for current customers?
16. How do you measure customer satisfaction on Technical Support tickets?
17. Does your company offer solution architecture consulting?
    17.1 Does this consultation include advice on integrating identity management within our existing information ecosystem, including data capture, marketing automation, operational reporting, business analytics, and other IT processes?