Ejemplos de criterios de selección de plataformas de gestión de acceso e identidades de cliente (CIAM)

Un punto de partida para la evaluación de proveedores

En este documento, se proporciona una lista de preguntas de ejemplo para ayudarle a crear una solicitud de propuestas para una solución de gestión de acceso e identidades de cliente (CIAM). Esta guía está concebida como punto de partida, por lo que debería ayudar a los equipos y las partes interesadas a identificar las necesidades y prioridades concretas de la organización. Consideramos que estas preguntas son criterios de evaluación básicos para comparar soluciones y proveedores de CIAM.

Información del proveedor

1. ¿Cuál es el nombre de su empresa?
2. Enumere todas las sucursales de la empresa y la dotación de personal de cada una de ellas.
3. ¿Cuánto tiempo lleva la empresa en el sector?
4. Proporcione una breve reseña de su empresa.
5. Proporcione una descripción general de la cartera de productos y servicios.
6. Describa la disponibilidad de su plataforma a escala mundial.
7. Proporcione información sobre las colaboraciones comerciales o técnicas con otras organizaciones.
8. Proporcione una descripción general de las finanzas de la empresa.

Experiencia y referencias

1. Describa la experiencia de su empresa en la provisión de soluciones CIAM.
2. ¿Cuántos clientes tiene?
3. Proporcione al menos cinco ejemplos de implementaciones activas.
4. ¿Cuál de sus clientes tiene un tamaño y alcance similares a nuestra organización?
5. Proporcione informes de analistas u otros estudios independientes que confirmen su liderazgo en el ámbito de las soluciones CIAM.
6. Proporcione ejemplos de invención, innovación o liderazgo de su empresa en desarrollos relacionados con soluciones CIAM.

Capacidades de CIAM

1. Describa detalladamente su gama de productos CIAM.
2. ¿Qué funciones de registro se admiten (CAPTCHA, verificación en línea, validación de datos, etc.)?
3. ¿Se admiten distintas redes sociales y proveedores de identidad para la autenticación (por ejemplo, Facebook, Google, Twitter, LinkedIn, etc.)?
4. ¿Pueden los clientes configurar fácilmente formularios para el usuario, de modo que se adapten a la imagen y características del sitio? ¿En qué medida son flexibles y personalizables estas pantallas?
5. Describa el proceso de integración de formularios del usuario en los sitios de los clientes.
6. Detalle los dispositivos que se integran con su solución. Incluya dispositivos móviles, tablets y dispositivos conectados y de IoT.
7. Proporcione información sobre la capacidad de respuesta.
8. ¿Qué kits de desarrollo de software (SDK) hay disponibles para las plataformas estándar y móviles?
9. ¿Admite su sistema el uso de diferentes idiomas en todos los campos (UTF-8/caracteres de doble byte) para países multilingües, así como de caracteres especiales (por ejemplo, la "ñ" en español, la "ö" en alemán o la "ç" en francés)?
10. ¿La solución es compatible con estándares abiertos?
11. ¿Ofrece su servicio funciones de generación de informes detallados?
12. Describa las funciones de autenticación de su plataforma.
13. Describa las funciones de control de acceso y gestión de políticas de acceso de su plataforma.
14. Describa las funciones de administración de su plataforma.
15. ¿Pueden los clientes crear y gestionar otros recursos tales como dispositivos, suscripciones o subperfiles?
16. Describa en qué medida es compatible la administración delegada en los casos de uso de los consumidores.
17. ¿Pueden los consumidores crear cuentas para amigos o familiares e invitarles a unirse?
18. ¿Se ofrece un servicio de autenticación centralizada para los usuarios finales?
19. ¿Pueden las aplicaciones web y móviles conectarse fácilmente a la plataforma utilizando bibliotecas estándar?
20. ¿Cómo almacena la plataforma los datos de consentimiento?
21. ¿Durante cuánto tiempo se mantiene el historial de auditorías para los consentimientos?
22. ¿Se admiten tanto el consentimiento general como el específico?
23. ¿Tienen los usuarios finales una visibilidad y un control totales de los datos de consentimiento?
24. ¿Se puede recopilar el consentimiento en contexto, según sea necesario?

25. ¿Pueden los usuarios finales descargar una copia de sus datos?
26. ¿Se pueden eliminar los datos de los usuarios finales previa solicitud?
27. ¿Su solución proporciona funciones de autorización configurables?
28. ¿Qué nivel de detalle admite la autorización (RBAC, ABAC, etc.)?
29. ¿Admite su solución la búsqueda dinámica de atributos de política?
30. ¿Admite su solución políticas que abarquen varios proveedores de identidad?
31. ¿Puede su solución proporcionar registros de auditoría de las decisiones de autorización? Por otro lado, ¿se pueden cifrar automáticamente los datos confidenciales en estos registros?
32. ¿Cómo se crean las políticas? Es decir, ¿dispone de herramientas visuales para crear políticas, o estas se crean mediante configuración de texto o código?
33. ¿Qué herramientas se proporcionan para asegurar la validez, la integridad y el análisis del impacto de sus políticas?
34. ¿Tiene su solución la capacidad de controlar quién puede crear/modificar/eliminar políticas?

Integraciones

1. ¿Con qué navegadores es compatible su plataforma? Especifique:
    - 1.1 Firefox
    - 1.2 Google Chrome
    - 1.3 Apple Safari
    - 1.4 Microsoft Edge
    - 1.5 Microsoft Internet Explorer
    - 1.6 Navegador Android
2. Describa el grado de integración con plataformas de terceros, incluidas, entre otras, las siguientes categorías:
    - 2.1 Soluciones CRM
    - 2.2 Plataformas y servicios de marketing por correo electrónico
    - 2.3 Otras plataformas de marketing digital
    - 2.4 Plataformas de comercio electrónico
    - 2.5 Soluciones CMS
    - 2.6 Soluciones de inteligencia empresarial y análisis
    - 2.7 Soluciones de SIEM y supervisión de registros

3. ¿Es su plataforma compatible con patrones de integración por lotes y en tiempo real?
4. Describa las opciones de formato disponibles para los datos de perfil que se recuperan de su plataforma.
5. ¿Están los datos de eventos disponibles como parte de una fuente? Enumere todos los eventos que están disponibles.
6. Describa los controles de los que disponen para asegurar el envío únicamente de datos con autorización y consentimiento a los sistemas de bajada.

API

1. Describa las siguientes interfaces de programación de aplicaciones (API) de su plataforma:
    - 1.1 API de registro (cliente y servidor)
    - 1.2 API de autenticación (cliente y servidor)
    - 1.3 API de actualización de cuentas (cliente y servidor)
    - 1.4 API administrativas
    - 1.5 API de consulta

Arquitectura de la plataforma, almacenamiento de datos e infraestructura

1. Describa la arquitectura de su plataforma y las formas de recuperación de los datos.
2. ¿Ofrece una base de datos estructurada y que se pueda consultar en tiempo real para los datos de perfiles de usuario recopilados durante el proceso de autenticación?
3. Describa la flexibilidad de su esquema de datos para añadir y eliminar campos de datos, y para cambiar los campos de opcionales a obligatorios, y viceversa.
4. Describa la capacidad de eliminar un elemento de datos de un registro de usuario (por ejemplo, si se solicita por motivos legales). Describa el proceso que sigue su solución para ello, conforme a las reglas de seguridad de acceso a los datos.
5. Describa qué sucede cuando un usuario elimina la cuenta de su solución.
6. Describa cómo su solución permite a los usuarios modificar los datos del perfil.
7. Proporcione detalles de la solución con respecto a la replicación de datos, la resiliencia y la disponibilidad de la infraestructura.
8. Proporcione detalles técnicos de sus instalaciones de almacenamiento de datos y copias de seguridad, incluidos la ubicación geográfica, el marco de seguridad física y lógica pertinente, y los procedimientos de copia de seguridad.
9. A modo de referencia, ¿cuántos registros de usuarios puede alojar como máximo?
10. ¿Cómo supervisan los clientes la disponibilidad del sistema?
11. ¿Qué nivel de disponibilidad del sistema garantizará su organización, y qué compensación económica se proporcionará en caso de no alcanzar dicho nivel?

12. Proporcione un resumen de su propuesta de procedimiento de continuidad del negocio en caso de producirse interrupciones técnicas u operativas de gran envergadura. Se pueden incluir los procesos de recuperación ante desastres.

13. ¿Es la solución escalable de forma dinámica bajo demanda? Por ejemplo, ¿es capaz de asumir promociones a gran escala que atraigan a muchos usuarios? Si no, ¿con cuánta antelación se debe informar para abordar un pico previsto? ¿Cuenta en este momento con la infraestructura necesaria para asumirlo?

14. Asimismo, ¿utiliza su solución una base de datos grande con margen suficiente para hacer frente a esta demanda?

15. ¿Qué pruebas de rendimiento independientes ha realizado? Comparta los resultados de dichas pruebas.

16. ¿Utiliza su plataforma una arquitectura de microservicios para escalar componentes de forma independiente?

17. ¿Incluye su plataforma repositorios independientes para perfiles de clientes y eventos web?

18. ¿Integra su infraestructura los perfiles de clientes con su actividad en la web?

19. ¿Incluye su infraestructura un sistema de canalización de datos para conciliar, transformar y ajustar datos para análisis e informes?

Ciberseguridad y protección de datos

Seguridad general

1. Proporcione un cuestionario de recopilación de información estandarizada cumplimentado.

2. Describa su arquitectura de seguridad. Incluya la seguridad de la capa de red, base de datos y aplicación.

3. ¿Tiene una visión general de la seguridad y la privacidad?

Programas de seguridad

1. ¿Cuenta con un programa de gestión de la seguridad de la información (PGSI)? Si la respuesta es afirmativa, ¿cómo se evalúa su eficacia?

2. ¿Cuenta con un programa de riesgo?

    2.1 Describa cómo realiza el seguimiento de riesgos conocidos y cómo garantiza una gestión adecuada de los mismos.

    2.2 Describa cómo realiza evaluaciones de riesgos formales. ¿Con qué frecuencia se realizan y cuál es su alcance?

3. ¿Cómo gestiona la protección antivirus?

Control de acceso

1. ¿Cómo gestiona el acceso de los empleados a los sistemas de producción?

2. ¿Utiliza la autenticación multifactorial?

Gestión de cambios

1. ¿Cuenta con una política de gestión de cambios?
2. ¿Cómo asegura el seguimiento de los procedimientos de gestión de cambios?
3. ¿Cómo se sistematiza la gestión de cambios durante el desarrollo de ingeniería de las principales ofertas de productos?
4. Describa el proceso de gestión de cambios para las configuraciones de aplicaciones de clientes.
5. Describa el proceso de gestión de cambios para las personalizaciones de clientes.
6. ¿Cómo informa a los clientes sobre el mantenimiento y los parches?
7. ¿Cómo informa a los clientes acerca de los lanzamientos de productos?

Protección de datos

1. Especifique si se cifran los datos almacenados y el procedimiento que se sigue.
2. Especifique si se cifran los datos en tránsito y el procedimiento que se sigue.
3. ¿Su solución proporciona controles específicos de acceso de seguridad para los distintos campos de datos, de forma que podamos controlar qué campos pueden ver, leer, modificar y eliminar otros sistemas, sitios web, sitios móviles y partes externas?
4. ¿Su solución proporciona varios niveles de seguridad para las aplicaciones y los usuarios que acceden a los datos almacenados? ¿Dichos niveles de seguridad se pueden aplicar por aplicaciones o funciones?
5. ¿Con qué mecanismos de detección de intrusos cuenta?

Gestión de claves

1. ¿Cómo gestiona las claves de cifrado?
2. ¿Podemos utilizar nuestra propia clave?

Gestión de contraseñas

1. ¿Codifica las contraseñas mediante hash?
2. ¿Qué factor de coste utiliza para el algoritmo de hash?
3. ¿Proporciona a cada usuario final valores de sal únicos?
4. ¿Cómo se gestiona la sal durante un restablecimiento de contraseña?
5. ¿Pueden los clientes elegir sus propias reglas de contraseña (expresiones regulares de contraseña propias)?

Durabilidad

1. ¿Qué durabilidad proporciona a los datos de los clientes?

Supervisión

1. ¿Proporciona una supervisión ininterrumpida?
2. ¿Informa a los clientes en tiempo real sobre el estado de la plataforma?
3. ¿Supervisa las tendencias en las aplicaciones de clientes?
4. ¿Cómo gestiona los ataques distribuidos persistentes y avanzados?
5. ¿Cómo gestiona los ataques de denegación de servicio (DoS)?
6. ¿Puede bloquear IP?
7. ¿Su solución permite exportar eventos de seguridad a una plataforma de gestión de seguridad o SIEM?

Protecciones de red

1. Describa sus firewalls.
2. ¿Utiliza grupos de seguridad?
3. ¿Utiliza nubes privadas virtuales (VPC)?
4. ¿Su solución está diseñada para Zero Trust?
5. ¿Qué elementos se refuerzan?

Continuidad del negocio y recuperación ante desastres (BCDR)

1. ¿Dispone de una política de continuidad del negocio? Detállela.
2. ¿Pone en práctica habitualmente sus planes de BCDR?
3. ¿Puede escribir simultáneamente los datos de los clientes en un centro de datos alternativo?
4. ¿Cuántas copias de seguridad hace de los datos de los clientes?
5. ¿Cuántas copias de seguridad hace de la plataforma central?
6. ¿Prueba la validez de las copias de seguridad para restauración? En caso afirmativo, ¿con qué frecuencia? ¿Están verificadas por auditores externos?
7. ¿Alguna vez ha implementado sus planes de recuperación ante desastres o de continuidad del negocio en una situación real? Si la respuesta es afirmativa, describa este hecho.

Pruebas de penetración y vulnerabilidad

1. ¿Con qué frecuencia realiza pruebas de penetración en la red?

Cumplimiento de normativas

1. ¿Cuál de las siguientes certificaciones de cumplimiento ha verificado una empresa de auditoría externa acreditada?

    1.1 SOC 2 tipo 2 sobre seguridad (criterios comunes): en caso afirmativo, proporcione el informe.

    1.2 SOC 2 tipo 2 sobre disponibilidad: en caso afirmativo, proporcione el informe.

    1.3 SOC 2 tipo 2 sobre confidencialidad: en caso afirmativo, proporcione el informe.

    1.4 SOC 2 tipo 2 sobre integridad de procesamiento

    1.5 SOC 2 tipo 2 sobre privacidad

    1.6 ISO 27001:2013: en caso afirmativo, proporcione el informe.

    1.7 ISO 27018:2014: en caso afirmativo, proporcione el enlace de la certificación.

    1.8 HIPAA: en caso afirmativo, proporcione el informe.

    1.9 HITECH: en caso afirmativo, proporcione el informe.

    1.10 Certificación CSA Star nivel 2: en caso afirmativo, proporcione el enlace de la certificación y el informe de certificación.

    1.11 Prácticas de privacidad: en caso afirmativo, proporcione la prueba de evaluación.

    1.12 Escudo de privacidad: en caso afirmativo, proporcione la prueba de evaluación.

Reglamento General de Protección de Datos (RGPD)

1. ¿Su solución proporciona flujos de trabajo para admitir solicitudes de datos conforme al RGPD?
2. Si los datos personales se transfieren más allá de las fronteras de un país, identifique los mecanismos de transferencia pertinentes, como la certificación de escudo de privacidad, las normas corporativas vinculantes (NCV) o las cláusulas contractuales estándar, que su empresa puede aplicar o proporcionar para legitimar la transferencia.
3. ¿Qué formación sobre el RGPD ha implementado?
4. ¿Cuenta con un responsable de seguridad de la información?
5. ¿Cuenta con un vicepresidente o jefe de Privacidad?
6. ¿Su solución ofrece funciones de gestión del consentimiento?

Atención al cliente y servicios

1. Proporcione una descripción general del proceso de implementación de la solución, las funciones de atención al cliente que estarán disponibles durante la implementación y el tiempo medio de comercialización.
2. Describa sus servicios de asistencia técnica, incluidos las opciones de asistencia ininterrumpida y los acuerdos de nivel de servicio.
3. Describa la estrategia y los servicios de asesoramiento que ofrece su empresa.
    3.1 ¿Tiene su empresa experiencia en integraciones de terceros o prácticas recomendadas de arquitectura empresarial?
4. Describa los servicios o programas de formación que ofrece su empresa.
5. ¿Cuál es el perfil buscado al contratar un ingeniero de asistencia técnica?
6. ¿Dónde se encuentran los equipos de asistencia técnica?
7. ¿Qué formación se proporciona a los equipos de asistencia técnica?
8. ¿Cómo se evalúan y forman los equipos de asistencia técnica con respecto a la calidad de los tickets?
9. ¿Cómo mide el éxito el equipo de asistencia técnica?
10. ¿Cuál es la relación entre los equipos de asistencia técnica y de ingeniería?
11. ¿Qué procesos se utilizan para proteger a los clientes de posibles errores de configuración por parte el equipo de asistencia técnica?
12. ¿Cómo protege a los clientes de solicitudes o cambios de configuración no autorizados?
13. ¿Qué tipos de datos envía el equipo de asistencia técnica al cliente de forma mensual o trimestral?
14. ¿Cuál es el proceso de derivación de las cuestiones relacionadas con la asistencia técnica?
15. ¿Cuál es su nivel de cumplimiento de los SLA para los clientes actuales?
16. ¿Cómo mide la satisfacción de los clientes con los tickets de asistencia técnica?
17. ¿Ofrece su empresa asesoramiento de arquitecturas de soluciones?
    17.1 ¿Incluye este asesoramiento consejos sobre la integración de la gestión de identidades en nuestro ecosistema de información existente, incluida la captura de datos, la automatización de marketing, informes operacionales, análisis empresariales y otros procesos de TI?

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma perimetral inteligente de Akamai llega a todas partes, desde la empresa a la nube, lo que permite a nuestros clientes y a sus negocios ser rápidos, inteligentes y seguros. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad perimetral, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente, análisis y una supervisión ininterrumpida durante todo el año sin precedentes. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com/es/es/, blogs.akamai.com/es/, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en akamai.com/es/es/locations.jsp. Publicado en abril de 2019.