Client Integration and JWT Differentiation

Our service is utilized by a diverse range of clients across various industries. Each client has unique requirements and integrates with our service in different ways. This document provides an overview of our key clients, their specific use cases, and how technical users can distinguish between them using the JWT (JSON Web Token).

1. Acme Corporation

Acme Corporation is a leading e-commerce platform that sells a wide variety of products. They leverage our service to handle user authentication, authorization, and personalized product recommendations.

Integration Details

- Acme Corporation integrates with our service through a RESTful API.
- They use OAuth 2.0 authorization code grant flow for user authentication.
- User roles and permissions are managed within their own system and passed to our service via JWT claims.
- Acme Corporation utilizes our product catalogue API to fetch product information and pricing details.

JWT Differentiation

- The JWT issued for Acme Corporation includes a custom claim `client_id` with the value `acme_corp`.
- The `roles` claim in the JWT contains Acme-specific roles such as "acme_admin", "acme_buyer", "acme_seller", etc.
- The `permissions` claim includes Acme-specific permissions like "manage_acme_products", "view_acme_orders", etc.

2. Globex Industries

Globex Industries is a multinational conglomerate with diverse business verticals. They use our service for secure employee authentication and access control across their internal applications.

Integration Details

- Globex Industries integrates with our service using SAML 2.0 for single sign-on (SSO).
- They have a custom user directory that syncs with our service via SCIM (System for Cross-domain Identity Management) protocol.
- access levels and departmental permissions are mapped to JWT claims.
- Globex Industries utilizes our audit logging and reporting APIs for compliance and security monitoring.

JWT Differentiation

- The JWT issued for Globex Industries includes a custom claim `client_id` with the value `globex_ind`.
- The `accessLevel` claim in the JWT represents Globex-specific access levels such as "globex_level1", "globex_level2", etc.
- The `departmentId` claim indicates the department to which the Globex employee belongs.
- The `globexEmployeeId` claim contains the unique identifier of the Globex employee.

3. Initech LLC

Initech LLC is a software development company that specializes in project management tools. They integrate with our service to provide secure authentication and authorization for their SaaS application.

Integration Details

- Initech LLC integrates with our service through a combination of OAuth 2.0 and OpenID Connect (OIDC) protocols.
- They utilize our user registration and profile management APIs to handle user onboarding and account updates.
- Initech LLC uses our SDK to implement multi-factor authentication (MFA) for enhanced security.
- They leverage our API gateway for rate limiting and request validation.

JWT Differentiation

- The JWT issued for Initech LLC includes a custom claim `client_id` with the value `initech`.
- The `roles` claim in the JWT contains Initech-specific roles such as "initech_admin", "initech_project_manager", "initech_developer", etc.
- The `permissions` claim includes Initech-specific permissions like "create_initech_project", "assign_initech_tasks", etc.
- The `initechSubscriptionTier` claim indicates the subscription tier of the Initech user.

4. Umbrella Corporation

Umbrella Corporation is a research and development company in the pharmaceutical industry. They use our service for secure access control and data protection in their internal research platform.

Integration Details

- Umbrella Corporation integrates with our service using a custom-built authentication plugin.

- They have a high-security setup with hardware security modules (HSMs) for key management and JWT signing.
- Umbrella Corporation utilizes our fine-grained access control APIs to enforce strict permissions based on user roles and project assignments.
- They leverage our encryption and tokenization services to protect sensitive research data.

JWT Differentiation

- The JWT issued for Umbrella Corporation includes a custom claim `client_id` with the value `umbrella_corp`.
- The `roles` claim in the JWT contains Umbrella-specific roles such as "umbrella_researcher", "umbrella_lab_manager", "umbrella_executive", etc.
- The `permissions` claim includes Umbrella-specific permissions like "access_umbrella_lab", "view_umbrella_research", etc.
- The `umbrellaProjectId` claim indicates the specific research project the user is associated with.

5. Stark Industries

Stark Industries is a leading technology company known for its cutting-edge innovations. They integrate with our service to provide secure authentication and authorization for their IoT devices and smart home ecosystem.

Integration Details

- Stark Industries integrates with our service using the OAuth 2.0 device authorization grant flow.
- They utilize our authentication APIs to generate and manage access tokens for their IoT devices.
- Stark Industries leverages our policy-based access control system to define and enforce permissions for different device types and user roles.
- They use our real-time event streaming API to receive updates and notifications related to device authentication and authorization events.

JWT Differentiation

- The JWT issued for Stark Industries includes a custom claim `client_id` with the value `stark_ind`.
- The `deviceType` claim in the JWT indicates the type of Stark Industries device, such as "stark_smartwatch", "stark_smartspeaker", etc.
- The `permissions` claim includes Stark-specific permissions like "control_stark_devices", "view_stark_device_data", etc.
- The `starkUserRole` claim represents the role of the Stark Industries user, such as "stark_homeowner", "stark_guest", etc.

6. Cyberdyne Systems

Cyberdyne Systems is an advanced artificial intelligence company that specializes in robotics and autonomous systems. They leverage our service for secure authentication and authorization in their AI-powered platforms.

Integration Details

- Cyberdyne Systems integrates with our service using a combination of OAuth 2.0 and JWT-based authentication.
- They utilize our machine learning-based anomaly detection APIs to identify and prevent unauthorized access attempts.
- Cyberdyne Systems uses our secure key management system to store and rotate encryption keys for their sensitive AI models and data.
- They leverage our multi-tenancy support to provide isolated environments for different clients and projects.

JWT Differentiation

- The JWT issued for Cyberdyne Systems includes a custom claim `client_id` with the value `cyberdyne`.
- The `aiPlatform` claim in the JWT indicates the specific Cyberdyne AI platform, such as "cyberdyne_skynet", "cyberdyne_genisys", etc.
- The `permissions` claim includes Cyberdyne-specific permissions like "train_cyberdyne_models", "deploy_cyberdyne_robots", etc.
- The `cyberdyneUserRole` claim represents the role of the Cyberdyne Systems user, such as "cyberdyne_engineer", "cyberdyne_operator", etc.

Conclusion

Our service supports a wide range of clients with diverse integration requirements and use cases. By utilizing custom claims and values in the JWT, technical users can easily distinguish between different clients and their specific roles, permissions, and attributes.

When implementing integrations or developing applications that interact with our service, it's essential to consider the unique characteristics and requirements of each client. The JWT claims provide a flexible and standardized way to convey client-specific information, enabling fine-grained access control, auditing, and customization.

As we continue to onboard new clients and expand our service offerings, we will update this document to reflect the latest integrations and JWT differentiation strategies. Our goal is to provide a seamless and secure authentication and authorization experience for all our clients while accommodating their distinct needs and workflows.

If you have any questions or require further assistance with client integration or JWT usage, please don't hesitate to reach out to our technical support team. We are

committed to ensuring the success and satisfaction of our clients in leveraging our service for their authentication and authorization needs.