Алианц България Холдинг АД

Задание за изпълнение на поръчка "Решение за управление на идентичността и достъпа - Local Identity and Access Management (LIAM) solution"

I. Обща информация

- Предмет на поръчката е предоставяне на "Решение за управление на идентичността и достъпа - Local Identity and Access Management (LIAM) solution" за нуждите на Алианц България Холдинг АД.
- Алианц България Холдинг АД е компания, състояща се от шест акционерни дружества - самостоятелни юридически лица. Компанията участник в конкурса кандидатства с условия валидни за всички дружества от групата. При спечелване на конкурса ще бъдат сключени отделни договори при условията, с които е спечелен конкурса с всяко от дружествата, които ще имат отношение към новосъздаденото решение.
- Дружествата условно се разделят на две групи (Застрахователни/ПОД и Банка/Лизинг) като всяка група дружества разполага с отделна ИТ среда, Активна Директория и бизнес апликации.
- Част от бизнес апликациите се предоставят от Групата Алианц, като достъпа до тях се управлява централизирано с решение, базирано на OneIdentity (GIAM).

II. Функционални изисквания

1. Solution Architecture

1.1. The solution must be capable of supporting two "tenants", per group of legal entities (insurance/bank), with separate access and management of the integrated assets, access management and governance functionalities.

1.2. The solution should feature a common and well-documented approach for the onboarding and integration of third-party and custom systems via prebuilt as well as programmable connectors.

1.3. Possible deployment scenarios:

- VMware-based virtual machines.
- Kubernetes containers (Azure Kubernetes Service).

1.4. In terms of service levels, application support is provider responsibility while infrastructure support remains with Allianz. The provider must maintain and update the solution to ensure compatibility with the latest version (or next to last, if supported by vendor) of all underlying IT technical components and operating systems.

1.5. For any infrastructure components related to critical functionality such as SSO portals, high availability methods shall be supported.

1.6. The solution should support Oracle Database for persistent data storage.

1.6.1. If the solution does not support and/or integrate with Oracle Database out-of-the-box, the supplier should also offer services for the installation, integration and continuous maintenance of the respective database infrastructure component.

2. Identities

2.1. The following identity types are in scope and must be supported by the solution:

2.1.1. Total number of identities to be managed: ~6600.

- Internal (~1100), including full-time and contract-based employees.
- External (~4500), including sales/partners/vendors.
- Expected natural deviation and annual increase (+/- ~ 5-7%).

3. IT Assets

3.1. Technical integration must be enabled to the following targets:

3.1.1. Interface to Central Identity Store (CIS) via REST API (read-only), which is synced to the HR solution SAP SuccessFactors and serves as single source of truth for digital identity data (internals).

3.1.2. 2 separate local Active Directories (insurance/bank).

3.1.3. Group IAM solution (GIAM, based on OneIdentity) via API.

3.1.4. ~40 local business applications, via AD or direct connector interface (DB/API).

3.1.5. ~20 Group business applications via GIAM API.

3.2. "Light" onboarding must be supported for IT assets that do not allow/support technical integration to LIAM, by providing the following functionalities:

3.2.1. Integration to ticketing system (ServiceNow, nVision).

3.2.2. Email notifications toward access administrators.

4. Identity Management Services

4.1. ID master data management:

4.1.1. Tooling must be able to support a single source of truth for all digital identity data related to internal employees (full-time or contract based).

4.1.2. Tooling must be able to support manual ID data entry for external identities (sales, vendors) and provide bulk upload/entry capabilities.

4.1.3. Tooling must be able to provide verified copies of all digital identity data for internals and externals.

4.1.4. Identity account reconciliation (comparing person's unique digital identity against agreed-upon authoritative source of truth) must be possible to ensure data integrity.

4.1.5. Analytics enabling detection of duplicate IDs (especially external IDs) and "inactive manager" cases should be possible.

5. Authentication & Authorization services

5.1. Authentication

5.1.1. Creation of account linked to unique ID and related lifecycle tasks (update, disable, enable) must be supported.

5.1.2. Support of Azure AD as authentication enforcement point.

5.2. Authorization

5.2.1. Tooling must enable authorization of a user based on authenticated digital identity and corresponding role entitlements.

5.2.2. For assets connected through technical interface, authorization must be given automatically upon role assignment, and for 'light-onboarded' assets authorization workflow through automatic ticket/email creation must be supported.

5.3. End-user password management

5.3.1. Setting, changing, and recovering password in self-service must be enabled.

5.3.2. Password policy (e.g., length and complexity requirement) must be enforced.

6. Access Management & Governance

6.1. Group Management

6.1.1. Tooling must enable creation, update, and deletion of active directory groups.

6.1.2. Batch group creation, change and deletion must be supported (e.g., via API/event driven import).

6.2. Role-based access control (RBAC) Management

Provides integration of enforcement of access based on entity's role (e.g., automated creation, update or deletion of access in a given application based on role data) for a given resource (e.g., system / platform / application)

6.2.1. Creation of Business Roles based on underlying activities and entitlements needed for activities, change of Business Roles and deletion of Business Roles must be enabled.

6.2.2. Addition, change and deletion of assets to role management tool must be possible.

6.2.3. Addition and deletion of entitlements to activity must be possible.

6.2.4. Management of Business Roles based on role domains must be enabled.

6.2.5. Staging of Business Roles (during role creation) to go through different levels of quality control and approval must be supported.

6.2.6. Entering of SoD conflicts within Business Roles and automatic check of conflicts upon creation or update of Business Roles must be enabled, differentiation between soft and hard SoD conflicts can be enabled.

6.2.7. Must support setting of role review schedule / date after which role has to be re-approved, and following escalation process if review not performed.

6.2.8. Setting role start date must be enabled.

6.2.9. Support analytics on Business Roles, incl. analysis of entitlements per role, overlaps between Business Roles, Business Roles targeting selected applications (incl. during role creation / staging phases).

6.2.10. Assignment and removal of Business Roles to identities (multiple business roles per user possible) must be possible.

6.2.11. Description of Business Roles in natural language to describe role in easy-to-understand manner must be enabled.

6.3. Automated role assignment

6.3.1. Automatic assignment of initial entitlements/privileges to new ID (birth rights).

6.3.2. Automatic assignment of Business Roles is possible based on given preconditions (including department, legal entity, job title, etc.).

6.4. SoD Enforcement

6.4.1. Prevention of assignment of Business Roles to users which form toxic combinations based on pre-defined SoD matrices must be supported.

6.4.2. Manual business role approval despite SoD conflict by a dedicated responsible approver must be possible (escalation for special cases only).

6.5. Access request, review, and approval workflow management

6.5.1. Access / role requests, approval, and review for internals as well as externals must be supported, for internals via self-service user interface.

6.5.2. Tooling must support four/six-eye-principle in approval process (e.g., approval by Line Manager / Business Owner / Security).

6.5.3. Delegation of the right to request, approve and review accesses / Business Roles on behalf of another person must be enabled.

6.5.4. Access assignment, change and deletion via API / event-driven must be enabled, enabling batch changes during transformation projects.

6.5.5. Roles / entitlements of user and recent history thereof must be visible for user and relevant stakeholders (e.g., line manager).

6.6. Automated reconciliations & remediations

6.6.1. Periodic and on-demand trigger for access review must be supported.

6.6.2. Detection of Mover / Leaver process with automatic initiation of access removal / review must be supported.

6.6.3. Automatic Target vs. As-is comparison, reporting and reconciliation out of tooling must be possible.

6.6.4. Reporting for access managers to verify completion of reviews and removal of obsolete accesses must be supported.

6.7. Access-related forensics

6.7.1. History of all Business Roles and entitlements (incl. accesses in 'light onboarded' assets) and related role management processes must be available centrally (incl. role creation, role approvals, role owners, role changes)

6.7.2. History of role usage must be available (incl. role assignments, list of Joiners, Movers, Leavers per period)

6.7.3. Reporting on requested Business Roles / entitlements must be possible for all assets, including assets which are 'light onboarded' (not having technical LIAM interface).

7. Stability & Monitoring

7.1. Logging

7.1.1. The solution shall incorporate detailed logging and auditing for any actions related to privileged user access, configuration changes, integration amendments, software health indicators and others related to the system's administration and sound operational stability.

7.1.2. The solution shall be able to integrate with a third-party Security & Information Event Management (SIEM) system using a standard protocol such as syslog, ODBC, file tailing or others.

7.2. Reporting

7.2.1. The solution shall be able to generate reports on-demand as well as based on a predefined schedule containing data as defined by the administrator configuring the report such as but not limited to actions performed by a specific user, changes on a specific application's configuration, etc.

7.3.

8. Security

8.1. The solution shall support the configuration of X.509 certificates in order to facilitate TLS encryption of data in motion between the system and its users.

8.2. The solution shall support data at rest encryption.

8.3. The solution shall support Multi Factor Authentication for privileged users accessing the system for administration using methods such as SMS, TOTP, biometrical data and third-party token providers.

8.4. The solution shall allow configuration of an IP-based whitelist to limit the range of network locations which are able to access the solution via GUI, CLI or other administrative means.

8.5. The solution shall support multiple levels of access for administrators based on their role and responsibilities within the organization for the management of the system.