DYNAMIC AUTHORIZATION CHALLENGES FOR THE BANKING AND FINANCE INDUSTRY

OVERVIEW

All financial institutions have multi-pronged challenges for data access control in the areas of privacy and compliance. First is the customer: protect consumer privacy for confidential financial information. Second is to meet global and local compliance regulations surrounding data access control, segregation of duty, and country-specific requirements. If authorization is not done right, it can lead to devastating financial repercussions.

BACKGROUND IN FINANCIAL INDUSTRY

For more than 10 years, Axiomatics has deployed products into numerous banking and finance customer environments. Their use cases differ and range from controlling access to financial records and transactions through to accessing sensitive data and data which is subject to legislation and banking regulations.

WHAT IS DYNAMIC AUTHORIZATION?

Axiomatics' dynamic authorization is a policy and attribute-based approach to access control that can be used at multiple layers within an enterprise such as databases, Big Data, applications, APIs, and microservices.

Authorization decisions are based on policies - not on individual roles. Policies include any number of factors to describe the conditions in which a user should be granted access. For example, device type, location, time of day, customer status, risk scores, and the user's relationship to the data being accessed are all examples of different factors that can be used in policies. Corporate policies are implemented in a centrally managed service which can be physically distributed and operated. The dynamic authorization service can be deployed on-premise, in the cloud, or in hybrid configurations depending on how application resources are deployed.

OVERALL BUSINESS BENEFITS

The banking industry has many instances where dynamic authorization delivers significant benefits such as policy-controlled data access filtering and data masking. The customer relationship management (CRM) database holds vital information about customers and their behaviours. A corporate policy mandates that only the marketing department can view data about customers, for example, but the policy also states that customer Social Security Numbers are considered sensitive and must be hidden. However, the marketing department wants access to customers' spending habits, borrowing habits, yearly income, etc. which can be used to create more attractive and personalized product and service offerings. With dynamic authorization and data masking applied to the Social Security field, marketing can now only see customer information important for marketing initiatives, and not the Social Security Numbers.

Dynamic authorization can address the most complex data access challenges for privacy, intellectual property (IP) protection, and secure sharing at the database layer – to secure data at the source. It also extends the power of ABAC to protect data in databases all the way down to individual table cells, ensuring users only have access to the data they need and nothing more.

Furthermore, dynamic authorization policies can be audited and certified to ensure that access controls are properly configured. Without it, this information is often buried in application code or database structures. Dynamic authorization gives you visibility into the details of access control settings and provides the transparency needed for auditors, security officers, data owners, regulators, and customers.

HOW TO PUT AUTHORIZATION INTO PRACTICE

Dynamic authorization can be applied to many use cases across the Banking and Finance industry. Here are just a handful of case studies that briefly outline the organisational challenges that Axiomatics has helped resolve for our customers.

USE CASE EXAMPLES

ONLINE PAYMENT AUTHORIZATION

- **Challenge:** International payment service wanted to reduce operational costs of transactions & address their audit concerns.
- **Resolution:** Axiomatics is used within the enterprise as the authorization service to secure web services and APIs used in the payments application.
- **Result:** The speed of transactions was increased as approvals could be automatically made if pre-determined conditions were met. Audit preparation is easier as policies and decisions are made and managed centrally and external to the applications.

DELEGATION

- **Challenge:** Large national bank was unable to use their role-based systems to manage the delegation of permissions for special cases.
- **Resolution:** Axiomatics attribute-based access technology was used to extend the roles used in existing business processes by adding a 'Delegation' attribute that defined who the authority is delegated to.
- **Result:** Bank staff have greater flexibility for meeting customer needs. They can grant permissions for specific purposes while still upholding business and regulatory policies regarding customer data. Delegations can be time-bound, removed when its legitimate need is no longer required, or 'passed' via caretakers. A range of delegations became possible, e.g. a parent-child delegation.

  For instance, as a parent, I want access to my underage children's financial records. Dynamic Authorization enables them to provide full access rights to guardians, but their wards are subject to withdrawal and transaction limits.

RELATIONSHIP MANAGEMENT

- **Challenge:** European bank needed to comply with regulations that oversaw the prevention of 'conflicts of interest' caused by existing relationships between employees (tellers) and their families, neighbours etc. The relationships associated with the employee will determine whether they can access the financial data of a customer regardless of their role with the bank.
- **Resolution:** Axiomatics was able to help them define access policies that described the relationship that is in conflict with the organisational policy and enabled them to enforce these compliance rules.
- **Result:** The bank is able to protect customer financial data from being shared with tellers that customers know personally. They are also able to provide evidence of compliance for auditing purposes.

ANOMALOUS BEHAVIOUR DETECTION AND RESPONSE

- **Challenge:** A National Bank had identified certain user behaviors that were associated with fraud. They wanted to detect these instances and terminate access to those users when it occurred.
- **Resolution:** Axiomatics implemented decision-making policies that described the behavior and triggered a denial of access once certain conditions were met.
- **Result:** By having a system that is more context- aware, the bank is able to reduce their financial losses associated with fraud and misuse. They can now detect excessive access to customer accounts; once the limit of acceptable use is reached, the system will refuse further access to the individual.

AXIOMATICS

USE CASE

DATA SHARING & REGULATION COMPLIANCE

- **Challenge:** Common to all our banking & finance customers, is the on-going challenge of data protection. Sharing or releasing customer data should only take place under very specific conditions.
- **Resolution:** Axiomatics provided policy-driven dynamic authorization solutions to help them control access to PII data and enable the masking of sensitive information (fine-grained data redaction).
- **Result:** These customers are now able to guarantee customer privacy, release customer data under strict need-to-share basis and ensure their compliance with data protection regulations (e.g. PCI-DSS).

SEPARATION OF DUTY

- **Challenge:** An investment bank wanted to eliminate the risk of 'rogue traders' who engage in speculative trading without authorization.
- **Resolution:** Axiomatics provided a policy-driven dynamic authorization solution to help them control access, approvals and reduce other behaviors that were indicative of speculation.
- **Result:** Dynamic authorization helped them to allow a trader to approve a transaction if and only if she/he did not initiate the transaction. It is also being used to prevent SoD violations in cases where the policy states that a trader can initiate a transaction for a client if she/he has not previously initiated a similar transaction in the last 10 hours for a competing client.

BIG DATA ANALYSIS

- **Challenge:** Small online bank needs to perform busi-ness analysis across different geo-regions to assist them in defining new financial products for their customers. However, this is difficult to achieve without compromising compliance & regulation.
- **Resolution:** Externalized access policies were put in place to ensure consistent controls are applied regardless of which applications are being used to request the data.
- **Result:** Business intelligence and data can be accessed and located from different geo-locations. Sensitive data is de-identified while keeping it discoverable, searchable, and sortable.

227 W Monroe St. Suite 2100
Chicago, IL 60606, USA
+1 (312) 374-3443

12020 Sunrise Valley Drive,
Suite 100 Reston, VA 20191
+1 (801) 556-9994
sales@axiomaticsfederal.com

Gamla Brogatan 23 B
111 20 Stockholm, Sweden
+46 (0)8 51 510 240