SEKURRA

Security, Privacy and Integrity Governance platform

Security, Privacy and Integrity-enhancing Data Governance

Trust by Design

As data becomes the most valuable asset to many organizations, data protecting is critical during the whole lifecycle of data existence. Additionally, the general regulations require extensive data protection, such as Europe's General Data Protection Regulation (GDPR) and NIST2 directive, and the state of California's CCPA.

SEKURRA is a service that provides data protection at the data layer leveraging Attribute Based Encryption (ABE) on-demand through a dedicated REST interface. Attribute Based Encryption is the core cryptography technology and its unique characteristic is built-in attribute based access control, that can support cross-industry use cases.

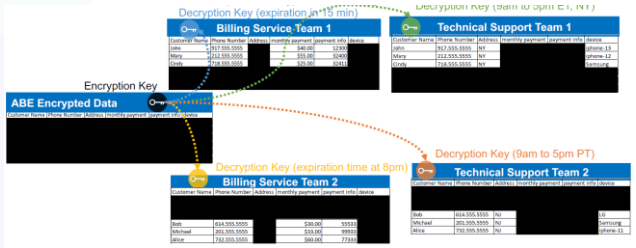
Compared to other cryptography techniques, the data encrypted with ABE requires a key to unlock specific data segment(s) with proper access control based on users' roles & responsibilities or entitlements – fine grained policy to specify different control down to cell level.

The data protected with SEKURRA solution overcomes the biggest issue of market available data access control platforms, where in-app masking is the only way for protecting he data on-the-fly, as long a user accesses the data through the application portal.

Regardless if targeting Multipart computation, Cloud data protection or Offline sharing, SEKURRA service can improve the safety of the data stored in a lake or shared between different parties.

Developed by: **NTT DATA Romania, NTT Research, NTT DATA Inc**

SEKURRA
Advanced Data Protection



Take advantage of Adaptive-ABAC

- One technology for two critical functions: Encryption & Attribute Based Access Control at data layer
- Last Line of defense with efficient encryption and attribute based access control (ABAC) benefits
- Fine-grained policy based data access & sharing
- Data centric consistent protection with access control policy independent of layer

How Adaptive-ABAC?

- Microsoft Azure environment or on-premise
- Content-Based Access Controls - policies are associated with user's private keys, whereas attributes are associated with ciphertexts. A user can decrypt a ciphertext if and only if its attributes satisfy user's private key's policy
- Role-Based Access Controls - attributes are associated with users and policies are associated with ciphertexts. A user can decrypt a ciphertext if and only if its attributes satisfy the policy

Why Adaptive-ABAC?

- Highly secure lifetime protection embedded with protected data/file no matter where data/file is stored
- Independent from specific vendor software implementations, e.g., multi-cloud/multi-vendor strategy
- Minimize large scale data breach risk with strict access control policy for different data segments

NTT DATA

USE CASE

- Access Control Management
- Data monetization
- Sensitive Data Protection
- Zero-trust

SECTORS

- Banking
- Public Sector – Civilian, Digital citizenship
- Healthcare
- Retail & Consumer
- Insurance
- Utilities, Gas, Oil and Renewable resources
- Telco, Media & Entertainment
- Manufacturing & Automotive
- Travel & Transportation

DIGITAL FOCUS AREA

- Data & Intelligence
- Intelligent Automation
- Optimize IT
- Internet of Things
- Customer Experience
- Cyber Security