Elevating Dynamic Data Masking to Address Contemporary Data Privacy Needs

Abstract

Rapidly evolving and increasingly stringent data protection regulations such as GDPR require organizations to ensure the privacy of personally identifiable and other sensitive data - both when accessing and provisioning data for a purpose. Data masking is a key enabler of data privacy with Static Data Masking (SDM) ensuring privacy of data at rest and Dynamic Data Masking (DDM) ensuring privacy of data in real time.

Dynamic data masking provides controlled access to information, depending on the role of user wishing to access the information using dynamic masking policies configured for the role. This technology allows varying set of dynamic masking policies to be configured for a multitude of roles, thereby delineating the scope of access for each role. This conventional approach has worked well thus far. However, as is the case with many technologies, changing times are imposing new expectations on DDM.

This paper describes some of the new age scenarios of dynamic data masking and the components needed to address these emerging requirements.
Dynamic Data Masking: Meeting the Demands of the New Age

Role is no longer the sole governing factor that determines the scope and level of access to given information for application users. Data protection regulations have added new dimensions to access-control: consent provided by end citizen on the use of their data, location from where data is accessed, and the duration for which a given application can be accessed. In other words, only “role” may no longer be used to enable universal and perennial access to information.

This requires organizations to reimagine the approach of dynamic data masking by factoring in the new controlling influencers:

Location: Data protection regulations are sensitive to user’s location, i.e. the location from where information is accessed. Configuration of dynamic masking policies therefore needs to be enhanced to allow/restrict access based on the geographical location of the user attempting to access information. While “role” may continue to have minimal access across locations, the additional layer of location-based masking rules can join forces with role-based rules and define what cannot be accessed from given location(s).

Citizenship: Access to a certain kind of information may need to be restricted to natural citizens of a country alone. Dynamic masking policies need to be configured along with citizenship considerations for the role attempting to access the information.

Multi-national Business: With global business becoming the new norm, enterprises more often than not, end up storing data of individuals that are citizens of different countries. For instance, HR applications of multinational organizations could house details of employees from multiple countries. Dynamic data masking policies need to be configured to address the varying nature of data privacy requirements of the countries involved.

Citizen Consent: Increasingly, it is imperative to gel consent management systems with dynamic data masking. Data protection regulations emphasize that citizens have a strong
say in how their data is used. Therefore, DDM software must check for overriding consent-choices from the citizen consent database, in addition to validating role-based masking rules.

**User’s Age:** Data protection regulations particularly focus on data privacy of children. Applications (especially web-enabled ones) can explicitly ask users to confirm their age. Depending on the bracket in which user’s age falls, dynamic data masking rules can kick in and restrict specific sections of the website, or block the entire website, as needed.

**Device:** For enhanced security, organizations may opt to restrict access based on the nature of device trying to access information. For instance, they can mandate that certain information from an application may not be accessed through handheld devices such as mobile phones. In this case, dynamic masking rules must be configured for various device-types accessing the information.

**Duration:** The principle of data minimization promulgated by data protection regulations often requires that information must be accessed for a clear purpose and only during the life of the purpose. Any access to information beyond the scope of defined purpose and the duration of the purpose needs to be restricted. Here, dynamic data masking policies will need to be configured considering both the role and the time-dimension.

**Proposed Framework**

In order to factor in the impact of new age influencers in determining access to information, the existing DDM framework can be enhanced (see Figure 1) using the following approach:

**Identifying Location:** The framework for dynamic data masking should have a provision to identify location or integrate with location finder application. This is essential for enabling the identification of geographical location of user accessing the information and deploying dynamic data masking policies based on user location.

**Capturing Citizenship Status and Residency of User:** The citizenship and residency of the application user should be
captured in the data stores to enable restricted access to the authorized user in line with the appropriate data protection regulations.

Integrating with Consent Management Solutions: The framework must be equipped to manage user consent or must have the provision to integrate with third party consent management solutions to enable data masking policies based on consent, purpose, and duration of consent validity.

Enabling Access to Retention Duration: The framework must have access to the repository storing the data around retention period of sensitive information. This will enable application of data masking rules based on varying retention periods for each user role.

Designing Dynamic Policy Framework: Determining real-time and dynamic access permission requires the support of an enhanced policy framework. Such a framework must consider multiple combinations of elements such as geographical location, residential status, consent, retention period, and IP address to determine the level of access a user has to sensitive information. Also, the framework should be dynamic enough to accommodate additional parameters swiftly, in tandem with evolving data protection regulations.
Integrating with Application User Repository: The framework must be capable of consuming user roles (as defined in user applications and data sources) or integrating with applications such as Active Directory - to expedite the configuration of dynamic data masking rules.

New Approach to get Dynamic Data Masking Right

The advent of stringent data protection regulations such as GDPR creates a pressing need for dynamic data masking technology that goes beyond merely enabling role-based access. The right dynamic data masking technology can amalgamate the principles of data consent and data minimization to enable role-based privileges to access information and handle a combination of scenarios created by modern influencers of data access.
About The Authors

Jayant Dani
Jayant Dani is the Chief Architect of TCS MasterCraft DataPlus, an integrated data management platform. With over 23 years of experience in IT industry, Jayant played a leading role in setting up Big Data practice at Tata Consultancy Services (TCS). He currently spearheads the conceptualization, architecture, design, and engineering of TCS MasterCraft™ DataPlus. His expertise spans technical leadership of large solution teams, client relationship management, and large scale implementations management. Jayant is an OpenGroup Certified Master Architect and Data Security Council of India (DSCI) certified Privacy Lead Assessor. Jayant is passionate about architecting technology solutions across industry verticals and has many publications to his credit. Jayant holds a Master of Engineering degree in Software Systems from BITS Pilani, India.

Sumeet Bhide
Sumeet Bhide handles Market Research, Marketing, and Learning and Development aspects of TCS MasterCraft™ DataPlus product. He has around 18 years of experience in TCS. He has successfully delivered some key IT projects in the areas of reengineering and migration. His areas of interest include Data Management, Test Data Management, and Data Privacy. He holds a Bachelor of Engineering degree in Electronics and Communication Systems, from Gujarat University, India.

Sameer Rane
Sameer Rane is a Consultant for TCS MasterCraft™ DataPlus, an integrated data management platform. Sameer handles market analyst engagements and marketing for TCS MasterCraft™ DataPlus. He has 15 years of experience in the IT industry and has played a leading role in maintenance, deployment, and management of software products and solutions. An expert in the technical leadership of solution delivery teams and customer relationship management, Sameer holds a Master of Science degree in Electronics and Telecommunications from Mumbai University, India.

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Contact
Visit the TCS MasterCraft™ page on www.tcs.com
Email: mastercraft.sales@tcs.com

Subscribe to TCS White Papers
Feedburner: http://feeds2.feedburner.com/tcswhitepapers