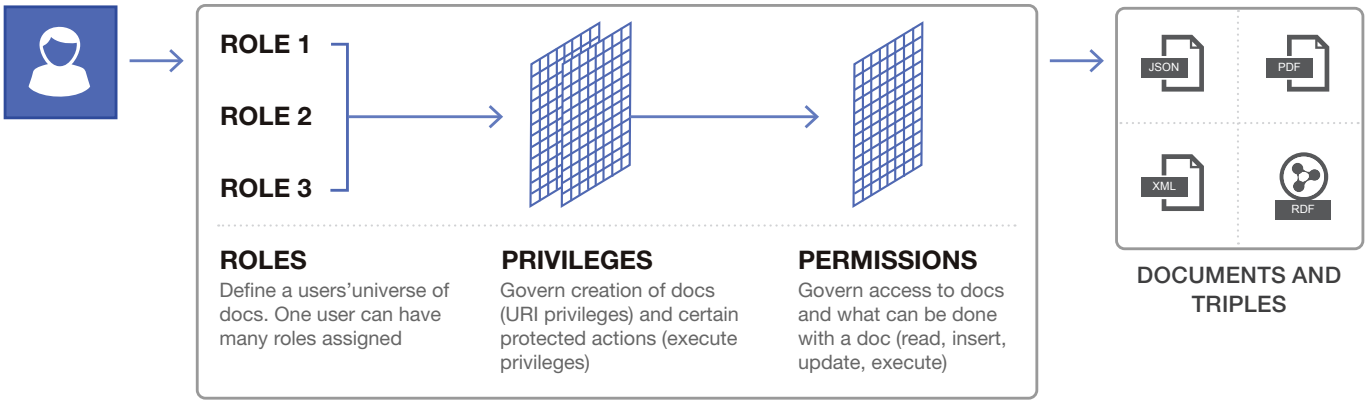
MarkLogic®

DATASHEET

Certified Security

Data security is critical to maintaining data integrity and trust. MarkLogic® has focused on having enterprise-grade security from the start, and has fine-grained, certified security that is required—providing a shield against today's cyber threats. It is for this reason that MarkLogic is chosen to run the most demanding, mission-critical applications at the heart of large investment banks, major healthcare organizations, and classified government systems.

ROLE-BASED ACCESS CONTROL AT THE DOCUMENT LEVEL



Key Aspects of MarkLogic's Security

Role Based Access Control (RBAC)

MarkLogic uses a document model to store data, and each document is governed by specific roles and permissions. By default, MarkLogic uses a role based access control (RBAC) security model in which each user is assigned any number of roles, and these roles are associated with any number of privileges and permissions. Privileges govern the creation of documents and execution of functions (URI and execute privileges) and permissions govern what can be done with a document (read, insert, update, execute). Security checks verify the necessary credentials before granting the requested action, and security information is stored in a specific security database in MarkLogic.

Certified for Mission-Critical Systems

MarkLogic is one of only six vendors that offers a database that is Common Criteria certified, and MarkLogic is the only NoSQL database with the certification. MarkLogic is also installed and operational on government systems that are PL3/ICD 503 and DITSCAP certified and accredited—top level certifications for classified systems in the US Intelligence Community and Department of Defense.

Common Criteria

The National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (NIAP CCEVS) provides an industry standard database security certification.

MarkLogic®

Advanced Encryption

Advanced encryption protects against unauthorized access of the database by a SysAdmin or Storage Admin. It allows data, configuration, and logs to be encrypted while the files are resting on disk using AES-256 encryption, and it conforms to FIPS 140 criteria. Encryption can be implemented using either an internal or external Key Management Systems (KMS).

Element Level Security

Element level security provides access control at the level of JSON properties or XML elements within documents, regardless of schema. Specific information inside a document may be hidden from users based on their role, while still providing access to other information in the document. Element level security is akin to "cell-level" security in relational databases.

Auditing

MarkLogic closely monitors database activity and makes it possible to audit document access and updates, configuration changes, administrative actions, code execution, and changes to access control.

External Authentication

MarkLogic supports external authentication using Lightweight Directory Access Protocol (LDAP) or Kerberos. MarkLogic also supports strong certificate-based authentication in Public Key Infrastructure (PKI).

Other Security Models

MarkLogic can also employ other security models, such as Attribute-Based Access Control (ABAC), Policy-Based Access Control (PBAC), or Label-Based Access Control (LBAC). These models further restrict access based on attributes (e.g., social security number, IP address, user's age, or time of day), policies, or simple labels representing "high" or "low" levels of trust.

Additional Options

Redaction

Redaction eliminates the exposure of sensitive information by making it possible to remove existing information or replace it with other values when exporting data or sharing. The process is simple, flexible, and is designed to work with large volumes of data.

External Key Management System (KMS) Support

This options makes it possible to use an external KMS (e.g., SafeNet or Vormetric) to help with advanced encryption, which is often done for the additional separation of concerns and ease of management.

Compartment Security

With compartment security, more complex rules can be applied to documents so that a user must have *all* of the right roles to access or create a document rather than just *one* of the rights roles. This is often useful when handling classified material.

About MarkLogic

MarkLogic is the world's best database for integrating data from silos, providing an operational and transactional Enterprise NoSQL database platform that integrates data better, faster, with less cost. Visit www.marklogic.com for more information.

MARKLOGIC CORPORATION
999 Skyway Road, Suite 200 San Carlos, CA 94070
+1 650 655 2300 | +1 877 992 8885 | www.marklogic.com | sales@marklogic.com