Document WorkBench™ for **High Security** Enterprise Content Management

High Security Implementation ensures adequate protection of valuable Information Assets

Document WorkBench™

Highlights

- Highly Secured.
- High Performance.
- Features Rich
- Highly Scalable
- Yet, easy to operate and manage.

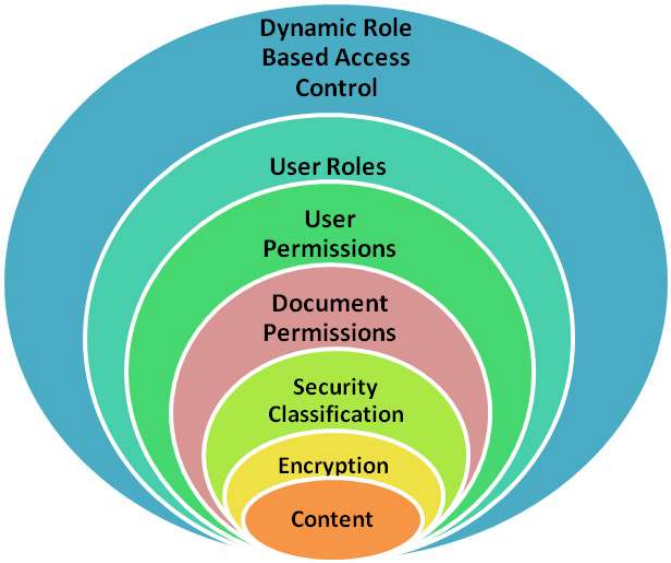
The Threats of Inadequately Protected Information Assets

Every organization maintains information that must be kept private. In today's business fraternity where corporate sensitive information is growing at phenomenal rates, failure to protect classified document and data content from unauthorized access or manipulation can prove to be immensely costly. In addition to the difficulty of keeping track and managing the growing volume of document content in varying sensitivities, security threats such as computer hacking, theft, fraud and sabotage are looming larger every day. Without a proper system to store and manage sensitive documents and allow only authorized access by appropriate personnel, classified proprietary information may likely fall into wrong hands which may have damaging consequences to an organization.

Document WorkBench™ High Security Solution

Document WorkBench™ is an award-winning Enterprise Content Management Solution recognized in the industry to be secure and robust. It is created with an underlying security concern in mind – protecting one's valuable Information Asset, and it is not only a complete suite of products that caters to the needs of organizations in managing their Complete Information Life-Cycle, but it also builds on State-of-the-Art encryption technology and incorporates many security features. Compared to conventional systems that provide encryption as an add-on layered module, Document WorkBench™ embeds inherent encryption into its architecture to ensure a complete protection mechanism while ensuring high performance by providing scalability to handle high volumes of documents.

Document WorkBench™ DRBC Security Architecture



Dynamic Role Based Access Control (DRBAC)

Document WorkBench™ DRBAC's implementation observes the followings:

1. **Principle of Least Privilege**; for achieving integrity objective where a user is given no more privilege than necessary to perform a job.
2. **Separation of duties**; for deterring fraud, e.g. Security Officer and System Administrator are 2 separate roles; Security Officer role is responsible for access control assignment while System Administrator takes care of administrative activities.
3. **Data abstraction**; to separate abstract properties of a data type from concrete details of its implementation.
4. **Positive visibility control**; to control documents visibility in search results according to a user's privilege with minimum performance impact in Content search.
5. **Document centric dynamic permissions control** using a key and lock concept for access control to Content.

Security Classification

Security classification helps group and identify documents by their sensitivity nature and associated user roles. There are up to 35 levels of security classification. The system also allows the ease of upgrading or downgrading the security classification by the System Security Officer (SSO).

Effective Permissions

Effective permissions ensure each user is provided with just sufficient access rights to carry each task efficiently while providing the administrative ease in maintaining a large and complex organization having a large number of different entities i.e. users, roles, departments, document types etc. Specific permission privileges or rights are assigned separately and independently to the different entities and the effective permissible access is the result of the mapping between the associated entities.

End-To-End Encryption

End-to-end encryption prevents revelation of sensitive information to anyone who tries to bypass security set up by utilizing the operating system level functions to access the documents since all documents are entirely encrypted and continually encrypted throughout the system from the moment it is captured until it reaches the final point, i.e. viewing, printing etc. Once stored and encrypted, the document stays encrypted, even in transmission. Any modification creates a new version while the original version remains intact.

Random Encryption Key Generation

Random encryption key generation renders any stolen keys useless because such keys are not re-used in subsequent user access. Every single transmissions of the document content from the server repository to the client function are based on the randomly generated unique encryption key. For transmission over the internet domain, public key can be utilized instead.

Print Control

Print restriction of specific documents to specific users may not only help to reduce the wastage of paper usage but also ensures that sensitive documents are not unnecessarily reproduced in hard copy form. Watermarking can be added to document printed to enhance traceability and trade mark protection.

Advanced Access Authentication

In addition to username and password verification, card key access verification can be incorporated into the system for two factors authentication and non-repudiation for added security control in user's access of highly classified document.

Support for External HSM Module

Document WorkBench™ High Security Solution supports external HSM system for alternative encryption keys and credential management.

For enquiries, contact

1. Sales Enquiry: sales@i-maginationgroup.com
2. Partner Program Enquiry: sales@i-maginationgroup.com
3. Tel: (65) 6490 9588
   Fax: (65) 6490 9599