

## White Paper



### Enterprise Data Security an Important Business initiative Master Data Management the silver bullet

---

Jairaj Asok Kumar

#### Abstract

Information security is a business imperative. Data security is cited as a top priority by the organizations and it is getting the largest share of enterprise IT budgets for the coming year.

Today's challenging market conditions and increasing enforcement of data privacy regulations make safeguarding your data more important than ever. Doing business is hard enough without the negative publicity and loss of business associated with data breaches and regulatory failures. Data security is critical to maintaining your customers' and partners' trust. By protecting data at the source-the following business imperatives are achieved:

- Lower the overall cost of securing your data
- Protect all aspects of your business from lost data
- Ensure compliance with data privacy regulations

This thought paper explores the concept of having an MDM implementation as the starting point for looking at your customer data and ensuring that security is built up, from the most essential element in your value pyramid, your end customers. Let us then explore the need for security, how it can be developed across a customer centric initiatives through a real life scenario.

For more information, Contact [askus@infosys.com](mailto:askus@infosys.com)

## Enterprise Data Security a Business imperative

Enterprise security is a much talked about concept in the current business environment. It is a definitive business imperative which is evoking interest within the CXO's. But does enterprise security figure in the key issue within the business stakeholder's community, definitely not or least likely?

Enterprise security means protecting the informational asset, the life blood of your organization, as enterprise data is discovered and is consumed at real time by employees, partners, and customers. Enterprise security gets complicated based on the three most critical paradigms:

- The compounding amount of information that companies have to store, secure, and manage;
- The increasing infrastructure complexity within the organization; and
- The diversity of government and industry regulations with which organizations must comply.

As data traverse through the plethora of network, there is high incidence for data getting compromised. It is next to impossible, to predict and ascertain that the data is foolproof (i.e. confidential) because hackers and people, who indulge in data theft, uses innovative ways and means to poach data and therefore a pre-emptive and proactive approach to managing the security issue is a must. This thought paper helps in discussing why we need Enterprise Data security, how an MDM implementation is the starting point for Enterprise data security.

## Master Data Management Implementations a starting point for Enterprise Data Security?

Fragmented approach for managing enterprise security is not good enough. It is essential that an enterprise wide security assessment program be taken along with a Master Data Management (MDM) implementation. MDM along with an underlying data governance program helps to bring into focus the need to look at information and hence forms the key starting point for evaluating security. Data stewards and data owners help to classify the enterprise data and helps in evaluating the rights of using this data across various stakeholders in the enterprise.

MDM looks at security implemented within its internal domain as Non Functional Requirements (NFRs) enforced by transaction level security (security of who should be able to run a transaction) and by data level security (who has the right to view and modify the data). MDM looks at external level security implementation by enforcing that the MDM solution be hosted in a secured or restricted zone. Additionally it enforces security by using the Application server features, which by default focuses on integration with third party tools like Light weight Directory Access Protocol (LDAP). The seamless integration of an MDM with an LDAP helps managing the Access Control lists (ACLs) to the data; determine the fine grained and coarse grained access to data through transactions, evaluating the Segregation of Duty (SOD) on who should be allowed to do a Create Read Update and Delete (CRUD) operation, classification of data, preferences of consumption of the data with organization and channel partners, etc.

Now that we know that an MDM implementation is the starting point for most Enterprise Architecture consolidation initiative, it is essential that the data owners or business stakeholders evaluate the master data and determine the rights for ownership of the master data.

## Business drivers to take up Enterprise Data Security using MDM

There are many business drivers for undertaking an Enterprise Data Security within an MDM solution. The key elements are listed below

- Regulatory requirements and compliance to SARBOX and governmental regulations
- Customers willing to pay a premium for ensuring that they have the sufficient level of anonymity by not having their personal data shared across channel partners and opting to participate in anti-spam and in do-not-call registry, where based on preference they would like to be contacted through various mechanism or delivery channel, if and only if there is a value in obtaining such personalized or customized communication.
- The loss of customer data would lead to financial losses, whereby if personal data is compromised a huge financial burden will have to be expended by the organization.
- Clear differentiator of having a risk based alignment to the way master data management is utilized within the organization.

## Enterprise Data Security the maturity curve

Enterprise Data Security considers various pillars to support that master data is not tampered and is being accessed for view or update by the right associate/consumer. The critical elements to be considered in Enterprise Data Security, especially from an MDM implementation perspective are

- Confidentiality – This indicates whether the data in transmission has not been viewed by any other entity. This is typically implemented in MDM solution using X509 certificates and hosting the MDM solution in secured zone.
- Integrity – This indicates whether the data has been tampered during transmission. This is typically implemented in MDM solution using secure socket layer communication (HTTPS) when required.
- Non-repudiation – This indicates whether the operation once confirmed can be further reviewed to ensure that there is trueness in the way the operation has been done, from the point of initiation to the point of consumption.
- Authentication – This indicates whether the end user is who he/she claims to be. This is usually implemented in MDM solution, using user name tokens (user id)
- Authorization – This indicates whether the end user has the rights to perform an operation. This is usually implemented in MDM solution, using an LDAP

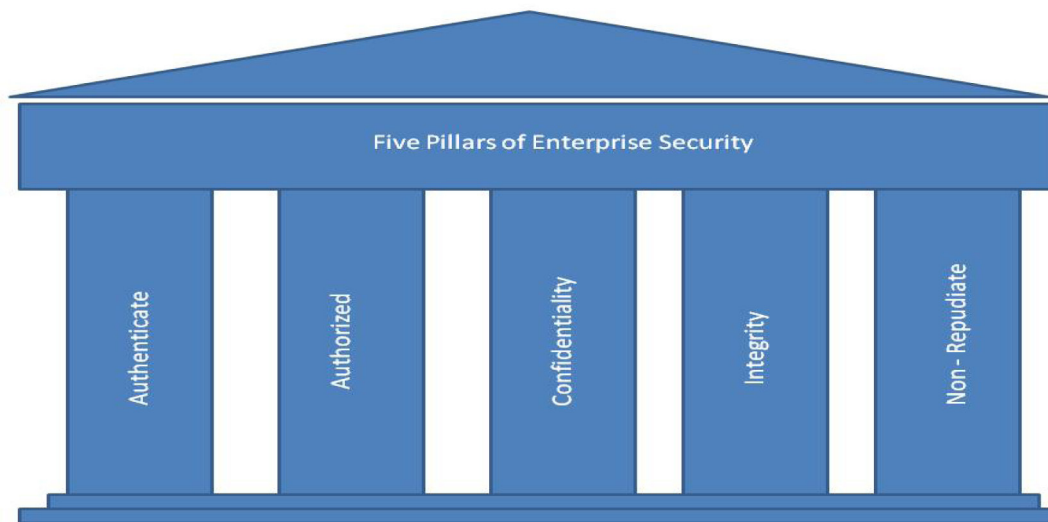


Figure 1 - Pillars of Enterprise Data Security

## Best Practices to overcome Enterprise Data Security challenges

This section now drills into the best practice to be implemented in an organization to overcome the Enterprise Data Security challenges.

- Evaluate a regulatory or compliance requirement that addresses security within your domain space. For example SARBOX compliance, HIPAA compliance, PCI-DSS, Basel 2, etc.
- Undertake an assessment of your existing IT Landscape and evaluate the investment to be set towards achieving a target IT landscape
- Assign a portion of your overall IT expenditure to build security from the grass root level
- Re-evaluate security during each phase of the project
- Ensure a Chief Risk Officer is appointed who could evaluate the risk/threat/vulnerability matrix of Enterprise data security
- The weakest cog in the security link is you, so start looking at security with you as the starting point.
- Educate others the need to have security and undertake a Segregation of Duties matrix.
- Classify your data security into various levels and determine the access rights and responsibilities of who should own the data.

## Case Study

### Enterprise Data Security

This case study refers to a retailer, who had considered that in addition to doing a customer centric MDM implementation, it requires to undertake an extensive Enterprise data security assessment program. The customer data that was in data silos between departments had absence of a central control on customer data. This led to an enterprise initiative of undertaking a security risk assessment and information classification exercise to handle security threats. The retailer was planning to diversify into banking segment by issuing credit card along with an issuing partner and had to obtain its entire IT landscape certified to comply with Payment Card Industry– Data Standards and Security regulatory requirements. It then classified the IT landscape into four clover leaves or domains, E.g. B2E, B2C, B2B and Stores, with MDM (along with supporting Access manager and Authorization engine) being the central hub by which security is managed. The central repository of profile data, be it its end customer or its internal staff or augmented support staff, where managed from a Central Tivoli Access Manager. The Tivoli Access manager was used to hold the fine grained permissions along with roles and responsibilities at a centralized level, with the profile data being validated across the various consumption points.

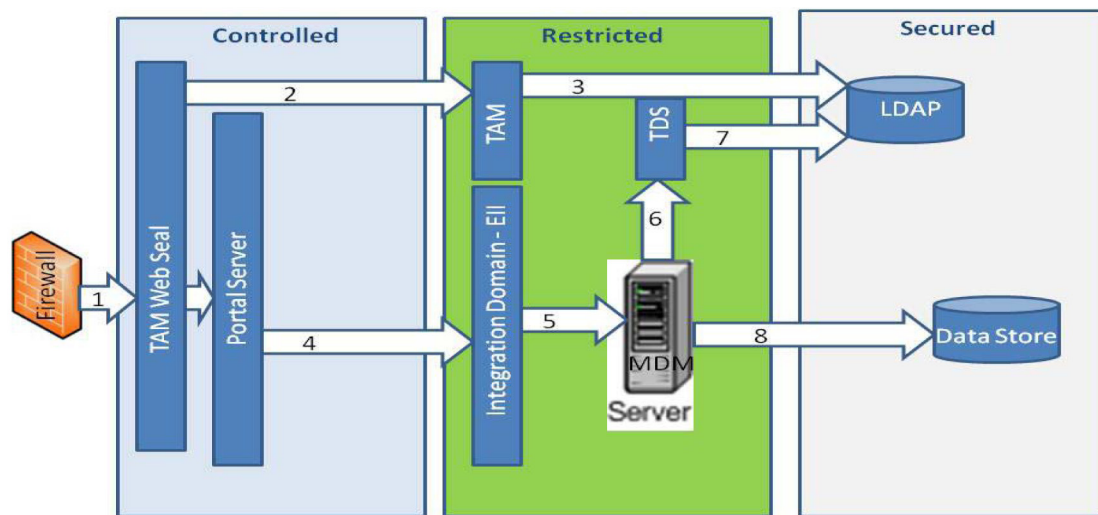


Figure 2 Master Data Management Server - Case study for Enterprise Data Security

The critical requirements for the above were driven based on the following NFRs in Master Data Management solution. The Payment Card Industry – Data security standards mandates that the critical data related to customer (credit card data) be masked in transmission. Additionally it also mandated that master data be classified for access by various role (in terms of who can update what, who can view what data etc). The implicit requirement was to plan where the MDM solution was hosted. The line of action was to have the MDM data store in the secured zone, and the various domains that acts as abstraction for the master data services to be hosted in the restricted zone. Additionally any consuming application from a non-secure zone had to have a look up with the central LDAP repository to obtain the principal profile data of the consumer (user name, roles and access rights/permissions). The same was then sent along with the request so that it could be evaluated at the Application server layer, in terms of Authorization. The Webservices based calls, were complimented with X509 certificates to ensure that WS-i\* security compliance were adhered to.

Master Data management also has the capability to provide rule based access to update/view the data, implemented through the Rule of Visibility features. The Transaction audit log feature supported capture of what transactions were performed and by whom.

As depicted in the diagram the complete end to end work flow was as below

- The master data consumption application from uncontrolled zone was initially authenticated at the Tivoli Access Manager Web seal to validate whether the user is someone who the organization is aware of.
- This was done by validating the user profile (user id) along with the Tivoli Access Manager
- The Tivoli Access manager did the verification with the centralized LDAP data store

- If the user was authenticated, the user id and permissions were passed along to the integration domain using Secured socket layer data transmission (where applicable) and attached with an X509 Digital certificate
- The integration domain where the user id and permission were further passed to the consuming application, where the X509 certificate was verified.
- Further the access to the perform the operation was validated against the Tivoli Directory Server
- There were subsequent lookup against the LDAP data store
- In case the user is authenticate and authorized to perform the transaction, MDM Server allows the request to be auctioned upon by the master data services. Over and above, the Rule of Visibility engine (ROV) further validated the access right in terms of view/update based on the permissions assigned to the end user.

## Conclusion

An MDM implementation thus ensures that the organization is protected at the various levels (infrastructure, data access/ consumption and data storage) against threats, infiltration, and loss of data. In the security paradigm, the weakest link is “you” or the project you initiate, so it is the responsibility of the primary stakeholder or the project sponsor, to ensure security strategy is imbibed into the day to day operations. An MDM implementation where customer data is secured across consumption points, within your value chain by your organization staff, by your customers and by your value partners is thus an effective starting point. Security strategy should be seen as a business enabler and the most critical assets, “your customer, your employees and your partner details” should be protected effectively at a centralized level, none other than through the Master data management program.

## References

- Enterprise Security: Guard that Data – by Shrikanth G
- Overview of Master Data Management Server security- by Miguel A Ortiz, Jr and Lee McCallum

## About Author

Jairaj is a Lead consultant at the Master Data Management (MDM) practice in Infosys. He has more than a decade of experience in leading the delivery of information management solutions (web application and business intelligence applications) for global companies in banking, insurance, high-end technology and retail in the U.S., U.K. and Australia.

Jairaj is an expert in MDM service-based offerings in data rationalization and consolidation, skill building through training and developing assets, re-usable artifacts and templates for MDM. He also has experience in information management consulting, channel partner accreditation/business process re-engineering/business transformation using web application and business intelligence/data warehousing.



For more information, contact [askus@infosys.com](mailto:askus@infosys.com)

## About Infosys

Many of the world's most successful organizations rely on Infosys to deliver measurable business value. Infosys provides business consulting, technology, engineering and outsourcing services to help clients in over 30 countries build tomorrow's enterprise.

For more information about Infosys (NASDAQ:INFY), visit [www.infosys.com](http://www.infosys.com).