

Holistic business approach for the protection of sensitive data

"Study of legal requirements and regulatory compliance at international level to define and implement data protection measures using encryption techniques"

Jose Luis Naranjo

TFM: Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Diciembre 2018



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FICHA DEL TRABAJO FINAL

Título del trabajo:	Holistic business approach for the protection of sensitive data <i>"Study of legal requirements and regulatory compliance at international level to define and implement data protection measures using encryption techniques"</i>
Nombre del autor:	<i>Jose Luis Naranjo</i>
Nombre del Supervisor:	<i>David Hernández García</i>
Fecha de entrega (mm/aaaa):	12/2018
Titulación:	<i>Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones</i>
Área del Trabajo Final:	<i>Ad hoc (Regulaciones de protección de datos y soluciones de cifrado)</i>
Idioma del trabajo:	<i>Inglés</i>
Palabras clave	<i>Encryption, Data Protection, Regulations</i>

Resumen del Trabajo (máximo 250 palabras):

La finalidad de este trabajo es mostrar el desafío de la protección de datos al que se enfrentan las empresas hoy en día para cumplir con los requisitos relevantes de las regulaciones existentes, y, por otro lado, identificar el uso del cifrado como solución para cumplir con dichos requisitos.

Para ello se llevó a cabo una metodología híbrida, entre investigación y práctica, analizando por un lado las regulaciones actuales y las soluciones de cifrado, y por otro, desplegando y probando una de las soluciones en distintos casos de uso para el cumplimiento con las regulaciones.

Como conclusiones observamos que vivimos en un mundo donde, los rápidos avances tecnológicos, conllevan la creación y modificación de leyes y regulaciones sobre protección de datos, a las que las empresas deben someterse y estar preparadas, existiendo una gran dependencia del cifrado de datos para el cumplimiento de los requisitos. Así que las empresas tienen que apoyarse en las soluciones de cifrado que existen en el mercado. Respecto a la solución de cifrado probada, Vormetric, cuenta con un amplio repertorio de herramientas y productos que a primera vista parecen ser capaces de cumplir con los requisitos solicitados por cualquier regulación que una empresa deba enfrentar en términos de protección de datos, ya sea en sus instalaciones, la nube o en entorno híbrido.

Como líneas de trabajo futuro, la configuración de un sistema de monitorización de seguridad, y la implementación y configuración de políticas de almacenamiento y retención de acuerdo con los requisitos de las

regulaciones.

Abstract (in English, 250 words or less):

The purpose of this work is to show the challenge of data protection faced by companies today to meet the relevant requirements of existing regulations, and, on the other hand, to identify the use of encryption as a solution to comply with these requirements.

For this, a hybrid methodology was carried out, between research and practice, analyzing on the one hand current regulations and encryption solutions, and on the other, deploying and testing one of the solutions in different use cases for compliance with regulations.

As conclusions we observe that we live in a world where, the rapid technological advances, entail the creation and modification of laws and regulations on data protection, to which companies must submit and be prepared, existing a great dependence on data encryption for the compliance with the requirements. So companies have to rely on the encryption solutions that exist in the market. Regarding the tested encryption solution, Vormetric, it has a wide range of tools and products that at first glance seem to be able to comply with the requirements requested by any regulation that a company must face in terms of data protection, whether in its facilities, the cloud or a hybrid environment.

As future lines of work, the configuration of a security monitoring system, and the implementation and configuration of storage and retention policies in accordance with the requirements of the regulations.

INDEX

1. Introduction	1
1.1 Data Privacy Compliance & Regulation	1
1.2 Financial, Medical & Private Individual data regulations	2
1.3 Objectives	2
1.3.1 Approach and method followed	2
1.3.2 Work Planning	3
2. Analysis of Main Regulations	5
2.1 GDPR	5
2.2 HIPAA	7
2.3 PCI-DSS	10
2.4 Encryption application	11
3. The World of Encryption	13
3.1 Encryption	13
3.2 Data Definitions & Classification	13
3.2.1 Commercial Classification	14
3.2.2 Government Classification	15
3.2.3 Restricted Information Types	15
3.3 Encryption Schemes	17
3.3.1 Regular (Unstructured) Data Encryption	18
3.3.2 Selective Encryption	19
3.3.3 Format-Preserving Encryption (FPE)	19
3.3.4 Searchable Encryption	20
3.3.5 Keyword extraction	20
3.3.6 Word-by-word	20
3.3.7 Local search tokenization	21
3.3.8 Search by prefix	21
3.3.9 Order-Preserving Encryption (OPE)	21
3.3.10 Data Tokenization	22
3.3.11 Fully Homomorphic Encryption	22
4. Encryption Solutions	23
4.1 Hytrust	24
4.2 SafeNet – GEMALTO	25
4.3 Thales: VORMETRIC	26
4.4 Encryption Solution Selection	26
4.4.1 Compliance with Laws and Regulation	27
4.4.1.1 GDPR	30
4.4.1.2 HIPAA	31
4.4.1.3 PCI-DSS	31
5. Experimental Analysis	34
5.1 Vormetric in depth	34
5.2 Vormetric deployment on Cloud	40
5.2.1 Securing health data in the cloud	40
5.2.1.1 Introduction	40
5.2.1.2 Architecture	41

5.2.1.3	Control Access	41
5.2.1.4	Data Encryption with VTE and Rekey Process	43
5.2.1.5	Deployment and Configuration	46
5.2.2	Securing financial data in the cloud	46
5.2.2.1	Introduction	46
5.2.2.2	Architecture	46
5.2.2.3	Components.....	48
5.2.2.4	Control Access	48
5.2.2.5	Analysis of data to be secured	49
5.2.2.6	Deployment and Configuration.....	51
6.	Conclusions and Future Work.....	52
7.	Glossary - Acronyms	53
8.	References.....	54
9.	Annexes	56
A.	Worldwide Regulations	
B.	Basic Best Practices for Regulation Compliance	
C.	Encryption Solutions: Hytrust & SafeNet	
D.	Experimental Analysis Use Cases Deployment	

Lista de figuras

- Figure 1: Research Procedure
- Figure 2: Practical Procedure
- Figure 3: Work Planning
- Figure 4: HIPAA
- Figure 5: Security's Safeguards
- Figure 6: Hytrust's Features
- Figure 7: Vormetric's Features
- Figure 8: PCI-DSS Requirements
- Figure 9: Vormetric Products Features
- Figure 10: Security Managed Controls
- Figure 11: Transparent Encryption work flow
- Figure 12: Encryption Key Manager
- Figure 13: Single Pane of Glass
- Figure 14: Access Control
- Figure 15: Agents and Guardpoints
- Figure 16: Application Encryption
- Figure 17: Application Encryption example (credit card)
- Figure 18: Tokenization with Dynamic Data Masking
- Figure 19: Tokenization example
- Figure 20: Vault-lessTokenization -Scale
- Figure 21: Transparent Encryption for Health use case
- Figure 22: Health use case Architecture
- Figure 23: Vormetric Data Security Overview
- Figure 24: Guardpoints
- Figure 25: DataxForm
- Figure 26: Live Data Transform
- Figure 27: Rekey Manual Coping Process
- Figure 28: Rekey DataxForm Process
- Figure 29: Rekey LDT Process
- Figure 30: Encryption Options Comparative
- Figure 31: Financial use case Architecture
- Figure 32: Users Control Access Actions
- Figure 33: Encryptions keys configured and deployed
- Figure 34: Token Groups configured and deployed
- Figure 35: Token Templates configured and deployed
- Figure 36: Token Template configuration example
- Figure 37: Tokenization Types

1. Introduction

1.1 Data Privacy Compliance & Regulation

In the current shift towards digitalization that continues to reshape industries, data remains front and center as the most valuable business asset. Thus, organizations are creating, sharing and storing data at an unprecedented level that continues to reshape industries, data remains front and center as the most valuable business asset.

Customers trust businesses to keep their data safe, and those businesses that operate globally face a complex patchwork of data protection regulations. In one survey after another about the adoption of cloud computing, CIOs and other technology leaders readily admit that their top concern is data security.

Helping to protect the confidentiality of data under companies care, there is a growing number of government and industry regulations and standards designed. This area has an obvious need for guidance due to the number of software vulnerabilities and actual data breaches. Unfortunately, many of the companies that experienced those breaches, which weren't ready and prepared, are now facing lawsuits filed by individuals, investors and other entities that claim they were harmed by the exposure of their information.

The pressure on Companies to maintain data confidentiality is really high, and so they turn to a variety of technologies to help protect the data. Encryption is a highly effective technology that is widely used to hide the real value of private or confidential data. Most organizations, being proactive, trying to prevent the loss of real data in the event of a breach, have chosen to encrypt sensitive data, but now many companies are also asking also whether encryption is actually required by law or not.

Until recently, the focus has been on encrypting data on-premises – within applications and databases, on laptops and desktop PCs, in transit on the network – all within an organization's own data center and network. With so many businesses now storing data in the cloud, data is moving off-premises and is handled by third-party cloud providers. This prompts us to look at the legal case for encrypting data in the cloud.

IT departments have been always dealing with Information Security, facing it as a strange issue. Organizations need to be concerned with complying with information security from top to bottom. Regulations, as laws, are there to help companies to improve information security, since in case of non-compliance would probably result in severe fines. Due to the many different sets of laws, it is never easy for a company to understand which regulations apply to them and which ones do not.

It is a fact that regulations require data protection. In and of themselves, laws and regulations pertaining to data protection and privacy do not guarantee that data breaches will not occur, and that private or sensitive data will not be exposed to unintended or unauthorized access. Nonetheless, companies that observe the regulations by putting the appropriate protective measures in place are far less likely to suffer a debilitating breach.

A high number of countries around the world have adopted comprehensive data protection laws. Some of these regulations on data protection and privacy, as well as industry specific regulations explicitly, require data encryption, while others leave the choice of protection measures to the data guardians. Most of the regulations contain provisions for stiff penalties for inadvertent disclosure of sensitive data that can be avoided if the data is encrypted.

1.2 Financial, Medical & Private Individual data regulations

There is a vast amount of regulations around the world that require companies to comply with them. Being out of the scope of this TFM the in-depth analysis of all of them, you can find a brief summary of the most important and known in the **annex "A" (Worldwide Regulations)**. For this reason, the following sections will describe those laws, regulations and standards that apply to the protection of financial, medical, private and/or confidential data that currently exist throughout the world, focusing only on three international regulations of the different areas to have an overall view:

- **The EU General Data Protection Regulation (GDPR)**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Payment Card Industry Data Security Standard (PCI DSS)**

1.3 Objectives

This TFM has two main objectives as its purpose. The first one, to show the challenge of data protection which companies are facing nowadays to meet the relevant requirements of existing laws and regulations. And, on the other hand, the use of encryption as a solution to comply with the requirements demanded by these regulations. Within this second point, there will be a study of the market solutions for encryption, and an analysis by describing their characteristics and features, applications and uses of the regulations, to justify the use of one of them as the most appropriate to perform the experimental tests and evaluate its robustness over the requirements analyzed in the first objective.

Below, the partial goals to be achieved with the completion of this work are listed and described and thus achieve the objectives described above:

1. Show a vision of the vast number of laws/regulations in force along with their requirements that apply to companies dealing with personal, banking and health information.
2. Explanation of the need for the use of encryption for the protection of data and information.
3. Identify the uses and applications of encryption for compliance with laws and regulations.
4. Analysis of current encryption market solutions.
5. Study, theoretical and practical, how the chosen encryption solution can help companies solve problems related to compliance with regulations.

1.3.1 Approach and method followed

For the development of the TFM, a hybrid methodology has been followed between research and practice. Next, the marked procedure for the elaboration of the TFM is shown:

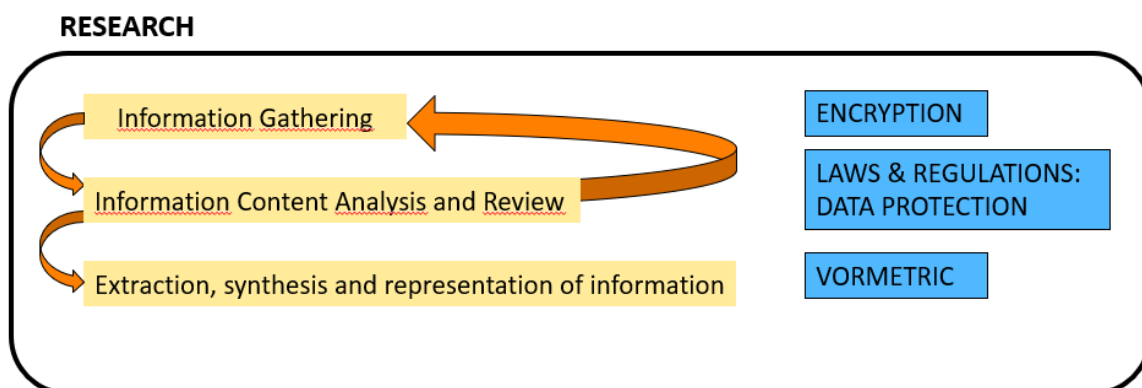


Figure 1: Research Procedure

- The process for each of the points on which a research methodology was applied, consisted of the following steps:

- Search and compilation of information on each of the subjects in question (the world of encryption, the current laws and regulations on data protection, and finally, encryption solutions features).
- Once the information had been collected, an analysis of its content was carried out, evaluating whether it covered the needs of the scope of the work to show the ideas and concepts desired. If not, new searches were carried out until the result complies with what was expected.
- As a last step, with the information acquired, the most relevant information was extracted, whose contribution to the TFM was considered of greater value, processing and synthesizing it for later presentation.

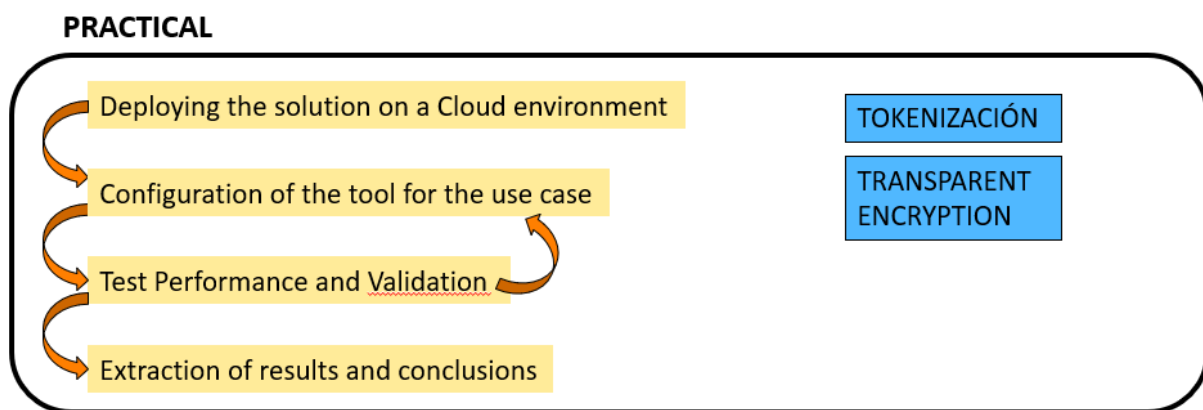


Figure 2: Practical Procedure

- The process for each of the points on which a practical methodology was applied, consisted of the following steps:

- As a starting point of the process, the deployment (installation and configuration) of the tool was carried out in a cloud environment.
- Next, for each of the use case to study ("Tokenization" and "Transparent Encryption"), the appropriate configurations was done.
- Once configured, the tests and tests designed for the case study weree carried out. In case of error, or unexpected results, roll-back to the previous step, to make the necessary modifications in the configuration.
- Finally, after completing the tests, the results were analyzed for the extraction of the conclusions.

1.3.2 Work Planning

The following image shows the outline/diagram of the temporal planning for the activities carried out in this TFM. For this, the estimated duration of the effort of each one of them was considered, and the existing dependencies, to identify the content of the work deliveries, PEC1, PEC2, PEC3 and PEC4, the final report.

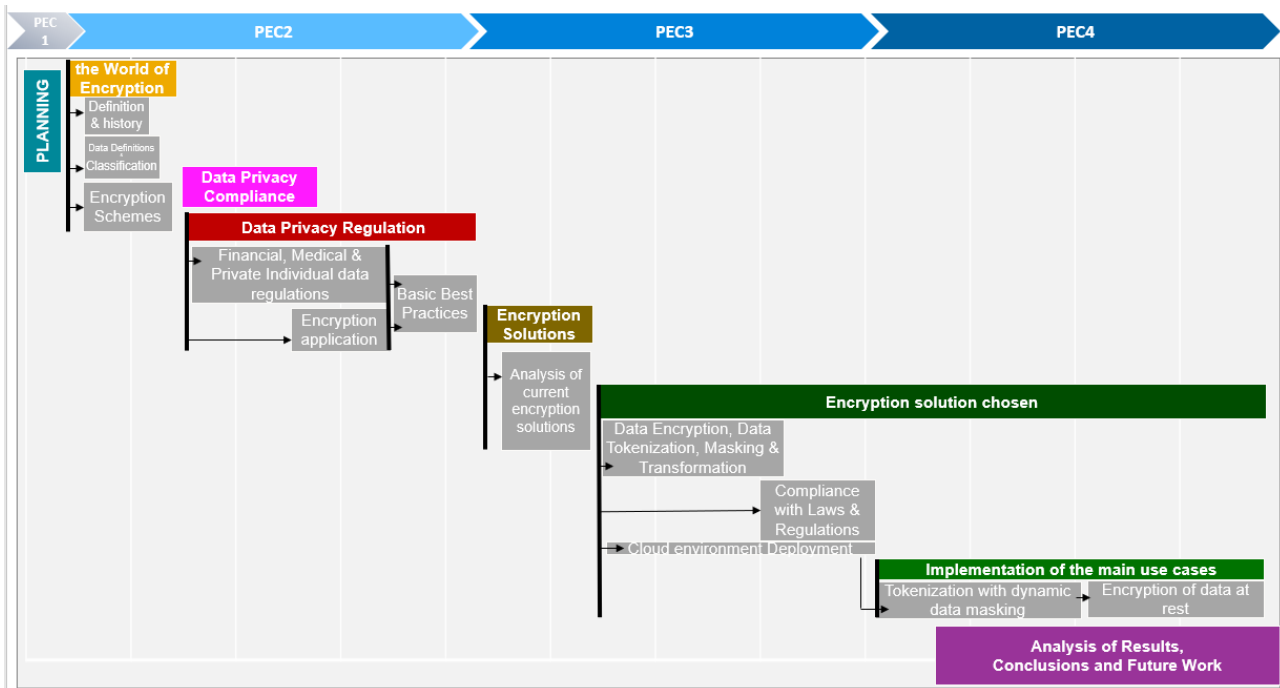


Figure 3: Work Planning

2. Analysis of Main Regulations

In this section we will describe the three regulations on which we will emphasize in this TFM: **GDPR**, **PCI-DSS** and **HIPAA**. As indicated previously, a brief description and information on a large representation of the current data protection regulations can be found in **Annex A (Worldwide Regulations)**. In the same way, in **Annex B (Basic Best Practices for Regulation Compliance)**, basic practices are described to follow for compliance in a generic way with the regulations.

2.1 GDPR

The General Data Protection Regulation (GDPR) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals' personal data within the European Union. GDPR reshapes the way organizations must approach data privacy, not just in the EU, but across the globe. GDPR regulations apply to the personal data of any individual in the EU, wherever information is handled.

IMPACT:

- Penalties up to 4% of annual worldwide turnover or €20 million, whichever is greater
- Cost of implementing compliance measures
- Recertification costs
- Negative impact on share price
- Lower sales volume & revenue

REGULATORY REQUIREMENTS

<ul style="list-style-type: none"> • Data protection officer <ul style="list-style-type: none"> ○ Appoint data protection officer ○ Assign roles and responsibilities within organization 	<ul style="list-style-type: none"> • Security mechanisms <ul style="list-style-type: none"> ○ Data inventory and process landscape ○ Control systems ○ Risk management and risk mitigation
<ul style="list-style-type: none"> • Accountability <ul style="list-style-type: none"> ○ Roles & responsibilities defined within organization, RACI ○ Policies, processes & procedures 	<ul style="list-style-type: none"> • Consent <ul style="list-style-type: none"> ○ Freely given, unambiguous, specific ○ Minors (under 16) ○ Withdrawal of consent
<ul style="list-style-type: none"> • Privacy by design <ul style="list-style-type: none"> ○ Technical and organizational measures to protect personal data ○ Retention periods 	<ul style="list-style-type: none"> • Notification process <ul style="list-style-type: none"> ○ Communicate data breach <ul style="list-style-type: none"> ▪ to individual ▪ to authorities within 72h
<ul style="list-style-type: none"> • Individual rights <ul style="list-style-type: none"> ○ Increased individual rights concerning personal data 	<ul style="list-style-type: none"> • 3rd party risk management <ul style="list-style-type: none"> ○ Controllers and processors share accountability in data processing

ORGANIZATIONAL CHALLENGES

<ul style="list-style-type: none"> • Regulatory Requirements • Unknown Data Supply Chain • Poor Data Quality • Duplicate Data 	<ul style="list-style-type: none"> • Advanced Security Need • Lack of Ownership • Dispersed Data • Manual Process
---	---

BENEFITS OF COMPLIANCE

<ul style="list-style-type: none"> • Improved data quality & data operations • Aligned security strategy • More data-driven business decisions 	<ul style="list-style-type: none"> • Sustainable value from data • Culture of data responsibility • More value from customer data
---	--

- Educated employees

- Competitive advantage as a trusted brand

Protecting personal data through privacy & security principles

GENERAL DATA PROTECTION REGULATION

- Harmonizes data protection across the EU and is overseen by a European Data Privacy Board & local regulators
- Widened scope (territorial and subject scope) with stricter rules for sensitive types of data, e.g. health, biometric, ethnic, etc.
- Stronger enforcement with painfully high penalties
- Increased accountability (DPOs are mandatory, direct obligations and liability for controllers and processors)
- Enhanced data subject rights (erasure, rectification, portability etc.)

PRIVACY PRINCIPLES

- Lawfulness, fairness, transparency
- Purpose limitation
- Minimization
- Accuracy
- Storage limitation
- Integrity & confidentiality
- Accountability

SECURITY PRINCIPLES

- Pseudonymization & encryption of personal data
- Confidentiality, integrity, availability, resilience
- Restore availability & access to data timely in case of physical or technical incident
- Process for regular testing, assessing & evaluating technical & organizational measures

Requirements: Data Protection & Security

Technical and organizational security measures include pseudonymization and encryption, the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems, the ability to restore the availability and access to personal data in a timely manner, and a process for regularly testing and evaluating the effectiveness of technical and organizational measures (Art.32).

Recommended Privacy Management Activities

- Maintain technical security measures, such as DLP, firewalls, and anti-malware.
- Maintain security protections for data-at-rest and in-transit.
- Maintain and regularly test Business Continuity and Disaster Recovery plans.
- Manage information obfuscation mechanisms, such as encryption, data segmentation, and anonymization.
- Manage access controls, such as role-based access.
- Maintain processes around the data retention and destruction.

How to address privacy by design & default

Selectable Controls	
LAWFULNESS, FAIRNESS, TRANSPARENCY	<ul style="list-style-type: none"> • Ensure the lawfulness of processing via consent, legal obligation, contractual obligation etc. • Maintain privacy notices to individuals when collecting their personal data
PURPOSE LIMITATION	<ul style="list-style-type: none"> • Perform data classification for personal data • Understand the purposes of personal data in the process • Revise required data fields / entries per process
ADEQUACY & MINIMIZATION	<ul style="list-style-type: none"> • Maintain a review process to minimize data personal data • Define and minimize mandatory fields for the collection of personal data • Delete or pseudonymize unneeded data

ACCURACY	<ul style="list-style-type: none"> • Define data entry criteria and checks • Validity checks under master data management • Data accuracy, quality and consistency checks across all systems • Data cleansing and data deletion • Accuracy check of third party data
STORAGE LIMITATION	<ul style="list-style-type: none"> • Review retention periods of personal data • Securely delete information that is no longer needed for this purpose or these purposes • Update, archive or securely delete information if it goes out of date
INTEGRITY	<ul style="list-style-type: none"> • Implement plausibility checks, checksums • Define entry criteria for data and check mechanisms to validate data • Implement transport-layer encryption • Avoid data redundancy • Consider pseudonymization, randomization, data scrubbing • DLP solutions
CONFIDENTIALITY	<ul style="list-style-type: none"> • Restrict data access on a need-to-know basis (access control with strong authentication) • Privileged account management • Encrypt or mask data (especially at rest and in transit) • Vulnerability management
ACCOUNTABILITY	<ul style="list-style-type: none"> • Define ownership (data owner, application owner, process owner) • Maintain relevant records of processing activities • Appoint a DPO • Allow individuals to monitor processing • Create, review and improve security features on an ongoing basis • Apply PIA where appropriate

2.2HIPAA

HIPAA - Health Insurance Portability and Accountability Act of 1996, also known as *Public Law 104-191* and the *Kennedy-Kassebaum Bill*, named after its creators, was passed by the US Congress, signed into law by Bill Clinton, and became effective on August 21, 1996.

The objective of HIPAA was to provide insurance portability, fraud enforcement, and administrative simplification for the healthcare industry.

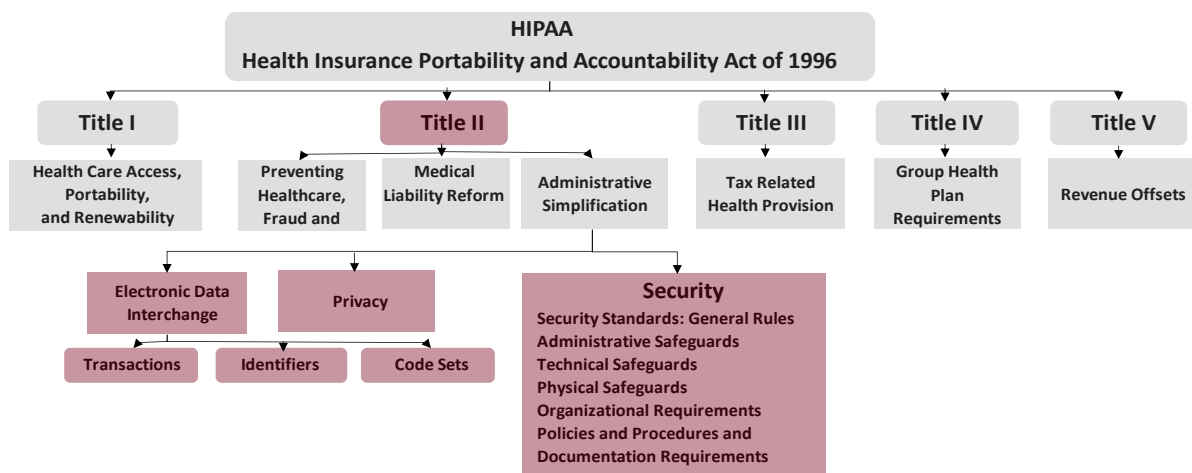


Figure 4: HIPAA

Electronic Protected Health Information, or ePHI, is patient health information which is computer based, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media. This information includes:

- Medical record number, account number or Social Security Number
- Patient demographic data like- address, date of birth, date of death, sex, e-mail / web address
- Dates of service like - date of admission, date of discharge
- Medical records, reports, test results, appointment dates

Personally Identified Information or PII that includes an individual's name in combination with any one or more of the following: Social Security Number, Driver's license number, credit / debit card # in combination with their access / security code or password.

Privacy Rule	<ul style="list-style-type: none"> • Privacy refers to protection of an individual's health care data. • Defines how patient information used and disclosed. • Gives patients privacy rights and more control over their own health information. • Outlines ways to safeguard Protected Health Information (PHI).
Security Rule	<ul style="list-style-type: none"> • Security means controlling: <ul style="list-style-type: none"> ○ Confidentiality of electronic protected health information (ePHI). ○ Storage of electronic protected health information (ePHI) ○ Access into electronic information
Electronic Data Exchange (EDI)	<ul style="list-style-type: none"> • Defines transfer format of electronic information between providers and payers to carry out financial or administrative activities related to health care. • Information includes coding, billing and insurance verification. • Goal of using the same formats is to ultimately make billing process more efficient.

Administrative safeguards: These are the administrative functions that should be implemented to meet the security standards.

Physical safeguards: These are the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion. They include restricting access to ePHI and retaining off site computer backups.

Technical safeguards: These are the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as it is being stored and/or transmitted.

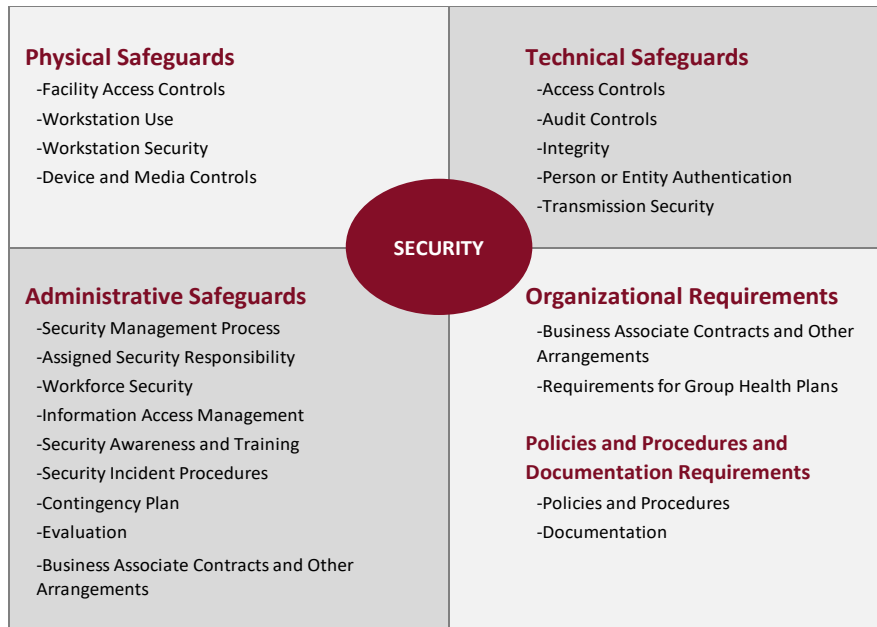


Figure 5: Security's Safeguards

There are two implementation specifications.

- **Required (R):** The covered entity must implement policies and/or procedures that meet what the implementation specification requires
- **Addressable (A):** Assess to see if it is reasonable
 - If not, document that fact and,
 - Implement an equivalent alternative measure, “a compensating control”

Administrative safeguards	
<u>Required</u>	<ul style="list-style-type: none"> • Risk Analysis • Risk Management Plan • Sanctions Policy • Information System Activity Review (audits) • Security Incident Response & Reporting • Data Backup Plan • Disaster Recovery Plan • Emergency Mode Operations • Periodic Evaluations of Standards Compliance • Business Associate Contracts and Other Arrangements
<u>Addressable</u>	<ul style="list-style-type: none"> • Workforce security authorizations • Workforce clearance procedure • Information access authorization procedures • Procedures for establishing and modifying access privileges • Security training • Log-in management • Password management • Virus protection • Security reminders

Physical safeguards	
<u>Required</u>	<ul style="list-style-type: none"> • Workstation Use Analysis • Workstation Security • Disposal of media <ul style="list-style-type: none"> • deletion of PHI prior to disposal, or • Secure disposal so data non-recoverable • Media Reuse <ul style="list-style-type: none"> • Deletion of PHI prior to re-use
<u>Addressable</u>	<ul style="list-style-type: none"> • Facility access contingency plans

	<ul style="list-style-type: none"> • Facility security plan • Physical access control and validation • Accountability for physical access • Data Backup and Storage
--	---

Technical safeguards	
Required	<ul style="list-style-type: none"> • Unique User Identification <ul style="list-style-type: none"> • No shared logins • Emergency access procedures • Audit controls <ul style="list-style-type: none"> • Logs of who created, edited or viewed PHI (e.g. required for applications, environments to the extent technologically feasible) and logs should be retained for the maximum amount of time permitted • Person and/or Entity Authentication <ul style="list-style-type: none"> • No systems without access control
Addressable	<ul style="list-style-type: none"> • Automatic logoff • Encryption at Rest (Highly Recommended) • Encryption in Transit • Authentication of the integrity of stored and transmitted PHI

2.3 PCI-DSS

PCI-DSS = *Payment Card Industry Data Security Standard*

Common set of industry tools and measurements to ensure safe handling of sensitive information. The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. Established by the credit card industry in response to an increase in identity theft and credit card fraud. Every merchant who handles credit card data is responsible for safeguarding that information and can be held liable for security compromises and must comply with PCI-DSS.

The PCI DSS consists of 12 published requirements, which in turn contain multiple subrequirements. The requirements are organized in six groups:

Requirement	Sub-Requirements
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel

Although most of the 12 requirements address issues such as security policies, access controls, antimalware software, and avoidance of default passwords, Requirements 3 and 4 focus on protection of the data itself. These two requirements collectively protect data as it moves over vulnerable networks and is stored. This area is where the PCI DSS overlaps most with many more-generic privacy mandates and data-breach-disclosure laws. Yet Requirements 3 and 4 can represent some of the most taxing aspects of PCI DSS compliance, often requiring unfamiliar

technologies and practices (such as key management) and involving multiple touchpoints within organizations, crossing business silos and political domains.

One of the most common and most effective approaches to protecting stored data is encryption — the process of encoding sensitive data so that only authorized parties can read it.

Protecting Stored Cardholder Data

- Under no circumstances (unless being an issuer) sensitive authentication data can't be stored (full magnetic stripe data,
- Card verification codes/values, personal identification numbers [PINs], PIN blocks, and so on) after authorization takes place.
- When no longer need certain data, it must be deleted securely.
- Certain data items can't be stored:

Account Data	Storage Permitted?	Render Unreadable?
Cardholder data		
Primary account number	Yes	Yes
Cardholder name	Yes	No
Service code	Yes	No
Expiration date	Yes	No
Sensitive authentication data		
Full magnetic strip data or equivalent on a chip	No	N/A
Card security code	No	N/A
PIN/PIN block	No	N/A

Risks Associated with PCI DSS Auditing and Compliance:

- Failure to comply can result in fines, increased fees, or even the termination of your ability to process credit cards.
- PCI DSS compliance cannot be considered in isolation; organizations are subject to multiple security mandates and data breach disclosure. On the other hand, PCI compliance projects can easily be sidetracked by broader security initiatives.
- PCI DSS includes common practices that are likely to be already in place. But some aspects, specifically those associated with encryption, might be new to the organization and implementations can be disruptive, negatively impacting operational efficiency if not designed correctly.
- Opportunities exist to reduce the scope of PCI DSS obligations and therefore reduce cost and impact; however, organizations can waste time and money, if they do not exercise care to ensure that new systems and processes will in fact be accepted as compliant.

2.4 Encryption application

Most regulations have common elements. Thus, for Enterprises to comply with regulatory regimes around the world, there are some key data protection technologies called for in virtually every set of regulations. These include:

- **Data access control**
- **Encryption and tokenization**
- **Encryption key management**
- **Keeping and monitoring user access logs**
- **The use of hardware security modules for executing encryption processes**
- **Encryption of data in motion**

In this way we observe that encryption is the cornerstone to be able to comply with any or all law, regulation on data protection.

Encryption and Key Management are critical to safeguarding data, because they ensure that if the data is breached it will be meaningless and worthless to those who retrieve it. Encryption-key management's role is essential, because if the cybercriminal has the keys, he or she has access to data in the clear. So best practice is for the organization that owns the data to maintain control of the keys. For example, if the data owner uses a cloud service provider, the data owner should retain within its own organization control of the keys. Best practice is also for the data-owning organization to encrypt the data before sending it to the cloud.

3. The World of Encryption

Nowadays it is very usual to hear in the technological world the word encryption, which has its origins in cryptography, and in the need to hide communications as the interest of the human being, in hiding his communications has always existed. Although cryptography has been around for several centuries, it is in recent years when it has been applied to the use and management of technology.

3.1 Encryption

Encryption is the art and science of hiding the meaning or intent of a communication from unintended recipients. Encryption can take many forms and be applied to every type of electronic communication, including text, audio, and video files as well as applications themselves. Encryption is an essential element in security controls, especially regarding the transmission of data between systems. There are various strengths of encryption, each of which is designed and/or appropriate for a specific use or purpose. Cryptography provides added levels of security to data during processing, storage, and communications. Over the years, mathematicians and computer scientists have developed a series of increasingly complex algorithms designed to ensure confidentiality, integrity, authentication, and nonrepudiation

Since the beginning of mankind, human beings have devised various systems of written communication, ranging from ancient hieroglyphics written on cave walls to flash storage devices stuffed with encyclopedias full of information in modern English. As long as mankind has been communicating, we've used secretive means to hide the true meaning of those communications from the uninitiated. Ancient societies used a complex system of secret symbols to represent safe places to stay during times of war. Modern civilizations use a variety of codes and ciphers to facilitate private communication between individuals and groups. In the following sections, you'll look at the evolution of modern cryptography and several famous attempts to covertly intercept and decipher encrypted communications.

Cryptography can be defined as science, which studies encryption or coding techniques designed to hide and understand messages and their representations, either linguistically, informally or in any feasible way. For technology it is important that cryptography gives us the attribute of confidentiality in digital communications, in electronic commerce as in the use of mobile applications.

The security of information is vital for the technological world, that is why the best ally is cryptography, it can be used for authentication, physical security, security in communication channels, privacy, to guarantee the non-repudiation of the data, as for anonymity.

Nowadays: Modern cryptosystems use computationally complex algorithms and long cryptographic keys to meet the cryptographic goals of confidentiality, integrity, authentication, and nonrepudiation. Modern cryptosystems do not rely on the secrecy of their algorithms. In fact, the algorithms for most cryptographic systems are widely available for public review in the accompanying literature and on the Internet. Opening algorithms to public scrutiny actually improves their security. Widespread analysis of algorithms by the computer security community allows practitioners to discover and correct potential security vulnerabilities and ensure that the algorithms they use to protect their communications are as secure as possible. Instead of relying on secret algorithms, modern cryptosystems rely on the secrecy of one or more cryptographic keys used to personalize the algorithm for specific users or groups of users. Existing three types of algorithms commonly used: symmetric encryption algorithms, asymmetric encryption algorithms, and hashing algorithms.

3.2 Data Definitions & Classification

Data classification is the primary means by which data is protected based on its need for **secretcy**, **sensitivity**, or **confidentiality**. Data classification is used to determine how much effort, money,

and resources are allocated to protect the data and control access to it. Data classification is the process of organizing items, objects, subjects, and so on into groups, categories, or collections with similarities. These similarities could include value, cost, sensitivity, risk, vulnerability, power, privilege, possible levels of loss or damage, or need to know.

The primary objective of data classification schemes is to formalize and stratify the process of securing data based on assigned labels of importance and sensitivity. Data classification is used to provide security mechanisms for storing, processing, and transferring data. It also addresses how data is removed from a system and destroyed. The following are benefits of using a data classification scheme:

- It demonstrates an organization's commitment to protecting valuable resources and assets.
- It assists in identifying those assets that are most critical or valuable to the organization.
- It lends credence to the selection of protection mechanisms.
- It is often required for regulatory compliance or legal restrictions.
- It helps to define access levels, types of authorized uses, and parameters for declassification and/or destruction of resources that are no longer valuable.
- It helps with data life-cycle management which in part is the storage length (retention), usage, and destruction of the data.

After the classification scheme is identified, the organization must create the criteria for setting the classification. The criteria by which data is classified vary based on the organization performing the classification. No set guidelines exist for setting the criteria, but some considerations are as follows:

- Who should be able to access or maintain the data?
- Which laws, regulations, directives, or liability might be required in protecting the data?
- For government organizations, what would the effect on national security be if the data were disclosed?
- For nongovernment organizations, what would the level of damage be if the data was disclosed or corrupted?
- Where is the data to be stored?
- What is the value or usefulness of the data?

The two common classification schemes are **government/military** classification and **commercial business/private sector** classification.

3.2.1 Commercial Classification

Classification of commercial or nongovernment organizations does not have a set standard. The classification used is dependent on the overall sensitivity of the data and the levels of confidentiality desired. Additionally, a nongovernment organization might consider the integrity and availability of the data in its classification model.

There is no formula in creating the classification system—the system used is dependent on the data. Some organizations use two types of classification: confidential and public. For others, a higher granularity might be necessary.

- | |
|---|
| - Sensitive: Data that is to have the most limited access and requires a high degree of integrity. This is typically data that will do the most damage to the organization should it be disclosed. |
| - Confidential: Data that might be less restrictive within the company but might cause damage if disclosed. |
| - Private: Private data is usually compartmental data that might not do the company damage but must be keep private for other reasons. Human resources data is one example of data that can be classified as private. |
| - Proprietary: Proprietary data is data that is disclosed outside the company on a limited basis or contains information that could reduce the company's competitive advantage, such as the technical specifications of a new product. |

- **Public:** Public data is the least sensitive data used by the company and would cause the least harm if disclosed. This could be anything from data used for marketing to the number of employees in the company.

3.2.2 Government Classification

Government classification of data is something created out of policy for maintaining national security or the privacy of citizen data. Military and intelligence organizations set their classifications on the ramifications of disclosure of the data. Civilian agencies also look to prevent unauthorized disclosure, but they also have to consider the integrity of the data.

The classifications for the sensitivity of data used in government and military applications are **top secret, secret, confidential, sensitive but unclassified, and unclassified**.

Top Secret: The threat profile for TOP SECRET reflects the highest level of capability deployed against the nation's most sensitive information and services. It is assumed that advanced state actors will prioritize compromising this category of information or service, using significant technical, financial and human resources over extended periods of time. Highly bespoke and targeted attacks may be deployed, blending human sources and actions with technical attack. Very little information risk can be tolerated. Disclosure of top secret data would cause severe damage to national security.

Secret: The threat profile for SECRET anticipates the need to defend against a higher level of capability than would be typical for the OFFICIAL level. This includes sophisticated, well-resourced and determined threat actors, such as some highly capable serious organized crime groups and some state actors. Reasonable steps will be taken to protect information and services from compromise by these actors, including from targeted and bespoke attacks. Disclosure of secret data would cause serious damage to national security. This data is considered less sensitive than data classified as top secret.

Confidential: Confidential data is usually data that is exempt from disclosure under laws such as the Freedom of Information Act but is not classified as national security data.

Sensitive But Unclassified (SBU): SBU data is data that is not considered vital to national security, but its disclosure would do some harm. Many agencies classify data they collect from citizens as SBU. In Canada, the SBU classification is referred to as protected (A, B, C).

Unclassified: Unclassified is data that has no classification or is not sensitive.

3.2.3 Restricted Information Types

Below are shown several types of Restricted Information that have been defined by The Information Security Office and the Office of General Counsel based on state and federal regulatory requirements. They're defined as follows:

- Authentication Verifier

An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to:

- Passwords
- Shared secrets
- Cryptographic private keys

- Covered Financial Information

"Covered information" means nonpublic personal information about a student or other third party who has a continuing relationship with Carnegie Mellon, where such information is obtained in connection with the provision of a financial service or product by Carnegie Mellon, and that is maintained by Carnegie Mellon or on Carnegie Mellon's behalf. Nonpublic personal information includes students' names, addresses and social security numbers as well as students' and parents'

financial information. Covered information does not include records obtained in connection with single or isolated financial transactions such as ATM transactions or credit card purchases.

- Electronic Protected Health Information ("EPHI")

EPHI is defined as any Protected Health Information ("PHI") that is stored in or transmitted by electronic media. For the purpose of this definition, electronic media includes:

- Electronic storage media includes computer hard drives and any removable and/or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.
- Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, an extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks and the physical movement of removable and/or transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

- Export Controlled Materials

Export Controlled Materials is defined as any information or materials that are subject to export control regulations.

- Federal Tax Information ("FTI")

FTI is defined as any return, return information or taxpayer return information that is entrusted to the University by the Internal Revenue Services.

- Payment Card Information

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

- Personally Identifiable Education Records

Personally Identifiable Education Records are defined as any Education Records that contain one or more of the following personal identifiers:

- Name of the student
- Name of the student's parent(s) or other family member(s)
- Social security number
- Student number
- A list of personal characteristics that would make the student's identity easily traceable
- Any other information or identifier that would make the student's identity easily traceable

- Personally Identifiable Information

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

- Protected Health Information ("PHI")

PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component, as defined in Carnegie Mellon's HIPAA Policy. PHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual

PHI does not include education records or treatment records covered by the Family Educational Rights and Privacy Act or employment records held by the University in its role as an employer.

- Controlled Technical Information ("CTI")

Controlled Technical Information means "technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination" per DFARS 252.204-7012.

- For Official Use Only ("FOUO")

Documents and data labeled or marked For Official Use Only are a pre-cursor of Controlled Unclassified Information (CUI) as defined by National Archives (NARA)

- Personal Data from European Union (EU)

The EU's General Data Protection Regulation (GDPR) defines personal data as any information that can identify a natural person, directly or indirectly, by reference to an identifier including

- Name
- An identification number
- Location data
- An online identifier
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

3.3 Encryption Schemes

In recent years there has been an added concern to preexisting compliance and privacy requirements, where companies are increasingly looking for encryption capabilities that protect their data in the cloud via company-owned encryption keys, while still preserving the functionality of the underlying cloud applications. Enterprises have chosen to leverage cloud services because of their simplicity and cost-effectiveness. However, concerns over government inspection of data, service provider breaches, and insufficient access controls have driven increasing use of cryptographic techniques for protecting data in the cloud. The increased demand for enhanced data security has driven the adoption and implementation of several new(er) encryption algorithms such as searchable, format-preserving, order-preserving, and homomorphic encryption schemes.

While this demand has spurred innovation and led to some creative solutions, it has also created widespread confusion and misleading vendor claims as to what is truly feasible from a data protection standpoint. In this environment, security practitioners seek clarity on the relative encryption strengths and weaknesses of various schemes. They also want more information about the trade-offs between security and application functionality, and the adverse impact that selecting the wrong encryption scheme may have on business operations. This paper aims to help practitioners understand the tradeoffs when using different types of encryption and choose the right schemes for protecting cloud storage applications. We consider the setting where only the client holds the key; hence, we focus on symmetric key encryption, as opposed to public key schemes.

The problem of choosing the right encryption scheme for an application can be broken into two tasks: choosing a suitable type of encryption (that is, a set of schemes permitting certain functionality), and then picking the best specific algorithm within that class. Despite what some marketing teams may say, there is no one silver bullet here – no mythical encryption scheme that offers full cloud application functionality and performance with unmatched crypto strength. This is because security and functionality/efficiency for cloud applications are almost always at odds with each other. Accordingly, practitioners must understand their company’s functional and security requirements, and the best security level a scheme of a given type can achieve. Then, they must select the type of encryption that effectively balances all goals for their specific use case. After that, a particular algorithm can be chosen. Let us first discuss the rationale for the latter task. It should be noted that no practical encryption scheme of any type can resist all possible attacks. For example, the brute-force search for the secret key is always possible. Luckily, such a search is usually infeasible, taking hundreds of years in the best case. But what about other, more practical attacks? Here, the choice of a particular scheme matters. Some schemes may appear secure but are not. For some (especially newer) designs, attacks might be developed in the future that render the schemes insecure, even if they are understood to be secure today. So, are there schemes with security guarantees? Yes, there are constructions that provably reach the best level of security for a given class, assuming the hardness of some mathematical problem (such as factoring big numbers). Such schemes are thoroughly analyzed by specialists and are often standardized by organizations such as the National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO). In our presentation below, we recommend some specific schemes that provably reach the best level of security for each class of encryption.

3.3.1 Regular (Unstructured) Data Encryption

Unencrypted Data (Plaintext)

123-12-1234

Encrypted Data (Ciphertext)

bG9yZW0gaXBzdW0gZG9sb3lgc2l0IGFtZXQNCg==

The main goal of a regular symmetric key encryption scheme is data confidentiality. Data integrity and sender authenticity are also important. The primitive can be used to encrypt arbitrary data (such as text documents, spreadsheets, PDFs, and presentations). While not all encryption schemes are good, there are many that provide very strong security guarantees. They are proven to hide all useful information about the data under reasonable assumptions. This implies that a practical attacker cannot find the key, the message, any bit of the message, and any function of the message, given a ciphertext. Moreover, no one can tell if two ciphertexts correspond to equal messages. In addition, the schemes may provide data integrity and sender authenticity. That means that no practical attacker can create a valid ciphertext or modify a legitimate ciphertext without the user noticing. While such schemes are the best candidates to encrypt data for remote storage, one must realize that strong security severely impacts application functionality, and several features of a SaaS application typically cease functioning. Specifically, search, document

preview, graphically rendered report data, logical operations, and mathematical calculations all cease functioning when data is encrypted with good regular encryption schemes. Regular encryption should be used for the most sensitive data requiring the highest security, even at the price of losing search and other types of an application's functionality.

Use if: Security is much more important than usability for cloud apps.

3.3.2 Selective Encryption

Unencrypted Data (Plaintext)

My social security number is 123-12-1234

Encrypted Data (Ciphertext)

My social security number is MTIzLTEyLTEyMzQtMTIzNDU2DQo=

Selective encryption encrypts only non-compliant substrings of a larger data. The core use case for this capability is to only encrypt sensitive data to ensure regulatory compliance, while leaving other data unencrypted to preserve as much of the application functionality as possible. This method of encryption is often used in conjunction with a content inspection and identification capability that enables users to encrypt based on policy.

Selective encryption is often used to encrypt data within collaborative content-sharing applications, intranets, or extranets where personnel may be working jointly on a project or support effort. In these situations, information is often uploaded and exchanged at a rapid pace, and an end-user can inadvertently post data that may violate compliance mandates. For example, a user who may be in a rush to complete a task while supporting a client, may enter personally identifiable information (PII) in a comment field in an application, which unintentionally violates a compliance regulation.

Sensitive data can be encrypted with regular encryption, and thus its security can be fully protected.

Use if: You need strong, configurable, policy-based protection of sensitive data that does not have to be searched on.

Selective encryption is configurable to use different encryption primitives, but for the highest possible security, use unstructured encryption primitives such as AES-GCM. If length preservation is desired, use format preserving encryption.

3.3.3 Format-Preserving Encryption (FPE)

Unencrypted Data (Plaintext)

123-12-1234

Encrypted Data (Ciphertext)

857-27-2973

FPE is an encryption method that preserves the length and the format of the original text. For example, using FPE, a company may take a credit card number and encrypt the card number such

that the resulting ciphertext is a 16-digit number with a valid Luhn checksum.⁵ Such functionality is useful when a specific format is required by the application. Typical scenarios requiring format preservation involve protection of credit card numbers, phone numbers, or PII such as Social Security numbers or account numbers. The benefit of FPE in these scenarios is that the application's field validation rules still function correctly, while the underlying data remains encrypted.

It is important to understand that any FPE leaks equality between plaintexts. (A good FPE encryption can hide everything else, and ciphertexts of distinct messages can look random.) An FPE scheme also cannot provide data integrity and sender authenticity.

Use if: The application requires server-side input validation checks, and the security requirements can tolerate equality leakage.

3.3.4 Searchable Encryption

Unencrypted Data (Plaintext)

1: 123-12-1234

2: 123-12-1235

3: 123-12-1234

Encrypted Data (Ciphertext)

1: MjMOMjMOMjMOLTEyMz Q1NjIzNDM0DQo=

2: VGhpcyBpcyBhIHhnbXB lwaGVydGV4dC43=

3: MjMOMjMOMjMOLTEyMz Q1NjIzNDM0DQo=

Search is utilized in virtually every application and is critical in a collaborative cloud environment. As mentioned, regular encryption hides data so well that search is not feasible. However, it is possible to efficiently search on encrypted data if one is willing to sacrifice some security. In general, any efficiently searchable encryption algorithm shares a common security weakness: equality of keywords is leaked, making certain statistical attacks possible.

3.3.5 Keyword extraction

In the case of unstructured data, keyword search can be preserved on encrypted documents by extracting keywords out of the document, deterministically encrypting and inserting them in a metadata header. The document itself can be encrypted with regular encryption.

Use if: It requires the ability to search documents for certain keywords only, and if the implications of leakage of keywords equality across different documents are acceptable.

3.3.6 Word-by-word

Another method for preserving search in an application is to encrypt each word individually (with searchable encryption). A query will contain an encryption of the required word. The benefit of this approach is that search is possible for any word in the document.

The main security drawback is that equality leakage makes statistical attacks possible. Functionality-wise, partial searches will not function. Complete words or strings must be passed

intact to succeed, and the possible ciphertext expansion caused by word-by-word encryption can lead to truncated data in fields that are length-limited in a structured data application.

Use If: It requires the ability to search for any keyword at the cost of more security.

3.3.7 Local search tokenization

Another method of enabling searchable encryption within an application is to leverage a local search tokenization index. This method functions by creating a local plaintext index of search words as data is sent to a cloud provider. In this scenario, any search terms entered by a user are looked up against the local search index, which then returns the results. This is an efficient implementation from a functional preservation standpoint, but it requires that users wanting to access the application have access to the local index. This will likely adversely impact mobile or remote users. It also potentially creates a target as an attack dictionary for the encrypted data in the cloud. Perhaps the biggest drawback of this method is that users must create on-premises systems that replicate much of the functionality of the cloud service. Essentially, using this scheme requires an on-premises “cloud” application that performs application functions, and turns the cloud into a dumb database.

Use if: Time, budget, and infrastructure can be afforded to use for deploying local search appliances.

3.3.8 Search by prefix

The prefix-searchable method allows users to search for keywords by specifying a common prefix. For example, when a user searches for ‘McD*’, they may be looking for McDonald’s, McDougal, and McDouglass. Not surprisingly, such an additional feature comes at a price of security. This is because equality of prefixes is leaked. The smaller the minimum allowed prefix and its increment, the higher the search flexibility, but the lower the security. For example, being able to search for strings starting with an arbitrary number of letters, such as “M”, “Mc”, or “McD”, means leaking equality of all substrings that the words in the text start with, and this can easily lead to statistical attacks. Moreover, in certain situations, particular queries can completely reveal some of the underlying plaintexts in the database.

Use if: Cloud app functionality is of utmost importance, and security requirements are of minimal importance.

3.3.9 Order-Preserving Encryption (OPE)

Unencrypted Data (Plaintext)

1: 17493058

2: 26573957

Encrypted Data (Ciphertext)

1: 746385647

2: 947385673

[Order of plaintexts is preserved.]

Searchable encryption, whose ciphertexts preserve order of plaintexts, is called order-preserving encryption (OPE). This additional capability has been highly sought after since the onset of the “cloud” era. The ability to index, search, and sort encrypted data in external servers provides enterprises with massive flexibility in their adoption and use of cloud services. Using OPE, an

organization can protect numeric or alpha-numeric fields, while preserving functionality like sorting and range queries in a cloud service. It is important to note that, as usual, great functionality comes with significant inherent security drawbacks. Realize also that leaking order implies leaking other related information.

Use if: When trading some security strength for the ability to sort encrypted data.

3.3.10 Data Tokenization

Unencrypted Data (Plaintext)

123-12-1234

Encrypted Data (Ciphertext)

372937784

Data tokenization involves creating tokens for each plaintext, storing the data and tokens locally, and then passing the tokens to the cloud application. Using this approach, a great deal of application functionality can be preserved. For example, searching for keywords and sorting the data on the server are possible. The security drawbacks of this method are similar to those of searchable and order-preserving encryption. In addition, the local storage for the data and the corresponding tokens should be protected. Another weakness is that the tokenization database must also be accessible by users, and thus may cause issues for remote or Mobile users.

Use if: You'd like something similar to searchable deterministic encryption but need to obey compliance rules for data residency.

3.3.11 Fully Homomorphic Encryption

Unencrypted Data (Plaintext)

123-12-1234

Encrypted Data (Ciphertext)

MjQ5MzU3Mjk4NzU0OTgyMzc0OTIzNzk0MjM3NDgyOTQzODI5NDIzMDk0ODIzZGZnYXNkZw==

Fully homomorphic encryption (FHE) is a method of encryption that allows for encrypted ciphertexts to be computed over by an untrusted party. This theoretically allows the client to ask the server to search the encrypted data for any function of the plaintexts (such as a given substring) or ask the server to compute, say, the average of all encrypted numbers in the database field; the server will not learn anything about the data. FHE has long been considered the holy grail of encryption, and there exist some early prototypes.

However, homomorphic encryption is a minimum of 15 years away from commercial viability due to poor performance, and this is a generous estimate, assuming that the rate of performance improvements to FHE remains at its current level.

While the technology holds promise, higher-level operations and real-world functionality are still many years away. Despite this fact, some vendors have made claims that they can deliver homomorphic encryption in practice today. Technical evaluators would be prudent to tread carefully before giving any credence to these types of claims. Even when FHE becomes feasible to use, its implementation will require significant code changes on the server side. And, for each query, search will be linear in the size of the database, which may be unacceptable for large databases.

4. Encryption Solutions

Among the large number of encryption solutions currently on the market today, we will focus on those prepared for different types of environments (on premise, cloud and hybrid), and whose products can cover the requirements of a complete encryption solution for secure data at rest, which are listed and described below.

Encryption-Enabled Data Security Functions
<p><u>There are four encryption-enabled data security functions:</u></p> <ul style="list-style-type: none">• Protect stored data• Verify identity• Preserve and verify data integrity• Protect data in transmission
Combining Security Functions
<p><u>Combining and coordinating the use of all four functions provides a higher level of data security. For example, data is:</u></p> <ul style="list-style-type: none">• Encrypted when initially stored• Only accessible to multi-factor cryptographically-authenticated users• Cryptographically integrity-checked each time it is accessed• Transmitted as encrypted data through an encrypted connection <p>If exfiltrated, unable to be accessed on unauthorized devices even if user credentials have been compromised</p>
Data Formats
<p><u>Encryption solutions may be suitable for one data format but not another. To provide adequate coverage, the type of encryption solution(s) employed should protect all applicable data formats:</u></p> <ul style="list-style-type: none">• Unstructured Data• Semi-Structured Data• Structured Data• Data Stream
Data Format Conversion
<p><u>During processing, applications may convert data from one type to another. Not all encryption solutions protect all data formats. Examples include:</u></p> <ul style="list-style-type: none">• Unstructured data can be converted to semi-structured data by appending metadata. When metadata is appended by a classification system, moving the data to a common storage location often follows.• Unstructured data can be converted to a binary large object (BLOB) and stored in a database field, and later extracted from the database and converted back into a file.• Structured data can be converted to unstructured or semi-structured data by storing the results of a database query as a file, or sending database query results in a stream to a web interface, where it may be stored on the machine hosting the web interface.• Unstructured, semi-structured, and structured data are all converted to a stream during transmission.
Database Encryption
<p><u>An entire database, or only selected portions of a database, may be encrypted.</u></p> <ul style="list-style-type: none">• Disk Encryption• Specific-field Encryption• Folder Encryption• Device Encryption• File Encryption
Encryption Key Managers
<ul style="list-style-type: none">• <u>Key security:</u> Unauthorized users with keys can decrypt data. Keys may or may not be stored encrypted.• <u>Key backup and recovery:</u> If keys are lost or corrupted and cannot be recovered, the data is

- unrecoverable (an availability breach).
- Key rotation: If keys cannot be rotated, then a potential or actual key compromise cannot be mitigated.
- Key update: Encryption algorithms lose strength or become more vulnerable over time. To maintain key strength, the strength and/or type of encryption algorithm used must be updateable.
- Key access control: Whoever has access to the key has access to the data. If that's a third party, they are a processor.

Access Control

- Centralized Administration of Granular Access
- Authrizaion Controls and Separation of Duties
- Prevent root users or system administrators from accessing sensitive data by enforcing access controls

Application Protection

A data-security solution that, at the application level, to encrypt sensitive data, so only authorized parties can read it. When encryption occurs at this level, data is encrypted across multiple (including disk, file and database) layers.

Pseudonymization - Tokenization

- Vault-base: Dynamic, Pre-generated. Requires costly synchronization capabilities to maintain reliability, high availability, and to keep it out of harm's way of collisions
- Vaultless: Light-weight and powerful tokenization solution which eliminates performance killing latency, deployment can fit in constrained environments such as smart cards, scalability and high availability become mundane tasks, and the total cost of ownership can be applied to tokenization instead of to the complex technology used to keep the token servers reliable

There is an innumerable number of encryption solutions such as *Protegrity, MicroFocus, Voltage Security, CipherCloud, NetSkope, Global Data, Sentinel, SkiHigh, Illumio*, including the solutions of large and well-known companies such as *Symantec, McAfee or CheckPoint*.

In the next sections we will focus on analyzing the encryption solutions offered only by three companies, **HYTRUST**, **SAFENET-GEMALTO** and **THALES-VORMETRIC**. Companies whose portfolio seems to provide a wide repertoire of products to meet the encryption needs to comply with regulations, used by a large number of important companies, and whose products, we have access to be able to deploy and test without incurring any cost.

4.1 Hytrust

The HyTrust Cloud Security Policy Framework (CloudSPF) allows organizations to automate the creation, application and enforcement of security policies for private and public cloud workloads, focused on the key attributes of the workload – People, Data and Infrastructure.

The Cloud Security Policy Framework (CloudSPF) is supported by a portfolio of HyTrust Workload Security solutions that address a wide range of security and compliance challenges from insider threats and data breaches to an ever-expanding security regulatory landscape.



Figure 6: Hytrust's Features

Features:

- Managing Encrypted Workloads in a Multi-Cloud Infrastructure
- Deep Workload Protection
- ENCRYPTION KEY MANAGER
- ACCESS CONTROL

For more details on the features and functionalities of Hytrust products, please refer to **Annex “C” (Encryption Solutions: Hytrust & SafeNet)**

4.2 SafeNet – GEMALTO

SafeNet data encryption and cryptographic key management products enable organizations to secure sensitive data in databases, applications, storage systems, virtualized platforms, and cloud environments.

Data-at-Rest Encryption Solutions

Whether storing data at rest in your physical data center, a private or public cloud, or in a third-party storage application, proper encryption and key management are critical factors in ensuring sensitive data is protected and your organization maintains compliance.

Features:

- ENCRYPTION DATAFORMAT
- DATABASE ENCRYPTION
- ENCRYPTION KEY MANAGER
- ACCESS CONTROL
- APPLICATION PROTECTION
- TOKENIZATION

For more details on the features and functionalities of SafeNet’s products, please refer to **Annex “C” (Encryption Solutions: Hytrust & SafeNet)**

4.3 Thales: VORMETRIC

The Vormetric Data Security Platform efficiently manages data-at-rest security across an entire organization. Built on an extensible architecture, Vormetric Data Security Platform products can be deployed individually, while sharing, key and policy management. With this platform's comprehensive, unified capabilities, we can efficiently scale to address the expanding security and compliance requirements, while significantly reducing total cost of ownership.

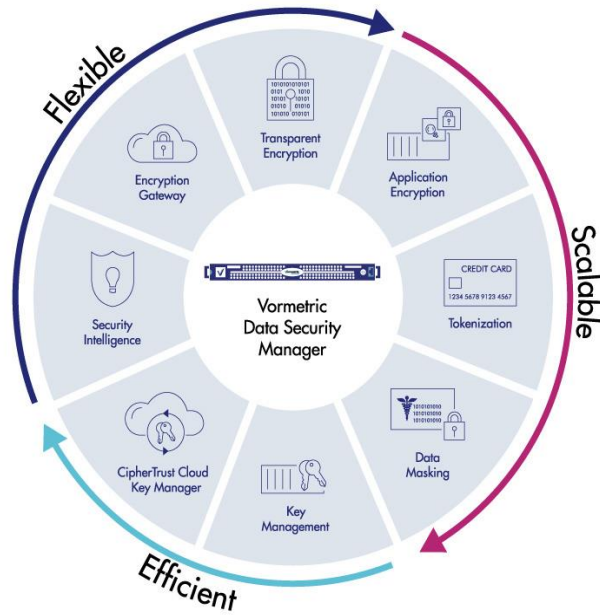


Figure 7: Vormetric's Features

Features:

- ENCRYPTION DATAFORMAT
- DATABASE ENCRYPTION
- ENCRYPTION KEY MANAGER
- ACCESS CONTROL
- APPLICATION PROTECTION
- TOKENIZATION

For more details on the features and functionalities of Thales' products, please refer to **section 5.1. Vormetric in depth.**

4.4 Encryption Solution Selection

After analyzing the encryption solutions, we can see how Hytrust stays behind, while SafeNet and Thales, they both have a variety of products that meet similarly with the full range of desired requirements to protect data at rest in order to comply with the regulations that companies are subject to.

FEATURES		VENDORS SOLUTIONS			
		THALES VORMETRIC	SAFENET GEMALTO	HYTRUST	
ENVIRONMENT SUPPORT	ON PREMISE	✓	✓	✓	
	PRIVATE CLOUD	✓	✓	✓	
	PUBLIC CLOUD	AWS	✓	✓	✓
		AZURE	✓	✓	✓
		GOOGLE	✓	✓	✓
HYBRID	✓	✓	✓		
ENCRYPTION DATAFORMAT	STRUCTURED DATA	✓	✓	✓	
	UNSTRUCTURED DATA	✓	✓	✓	
DATABASE ENCRYPTION	DISK ENCRYPTION	✓	✓	✓	
	FOLDER ENCRYPTION	✓	✓	✓	
	FIELD-SPECIFIC ENCRYPTION	✓	✓	✓	
	DEVICE ENCRYPTION	✓	✓	✓	
	FILE ENCRYPTION	✓	✓	✓	
ENCRYPTION KEY MANAGER	KEY BACKUP & RECOVERY	✓	✓	✓	
	KEY ROTATION	✓	✓	✓	
	KEY UPDATE	✓	✓	✓	
ACCESS CONTROL	CENTRALIZED ADMINISTRATION OF GRANULAR ACCESS	✓	✓	✓	
	AUTHORIZATION CONTROLS & SEPARATION OF DUTIES	✓	✓	✓	
APPLICATION PROTECTION	APPLICATION LEVEL ENCRYPTION	✓	✓	✗	
TOKENIZATION	VAULT-BASE	✗	✗	✗	
	VAULTLESS	✓	✓	✗	
	FORMAT PESERVING FORMAT	✓	✓	✗	

Due to the similarity of both solutions, the choice of one tool or another, could be defined by the price, possible integrations/compatibility with other services or tools already implemented, as well as their performance. In our case, we will choose to implement the technical cases, and test the robustness of the solution itself, from the manufacturer "**Thales-Vormetric**", product already known and used previously.

Once the tool to use for the practical cases to prove its robustness of encryption and tokenization to comply with the established regulations is chosen, we will first analyze and expose, how the solution can comply with the necessary requirements, in general for the wide number of regulations and laws, and more specifically, for the three previously identified, PCI, HIPAA and GDPR.

4.4.1 Compliance with Laws and Regulation

To show a global vision of how Thales' security solutions portfolio offers the suitable products to comply with the requirements established by data protection and privacy regulations around the world, we will base ourselves on the publication of NIST, 800-53.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides guidance for the selection of security and privacy controls for federal information systems and organizations. Published by the National Institute of Standard and Technology, the publication

details items from the Risk Management Framework that address security controls required to meet requirements in the Federal Information Processing Standard (FIPS) 200.

To create a technically sound and broadly applicable set of security controls for information systems and organizations, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, industrial/process control, and intelligence communities as well as controls defined by national and international standards organizations. The objective of NIST Special Publication 800-53 is to provide a set of security controls that can satisfy the breadth and depth of security requirements levied on organizations, mission/business processes, and information systems and that is consistent with and complementary to other established information security standards.

The catalog of security controls in Special Publication 800-53 can be effectively used to protect information and information systems from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios. The controls can also be used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements.

The security controls facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent/repeatable manner—thus we will indicate for each of the controls from the publication of the NIST, 800-53, the products offered by Thales-Vormetric to comply with the indicated baseline, and in what way.

Security Control Identifiers and Family Names:

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

SECURITY CONTROL FAMILY	COMPLIANCE BASELINE	THALES SECURITY PRODUCT MAPPING
Access Controls (AC)	<ul style="list-style-type: none"> • Access Enforcement • Account Management • Separation of Duties • Least Privilege 	Through the use of kernel- level agents providing Suite B and AES 256 Encryption, the Vormetric Data Security Manager exceeds and augments current access- control solutions at the file, directory, drive, or target level at the Operating System and provides Least Privilege.
Awareness and Training (AT)	<ul style="list-style-type: none"> • Training Policies • Security Awareness Training • Role Based Security Training 	Deployment of Vormetric Transparent Encryption is a part of program’s Defense-In-Depth security architecture to protect sensitive data through fine-grained access controls and encryption at rest. On initial deployment, Thales Advanced Solutions Group and a host of learning options (in-class, online) are used to train staff to use the solution. Vormetric Transparent Encryption has low administrative burden, and the training provided covers tasks and responsibilities for each desired/deployed role, with appropriate documentation provided.

Audit and Accountability (AU)	<ul style="list-style-type: none"> • Audit Events • Content • Response • Capacity • Non-Repudiation • Report Generation 	Vormetric Transparent Encryption provides full audit data at the Vormetric Data Security Manager and at host agents in an open format and can integrate with a program or agency's audit reduction tool or SIEM solution.
Security Assessment and Authorization (CA)	<ul style="list-style-type: none"> • System Interconnects • Plan of Action and Milestones • Continuous Monitoring 	Vormetric Transparent Encryption can be tested as a part of an Information System. The agents are installed on operating systems that undergo security hardening and STIG configurations. The Vormetric Data Security Manager is FIPS 140-2 Level 2 or Level 3 Compliant depending upon configuration.
Configuration Management (CM)	<ul style="list-style-type: none"> • Baseline Configuration • Change Control • Security Impact Analysis • Least Functionality 	The configuration of the Vormetric DSM can be changed to match operational requirements for access control and encryption at rest, and can be saved, backed up, and added to a CMDB in order to track changes over time.
Contingency Planning (CP)	<ul style="list-style-type: none"> • Contingency Plan • Contingency Testing 	The Vormetric DSM component can operate in a clustered environment in active or standby mode and can be added to a program's COOP/DR strategy.
Identification and Authentication (IA)	<ul style="list-style-type: none"> • Organizational Users • Device Login • Authentication Management • Cryptographic Module • Incident Handling 	Identification is provided through local web GUI login or Active Directory/LDAP Integration at the Vormetric Data Security Manager appliance. Authentication is provided through the use of kernel level system access to files, folders, and applications
Incident Response (IR)	<ul style="list-style-type: none"> • Incident Response Testing • Training • Handling • Monitoring 	The Vormetric Data Security Platform processes incidents at the individual component level (host system, web GUI, Vormetric DSM). These incidents and audit events are in an open syslog format that can be sent to an information system's monitoring/reporting tool, including 3rd party SIEM solutions. Log file formats can be tailored to match a program's security policy for user and application behavior.
Maintenance (MA)	<ul style="list-style-type: none"> • Controlled Maintenance • Tools 	As a part of the FIPS 140-2 level 3 certification, the Vormetric Data Security Manager is tamper resistant. Additionally, maintenance and audit sessions can be separated by domain and by administrator login.
Media Protection (MP)	<ul style="list-style-type: none"> • Media Access • Media Marking • Storage Transport 	As a part of the FIPS 140-2 level 3 compliance evaluation the Vormetric Data Security Manager has the ability to be zeroized at the appliance console.
Physical and Environmental Protection (PE)	<ul style="list-style-type: none"> • Access Authorizations • Control • Transmission 	The Vormetric Data Security Manager is a 17"x17"x3" hardware device and can be secured in a lockable data center rack enclosure.
Planning (PL)	<ul style="list-style-type: none"> • Security Architecture • Concept of Operations 	Vormetric Transparent Encryption provides fine-grained access policies and AES256 encryption that can be used to limit privileged user access and implement least-privilege principles for users authorized for access to sensitive data.
Personnel Security (PS)	<ul style="list-style-type: none"> • Personnel Termination and Transfer 	Vormetric Transparent Encryption should be operated by personnel at the appropriate level of clearance and information system access.
Risk Assessment (RA)	<ul style="list-style-type: none"> • Security Categorization • Vulnerability Scanning 	Vormetric Transparent Encryption can be used as part of a risk-assessment process at both components in its architecture in an information system; The Vormetric DSM is FIPS 140-2 Level 3 compliant and the Host Agents can

		be installed on hardened servers to minimize risk.
System and Services Acquisition (SA)	<ul style="list-style-type: none"> • Allocation of Resources • System Development Life Cycle 	System Components of the Vormetric Data Security Manager are assembled in US in Thales eSecurity's facility in San Jose, CA. It is FIPS 140-2 Level 3 compliant.
Systems and Communications Protection (SC)	<ul style="list-style-type: none"> • Application Partitioning • Security Function Isolation • Confidentiality and Integrity • Cryptographic Key Management • Platform Agnosticism 	<p>As a part of the Vormetric Transparent Encryption solution, AES 256 encryption keys are passed through an encrypted wrapper.</p> <p>The Administrator Web Interface is accessed through HTTPS.</p> <p>Agent-to-Vormetric DSM communication is accomplished through the use of ephemeral ports. This provides an additional layer of encryption-key protection, reducing risk</p>
Systems and Information Integrity (SI)	<ul style="list-style-type: none"> • Certified only for FIPS 140-2 Levels 1 and 2. 	<p>System Integrity on the Vormetric Transparent Encryption product is satisfied through the Vormetric DSM's FIPS 140-2 validation.</p> <p>Host agents installed on an Information System's server provide encryption-at-rest capabilities to enhance system integrity.</p>
Program Management (PM)	<ul style="list-style-type: none"> • Security Alerts and Advisories • Software and Information Integrity 	Program Management controls are typically implemented at an Organization Level and not directed to Information Systems. As such, it is not a technical control that the Vormetric Transparent Encryption addresses.

More specifically, we will focus on the following sections on how the chosen Thales eSecurity encryption solution, Vormetric, complies with GDPR, HIPAA and PCI regulations.

4.4.1.1 GDPR

Thales eSecurity can help comply with the critical Article 32 and 34 GDPR rules related to:

- The pseudonymization and encryption of personal data;
- Assessing the effectiveness of security measures;
- The unauthorized access to personal data.

Encrypt Both Structured and Unstructured Data

Vormetric file-based transparent encryption provides the kind of "state of the art" data protection the GDPR specifies. Using Vormetric's encryption, your organization can render private data unintelligible to a cyber-intruder even in the event of a breach, thereby avoiding the breach notification requirement outlined in Article 34. The Article states that notification to the data subject shall not be required if the organization "has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption."

In addition to avoiding a costly breach notification process, you can prevent substantial reputational damage resulting from a publicized breach.

Prevent Unauthorized Access to Personal Data

Thales eSecurity products and solutions help our customers prevent unauthorized access to personal data, thus enabling compliance with Article 32. Specifically, our Vormetric Data Security Platform enables separation of duties between privileged administrators and data owners and supports two-factor authentication. Our nShield HSMs also help customers set up high-assurance authentication of users and processes attempting to access personal data.

Test, Assess and Evaluate Data Security Effectiveness

Vormetric's Security Intelligence produces detailed security event logs that are easy to integrate with Security Information and Event Management (SIEM) systems to produce the kind of security reports necessary for GDPR compliance. These enterprise network security information logs produce an auditable trail of permitted and denied access attempts from users and processes, delivering unprecedented insight into file access activities. These enterprise network security information logs can report unusual or improper data access and accelerate the detection of insider threats, hackers and the presence of advanced persistent threats that defeat perimeter security.

4.4.1.2 HIPAA

Thales eSecurity provides solutions to help implement technical safeguards for ePHI through:

- Encryption of data wherever it resides;
- Encryption and key management;
- Data access controls.

Encryption of ePHI

Vormetric Transparent Encryption provides file and volume level data-at-rest encryption to protect ePHI from unauthorized access. Vormetric Application Encryption adds another layer of security and HIPAA/HITECH compliance capabilities, enabling organizations to easily build HIPAA/HITECH encryption capabilities into internal applications at the field and column level.

Strong Key Management

Vormetric Key Management provides the integrated, secure encryption key management that meets HIPAA encryption requirements to separate keys and encrypted data. This solution enables centralized management of encryption keys for other environments and devices including KMIP compatible hardware, Oracle and SQL Server TDE master keys and digital certificates. And Thales nShield HSMs provide FIPS 140-2-certified, hardware-based protection and management of organizations' most critical keys.

Data Access Controls

Vormetric Data Security Platform access controls extend data breach protection by limiting data access to authorized personnel and programs. In addition, the Platform's data access monitoring generates the security intelligence information required to identify accounts that represent a threat because of a malicious insider or malware-compromised account credentials.

4.4.1.3 PCI-DSS

Thales eSecurity can help organizations working with cardholder data comply with several aspects of PCI DSS compliance and auditing, including:

- Protecting stored cardholder data;
- Encryption of data in transmission;
- Restricting access to cardholder data;
- Identifying and authenticating access to system components;
- Tracking and monitoring all access to data.

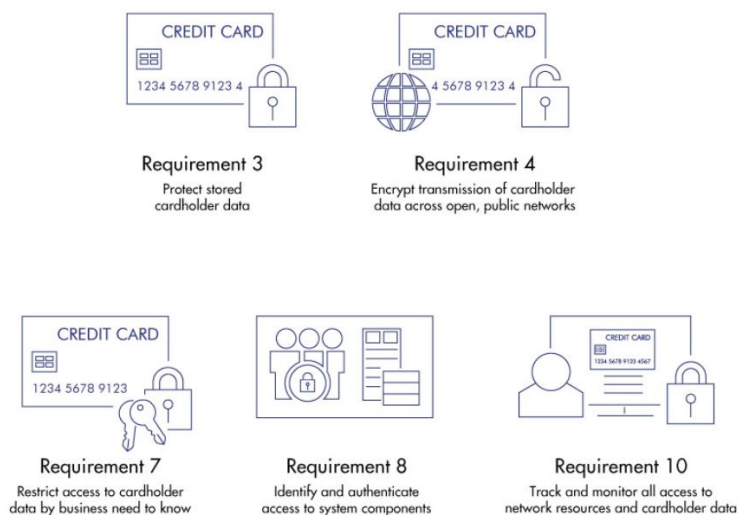


Figure 8: PCI-DSS Requirements

Thales eSecurity offers integrated products and services that enable to protect stored cardholder data, encrypt it for transfer, and restrict access on a need to know basis. In addition, Thales works closely with partners to offer comprehensive solutions that can reduce the scope of your PCI DSS compliance burden.

Addressing the Six Core Principles of PCI DSS

Thales eSecurity offers comprehensive PCI DSS compliance software solutions that help organizations address the six core principles of PCI DSS:

- **Protect cardholder data.** Compliance with PCI DSS requires the encryption of cardholder data flowing over public networks and the protection of stored cardholder data. This begins at the transaction. Thales eSecurity nShield and payShield HSMs work with leading mobile device payment acceptance (mPOS) solutions as well as leading payments data protection solutions to protect cardholder data and help ensure PCI DSS compliance. Merchant organizations also need to deploy network encryption and SSL/TLS encryption for protecting data in transit and technologies such as Vormetric Transparent Encryption for storage and database encryption, Vormetric Application Encryption, Vormetric Tokenization with Dynamic Masking, and ‘point-to-point’ encryption to protect data at rest and reduce scope.
- **Implement strong access control measures.** All data protection techniques go hand-in-hand with access controls. Cryptographic technologies such as PKI and digital certificates are widely used to go beyond password-grade security for authenticating users and systems. Furthermore, using the Vormetric Data Security Manager and Vormetric Encryption Key Management to control access to data decryption keys so as to unlock encrypted data only on a “need to know” basis provides a powerful additional layer of security.
- **Build and maintain a secure network.** In addition to network level encryption, an essential component of network security is the strong authentication of network devices; digital credentials are increasingly employed at the device level to control network access and are an important security consideration for a corporate PKI.
- **Regularly monitor and test networks.** Control and monitoring of all network access to sensitive data, including that by privileged users, must be underpinned by PCI-compliant audit logs. Vormetric Transparent Encryption provides logging of access at the file-system level, supporting log storage in the Vormetric Data Security Manager, in an organization’s security information and event management (SIEM) system, or in another log collection solution.
- **Maintain a vulnerability management program.** The rise of advanced persistent attacks that attempt to corrupt business applications by injecting malware has brought the use of

digital signatures and code signing into focus as a way to prove the integrity and authenticity of business systems and application software.

- **Maintain an information security policy.** PCI DSS places great emphasis on establishing a clear separation of duties between staff members to minimize the risk of insider attack. The Vormetric Data Security Manager provides a powerful mechanism to enforce this separation and for creating a trusted record of events to demonstrate compliance.

5. Experimental Analysis

5.1 Vormetric in depth

The Vormetric Data Security Platform delivers capabilities for transparent file-level encryption, application-layer encryption, tokenization, dynamic data masking, cloud encryption gateway, integrated key management, privileged user access control, and security intelligence.

With the solution, we can address security policies and compliance mandates across databases, files, and big data nodes—whether assets are located in cloud, virtualized, or traditional environments.

Characteristics and Features

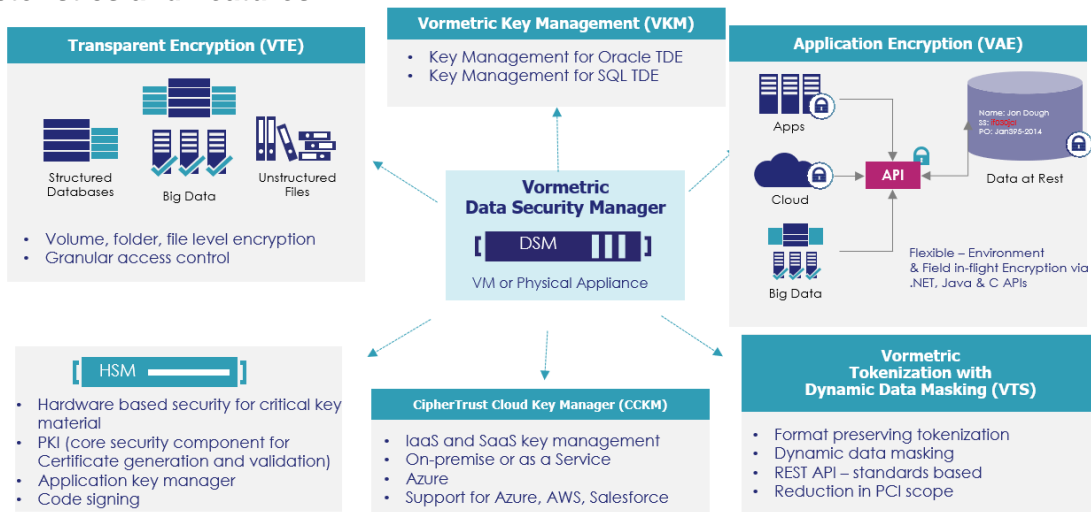


Figure 9: Vormetric Products Features

ENCRYPTION DATAFORMAT

Vormetric Transparent Encryption

Vormetric Transparent Encryption is an easy to deploy software agent that runs across Windows, Linux and UNIX platforms. Both structured and unstructured data are encrypted without changing applications or user experience.

With Vormetric Transparent Encryption (VTE), organizations can secure unstructured files, wherever they reside - onsite or in the cloud. The VTE file encryption system allows to secure sensitive data in spreadsheets, documents, presentations, images and more. Unlike other file encryption offerings, VTE enables security teams to implement file level encryption without having to make changes to the organization’s applications, infrastructure or business practices.

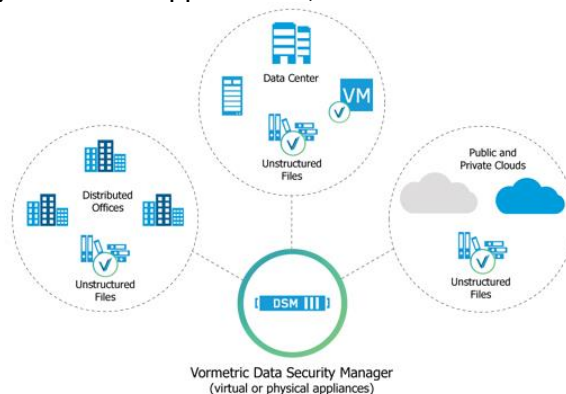


Figure 9: Transparent Encryption

DATABASE ENCRYPTION

Vormetric Transparent Encryption

Vormetric Transparent Encryption offers the capabilities needed to employ strong database encryption, with minimal effort and performance implications. With Vormetric Transparent Encryption, sensitive data in databases can be secured across the enterprise, whether the DB running is Oracle, IBM DB2, Microsoft SQL Server, MySQL, Sybase, NoSQL environments, or any combination thereof.

Core product for securing data at rest adding security managed controls:

- Encryption
- Access control
- Auditing
- Centralized security management
 - Key management
 - Policy management
 - Host management
 - Audit management

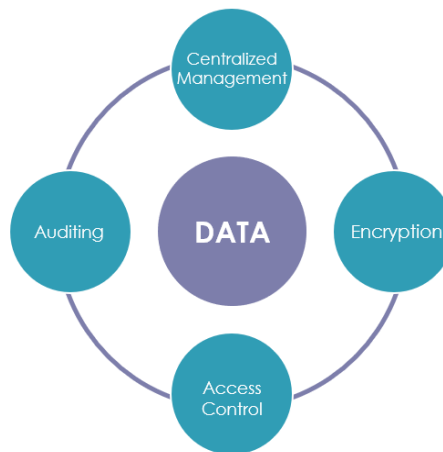


Figure 10: Security Managed Controls

How Vormetric Transparent Encryption Works

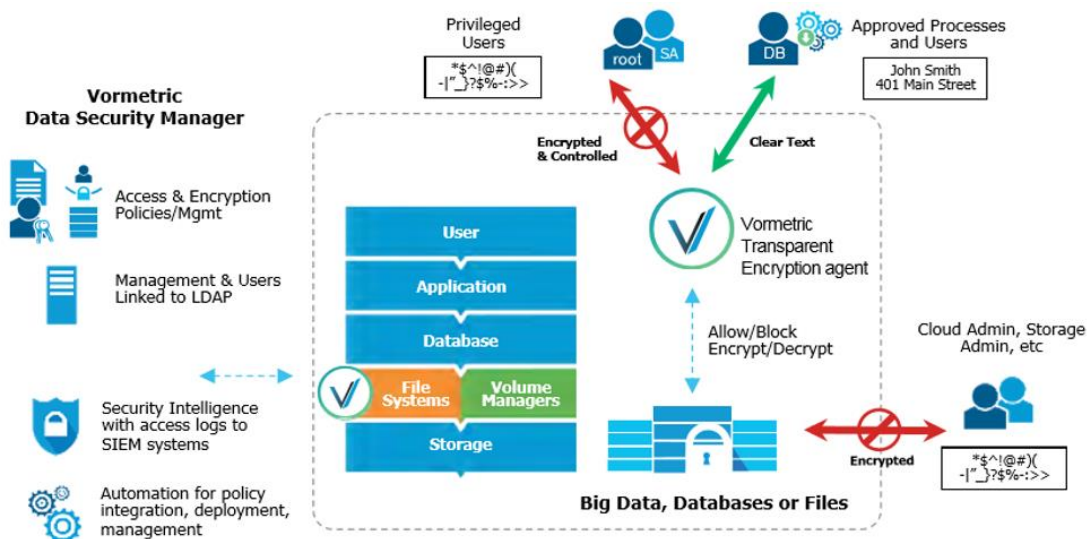


Figure 11: Transparent Encryption work flow

ENCRYPTION KEY MANAGER

Superior Key Management

- Creation – Keys are created and managed within a secure data store
- Use – Keys can be used by name and not by value
- Management – keys inherently are well managed including security, use, and transmission

Superior Implementation Security

- Manage scope of systems able to use keys

Manage use of Application Encryption Agent



Figure 12: Encryption Key Manager

Solution Vision: Control Cloud Data Risk in a Single Pane of Glass

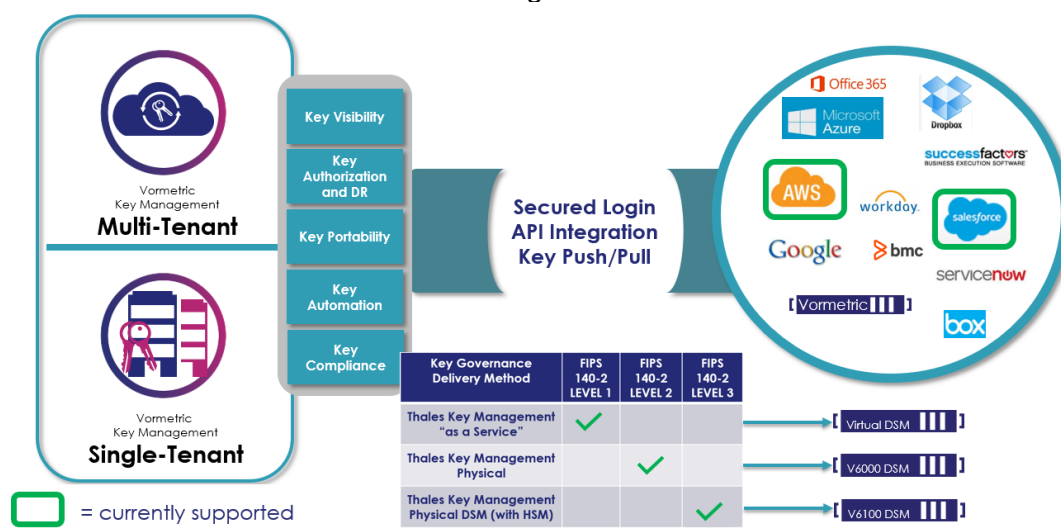


Figure 13: Single Pane of Glass

Key life cycle management

- Generate and store Keys in FIPS 140-2 Level 1, 2 or 3 assured environments
- Upload key into Public Clouds(BYOK), Update, delete, Rotate (on-demand or Auto)
- Key Disaster Recovery – backup keys
- Synchronize keys (Manage ALL keys – External/BYOK or native)
- Manage keys across Salesforce, Azure and AWS

Reports

- Operational insight of keys inside the Cloud – Who, When and What consumed those keys

Email notifications

- Get notified to meet compliance such as 30-day key rotations etc.

Single pane-of-glass across multiple Clouds

ACCESS CONTROL

Vormetric User Access Control:

File access policies can be very granular. User access can be controlled by application, allowed operations, time and the file or resource they attempt to access.

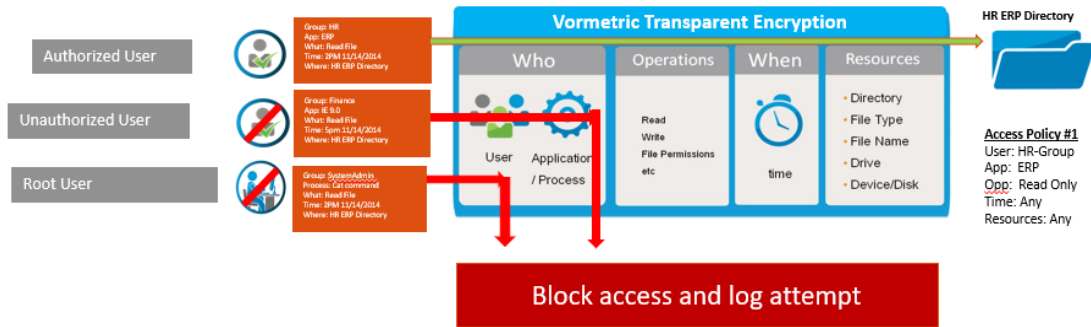


Figure 14: Access Control

The DSM Security Administrator creates policies to protect data. Policies employ two mechanisms to do this:

- Data encryption - Specify that data written to a particular directory (called a GuardPoint) is encrypted, and that data will only be decrypted by specified protected host users. Anyone else who tries to access it will only get useless, unencrypted data.
- Access control - Specify which protected host users can access which files and directories in a GuardPoint. Policies can specify which executables and actions can be used, and at what times.

Policies govern file access and encryption in VTE-protected directories called GuardPoints. Policies can enable auditing such that each time a protected host user accesses a GuardPoint, a log message is created with all the details. As seen in the visual below, a VTE policy consists of a set of rules that control how GuardPoint data can be accessed by protected host users and processes. A GuardPoint is the starting point on a particular host (often a file directory) at which to apply a policy. The File System Agent runs on the protected host and retrieves the list of GuardPoints and associated policies from the DSM to which it is registered. The agent intercepts all attempts to access data inside the GuardPoint and applies the rules of the policy.

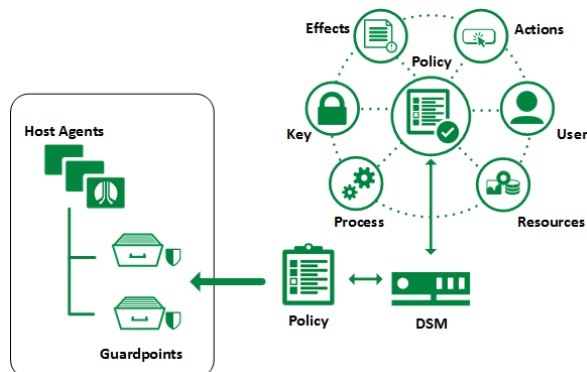


Figure 15: Agents and Guardpoints

APPLICATION PROTECTION

Vormetric Application Encryption

For organizations that need to apply more granular encryption, including at the column or field level within databases, Thales offers Vormetric Application Encryption. Vormetric Application Encryption simplifies the integration of encryption into existing corporate applications and features standard-based APIs, which are used to perform cryptographic and key management operations. Users can choose between standards-based AES encryption and scheme maintaining format preserving encryption (FPE).

A set of APIs that performing cryptographic and key management operations.

Users write code against these APIs and incorporate those calls in their applications to protect sensitive data.

Supported API operations:

- Key Management
 - Generate key – Symmetric and Asymmetric
 - Find key – find keys based on certain attributes
 - Export/Import
- Cryptographic operations
 - Encrypt/Decrypt – simple encrypt/decrypt values
 - Encrypt/Decrypt bulk data – multipart and stream encryption/decryption
 - Signing – hashing

How Vormetric Application Encryption Works

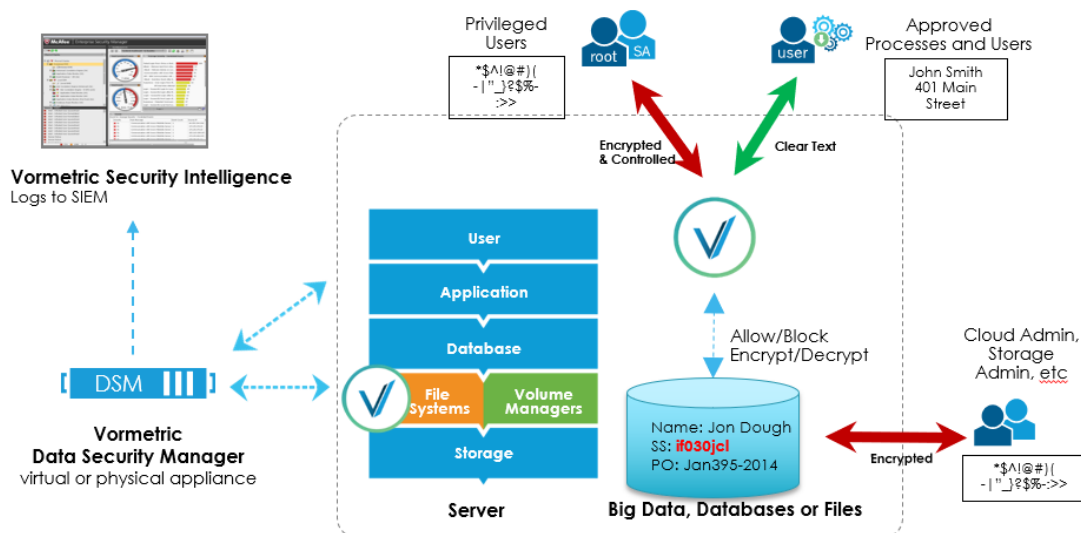


Figure 16: Application Encryption

- Example: Securing credit card data

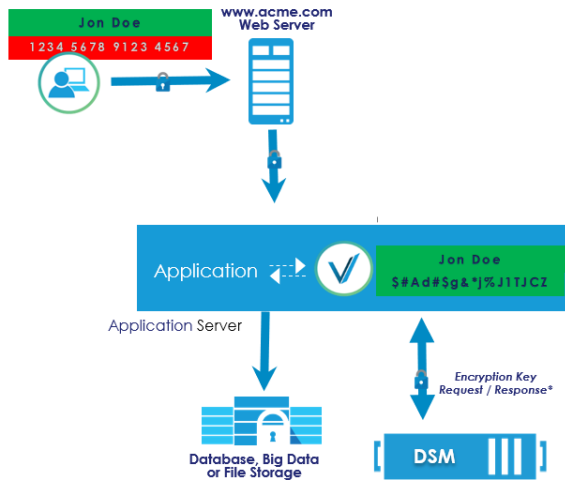


Figure 17: Application Encryption example (credit card)

TOKENIZATION

Vormetric Tokenization with Dynamic Data Masking

Vormetric Vaultless Tokenization with Dynamic Data Masking dramatically reduces the cost and effort required to comply with security policies and regulatory mandates like PCI DSS. The solution delivers capabilities for database tokenization and dynamic display security. Now objectives for securing and anonymizing sensitive assets can efficiently be addressed with vaultless tokenization—whether they reside in data center, big data, container or cloud environments.

Tokenization Architecture:

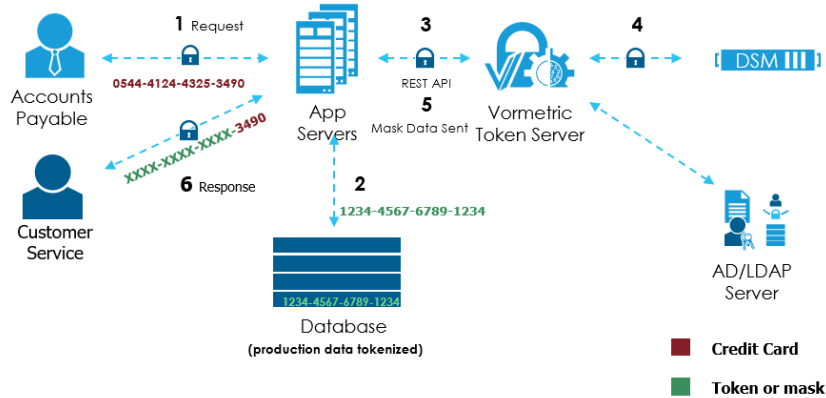


Figure 18: Tokenization with Dynamic Data Masking

Tokenization Example:

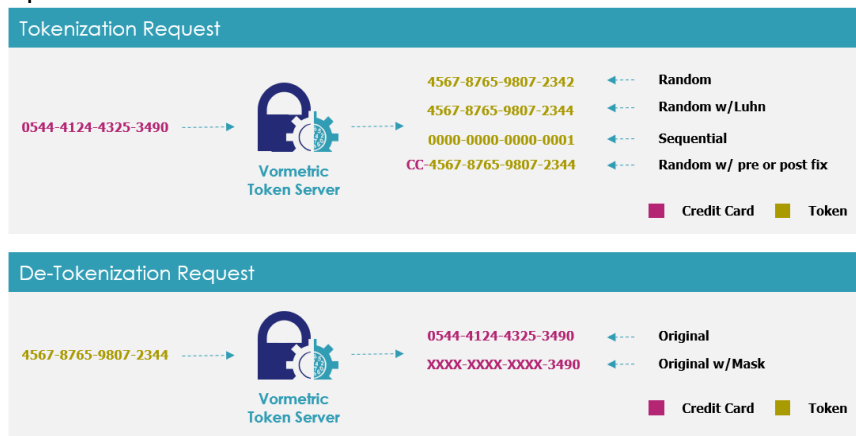


Figure 19: Tokenization example

Vault-less Tokenization – Scale:

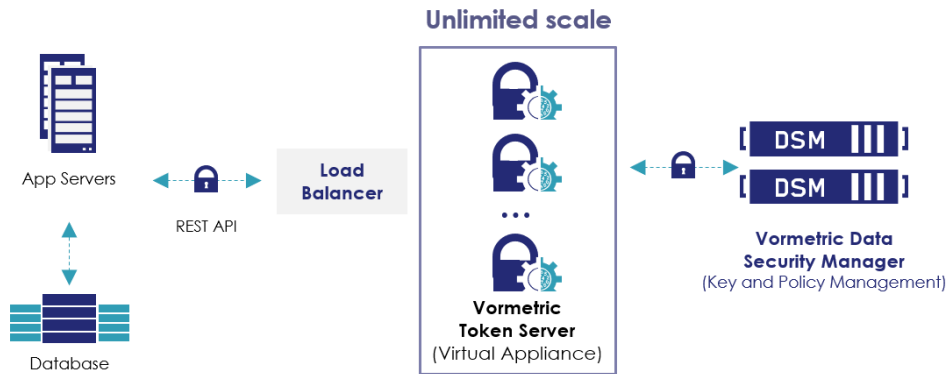


Figure 20: Vault-less Tokenization -Scale

Customers can scale up or down depending on their business needs by spinning up Token Server VMs.

5.2 Vormetric deployment on Cloud

To test the necessary features of the solution's encryption and its robustness to meet the requirements of the regulations, we deployed the following Vormetric VTS (Vormetric Token Service) and DSM (Data Security Manager) products on Amazon's cloud platform, AWS, to implement “Transparent Encryption” and “Tokenization with Dynamic data-masking”.

For the case of Transparent Encryption, we will expose a scenario of a health company whose services upload personal and medical data of patients to the cloud. And in the case of Tokenization, we will expose a scenario with a financial company (a bank), which will upload company and customer data to the cloud.

5.2.1 Securing health data in the cloud

5.2.1.1 Introduction

To secure data for a Health company in the cloud, we will use Vormetric Transparent Encryption solution, which protects data with file and volume level data-at-rest encryption, access controls, and data access audit logging without re-engineering applications, databases or infrastructure. Deployment is simple, scalable and fast, with agents installed above the file system on servers or virtual machines to enforce data security and compliance policies. Access policies and encryption key are managed by the Vormetric Data Security Manager, and can span local data centres, cloud environments and hybrid deployments.

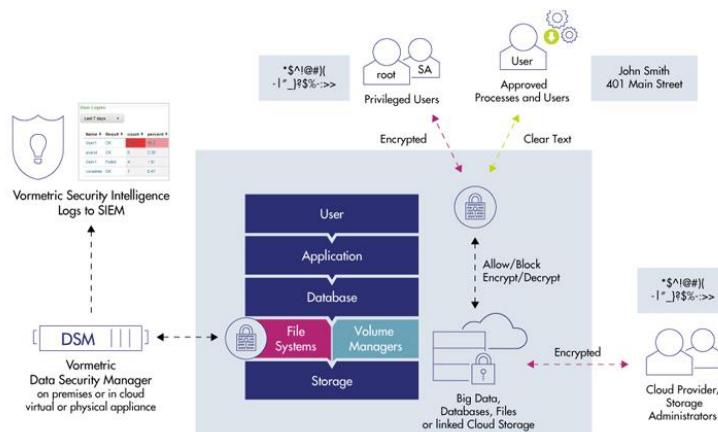


Figure 21: Transparent Encryption for Health use case

5.2.1.2 Architecture

For the health company scenario, where a company uploads company and customer data (containing confidential, health and personal data) to the cloud, the following architecture was deployed in AWS:

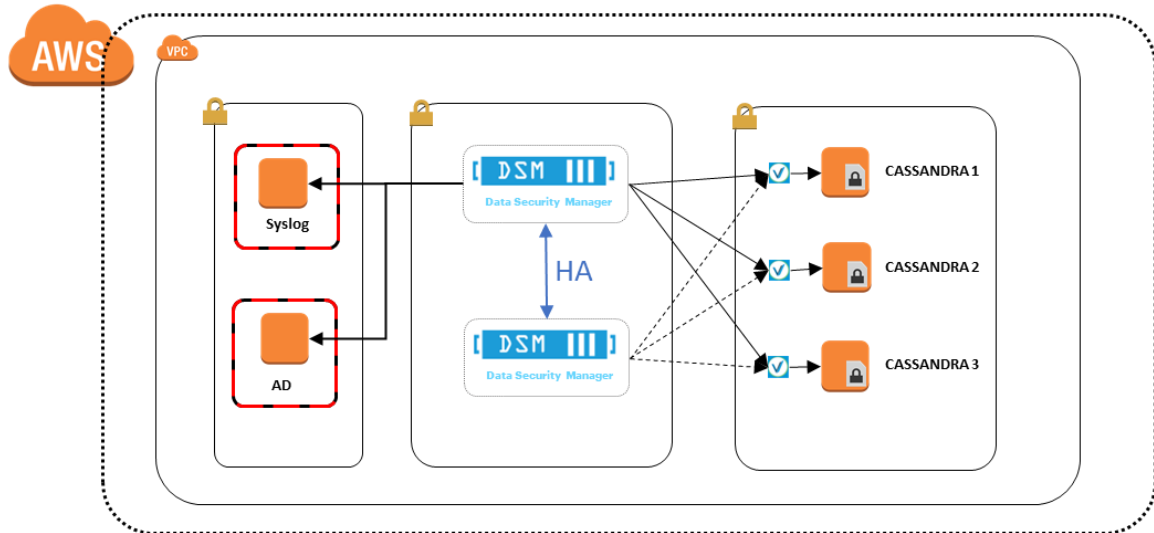


Figure 22: Health use case Architecture

Vormetric Transparent Encryption deployment consisted of the following components:

1. **Vormetric Data Security Manager (DSM).** It is the central component of VTE, storing and managing host encryption keys, data access policies, administrative domains and administrator profiles (two instances configured in HA).
2. **Vormetric Transparent Encryption agents.** The agents communicate with the DSM and implement the security policies on their protected host systems. The communication between agents and DSM is via SSL.
3. **LDAP/Active Directory Server.** This server is going to be used to import and authenticate Vormetric Data Security Manager users. It is accessed via LDAP or LDAPS.
4. **Remote Syslog Server.** DSM sends system log messages to this Syslog Server.
5. **Cluster Cassandra.** It is a distributed NoSQL database management system designed to handle large amounts of data across many commodity servers, providing high availability with no single point of failure. Cassandra clusters (three instances) offers asynchronous masterless replication allowing low latency operations.

5.2.1.3 Control Access

According to the Control Access desired requirements, Vormetric allows to do the following different functions to each DSM role/user, offering a Centralized Administration of Granular Access, Authorization Controls and Separation of Duties, as well as preventing root users or system administrators from accessing sensitive data by enforcing access controls.

- **DSM System Administrator** create or remove other DSM administrators of any type, change their passwords, create or remove domains, and assign a DSM Domain Administrator to each domain. The DSM System Administrator cannot perform any security procedures in any domain.
- **DSM Domain Administrator:** add or remove DSM Security Administrators to domains, and assign some or all the following roles to each one:

- **Audit:** Allow a DSM Security Administrator to generate and view logging data for file accesses.
- **Key:** Allow a DSM Security Administrator to create, edit, and delete encryption keys.
- **Policy:** Allow a DSM Security Administrator to create, edit, and delete policies. A policy is a set of rules that specify who can access which files with what executable during what times. Policies are described in more detail later.
- **Host:** Allow a DSM Security Administrator to configure, modify, and delete hosts and host groups.
- **Challenge & Response.** Generate a temporary password to give to a system user to decrypt cached encryption keys when there is no connection to the DSM.

DSM Domain Administrators cannot remove domains and cannot perform in any of the domain security roles.

- **DSM Security Administrators:** perform the data protection work specified by their roles. These roles, allow them to create policies, configure hosts, audit data usage patterns, apply GuardPoints and perform other duties.

Just for simplicity in this test case, the three administrator types can be combined into the following DSM hybrid administrators:

- **DSM Security and Domain Administrator:** This administrator can perform the tasks of DSM Domain and DSM Security Administrator.
- **DSM Administrator of type All:** This administrator can perform the tasks of all three of the DSM administrative types.

The DSM administrator's primary responsibility is to create policies that allow or deny access to specified users in specified directories called *GuardPoints*. A *policy* is a set of *rules* that must be satisfied before a user can access data in a GuardPoint.

Each time a user attempts to access data in a GuardPoint, the security rules ask:

- **What data is being accessed?**
 - ➔ Are these files or folders protected?
- **Who is attempting to access protected data?**
 - ➔ Is this user permitted to access this files and directory?
- **Which applications are authorized?**
 - ➔ Is the executable used to access the data permitted on these files and directories?
- **When is the data being accessed?**
 - ➔ What hours and days of the week can these files and directories be accessed?
- **How is the data being accessed?**
 - ➔ What processes (read, write, delete, rename...) are permitted on these files and directories?

Criteria	Action
Resource	Specifies which files and/or directories in a guard point are to be blocked. Example: /data/cassandra/data
User	Specifies a which users or groups of users can access the files.
Process	Specifies executables that can operate on the files.
When	Specifies the time range when files can be accessed.
Action	Specifies the allowed file action. Example: read, write, remove, rename, make directory.

When all the access rules in a policy match, VTE enables the policy's *effect*. The effect specifies three things:

- Whether to permit or deny access
- If the data should be encrypted or decrypted for the specified user
- If to audit access attempts

Effect	Action
Permit	Permit access to the data.
Deny	Deny access to the data.
Apply Key	Encrypt data written into guard point with the key specified in the <i>Key Selection Rules</i> Tab. Decrypt data that is accessed using the same key.

A policy's rules and effects allow to specify that some users can have read/copy access, but not decrypting privileges. This allows system administrators to see the file's meta-data such as filename, size, and so on, and thus perform tasks such as backups and moves, while the data in the files remain in an encrypted state.

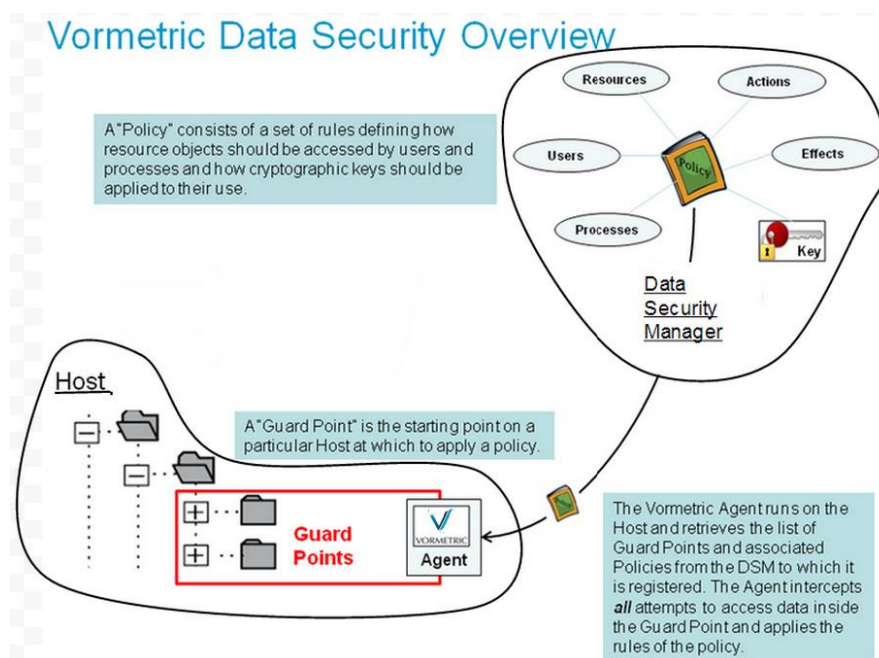


Figure 23: Vormetric Data Security Overview

5.2.1.4 Data Encryption with VTE and Rekey Process

Initial Encryption Directory

The different methodologies to encrypt data are defined below:

- **Initial Encryption:** Add an encryption rule to a GuardPoint policy, then copy files into that GuardPoint. File copied into the GuardPoint will be encrypted. Note that files already in the GuardPoint when the policy is changed are not encrypted. To encrypt files in a GuardPoint with this method, the files must first be moved out of the GuardPoint, add the encryption rule, then files must be moved back into the GuardPoint.

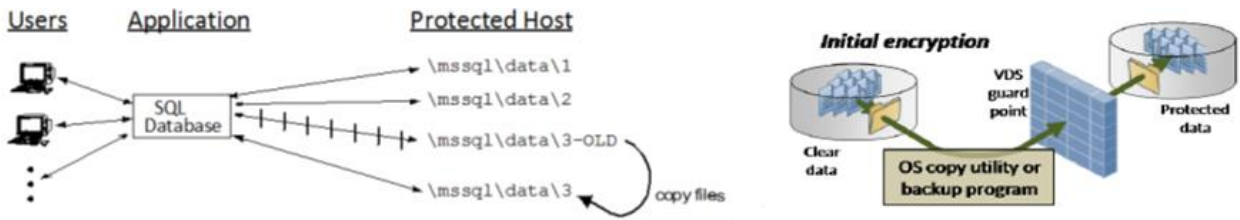


Figure 24: Guardpoints

- **DataxForm:** Using a Vormetric utility called **dataxform** which encrypts files in a directory without having to move them in and out of the directory as is required in the first method.

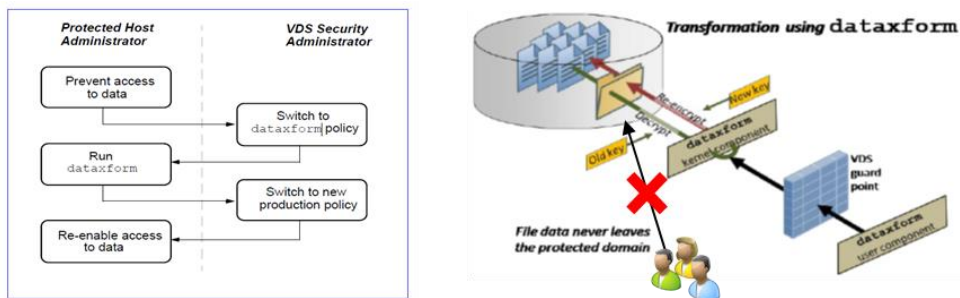


Figure 25: DataxForm

- **Live Data Transform (LDT):** feature enables DSM Security Administrators to encrypt (or rekey) GuardPoint data without blocking user or application access to that data. In standard VTE deployments, access to data is blocked during initial encryption or rekeying of data. With Live Data Transformation (LDT), encryption and rekeying of data takes place in the background, without disrupting user or application access.

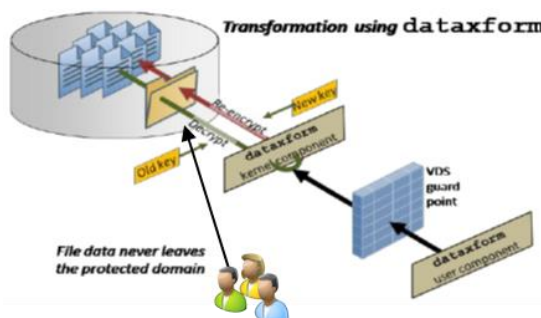


Figure 26: Live Data Transform

Re-Key Process

The different methodologies for Re-Key process are defined below:

- **Manual Coping:** A GuardPoint is created on new directory or device and guarded using a new encryption key, then the data is copied from the original GuardPoint to the new GuardPoint. During the copy, data is decrypted with the original key and encrypted with the new key when it is placed in the new GuardPoint. This method does not require exclusive access to the original GuardPoint but requires extra storage space of at least the amount of data to be copied. It also requires more key steps to ensure that the newly re-encrypted data is both protected by a policy using the new key and known to users or applications that require access to the data.

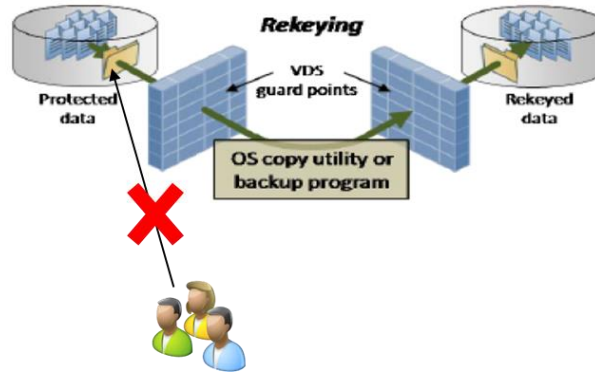


Figure 27: Rekey Manual Coping Process

- **Using DataxForm:** Data is encrypted in place using the *dataxform* utility. This method is fast and easy but requires total and exclusive access to the GuardPoint. All users and applications must be blocked from accessing the data until the *dataxform* is finished executing.

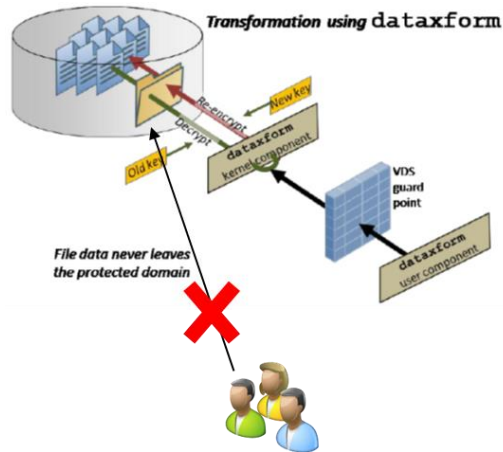


Figure 28: Rekey DataxForm Process

- **Using Live Data Transformation (LDT):** A separately licensed feature of Vormetric Transparent Encryption (VTE) that allows to transform (encrypt or decrypt) or rekey GuardPoint data without blocking use or application access to that data. The LDT feature uses 'versioned keys', which automatically expire and rotate, as defined by the key's settings. The key rotation and key expiration occur in the background.

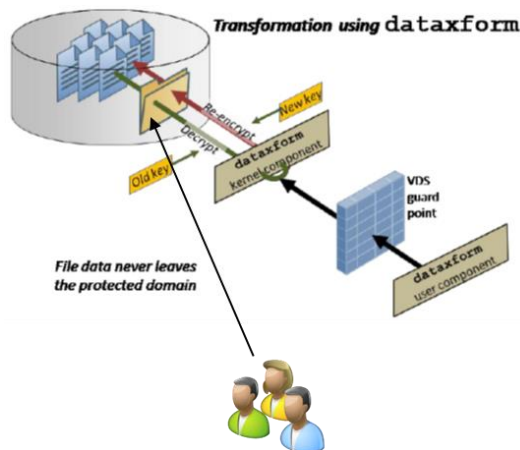


Figure 29: Rekey LDT Process

Comparative of encryption options

The following table shows a comparison of the different encryption options:






















	COPY METHOD	dataxform METHOD	Live Data Transformation
Temporary storage required?	Equal to size of file set 	Sufficient to hold a list of path names of files in file set. 	Sufficient to hold a list of path names of files in file set. 
Security?	File data is unprotected while in copy utility's buffers. 	File data is never outside the VDS GuardPoint. 	File data is never outside the VDS GuardPoint. 
Initial encryption "flexibility"?	Files can be copied directly from source to VDS-protected destination. 	Files must be in a protected location before transformation. 	Files must be in a protected location before transformation. 
Operational impact?	Files cannot be used during transformation. Path names or operating procedures must be adjusted after transformation. 	Files cannot be used during transformation. No other impact on operating procedures. 	Files can be used during transformation. No other impact on operating procedures. 
Recoverability?	Restart copy operation at or prior to point of failure. 	Files undergoing transformation at point of failure must be discovered from dataxform logs and restored from backup. 	LDT automatically detects which files may have been incompletely transformed and encrypt/rekey them again. 
Cost?	Included in VTE license. 	Included in VTE license. 	LDT is a separately licensed feature. 
Effort?	Manual interaction would be necessary to copy the files between directories and after transformation, either both file sets must be renamed (the old path to a new name, and the new path to the old name), or applications must be adapted to process the transformed data set at the new directory name. In addition, if a copy-based transformation is interrupted, the administrator must copy the files again. 	High effort in administration tasks like disable access to the files to be transformed, create a dataxform policy with appropriate encryption key(s) and applies it to the GuardPoint, run the dataxform utility on the GuardPoint directory with the appropriate parameters and options, examine dataxform logs to detect which files may have been incompletely transformed, etc. 	Only manual interaction to change the key settings in the rekey/encryption policies. 

Figure 30: Encryption Options Comparative

Based on the previous comparison it was decided to use DataxForm for initial encryption and for re-key process.

5.2.1.5 Deployment and Configuration

For more details or to deepen the steps taken to deploy and configure the elements to obtain and test the scenario of a health company protecting their data in the cloud, please refer to the **Annex "D" (Experimental Analysis Use Cases Deployment)**, where the actions performed for the following points are explained:

- DMS Deployment requirements
- Solution's Components
- AD/LDAP server integration
- Creation and configuration of Policies
- Agents
- DSM HA Configuration
- Syslog Server configuration

5.2.2 Securing financial data in the cloud

5.2.2.1 Introduction

For the financial company scenario, where a bank uploads company and customer data (financial and personal) to the cloud for processing and later use it to perform analysis, calculation of statistics and possible advertising campaigns, we deployed and use Vormetric Tokenization with Dynamic Data Masking (VTS).

5.2.2.2 Architecture

The following image show a high-level architecture diagram of our solution deployed in AWS:

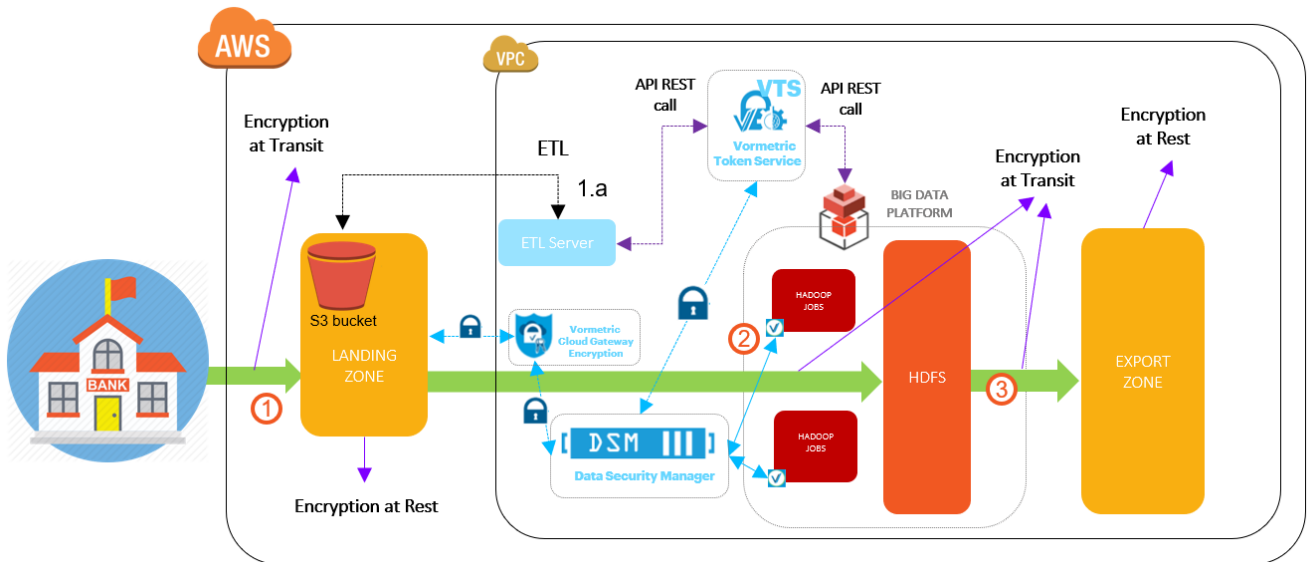


Figure 31: Financial use case Architecture

1. The initial loads of the files are performed on the "landing zone", a S3 bucket encrypted at rest using Vormetric Cloud Encryption Gateway (By focusing on the Tokenization part, for resource and time issues, the bucket encryption was done using native AWS encryption, using AWS KMS), from where ETL processes are launched through AWS EMR (Amazon ElasticMapReduce provides a managed Hadoop framework that makes it easy, fast, and cost-effective to process vast amounts of data across dynamically scalable Amazon EC2 instances) with integration with Vormetric VTS. For the creation of the file FPE/SST/DM where certain fields will be encrypted, tokenized or masked, an ETL includes in its flow the interaction with the solution of VTS (1.a), which will be called for protection of the sensitive fields. The resulting FPE/SST/DM file is deposited in the "landing zone".
2. The protected files of the landing zone are exported to the Hadoop cluster (encryption at rest using Vormetric Transparent Encryption) for processing tasks. Eventually, it may be necessary to re-identify certain fields, for example to execute certain analyzes and processes that require the fields in "clear" or in their "unaltered" form, so this action is possible from the cluster of Hadoop by calling the VTS service.
3. Finally, the protected analytical files (in the event that the Hadoop cluster has eventually re-identified data, the resulting files would be protected again by calling the VTS solution) are deposited in the export zone from where they are stored. They can perform ETL processes that act as input for example BI tools or other applications such as a campaign manager.

The objectives to achieve with Vormetric Tokenization and the architecture shown above are the following:

- **Replace sensitive data in databases with tokens**, reducing the number of places in which plain text credit card numbers reside, and thus reduce the scope of complying with the Payment Card Industry Data Security Standard (PCI DSS) and corporate security policies.
- **Preserve the format of data** in a way that reduces the operational impact associated with encryption and other obfuscation techniques: tokenizing the credit card field in the database, yet keep the tokenized information in a format that is compatible with associated applications.
- **Enable outsourcing application testing and running analytics** without giving access to sensitive assets because the format of the data has been preserved.

- **Create strong separation of duties** between privileged administrators and data owners. In this way, IT administrators, such as hypervisor, cloud, storage, and system administrators can perform their tasks without access to the sensitive data residing on those systems.
- **Enable dynamic data masking**—the ability to establish varying levels of data redaction for different database users as enabling customer service personnel to access the last four digits of a customer’s credit card number, while an accounts payable representative can access the full credit card number

5.2.2.3 Components

Vormetric Tokenization consists of the following components:

1. **Vormetric Token Server (VTS).** A virtual appliance that:
 - Receives REST API calls to tokenize and detokenize sensitive data.
 - Authenticates users or uses the AD/LDAP server to authenticate users. Applies user profiles to determine the permissions of users.
 - Tokenizes (encrypts) sensitive data, using a key from the DSM.
 - Decrypts the token using a key from the DSM. Applies dynamic data masking as appropriate.
 - Sends the detokenized data to the requesting client.
 - Provides a Token Server GUI to create/delete users/groups, specify user/group permissions, define data masks, and create token groups
2. **Vormetric Data Security Manager (DSM).** Holds the keys used for tokenizing (encrypting) data.
3. **LDAP/Active Directory server.** This server is going to be used to import and authenticate Vormetric Tokenization users. It is accessed via LDAP or LDAPS.
4. **Remote Logging server.** We can configure our system to send system log messages to a syslog server.

5.2.2.4 Control Access

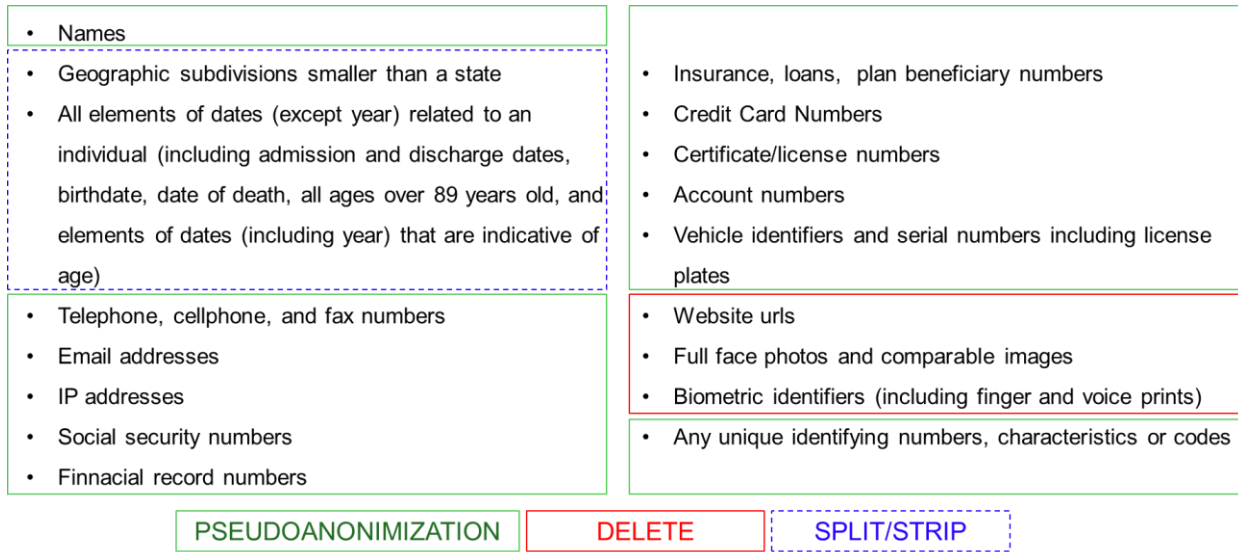
Depending of the business needs, different users with different permissions can be created. The following table shows the users/roles identified and created as well as those permissions/privileges that are granted for each of them:

User \ Action	User Administration (dsm users, vts users)	Key Management	Token Templates/Groups management	Call API	RAW data access	Tokenized data access
DSM System Administrator	✓	✗	✗	✗	✗	✗
DSM Security and Domain Administrator	✗	✓	✗	✗	✗	✗
VTS Administrator	✓	✗	✓	✗	✗	✗
Big-Data automated processes	✗	✗	✗	✓	✓	✓
Business owners	✗	✗	✗	✓	✓	✗
Data Scientist	✗	✗	✗	✗	✗	✓

Figure 32: Users Control Access Actions

5.2.2.5 Analysis of data to be secured

For the analysis, and subsequent data processing, we identify those data fields that the financial entity could obtain and use from its clients, and we performed a classification, of which must be tokenized, eliminated or split:



Once this separation was made, we were ready to create the corresponding keys for tokenization, the token groups and the templates for each specific case identified above:

- Credit Card numbers
- “Open fields”, where sensitive data could be stored (Addresses, names...)
- Unique identifier numbers, codes...
- Email addresses
- Telephone Numbers
- Names text fields
- Insurance, Loans, credit... contract numbers
- Bank Account numbers

- Encryption Keys: We will create 8 keys for each of the cases.

-



Figure 33: Encryptions keys configured and deployed

Token Groups:

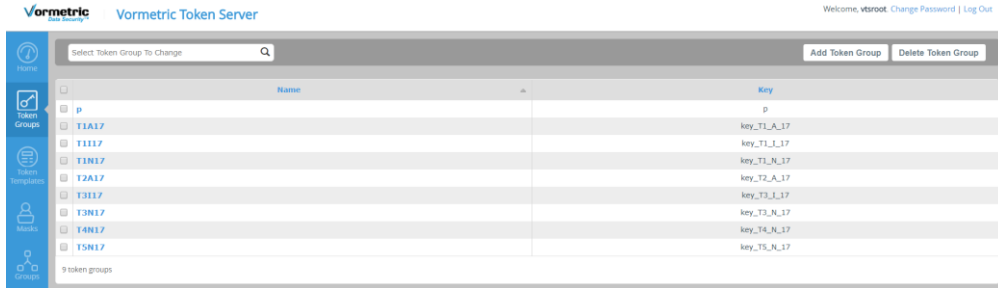


Figure 34: Token Groups configured and deployed

Token Templates:



Figure 35: Token Templates configured and deployed

Token Template Config:

Template: T1A17

Format: FPE, format preserving encryption

Characters to use: Alphanumeric

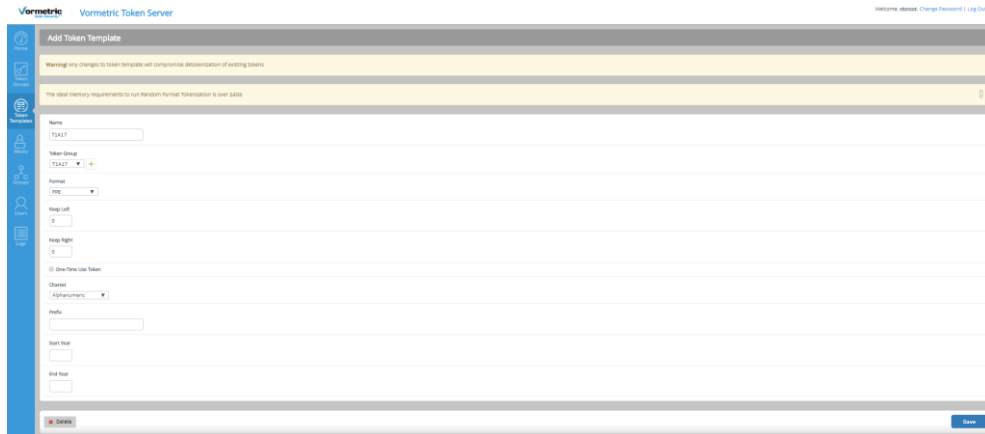


Figure 36: Token Template configuration example

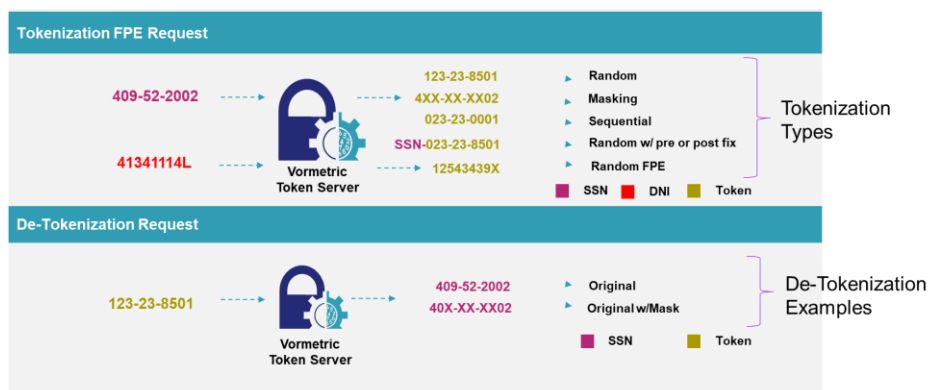


Figure 37: Tokenization Types

In the following table we will show the operation of each of the templates with an example:

tokentemplate: T1N17 → Credit Card numbers			
{	"tokengroup": "T1N17",	"data": "12313212321",	"tokentemplate": "T1N17"} ->
{	"token": "91308907408",	"status": "Succeed"}	
tokentemplate: T1A17 → Open fields			
{	"tokengroup": "T1A17",	"data": "hola que tal como estas 1232131%\$&",	"tokentemplate": "T1A17"} ->
{	"token": "6T6R yp8 xaB HglO JjchX Zvx4rlw%\$&",	"status": "Succeed"}	
tokentemplate: T1A17 → Unique identifier numbers, codes...			
{	"tokengroup": "T1I17",	"data": "asdsda2231@dsdas123",	"tokentemplate": "T1I17"} ->
{	"token": "[FBJ]ujd&E9e#sqsl",	"status": "Succeed"}	
tokentemplate: T2A17 → Email addresses			
{	"tokengroup": "T2A17",	"data": "U.prueba2@dominio21.com",	"tokentemplate": "T2A17"} ->
{	"token": ".IPoSScNT@pWcEZ6NMV.rDA",	"status": "Succeed"}	
tokentemplate: T3N17 → Telephone Numbers			
{	"tokengroup": "T3N17",	"data": "123456789",	"tokentemplate": "T3N17"} ->
{	"token": "481526585",	"status": "Succeed"}	
tokentemplate: T3I17 → Names text fields			
{	"tokengroup": "T3I17",	"data": "Pepe, López, Jiménez, 99,)= 23,?¿=08765432)",	"tokentemplate": "T3I17"} ->
{	"token": "{u 7T@2ó3awU5aH[éNQ,?Cyah1dUBOAnG¿JQ*n}7Ru}9",	"status": "Succeed"}	
tokentemplate: T4N17 → Insurance, Loans, credit... contract numbers			
{	"tokengroup": "T4N17",	"data": "00730100223323232323",	"tokentemplate": "T4N17"} ->
{	"token": "008144404786235559172",	"status": "Succeed"}	
tokentemplate: T5N17 → Account numbers			
{	"tokengroup": "T5N17",	"data": "4444222233331111",	"tokentemplate": "T5N17"} ->
{	"token": "0130266131453287",	"status": "Succeed"}	

5.2.2.6 Deployment and Configuration

For more details or to deepen the steps taken to deploy and configure the elements to obtain and test the scenario of a financial company protecting their data in the cloud, please refer to the **Annex “D” (Experimental Analysis Use Cases Deployment)**, where the actions performed for the following points are explained:

- VTS Deployment requirements
- Configure DMS to enable VTS Installation
- VTS and DSM Configuration
- VTS Registration with DSM
- VTS Cluster (HA Configuration)

6. Conclusions and Future Work

In general terms we can mention the following conclusions:

The first conclusion we reached at the beginning of the completion of the master's thesis is that we live in a world where, with the rapid technological advances, entails the creation and modification of laws and regulations on data protection, to which companies have to submit and be prepared.

The second conclusion, is the great dependence on data encryption for compliance with the requirements of laws and regulations. So companies have to rely on encryption solutions that exist in the market. Among the large number of encryption solutions, there is a wide variety of specific products for different requirements. Analyzing the products of different manufacturers we could see that not all have a complete portfolio to cover all the needs that a company could have to comply with all the regulations on which it was affected.

Below we detail the conclusions obtained about the Thales-Vormetric encryption solution:

We could see that Thales has an encryption solution with a wide repertoire of tools and products that at first glance seem to be able to cope with any requirement requested by any regulation that any company has to face in terms of data protection, either on premise, in the cloud, or in a hybrid environment.

In the scenario of a healthcare company, using Transparent Encryption, we could see the simplicity and robustness, of encrypting specific database folders, controlling access, both of the users that can obtain the stored data, and the administrators to make changes of configuration.

For the scenario of the financial institution, with a greater level of complexity, when making tokenization instead of encryption, for the later use of the data anonymously, we could see the granularity level of access control, and the flexibility to create templates for each type of data and the type of use that would be given.

In the tasks to be identified as future work, there would be the extension of the scope of use cases, which would include the following:

The implementation and monitoring of encryption in transit (not only at rest)

The configuration of a security monitoring system (SIEM) to detect use cases as unauthorized access to both data and settings, data breaches, corrupted data...

Implementation and configuration of storage and retention policies in accordance with the requirements of the regulations (keeping data as long as law requires depending on the type of data, and the elimination of that data without need of being retained any longer) as well as the installation of mechanisms that ensure access or deletion of user data upon request as indicated by current data protection laws.

7. Glossary - Acronyms

AES	Advanced Encryption Standard
API	Application Program Interface
FIPS	Federal Information Processing Standard
FPE	Format Preserving Encryption
FHE	Fully Homomorphic Encryption
ISO	International Organization for Standardization
mPOS	Mobile Device Payment Acceptance
PKI	Public Key Infrastructure
SIEM	Security Information and Event Management
AD	Active Directory
DPO	Data Protection Officer
DEK	Data Encryption Keys
DLP	Data Loss Prevention
DM	Dynamic Masking
DSM	Vormetric Data Security Manager
ePHI	Electronic Protected Health Information
ETL	Extract, Transform and Load
HA	High Availability
HIPAA	Health Insurance Portability and Accountability Act
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LDT	Live Data Transformation
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PHI	Protected Health Information
SST	Secure Stateless Tokenization
TE	Transparent Encryption
GDPR	The EU General Data Protection Regulation
VTE	Vormetric Transparent Encryption

8. References

Data Privacy Regulation & Compliance

1. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
2. <https://www.iso.org/standard/54533.html>
3. <https://www.iso.org/standard/62777.html>
4. <https://www.pcisecuritystandards.org/>
5. https://www.pcisecuritystandards.org/documents/PCI_HSM
6. <https://www.fda.gov/aboutfda/transparency/basics/ucm194879.htm>
7. <https://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act>
8. <https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/html/PLAW-106publ102.htm>
9. <https://www.hhs.gov/hipaa/index.html>
10. https://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf
11. https://www.dfs.ny.gov/about/cybersecurity_faqs.htm
12. https://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf
13. <https://www.ffiec.gov/>
14. <https://www.fedramp.gov/>
15. <https://nvd.nist.gov/800-53>
16. <http://www.sox-online.com/>
17. <https://iapp.org/news/a/gdpr-matchup-mexicos-federal-data-protection-law-held-by-private-parties-and-its-regulations/>
18. <https://es.wikipedia.org/wiki/EIDAS>
19. <https://gdpr-info.eu/>
20. <https://eugdpr.org/>
21. http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en
22. <https://www.gov.za/documents/protection-personal-information-act>
23. <https://www.legislation.gov.au/Details/C2017A00012>
24. <https://www.realestate-tokyo.com/living-in-tokyo/immigration-government/my-number/>
25. <http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework.aspx>
26. <https://privacy.gov.ph/wp-content/uploads/IRR-of-the-DPA.pdf>
27. http://www.koreanlii.or.kr/w/index.php/Personal_Information_Protection_Act?ckattempt=1
28. [Standard: PCI Data Security Standard \(PCI DSS\) \[Best Practices for Maintaining PCI DSS Compliance Special Interest Group PCI Security Standards Council\]](#)

The World of Encryption

- a. <https://en.wikipedia.org/wiki/Encryption>
- b. https://en.wikipedia.org/wiki/History_of_cryptography
- c. https://en.wikipedia.org/wiki/Timeline_of_cryptography
- d. https://en.wikipedia.org/wiki/Category:Cryptography_lists_and_comparisons
- e. <https://study.com/academy/lesson/the-history-of-encryption.html>
- f. <https://searchsecurity.techtarget.com/definition/encryption>
- g. <https://cs.stanford.edu/people/eroberts/courses/soco/projects/public-key-cryptography/history.html>
- h. <https://access.redhat.com/blogs/766093/posts/1976023>
- i. <https://www.technewsworld.com/story/70437.html>
- j. <https://www.irs.gov/pub/irs-pdf/p1075.pdf>
- k. <https://www.cmu.edu/policies/student-and-student-life/privacy-rights-students.html>
- l. <https://www.cmu.edu/policies/information-technology/gramm-leach-bliley-act.html>
- m. <https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012>
- n. <https://www.archives.gov/cui/registry/category-list>
- o. **CISSP: Certified Information Systems Security Professional Study Guide** (James M. Stewart, Mike Chapple, Darril Gibson).
- p. M. Bellare, A. Desai, E. Jorjani and P. Rogaway, “**A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation**,” FOCS '97, 1997.
- q. M. Bellare, R. Canetti and H. Krawczyk, “**Keying Hash Functions for Message Authentication**,” Crypto '96, 1996.
- r. M. Bellare and C. Namprempre, “**Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm**,” Asiacrypt '00, 2000.
- s. D. McGrew, J. Viega. “**The Galois/Counter Mode of Operation (GCM)**,” NIST Computer Security Division, 2005.
- t. H. P. Luhn, “**Computer for verifying numbers**,” US Patent 2950048, 1960.
- u. M. Bellare, T. Ristenpart, P. Rogaway and T. Stegers, “**Format-Preserving Encryption**,” Selected Areas in Cryptography '09, 2009.

9. Annexes

A. Worldwide Regulations

▪ Global regulations and standards

This section includes international standards, such as those from the International Organization for Standardization (ISO) and the Payment Card Industry Security Standards Council (PCI SSC) as well as regional standards that have taken on global significance.

Data Breach Notification Laws

Data breach notification requirements on loss of personal information have increasingly been enacted by nations around the globe as well as by U.S. state governments. Data breach disclosure laws and notification requirements vary by jurisdiction, but almost universally include a “safe harbor” clause, if the data lost was encrypted.

REGULATION: Breach Disclosure Laws Widespread National data breach disclosure laws include the UK Data Protection Act, EU General Data Protection Regulation (GDPR), South Korea’s Personal Information Protection Act, Australian Privacy Act and others.

Prevention of Data Breaches a Complex Task: Data breach protection and prevention is not as simple as implementing hardware-level disk encryption or OS-level encryption within systems. Attacks are increasingly able to penetrate perimeter defenses, compromise accounts, and mine data without targets even being aware of the attack. With this kind of activity, simple encryption schemes won’t prevent a data breach. Attackers will access accounts that allow them to decrypt and extract personal data. Driving this are criminal groups willing and able to pay for stolen personal information that has direct monetary value.

Data Protection Requires a Data-Centric Focus: A data-centric focus on preventing the loss of personal information requires:

- Encryption of personal data wherever it resides, including file-systems databases, web repositories, cloud environments, big-data environments and virtualization implementations.
- Policy-based access controls to assure that only authorized accounts and processes can see the data.
- Monitoring authorized accounts that access data, to ensure these accounts have not been compromised.

Data Residency

With more than 100 national data-privacy laws on the books as of the end of 2016 (including the landmark GDPR in Europe), any global enterprise, SaaS vendor or cloud solution provider needs to pay attention to how data-residency requirements for data-at-rest can be met within their environment.

REGULATION: One General Rule Though there is a wide variation between requirements, meeting this single rule ensures that your organization remains in compliance:

- No customer or employee data may be accessible to those outside of their home legal jurisdiction
- Exception: When explicit consent is given on a per-usage basis

The solution to the problem is to encrypt all data-at-rest and only allow access to data-at-rest from the jurisdiction where it originates.

ISO/IEC 27002:2013

Designed for organizations to use as a reference for selecting controls within the process of

implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls.

REGULATION: Among the best practices called for in ISO/IEC 27002 are:

- Data access controls
- Cryptographic control of sensitive data
- Recording and archiving “all significant events concerning the use and management of user identities and secret authentication information” and protecting those records from “tampering and unauthorized access.”

ISO 27799:2016

ISO 27799:2016 provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information. It is based upon and extends the general guidance provided by ISO/IEC 27002:2013 and addresses the special information security management needs of the health sector and its unique operating environments.

REGULATION: Among the best practices called for in ISO/IEC 27002 are:

- Data access controls
- Cryptographic control of sensitive data
- Management and protection of encryption keys
- Recording and archiving “all significant events concerning the use and management of user identities and secret authentication information” and protecting those records from “tampering and unauthorized access.”

Payment Card Industry Hardware Security Module (PCI HSM)

The PCI HSM specification defines a set of logical and physical security compliance standards for HSMs specifically for the payments industry.

REGULATION: Certification Objectives: HSMs play a critical role in securing payment transactions, so it is essential that the HSMs themselves are kept secure throughout their lifecycle— from manufacturing and shipment to operation and decommissioning. The PCI HSM compliance certification standard provides HSM vendors with a strict set of security requirements and a rigorous process for having platforms assessed against these requirements.

PCI HSM compliance certification is increasingly becoming a fundamental requirement for various payment processes, including PIN processing, card verification, card production, ATM interchange, cash-card reloading and key generation.

▪ Americas Regulations and Standards

This section covers regulations organizations in or dealing with the U.S. government must comply with as well as U.S. Federal and State regulations applying to digital security at large. It also includes a section on the Mexico Data Protection Law.

FDA/DEA Regulatory Compliance

Controlled Substance Ordering System (CSOS)

REGULATION: The DEA’s Controlled Substance Ordering System (CSOS) allows for secure electronic transmission of Schedule I-V controlled-substance orders without the supporting paper Form 222.

The DEA requires auditors to validate that the cryptographic modules are FIPS 140-2 certified. Auditors must also validate all aspects of the software that are addressed in the regulations

Electronic Prescriptions for Controlled Substances (EPCS)

REGULATION

EPCS revises DEA's regulations to provide practitioners with the option of writing prescriptions for controlled substances electronically. The regulations also permit pharmacies to receive, dispense, and archive electronic prescriptions.

The DEA's requirements for EPCS include:

- (16) The digital signature functionality must meet the following requirements:
 - (i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in Section 1311.08.
 - (iii) The electronic prescription application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in Section 1311.08.

In addition, in "§1311.205 Pharmacy application requirements" in the same DEA publication, the section states:

- (4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirements:
 - (i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140–2 Security Level 1 validated. FIPS 140–2 is incorporated by reference in Section 1311.08.
 - (iii) The pharmacy application's private key must be stored encrypted on a FIPS 140–2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140–2 is incorporated by reference in Section 1311.08.

Federal Information Security Modernization Act (FISMA)

FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government.

REGULATION: FISMA Requirements according to TechTarget's SearchSecurity website:

FISMA requires program officials, and the head of each agency, to conduct annual reviews of information-security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner.

The National Institute of Standards and Technology (NIST) outlines nine steps toward FISMA compliance:

1. Categorize the information to be protected.
2. Select minimum baseline controls.
3. Refine controls using a risk assessment procedure.
4. Document the controls in the system security plan.
5. Implement security controls in appropriate information systems.
6. Assess the effectiveness of the security controls once they have been implemented.
7. Determine agency-level risk to the mission or business case.
8. Authorize the information system for processing.
9. Monitor the security controls on a continuous basis.

Gramm Leach Bliley Act (GLBA)

The GLBA also known of as the Financial Services Modernization Act applies to U.S. financial institutions and governs the handling of non-public personal information. The act includes requirements for protecting customer financial records and other personal information.

REGULATION: Requirements:

Section 501(b) of the GLBA requires financial institutions to protect the security, confidentiality and integrity of non-public customer information through “administrative, technical and physical safeguards.” The GLBA also requires each financial institution to implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size, complexity and scope of activities of the institution.

These include:

- Ensuring the security and confidentiality of customer records and information
- Protecting against any anticipated threats or hazards to the security or integrity of such records
- Protecting against unauthorized access to or use of such records or information, which could result in substantial harm or inconvenience to any customer.

Implications:

- For organizations affected by the standard, these privacy regulations, combined with referenced requirements under the Federal Deposit Insurance Act – section 36, result in the need to:
- Safeguard and monitor customer records and information
- Create and maintain effective risk assessments Identify, implement and audit specific internal-security controls that protect this data

National Association of Insurance Commissioners Data Security Model Law

Adopted in late 2017, the National Association of Insurance Commissioners (NAIC) Data Security Model Law (Model Law) establishes standards that compel insurers and other entities licensed by state insurance departments to develop, implement, and maintain an information security program; investigate any cybersecurity events; and notify the state insurance commissioner of such events. To support insurers’ efforts, the NAIC has published “Principles for Effective Cybersecurity: Insurance Regulatory Guidance.”

The NAIC is encouraging states to introduce and pass this legislation now, and the US Treasury Department has indicated that it will take action at the federal level if the Model Law is not adopted by states within five years. Once a state adopts the law, insurers will have only one year to comply with most of its stipulations.

MODEL LAW:

The According to Section 2 of the act:

The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.

Section 3 also notes:

“Cybersecurity Event” means an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System. The term “Cybersecurity Event” does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization.

Section 4. Information Security Program D. Risk Management

Based on its Risk Assessment, the Licensee shall:

(2) Determine which security measures listed below are appropriate and implement such security measures.

(a) Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;

- (d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;
- (e) Adopt secure development practices for in-house developed applications utilized by the Licensee ...;
- (g) Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;
 - (i) Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events ...;
- (k) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.

New York State Cybersecurity Requirements for Financial Services Companies

The New York State Cybersecurity Requirements for Financial Services Companies took effect March 1, 2017. Covered entities are “required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations.”

REGULATION: New York State’s Department of Financial Services Cybersecurity Requirements for Financial Services Companies regulation:

Is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization’s cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity’s cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

“Section 500.06 Audit Trail” of the official document notes:

Each covered entity shall ... include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

And

As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

National Credit Union Administration (NCUA) Regulatory Compliance

The Federal Financial Institutions Examination Council (FFIEC) develops uniform reporting systems for federally supervised financial institutions, including credit unions. The Council helps credit unions prepare for NCUA audits and comply with federal mandates and standards, including those for data security. Among these are:

- Access rights administration
- Encryption and key management
- Security intelligence

REGULATION: Access Rights Administration according to FFIEC:

Financial institutions should have an effective process to administer access rights. The process should include:

- Assigning users and devices only the access required to perform their required functions
- Updating access rights based on personnel or system changes
- Periodically reviewing users' access rights at an appropriate frequency based on the risk to the application or system

Encryption and Key Management. FFIEC also notes:

- Encryption: *Financial institutions should employ an encryption strength sufficient to protect information from disclosure until such time as the information's disclosure poses no material threat. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure Encryption may also be used to protect data-in-storage. The implementation may encrypt a file, a directory, a volume, or a disk.*
- Encryption-Key Management: *Since security is primarily based on the encryption keys, effective key management is crucial. Effective key management systems are based on an agreed set of standards, procedures, and secure methods that address Source: ISO 17799, 10.3.5.2*

NIST 800-53 /FedRAMP

Beginning June 5, 2014, federal agencies are required to meet new standards for use of cloud computing under the FedRAMP initiative. With the combination of the push to cloud computing and with federal data breaches of personally identifiable information (PII) 2.5 times higher than in 2009, agencies now more than ever need to think about how to meet internal data security standards, as well as the extended security controls required for use of cloud-computing resources

REGULATION: NIST 800-53 and FedRAMP

The NIST 800-53 publication details security controls for Federal information systems as required by the FIPS 200 publication and was recently updated to revision 4 to detail the extended security controls required for agency use of cloud computing under FedRAMP.

REGULATION: FIPS 200 and FISMA

FIPS 200 supports the FISMA Act of 2002 requiring Federal agencies to implement and document information-security programs.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act of 2002 (SOX) is a United States federal law enacted on 30 July 2002, which sets standards for all U.S. public company boards, management, and public accounting firms. The primary sections of the SOX Act that concern protecting data are SOX Act sections 302 and 404.

REGULATION: Sarbanes-Oxley Act section 404 has two major compliance requirements:

- Management is accountable for establishing and maintaining internal controls and procedures that enable accurate financial reporting and assessing this posture every fiscal year in an internal control report.
- Public-accounting firms that prepare or issue yearly audits must attest to, and report on, this yearly assessment by management.

Sarbanes-Oxley Act section 302 expands this with compliance requirements to:

- List all deficiencies in internal controls and information, as well as report any fraud involving internal employees.
- Detail significant changes in internal controls, or factors that could have a negative impact

on internal controls.

Implications: The SOX compliance requirement implications for public companies to protect data are:

- Any financial information needs to be safeguarded, and its integrity assured.
- Specific internal-security controls need to be identified that protect this data, auditing must take place, and this security posture re-assessed every year – including any changes or deficiencies as a result of changing conditions.

Mexico Data Protection Law

Mexico's Data Protection Laws, and specifically, "Ley Federal de Protección de Datos Personales en Posesión de los Particulares", call for best-practice dataprotection solutions.

REGULATION: Mexico's Data Protection Law (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) became effective July 6, 2010.

"the objective of the General Law for the Protection of Personal Data is to establish the foundational principles and procedures to guarantee the right of all people to protect their personal information in possession of other subjects." (El Economista on 26 January 2017)

"The approval of the General Law for the Protection of Personal Data by Mexico's Legislature represents a significant advancement for the right of people to control the handling of their personal information." (El Financiero: Areli Cano Guadiana, Commissioner for the Institute on Transparency, Access to Information and Protection of Personal Data asserts)

"The Law applies to personal data that are processed, transferred, or disposed by private persons or entities. "Personal data" includes any information pertaining to an identified or identifiable natural person. Data controllers must have in place appropriate administrative, technical, and physical safeguards in order to ensure that personal data are protected from loss, damage, alteration, destruction, and unauthorized access or use." (Francoise Gilbert, Data privacy and security expert)

Penalties: According to the resolution enacted by the Honorary Representative Council of the National Commission on Minimum Salaries, infractions and Sanctions dictated by Chapter X of the General Law for the Protection of Personal Data are set between 100 and 320,000 days of minimum salary within the Federal District, which can amount to 6,500 to 20,700,000 Mexican pesos.

▪ **EMEA Regulations and Standards (Europe, Middle East and Africa)**

This section covers regulations specific to the European Union (EU, Middle East and Africa). These include Electronic Identification and Trust Services (eIDAS), the General Data Protection Regulation (GDPR), the Payment Services Directive 2 (PSD 2).

The EU's Electronic Identification and Trust Services (eIDAS)

The European Union's Electronic Identification and Trust Services (eIDAS) Regulation was developed to help establish a single European market for secure electronic commerce. For organizations that handle online transactions with European citizens, the Regulation will present significant opportunities, but it will also create new requirements.

REGULATION: eIDAS is a EU regulation that establishes standards for electronic identities, authentication and signatures. The goal of the Regulation is to encourage the creation of a single European market for secure electronic commerce.

The eIDAS Regulation applies to government bodies and businesses that provide online services to European citizens and that recognize or use identities, authentication, or signatures.

eIDAS requires that government and public commercial services recognize standard signature

formats and pan-European identities. This applies to services associated with tax statements, insurance contracts, banking agreements, business-to-business electronic invoicing and pharmaceutical records.

It also applies to commercial services that require a EU identity, for example, so-called “know your customer” services in banking. In addition, any trust services associated with these activities will be regulated by eIDAS.

EU Payment Services Directive 2 (PSD2)

The data security requirements for the revised EU Payment Services Directive PSD2 are still evolving. However, they will certainly call for a suite of industry best-practice solutions, as organizations work to increase security while maintaining high user-experience satisfaction levels.

REGULATION: According to the European Commission:

The current Payment Services Directive (PSD) was adopted in 2007. This legislation provides the legal foundation for an EU single market for payments, to establish safer and more innovative payment services across the EU. The objective is to make cross-border payments as easy, efficient and secure as ‘national’ payments within a Member State.

PSD2: Also, according to the European Commission:

The Commission proposed to review the PSD to update it to take into account new types of payment services, such as payment initiation services.

PSD2’s main objectives are to:

- Contribute to a more integrated and efficient European payments market
- Improve the level playing field for payment service providers (including new players) Make payments safer and more secure
- Protect consumers
- Encourage lower prices for payments

South Africa’s Protection of Personal Information Act

South Africa’s Protection of Personal Information (POPI) Act aims to ensure that organizations operating in South Africa exercise proper care when collecting, storing or sharing personal data.

REGULATION: South Africa’s POPI Act, which became law on 11th April 2014, requires organizations to adequately protect sensitive data or face large fines, civil law suits or even prison. The Act extends certain rights to data subjects that give them control over how their personal information can be collected, processed, stored and shared.

Guideline Descriptions:

- According to Chapter 11 (Offences, Penalties and Administrative Fines) of the POPI Act:
 - 107. Any person convicted of an offence in terms of this Act, is liable, in the case of a contravention of–
 - section 100, 103(1), 104(2), 105(1), 106(1), (3) or (4) to a fine or to imprisonment for period not exceeding 10 years, or to both a fine and such imprisonment; or
 - section 59, 101, 102, 103(2) or 104(1), to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.
- According to Chapter 11, “a Magistrate’s Court has jurisdiction to impose any penalty provided for in section 107.”

▪ APAC Regulations and Standards (Asia Pacific)

This section includes discussions of regulations from countries based in the Asia-Pacific region,

including Australia, Japan, Singapore, The Philippines and South Korea.

Australia Privacy Amendment (Notifiable Data Breaches) Act 2017

REGULATION: On February 13, 2017, the Australian Senate passed a bill establishing a mandatory requirement to notify the Privacy Commissioner and affected individuals of “eligible” data breaches. The Privacy Amendment (Notifiable Data Breaches) Act 2016 amends Australia’s Privacy Act 1988 and is slated to take effect on February 22, 2018 if no earlier date is proclaimed.

Penalties according to Global Legal Monitor:

A failure to notify that is found to constitute a serious interference with privacy under the Privacy Act 1988 can be penalized with a fine of up to AU\$1.8 million.

Japan My Number Compliance

REGULATION: The data-security requirements for businesses handling data associated with an individual’s Japanese “My Number” are governed primarily by Japan’s “Personal Information Protection Act (PIPA).” These include:

- Taking necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of personal data
- Exercising necessary and appropriate supervision over the employees handling the data to ensure the security control of the personal data
- Exercising necessary and appropriate supervision over any persons of organizations entrusted with the data to ensure the security control of the entrusted personal data.

Monetary Authority of Singapore Guidance (MAS)

To safeguard sensitive customer data and comply with MAS’s Technology Risk Management (TRM) guidelines, organizations need to apply consistent, robust, and granular controls.

REGULATION: The Monetary Authority of Singapore (MAS) published TRM Guidelines to help financial firms establish sound technology risk management, strengthen system security, and safeguard sensitive data and transactions.

The TRM contains statements of industry best practices that financial institutions conducting business in Singapore are expected to adopt. The MAS makes clear that, while the TRM requirements are not legally binding, they will be a benchmark the MAS uses in assessing the risk of financial institutions.

Guideline Descriptions:

- 8.4.4 The Financial Institution (FI) should encrypt backup tapes and disks, including USB disks, containing sensitive or confidential information before they are transported offsite for storage.
- 9.1.6 Confidential information stored on IT systems, servers and databases should be encrypted and protected through strong access controls, bearing in mind the principle of “least privilege”.
- 11.0.1.c Access control principle – The FI should only grant access rights and system privileges based on job responsibility and the necessity to have them to fulfill one’s duties. The FI should check that no person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.
- 11.1.1 The FI should only grant user access to IT systems and networks on a need-to-use basis and within the period when the access is required. The FI should ensure that the resource owner duly authorizes and approves all requests to access IT resources.
- 11.2 Privileged Access Management.
- 11.2.3.d. Grant privileged access on a “need-to have” basis.
- 11.2.3.e. Maintain audit logging of system activities performed by privileged users.
- 11.2.3.f. Disallow privileged users from accessing systems logs in which their activities are being captured.

- 13 Payment card security (automated teller machines, credit and debit cards).

Philippines Data Privacy Act of 2012

The rules derived from Philippines Data Privacy Act of 2012:

“..Further enforce the Data Privacy Act and adopt generally accepted international principles and standards for personal data protection. They safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development. These Rules also recognize the vital role of information and communications technology in nation-building and enforce the State’s inherent obligation to ensure that personal data in information and communications systems in the government and in the private sector are secured and protected.”

The Act and these Rules apply to the processing of personal data by any natural and juridical person in the government or private sector.

REGULATION: Technical Security Requirements

Section 28 of the rules, entitled Guidelines for Technical Security Measures, offers the following direction:

Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

- a) *A security policy with respect to the processing of personal data;*
- b) *Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;*
- d) *Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;*
- g) *Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.*

South Korea’s PIPA

South Korea’s Personal Information Protection Act (PIPA), came into force on 30 September 2011, and is one of the strictest data protection regimes in the world. It is also supported by sector-specific legislation:

The Act on Promotion of Information and Communication Network Utilization and

- Information Protection (the IT Network Act)
- The Use and Protection of Credit Information Act (UPCIA)

REGULATION: Breach Notification: PIPA places many obligations on organizations in both the public and private sectors, including mandatory data breach notification to data subjects and other authorities including the Korean Communications Commission (KCC).

Data Security: PIPA imposes a duty on information managers (i.e. data controllers) to take the “technical, administrative and physical measures necessary for security safety ... to prevent personal information from loss, theft, leakage, alteration or damage.”

Official Policy Statement: Organizations are required to establish an official statement of those security measures.

Internal Privacy Officer: An internal privacy officer must be appointed (regardless of the size or

nature of the organization) to oversee data processing activities. The internal privacy officer will be held accountable and be subject to any criminal investigations following a breach.

Encryption for Personal Identifiable Information (PII): Article 24(3) of PIPA places express restrictions on the management of unique identifying information, and requires information managers to take “necessary measures, ... including encryption,” in order to prevent loss, theft, leakage, alteration or damage. Similarly, Articles 25(6) and 29 require “necessary measures” to be implemented to ensure that personal information may not be lost, stolen, altered or damaged.

Strict Enforcement: South Korea also has a track record of enforcement of data protection laws. Chapter 9 of PIPA contains severe sanctions for data security breaches including fines of up to 50 million won and imprisonment of up to five years.

B. Basic Best Practices for Regulation Compliance

Some Industries and organizations may have to comply with multiple regulations or are required to meet information security standards established by laws. As explained in previous sections, some example could be the financial industry being subject to the requirements of the Graham-Leach-Bliley (GLB) Act. Health care providers, health insurers and health information data processors which are bound by the Healthcare Insurance Portability and Accountability Act (HIPAA), or Publicly traded companies' responsibilities under the Sarbanes-Oxley (SOX) Act include the protection of financial systems from fraud and abuse. Besides laws and regulations, there are also a number of voluntary standards available to organizations that wish to benchmark their security programs against industry best practices.

In such cases it is best to outline all the regulations that impact the company first. Knowing what expertise is available and which standards are relevant to the company's sector are the first steps to ensure organizations are regulation compliant. Once done, a determination can be made for which security controls to implement that satisfy the requirements of all the regulations that need to be complied with. This process can (more than likely) reduce the amount of money organizations spend on compliance efforts because it reduces duplication of effort and the likelihood that competing systems would be put in place to satisfy the same regulatory requirement.

The following will describe the steps to follow as "Best practices" to proceed to comply with the laws, specific regulations that may apply to companies.

- **Interpretation of laws and regulations**

Regulations are rarely technical documents with step-by-step instructions, being written by legal experts, as they must be crafted in such a manner to allow them to be debated robustly by teams of experts in a court of law.

Organizations must identify if they have the expertise to interpret and apply these regulations to their practices. If the in-house resources fulfill the competences required, or if or there is a need to subcontract additional help. Many security companies supply assessment services against recognized standards and best practices. Often, they will provide advice to improve security and data privacy and the documented results can be used to validate the organization's performance.

- **General & Sector-Specific Regulations Identification**

After expertise has been engaged (in-house or otherwise), identifying regulations relevant to the organization can be started.

- As a starting point, recommendable to begin with the most general ones like FISMA, NIS Directive or GDPR.
- After reviewing the most general ones, the focus can then be placed on regulations specific to the organization's sector, be it finance, healthcare, etc. Very important to bear in mind that the geographic jurisdiction(s) where the company operates will dictate what regulations apply. For instance, if the organization is based in Canada but carries out work in France, then it may be liable to comply with French as well as Canadian regulations. On the other hand, the use of Cloud computing resources for storing and processing data which must also be considered, is an ongoing issue with discussions on geographic jurisdiction.

- **Standards**

Standards are guidelines, which usually are drawn up by industry actors and agreed upon via a consensus process and finally approved by a recognized body, which can significantly assist an organization on the path to regulatory compliance. Standards are not legal documents, and various bodies publish guidelines that may be useful to particular organizations. Standards are not legal documents, and various bodies publish guidelines that may be useful to particular organizations. There is correlation between organizations that fully conform with standards and those that are compliant with regulation.

The first step towards compliance is conforming with relevant standards, and mirroring the

regulation environment, there are general standards and sector-specific standards, where the more recognized the standard a company conforms with, the closer it gets to complying with regulation.

Highlight that complying with standards is voluntary and complying with regulations is mandatory, as regulations are legal and/or industry requirements, laid down by government or statutory authority, that can be used to force organizations to carry out certain security measures or impose penalties if measures are not carried out.

- **Implementation Effort Planning**

Once relevant regulations and supporting standards have already been identified, an assessment must be performed to estimate how much work will be involved to implement the standards. Points to be considered:

- Possible changes to existing work practices
- Staff training
- Additional resources as online storage
- Gathering and storing of accompanying evidence

These points will help to develop a cost-benefit analysis, obtaining as output whether the costs outweigh the benefits or not.

Once the target standards have been identified, organizations should map existing practices to them, building their own bank of evidence. This set of data will demonstrate to standardization bodies that relevant standards are being implemented. If and when required, it will also help demonstrate that regulations are being followed.

Standards should serve as an outline and reference during the writing and updating of an organization's security policies. By combining the high-level best practices of the standards with the specific business knowledge distributed throughout the organization, policies can be developed that combine security with business needs.

Standards must be translated into measurable actions. The key for that will be clarity and consistency. The same procedural and policy documents built up to meet the standards in front of everyone in the organization should be able to make them come to the same conclusions as to the security measures that are needed to meet the standard.

- **Risk Management**

The next step after initial compliance data are in place is to ensure they are updated regularly by building compliance into the organization's risk management program.

Although they can be differentiated in detail, most organizational risk management strategies are built on a continuum: identify, analyze, evaluate, treat and monitor.

Identifying laws that the organization must comply with, is the first part of assessing compliance risk. Regular analysis of compliance must be given due attention in the organization's overall risk management program. Responsibility must be assigned to the appropriate person, who will consider compliance in legal terms but also separately at operational and reputational levels.

The risks being taken must be understood and documented, as well as their mitigating factors. Informed decisions as to whether to accept a risk must be made and documented too. Periodically review accepted risks to determine whether new mitigations are available and whether the risk is still acceptable

Having a well-defined process to handle exceptions will allow the organization to deal with situations that fall outside of those anticipated when the policies were written. Companies must be prepared for exceptions, as they have different needs and tolerance for risk. Being prepared to deal with situations when a business need conflicts with a security best practice, will save time, money and aggravation

- **Auditing**

Auditing will be the last step to verify an organization's compliance. And this can be done internally, externally or both.

C. Encryption Solutions: Hytrust & SafeNet

Hytrust

Managing Encrypted Workloads in a Multi-Cloud Infrastructure

HyTrust DataControl allows you to manage your encrypted workloads across different infrastructures. DataControl works on-premises and with the leading public cloud platforms, but also with hyperconvergence and storage solutions. With DataControl, you get a centralized and scalable solution to control all your encryption keys. DataControl includes the VMware certified HyTrust KeyControl Key Management Server (KMS).

HyTrust DataControl – Workload Encryption and Integrated Key Management Provides strong data-at-rest encryption for workloads in any cloud, along with easy-to-deploy key management that organizations control, whether workloads are running in a private cloud powered by vSphere or in public clouds like IBM SoftLayer, Microsoft Azure, vCloud Air, or AWS—throughout the entire workload lifecycle. DataControl also supports the highest levels of availability by offering the ability to rekey workloads without taking applications offline.

Deep Workload Protection

Apply strong security and protection for workloads throughout their lifecycle, from boot to backup, and final decommissioning stage.

DataControl provides granular encryption for better security. The protection boundary does not stop at the hypervisor or at the data store; VMs are individually encrypted. Inside the VM, unique keys can be assigned to encrypt each partition, including the boot (OS) disk and swap partitions.

Easy to Deploy and Manage

DataControl provides deployment flexibility with a single interface for all workload encryption, which eliminates the complexity of using each platform's own encryption feature separately. The user experience is great for administrators and zero downtime encryption allows for frequent and more secure re-keying while the workload remains accessible. High Availability clustering ensures your disaster recovery is not impaired by losing access to the critical key management system of DataControl.

ENCRYPTION KEY MANAGER

HyTrust KeyControl – Workload Encryption Key Management Simplifies the process of key management for workloads that do not require sophisticated policy-based key management, but need to scale to enterprise-level performance. Organizations retain full ownership of encryption keys with policy-based controls to protect data and meet compliance requirements. KeyControl works with both DataControl and third-party encryption solutions

ACCESS CONTROL

DataControl allows for robust policy-based access controls to enforce separation of duties across different user personas. Prevent root users or system administrators from accessing sensitive data by enforcing access controls on encrypted volumes. For hybrid cloud deployments, prevent your cloud service providers' administrators, often responsible for patching and other operational upkeep, from ever accessing encrypted data. DataControl allows for custom controls across a variety of use cases to enable greater security across multi-cloud deployments.

SafeNet-Gemalto

ENCRYPTION DATAFORMAT

Protecting structured data at rest in databases and applications:

For sensitive and regulated data residing in databases and applications, Gemalto provides encryption and tokenization solutions to ensure the security of information throughout its lifecycle. Organizations can retain control of their data and meet compliance standards by ensuring only authorized individuals are able to decrypt and view sensitive information

Protecting unstructured data at rest in files and storage:

The majority of an organization's data is unstructured – text files, photos, videos, presentations, emails, web pages, and other sensitive business documents. Gemalto's SafeNet encryption solutions protect sensitive data as it is accessed, shared, and stored beyond the traditional data center.

DATABASE ENCRYPTION

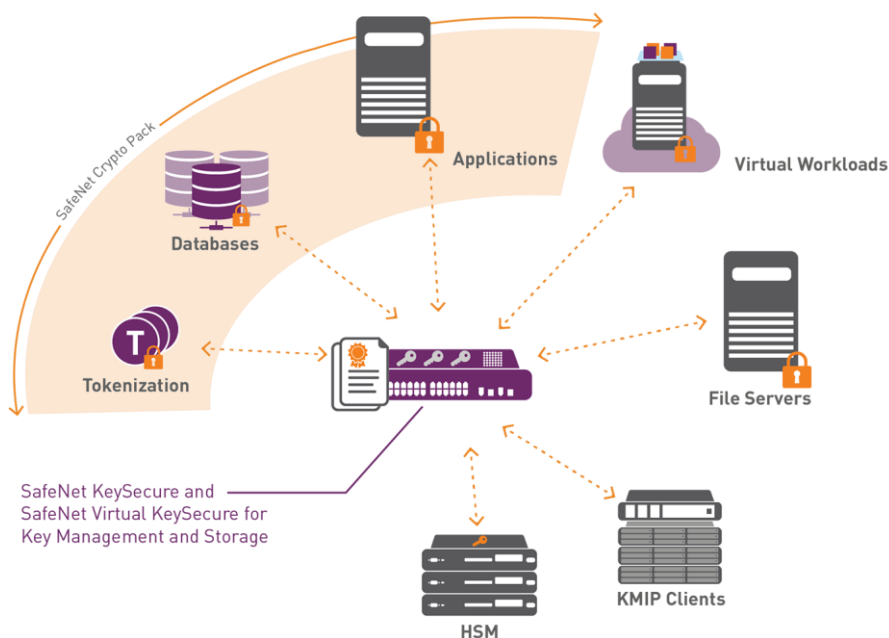
SafeNet ProtectDB:

- Transparent and efficient database encryption of sensitive column-level data
- Works in tandem with Gemalto's FIPS 140-2 up to Level 3 validated SafeNet KeySecure enterprise key manager to provide complete ownership and centralized administration of all keys and policies
- Granular access controls can be applied based upon role, user, time of day, and other variables, including the ability to prevent database administrators (DBAs) from impersonating another user
- Built-in and automated key rotation and data re-keying
- Comprehensive logging and auditing capabilities to track access to encrypted data and keys
- Ability to offload database encryption to SafeNet KeySecure for external processing power

ENCRYPTION KEY MANAGER

Secure key management and storage of encryption keys:

With Gemalto, organizations can centrally, efficiently, and securely store and manage cryptographic keys and policies – across the key management lifecycle and throughout the enterprise.



- **Heterogeneous Key Management.** Manage keys for a variety of encryption products including tokenization, and applications through SafeNet Data Protection Connectors, as well as selfencrypting drives, tape archives, Storage Area Networks, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.
- **Multiple Key Types.** Centrally manage Symmetric and Asymmetric Keys, secret data, and X.509 certificates along with associated policies.
- **Full Lifecycle Key Support and Automated Operations.** Simplify the management of encryption keys across the entire lifecycle including secure key generation, storage and backup, key distribution, deactivation and deletion. Automated, policy driven operations simplify key expiry and rotation tasks.
- **Centralized Administration of Granular Access, Authorization Controls and Separation of Duties.** Unify key management operations across multiple encryption deployments and products, while ensuring administrators are restricted roles defined for their scope of responsibilities, from a centralized management console. Also, SafeNet KeySecure can utilize existing LDAP or AD directories to map administrative and key access for application and end users.
- **High-Availability and Intelligent Key Sharing.** Deploy in flexible, high-availability configurations within an operations center and across geographically dispersed centers or service provider environments using an active-active mode of clustering.
- **Auditing and Logging.** Detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading 3rd party SIEM tools.
- **Next-Generation Storage and Archive Solution.** Simplify secure storage and efficiently scale data centers while reducing costs and complexity, with SafeNet KeySecure and leading storage vendors such as NetApp, Dell, Nutanix, IBM, Hitachi, and HPE.

ACCESS CONTROL

Gemalto offers granular encryption and role-based access control for structured and unstructured data residing in databases, applications, files, and storage containers. With centralized key management and a hardened root of trust, organizations can ensure their master keys are protected and data remains secure

APPLICATION PROTECTION

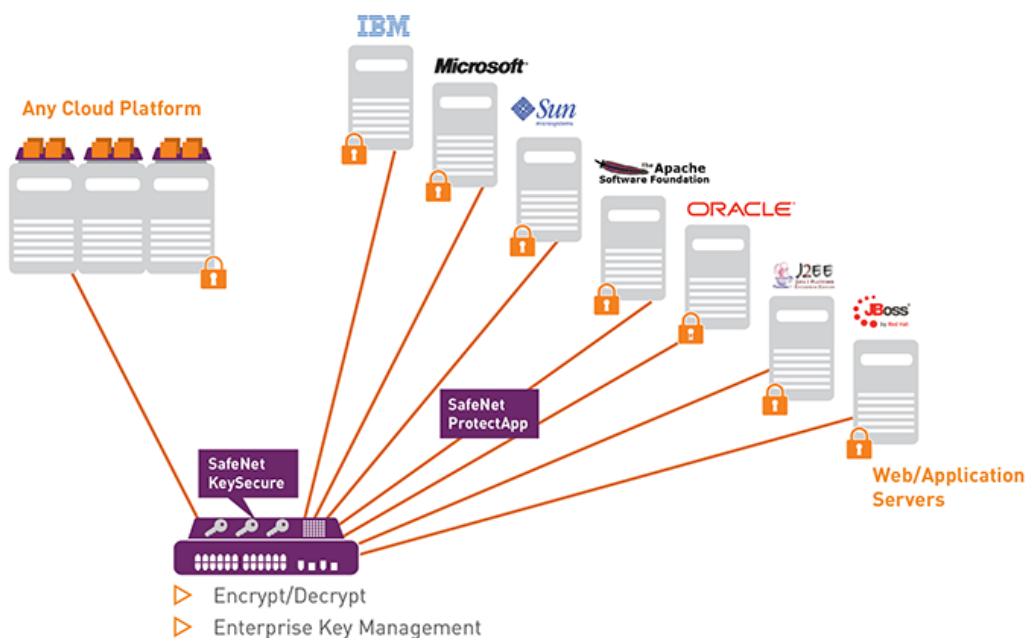
SafeNet ProtectApp: Application Protection Solutions

SafeNet ProtectApp provides an interface for key management operations, as well as application-level encryption of sensitive data. Once deployed, data is kept secure across its entire lifecycle, no matter where it is transferred, backed up, or copied.

Using Safenet ProtectApp APIs, both structured and unstructured data can be secured in multi-vendor application server infrastructures. SafeNet ProtectApp's application-level encryption can be deployed across on-premises, virtual, cloud, and hybrid environments.

- Deployed with SafeNet KeySecure, a FIPS 140-2 up to Level 3 validated enterprise key manager to provide centralized administration of all keys and policies
- Granular access controls to ensure only authorized users or applications can view protected data
- Support for Format Preserving Encryption (FPE)
- Broad standard and interface support, including web services (SOAP and REST)
- Built-in, automated key rotation and data re-keying
- Comprehensive logging and auditing capabilities
- Ability to offload encryption to SafeNet KeySecure for external processing power

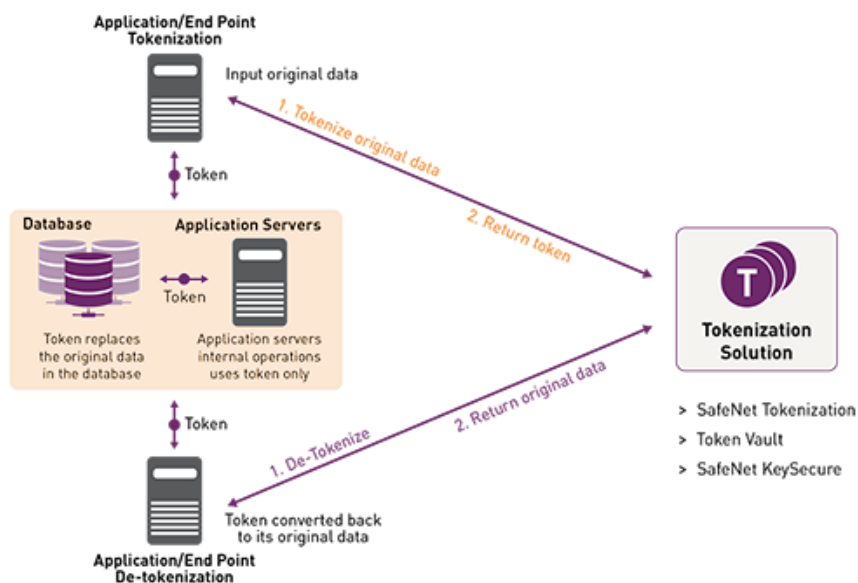
SafeNet ProtectApp and SafeNet KeySecure



TOKENIZATION SafeNet Tokenization

SafeNet Tokenization from Gemalto protects sensitive information by replacing it with a surrogate value that preserves the length and format of the data. The solution tokenizes numeric and alphanumeric data and returns tokens in an unlimited number of formats.

SafeNet Tokenization Deployment



SafeNet Tokenization Features:

- Apply transparent and secure application-level tokenization to structured sensitive data across on-premises, virtual, public cloud, and hybrid cloud environments
- Works with SafeNet KeySecure to provide centralized administration of all keys and policies
- Granular access controls to ensure only authorized users or applications can view protected tokens and data
- Unlimited data type support enables tokenization of primary account numbers (PAN), as

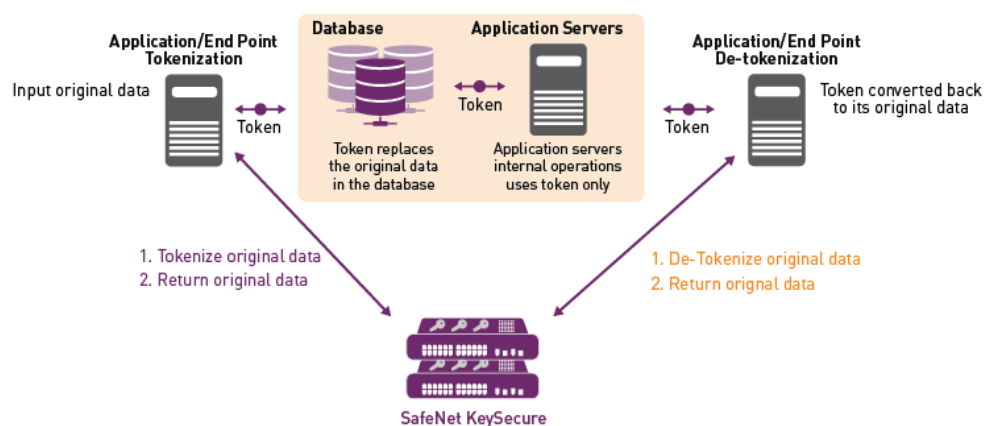
well as other data types (PCI, PII, PHI, etc.) in any environment including payment systems and big data environments

- Broad token format support, including regular expressions and customized formats
- No changes required to applications, databases, or legacy systems with Format Preserving Tokenization (FPT)
- Fast and easy deployment with web services (SOAP and REST/JSON), as well as the ability to leverage bulk tokenization and batch APIs
- Built-in, automated key rotation and data re-keying
- Track user access to tokens and protected data with comprehensive logging and auditing capabilities

SafeNet Tokenization Benefits

- **Proven data protection:** Secure structured sensitive data with transparent, application-level tokenization
- **Ensure Compliance:** Comply with internal security policies and regulatory mandates; Meets PCI Tokenization Guidelines and Visa Tokenization best practices
- **Centralize and Streamline Data Security:** Unify administration and extend data protection to all layers of the technology stack with SafeNet KeySecure and the full portfolio of SafeNet encryption solutions
- **Leverage the Cloud Securely:** Maintain complete ownership and control of your data and keys in virtual, public cloud, and hybrid environments
- **Speed Time to Deployment:** Simplify integration and ongoing processes by leveraging SafeNet Tokenization's web services, APIs, and bulk tokenization capabilities.

SafeNet Vaultless Tokenization (SVT) replaces sensitive data with a random, surrogate value or 'token' much like traditional tokenization solutions, but without the underlying database or 'token vault' that matches original data and tokens. The vaultless approach is quick and easy to deploy while being well suited for large scale, distributed environments.



D. Experimental Analysis Use Cases Deployment

HEALTH CASE CONFIGURATION AND DEPLOYMENT

INSTALLATION AND CONFIGURATION PLAN

1. Prerequisites for Installing Vormetric Transparent Encryption
2. Installing the DSM AMIs
3. Configure the DSMs using the CLI
4. Configure the DSM settings for the AD/LDAP server.
5. Configure and remote logging and add remote syslog server with Security Intelligence and Event Management.
6. Configure the DSM HA
7. Install external certificate authority

DSM REQUIREMENTS

Requirements:

- The recommended minimum virtual hardware configuration for production environments is:
 - Number of CPU cores: 4
 - RAM: 4 GB minimum.
 - Hard Disk Space: 150 GB

In the AWS environment, we deployed instance type is m4.xlarge:

Model	vCPU*	Mem (GiB)	Storage	Dedicated EBS Bandwidth (Mbps)	Network Performance
m4.xlarge	4	16	EBS-only	750	High

VTE deployed

To be able to apply protection policies in any Host it is necessary to install the VTE agent and register it in the Data Security Manager.

DataBase Deployed

The DBs deployed have the following characteristics:

Cassandra

- Number of CPU cores: 8
- RAM: 15 GB minimum.

In the AWS environment, the recommended instance type is c4.2xlarge.

Syslog deployed

The Syslog deployed has the following characteristics:

- Number of CPU cores: 2
- RAM: 8 GB

In the AWS environment, the recommended instance type is m4.large

DSM Ports Configuration

The following table lists the communication direction and purpose of each port we must open.

Post registration communication with the DSM is over ports:

Port	Protocol	Communication Direction	Purpose
8080	TCP	VTE → DSM	Default TCP/IP port for HTTP that is used once to perform the initial certificate exchange between a VTE host and DSM.
8447	TCP	VTE → DSM	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also, for secure communication between DSMs in HA cluster.
7025	TCP	DSM → DSM	DSM to DSM for failover communication
8444	TCP	VTE → DSM	Upload VTS log messages to DSM
5696	TCP	KMIP ↔ DSM	Allows communication between the KMIP client and primary DSM
8443	TCP	Browser ↔ DSM	TCP/IP port through which the VTE communicates with the DSM to exchange configuration. The VTE establishes a secure connection to the DSM via certificate exchange using this port.
8446	TCP	VTE → DSM	Configuration exchange (policy/key pull) using Elliptic Curve Cryptography (Suite B)
7024	TCP	VTE ↔ DSM	Request policy updates
8448	TCP	DSM ↔ DSM	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also, for secure communication between DSMs in HA cluster.
161	TCP	SNMP queries → DSM	SNMP queries from an external manager
8445	TCP	DSM ↔ DSM	Management Console, VMSSC, and fall back for HA communication in case port 8448 is dropped.

AD/LDAP server integration

The integration of the DSMs with Active Directory has been configured to carry out the authentication of the administrators of the tool.

The following group was created in AD: Test_DSMSsystemAdmins

And the following users were included:

- Domain and Security Administrator
- System Administrator
- System Administrator

The following steps describe how DSM was configured with the AD/LDAP server authentication:

- 1) Log like System Administrator in DSM in and select System > LDAP.
- 2) Enter the URL of the LDAP server in the Directory URL field. If a secure LDAP URL is specified here, then its LDAPS Server Certificate in PEM format must also be entered in LDAPS Server Certificate.
- 3) Enter a Base Distinguished Name.
- 4) (Optional) Enter up to a 256-character string to filter searches, in the LDAP Query field.
- 5) (Optional) Enter the LDAP user login name in the Login field.
- 6) (Optional) Enter the LDAP password in the Password field. Enter it again in Confirm Password.
- 7) LDAPS Server Certificate: If a secure LDAP path was entered in the Directory URL field, click Browse and navigate to the location of the Root CA Certificate. The CA certificate must be in PEM format. This field does not allow direct user input to avoid typographic errors.
- 8) The CA Certificate Exists box will be checked if the LDAPS Server Certificate has been uploaded to the DSM.
- 9) Enter the "Object Class" attribute in the User Object Class field.
- 10) Enter the user attribute containing the unique user ID in the Login Name Attribute field. This is the AD/LDAP schema attribute to be used as the LDAP user login name.
- 11) (Optional) Enter the user attributes desired in the User Description Attribute(s) field. To enter multiple attributes, separate values with a semicolon.
- 12) (Optional) Email Attribute: This is the AD/LDAP schema attribute to be used as LDAP user email.
- 13) Enter the group "Object Class" attribute in the Group Object Class field.
- 14) Click OK to save the settings on the page or click Clear to clear the form. We can also click Clear any time later to delete the AD/LDAP settings.

The Import function allows Administrators to import data from an Active Directory (AD). Once an AD has been identified and configured, the DSM Administrator can import the desired values. To import values from an AD we will need to introduce an LDAP login ID and password:

- 1) Select the Administrators > All tab. Click Import.
- 2) Enter the Login ID and Password. If the Login and Password were entered under LDAP Server Settings on the *AD/LDAP Details* window, these values will be populated and do not need to be re-entered. We may also enter a different Login and Password in place of these stored values when we import administrators.
- 3) Click Connect.
- 4) The *LDAP Users* window displays LDAP user names.

Once the administrators have been imported we can established the value from "User Type" drop down box to define the type of Administrator or role of the values we import.

Current Policies created

VTE is based on controlling access to and encrypting sensitive data files. These files maybe data files within a structured data store of a database or other data files that reside in the file system or in file shares.

Guard Points are the points (directories) within the file system where we apply a VTE policy. Once applied the VTE policy governs all access to files within the guard point this includes files in any subdirectory of the guard point.

A TE Policy is a set of rules that govern every IO performed within the guard point's directories. The IO characteristics are evaluated according to the policy's rules and once a matching policy rule is found the effect of the rule is performed.

The policies currently applied in the AWS environment are summarized below:

Policy name	Policy type	Resources	User	Process	Action	Effect	When	Browsing
Vorm_Cas_Operations	Standard	/data/cassandra_new/data	CasN_User	All process	all_ops	Permit, Audit, Apply_key	24 H	On
	Standard	/data/cassandra_new/data	Root_User_CasN	All process	read, f_rd_att, f_rd_sec, d_rd, d_rd_sec, f_rd, d_rd_att, f_cre, f_link, d_mkdir	Permit, Audit	24 H	On
	Standard	/data/cassandra_new/data	EC2_Users_CasN	All process	read, f_rd_att, f_rd_sec, d_rd, d_rd_sec, f_rd, d_rd_att, f_cre, f_link, d_mkdir	Permit, Audit	24 H	On
	Standard	/data/cassandra_new/data	All users	All process	all_ops	Deny, Audit, Apply_key	24 H	On

Select	Order	Resource	User	Process	Action	Effect	When Browsing
<input type="checkbox"/>	1		Cas1_User		all_ops	Apply Key, Audit, Permit	Yes
<input type="checkbox"/>	2		Root_User_Cas1		read, f_rd_att, f_rd_sec, d_rd, d_rd_sec, f_rd, d_rd_att, f_cre, f_link, d_mkdir	Audit, Permit	Yes
<input type="checkbox"/>	3		EC2_Users_Cas1		read, f_rd_att, f_rd_sec, d_rd, d_rd_sec, f_rd, d_rd_att, f_cre, f_link, d_mkdir	Audit, Permit	Yes
<input type="checkbox"/>	4				all_ops	Apply Key, Deny, Audit	Yes

Agents communication

Domain and Security Administrator user of the domain must access to DSM, clicking on 'Hosts' drop-down menu we can verify that 'Pushing Status' in all agents is 'Done' instead of 'Pending':

FS Agent	Key Agent	One Way Communication	Delete Pending	License Type	Docker Enabled	Description	Sharing
Reg. Allowed: <input checked="" type="checkbox"/> Comm. Enabled: <input checked="" type="checkbox"/> Pushing Status: Done	Reg. Allowed: <input checked="" type="checkbox"/> Comm. Enabled: <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TERM	<input type="checkbox"/>		
Reg. Allowed: <input checked="" type="checkbox"/> Comm. Enabled: <input checked="" type="checkbox"/> Pushing Status: Done	Reg. Allowed: <input checked="" type="checkbox"/> Comm. Enabled: <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TERM	<input type="checkbox"/>		
Reg. Allowed: <input checked="" type="checkbox"/> Comm. Enabled: <input checked="" type="checkbox"/> Pushing Status: Done	Reg. Allowed: <input checked="" type="checkbox"/> Comm. Enabled: <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TERM	<input type="checkbox"/>		

Guarded status policies

Clicking on 'Hosts' drop-down menu we can check the status of the policies in each of the nodes:

Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Status	Rekey Status
	/data/cassandra/data/		Directory (Auto Guard)	RochePRDEU	<input type="checkbox"/>	<input checked="" type="checkbox"/>	●	N/A

DSM High Availability configuration

We set 2 DSMs configured in high availability. The following describes the steps carried out for the configuration in HA:

Adding DSM2 to DSM1 database

- 1) Install and configure two DSMs.
- 2) On DSM1 (primary), log on to the Management Console as System Administrator.
- 3) Click High Availability in the menu bar. The High Availability Servers window opens.
NOTE: The license must be installed on the primary DSM before HA can be configured.
- 4) Click Add. The Add Server window opens.
- 5) In Server Name, enter the hostname of DSM2 (failover).
- 6) Click Ok. DSM2 is listed in the High Availability Servers with the role of Failover.

Registering DSM2 as a failover with DSM1

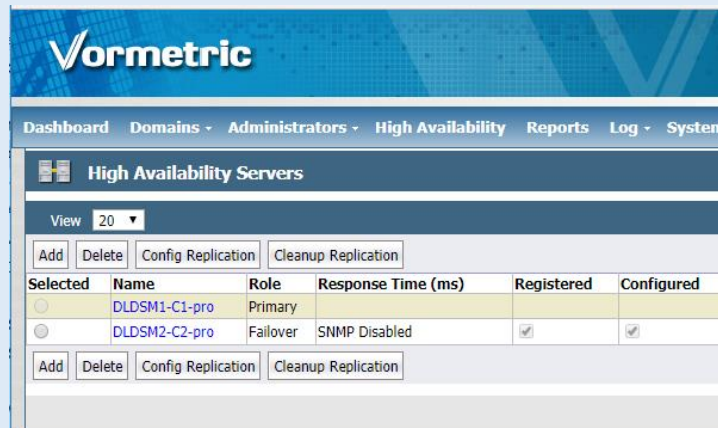
- 1) On DSM2, log on to the DSM CLI.
- 2) Type `convert2failover`
- 3) Follow the prompts:
 - a. Type `yes` to continue.
 - b. Type the host name or FQDN of DSM1, the primary server.
 - c. Type the name of an administrator of type System Administrator or All that is configured on DSM1.
 - d. Type the same administrator's password.
 - e. Press Enter to use the default name for the local host. Do not change this name.
- 4) The primary DSM will issue the certificate using the information provided.
- 5) Type `yes` to continue. The installation utility creates certificates, completes the installation process, and then starts the DSM. This may take a few minutes.
- 6) On DSM1 on the Management Console, click the Dashboard tab.
- 7) Match the fingerprint from the output on DSM2 with the RSA CA fingerprint on the Dashboard.
- 8) Click the High Availability tab. In the row for the failover DSM, the Registered check box should be selected.

Configuring replication

After failover is configured, we needed to configure the primary to replicate its information to the new failover.

- 9) In the Selected column, select the failover DSM.
- 10) Click Config Replication. A dialog box opens, prompting us to continue.
- 11) Click OK. The Configured check box for the failover DSM should be enabled after configuration completes.
- 12) Verify that the failover DSM configuration completed successfully. The Synchronization

Status column should contain a green circle indicating that the failover has been synchronized with the primary. Check the High Availability Servers window on the primary DSM.



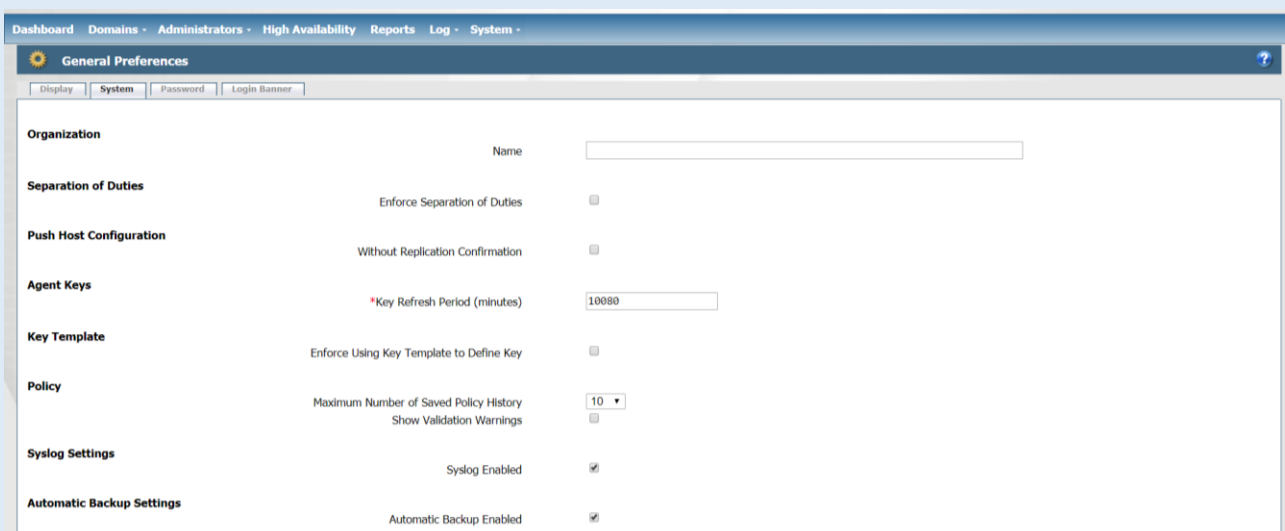
Redirect log messages to a remote syslog server

Have the following information describe the steps needed to start the Syslog integration process.

- IP address or host name of Syslog server
- Transport protocol to connect to Syslog server
- Port number for the Syslog server

Following are the high-level steps for integrating VDS with a Splunk system.

- 1) Enable logging to a syslog server.
 - a. Log on to the DSM Management Console as an administrator of type System or All.
 - b. Click System > General Preferences. The *General Preferences* window opens.
 - c. Click the System tab on the *General Preferences* page
 - d. Under Syslog Settings, click Syslog Enabled.

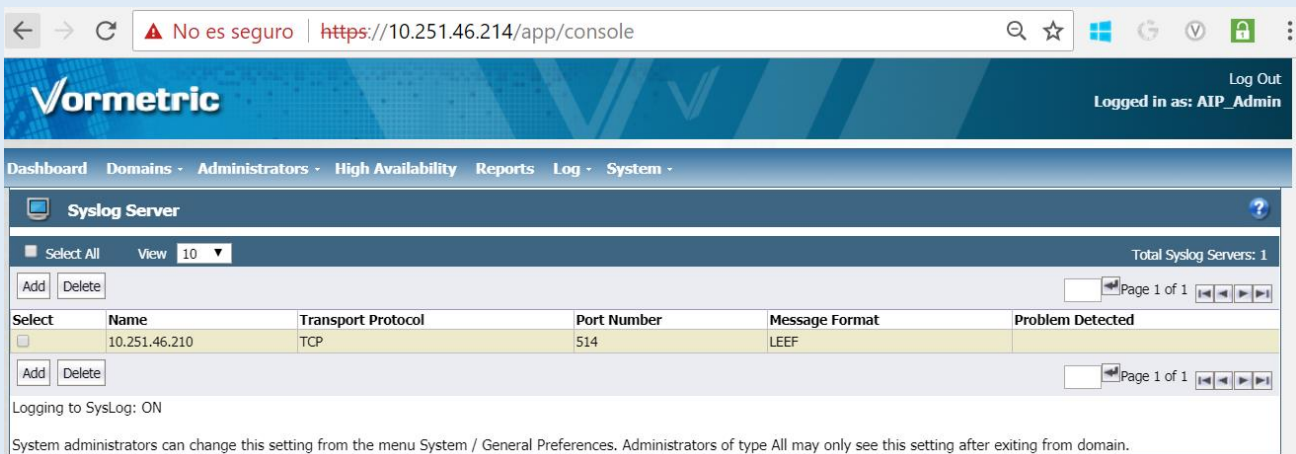


- e. Click Apply. The DSM now allows logging to a syslog server.

- 2) Configure message format log output from the DSM.

- a. Log into the DSM Management Console as an administrator of type System or All.

- b. Click the Log tab and select Syslog. The *Syslog Server* window opens.
 - c. Click Add and enter the following information:
 - i. Server Name—The host name or IP address of a syslog server. Use a syslog server that is accessible to the primary DSM and all the failover DSMs in the HA cluster.
 - ii. Transport Protocol—Select UDP, TCP, or TLS from the dropdown menu. If we select TLS, a dialog box displays for us to browse to a Certificate.
 NOTE: For syslog servers configured with the UDP transport protocol, ensure that UDP packets are not blocked by a firewall or switch rules.
 NOTE: If we add a syslog certificate (when using the TLS protocol), we must do a system > server restart from the CLI. After restart, verify that the syslog server is logging messages as expected.
 - iii. Port Number—The port number the transport protocol uses to connect to the syslog server.
 - iv. Message Format— Chose the format
 - d. Click Ok. Verify the details on the summary screen.
 - e. Define a syslog server for DSM logging for each domain where agent systems have been defined. Select Domains > Switch Domains.
 - f. Select a domain and click Switch to domain.
- Repeat steps 2 through 4. for each domain where agents are registered.



FINANCIAL CASE CONFIGURATION AND DEPLOYMENT

INSTALLATION AND CONFIGURATION PLAN

These are the high-level steps performed to install Vormetric Tokenization:

1. Prerequisites for Installing Vormetric Tokenization
2. Configure the DSM to enable the VTS installation
3. Installing the VTS AMIs
4. Use the CLI (Vormetric Token Server Administrative Command Line Interface (CLI)) to configure the Token Server settings for the hostname, network settings, import a server certificate, and DSM server.
5. Create VTS HA cluster
6. Configure the Token Server settings for the AD/LDAP server.
7. Configure and remote logging and add remote syslog server with Security Intelligence and

Event Management.

8. Restart the Token Server
9. Configure the VTS using the GUI (basic steps to test the API REST).

PREREQUISITES FOR INSTALLING VORMETRIC TOKENIZATION

VTS REQUIREMENTS

Vormetric Token Servers are virtual machines. Requirements:

- The recommended minimum virtual hardware configuration for production environments is:
 - Number of CPU cores: 16
 - RAM: 24 GB minimum. 32 GB recommended if VTS will be used to tokenize credit card numbers longer than 16 digits.
 - Hard Disk Space: 200 GB

In the AWS environment, we deployed instance type m4.10xlarge:

Model	vCPU*	Mem (GiB)	Storage	Dedicated EBS Bandwidth (Mbps)	Network Performance
m4.4xlarge	16	64	EBS-only	2,000	High

Gather this Vormetric Token Server information for system configuration:

Name
Token Server system hostname
Token Server IP address
Token Server subnet prefix length
Token Server default gateway
DNS Server IP address

ACTIVE DIRECTORY/LDAP SERVER REQUIREMENTS

- Access to the AD/LDAP server containing users and groups that will have Vormetric Tokenization privileges.
- For LDAPS, the LDAP server's CA certificate needs to be imported into the Token Server.
- If we use the three example Active Directory groups (vtsUsers, vtsManager, and vtsSuperuser) below, create these groups before doing "Configure the Token Server settings for the AD/LDAP server".

Gather this AD/LDAP information for system configuration:

Name	Description
LDAP Server URI	Hostname, port and protocol of LDAP server. Example: ldaps://ads.example.com:636
Binding DN	FQDN of user that has access to the LDAP Server Example: vts0@ads.example.com
Binding password	The credential of above user Example: H838%i2hz9*%^86&^*
user search scope	Search criteria of user object in AD/LDAP server

	Example: dc=corp,dc=example,dc=com
user group search scope	Search criteria of user group inside AD/LDAP Example: cn=Users,dc=corp,dc=example, dc=com
user search filter	Name of user field in AD/LDAP Example: sAMAccountName for AD, uid for LDAP
Token Server active user group	Group that user can access Token Server RESTful API Example: cn=vtsUsers,cn=User,dc=corp, dc=example, dc=com
Token Server super user group	Group that can access the GUI and REST APIs. Example: cn=vtsSuperuser,cn=Users,dc=corp, dc=example, dc=com
Group member selector	UNIX/Linux LDAP only. The LDAP attribute which designates a group member within a group. Example: member or memberUID
group object class	UNIX/Linux LDAP only. The LDAP attribute that identifies a group of users. Example: posixGroup or groupOfNames
User prefix	UNIX/Linux LDAP only. The LDAP attribute to be used to prefix the username when searching for username in the LDAP database Example: uid, cn, sn
CA Certificate	For LDAPS only: Access to root and intermediate CA certificates for the LDAPS server in .pem file format. May require a Certificate Management tool

REMOTE LOGGING SERVER

Some information is required to redirect log messages to a remote logging server. Gather this remote logging server information for system configuration:

Name
Remote logging server name or IP address
Remote logging server port (TCP)

PORT CONFIGURATION

• INCOMING PORTS TO CONFIGURE FOR VTS

Port	Protocol	Communication Direction	Purpose
22	TCP	Management Console →VTS	Administration CLI SSH access
443	TCP	Browser → VTS Requester → VTS	HTTPS access for Administration GUI and REST/JSON API
5432	TCP	VTS ↔ VTS	PostgreSQL Bi-Directional Replication (BDR) port for database replication across nodes

• OUTGOING PORTS TO CONFIGURE FOR VTS

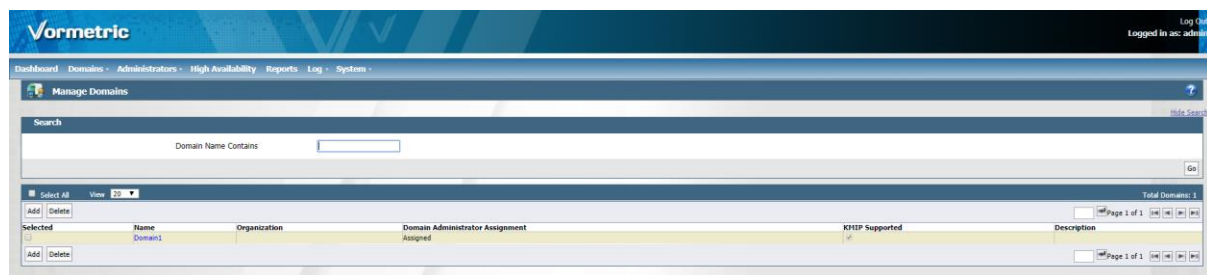
Port	Protocol	Communication Direction	Purpose
User-defined	TCP	VTS → Log Server	Remote logging
123	UDP	VTS ↔ NTP Server	Optional network time synchronization
389	TCP	VTS → LDAP Server	LDAP connection
636	TCP	VTS → LDAPS Server	Optional LDAPS (LDAP over SSL)

			connection
7024	TCP	VTS → DSM	Request policy updates
8080	TCP	VTS → DSM	Default TCP/IP port for HTTP that is used once to perform the initial certificate exchange between a VTS host and DSM.
8443	TCP	VTS → DSM	TCP/IP port through which the VTS communicates with the DSM to exchange configuration. The VTS establishes a secure connection to the DSM via certificate exchange using this port.
8444	TCP	VTS → DSM	Upload VTS log messages to DSM
8446	TCP	VTS → DSM	Configuration exchange (policy/key pull) using Elliptic Curve Cryptography (Suite B)
8447	TCP	VTS → DSM	VTS uploads log messages to DSM using Elliptic Curve Cryptography

CONFIGURE THE DSM TO ENABLE THE VTS INSTALLATION

Add a Domain

- a. If we are already logged into the Management Console, log out and log in again as the DSM System Administrator admin. Otherwise, just log on as admin.
- b. Click Domains > Manage Domains to bring up the Manage Domains window.
- c. If we are in a domain click Exit Domain to exit the domain and then click Manage Domains.

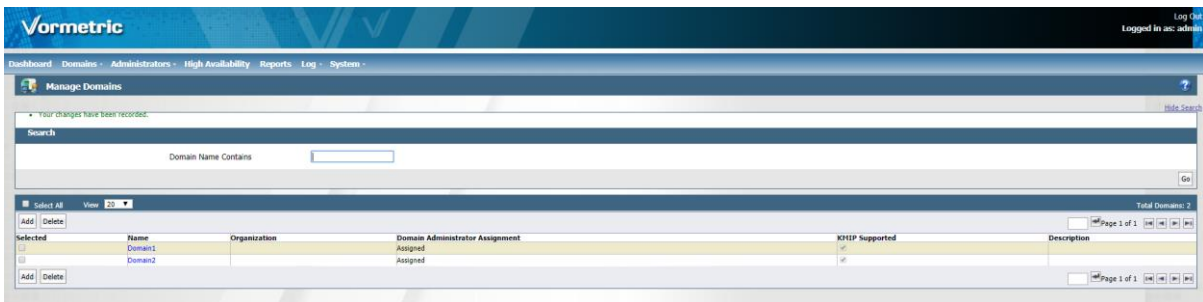


- d. Click Add. The Add Domain window opens.

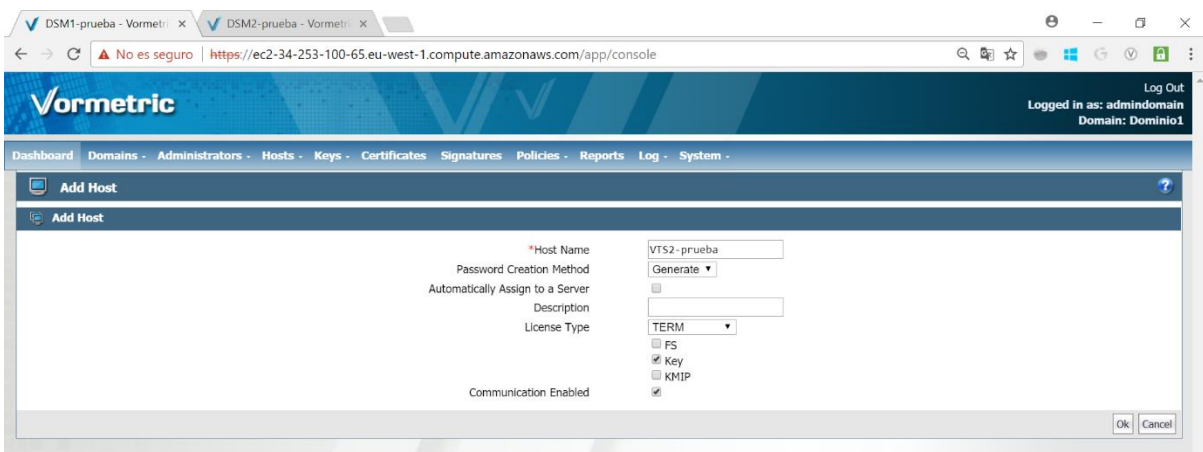
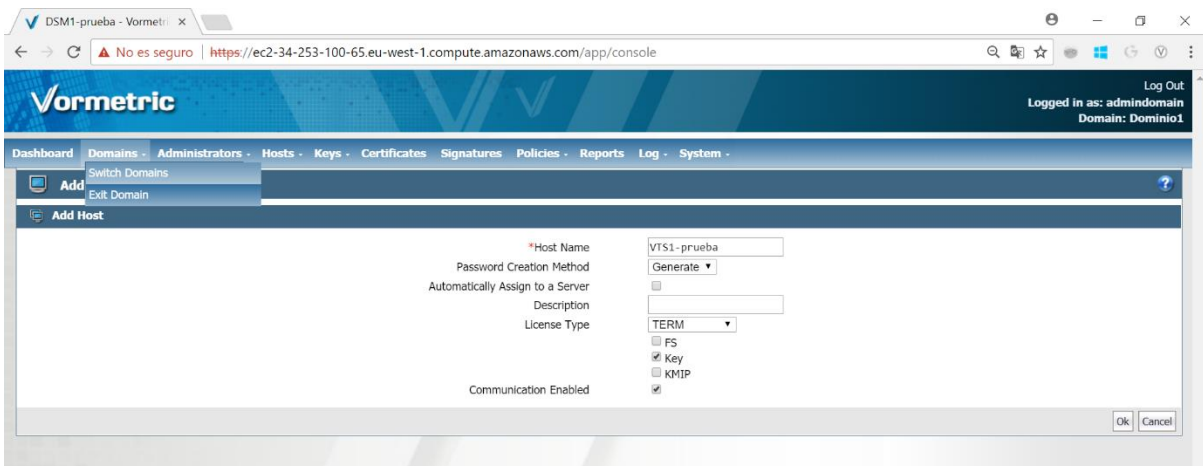


- e. Under the General tab, we can provide a name for the domain and some other optional information:
 - I. Name: Domain2.
 - II. Organization: (Optional)
 - III. Description: (Optional)
 - IV. Help Desk Information: (Optional)

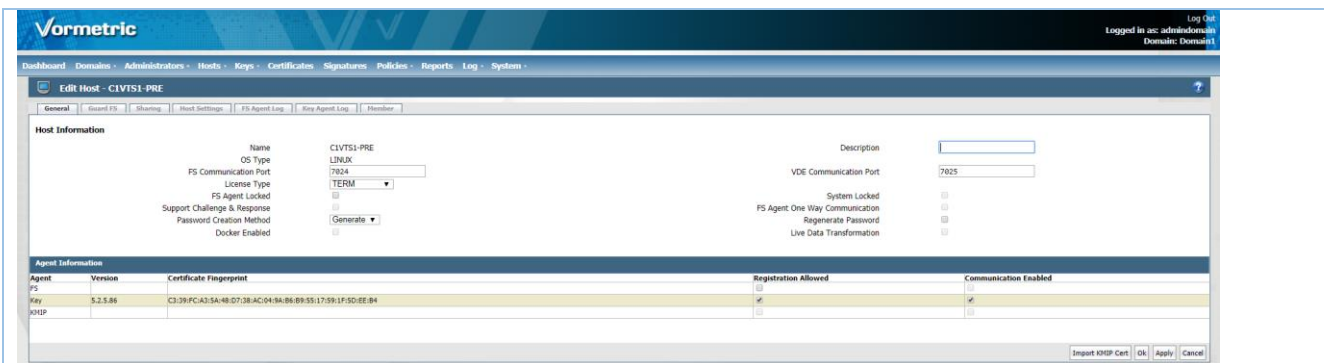
- f. Click Apply to save the domain information.
- g. Click the Assign Admin tab to assign an administrator.



3) Add the VTS hostnames to DSM database. On the DSM Management Console click Hosts > Add. The Agent type is Key; License type is set as per our DSM licensing agreement; all other parameters can be left as is. Click Ok.



Click on the host name to go to the Edit Host page. Under Key Agent column, check the Communication Enabled and Registration Allowed checkboxes, and click Ok.



CONFIGURING THE VTS

The following subsections describe how VTS was configured.

SET THE VTS NETWORK SETTINGS

In this section we configure the Token Server network settings:

- Set the IP address of the Token Server virtual machine.
- Assign the default gateway.
- Assign the DNS server

To do it, next steps were followed:

1. Using the tokenization CLI on the VTS, navigate to the *network* commands menu.

```
0000:vormetric$ network
```

2. Set the IP address for the Token Server virtual machine. There are two ethernet cards, eth0 and eth1. Assign an IP address to eth0 with the following command:

```
0001:network$ ip address set <Token Server IP address>/<address prefix length> dev eth0
```

Verify the interface settings. Type:

```
0002:network$ ip address show
```

3. Add the IP address for the default gateway:

```
0003:network$ ip route add default via <IP address for the default gateway, ex: 10.3.0.1> dev eth0
```

Verify the route settings. Type:

```
0004:network$ ip route show
```

Main routing table

```
10.3.0.0/16 dev eth0 proto kernel scope link src 10.3.20.11
```

```
10.4.0.0/16 dev eth1 proto kernel scope link src 10.4.99.122
```

```
169.254.0.0/16 dev eth0 scope link metric 1002
```

```
169.254.0.0/16 dev eth1 scope link metric 1003
```

```
default via 10.3.0.1 dev eth0
```

```
ip route show SUCCESS
```

4. If we are using DNS, set the primary DNS server for the Token Server. Type:

```
0005:network$ dns dns1 <IP address for dns1>
```

5. If we have a second or third DNS server, set them for the Token Server. Type

```
0006:network$ dns dns2 <IP address for dns2>
```

6. If we want to set the search domain, type

```
0007:network$ dns search <search_domain>
```

7. Show the DNS settings. Type

```
0008:network$ dns show
search i.vormetric.com
nameserver 10.3.110.104
nameserver 10.0.5.248
DNS show SUCCESS
```

8. Return to the main menu. Type

```
0009:network$ up
0010:vormetric$
```

SET THE VTS HOSTNAME

Even though we have set a Token Server host name when we created the virtual machine, we must also set a host name in the Vormetric system using the tokenization CLI.

1. In the Token Server CLI, navigate to the *system commands* menu. Type:

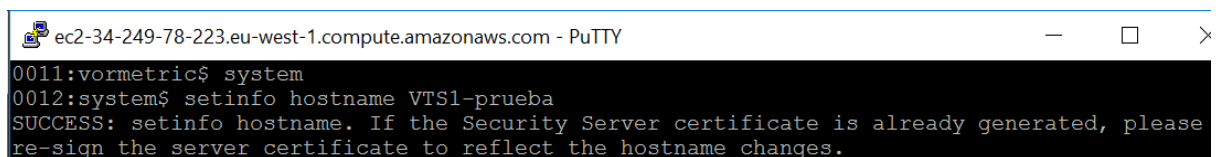
```
0010:vormetric$ system
```

2. Set the VTS hostname with the `setinfo` command:

```
0011:system$ setinfo hostname <Fully Qualified Host Name>
```

```
SUCCESS: setinfo hostname. If the Security Server certificate is already generated, please re-sign the server certificate to reflect hostname changes.
```

NOTE: If we change the VTS hostname, either generate a new self-signed server certificate or import a server certificate (see below).



```
ec2-34-249-78-223.eu-west-1.compute.amazonaws.com - PuTTY
0011:vormetric$ system
0012:system$ setinfo hostname VTS1-prueba
SUCCESS: setinfo hostname. If the Security Server certificate is already generated, please re-sign the server certificate to reflect the hostname changes.
```

IMPORT A SERVER CERTIFICATE

By default, the system automatically uses a self-signed certificate for https. We must regenerate the self-signed certificate (for the test/demo installation) or install a 3rd party certificate from a CA (for production) so others know we are verified.

1. To regenerate the self-signed certificate run:

0012:security\$ server-cert creatcertss

Enter answers to the informational questions and restart the web server when asked.

```
ec2-34-249-78-223.eu-west-1.compute.amazonaws.com - PuTTY
0014:vormetric$ security
0015:security$ server-cert creatcertss
Continue to create self-signed certificate? (yes|no)[no]:yes
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ES
State or Province Name (full name) []:Spain
Locality Name (eg, city) [Default City]:Madrid
Organization Name (eg, company) [Default Company Ltd]:Accenture
Organizational Unit Name (eg, section) []:Accenture
Common Name (eg, your name or your server's hostname) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Signature ok
subject=/C=ES/ST=Spain/L=Madrid/O=Accenture/OU=Accenture
Getting Private key
Successfully created self-signed certificate for token server.
SSL Certificate on VTS updated successfully.
Do you want to restart tokenization server (yes|no)[no]:yes
Stopping monit: [ OK ]
Stopping
Stopping nginx: [ OK ]
Stopping uwsgi
Stopping vaed [ OK ]

VAED is stopped.
Starting VTS
Starting vaed [ OK ]

VAED is running.
Using PKCS11 library at path: /opt/vormetric/DataSecurityExpert/agent/pkcs11/lib/libvorpksa
```

2. (Recommended.) Import an authenticated 3rd-party CA certificate to the Token Server. Use an SSH terminal like xterm or PuTTY to do this.

- a. On the tokenization CLI, go the *Security* submenu and enter `server-cert generatecsr` to generate a certificate request:

0013:security\$ server-cert generatecsr

- b. Follow system prompts. A certificate request displays on the secure shell:

```
----- BEGIN CERTIFICATE REQUEST -----
. . .
----- END CERTIFICATE REQUEST -----
```

- c. Copy and paste the certificate request including the "REQUEST" lines onto a third-party certificate request form, for example GoDaddy, Thwart, or Verisign.

- d. After getting the certificate, run `security importcert` on the CLI command line:

0014:security\$ server importcert

We will be prompted to continue. Type `yes`.

- e. Copy and paste the entire certificate including the CERTIFICATE lines shown below.

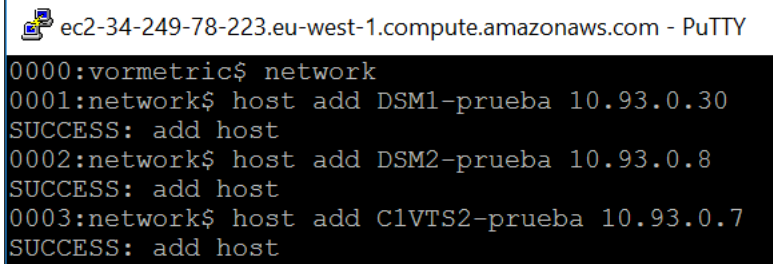
```
----- BEGIN CERTIFICATE REQUEST -----
. . .
----- END CERTIFICATE REQUEST -----
```

- f. Type "Ctrl-d" to end the input.
- g. The Token Server will import the certificate and try to verify that the imported certificate matches the private key generated at the time as the certificate was generated.
- h. The system will prompt to restart the web server. Type *yes*. The web server component of the Token Server will be restarted, and the new certificate will take effect. The system is set up using the third-party server certificate for SSL connections.

REGISTERING VTS WITH DSM

- 1) If there is no DNS, we have to add the hostname of our DSM into `/etc/hosts`. Going to the `network` submenu in the Admin CLI and enter:

```
host add <dsm hostname> <dsm IP Address>
```



```
ec2-34-249-78-223.eu-west-1.compute.amazonaws.com - PuTTY
0000:vormetric$ network
0001:network$ host add DSM1-prueba 10.93.0.30
SUCCESS: add host
0002:network$ host add DSM2-prueba 10.93.0.8
SUCCESS: add host
0003:network$ host add C1VTS2-prueba 10.93.0.7
SUCCESS: add host
```

- 2) Ask the DSM Administrator to add the Vormetric Token Server hostname to DSM database.

On the DSM Management Console, the DSM Administrator must click Hosts > Add. The *Agent type* is Key; *License type* is set as per our DSM licensing agreement; all other parameters can be left as is. Click Ok. After this, the Administrator must click on the host name to go to the *Edit Host* page. Under *Key Agent* column, check the Communication Enabled and Registration Allowed checkboxes, and click Ok.

- 3) Register the Token Server to DSM. Go to 'vae' submenu of VTS CLI and run:

```
0012:network$ up
```

```
0013:vormetric$ vae
```

```
0014:vae$ register <dsm hostname>
```



```

ec2-34-249-78-223.eu-west-1.compute.amazonaws.com - PuTTY
0020:vormetric$ vae
0021:vae$ register DSM1-prueba

Welcome to the Vormetric Key Agent
Registration Program.

Agent Type: Vormetric Key Agent
Agent Version: 5.2.5.86

Generating EC certificate signing request for the pkcs11...done.
Signing certificate...done.

The following is the fingerprint of the EC CA certificate.
Please verify that it matches the fingerprint shown on the Dashboard
page of the Management Console. If they do not match, it can indicate an
unsuccessful setup or an attack.

39:52:08:67:3F:3D:12:88:E8:C0:89:7B:0A:63:AA:B5:2A:81:DB:23

The following is the fingerprint for this agent on this host.
Please verify that it matches the fingerprint shown for this host on the
Edit Host window of the Management Console.

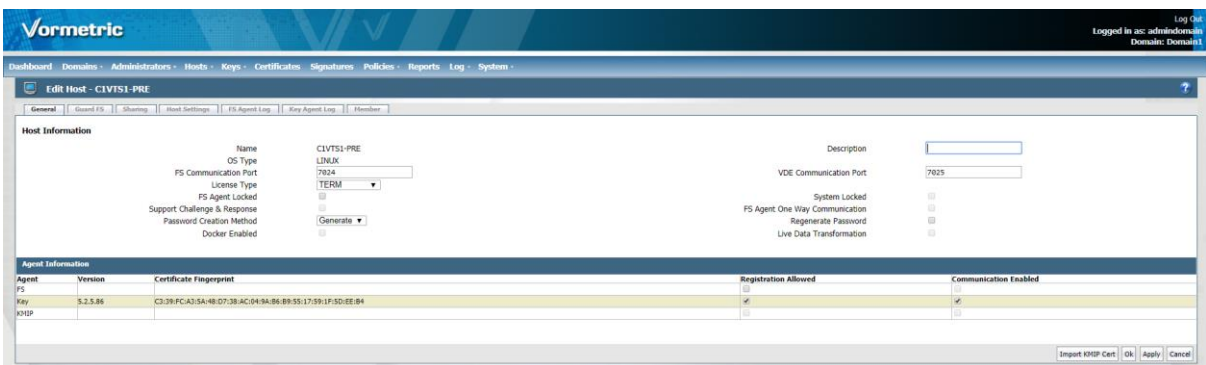
66:B2:56:4C:88:8F:ED:FD:3D:B0:6A:CB:8B:E6:42:1F:F3:B2:26:0C

Successfully registered the Vormetric Key Agent with the primary
Vormetric Data Security Server on DSM1-prueba.

Register VAE to DSM Server SUCCESS.
Restarting the web server...
nginx: [warn] "ssl_stapling" ignored, no OCSP responder URL in the certificate
Using PKCS11 library at path: /opt/vormetric/DataSecurityExpert/agent/pkcs11/lib/libvorpks
11.so
Using PKCS11 library at path: /opt/vormetric/DataSecurityExpert/agent/pkcs11/lib/libvorpks
11.so
Stopping nginx: [ OK ]
nginx: [warn] "ssl_stapling" ignored, no OCSP responder URL in the certificate
Using PKCS11 library at path: /opt/vormetric/DataSecurityExpert/agent/pkcs11/lib/libvorpks
11.so
Using PKCS11 library at path: /opt/vormetric/DataSecurityExpert/agent/pkcs11/lib/libvorpks
11.so
0022:vae$ [ OK ]

```

After register the DSM, the Certificate Fingerprint appears in the Host Information section in Management Console.



CREATE A VTS CLUSTER

HA is important, as data would be lost in case the token server fails. VTS supports up to four HA nodes. Thus, we created a multi-master VTS HA cluster before completing VTS configuration.

- 1) Create a new cluster:

```

0015:cluster$ create node_IP_address

Stopping postgresql-9.4 service: [ OK ]

Saving config files [ OK ] Initializing database ... OK

```

. . .

You have installed Django's auth system, and don't have any superusers defined. Would you like to create one now? (yes/no): yes

Username (leave blank to use 'root'): vtsroot (*login name for VTS GUI*)

Email address: Password: (*password for VTS GUI*)

Password (again): (*password for VTS GUI*)

Superuser created successfully. Pre-populating vts database...

. . .

Create cluster SUCCESS.

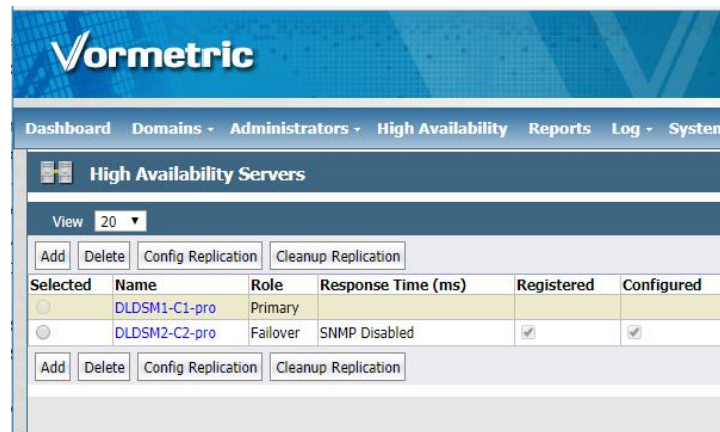
The Username and Password are the credentials used to access the VTS GUI on any machine in the cluster.

- 2) For a second or a subsequent node, to join this node to the cluster:

```
0015:cluster$ join <node_IP_address> <IP_address_of_first_node_in_cluster>
```

- 3) Finally, we can Test the node by accessing the VTS GUI. Use the user name and password we defined earlier with the create command.

https://node_IP_address/admin



Jose Luis Naranjo Rico

TFM: Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (**MISTIC**)

**Holistic business approach
for the protection of sensitive data**

"Study of legal requirements and regulatory compliance at international level to define and implement data protection measures using encryption techniques"

Diciembre 2018