[Ascend Encryption Process v1.20 - CS Ascend - Confluence Global (experian.com)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20" \l "AscendEncryptionProcessv1.20-_Toc42639413)

Experian Ascend Security for Clouds provides technology solutions for all of CIS encryption and key management, supporting our business to deliver for internal and external customers, applications and cloud systems. Use this page to navigate content and information on the platforms and services we offer.

[Skip to end of metadata](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#page-metadata-end)

* Created by [Muppavarapu, Deepika](https://pages.experian.com/display/~c59653a), last modified on [Jun 10, 2020](https://pages.experian.com/pages/diffpagesbyversion.action?pageId=713737945&selectedPageVersions=11&selectedPageVersions=12)

[Go to start of metadata](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#page-metadata-start)

**Ascend**  
**Encryption Process**  
**Contents**  
[1. Overview](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639410)  
[2. Ascend Encryption Types](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639411)  
[2.1 Data in Transit](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639412)  
[2.1.1 PGP Encryption](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639413)  
[*2.1.2* Hybrid Encryption (combination of Asymmetric and Symmetric key)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639414)  
[2.1.3 Payload Encryption (combination of Asymmetric and Symmetric key)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639415)  
[2.2 Data at Rest](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639416)  
[2.3 Product use cases and policies](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639417)  
[2.3.1 Data transfer and disk-level encryption (PII data)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639418)  
[2.3.2 Field-level encryption (PII data using single key)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639419)  
[2.3.3 Field-level encryption (PII data using multiple keys)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639420)  
[2.3.4 Database encryption (PII data using TDE)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639421)  
[3. Ascend Key Management Process](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639422)  
[3.1 Key Management Service](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639423)  
[3.1.1 Experian Gemalto SafeNet KeySecure](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639424)  
[3.1.2 AWS Key Management Service](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639425)  
[3.1.3 AWS CloudHSM (Future plan)](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639426)  
[3.2 Connectors and API](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639427)  
[3.2.1 Experian Gemalto SafeNet KeySecure Connectors](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639428)  
[3.2.2 AWS Key Management Service API](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639429)  
[4. Appendix](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639430)  
[4.1 Ascend Encryption Infrastructure](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639431)  
[4.2 Ascend Key Management Hybrid Architecture](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639432)  
[5. Experian references:](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20#AscendEncryptionProcessv1.20-_Toc42639433)

**Intended Audience and Personas\*** *(\*create link to personas definition page)*

* Ascend Infrastructure Team
* Ascend Development Team (Developer, Admin)
* Ascend SRE Team (Engineer, Admin)
* Experian Information Security Team (Analyst, Analyst- Elevated)
* Experian Global Data Protection Team
* Experian Corporate Internal Audit, Legal, Compliance, Privacy Teams (Auditor, Security Analyst)
* Data/Datalake/Data Warehouse Architect (Data Custodian)

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| January 6, 2020 | 1.0 | Initial Version | Sai Tallapaka |
| April 1, 2020 | 1.1 | Updated | Sai Tallapaka |
| June 1, 2020 | 1.2 | Updated | Sai Tallapaka |
| June 7, 2021 | 1.3 | Updated | Sai Tallapaka, Satchit Dokras |

Overview

This document defines the Ascend encryption and associated key management policies and practices. The purpose of this document is to ensure that data is secured while in transit and at rest.  
Ascend policies on encryption and key management ensures that key lifecycle and the levels of encryption are deployed in alignment conformance with Experian security principles and policies and adhere to regulatory and industry conformance standards.

The policies and procedures stated in this document apply to internal and external handling of data within Ascend products and services. This also applies within Experian and 3rd parties including clients and partners who provide data to and access data within the Ascend Technology Platform. The procedures are designed to be prescriptive yet simple and clear to deploy in order to gain consistency for the Ascend use cases and workflows. In this way, they also offer transparency on how data security has been designed into our Ascend architecture.

Additionally, as our Ascend platform is increasingly a cloud-based service, this document addresses data security aspects necessitated by the use of public clouds (AWS mainly, but also Azure, GCP and OCI). Finally, this document now embodies the Experian CIS 3-I Cloud Cybersec Framework *(create link to page)*, where the NIST cybersecurity components are incorporated in considering the security functions of Govern, Identify, Protect, Detect, Respond and Recover. It therefore supports the objective of continuously increasing the robustness of Ascend’s data protection capabilities.

**This is a living document and will be kept up to date as Ascend policies and procedures are modified and enhanced**

Encryption and Key Management Policy

The encryption policies focus on the protection of data in its lifecycle at and with Experience and its customer/ third party custodians. Encryption types (symmetric, asymmetric), levels (strength, generation) and protocols (private, public, nation state) are selected based on the category of data (messaging, controls, channels, payload, applications, etc), and its state (in transit, at rest and in use).

The policy and its structure is below, followed by details for each type to encryption and key management

1. All(?) data in transit, at rest and in use.
   1. Data in Transit
      1. Channel level encryption
      2. Content level encryption
      3. API-based payload encryption
   2. Data at Rest.
      1. Disk level encryption:
         1. Full disk encryption
         2. Object level encryption
            1. Database
            2. File share
            3. Storage elements
         3. File level encryption
         4. Database level encryption
         5. Field/column level encryption – [Sample AWS Link](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html)
   3. Data in Use
      1. In application
      2. In memory computing
      3. In isolated cloud environments – Nitro Enclave
2. Keys used for encryption of data
   1. Key Management
   2. Keys lifecycle management
3. All data protection policies
   1. Clear Responsible, Accountable, Consulted, Informed (RACI) models
   2. Policy orchestration
   3. Periodic reviews
   4. Detection and monitoring tools
   5. Procedures
4. Consider client data, distributed data and AI ML nuances (to be developed further….)!

# Policies

1. All data in transit, at rest and in use must be encrypted.

The encryption protocol used must be at the highest level sustainable by industry and customer capability, and periodically upgraded. The authorization to use encryption must be independent from how access to the underlying data is controlled.

Encryption enveloping, where encryption keys are themselves encrypted are to be a standardized procedure.

* 1. Data in Transit: The considerations include channel level and content level encryption.
     1. Channel level encryption: This addresses network security for data in transit.
        1. All network transport must adhere to a minimum of TLS 1.2 protocol between Experian, Experian entities and its external stakeholders.
        2. The internal server-side may have earlier TLS 1.1 version as well as TLS 1.2.
        3. Future Roadmap: Where possible (without loss if any existing functionality or applications capability), the migration and adoption of TLS 1.3 should be deployed, and mutual TLS/mTLS with hybrid TLS 1.2/1.3 is permitted. There is no timeline defined for this yet.
     2. Content level encryption: This addresses file and payload transfers which will also be within the encrypted channel.
        1. Content will be fully encrypted during transfers using PGP Encryption. Hybrid encryption using symmetric and asymmetric keys will be considered as a future roadmap capability.
     3. API-based payload encryption: This addresses data exchanges through application and system APIs. The payload to be encrypted could be a record made up of multiple fields or select sensitive fields within the payload.
        1. All payload transfers through APIs will have end to end encryption based on the JavaScript Object Signing and Encryption (JOSE) framework rendered with
     + JSON Web Signature (JWS)
     + JSON Web Encryption (JWE) - RFC7516
     + JSON Web Key (JWK) - RFC7517
     + JSON Web Algorithms (JWA) - RFC7518
     + JSON Web Token (JWT) - RFC7519
     + JSON Web Key Thumbprint - RFC7638
     + JWS Unencoded Payload Option - RFC7797
     + CFRG Elliptic Curve ECDH and Signatures - RFC8037
     + secp256k1 EC Key curve support
  2. Data at Rest: The considerations include disk, object, file, database and field/column level encryptions.
     1. Disk level encryption:
        1. Full disk encryption by default is mandatory. This may be configured using vendor or cloud service provider capabilities or augmented with Experian encryption.
        2. Object level encryption: These may be configured using vendor or cloud service provider capabilities or augmented with Experian encryption.
           1. Database (e.g. Oracle, DB2, MS SQL, MySQL, NoSQL, SycllaDB, RocksDB, Aurora, Dynamo, Redis, RedShift, RDS, etc.)
           2. File share (e.g. SAN, NAS, FSx, etc.)
           3. Storage elements (e.g. S3, EBS, EMRFS, etc.)
        3. File level encryption: Encryption using PGP is mandatory
        4. Database level encryption: Standard Transparent Data Encryption as offered by the database vendors is mandatory with AES 256. Else, Experian managed encryption at AES256 is to be deployed.
        5. Field/column level encryption: A single key encryption schema will be adopted using AES256. Multi-level key will be validated and standardized in roadmap timeline.
  3. Data in Use: This addresses the protection of data that is being processed for any application or functional requirements with a necessary unencrypted state. It covers three states- in application, in memory and in isolated compute environments in clouds (eg AWS Nitro Enclaves). Although these are roadmap
     1. In application: Before infrastructure is offered to applications, it must be ensured that application level encryption is designed in and data is protected at point of creation. This may include encryption using Experian services, tokenizing (PKCS#11), masking and access control and logging capabilities. Data abstraction techniques will be deployed to ensure protection at a common point and the management of distributed data and its computing in multiple environments.
     2. In memory computing: It is required to ensure infrastructure deployments where trusted computing environments follow industry validated standards such as TCB (Trusted Computing Base) and Intel’s TXT (Trusted Execution Technology). Here, encrypted data hand off to OS and processors as cleartext follows trusted protocols.
     3. In isolated cloud environments: As native applications development in cloud becomes mainstream for Experian, and more applications are migrated into VPCs, it is important to deploy cloud native enclaves established and controlled by Experian. This standard will be established for a roadmap.

1. Keys used for encryption of data within the Ascend platform by default will be generated by following the process and procedures of Experian's Key Management infrastructure. If regional or other technical environment restrictions do not permit this, the keys used will be from a subset of approved encryption schemas cataloged by Experian Ascend.
   1. The authorization to use encryption must be independent from how access to the underlying data is controlled. Cloud key management is to be deployed using Experian key management tools and access controls for key lifecycle and operations management. It will leverage cloud service provider hardware security modules or HSMs, key logs and analysis native tools where possible.
   2. Key Management will balance the two core objectives- key risk management (maximum protection and privacy, consistency, integrity, resilience), and business enablement (minimized operational latency and cost, with workflow transparency, user trust)
   3. Keys will be managed for their lifecycles (design, build, run, govern) with clear procedures and responsibilities identified for selection and establishment of keys, custodians, protection, rotations and end of life objectives.
2. All data protection policies and technology roadmaps will be generated, authorized, and maintained by the Ascend security organization. They will be ratified by CSO, legal and compliance offices with an Ascend VP level sign-off attesting they meet Experience policies and standards and embody all elements of the CIS 3I Cybersecurity Framework.
   1. Clear Responsible, Accountable, Consulted, Informed (RACI) models for personas and roles will be developed and maintained.
   2. Policy orchestration considerations for automated procedures and systems must be designed in with trustworthy change management.
   3. Periodic reviews of encryption methods and key lifecycle management must be made at pre-determined governance cadence, as required by special customer requirements, as well as those triggered by security events
   4. Detection and monitoring tools that automate encryption policy enforcement must be incorporated into the encryption and key lifecycle management. These include cleartext detection in applications, infrastructure, data in transit, at rest and in use and in cloud and enclave environments.
   5. Procedures must include respond and recover methodologies that are within risk management and SLA guidelines with clear RACI models that include cloud and third party vendors, customers and extended Experian environments as relevant.

##### *Consider encryption call outs for client data enclaves/sandboxes, distributed data policy persistence and AI ML privacy intent for this section!*

Ascend Personas for Encryption and Key Lifecycle Management

For Ascend, the number of personas are several based on organizational structure, but encryption applies to only those few who are owners and users. Encryption roles are even more limited to very restrictive roles to gain maximum control on data security. This section defines the personas, their encryption use cases, and specific encryption roles assigned to them.

…

Ascend personas are defined below specifically pertaining to the infrastructure operations and usage of cloud services; additional sub-personas are also identified as those that adopt personas for a periodic, just-in-time or on-going purpose. Finally, persona details for encryption and key lifecycle management are also described here.

1. Persona: Developer
   1. Developer
   2. DevSecOps Engineer
   3. Database Administrator
   4. Architect
2. [Persona: Site Reliability Engineer](https://www.ibm.com/docs/en/cloud-paks/cp-management/1.3.0?topic=about-personas-use-cases" \l "SRE_persona)
   1. Cloud Administrator
   2. Security Engineer
   3. Compliance Engineer
3. Persona: Data Security Officer
   1. Security Architect
   2. Security Lead
   3. Security Analyst
4. Persona: Data Analyst
   1. Data analyst
   2. AI-ML data scientist, modeler
   3. AI-ML data engineer
5. Persona: Product Support Lead
   1. Product manager
   2. Product technical program manager
6. Persona: External Users of Ascend sandbox (PaaS) and data services (DataaaS linking Experian and client data)
   1. Client/ Third Party DevOps
   2. Admin for data federation
   3. Services and systems Engineering
   4. Product control planes Engineering
   5. Partner developer account and SRE
7. Persona: Client Support Lead
   1. I&D implementation and delivery, data onboarding engineer
      1. Analyst (no PII access)
      2. Client Support
   2. Client Success data analysts/maintain
   3. Analyst-X (PII/PCI access)
8. Persona: Auditor/Analyst
   1. Auditor
   2. Financial Analyst
   3. Risk Manager
   4. Compliance manager

##### To be edited-(Rajit/Imtiaz../Sai)🡪

Persona: Developer …

Description: As an Ascend developer, you architect, build (provision) and govern the cloud infrastructure with the associated workflows and workloads for both internal product and functional applications, and external customer and third-party sandboxed environments and Experian marketplaces.

Therefore, as a developer, you adopt one or many sub-personas such as:

* **Core developer**, builds and ensures functionality of Ascend Platform and its services

Architect, where you design infrastructure, databases, security and governance.

* **DevSecOps Engineer**, where you can discover the traditional and modern services of the application, deploy applications by using the DevOps pipeline to drive a consistent process for delivering changes, and ensure that applications meet their goals of stability and security.
* **Database Administrator** where you architect and manage databases and are a custodian of data sets and their lifecycle.

Privileges and acceptable roles: You have access at baseline privileges. You use Terraform for provisioning and perform as an infrastructure change engineering expert. You can also escalate to Developer-X status for a short term with additional privileges for testing. If accessing Personally Identifiable Information (PII), you will be able to so though only through permissible roles.

Encryption and key management Responsibilities: In terms of data protection, it is your responsibility to pay unconditional attention to the purposes of cloud infrastructure usage for data sets tagged as PII. In doing so, all aspects of encryption and key lifecycle management will be deployed per the policies and procedures marked in this document and maintained at current standard. Finally, you also design in and support ongoing test, audit, monitoring, reporting, response and recovery as governance functions for data protection.

### Edit tasks with relevant Ascend workflow. Add a column to reference where these tasks impact security and encryption

| **Tasks** | **References** |
| --- | --- |
| View applications across clusters on one console. |  |
| Create or provision Kubernetes resources for a project. |  |
| Use open-source technology and frameworks to package and deploy applications into clusters. |  |
| Understand how resources are used by Kubernetes deployments over time. |  |
| Monitor application performance, such as availability and response time. |  |
| Check policy violations and vulnerabilities and get clear remediation suggestions. |  |

| **Tasks** | **References** |
| --- | --- |
| Manage applications and services across multiple cloud environments on one console. |  |
| Manage multiple clusters across multiple cloud environments on one console. |  |
| Automate provisioning of infrastructure and applications across multiple cloud environments with optional workflow orchestration. |  |
| Manage authentication and authorization across multiple cloud environments. |  |
| Manage logging, keys, and other Kubernetes configurations. |  |
| Flexible deployment for application updates. |  |

##### To be edited-(Sri/Sai)🡪

Persona: Site Reliability Engineer …

Description: As an Ascend SRE, you maintain application availability, reliability, and performance from the product user's perspective in the cloud infrastructure; create runbooks to automate responses to incidents, and apply critical updates to production environments without impacting users; respond to and recover from various outages in underlying IaaS or CaaS services and prevent security breaches; and provide developers access to relevant logs, events, and performance metrics necessary to troubleshoot and quickly resolve problems.

You also engage with internal and external stakeholder such as developers, product owners, customers and third parties. Therefore, you adopt sub-personas of:

* **Reliability Engineer**
* **Cloud Administrator**

In your reliability engineering and administrator work, you manage to the CI/CD pipeline, leverage automation in operations, security and customer success, and ensure the consistent performance and continuous improvements of the cloud environment. Therefore, you perform as an infrastructure provisioner, change engineering expert, incident researcher, remediation engineer and governance custodian for the site operations.

* **Security Engineer and**
* **Compliance Engineer**.

As a Security and Compliance Engineer, you use Ascend security policies to create policies to configure cloud workloads, assign policies to clusters, view policy compliance status, look for security incidents and check code vulnerabilities. You can ensure that clusters are configured according to corporate security policies and procedures, and applications are on boarded to clouds securely and in compliance.

Privileges and acceptable roles: You have access at baseline privileges as a cloud administrator and get escalated privileges only through using Terraform infrastructure as a code. You can also escalate to Developer-X status for a short term with additional privileges for testing. If accessing Personally Identifiable Information (PII) or making organization level changes, you will be able to so though only through permissible super admin role. However, only a strictly limited number shall have super admin status on a full-time or just-in-time basis.

Encryption and key management Responsibilities: In terms of data protection, it is your responsibility to pay unconditional attention to the purposes of cloud infrastructure usage for data sets tagged as PII. In doing so, you will ensure the ongoing maintenance and performance of all aspects of encryption and key lifecycle management that have been per the policies and procedures marked in this document. You will rotate, reversion and maintained to make current with upgraded Experian and Ascend standards. Finally, you also offer engineering support for ongoing test, audit, monitoring, reporting, response and recovery as governance functions for data protection.

As a Site Reliability Engineer (SRE), you can complete the following tasks:

### Edit tasks with relevant Ascend workflow. Add a column to reference where these tasks impact security and encryption

| **Tasks** | **References** |
| --- | --- |
| Receive notification reports for cluster and application incidents. |  |
| Check the application performance by using synthetic tests.​ |  |
| Check the resource usage issues. |  |
| Check whether there are pods that are not running and restart these pods. |  |
| Document the runbook for automatic resolution of such issues in the future. |  |
| Manage all security requirements and view policy compliance and vulnerability status across multiple cloud environments on one console. |  |
| Set up compliance policies to guard against exposures, internal protocols, and adhere to government regulations​.​ |  |
| Set up the Vulnerability Advisor to scan images. ​ |  |

##### To be edited-(Sri/Sai)🡪

Persona: Data Security Officer …

Description: As a data security officer for Ascend, you create policies and procedures, architect and govern the end-to-end security perimeter for Ascend, cloud services, third party and customer services. You classify data as PII, identify security threats to enable policies and procedures, map data set types and standardize tags for them, and use the full range of obfuscation, tokenization and encryption to protect PII data. You incorporate technology advancements enabling security automation and compliance. You adopt the personas of:

* **Security Architect**
* **Security Lead**
* **Security Analyst**.

As a **Data Security Officer** for cloud infrastructures, you also use Ascend security policies to create policies to configure cloud workloads, assign policies to clusters, view policy compliance status, look for security incidents and check code vulnerabilities. You can ensure that clusters are configured according to corporate security policies and procedures, and applications are on boarded to clouds securely and in compliance. You identify vulnerabilities and monitor and remediate for them through DevSecOps and SRE.

You closely align with the Experian CSO/CTO’s roadmaps and security investments, EITS architectures, and GSO policies and procedures. In effect, you serve as the custodian of data security for Ascend.

Privileges and acceptable roles: As a data security officer, you have access at baseline privileges as a cloud administrator and get escalated privileges through using Terraform infrastructure as a code. You can also escalate to Developer-X status for a short term with additional privileges for testing. If accessing Personally Identifiable Information (PII) or making organization level changes, you will be able to so though only through permissible super admin role. However, only a strictly limited number shall have super admin status on a full-time or just-in-time basis.

Encryption and key management Responsibilities: You define the encryption and key management protocols for every type of data encryption, manage the policies on it, architect it within Ascend and customer cloud enclaves, set standards for their lifecycle management, and identify tools and services that support the encryption and key management operations across the extended Experian perimeter. You monitor the encryption logs for aberrations, mis-configurations, remediations and breach management. You will rotate, reversion and maintained to make current with upgraded Experian and Ascend standards. You also offer engineering support for ongoing test, audit, monitoring, reporting, response and recovery as governance functions for data protection. Finally, you support data security compliance and cost governance to the Experian standards.

As an Ascend Data Security Officer, you can complete the following tasks:

| **Tasks** | **References** |
| --- | --- |
| Receive notification reports for cluster and application incidents. |  |
| Check the application performance by using synthetic tests.​ |  |
| Check the resource usage issues. |  |
| Check whether there are pods that are not running and restart these pods. |  |
| Document the runbook for automatic resolution of such issues in the future. |  |
| Manage all security requirements and view policy compliance and vulnerability status across multiple cloud environments on one console. |  |
| Set up compliance policies to guard against exposures, internal protocols, and adhere to government regulations​.​ |  |
| Set up the Vulnerability Advisor to scan images. ​ |  |

##### To be edited-(Rajit/Sai)🡪

Persona: Data Analyst …

Description: As an Experian **Data Analyst**, you have personas that include:

* **AI-ML data scientist, (modeler)**
* **AI-ML data engineer**

You consider a variety of centralized and distributed data and avail of relevant sets in enabling new products as well as maximizing the value of existent ones. You do not have access to any clear text data that is PII or customer proprietary, and work closely with DevSecOps and SRE to make available to you secure and hygienized mirrored and production data, and cloud environments to work in.

Privileges and acceptable roles: You have access as a data analyst to non-PII data for analysis that is approved of and in keeping with Experian privacy and contractual agreements. You get escalated privileges to mirrored non-PII data, but the context of data use must conform to original and contractual intents. You do not have any privileges to customer-owned data in customer enclaves. You do get escalated Analyst-X privileges when accessing S3 and Athena storages in AWS. You also have access privilege to metadata and its tagging that aids in AI-ML and distributed data analysis, warehousing and in-memory processing, but must ensure all new tags created in clear text do not expose unacceptable privacy and security information.

Encryption and key management Responsibilities: You are the custodian of the data you use in that it must be used in the contractual and governance context of Experian. Therefore, you must encrypt and manage the privacy of the data used in an alternative context if it is deemed to be offering interpretable sensitive or PII information.

As a Data Analyst, you can complete the following tasks:

### Edit tasks with relevant Ascend workflow. Add a column to reference where these tasks impact security and encryption

| **Tasks** | **References** |
| --- | --- |
| Receive notification reports for cluster and application incidents. |  |
| Check the application performance by using synthetic tests.​ |  |
| Check the resource usage issues. |  |
| Check whether there are pods that are not running and restart these pods. |  |
| Document the runbook for automatic resolution of such issues in the future. |  |
| Manage all security requirements and view policy compliance and vulnerability status across multiple cloud environments on one console. |  |
| Set up compliance policies to guard against exposures, internal protocols, and adhere to government regulations​.​ |  |
| Set up the Vulnerability Advisor to scan images. ​ |  |
| Set up Mutation advisor to do runtime protection of the containers​. |  |
| Assign appropriate policies to various clusters per documented procedures. |  |
| Receive alerts if there are compliance failures in the clusters and assign people to remediate.​ |  |
| Integrate with other security software, such as Security Information and Event Management (SIEM) tools to get a holistic view of corporate security posture​. |  |

##### To be edited- (Swetha, Amit)🡪

Persona: Product Support Lead …

Description: As an Ascend Product Support Lead, you work principally as:

* **Product Manager** where you work mainly with external customers and ensure functional specifications, SLAs, testing cases, customer specifications and change management is supported for the product line and operationalized. You monitor costs, analyze, remediate and optimize per IT, customer business and product objectives.
* **Product Technical Program Manager** with stakeholders that are internal DevSecOps, SRE, Security, Compliance, Finance, as well as external customers and third parties through the business units as required for secure product operations.

Privileges and acceptable roles: You have access at very limited read-only and non-PII privileges. You may be offered limited, short-term privileges to perform functional and cost analysis and cloud account planning. Largely, you are the recipient of reports and views made available by SRE for your role in AWS Cloud Health or similar reporting.

Encryption and key management Responsibilities: You need to recognize PII tags in systems, workflows and workloads as you conduct your support work and ensure that you work within procedural guidelines consistent with Experian, Ascend and the clients. As you support products in development or deployment, you are expected to offer threat and vulnerability predictions to the architects and engineers from a data protection lifecycle perspective and your personal knowledge of product support functions. Where encryption or key management is seen to be compromised, you must do immediate escalation and enable SRE and security teams to respond and remediate with urgency, offering your complete observations and analysis.

As a Product Support Lead, you can complete the following tasks:

### Edit tasks with relevant Ascend workflow. Add a column to reference where these tasks impact security and encryption

| **Tasks** | **References** |
| --- | --- |
| Receive notification reports for cluster and application incidents. |  |
| Check the application performance by using synthetic tests.​ |  |
| Check the resource usage issues. |  |
| Check whether there are pods that are not running and restart these pods. |  |
| Document the runbook for automatic resolution of such issues in the future. |  |

##### To be edited-(Sri/Sai/Gopi)🡪

Persona: External Users …

Description: As Ascend external users, you are client sandbox (PaaS) users and data services (DataaaS linking Experian and client data) users. You therefore may have one or more of the following personas:

* **Client/ Third Party DevOps**
* **Admin for data federation managing own users in platform models (eg: IAM at client)**
* **Services and systems linking service account, clients**
* **Product control planes (eg: Cloudera, Databricks,..)**
* **Partner developer account and SRE**

As external users, you work closely with internal Ascend DevSecOps, SRE, Security, Compliance, Finance, as well as external customers and third parties. You represent the client business units for building secure product operations with functional specifications, SLAs, testing cases, customer specifications, change management and operations. You support cost controls, incident management, and optimize performance per IT and product line objectives.

Privileges and acceptable roles: As external users, you are given DevOps level access to the Ascend platform and data services enclaves per your roles as Client/ Third Party DevOps, Services and systems engineering, product control planes engineering, and partner developer account and SRE. You are offered limited Admin level access for data federation.

Encryption and key management Responsibilities: You are responsible for establishing and utilizing Ascend and your own encryption and key management services per the mutually contracted policies and procedures.

### Edit tasks with relevant Ascend workflow. Add a column to reference where these tasks impact security and encryption

| **Tasks** | **References** |
| --- | --- |
| Manage all security requirements and view policy compliance and vulnerability status across multiple cloud environments on one console. |  |
| Set up compliance policies to guard against exposures, internal protocols, and adhere to government regulations​.​ |  |
| Set up the Vulnerability Advisor to scan images. ​ |  |
| Set up Mutation advisor to do runtime protection of the containers​. |  |
| Assign appropriate policies to various clusters. |  |
| Receive alerts if there are compliance failures in the clusters and assign people to remediate.​ |  |
| Integrate with other security software, such as Security Information and Event Management (SIEM) tools to get a holistic view of corporate security posture​. |  |

##### To be edited-(Sri/Sai)🡪

Persona: Client Support Lead …

Description: As an Ascend Customer Support Lead, you maintain cloud infrastructure services for individual customers with confidentiality, integrity and availability, and ensure reliability and performance for customers. You engage with internal and external stakeholder such as developers, product owners, customers and third parties. Therefore, you perform as a services provisioner, change engineering analyst, incident researcher, and governance custodian for the customers’ site operations. You therefore have personas such as:

* **I&D engineer for implementation and delivery and data onboarding**
* **Analyst (no PII access)**
* **Client Support**
* **Client Success data analysts/maintain**
* **Analyst-X (PII/PCI access)**

Privileges and acceptable roles: You have access at baseline privileges as a cloud analyst for customer private clouds or enclaves. Thus, you can view monitoring and analysis tools such as ADS read only from S3, CloudHealth, CloudWatch and CloudTrails in AWS to support customer inquiries, and get short-term escalated privileges to help customers configure and troubleshoot, but not see or work on PII. If accessing Personally Identifiable Information (PII) or making organization level changes, you will be able to so though only through a permitted as Analyst-X in Ascend and with customer approval.

Encryption and key management Responsibilities: You are permitted to access encryption and key management logs, configurations and monitoring functions for the sake of analysis and customer support and training purposes only. In this sense, you will validate these for Ascend and the clients to be in conformance with Ascend and Experian policies as well as with customer requirements. All changes, further analysis and remediations will be escalated through Customer DevOps who will have further levels of authorization.

As a Client Support Lead, you can complete the following tasks:

| **Tasks** | **References** |
| --- | --- |
| Receive notification reports for cluster and application incidents. |  |
| Check the application performance by using synthetic tests.​ |  |
| Check the resource usage issues. |  |
| Check whether there are pods that are not running and restart these pods. |  |
| Document the runbook for automatic resolution of such issues in the future. |  |
| Manage all security requirements and view policy compliance and vulnerability status across multiple cloud environments on one console. |  |
| Set up compliance policies to guard against exposures, internal protocols, and adhere to government regulations​.​ |  |
| Set up the Vulnerability Advisor to scan images. ​ |  |

##### To be edited-(Sri/Sai/Gopi)🡪

Persona: Auditor/Analyst …

Description: As an Experian **Auditor or Analyst** for Ascend, you manage the integrity, risk, costs and governance of Ascend and the data it holds or communicates. You perform the functions of an internal auditor (technology, systems, processes, access controls, data encryption integrity), financial analyst (AWS billing audit), risk manager (vulnerability, impact analysis and audit) or compliance manager (controls, governance, reporting integrity and audits).

Privileges and acceptable roles: You have access at very limited read-only and non-PII privileges. You conduct almost all your work through standardized consoles that are bespoke, industry products or cloud service provider products, and this workflow and reporting is largely automated. However, for custom queries, you revert to SRE to obtain more granular information through an escalation.

Encryption and key management responsibilities: You will ensure that your workspace is restricted to the Experian secured environments where encryption and data security policies and controls are maintained. If any information is to transported to third parties, you will establish secure communications, data encryption and monitoring through SRE and use Experience standard channels.

As a Auditor/Analyst, you can complete the following tasks:

| **Tasks** | **References** |
| --- | --- |
| Manage all security requirements and view policy compliance and vulnerability status across multiple cloud environments on one console. |  |
| Set up compliance policies to guard against exposures, internal protocols, and adhere to government regulations​.​ |  |
| Set up the Vulnerability Advisor to scan images. ​ |  |
| Set up Mutation advisor to do runtime protection of the containers​. |  |
| Assign appropriate policies to various clusters. |  |
| Receive alerts if there are compliance failures in the clusters and assign people to remediate.​ |  |
| Integrate with other security software, such as Security Information and Event Management (SIEM) tools to get a holistic view of corporate security posture​. |  |

Procedures for Ascend Encryption and Key Lifecycle Management

This section defines the procedures for all aspects of encryption and key management selection, devsecops deployment, SRE operation, lifecycle maintenance, analytics, respond and recover, upgrades and compliance and governance. It covers the types of encryption for data in transit, at rest and in use based on the framework and policies defined earlier in this document.

1. All data in transit, at rest and in use.

## Procedure: Identification, selection and operationalization of encryption and key management

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Responsible Owner** | **Process Step** | **Details** | **Approval** | **Reference** |
| **1** | Data Security Officer | Plan | Identify encryption and KM types based on policy; create architectural and adoption plan and process | VP Engg; CSO | Link: Plan and program document |
| **2** | Data Security Officer, DevSecOps Lead | Test | Develop tests for tools and systems that will be used for encryption and KM and test with SRE on use cases to validate efficacy and operability; ensure key lifecycle management including resilience, BU/DR, exchange across perimeters | VP Engg; CSO | Link: Test program |
| **3** | SRE Lead | Deploy | Operationalize across Experian and third parties with SLAs in place; Train DevSecOps and SRE; organize for ongoing management and SLAs; ensure metrics and security events are reported and acted upon per procedures | VP SRE | Link: Catalog of encryption and KM services; procedures for adopting and operating these for use cases |
| **4** | SRE Lead | Maintain | Ensure all upgrades are maintained, logs monitored continuously, and reports reviewed for controls and improvements. Periodically raise awareness and training across DevSecOps and SRE, and stakeholders particularly for PII | VP SRE | Link: Governance and upgrades |
| **5** | Data Security Officer, SRE Lead | Respond, Recover | Build, train, maintain deep analytic capability to respond to events and to recover per procedures and SLAs. Patch, eradicate breaches and vulnerabilities, upgrade policies, protocols, procedures, awareness, training, reporting and analytics. | VP Engg; CSO | Link: Respond and recovery plan |
| **6** | Data Security Officer | Comply, Govern | Monitor and improve integrity, costs, business efficiency of deployments to meet with compliance and governance requirements of Experian and third parties | VP Engg; CSO | Link: Plan and program document |
|  |  |  |  |  |  |

* 1. Data in Transit
     1. Channel level encryption
     2. Content level encryption
     3. API-based payload encryption
  2. Data at Rest.
     1. Disk level encryption:
        1. Full disk encryption
        2. Object level encryption
           1. Database
           2. File share
           3. Storage elements
        3. File level encryption
        4. Database level encryption
        5. Field/column level encryption
  3. Data in Use
     1. In application
     2. In memory computing
     3. In isolated cloud environments

1. Keys used for encryption of data
   1. Key Management
   2. Keys lifecycle management

# Establishment of Encryption and Key Management Systems

The data in transit and data at rest are to be encrypted as per Experian security policies. In the event the data includes PII data, Experian hosted keys leveraging Gemalto SafeNet infrastructure is to be used for encryption.

Data in Transit

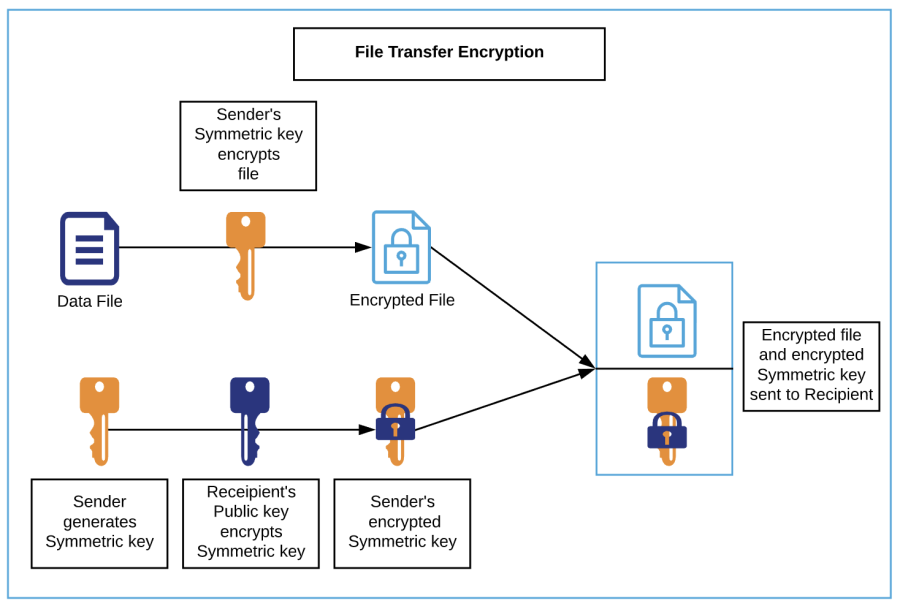
For data in transit, ascend shall leverage hybrid encryption (a combination of asymmetric key and symmetric key).  
The keys that shall be used for this purpose are

* PGP-based (for legacy support) OR
* Combination of asymmetric key and symmetric key

**PGP Encryption**

1. For data being sent as files from Ascend to Client (external 3rd party or internal systems at Experian)
   1. A secure channel, e.g. SFTP, is used for data transfer
   2. Client sends their PGP public key to the Ascend authorized representative
   3. The file(s) are encrypted with the shared Client-specific PGP public key
   4. The file(s) are either pushed to a pre-authorized Client location or pulled by the Client from an authorized Ascend location (S3 bucket) over the secure channel.
2. For data being sent as files from Client to Ascend
   1. A secure channel, e.g. SFTP, is used for data transfer
   2. Ascend generates PGP key pair and stores PGP private key in AWS Secrets Manager
   3. Ascend sends their PGP public key to the client authorized representative
   4. Client encrypts file(s) with Ascend PGP public key
   5. Client sends file(s) to the pre-authorized Ascend location in AWS.
   6. On receipt of encrypted file(s) at the authorized Ascend location, the file can be decrypted with the Ascend PGP private key (held in AWS Secrets Manager).

**Hybrid Encryption (combination of Asymmetric and Symmetric key)**



1. **Encryption flow**: For data being sent as files from Ascend to Client (external 3rd party or internal systems at Experian) OR Client to Ascend
   1. A secure channel, e.g., SFTP, is used for data transfer
   2. Recipient generates Asymmetric key pair, secures private key and sends their public key to the sender's authorized representative
   3. Sender generates a Symmetric key
   4. Sender encrypts file(s) with Symmetric key
   5. Sender encrypts Symmetric key with Recipient's public key
   6. The file(s) and the encrypted Symmetric key are sent to the Recipient to the pre-authorized location.
2. **Decryption flow**: For data received as files by Ascend from Client (external 3rd party or internal systems at Experian) OR Client from Ascend
   1. A secure channel, e.g., SFTP, is used for data transfer
   2. Recipient decrypts the encrypted Symmetric key with their private key to extract the Symmetric key
   3. Recipient decrypts file(s) with the Symmetric key.

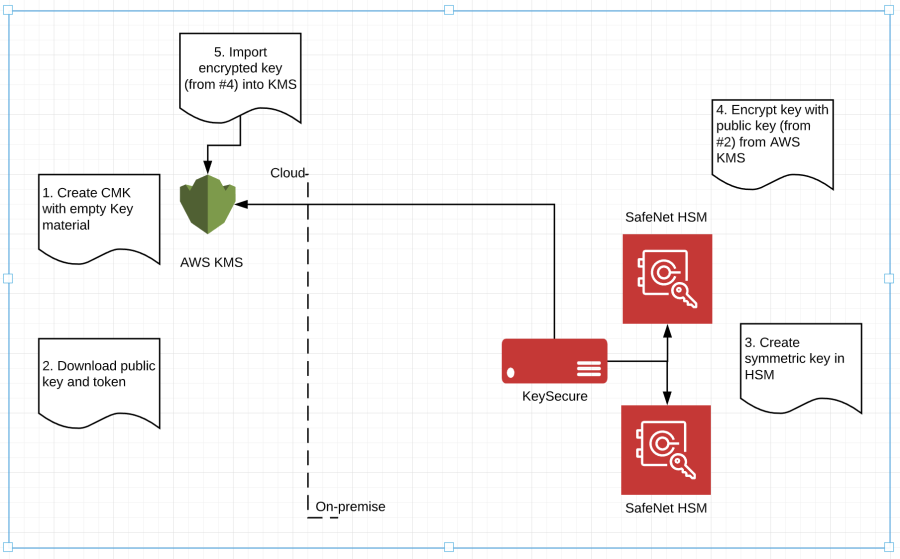
**Payload Encryption (combination of Asymmetric and Symmetric key)**

This scenario shall apply when APIs are used for data exchange. The payload to be encrypted could be a record made up of multiple fields or select sensitive fields within the payload.

1. Data at Rest *(Note: Approach in progress)*:

For data at rest, Ascend shall leverage symmetric keys. The levels of encryption can be at the disk level, file level, database level, field/column level and a combination of these depending on the product requirements. The level of encryption will be impacted by personally identifiable information (PII) data. Further, PII data in itself can be categorized as sensitive PII data (e.g., social security number, bank account number) and non-sensitive PII data (e.g., date of birth) and more than one key can be used to encrypt based on the category of PII data. Encryption at the disk-level (an S3 bucket, EBS or EMR for AWS)

* 1. For S3 buckets holding non-PII data, default encryption provided by AWS can be utilized
  2. For EBS and EMR volumes holding non-PII data, default encryption provided by AWS can be utilized
  3. For S3 buckets and other AWS components that hold PII data, keys generated within Experian's Gemalto SafeNet HSM infrastructure must be utilized
     1. Generate keys within Experian's Gemalto SafeNet infrastructure
     2. Import to AWS KMS leveraging envelope encryption provided by AWS for customer managed keys (CMK)
     3. Encrypt the S3 bucket with the imported Experian key.

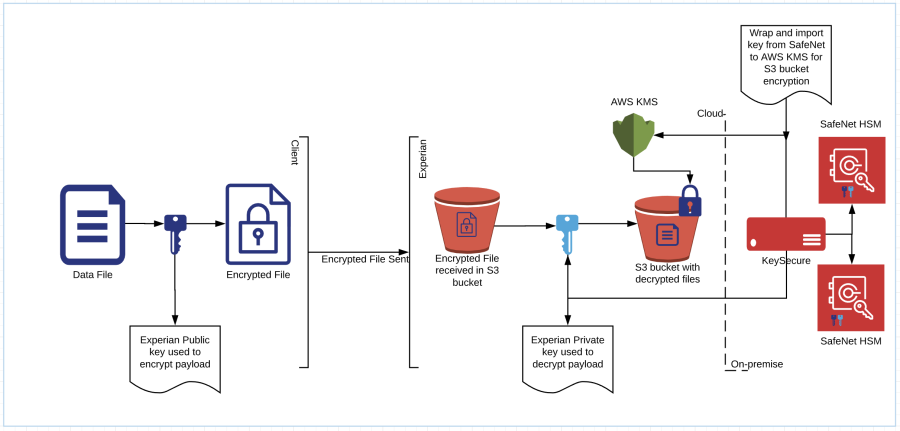
Import Experian Key (CMK) into AWS KMS   
  
References:  
[AWS Key Management Service](https://pages.experian.com/display/RGPM/Key+Management+Service)  
[Importing Experian keys to AWS KMS](https://pages.experian.com/display/ASPLIN/Importing+Custom+Key+to+KMS)

1. Encryption at the file-level *(Note: Approach in progress)*
   1. *Experian's Gemalto SafeNet provides 2 options for file-level encryption:* ***ProtectFile and ProtectFuse****. ProtectFile has kernel dependencies and incompatibilities limiting its use. ProtectFuse is still in deployment mode. Once ProtectFuse is made available within Experian, it will be used for file level encryption.*
2. Encryption at the database-level *(Note: Approach in progress)*
   1. Storage object encryption – Same approach as 2.2 (1) Encryption at the disk-level shall be applied
   2. *Transparent data encryption (TDE) – Experian's Gemalto SafeNet provides ProtectDB as a solution for encrypting databases but limited to Oracle, IBM DB2 and MS SQL Server. When applicable this shall be utilized.*
   3. *Big Data Security – Experian's Gemalto SafeNet provides TDE for Hadoop and NoSQL DB. Licensing is unavailable at this point in time.*
3. Encryption at the field/column level *(Note: Approach in progress)*

Product use cases and policies

**Data transfer and disk-level encryption (PII data)**

This scenario is applicable in the scenario where PII data is part of the payload that is being transferred. The sequence of the data flow would include:

1. Using PGP public key to encrypt and transfer the payload to an Ascend landing zone (S3 bucket)
2. Decrypt the payload with the PGP private key
3. PII Data - Transfer and Storage Store the decrypted payload in an S3 bucket encrypted with Experian keys. 

**Field-level encryption (PII data using single key)**

Approach in progress

**Field-level encryption (PII data using multiple keys)**

Approach in progress

**Database encryption (PII data using TDE)**

Approach in progress

Ascend Key Management Process

As part of Ascend data encryption process, the keys generated for this purpose shall leverage a combination of Experian's Encryption and Key Management provided Gemalto SafeNet infrastructure, AWS KMS or AWS CloudHSM (future plan).

Ascend's key management process will utilize both symmetric and asymmetric keys. The key strengths and ciphers will be adherence with Experian Global Security Office policies and technical security baselines for encryption and public key cryptography.

References:  
[Experian Encryption and Key Management GSO](https://pages.experian.com/display/EEDP/Encryption+and+Key+Management+GSO)  
[AWS Key Management Service](https://pages.experian.com/display/RGPM/Key+Management+Service)

Key Management Service

**Experian Gemalto SafeNet KeySecure**

Experian provides the key management infrastructure that includes Gemalto SafeNet KeySecure and Hardware Security Modules (HSM). The HSMs are hosted on-premises at McKinney, TX and Allen, TX.  
Experian's key management infrastructure must be utilized if a product that will be part of the Ascend Platform includes PII data.  
References:  
[Experian Key Management Infrastructure](https://pages.experian.com/display/EEDP/Encryption+Platform+Architecture?preview=/271005932/280699562/EEPDataFlow_v6.pdf)

**AWS Key Management Service**

AWS KMS is a managed key management service provided by Amazon. AWS KMS can be utilized for default encryption methods using AWS KMS generated keys when any product on Ascend does not include PII data. AWS KMS can be utilized for products on Ascend that include PII Data by leveraging customer managed keys (CMK) wherein the keys are generated within Experian's Gemalto SafeNet infrastructure and imported into AWS KMS.

**AWS CloudHSM (Future plan)**

AWS CloudHSM is a managed HSM service that enables Experian to create and manage its keys in the AWS cloud.

AWS CloudHSM can be utilized for all products on Ascend Platform for both PII and non-PII data in tandem within Experian's Gemalto SafeNet infrastructure.

Connectors and API

**Experian Gemalto SafeNet KeySecure Connectors**

As part of the Experian Gemalto SafeNet infrastructure, a set of connectors are provided for key management and encryption services.

1. **ProtectApp**: This connector shall be the primary connector used by Ascend products for encryption/decryption of file, field and column level data.
2. **ProtectDB**: This connector shall be used by Ascend products on a limited basis depending on the type of database being used and supported by Gemalto SafeNet.

References:  
[Experian Key Management Infrastructure - Connectors](https://pages.experian.com/display/EEDP/Working+with+Connectors+-+Types+of+Encryption+Tools)

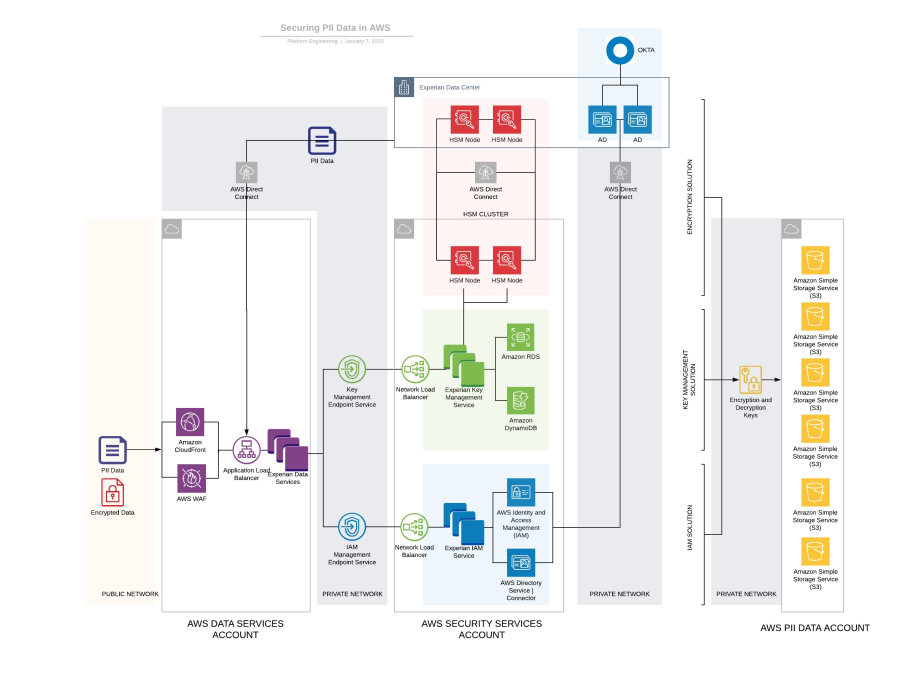
**AWS Key Management Service API**

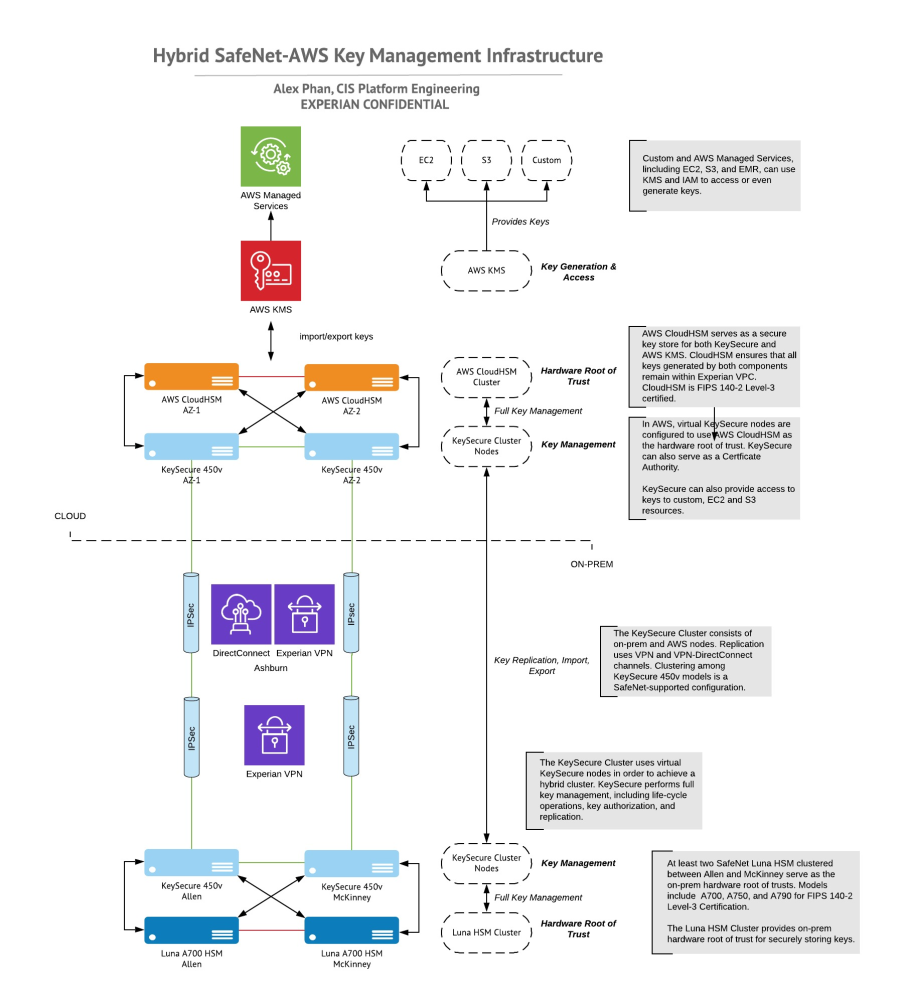
AWS KMS provides a set of APIs and SDKs for key management and encryption/decryption activities.  
For general purpose AWS KSM use, the AWS KMS APIs shall be utilized.  
For AWS CloudHSM, KeySecure or industry standard cryptographic libraries shall be utilized.  
References:  
[AWS KMS APIs](https://docs.aws.amazon.com/kms/latest/developerguide/programming-top.html)

Appendix

Ascend Encryption Infrastructure

Ascend Key Management Hybrid Architecture



  
Experian references:

|  |  |
| --- | --- |
| **Name** | **Title** |
| **Sai Tallapaka** | Head of Platform Security |
| **Alexander Phan** | Architect (Security) |
| **Gopi Chand Mummineni** | Director, Ascend Core Platform |
| **Satya Jasti** | Architect (Infrastructure) |
| **Subhojit Goswami** | Global Head of Data Protection |

[Like](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20)Be the first to like this

* No labels
* [Edit Labels](https://pages.experian.com/pages/viewpage.action?spaceKey=RGPM&title=Ascend+Encryption+Process+v1.20)

Top of Form

Write a comment…

# BACKUP

# RACI for Personas and Roles

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roles  Personas | Developer  Architect? | Admin | SRE | SRE-Admin | Analyst | Analyst-Elevated | Auditor | Security-Analyst |  | Custodian |
| CIS 3I Cybersec Framework | Protect, Architect | Developer | Maintain | Monitor | Respond | Recover | Audit | Upgrade |  | Govern |
|  | **Developer** | **Developer-X** | **DevOpsAdmin only thru Tform** | **SuperAdmin** | **Analyst** | **Analyst-X** | **ReadOnly-Admin** | **Custodian** | **DBA** | **Financial** |
| Developer  - DevSecOps Engineer | XXXX  XXX | Short lived role for test | infra change eng experts with Terraform |  |  | Only for PII access permitted roles |  | We shd!! Just kms |  |  |
| Site Reliability Engineer  - Cloud Administrator |  |  | XXX  XXX | 5 folks have access to devops X for PII, org level changes |  |  |  | Kms lifecycle engr |  |  |
| Cloud Administrator (Good!) |  |  |  |  |  |  |  |  |  |  |
| DevSecOps Engineer |  |  |  |  |  |  |  |  |  |  |
| Database Administrator |  |  |  |  |  |  |  |  | XXXX |  |
| Security Analyst  Security Architect |  |  |  |  |  |  | XXXX |  |  |  |
| Security Owner(?) custodian role |  |  |  |  |  |  |  | XXXX |  |  |
| Data Analyst (architect?) |  |  |  |  | Analyst, -X for S3, Athena access |  |  |  |  |  |
| Auditor Risk Manager  Compliance manager |  |  |  |  |  |  | XXXX  Through tool sets like Prisma, mVision/McAfee |  |  |  |
| Product Support |  |  |  |  |  |  | XXXX |  |  |  |
| Client Support | Dedicate sandbox-data, infra, tools, anyl,,Amex.. developers |  |  |  |  |  | ADS read only from S3 |  |  |  |
| Governance |  |  |  |  |  |  | XXXX billing, policies,.. |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

1. Persona: GSO/EITS/Misc/Other BUs

set data classification sec officer

Level of xptn Sec officer

Key creation Sec officer

Access control to keys SRE

Xptn services, crypto licenses- SRE

## Some ideas on External Customer personas:

Mid-sized company personas summarized by Deloitte:

* •Credit Supervisor, Mid-sized company: Someone who purchases a few key products
* •Collections Manager, Mid-sized company: Someone who buys products to help debt collection and tracks accounts receivable and recovery rates
* Researcher – Live Chat, Phone numbers (All business sizes)
* •Strat Client
* •IT / Technologist (Large to mid-size)
* •Regulatory / Governance (Large to mid-size)
* •Indirect / Reseller (Large to mid-size)
* •Lending Operations (All business sizes)

[Skip to end of metadata](https://pages.experian.com/display/EIMTEAMS/EITS+EIMTeams+Home#page-metadata-end)

* Created by [devopsint](https://pages.experian.com/display/~devopsint), last modified by [Crawford, Kristopher](https://pages.experian.com/display/~C68738A) on [Apr 23, 2021](https://pages.experian.com/pages/diffpagesbyversion.action?pageId=689878948&selectedPageVersions=64&selectedPageVersions=65)

[Go to start of metadata](https://pages.experian.com/display/EIMTEAMS/EITS+EIMTeams+Home#page-metadata-start)

Top of Form



Search

Bottom of Form

About

We are part of Enterprise Information Management in EITS. We manage build and support of various database systems; including Relational databases, NO-SQL databases and database replication services.

Our Mission

Our mission is to provide best support to all the Business Units and keep databases available to maximum.

DBaaS Information

Roadmap

[Click to view the DBaaS Roadmap.](https://pages.experian.com/download/attachments/785971447/roadmap.pptx?version=1&modificationDate=1610484620600&api=v2)

EITS DBA Groups

**Contacts Matrix:** [Basic Communications](https://pages.experian.com/download/attachments/785971447/Contacts.pdf?version=1&modificationDate=1608429396525&api=v2)

Engaging DBA

How to request a Database

[Instructions to request a database](https://pages.experian.com/download/attachments/689878948/Instructions%20to%20request%20a%20database.pdf?version=1&modificationDate=1611342109818&api=v2)

How to request for DBA Support

[Steps to request DBA support](https://pages.experian.com/download/attachments/689878948/Steps%20to%20request%20DBA%20support.pdf?version=1&modificationDate=1611342109897&api=v2)

RDBMS

Relational Database Management Systems (RDBMS)

A relational database is based on the relational model of data, which organizes data into one or more tables of rows and columns, with a unique key for each row. A software system used to maintain relational databases is a relational database management system (RDBMS).

[**Learn more >>>**](https://pages.experian.com/display/EIMTEAMS/Relational+Database+RDBMS)

NoSQL

NoSQL

NoSQL is an approach to database design that can accommodate a wide variety of data models, including key-value, document, columnar and graph formats. NoSQL, which stands for "not only SQL," is an alternative to traditional relational databases in which data is placed in tables and data schema is carefully designed before the database is built.

[**Learn more >>>**](https://pages.experian.com/display/EIMTEAMS/NoSQL)

Data Replication Support

Data Replication Management

Data replication is the process of storing the same data in multiple locations to improve data availability and accessibility, and to improve system resilience and reliability. When businesses run multiple replicas on multiple servers, users can access data faster.

[**Learn more >>>**](https://pages.experian.com/display/EIMTEAMS/Data+Replication+Management)

Important docs: <https://docs.aws.amazon.com/kms/latest/developerguide/services-nitro-enclaves.html>

<https://docs.aws.amazon.com/enclaves/latest/user/set-up-attestation.html>

<https://docs.aws.amazon.com/enclaves/latest/user/verify-root.html>

Workshop section where you can see vsock-proxy pointing to an external URL: <https://nitro-enclaves.workshop.aws/en/my-first-enclave/secure-local-channel.html> Bottom of Form

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html>

<https://github.com/aws/aws-nitro-enclaves-sdk-c/blob/main/docs/kmstool.md>