Column Level Encryption Enterprise

The data security challenge

Protecting sensitive and regulated data is a top priority for today's corporate boards and C-suite executives. Arguably, the toughest job for the CIO and CISO is striking a balance between the competing needs to both share and protect information. The stakes are increasingly high with regulatory censure, fines, reputational damage, loss of business and legal exposure all being potential consequences from even small lapses in data confidentiality, privacy and integrity.

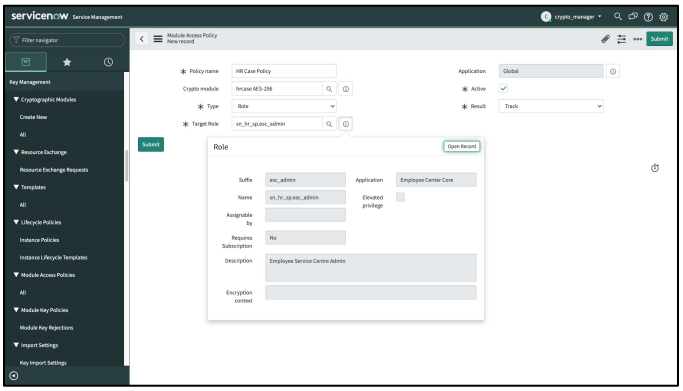
ServiceNow® Column Level Encryption Enterprise

Encryption is a data protection control that is increasingly being utilized to mitigate the risk of unauthorized or unlawful data processing of sensitive and regulated data. Examples of regulated data include Personally Identifiable Information (PII), Protected Health Information (PHI), Client Identifiable Data (CID), export-controlled information, intellectual property, financial information subject to Sarbanes-Oxley compliance, and Cardholder Data (CD).

ServiceNow Column Level Encryption Enterprise (CLEE) provides field and attachment-based data encryption within instances of the Now Platform. With CLEE, security administrators can configure which specific data to encrypt within a specific table. Common use cases for CLEE include:

- Enforcing confidentiality of sensitive and regulated data within the database and user interface, reducing the risk of unauthorized disclosures or data exfiltration
- Enabling customers to comply with governmental and industry certification requirements and regulations
- Limiting key-access to sensitive data based on defined roles, defined script assignments, system user, application scope and domain membership

CLEE does not impact orchestration, reporting or workflows for authorized users and can apply AES-128 or AES-256 encryption algorithms based on the customer's choice. Key access for encryption and decryption can be based on a user's role or group membership, allowing only those users with a particular role or group membership to interact with data in a decrypted state.



Module access policies

Increase value
Extend the value of your ServiceNow enterprise services with high confidence in data confidentiality, privacy and integrity.

Reduce and manage risk

Apply native application-level encryption of your most sensitive data to help meet your compliance and governance requirements.

Maximize data protection

Utilize encryption and key lifecycle management capabilities that are designed and built to NIST 800-57 standards.

Greater control of data security

Encrypt your data with encryption keys that you supply and manage.

Maintain user experience

Provide unencumbered orchestration, workflows and reporting of CLEE-supported fields.

CLEE uses ServiceNow's Key Management Framework (KMF) which enables flexible encryption policies and API support. The KMF provides enhanced key management capabilities following NIST 800-57 guidelines and gives customers the choice of providing their own keys (bring your own keys, BYOK) or using keys randomly generated by ServiceNow. Customer keys are re-encrypted (wrapped) with multiple higher-level keys, with the root key being stored in a Hardware Security Module (HSM) within the ServiceNow cloud infrastructure in redundant secure key storage appliances.

At its core, the KMF provides an interface for the following:

- Segregation of duties with dedicated roles for KMF administration, cryptographic management and operations, audit, and integration
- Configuration of cryptographic specifications for unique cryptographic purposes and key types
- Symmetric keys for encryption/decryption, key wrap and unwrap, and authentication
- Asymmetric keys for digital signatures, encryption and decryption, and key wrap and unwrap
- Key origination, creation, activation, deactivation, revocation, recovery, removal, retention, and renewal

Encryption keys can be customer-managed or ServiceNow-managed, with dual controls required for generating, deleting, or exporting keys. Cryptographic management is undertaken by a specific team within the ServiceNow's security group.

Key Lifecycle Management

Create, revoke, rotate, and suspend keys on a customer-defined cadence. Encrypt data with keys you supply and define.

Modular Access Policies

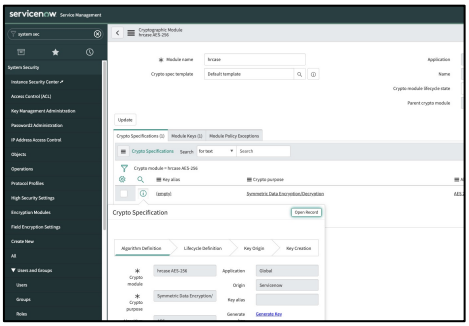
Assign granular key access rights to scripts, roles and system based on the individual crypto use-case.

Key Protection

All key protection and generation is based on Federal Information Processing Standards (FIPS) 140-2-L3 High Security Modules.

Key Access Auditability

See key usage statistics and retain audit data to adhere to regulatory and internal compliance policies.



Key lifecycle management

> “Your confidence in our ability to repel security threats, protect your data, and help you comply with global mandates is essential to our partnership with you.

servicenow

SN-DataSheet-Name-062021