Encrypt Sensitive Data in Salesforce and Comply with Security Regulations

brimit

A multitude of data regulations

Nowadays, data storage and processing are heavily regulated by numerous protection laws, and businesses dealing with sensitive information are forced to comply with them. Data encryption is the most common requirement. Below are some common data types and applicable regulations, all of which require data encryption.

Financial data

- **NYCRR 500 Cybersecurity**
- **PCI DSS**
- **GLBA**

Health data

- **HIPAA**

Personal data online

- **GDPR**
- **CCPA**
- **PIPEDA**

A multitude of data regulations

Any platforms or tools businesses use to process data have to comply with security regulations. Salesforce, which enjoys popularity across industries such as finance, health care, e-commerce, etc., is not an exception. According to Brimit Salesforce team, nine out of ten customers have a product regulated by a data protection law. Failure to adhere to such regulations may result in legal and financial penalties, compromised data, as well as reputational damage.

Encryption available in Salesforce

Under existing regulations, organizations are required to securely store and process information such as:

- ✓ account usernames and passwords
- ✓ passphrases
- ✓ security and access tokens
- ✓ credit/debit card numbers and account data
- ✓ personal information: name, phone number, e-mail, address, income, gender, age, ethnicity, and education
- ✓ health data
- ✓ media access control address, serial numbers, and IP addresses

Salesforce provides several tools for encrypting data:

- ✓ encrypted text fields (classic encryption)
- ✓ Salesforce Shield
  - · event monitoring
  - · Field Audit Trail
  - · Shield Platform Encryption
- ✓ Protecting data in Apex
  - · Apex encryption (Crypto class)

Table 1. Applicability of encryption tools to data protection regulations

Regulation	Requirements	Encryption tool fit		
		Encrypted Text Fields	Salesforce	Protecting data in Apex
NYCRR 500	NIST-compliant, 256-bit Advanced Encryption Standard (AES encryption)	✗ (up to 128 bit)	✓	✓
	Store encryption keys apart from the encrypted financial data in a security device specifically designed for this task	? [1]	✓	✓
	The Key Management Interoperability Protocol (KMIP)	✓ [2]	✓ [2]	✓ [2]
	Encryption of sensitive data both in transit and at rest	✗	✓	✗
PCI DSS	AES encryption (128 bit and higher)	✓	✓	✓
	PGP implemented	✓ [3]	✓ [3]	✓ [3]
	Keep encryption keys and data separate	? [1]	✓	✓
HIPAA	End-to-end encryption (E2EE)	✓ [3]	✓ [3]	✓ [3]
	AES encryption (128 bit and higher)	✓	✓	✓
	OpenPGP implemented	✓ [3]	✓ [3]	✓ [3]
GDPR5 [5]	S/MIME implemented	✓ [4]	✓ [4]	✓ [4]
	End-to-end encryption (E2EE)	✓ [3]	✓ [3]	✓ [3]
	AES encryption (128 bit and higher)	✓	✓	✓
CCPA	End-to-end encryption (E2EE)	✓ [3]	✓ [3]	✓ [3]
	AES encryption (128 bit and higher)	✓	✓	✓

Footnotes:

[1] Salesforce most likely stores them separately and doesn't provide control over the keys.

[2] Requires a third-party solution, which stores software on a KMIP-compliant server.

[3] Features out-of-the-box functionality to ensure regulatory compliance.

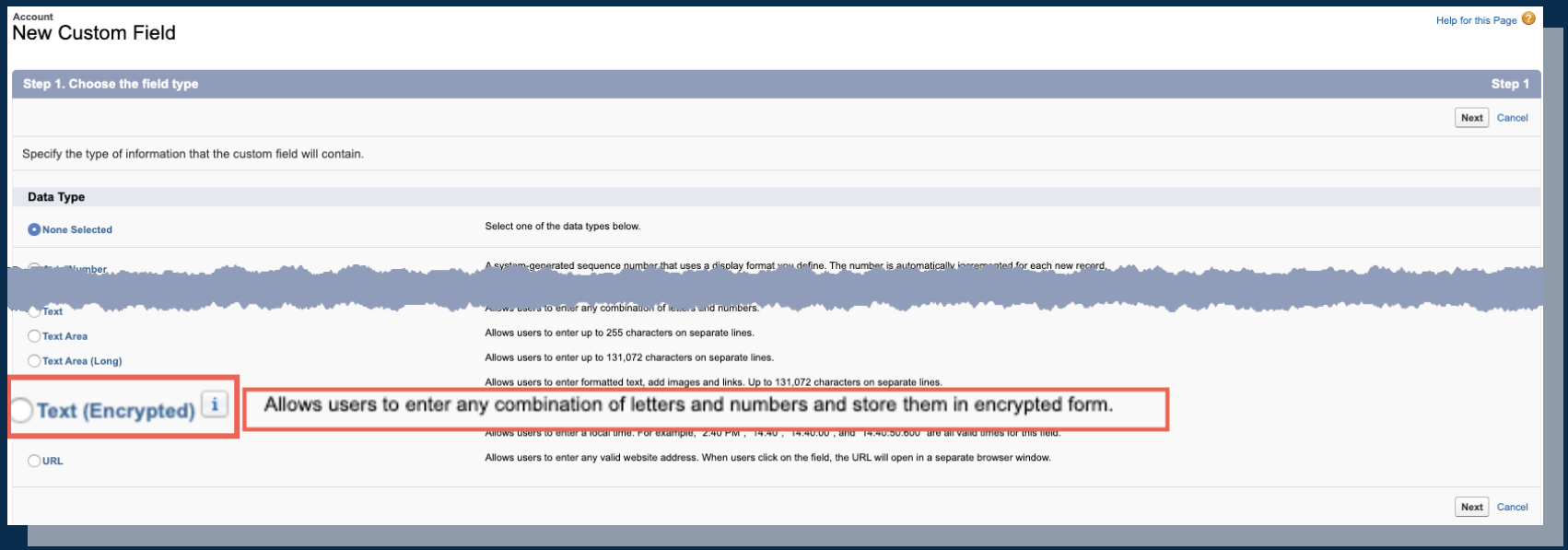
[4] Not available out of the box, but there's a workaround.

[5] There are no explicit requirements for encryption. What's required is pseudonymization. If pseudonymization is performed by means of encryption, that’s fine. The developers need to choose the most common encryption method.

Encrypted text fields **(classic encryption)**

Salesforce provides encrypted text fields out of the box, at no extra cost.

This classic encryption method allows for protecting a custom text field, which a user creates for a particular purpose. The encrypted text field is called Text (Encrypted).

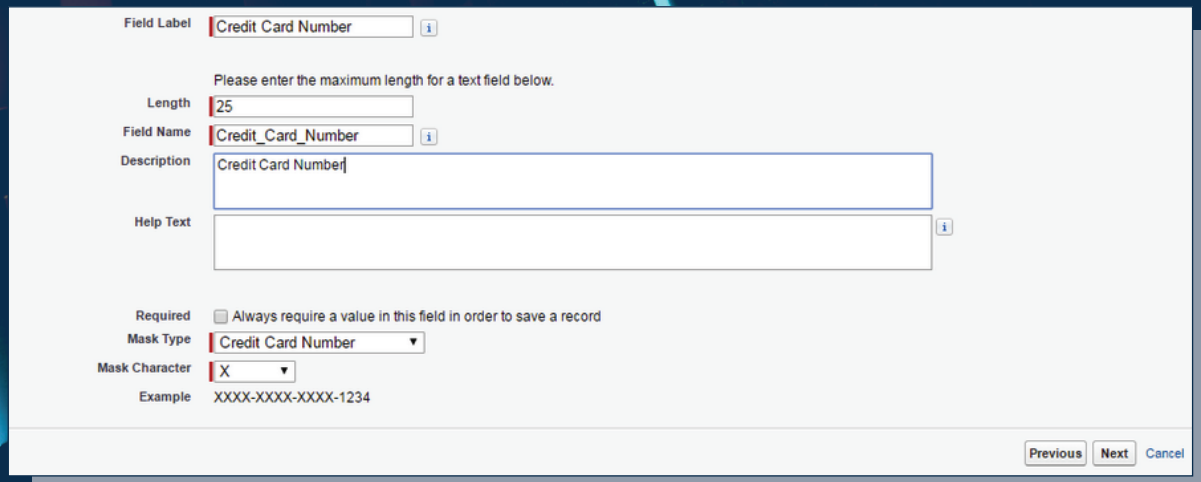


How the encrypted text fields work in Salesforce

Encrypted text fields (classic encryption)

Encrypted custom text fields may contain letters, numbers, or symbols, which will be stored and transmitted in an encrypted format with AES 128-bit keys. The encrypted fields have value for users who have View Encrypted Data permission. We do not recommend storing authentication data in the encrypted custom fields. However, these fields are suitable for storing other types of sensitive data (credit card information, social security numbers, etc.).

Encrypted text fields have the option of "masking" parts of sensitive information, for example, showing the last four digits of a credit card number while hiding the rest.



Using encrypted text fields to mask a card number

The following masking options are available in encrypted text fields:

- ✓ **all digits**
- ✓ **all digits except for the last four**
- ✓ **a credit card number (as shown in the example above)**
- ✓ **a national insurance number**
- ✓ **a social security number**
- ✓ **a social insurance number**

Salesforce Shield

Salesforce Shield provides three services:

Event Monitoring

Field Audit Trail

Shield Platform Encryption

Event Monitoring

Event monitoring allows you to identify which type of data was viewed by a particular user, which network was used to access the data (including the IP address), and how a user interacted with the data. This enables you to have control over scenarios such as who printed a document, viewed a page, or exported data.

Field Audit Trail

Field Audit Trail does a similar job to Field History Tracking, only expanding the tracking period to 10 years and allowing 60 fields to be tracked per object. This way you can get all the information required to understand when a particular set of data was changed and who made the changes.

Shield Platform Encryption

Shield Platform Encryption enables an administrator to encrypt data on the database level of Salesforce. At the same time, users will be able to access the encrypted data if they have relevant permissions. In general, data can be masked but not encrypted, or encrypted but not masked. For example, regulators often require that only the last four digits of a credit card number be visible to users. Applications typically mask the rest of the number, meaning they replace the digits with asterisks on the user's screen. Without encryption, you can still see the digits that are masked if you have access to the database where they are stored.

Protecting data in Apex

Apex is a proprietary, object-oriented programming language developed by Salesforce. The language is used to customize Salesforce products and encrypt data.

Apex encryption (Crypto class)

Apex gives you the flexibility to write custom cryptographic functions as well as the ability to leverage a wide range of prebuilt functions. Using this method, you can encrypt any text with the keys that you define. However, you'll need a Salesforce developer to implement Apex properly.

Encryption and decryption can be done using the AES128, AES192, and AES256 algorithms. To ensure data integrity, the method supports such algorithms as MD5, SHA-1, SHA-2 (SHA-256 and SHA-512). RSA can be used for digital signatures.

Table 2. Apex encryption methods and supported standards.

Method	Supported Standarts
Encrypt() **EncryptWithManagedIv()** **Decrypt()** **DecryptWithManagedIv()**	**AES128, AES192, AES256 for encryption. PCKS#5 padding and Cipher Block Chaining.**
generateDigest() **generateMac()**	**MD5, SHA1, SHA256, SHA512**
sign()	**SHA1 with RSA**

With multiple encryption methods available, Salesforce ensures data security and compliance with existing regulations across the finance, healthcare, and other industries. Salesforce is a trusted platform and is used by industry giants such as AXA, Barclays, American Express, GE Capital, American Red Cross, Lilly, St John of God Health Care, Adidas, Samsonite, T-Mobile, etc.

Get a Toolset for Generating More Leads and Closing More Deals

How we emplement sales and marketing tools:

https://www.brimit.com/services/sales-and-marketing-tool-implementation

What we do with Salesforce:

https://www.brimit.com/technologies/salesforce