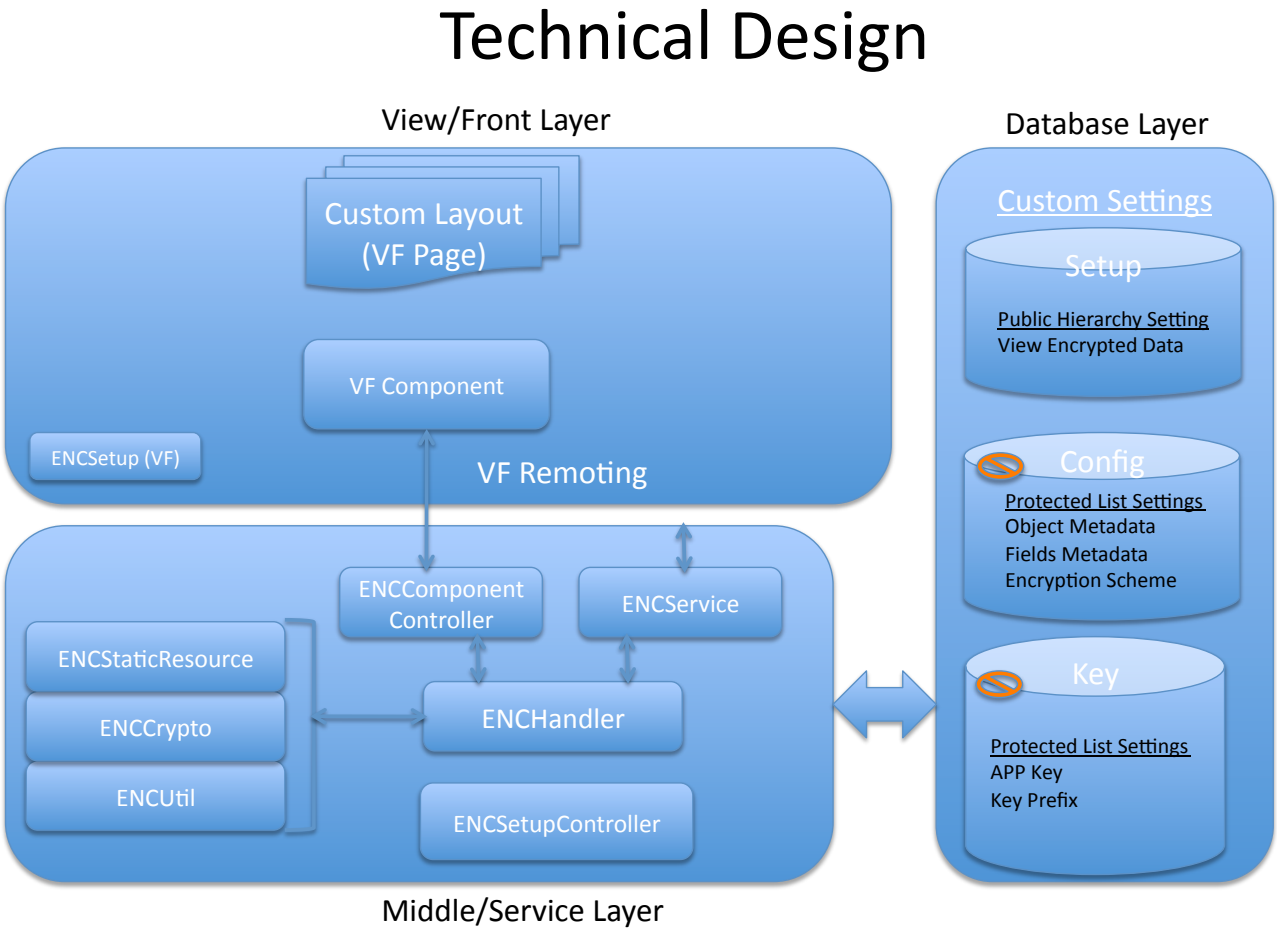
ENCRYPTIK TECHNICAL DOCUMENT

TECHNICAL DIAGRAM OF ENCRYPTIK



ENCRYPTIK Components:

A) Key Management

The key management module of Encryptik stores the key in an encrypted format. This key is used every time during the encryption and decryption of data.

This key is encrypted using a random key called " Support Key". The Support key that is used is masked using a masking algorithm that masks this key in the characters that are not available in the generic keyboard.

The keys are stored in a protected custom settings called (App Key), which are accessible only by the application.

B) Configuration Management

The application configuration that includes the object and the respective fields that needs to be encrypted, these details are handled by the configuration management module.

With this module administrator can configure all the objects and its respective fields that needs to be encrypted and also the schemes that are applied for the encryption.

The schemes supports the following data types (Text/String, Phone,Fax,URL).

Once a scheme is attached to a field, it can't be changed. The Administrator gets an option to Activate/De-activate fields for encryption.

De-activation of encryption for the whole object is not supported.

The configuration management only showcases those objects for which trigger can be created.

All these data are also stored in a protect custom settings called (App Config), which are accessible only by the application.

C) Access Management

Access management ensures that the encrypted data can be viewed by authorised users only.

Administrators can set the access management wherein they can restrict users to view the encrypted data organization level, profile level or user level.

The app settings can be configured by the administrator using the Custom settings option. By default, the application sets the permission as organization wide view of decrypted data.

D) Encryption module

Encryptik module sits on top of the database layer of salesforce. This module interacts with configuration management module to get the objects and the fields and the schemes for encryption and interacts with the key management module to use the keys for performing the encryption.

The encryption module uses the triggers to communicate with the database.

Encryption Schemes

The following encryption schemes are available with the Encryptik application (1.20 version)

SCHEMES	FUNCTION
Text Type-1 Encryption Scheme	String encryption using AES256 Crypto.EncryptWithManagedIV()
Text Type-2 Encryption Scheme	String encryption using AES256 Crypto.Encrypt(). (If search required)
Tokenization Scheme	This is applicable to string having separators (,-) etc and want to preserve it. For example ABC,XYZ will be encrypted as XXX,XXX wherein the , is not encrypted and is kept intact

Phone/Fax Left Encryption Scheme	The first 3 characters of the Phone will not be encrypted and the rest are encrypted.
Phone/Fax Right Encryption Scheme	The last 3 characters of the Phone will not be encrypted and the rest are encrypted.
URL Encryption Scheme	Retains the URL details like WWW and .COM of the URL string.
Phone/Fax Encryption Scheme	Number encryption

The following encryption schemes are available with the Encryptik application (June 2014 release)

ENCRYPTION SCHEMES

SCHEMES	**FUNCTION**
Text Type-1 Encryption Scheme	- String encryption using AES256 Crypto.EncryptWithManagedIV(). - Highest level of encryption. - Generates encrypted text which contains minimum of 48 characters - Scheme can't be applied to fields less than 50 characters in length - Fields with 80 character length can only enter 45 characters of data - Fields with 255 character length can only enter 170 characters of data - Not Searchable
Text Type-2 Encryption Scheme	- String encryption using AES256 Crypto.Encrypt() - Applicable for fields less than 50 characters - Generates encrypted text of minimum of 28 characters - Is Searchable
Token Encryption Scheme	- This is applicable to string having separators (,-) etc and want to preserve it. - For example ABC,XYZ will be encrypted as XXX,XXX wherein the , is not encrypted and is kept intact - Suitable for fields having "," separated data that needs to be kept intact.
URL Encryption Scheme	- URL Encryption scheme - Retains the URL details like WWW and .COM of the URL string.
Phone/Fax Encryption Scheme	- For Phone/Fax Data types

TOKENISATION SCHEMES

This scheme does not use AES256 algorithm but uses the private key for tokenisation

SCHEMES	FUNCTION
Email Tokenisation Scheme	- For Email data types - Tokenisation done to the email preserving the domain name
Text Tokenisation Scheme	- Applicable for fields size with 24 characters and less. - Tokenisation uses 4 more characters in addition to the actual data length. - E.g. Fields with 24 character length can only enter 20 characters of data
Percent Tokenisation Scheme	- Tokenisation scheme for Percentage data types
DateTime Tokenisation Scheme	- Handles DateTime data types
Date Tokenisation Scheme	- Handles Date data type
Double Tokenisation Scheme	- For Double and Currency data types
Numeric masking Tokenisation Scheme	- For numeric data types wherein the length is fixed - Used for specific fields where the data comes in the same length and it can’t be increased
Text masking Tokenisation Scheme	- For text data types wherein the length is fixed - Used for specific fields where the data comes in the same length and it can’t be increased