DATA SHEET

Format Preserving Encryption

Format Preserving Encryption

- Format Preserving Encryption
  - Sotero provides Format Preserving Encryption (FPE) option to protect sensitive elements in the data-stores.
  - Sotero FPE is implemented following NIST approved FF1 - Format Preserving Algorithms
  - Sotero FPE operates on String data type
  - When data is encrypted using FPE algorithm resultant cipher text is of same format as the plain text.
  - Encryption key, tweak are required for both encryption and decryption operations.
  - Key
    - ◊ Both key is internally generated and stored in the vault.
    - ◊ Generated key is of length 256 bits.
  - Tweak
    - ◊ Internally generated and stored in the vault.
    - ◊ Option to supply tweak to randomize low cardinality values

FPE - Configurations - Encryption Type

- FPE Encryption Type
  - FPE -
    - ◊ Use internally generated tweak, generated key and specified Alphabet for encrypt and decrypt operations.
    - ◊ This mode is required if encrypted values are stored in the database and are used for equality and filtering operations in the database.
- FPE-DYNAMIC-TWEAK

- Uses internally generated key, supplied tweak and specified Alphabet for encrypt and decrypt operations.
- This should only be applied to strengthen the encryption of low cardinality fields like gender.
- If a field is encrypted with dynamic tweak ability to filter using where clauses is not supported.

Encryption Process

- Algorithm takes in following elements and will return cipher text
  - Incoming plain text
  - Configured Alphabet
  - Predefined Special Characters
  - Key
  - Tweak (internally generated or supplied)
- Cipher text will include characters defined in the alphabet along with special characters in the plain text values
- Special characters will not be encrypted and are left as they are to retain format.
- If incoming plain text value has characters which are not part of the defined alphabet and defined special characters:
  - EBCDIC and NUMERIC- Will throw invalid input
  - ASCII, EASCII, UNICODE - Will leave the character as is in the cipher text

FPE - Configurations - Alphabet

- FPE EBCDIC
  - Includes :

‘â’ ,’ä’ ,’à’ ,’á’ ,’ã’ ,’å’ ,’ç’ ,’ñ’ ,’¢’ ,’é’ ,’ê’ ,’ë’ ,’è’ ,’í’ ,’î’ ,’ï’ ,’ì’ ,’ß’ ,’¬’ ,’Â’ ,’Ä’ ,’À’ ,’Á’ ,’Ã’ ,’Å’ ,’Ç’ ,’Ñ’ ,’¦’ ,’ø’ ,’É’ ,’Ê’ ,’Ë’ ,’È’ ,’Í’ ,’Î’ ,’Ï’ ,’Ì’ ,’Ø’ ,’a’ ,’b’ ,’c’ ,’d’ ,’e’ ,’f’ ,’g’ ,’h’ ,’i’ ,’«‘ ,’»’ ,’ð’ ,’ý’ ,’þ’ ,’±’ ,’°’ ,’j’ ,’k’ ,’l’ ,’m’ ,’n’ ,’o’ ,’p’ ,’q’ ,’r’ ,’a’ ,’o’ ,’æ’ ,’¸’ ,’Æ’ ,’µ’ ,’s’ ,’t’ ,’u’ ,’v’ ,’ w’ ,’x’ ,’y’ ,’z’ ,’¡’ ,’¿’ ,’Ð’ ,’Ý’ ,’Þ’ ,’®’ ,’·’ ,’©’ ,’§’ ,’¶’ ,’1⁄4’ ,’1⁄2’ ,’3⁄4’ ,’¯’ ,’¨’ ,’˝’ ,’×’ ,’A’ ,’B’ ,’C’ ,’D’ ,’E’ ,’F’ ,’G’ ,’H’ ,’I’ ,’ô’ ,’ö’ ,’ò’ ,’ó’ ,’õ’ ,’J ‘ ,’K’ ,’L’ ,’M’ ,’N’ ,’O’ ,’P’ ,’Q’ ,’R’ ,’1’ ,’û’ ,’ü’ ,’ù’ ,’ú’ ,’ÿ’ ,’÷’ ,’S’ ,’T’ ,’U’ ,’V’ ,’W’ ,’X’ ,’Y’ ,’Z’ ,’2’ ,’Ô’ ,’Ö’ ,’Ò’ ,’Ó’ ,’Õ’ ,’0’ ,’1’ ,’2’ ,’3’ ,’4’ , ‘5’ ,’6’ ,’7’ ,’8’ ,’9’ ,’3’ ,’Û’ ,’Ü’ ,’Ù’ ,’Ú’

  - Special Chars :

!\”#$%&’()*+,-./:;<=>?@[\\]^_ `{|}~£¥€\\E\\{Space}

- FPE EASCII

  - Includes :

‘ó’, ‘I’, ‘V’, ‘è’, ‘Ý’, ‘Y’, ‘p’, ‘j’, ‘É’, ‘ü’, ‘Œ’, ‘ß’, ‘u’, ‘š’, ‘x’, ‘F’, ‘9’, ‘Å’, ‘8’, ‘Ð’, ‘Ñ’, ‘l’, ‘Ó’, ‘ï’, ‘é’, ‘G’, ‘X’, ‘h’, ‘ñ’, ‘a’, ‘Ë’, ‘o’, ‘Ž’, ‘r’, ‘M’, ‘6’, ‘y’, ‘á’, ‘c’, ‘û’, ‘K’, ‘ø’, ‘t’, ‘Î’, ‘À’, ‘Š’, ‘ô’, ‘Ú’, ‘ò’, ‘ë’, ‘à’, ‘ì’, ‘Ù’, ‘Æ’, ‘q’, ‘A’, ‘5’, ‘Ö’, ‘S’, ‘2’, ‘d’, ‘s’, ‘Ç’, ‘Ï’, ‘v’, ‘Þ’, ‘œ’, ‘0’, ‘ä’, ‘T’, ‘Ø’, ‘Ì’, ‘È’, ‘b’, ‘g’, ‘7’, ‘Â’, ‘4’, ‘J’, R’, ‘Z’, ‘E’, ‘Í’, ‘Ã’, ‘1’, ‘w’, ‘ú’, ‘ê’, ‘Q’, ‘m’, ‘U’, ‘H’, ‘B’, ‘å’, ‘ƒ’, ‘Ò’, ‘z’, ‘â’, ‘ý’, ‘n’, ‘ç’, ‘Û’, ‘þ’, ‘ž’, ‘Ä’, ‘õ’, ‘f’, ‘Á’, ‘ã’, ‘Ÿ’, ‘Ê’, ‘e’, ‘W’, ‘ö’, ‘æ’,‘Õ’, ‘O’, ‘ÿ’, ‘P’, ‘Ô’, ‘D’, ‘Ü’, ‘ï’, ‘C’, ‘ù’, ‘î’, ‘k’, ‘N’, ‘í’, ‘ð’, ‘L’, ‘3’

  - Special Chars :

Any character which is not in Includes set

- FPE ASCII

  - Includes :

‘a’, ‘b’, ‘c’, ‘d’, ‘e’, ‘f’, ‘g’, ‘h’, ‘i’, ‘j’, ‘k’, ‘l’, ‘m’, ‘n’, ‘o’, ‘p’, ‘q’, ‘r’, ‘s’, ‘t’, ‘u’, ‘v’, ‘w’, ‘x’, ‘y’, ‘z’, ‘A’, ‘B’, ‘C’, ‘D’, ‘E’, ‘F’, ‘G’, ‘H’, ‘I’, ‘J’, ‘K’, ‘L’, ‘M’, ‘N’, ‘O’, ‘P’, ‘Q’, ‘R’, ‘S’, ‘T’, ‘U’, ‘V’, ‘W’, ‘X’, ‘Y’, ‘Z’, ‘0’, ‘1’, ‘2’, ‘3’, ‘4’, ‘5’, ‘6’, ‘7’, ‘8’, ‘9’

  - Special Chars :

Any character which is not in Includes set

- FPE Unicode

  - Includes :

All characters which are identified as letters in unicode set

  - Special Chars :

Any character which is not in Includes set

- FPE Numbers

  - Includes :

‘0’, ‘1’, ‘2’, ‘3’, ‘4’, ‘5’, ‘6’, ‘7’, ‘8’, ‘9’

  - Special Chars :

!\”#$%&’()*+,-./:;<=>?@[\\]^_ `{|}~£¥€\\E\\{Space}

Examples:

Plain Text	Cipher Text
John M. Smith	nhCp s. um6ml
149-454-8548	ÏÊw-ÔKÑ-æ14Ö
06A281971	¡N¶ECW°fv
first.lastname@somedomain.com	BÖo¢ó.ØWZoÁÇçw@2mû·H·ÎX°2.ä2Ê

Examples: EBCDIC Option - FPE-DYNMAIC-TWEAK

Plain Text	Supplied	Cipher Text
John M. Smith	343240017491752	K
149-454-8548	3529622780412802	ò
06A281971	5602235555827768	ç
first.lastname@somedomain.com	5212301132236303	Í

Examples: Numeric Option

Plain Text	Cipher Text
343240017491752	630462105045672
99.216.126.116/16	02.630.594.508/44
0378-0611	5774-0211
(455) 7107121	(149) 7243816
648 840 9537	551 317 1967
+62 827 704 5786	+96 633 369 6080