DATASHEET

Format Preserving Encryption (FPE) Options

Sotero-FPE

Format Preserving Encryption

- Sotero provides Format Preserving Encryption (FPE) options to protect sensitive elements in data stores. When data is encrypted using FPE algorithms, resulting ciphertext is of the same format as the original text.
- Sotero FPE Options use FF1 and FNR Algorithms.
- Encryption key is required for both encryption and decryption operations.
- Key
  - Key is internally generated and stored in the vault.
  - Generated key is of length 256 bits for all modes other than Numeric
  - Generated key is of length 128 bits for Numeric option
- Tweak
- Internally generated and stored in the vault.

Sotero FPE Modes and Data Types

Data Type	Mode	Algorithm	Key Size	Comment
String	ASCII, EBCDIC, UNICODE	FF1	256	Length and format of the string is preserved
String with Numbers (phone)	NUMERICLP	FF1	256	Length and format of the string is preserved
Number	NUMERICLP	FF1	256	Number of digits in encrypted value is same as plain text value
Number	Numeric	FNR	128	Number of digits are not preserved

Encryption Process

- Algorithm accepts the following elements as input and will return ciphertext as output
    - 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 that 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

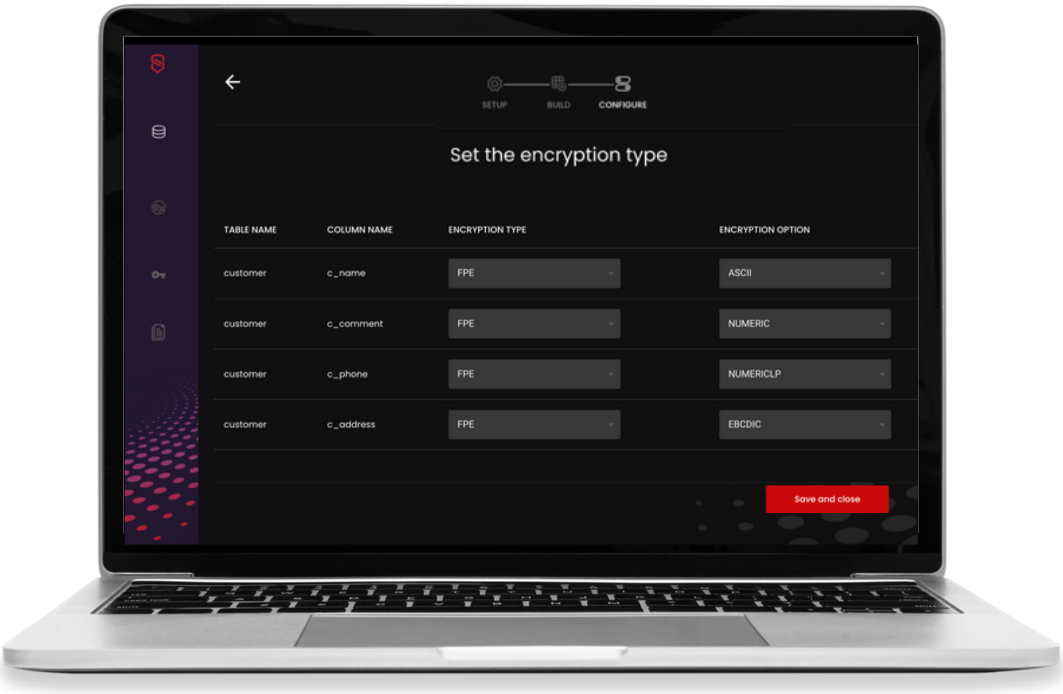
FPE - Configurations - Alphabet

FPE EBCDIC

'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}



Set the encryption type

TABLE NAME	COLUMN NAME	ENCRYPTION TYPE	ENCRYPTION OPTION
customer	c_name	FPE	ASCII
customer	c_comment	FPE	NUMERIC
customer	c_phone	FPE	NUMERICLP
customer	c_address	FPE	EBCDIC

Sotero™

FPE EASCII

'ó', 'I', 'V', 'è', 'Ý', 'Y', 'p', 'j', 'É', 'ü', 'Œ', 'ß', 'u', 'š', 'x', 'F', '9', 'Å', '8', 'Đ', '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', 'i', 'C', 'ù', 'î', 'k', 'N', 'í', 'ð', 'L', '3'

Special Chars

Any character which is not in Includes set

FPE ASCII

'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

All characters which are identified as letters in unicode set

Special Chars

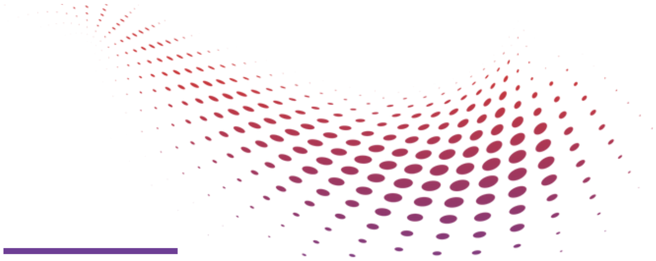
Any character which is not in Includes set

FPE Numbers

'0', '1', '2', '3', '4', '5', '6', '7', '8', '9'

Special Chars

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



Examples

Examples - FPE ASCII

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

Examples - FPE NumericLP

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

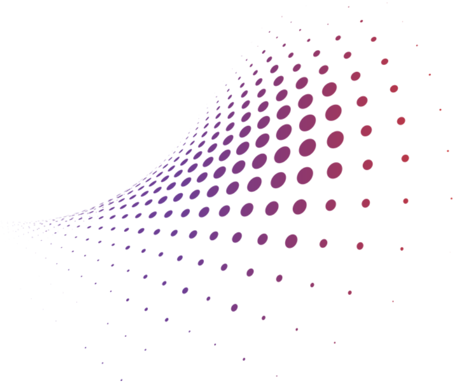
Sotero-OPE

Order Preserving Encryption

- Sotero supports randomized OPE scheme to support range queries on the numeric data type
- Encryption key required for both encryption and decryption operations.
- Key
  - Key is internally generated and stored in the vault.
  - Generated key is of length 256 bits
- Queries
  - Both range and equality queries are supported on the columns configured with OPE encryption

Examples

Plain Text	Cipher Text
100	24678
200	58976
300	98765



About Sotero

Sotero is the global innovator and leader in revolutionary data security. Sotero is a cloud-native data protection platform that protects ALL cloud data types, applications, and stores from catastrophic cyber attacks. Sotero protects your data in the cloud with no costly, time-consuming deployment or downtime. Advanced encryption and real-time machine learning techniques allow organizations to solve for insider and outsider threats while meeting compliance requirements with actionable audit logs. The platform enables fast deployments that enable data to be shared securely and used with confidence. With point and click set-up, Sotero's data security platform is easy to deploy and manage with no impact on user experience. Organizations can now be protected in a matter of days, not weeks or months.