Generate Keys - V1.0.0

# Overview

The Generate Key plugin is used to generate private and public keys with the PKCS#8 format and save them as .pem document and Text format based on the smart service.

**Smart Services**

1. Generate Keys as Document
2. Generate Keys as Text

# Generate Keys as Document

This Smart service generates Key using RSA, Hmac or EC algorithms with PKCS#8 format and saves it in Appian document in .pem format.

## Parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No** | **Name** | **Type** | **Description** |
| 1 | New Document Name | Text | Name for the new document created.The suffix “\_private\_key and \_public\_key” will be added to the document name. |
| 2 | New Document Description | Text | The description for the newly created documents. |
| 3 | algorithm | Text | Provide the algorithm which is used to generate the keys. Valid algorithms are RSA, Hmac or EC |
| 4 | Size | Text | Provide the key size based on the algorithm specified. For RSA algorithm provide 256 or 512 or 1024 or 2048, for Hmac, provide 256 or 384 or 512 and for EC provide 256 or 384 or 521 for curve type. If key size mismatched error will be thrown |
| 5 | Passphrase Scs(optional) | Text | The third-party credentials key is from the Secure credentials store. |
| 6 | Use Per User Credential (Optional) | Boolean | Opt true to use the third-party credentials based on user otherwise false |
| 7 | Save In Folder | Folder | The folder where the creates documents should be saved. |

## Output:

**Private Key –** The created private key document.

**Public Key -** The created public key document.

**Error Occurred –** Returns true if error occurred else false.

**Error Message –** Returns the error message if it occurred.

## Screenshot:



# Generate Keys as Text

This Smart service generates Key using RSA, Hmac or EC algorithms with PKCS#8 format and returns as Text.

## Parameters

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No** | **Name** | **Type** | **Description** |
| 1 | algorithm | Text | Provide the algorithm which is used to generate the keys. Valid algorithms are RSA, Hmac or EC |
| 3 | size (Optional) | Text | Provide the key size based on the algorithm specified. For RSA algorithm provide 256 or 512 or 1024 or 2048, for Hmac, provide 256 or 384 or 512 and for EC provide 256 or 384 or 521 for curve type. If key size mismatched error will be thrown. |
| 3 | Passphrase Scs (optional) | Text | The third-party credentials key is from the Secure credentials store. |
| 4 | Use Per User Credential (Optional) | Boolean | Opt true to use the third-party credentials based on user otherwise false |

## Output:

**Private Key –** The created private key text.

**Public Key -** The created public key text.

**Error Occurred –** Returns true if error occurred else false.

**Error Message –** Returns the error message if it occurred.

## Screenshot:

