



API Reference

AWS Payment Cryptography Data Plane



API Version 2022-02-03

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Payment Cryptography Data Plane: API Reference

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Welcome	1
Actions	2
DecryptData	3
Request Syntax	4
URI Request Parameters	4
Request Body	4
Response Syntax	5
Response Elements	5
Errors	6
See Also	7
EncryptData	9
Request Syntax	10
URI Request Parameters	10
Request Body	11
Response Syntax	12
Response Elements	12
Errors	13
See Also	14
GenerateAs2805KekValidation	15
Request Syntax	15
URI Request Parameters	16
Request Body	16
Response Syntax	17
Response Elements	17
Errors	18
See Also	19
GenerateAuthRequestCryptogram	20
Request Syntax	20
URI Request Parameters	21
Request Body	21
Response Syntax	22
Response Elements	22
Errors	23
See Also	24

GenerateCardValidationData	25
Request Syntax	25
URI Request Parameters	25
Request Body	26
Response Syntax	27
Response Elements	27
Errors	28
See Also	29
GenerateMac	30
Request Syntax	30
URI Request Parameters	30
Request Body	31
Response Syntax	32
Response Elements	32
Errors	33
See Also	34
GenerateMacEmvPinChange	35
Request Syntax	36
URI Request Parameters	36
Request Body	36
Response Syntax	38
Response Elements	39
Errors	41
See Also	42
GeneratePinData	43
Request Syntax	43
URI Request Parameters	44
Request Body	44
Response Syntax	46
Response Elements	46
Errors	48
See Also	49
ReEncryptData	50
Request Syntax	50
URI Request Parameters	51
Request Body	51

Response Syntax	53
Response Elements	53
Errors	54
See Also	55
TranslateKeyMaterial	56
Request Syntax	56
URI Request Parameters	57
Request Body	57
Response Syntax	57
Response Elements	58
Errors	58
See Also	59
TranslatePinData	60
Request Syntax	61
URI Request Parameters	62
Request Body	62
Response Syntax	64
Response Elements	65
Errors	66
See Also	66
VerifyAuthRequestCryptogram	68
Request Syntax	68
URI Request Parameters	69
Request Body	69
Response Syntax	70
Response Elements	71
Errors	72
See Also	73
VerifyCardValidationData	74
Request Syntax	74
URI Request Parameters	75
Request Body	75
Response Syntax	76
Response Elements	76
Errors	77
See Also	78

VerifyMac	79
Request Syntax	79
URI Request Parameters	79
Request Body	79
Response Syntax	81
Response Elements	81
Errors	82
See Also	83
VerifyPinData	84
Request Syntax	84
URI Request Parameters	85
Request Body	85
Response Syntax	87
Response Elements	87
Errors	89
See Also	90
Data Types	91
AmexAttributes	94
Contents	94
See Also	95
AmexCardSecurityCodeVersion1	96
Contents	96
See Also	96
AmexCardSecurityCodeVersion2	97
Contents	97
See Also	97
As2805KekValidationType	98
Contents	98
See Also	98
As2805PekDerivationAttributes	100
Contents	100
See Also	100
AsymmetricEncryptionAttributes	101
Contents	101
See Also	101
CardGenerationAttributes	102

Contents	102
See Also	103
CardHolderVerificationValue	104
Contents	104
See Also	105
CardVerificationAttributes	106
Contents	106
See Also	107
CardVerificationValue1	109
Contents	109
See Also	109
CardVerificationValue2	110
Contents	110
See Also	110
CryptogramAuthResponse	111
Contents	111
See Also	111
CryptogramVerificationArpcMethod1	113
Contents	113
See Also	113
CryptogramVerificationArpcMethod2	114
Contents	114
See Also	114
CurrentPinAttributes	116
Contents	116
See Also	116
DerivationMethodAttributes	117
Contents	117
See Also	118
DiffieHellmanDerivationData	119
Contents	119
See Also	119
DiscoverDynamicCardVerificationCode	120
Contents	120
See Also	121
DukptAttributes	122

Contents	122
See Also	122
DukptDerivationAttributes	124
Contents	124
See Also	125
DukptEncryptionAttributes	126
Contents	126
See Also	127
DynamicCardVerificationCode	128
Contents	128
See Also	129
DynamicCardVerificationValue	130
Contents	130
See Also	131
EcdhDerivationAttributes	132
Contents	132
See Also	133
Emv2000Attributes	135
Contents	135
See Also	136
EmvCommonAttributes	137
Contents	137
See Also	139
EmvEncryptionAttributes	140
Contents	140
See Also	141
EncryptionDecryptionAttributes	143
Contents	143
See Also	144
Ibm3624NaturalPin	145
Contents	145
See Also	146
Ibm3624PinFromOffset	147
Contents	147
See Also	148
Ibm3624PinOffset	149

Contents	149
See Also	150
Ibm3624PinVerification	151
Contents	151
See Also	152
Ibm3624RandomPin	153
Contents	153
See Also	154
IncomingDiffieHellmanTr31KeyBlock	155
Contents	155
See Also	157
IncomingKeyMaterial	158
Contents	158
See Also	158
KekValidationRequest	159
Contents	159
See Also	159
KekValidationResponse	160
Contents	160
See Also	160
MacAlgorithmDukpt	161
Contents	161
See Also	162
MacAlgorithmEmv	163
Contents	163
See Also	164
MacAttributes	165
Contents	165
See Also	166
MasterCardAttributes	167
Contents	167
See Also	168
OutgoingKeyMaterial	169
Contents	169
See Also	169
OutgoingTr31KeyBlock	170

Contents	170
See Also	170
PinData	171
Contents	171
See Also	171
PinGenerationAttributes	173
Contents	173
See Also	174
PinVerificationAttributes	175
Contents	175
See Also	175
ReEncryptionAttributes	176
Contents	176
See Also	176
SessionKeyAmex	177
Contents	177
See Also	177
SessionKeyDerivation	178
Contents	178
See Also	179
SessionKeyDerivationValue	180
Contents	180
See Also	180
SessionKeyEmv2000	182
Contents	182
See Also	183
SessionKeyEmvCommon	184
Contents	184
See Also	185
SessionKeyMastercard	186
Contents	186
See Also	187
SessionKeyVisa	188
Contents	188
See Also	188
SymmetricEncryptionAttributes	189

Contents	189
See Also	189
TranslationIsoFormats	191
Contents	191
See Also	192
TranslationPinDataAs2805Format0	193
Contents	193
See Also	193
TranslationPinDataIsoFormat034	194
Contents	194
See Also	194
TranslationPinDataIsoFormat1	195
Contents	195
See Also	195
ValidationExceptionField	196
Contents	196
See Also	196
VisaAmexDerivationOutputs	197
Contents	197
See Also	198
VisaAttributes	199
Contents	199
See Also	200
VisaPin	201
Contents	201
See Also	201
VisaPinVerification	202
Contents	202
See Also	202
VisaPinVerificationValue	203
Contents	203
See Also	203
WrappedKey	204
Contents	204
See Also	204
WrappedKeyMaterial	206

Contents	206
See Also	206
WrappedWorkingKey	208
Contents	208
See Also	209

Welcome

You use the AWS Payment Cryptography Data Plane to manage how encryption keys are used for payment-related transaction processing and associated cryptographic operations. You can encrypt, decrypt, generate, verify, and translate payment-related cryptographic operations in AWS Payment Cryptography. For more information, see [Data operations](#) in the *AWS Payment Cryptography User Guide*.

To manage your encryption keys, you use the [AWS Payment Cryptography Control Plane](#). You can create, import, export, share, manage, and delete keys. You can also manage AWS Identity and Access Management (IAM) policies for keys.

This document was last published on September 18, 2026.

Actions

The following actions are supported:

- [DecryptData](#)
- [EncryptData](#)
- [GenerateAs2805KekValidation](#)
- [GenerateAuthRequestCryptogram](#)
- [GenerateCardValidationData](#)
- [GenerateMac](#)
- [GenerateMacEmvPinChange](#)
- [GeneratePinData](#)
- [ReEncryptData](#)
- [TranslateKeyMaterial](#)
- [TranslatePinData](#)
- [VerifyAuthRequestCryptogram](#)
- [VerifyCardValidationData](#)
- [VerifyMac](#)
- [VerifyPinData](#)

DecryptData

Decrypts ciphertext data to plaintext using a symmetric (TDES, AES), asymmetric (RSA), or derived (DUKPT or EMV) encryption key scheme. For more information, see [Decrypt data](#) in the *AWS Payment Cryptography User Guide*.

You can use an decryption key generated within AWS Payment Cryptography, or you can import your own decryption key by calling [ImportKey](#). For this operation, the key must have `KeyModesOfUse` set to `Decrypt`. In asymmetric decryption, AWS Payment Cryptography decrypts the ciphertext using the private component of the asymmetric encryption key pair. For data encryption outside of AWS Payment Cryptography, you can export the public component of the asymmetric key pair by calling [GetPublicCertificate](#).

This operation also supports dynamic keys, allowing you to pass a dynamic decryption key as a TR-31 `WrappedKeyBlock`. This can be used when key material is frequently rotated, such as during every card transaction, and there is need to avoid importing short-lived keys into AWS Payment Cryptography. To decrypt using dynamic keys, the `keyARN` is the Key Encryption Key (KEK) of the TR-31 wrapped decryption key material. The incoming wrapped key shall have a key purpose of `D0` with a mode of use of `B` or `D`. For more information, see [Using Dynamic Keys](#) in the *AWS Payment Cryptography User Guide*.

For symmetric and DUKPT decryption, AWS Payment Cryptography supports TDES and AES algorithms. For EMV decryption, AWS Payment Cryptography supports TDES algorithms. For asymmetric decryption, AWS Payment Cryptography supports RSA.

When you use TDES or TDES DUKPT, the ciphertext data length must be a multiple of 8 bytes. For AES or AES DUKPT, the ciphertext data length must be a multiple of 16 bytes. For RSA, it could be equal to the key size unless padding is enabled.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [EncryptData](#)
- [GetPublicCertificate](#)

- [ImportKey](#)

Request Syntax

```
POST /keys/KeyIdentifier/decrypt HTTP/1.1
Content-type: application/json

{
  "CipherText": "string",
  "DecryptionAttributes": { ... },
  "WrappedKey": {
    "KeyCheckValueAlgorithm": "string",
    "WrappedKeyMaterial": { ... }
  }
}
```

URI Request Parameters

The request uses the following URI parameters.

[KeyIdentifier](#)

The keyARN of the encryption key that AWS Payment Cryptography uses for ciphertext decryption.

When a WrappedKeyBlock is provided, this value will be the identifier to the key wrapping key. Otherwise, it is the key identifier used to perform the operation.

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

Request Body

The request accepts the following data in JSON format.

CipherText

The ciphertext to decrypt.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4224.

Pattern: (?:[0-9a-fA-F][0-9a-fA-F])+

Required: Yes

DecryptionAttributes

The encryption key type and attributes for ciphertext decryption.

Type: [EncryptionDecryptionAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

WrappedKey

The WrappedKeyBlock containing the encryption key for ciphertext decryption.

Type: [WrappedKey](#) object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "KeyArn": "string",
  "KeyCheckValue": "string",
  "PlainText": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

KeyArn

The keyARN of the encryption key that AWS Payment Cryptography uses for ciphertext decryption.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

PlainText

The decrypted plaintext data in hexBinary format.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4224.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)

- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

EncryptData

Encrypts plaintext data to ciphertext using a symmetric (TDES, AES), asymmetric (RSA), or derived (DUKPT or EMV) encryption key scheme. For more information, see [Encrypt data](#) in the *AWS Payment Cryptography User Guide*.

You can generate an encryption key within AWS Payment Cryptography by calling [CreateKey](#). You can import your own encryption key by calling [ImportKey](#).

For this operation, the key must have `KeyModesOfUse` set to `Encrypt`. In asymmetric encryption, plaintext is encrypted using public component. You can import the public component of an asymmetric key pair created outside AWS Payment Cryptography by calling [ImportKey](#).

This operation also supports dynamic keys, allowing you to pass a dynamic encryption key as a TR-31 `WrappedKeyBlock`. This can be used when key material is frequently rotated, such as during every card transaction, and there is need to avoid importing short-lived keys into AWS Payment Cryptography. To encrypt using dynamic keys, the keyARN is the Key Encryption Key (KEK) of the TR-31 wrapped encryption key material. The incoming wrapped key shall have a key purpose of D0 with a mode of use of B or D. For more information, see [Using Dynamic Keys](#) in the *AWS Payment Cryptography User Guide*.

For symmetric and DUKPT encryption, AWS Payment Cryptography supports TDES and AES algorithms. For EMV encryption, AWS Payment Cryptography supports TDES algorithms. For asymmetric encryption, AWS Payment Cryptography supports RSA.

When you use TDES or TDES DUKPT, the plaintext data length must be a multiple of 8 bytes. For AES or AES DUKPT, the plaintext data length must be a multiple of 16 bytes. For RSA, it could be equal to the key size unless padding is enabled.

To encrypt using DUKPT, you must already have a BDK (Base Derivation Key) key in your account with `KeyModesOfUse` set to `DeriveKey`, or you can generate a new DUKPT key by calling [CreateKey](#). To encrypt using EMV, you must already have an IMK (Issuer Master Key) key in your account with `KeyModesOfUse` set to `DeriveKey`.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [DecryptData](#)
- [GetPublicCertificate](#)
- [ImportKey](#)
- [ReEncryptData](#)

Request Syntax

```
POST /keys/KeyIdentifier/encrypt HTTP/1.1
Content-type: application/json
```

```
{
  "EncryptionAttributes": { ... },
  "PlainText": "string",
  "WrappedKey": {
    "KeyCheckValueAlgorithm": "string",
    "WrappedKeyMaterial": { ... }
  }
}
```

URI Request Parameters

The request uses the following URI parameters.

[KeyIdentifier](#)

The keyARN of the encryption key that AWS Payment Cryptography uses for plaintext encryption.

When a WrappedKeyBlock is provided, this value will be the identifier to the key wrapping key. Otherwise, it is the key identifier used to perform the operation.

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

Request Body

The request accepts the following data in JSON format.

EncryptionAttributes

The encryption key type and attributes for plaintext encryption.

Type: [EncryptionDecryptionAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

PlainText

The plaintext to be encrypted.

Note

For encryption using asymmetric keys, plaintext data length is constrained by encryption key strength that you define in `KeyAlgorithm` and padding type that you define in `AsymmetricEncryptionAttributes`. For more information, see [Encrypt data](#) in the *AWS Payment Cryptography User Guide*.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4096.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

Required: Yes

WrappedKey

The `WrappedKeyBlock` containing the encryption key for plaintext encryption.

Type: [WrappedKey](#) object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CipherText": "string",
  "KeyArn": "string",
  "KeyCheckValue": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CipherText

The encrypted ciphertext.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4224.

Pattern: (?:[0-9a-fA-F][0-9a-fA-F])+

KeyArn

The keyARN of the encryption key that AWS Payment Cryptography uses for plaintext encryption.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

GenerateAs2805KekValidation

Generates a `KekValidationRequest` or a `KekValidationResponse` for node-to-node initialization between payment processing nodes using [Australian Standard 2805 \(AS2805\)](#).

During node-to-node initialization, both communicating nodes must validate that they possess the correct Key Encrypting Keys (KEKs) before proceeding with session key exchange. In AS2805, the sending KEK (KEKs) of one node corresponds to the receiving KEK (KEKr) of its partner node. Each node uses its KEK to encrypt and decrypt session keys exchanged between the nodes. A KEK can be created or imported into AWS Payment Cryptography using either the [CreateKey](#) or [ImportKey](#) operations.

To use `GenerateAs2805KekValidation` to generate a KEK validation request, set `KekValidationType` to `KekValidationRequest`. This operation returns both `RandomKeySend` (KRs) and `RandomKeyReceive` (KRr) as response values. The partnering node receives the KRs, uses its KEKr to decrypt it, and generates a KRr which is an inverted value of KRs. The node receiving the KRr validates it against its own KRr generated during KEK validation request outside of AWS Payment Cryptography.

You can also use this operation to generate a KEK validation response, by setting `KekValidationType` to `KekValidationResponse` and providing the incoming KRs. This operation then calculates a KRr. To learn more about more about node-to-node initialization, see [Validation of KEK](#) in the *AWS Payment Cryptography User Guide*.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Request Syntax

```
POST /as2805kekvalidation/generate HTTP/1.1
Content-type: application/json

{
  "KekValidationType": { ... },
  "KeyIdentifier": "string",
  "RandomKeySendVariantMask": "string"
```

```
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

KekValidationType

Defines whether to generate a KEK validation request or KEK validation response for node-to-node initialization.

Type: [As2805KekValidationType](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

KeyIdentifier

The keyARN of sending KEK that AWS Payment Cryptography uses for node-to-node initialization

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

RandomKeySendVariantMask

The key variant to use for generating a random key for KEK validation during node-to-node initialization.

Type: String

Valid Values: `VARIANT_MASK_82C0` | `VARIANT_MASK_82`

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "KeyArn": "string",
  "KeyCheckValue": "string",
  "RandomKeyReceive": "string",
  "RandomKeySend": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

KeyArn

The keyARN of sending KEK that AWS Payment Cryptography validates for node-to-node initialization

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the sending KEK that AWS Payment Cryptography validates for node-to-node initialization.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

RandomKeyReceive

The random key generated for receiving KEK validation. The initiating node sends this key to its partner node for validation.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 48.

Pattern: (?:[0-9a-fA-F]{16}|[0-9a-fA-F]{32}|[0-9a-fA-F]{48})

RandomKeySend

The random key generated for sending KEK validation.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 48.

Pattern: (?:[0-9a-fA-F]{16}|[0-9a-fA-F]{32}|[0-9a-fA-F]{48})

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

GenerateAuthRequestCryptogram

Generates an Authorization Request Cryptogram (ARQC) for an EMV chip payment card authorization. For more information, see [Generate auth request cryptogram](#) in the *AWS Payment Cryptography User Guide*.

ARQC generation uses an Issuer Master Key (IMK) for application cryptograms (TR31_E0_EMV_MKEY_APP_CRYPTGRAMS) to derive a session key, which is then used to generate the cryptogram from the provided transaction data (when applicable). To use this operation, you must first create or import an IMK-AC key by calling [CreateKey](#) or [ImportKey](#). The `KeyModesOfUse` should be set to `DeriveKey` for the IMK-AC encryption key.

Important

This operation is intended for development and testing scenarios only. It is not recommended to use this operation as a substitute for card-based cryptogram generation in production payment flows.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [VerifyAuthRequestCryptogram](#)

Request Syntax

```
POST /cryptogram/generate HTTP/1.1
Content-type: application/json

{
  "KeyIdentifier": "string",
  "MajorKeyDerivationMode": "string",
  "SessionKeyDerivationAttributes": { ... },
  "TransactionData": "string"
```

```
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

KeyIdentifier

The keyARN of the IMK-AC (TR31_E0_EMV_MKEY_APP_CRYPTOGRAMS) that AWS Payment Cryptography uses to generate the ARQC.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

MajorKeyDerivationMode

The method to use when deriving the major encryption key for ARQC generation within AWS Payment Cryptography.

Type: String

Valid Values: `EMV_OPTION_A` | `EMV_OPTION_B`

Required: Yes

SessionKeyDerivationAttributes

The attributes and values to use for deriving a session key for ARQC generation within AWS Payment Cryptography.

Type: [SessionKeyDerivation](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

TransactionData

The transaction data that AWS Payment Cryptography uses for ARQC generation.

The same transaction data is used for ARQC verification by the issuer using [VerifyAuthRequestCryptogram](#).

Type: String

Length Constraints: Minimum length of 2. Maximum length of 1024.

Pattern: [0-9a-fA-F]+

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "AuthRequestCryptogram": "string",
  "KeyArn": "string",
  "KeyCheckValue": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AuthRequestCryptogram

The Authorization Request Cryptogram (ARQC) generated by AWS Payment Cryptography using the specified key and transaction data.

Type: String

Length Constraints: Fixed length of 16.

Pattern: `[0-9a-fA-F]+`

KeyArn

The keyARN of the IMK-AC that AWS Payment Cryptography uses for ARQC generation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

GenerateCardValidationData

Generates card-related validation data using algorithms such as Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2), or Card Security Codes (CSC). For more information, see [Generate card data](#) in the *AWS Payment Cryptography User Guide*.

This operation generates a CVV or CSC value that is printed on a payment credit or debit card during card production. The CVV or CSC, PAN (Primary Account Number) and expiration date of the card are required to check its validity during transaction processing. To begin this operation, a CVK (Card Verification Key) encryption key is required. You can use [CreateKey](#) or [ImportKey](#) to establish a CVK within AWS Payment Cryptography. The KeyModesOfUse should be set to Generate and Verify for a CVK encryption key.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [ImportKey](#)
- [VerifyCardValidationData](#)

Request Syntax

```
POST /cardvalidationdata/generate HTTP/1.1
Content-type: application/json
```

```
{
  "GenerationAttributes": { ... },
  "KeyIdentifier": "string",
  "PrimaryAccountNumber": "string",
  "ValidationDataLength": number
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GenerationAttributes

The algorithm for generating CVV or CSC values for the card within AWS Payment Cryptography.

Type: [CardGenerationAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

KeyIdIdentifier

The keyARN of the CVK encryption key that AWS Payment Cryptography uses to generate card data.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN), a unique identifier for a payment credit or debit card that associates the card with a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: `[0-9]+`

Required: Yes

ValidationDataLength

The length of the CVV or CSC to be generated. The default value is 3.

Type: Integer

Valid Range: Minimum value of 3. Maximum value of 5.

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "KeyArn": "string",
  "KeyCheckValue": "string",
  "ValidationData": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

KeyArn

The keyARN of the CVK encryption key that AWS Payment Cryptography uses to generate CVV or CSC.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

ValidationData

The CVV or CSC value that AWS Payment Cryptography generates for the card.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 5.

Pattern: `[0-9]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerError

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

GenerateMac

Generates a Message Authentication Code (MAC) cryptogram within AWS Payment Cryptography.

You can use this operation to authenticate card-related data by using known data values to generate MAC for data validation between the sending and receiving parties. This operation uses message data, a secret encryption key and MAC algorithm to generate a unique MAC value for transmission. The receiving party of the MAC must use the same message data, secret encryption key and MAC algorithm to reproduce another MAC value for comparison.

You can use this operation to generate a DUPKT, CMAC, HMAC or EMV MAC by setting generation attributes and algorithm to the associated values. The MAC generation encryption key must have valid values for KeyUsage such as TR31_M7_HMAC_KEY for HMAC generation, and the key must have KeyModesOfUse set to Generate.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [VerifyMac](#)

Request Syntax

```
POST /mac/generate HTTP/1.1
Content-type: application/json

{
  "GenerationAttributes": { ... },
  "KeyIdentifier": "string",
  "MacLength": number,
  "MessageData": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

GenerationAttributes

The attributes and data values to use for MAC generation within AWS Payment Cryptography.

Type: [MacAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

KeyIdIdentifier

The keyARN of the MAC generation encryption key.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

MacLength

The length of a MAC under generation.

Type: Integer

Valid Range: Minimum value of 4. Maximum value of 32.

Required: No

MessageData

The data for which a MAC is under generation. This value must be hexBinary.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 8192.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "KeyArn": "string",
  "KeyCheckValue": "string",
  "Mac": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

KeyArn

The keyARN of the encryption key that AWS Payment Cryptography uses for MAC generation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Mac

The MAC cryptogram generated within AWS Payment Cryptography.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 128.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

GenerateMacEmvPinChange

Generates an issuer script mac for EMV payment cards that use offline PINs as the cardholder verification method (CVM).

This operation generates an authenticated issuer script response by appending the incoming message data (APDU command) with the target encrypted PIN block in ISO2 format. The command structure and method to send the issuer script update to the card is not defined by this operation and is typically determined by the applicable payment card scheme.

The primary inputs to this operation include the incoming new encrypted pinblock, PIN encryption key (PEK), issuer master key (IMK), primary account number (PAN), and the payment card derivation method.

The operation uses two issuer master keys - secure messaging for confidentiality (IMK-SMC) and secure messaging for integrity (IMK-SMI). The SMC key is used to internally derive a key to secure the pin, while SMI key is used to internally derive a key to authenticate the script response as per the [EMV 4.4 - Book 2 - Security and Key Management](#) specification.

This operation supports Amex, EMV2000, EMVCommon, Mastercard and Visa derivation methods, each requiring specific input parameters. Users must follow the specific derivation method and input parameters defined by the respective payment card scheme.

Note

Use [GenerateMac](#) operation when sending a script update to an EMV card that does not involve PIN change. When assigning IAM permissions, it is important to understand that [EncryptData](#) using EMV keys and [GenerateMac](#) perform similar functions to this command.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [EncryptData](#)
- [GenerateMac](#)

Request Syntax

```
POST /macemvpinchange/generate HTTP/1.1
Content-type: application/json

{
  "DerivationMethodAttributes": { ... },
  "MessageData": "string",
  "NewEncryptedPinBlock": "string",
  "NewPinPekIdentifier": "string",
  "PinBlockFormat": "string",
  "SecureMessagingConfidentialityKeyIdentifier": "string",
  "SecureMessagingIntegrityKeyIdentifier": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

DerivationMethodAttributes

The attributes and data values to derive payment card specific confidentiality and integrity keys.

Type: [DerivationMethodAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

MessageData

The message data is the APDU command from the card reader or terminal. The target encrypted PIN block, after translation to ISO2 format, is appended to this message data to generate an issuer script response.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 1024.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

Required: Yes

NewEncryptedPinBlock

The incoming new encrypted PIN block data for offline pin change on an EMV card.

Type: String

Length Constraints: Fixed length of 16.

Pattern: `[0-9a-fA-F]+`

Required: Yes

NewPinPekIdentifier

The keyARN of the PEK protecting the incoming new encrypted PIN block.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

PinBlockFormat

The PIN encoding format of the incoming new encrypted PIN block as specified in ISO 9564.

Type: String

Valid Values: `ISO_FORMAT_0` | `ISO_FORMAT_1` | `ISO_FORMAT_3`

Required: Yes

SecureMessagingConfidentialityKeyIdentifier

The keyARN of the issuer master key (IMK-SMC) used to protect the PIN block data in the issuer script response.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

SecureMessagingIntegrityKeyIdentifier

The keyARN of the issuer master key (IMK-SMI) used to authenticate the issuer script response.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

Response Syntax

HTTP/1.1 200

Content-type: application/json

```
{
  "EncryptedPinBlock": "string",
  "Mac": "string",
  "NewPinPekArn": "string",
  "NewPinPekKeyCheckValue": "string",
  "SecureMessagingConfidentialityKeyArn": "string",
  "SecureMessagingConfidentialityKeyCheckValue": "string",
  "SecureMessagingIntegrityKeyArn": "string",
  "SecureMessagingIntegrityKeyCheckValue": "string",
  "VisaAmexDerivationOutputs": {
    "AuthorizationRequestKeyArn": "string",
    "AuthorizationRequestKeyCheckValue": "string",
    "CurrentPinPekArn": "string",
    "CurrentPinPekKeyCheckValue": "string"
  }
}
```

```
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

EncryptedPinBlock

Returns the incoming new encrypted PIN block.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[0-9a-fA-F]+`

Mac

Returns the mac of the issuer script containing message data and appended target encrypted pin block in ISO2 format.

Type: String

Length Constraints: Minimum length of 8. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

NewPinPekArn

Returns the keyArn of the PEK protecting the incoming new encrypted PIN block.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

NewPinPekKeyCheckValue

The key check value (KCV) of the PEK uprotecting the incoming new encrypted PIN block.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

[SecureMessagingConfidentialityKeyArn](#)

Returns the keyArn of the IMK-SMC used by the operation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

[SecureMessagingConfidentialityKeyCheckValue](#)

The key check value (KCV) of the SMC issuer master key used by the operation.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

[SecureMessagingIntegrityKeyArn](#)

Returns the keyArn of the IMK-SMI used by the operation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

[SecureMessagingIntegrityKeyCheckValue](#)

The key check value (KCV) of the SMI issuer master key used by the operation.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

VisaAmexDerivationOutputs

The attribute values used for Amex and Visa derivation methods.

Type: [VisaAmexDerivationOutputs](#) object

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerError

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

GeneratePinData

Generates pin-related data such as PIN, PIN Verification Value (PVV), PIN Block, and PIN Offset during new card issuance or reissuance. For more information, see [Generate PIN data](#) in the *AWS Payment Cryptography User Guide*.

PIN data is never transmitted in clear to or from AWS Payment Cryptography. This operation generates PIN, PVV, or PIN Offset and then encrypts it using Pin Encryption Key (PEK) to create an EncryptedPinBlock for transmission from AWS Payment Cryptography. This operation uses a separate Pin Verification Key (PVK) for VISA PVV generation.

Using ECDH key exchange, you can receive cardholder selectable PINs into AWS Payment Cryptography. The ECDH derived key protects the incoming PIN block. You can also use it for reveal PIN, wherein the generated PIN block is protected by the ECDH derived key before transmission from AWS Payment Cryptography. For more information on establishing ECDH derived keys, see the [Generating keys](#) in the *AWS Payment Cryptography User Guide*.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [GenerateCardValidationData](#)
- [TranslatePinData](#)
- [VerifyPinData](#)

Request Syntax

```
POST /pindata/generate HTTP/1.1
Content-type: application/json

{
  "EncryptionKeyIdentifier": "string",
  "EncryptionWrappedKey": {
    "KeyCheckValueAlgorithm": "string",
    "WrappedKeyMaterial": { ... }
```

```
{,
  "GenerationAttributes": { ... },
  "GenerationKeyIdentifier": "string",
  "PinBlockFormat": "string",
  "PinDataLength": number,
  "PrimaryAccountNumber": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

EncryptionKeyIdentifier

The keyARN of the PEK that AWS Payment Cryptography uses to encrypt the PIN Block. For ECDH, it is the keyARN of the asymmetric ECC key.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

EncryptionWrappedKey

Parameter information of a WrappedKeyBlock for encryption key exchange.

Type: [WrappedKey](#) object

Required: No

GenerationAttributes

The attributes and values to use for PIN, PVV, or PIN Offset generation.

Type: [PinGenerationAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

GenerationKeyIdentifier

The keyARN of the PEK that AWS Payment Cryptography uses for pin data generation.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

PinBlockFormat

The PIN encoding format for pin data generation as specified in ISO 9564. AWS Payment Cryptography supports ISO_Format_0, ISO_Format_3 and ISO_Format_4.

The ISO_Format_0 PIN block format is equivalent to the ANSI X9.8, VISA-1, and ECI-1 PIN block formats. It is similar to a VISA-4 PIN block format. It supports a PIN from 4 to 12 digits in length.

The ISO_Format_3 PIN block format is the same as ISO_Format_0 except that the fill digits are random values from 10 to 15.

The ISO_Format_4 PIN block format is the only one supporting AES encryption.

Type: String

Valid Values: ISO_FORMAT_0 | ISO_FORMAT_1 | ISO_FORMAT_3 | ISO_FORMAT_4

Required: Yes

PinDataLength

The length of PIN under generation.

Type: Integer

Valid Range: Minimum value of 4. Maximum value of 12.

Required: No

PrimaryAccountNumber

The Primary Account Number (PAN), a unique identifier for a payment credit or debit card that associates the card with a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9] +

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "EncryptedPinBlock": "string",
  "EncryptionKeyArn": "string",
  "EncryptionKeyCheckValue": "string",
  "GenerationKeyArn": "string",
  "GenerationKeyCheckValue": "string",
  "PinData": { ... }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

EncryptedPinBlock

The PIN block encrypted under PEK from AWS Payment Cryptography. The encrypted PIN block is a composite of PAN (Primary Account Number) and PIN (Personal Identification Number), generated in accordance with ISO 9564 standard.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[0-9a-fA-F]+`

EncryptionKeyArn

The keyARN of the PEK that AWS Payment Cryptography uses for encrypted pin block generation. For ECDH, it is the keyARN of the asymmetric ECC key.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

EncryptionKeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

GenerationKeyArn

The keyARN of the pin data generation key that AWS Payment Cryptography uses for PIN, PVV or PIN Offset generation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

GenerationKeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

PinData

The attributes and values AWS Payment Cryptography uses for pin data generation.

Type: [PinData](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

ReEncryptData

Re-encrypt ciphertext using DUKPT or Symmetric data encryption keys.

You can either generate an encryption key within AWS Payment Cryptography by calling [CreateKey](#) or import your own encryption key by calling [ImportKey](#). The KeyArn for use with this operation must be in a compatible key state with KeyModesOfUse set to Encrypt.

This operation also supports dynamic keys, allowing you to pass a dynamic encryption key as a TR-31 WrappedKeyBlock. This can be used when key material is frequently rotated, such as during every card transaction, and there is need to avoid importing short-lived keys into AWS Payment Cryptography. To re-encrypt using dynamic keys, the keyARN is the Key Encryption Key (KEK) of the TR-31 wrapped encryption key material. The incoming wrapped key shall have a key purpose of D0 with a mode of use of B or D. For more information, see [Using Dynamic Keys](#) in the *AWS Payment Cryptography User Guide*.

For symmetric and DUKPT encryption, AWS Payment Cryptography supports TDES and AES algorithms. To encrypt using DUKPT, a DUKPT key must already exist within your account with KeyModesOfUse set to DeriveKey or a new DUKPT can be generated by calling [CreateKey](#).

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [DecryptData](#)
- [EncryptData](#)
- [GetPublicCertificate](#)
- [ImportKey](#)

Request Syntax

```
POST /keys/IncomingKeyIdentifier/reencrypt HTTP/1.1
Content-type: application/json
```

```
{
  "CipherText": "string",
  "IncomingEncryptionAttributes": { ... },
  "IncomingWrappedKey": {
    "KeyCheckValueAlgorithm": "string",
    "WrappedKeyMaterial": { ... }
  },
  "OutgoingEncryptionAttributes": { ... },
  "OutgoingKeyIdentifier": "string",
  "OutgoingWrappedKey": {
    "KeyCheckValueAlgorithm": "string",
    "WrappedKeyMaterial": { ... }
  }
}
```

URI Request Parameters

The request uses the following URI parameters.

IncomingKeyIdentifier

The keyARN of the encryption key of incoming ciphertext data.

When a WrappedKeyBlock is provided, this value will be the identifier to the key wrapping key. Otherwise, it is the key identifier used to perform the operation.

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

Request Body

The request accepts the following data in JSON format.

CipherText

Ciphertext to be encrypted. The minimum allowed length is 16 bytes and maximum allowed length is 4096 bytes.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4224.

Pattern: (?:[0-9a-fA-F][0-9a-fA-F])+

Required: Yes

IncomingEncryptionAttributes

The attributes and values for incoming ciphertext.

Type: [ReEncryptionAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

IncomingWrappedKey

The WrappedKeyBlock containing the encryption key of incoming ciphertext data.

Type: [WrappedKey](#) object

Required: No

OutgoingEncryptionAttributes

The attributes and values for outgoing ciphertext data after encryption by AWS Payment Cryptography.

Type: [ReEncryptionAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

OutgoingKeyIdentifier

The keyARN of the encryption key of outgoing ciphertext data after encryption by AWS Payment Cryptography.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

OutgoingWrappedKey

The WrappedKeyBlock containing the encryption key of outgoing ciphertext data after encryption by AWS Payment Cryptography.

Type: [WrappedKey](#) object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "CipherText": "string",
  "KeyArn": "string",
  "KeyCheckValue": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CipherText

The encrypted ciphertext.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4224.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

KeyArn

The keyARN (Amazon Resource Name) of the encryption key that AWS Payment Cryptography uses for plaintext encryption.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

TranslateKeyMaterial

Translates an cryptographic key between different wrapping keys without importing the key into AWS Payment Cryptography.

This operation can be used when key material is frequently rotated, such as during every card transaction, and there is a need to avoid importing short-lived keys into AWS Payment Cryptography. It translates short-lived transaction keys such as [PEK](#) generated for each transaction and wrapped with an [ECDH](#) derived wrapping key to another [KEK](#) wrapping key.

Before using this operation, you must first request the public key certificate of the ECC key pair generated within AWS Payment Cryptography to establish an ECDH key agreement. In `TranslateKeyData`, the service uses its own ECC key pair, public certificate of receiving ECC key pair, and the key derivation parameters to generate a derived key. The service uses this derived key to unwrap the incoming transaction key received as a `TR31WrappedKeyBlock` and re-wrap using a user provided KEK to generate an outgoing `Tr31WrappedKeyBlock`.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [CreateKey](#)
- [GetPublicCertificate](#)
- [ImportKey](#)

Request Syntax

```
POST /keymaterial/translate HTTP/1.1
Content-type: application/json

{
  "IncomingKeyMaterial": { ... },
  "KeyCheckValueAlgorithm": "string",
  "OutgoingKeyMaterial": { ... }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

IncomingKeyMaterial

Parameter information of the TR31WrappedKeyBlock containing the transaction key.

Type: [IncomingKeyMaterial](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

KeyCheckValueAlgorithm

The key check value (KCV) algorithm used for calculating the KCV of the derived key.

Type: String

Valid Values: CMAC | ANSI_X9_24 | HMAC | SHA_1

Required: No

OutgoingKeyMaterial

Parameter information of the wrapping key used to wrap the transaction key in the outgoing TR31WrappedKeyBlock.

Type: [OutgoingKeyMaterial](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
  "WrappedKey": {
    "KeyCheckValue": "string",
    "WrappedKeyMaterial": "string",
    "WrappedKeyMaterialFormat": "string"
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

[WrappedKey](#)

The outgoing KEK wrapped TR31WrappedKeyBlock.

Type: [WrappedWorkingKey](#) object

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

TranslatePinData

Translates encrypted PIN block from and to ISO 9564 formats 0,1,3,4. For more information, see [Translate PIN data](#) in the *AWS Payment Cryptography User Guide*.

PIN block translation involves changing a PIN block from one encryption key to another and optionally change its format. PIN block translation occurs entirely within the HSM boundary and PIN data never enters or leaves AWS Payment Cryptography in clear text. The encryption key transformation can be from PEK (Pin Encryption Key) to BDK (Base Derivation Key) for DUKPT or from BDK for DUKPT to PEK.

AWS Payment Cryptography also supports use of dynamic keys and ECDH (Elliptic Curve Diffie-Hellman) based key exchange for this operation.

Dynamic keys allow you to pass a PEK as a TR-31 WrappedKeyBlock. They can be used when key material is frequently rotated, such as during every card transaction, and there is need to avoid importing short-lived keys into AWS Payment Cryptography. To translate PIN block using dynamic keys, the keyARN is the Key Encryption Key (KEK) of the TR-31 wrapped PEK. The incoming wrapped key shall have a key purpose of P0 with a mode of use of B or D. For more information, see [Using Dynamic Keys](#) in the *AWS Payment Cryptography User Guide*.

Using ECDH key exchange, you can receive cardholder selectable PINs into AWS Payment Cryptography. The ECDH derived key protects the incoming PIN block, which is translated to a PEK encrypted PIN block for use within the service. You can also use ECDH for reveal PIN, wherein the service translates the PIN block from PEK to a ECDH derived encryption key. For more information on establishing ECDH derived keys, see the [Creating keys](#) in the *AWS Payment Cryptography User Guide*.

The allowed combinations of PIN block format translations are guided by PCI. It is important to note that not all encrypted PIN block formats (example, format 1) require PAN (Primary Account Number) as input. And as such, PIN block format that requires PAN (example, formats 0,3,4) cannot be translated to a format (format 1) that does not require a PAN for generation.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Note

AWS Payment Cryptography currently supports ISO PIN block 4 translation for PIN block built using legacy PAN length. That is, PAN is the right most 12 digits excluding the check digits.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [GeneratePinData](#)
- [VerifyPinData](#)

Request Syntax

```
POST /pindata/translate HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "EncryptedPinBlock": "string",
  "IncomingAs2805Attributes": {
    "SystemTraceAuditNumber": "string",
    "TransactionAmount": "string"
  },
  "IncomingDukptAttributes": {
    "DukptKeyDerivationType": "string",
    "DukptKeyVariant": "string",
    "KeySerialNumber": "string"
  },
  "IncomingKeyIdentifier": "string",
  "IncomingTranslationAttributes": { ... },
  "IncomingWrappedKey": {
    "KeyCheckValueAlgorithm": "string",
    "WrappedKeyMaterial": { ... }
  },
  "OutgoingDukptAttributes": {
    "DukptKeyDerivationType": "string",
    "DukptKeyVariant": "string",
    "KeySerialNumber": "string"
  }
}
```

```
  },  
  "OutgoingKeyIdentifier": "string",  
  "OutgoingTranslationAttributes": { ... },  
  "OutgoingWrappedKey": {  
    "KeyCheckValueAlgorithm": "string",  
    "WrappedKeyMaterial": { ... }  
  }  
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

EncryptedPinBlock

The encrypted PIN block data that AWS Payment Cryptography translates.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: (?:[0-9a-fA-F][0-9a-fA-F])+

Required: Yes

IncomingAs2805Attributes

The attributes and values to use for incoming AS2805 encryption key for PIN block translation.

Type: [As2805PekDerivationAttributes](#) object

Required: No

IncomingDukptAttributes

The attributes and values to use for incoming DUKPT encryption key for PIN block translation.

Type: [DukptDerivationAttributes](#) object

Required: No

IncomingKeyIdentifier

The keyARN of the encryption key under which incoming PIN block data is encrypted. This key type can be PEK or BDK.

For dynamic keys, it is the keyARN of KEK of the TR-31 wrapped PEK. For ECDH, it is the keyARN of the asymmetric ECC key.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

IncomingTranslationAttributes

The format of the incoming PIN block data for translation within AWS Payment Cryptography.

Type: [TranslationIsoFormats](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

IncomingWrappedKey

The WrappedKeyBlock containing the encryption key under which incoming PIN block data is encrypted.

Type: [WrappedKey](#) object

Required: No

OutgoingDukptAttributes

The attributes and values to use for outgoing DUKPT encryption key after PIN block translation.

Type: [DukptDerivationAttributes](#) object

Required: No

OutgoingKeyIdentifier

The keyARN of the encryption key for encrypting outgoing PIN block data. This key type can be PEK or BDK.

For ECDH, it is the keyARN of the asymmetric ECC key.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

OutgoingTranslationAttributes

The format of the outgoing PIN block data after translation by AWS Payment Cryptography.

Type: [TranslationIsoFormats](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

OutgoingWrappedKey

The WrappedKeyBlock containing the encryption key for encrypting outgoing PIN block data.

Type: [WrappedKey](#) object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "KeyArn": "string",
  "KeyCheckValue": "string",
```

```
"PinBlock": "string"  
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

KeyArn

The keyARN of the encryption key that AWS Payment Cryptography uses to encrypt outgoing PIN block data after translation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

PinBlock

The outgoing encrypted PIN block data after translation.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)

- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

VerifyAuthRequestCryptogram

Verifies Authorization Request Cryptogram (ARQC) for a EMV chip payment card authorization. For more information, see [Verify auth request cryptogram](#) in the *AWS Payment Cryptography User Guide*.

ARQC generation is done outside of AWS Payment Cryptography and is typically generated on a point of sale terminal for an EMV chip card to obtain payment authorization during transaction time. For ARQC verification, you must first import the ARQC generated outside of AWS Payment Cryptography by calling [ImportKey](#). This operation uses the imported ARQC and an major encryption key (DUKPT) created by calling [CreateKey](#) to either provide a boolean ARQC verification result or provide an ARPC (Authorization Response Cryptogram) response using Method 1 or Method 2. The ARPC_METHOD_1 uses AuthResponseCode to generate ARPC and ARPC_METHOD_2 uses CardStatusUpdate to generate ARPC.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [VerifyCardValidationData](#)
- [VerifyPinData](#)

Request Syntax

```
POST /cryptogram/verify HTTP/1.1
Content-type: application/json

{
  "AuthRequestCryptogram": "string",
  "AuthResponseAttributes": { ... },
  "KeyIdentifier": "string",
  "MajorKeyDerivationMode": "string",
  "SessionKeyDerivationAttributes": { ... },
  "TransactionData": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

AuthRequestCryptogram

The auth request cryptogram imported into AWS Payment Cryptography for ARQC verification using a major encryption key and transaction data.

Type: String

Length Constraints: Fixed length of 16.

Pattern: `[0-9a-fA-F]+`

Required: Yes

AuthResponseAttributes

The attributes and values for auth request cryptogram verification. These parameters are required in case using ARPC Method 1 or Method 2 for ARQC verification.

Type: [CryptogramAuthResponse](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

KeyIdIdentifier

The keyARN of the major encryption key that AWS Payment Cryptography uses for ARQC verification.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

MajorKeyDerivationMode

The method to use when deriving the major encryption key for ARQC verification within AWS Payment Cryptography. The same key derivation mode was used for ARQC generation outside of AWS Payment Cryptography.

Type: String

Valid Values: EMV_OPTION_A | EMV_OPTION_B

Required: Yes

SessionKeyDerivationAttributes

The attributes and values to use for deriving a session key for ARQC verification within AWS Payment Cryptography. The same attributes were used for ARQC generation outside of AWS Payment Cryptography.

Type: [SessionKeyDerivation](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

TransactionData

The transaction data that AWS Payment Cryptography uses for ARQC verification. The same transaction is used for ARQC generation outside of AWS Payment Cryptography.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 1024.

Pattern: [0-9a-fA-F] +

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
  "AuthResponseValue": "string",
  "KeyArn": "string",
  "KeyCheckValue": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AuthResponseValue

The result for ARQC verification or ARPC generation within AWS Payment Cryptography.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16.

Pattern: [0-9a-fA-F]+

KeyArn

The keyARN of the major encryption key that AWS Payment Cryptography uses for ARQC verification.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

VerificationFailedException

This request failed verification.

Reason

The reason for the exception.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

VerifyCardValidationData

Verifies card-related validation data using algorithms such as Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) and Card Security Codes (CSC). For more information, see [Verify card data](#) in the *AWS Payment Cryptography User Guide*.

This operation validates the CVV or CSC codes that is printed on a payment credit or debit card during card payment transaction. The input values are typically provided as part of an inbound transaction to an issuer or supporting platform partner. AWS Payment Cryptography uses CVV or CSC, PAN (Primary Account Number) and expiration date of the card to check its validity during transaction processing. In this operation, the CVK (Card Verification Key) encryption key for use with card data verification is same as the one in used for [GenerateCardValidationData](#).

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [GenerateCardValidationData](#)
- [VerifyAuthRequestCryptogram](#)
- [VerifyPinData](#)

Request Syntax

```
POST /cardvalidationdata/verify HTTP/1.1
Content-type: application/json
```

```
{
  "KeyIdentifier": "string",
  "PrimaryAccountNumber": "string",
  "ValidationData": "string",
  "VerificationAttributes": { ... }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

KeyIdentifier

The keyARN of the CVK encryption key that AWS Payment Cryptography uses to verify card data.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN), a unique identifier for a payment credit or debit card that associates the card with a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: `[0-9]+`

Required: Yes

ValidationData

The CVV or CSC value for use for card data verification within AWS Payment Cryptography.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 5.

Pattern: `[0-9]+`

Required: Yes

VerificationAttributes

The algorithm to use for verification of card data within AWS Payment Cryptography.

Type: [CardVerificationAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "KeyArn": "string",
  "KeyCheckValue": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

KeyArn

The keyARN of the CVK encryption key that AWS Payment Cryptography uses to verify CVV or CSC.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

VerificationFailedException

This request failed verification.

Reason

The reason for the exception.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

VerifyMac

Verifies a Message Authentication Code (MAC).

You can use this operation to verify MAC for message data authentication such as . In this operation, you must use the same message data, secret encryption key and MAC algorithm that was used to generate MAC. You can use this operation to verify a DUPKT, CMAC, HMAC or EMV MAC by setting generation attributes and algorithm to the associated values.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [GenerateMac](#)

Request Syntax

```
POST /mac/verify HTTP/1.1
Content-type: application/json

{
  "KeyIdentifier": "string",
  "Mac": "string",
  "MacLength": number,
  "MessageData": "string",
  "VerificationAttributes": { ... }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

KeyIdIdentifier

The keyARN of the encryption key that AWS Payment Cryptography uses to verify MAC data.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

Mac

The MAC being verified.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 128.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

Required: Yes

MacLength

The length of the MAC.

Type: Integer

Valid Range: Minimum value of 4. Maximum value of 32.

Required: No

MessageData

The data on for which MAC is under verification. This value must be hexBinary.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 8192.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

Required: Yes

VerificationAttributes

The attributes and data values to use for MAC verification within AWS Payment Cryptography.

Type: [MacAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "KeyArn": "string",
  "KeyCheckValue": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

KeyArn

The keyARN of the encryption key that AWS Payment Cryptography uses for MAC verification.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

KeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerErrorException

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

VerificationFailedException

This request failed verification.

Reason

The reason for the exception.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

VerifyPinData

Verifies pin-related data such as PIN and PIN Offset using algorithms including VISA PVV and IBM3624. For more information, see [Verify PIN data](#) in the *AWS Payment Cryptography User Guide*.

This operation verifies PIN data for user payment card. A card holder PIN data is never transmitted in clear to or from AWS Payment Cryptography. This operation uses PIN Verification Key (PVK) for PIN or PIN Offset generation and then encrypts it using PIN Encryption Key (PEK) to create an EncryptedPinBlock for transmission from AWS Payment Cryptography.

For information about valid keys for this operation, see [Understanding key attributes](#) and [Key types for specific data operations](#) in the *AWS Payment Cryptography User Guide*.

Cross-account use: This operation supports cross-account use when the key has a resource-based policy that grants access. For more information, see [Resource-based policies](#).

Related operations:

- [GeneratePinData](#)
- [TranslatePinData](#)

Request Syntax

```
POST /pindata/verify HTTP/1.1
Content-type: application/json

{
  "DukptAttributes": {
    "DukptDerivationType": "string",
    "KeySerialNumber": "string"
  },
  "EncryptedPinBlock": "string",
  "EncryptionKeyIdentifier": "string",
  "EncryptionWrappedKey": {
    "KeyCheckValueAlgorithm": "string",
    "WrappedKeyMaterial": { ... }
  },
  "PinBlockFormat": "string",
  "PinDataLength": number,
  "PrimaryAccountNumber": "string",
```

```
"VerificationAttributes": { ... },  
"VerificationKeyIdentifier": "string"  
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

DukptAttributes

The attributes and values for the DUKPT encrypted PIN block data.

Type: [DukptAttributes](#) object

Required: No

EncryptedPinBlock

The encrypted PIN block data that AWS Payment Cryptography verifies.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[0-9a-fA-F]+`

Required: Yes

EncryptionKeyIdentifier

The keyARN of the encryption key under which the PIN block data is encrypted. This key type can be PEK or BDK.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

EncryptionWrappedKey

Parameter information of a WrappedKeyBlock for encryption key exchange.

Type: [WrappedKey](#) object

Required: No

PinBlockFormat

The PIN encoding format for pin data generation as specified in ISO 9564. AWS Payment Cryptography supports ISO_Format_0 and ISO_Format_3.

The ISO_Format_0 PIN block format is equivalent to the ANSI X9.8, VISA-1, and ECI-1 PIN block formats. It is similar to a VISA-4 PIN block format. It supports a PIN from 4 to 12 digits in length.

The ISO_Format_3 PIN block format is the same as ISO_Format_0 except that the fill digits are random values from 10 to 15.

Type: String

Valid Values: ISO_FORMAT_0 | ISO_FORMAT_1 | ISO_FORMAT_3 | ISO_FORMAT_4

Required: Yes

PinDataLength

The length of PIN being verified.

Type: Integer

Valid Range: Minimum value of 4. Maximum value of 12.

Required: No

PrimaryAccountNumber

The Primary Account Number (PAN), a unique identifier for a payment credit or debit card that associates the card with a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: `[0-9]+`

Required: No

VerificationAttributes

The attributes and values for PIN data verification.

Type: [PinVerificationAttributes](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

VerificationKeyIdentifier

The keyARN of the PIN verification key.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
  "EncryptionKeyArn": "string",
  "EncryptionKeyCheckValue": "string",
  "VerificationKeyArn": "string",
  "VerificationKeyCheckValue": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

EncryptionKeyArn

The keyARN of the PEK that AWS Payment Cryptography uses for encrypted pin block generation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

EncryptionKeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

VerificationKeyArn

The keyARN of the PIN encryption key that AWS Payment Cryptography uses for PIN or PIN Offset verification.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

VerificationKeyCheckValue

The key check value (KCV) of the encryption key. The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed.

AWS Payment Cryptography computes the KCV according to the CMAC specification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Errors

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

InternalServerError

The request processing has failed because of an unknown error, exception, or failure.

HTTP Status Code: 500

ResourceNotFoundException

The request was denied due to an invalid resource error.

ResourceId

The resource that is missing.

HTTP Status Code: 404

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 429

ValidationException

The request was denied due to an invalid request error.

fieldList

The request was denied due to an invalid request error.

HTTP Status Code: 400

VerificationFailedException

This request failed verification.

Reason

The reason for the exception.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby V3](#)

Data Types

The Payment Cryptography Data Plane API contains several data types that various actions use. This section describes each data type in detail.

Note

The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- [AmexAttributes](#)
- [AmexCardSecurityCodeVersion1](#)
- [AmexCardSecurityCodeVersion2](#)
- [As2805KekValidationType](#)
- [As2805PekDerivationAttributes](#)
- [AsymmetricEncryptionAttributes](#)
- [CardGenerationAttributes](#)
- [CardHolderVerificationValue](#)
- [CardVerificationAttributes](#)
- [CardVerificationValue1](#)
- [CardVerificationValue2](#)
- [CryptogramAuthResponse](#)
- [CryptogramVerificationArpcMethod1](#)
- [CryptogramVerificationArpcMethod2](#)
- [CurrentPinAttributes](#)
- [DerivationMethodAttributes](#)
- [DiffieHellmanDerivationData](#)
- [DiscoverDynamicCardVerificationCode](#)
- [DukptAttributes](#)
- [DukptDerivationAttributes](#)

- [DukptEncryptionAttributes](#)
- [DynamicCardVerificationCode](#)
- [DynamicCardVerificationValue](#)
- [EcdhDerivationAttributes](#)
- [Emv2000Attributes](#)
- [EmvCommonAttributes](#)
- [EmvEncryptionAttributes](#)
- [EncryptionDecryptionAttributes](#)
- [Ibm3624NaturalPin](#)
- [Ibm3624PinFromOffset](#)
- [Ibm3624PinOffset](#)
- [Ibm3624PinVerification](#)
- [Ibm3624RandomPin](#)
- [IncomingDiffieHellmanTr31KeyBlock](#)
- [IncomingKeyMaterial](#)
- [KekValidationRequest](#)
- [KekValidationResponse](#)
- [MacAlgorithmDukpt](#)
- [MacAlgorithmEmv](#)
- [MacAttributes](#)
- [MasterCardAttributes](#)
- [OutgoingKeyMaterial](#)
- [OutgoingTr31KeyBlock](#)
- [PinData](#)
- [PinGenerationAttributes](#)
- [PinVerificationAttributes](#)
- [ReEncryptionAttributes](#)
- [SessionKeyAmex](#)
- [SessionKeyDerivation](#)
- [SessionKeyDerivationValue](#)

- [SessionKeyEmv2000](#)
- [SessionKeyEmvCommon](#)
- [SessionKeyMastercard](#)
- [SessionKeyVisa](#)
- [SymmetricEncryptionAttributes](#)
- [TranslationIsoFormats](#)
- [TranslationPinDataAs2805Format0](#)
- [TranslationPinDataIsoFormat034](#)
- [TranslationPinDataIsoFormat1](#)
- [ValidationExceptionField](#)
- [VisaAmexDerivationOutputs](#)
- [VisaAttributes](#)
- [VisaPin](#)
- [VisaPinVerification](#)
- [VisaPinVerificationValue](#)
- [WrappedKey](#)
- [WrappedKeyMaterial](#)
- [WrappedWorkingKey](#)

AmexAttributes

Parameters to derive the confidentiality and integrity keys for a payment card using Amex derivation method.

Contents

ApplicationTransactionCounter

The transaction counter of the current transaction that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

AuthorizationRequestKeyIdentifier

The keyArn of the issuer master key for cryptogram (IMK-AC) for the payment card.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

MajorKeyDerivationMode

The method to use when deriving the master key for a payment card using Amex derivation.

Type: String

Valid Values: `EMV_OPTION_A` | `EMV_OPTION_B`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN). Typically 00 is used, if no value is provided by the terminal.

Type: String

Length Constraints: Fixed length of 2.

Pattern: [0-9]+

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9]+

Required: Yes

CurrentPinAttributes

The encrypted pinblock of the old pin stored on the chip card.

Type: [CurrentPinAttributes](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AmexCardSecurityCodeVersion1

Card data parameters that are required to generate a Card Security Code (CSC2) for an AMEX payment card.

Contents

CardExpiryDate

The expiry date of a payment card.

Type: String

Length Constraints: Fixed length of 4.

Pattern: [0-9]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AmexCardSecurityCodeVersion2

Card data parameters that are required to generate a Card Security Code (CSC2) for an AMEX payment card.

Contents

CardExpiryDate

The expiry date of a payment card.

Type: String

Length Constraints: Fixed length of 4.

Pattern: [0-9]+

Required: Yes

ServiceCode

The service code of the AMEX payment card. This is different from the Card Security Code (CSC).

Type: String

Length Constraints: Fixed length of 3.

Pattern: [0-9]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

As2805KekValidationType

Parameter information for generating a random key for KEK validation to perform node-to-node initialization.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

KekValidationRequest

Parameter information for generating a KEK validation request during node-to-node initialization.

Type: [KekValidationRequest](#) object

Required: No

KekValidationResponse

Parameter information for generating a KEK validation response during node-to-node initialization.

Type: [KekValidationResponse](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

As2805PekDerivationAttributes

Parameter information to use a PEK derived using AS2805.

Contents

SystemTraceAuditNumber

The system trace audit number for the transaction.

Type: String

Length Constraints: Fixed length of 6.

Pattern: [0-9]+

Required: Yes

TransactionAmount

The transaction amount for the transaction.

Type: String

Length Constraints: Fixed length of 12.

Pattern: [0-9]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AsymmetricEncryptionAttributes

Parameters for plaintext encryption using asymmetric keys.

Contents

PaddingType

The padding to be included with the data.

Type: String

Valid Values: PKCS1 | OAEP_SHA1 | OAEP_SHA256 | OAEP_SHA512

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CardGenerationAttributes

Card data parameters that are required to generate Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2), or Card Security Codes (CSC).

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

AmexCardSecurityCodeVersion1

Card data parameters that are required to generate a Card Security Code (CSC2) for an AMEX payment card.

Type: [AmexCardSecurityCodeVersion1](#) object

Required: No

AmexCardSecurityCodeVersion2

Card data parameters that are required to generate a Card Security Code (CSC2) for an AMEX payment card.

Type: [AmexCardSecurityCodeVersion2](#) object

Required: No

CardHolderVerificationValue

Card data parameters that are required to generate a cardholder verification value for the payment card.

Type: [CardHolderVerificationValue](#) object

Required: No

CardVerificationValue1

Card data parameters that are required to generate Card Verification Value (CVV) for the payment card.

Type: [CardVerificationValue1](#) object

Required: No

CardVerificationValue2

Card data parameters that are required to generate Card Verification Value (CVV2) for the payment card.

Type: [CardVerificationValue2](#) object

Required: No

DynamicCardVerificationCode

Card data parameters that are required to generate CDynamic Card Verification Code (dCVC) for the payment card.

Type: [DynamicCardVerificationCode](#) object

Required: No

DynamicCardVerificationValue

Card data parameters that are required to generate CDynamic Card Verification Value (dCVV) for the payment card.

Type: [DynamicCardVerificationValue](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CardHolderVerificationValue

Card data parameters that are required to generate a cardholder verification value for the payment card.

Contents

ApplicationTransactionCounter

The transaction counter value that comes from a point of sale terminal.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

UnpredictableNumber

A random number generated by the issuer.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 8.

Pattern: `[0-9a-fA-F]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CardVerificationAttributes

Card data parameters that are required to verify Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2), or Card Security Codes (CSC).

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

AmexCardSecurityCodeVersion1

Card data parameters that are required to generate a Card Security Code (CSC2) for an AMEX payment card.

Type: [AmexCardSecurityCodeVersion1](#) object

Required: No

AmexCardSecurityCodeVersion2

Card data parameters that are required to verify a Card Security Code (CSC2) for an AMEX payment card.

Type: [AmexCardSecurityCodeVersion2](#) object

Required: No

CardHolderVerificationValue

Card data parameters that are required to verify a cardholder verification value for the payment card.

Type: [CardHolderVerificationValue](#) object

Required: No

CardVerificationValue1

Card data parameters that are required to verify Card Verification Value (CVV) for the payment card.

Type: [CardVerificationValue1](#) object

Required: No

CardVerificationValue2

Card data parameters that are required to verify Card Verification Value (CVV2) for the payment card.

Type: [CardVerificationValue2](#) object

Required: No

DiscoverDynamicCardVerificationCode

Card data parameters that are required to verify CDynamic Card Verification Code (dCVC) for the payment card.

Type: [DiscoverDynamicCardVerificationCode](#) object

Required: No

DynamicCardVerificationCode

Card data parameters that are required to verify CDynamic Card Verification Code (dCVC) for the payment card.

Type: [DynamicCardVerificationCode](#) object

Required: No

DynamicCardVerificationValue

Card data parameters that are required to verify CDynamic Card Verification Value (dCVV) for the payment card.

Type: [DynamicCardVerificationValue](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CardVerificationValue1

Card data parameters that are required to verify CVV (Card Verification Value) for the payment card.

Contents

CardExpiryDate

The expiry date of a payment card.

Type: String

Length Constraints: Fixed length of 4.

Pattern: [0-9]+

Required: Yes

ServiceCode

The service code of the payment card. This is different from Card Security Code (CSC).

Type: String

Length Constraints: Fixed length of 3.

Pattern: [0-9]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CardVerificationValue2

Card data parameters that are required to verify Card Verification Value (CVV2) for the payment card.

Contents

CardExpiryDate

The expiry date of a payment card.

Type: String

Length Constraints: Fixed length of 4.

Pattern: [0-9] +

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CryptogramAuthResponse

Parameters that are required for Authorization Response Cryptogram (ARPC) generation after Authorization Request Cryptogram (ARQC) verification is successful.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

ArpcMethod1

Parameters that are required for ARPC response generation using method1 after ARQC verification is successful.

Type: [CryptogramVerificationArpcMethod1](#) object

Required: No

ArpcMethod2

Parameters that are required for ARPC response generation using method2 after ARQC verification is successful.

Type: [CryptogramVerificationArpcMethod2](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CryptogramVerificationArpcMethod1

Parameters that are required for ARPC response generation using method1 after ARQC verification is successful.

Contents

AuthResponseCode

The auth code used to calculate APRC after ARQC verification is successful. This is the same auth code used for ARQC generation outside of AWS Payment Cryptography.

Type: String

Length Constraints: Fixed length of 4.

Pattern: [0-9a-fA-F]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CryptogramVerificationArpcMethod2

Parameters that are required for ARPC response generation using method2 after ARQC verification is successful.

Contents

CardStatusUpdate

The data indicating whether the issuer approves or declines an online transaction using an EMV chip card.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9a-fA-F]+`

Required: Yes

ProprietaryAuthenticationData

The proprietary authentication data used by issuer for communication during online transaction using an EMV chip card.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CurrentPinAttributes

The parameter values of the current PIN to be changed on the EMV chip card.

Contents

CurrentEncryptedPinBlock

The encrypted pinblock of the current pin stored on the chip card.

Type: String

Length Constraints: Fixed length of 16.

Pattern: `[0-9a-fA-F]+`

Required: Yes

CurrentPinPekIdentifier

The keyArn of the current PIN PEK.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DerivationMethodAttributes

Parameters to derive the payment card specific confidentiality and integrity keys.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Amex

Parameters to derive the confidentiality and integrity keys for a payment card using Amex derivation method.

Type: [AmexAttributes](#) object

Required: No

Emv2000

Parameters to derive the confidentiality and integrity keys for a payment card using Emv2000 derivation method.

Type: [Emv2000Attributes](#) object

Required: No

EmvCommon

Parameters to derive the confidentiality and integrity keys for a payment card using Emv common derivation method.

Type: [EmvCommonAttributes](#) object

Required: No

Mastercard

Parameters to derive the confidentiality and integrity keys for a payment card using Mastercard derivation method.

Type: [MasterCardAttributes](#) object

Required: No

Visa

Parameters to derive the confidentiality and integrity keys for a payment card using Visa derivation method.

Type: [VisaAttributes](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DiffieHellmanDerivationData

The shared information used when deriving a key using ECDH.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

SharedInformation

A string containing information that binds the ECDH derived key to the two parties involved or to the context of the key.

It may include details like identities of the two parties deriving the key, context of the operation, session IDs, and optionally a nonce. It must not contain zero bytes. It is not recommended to reuse shared information for multiple ECDH key derivations, as it could result in derived key material being the same across different derivations.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 2048.

Pattern: `(?:[0-9a-fA-F][0-9a-fA-F])+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DiscoverDynamicCardVerificationCode

Parameters that are required to generate or verify dCVC (Dynamic Card Verification Code).

Contents

ApplicationTransactionCounter

The transaction counter value that comes from the terminal.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

CardExpiryDate

The expiry date of a payment card.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9]+`

Required: Yes

UnpredictableNumber

A random number that is generated by the issuer.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 8.

Pattern: `[0-9a-fA-F]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DukptAttributes

Parameters that are used for Derived Unique Key Per Transaction (DUKPT) derivation algorithm.

Contents

DukptDerivationType

The key type derived using DUKPT from a Base Derivation Key (BDK) and Key Serial Number (KSN). This must be less than or equal to the strength of the BDK. For example, you can't use AES_128 as a derivation type for a BDK of AES_128 or TDES_2KEY.

Type: String

Valid Values: TDES_2KEY | TDES_3KEY | AES_128 | AES_192 | AES_256

Required: Yes

KeySerialNumber

The unique identifier known as Key Serial Number (KSN) that comes from an encrypting device using DUKPT encryption method. The KSN is derived from the encrypting device unique identifier and an internal transaction counter.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 24.

Pattern: (?:[0-9a-fA-F]{16}|[0-9a-fA-F]{20}|[0-9a-fA-F]{24})

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DukptDerivationAttributes

Parameters required for encryption or decryption of data using DUKPT.

Contents

KeySerialNumber

The unique identifier known as Key Serial Number (KSN) that comes from an encrypting device using DUKPT encryption method. The KSN is derived from the encrypting device unique identifier and an internal transaction counter.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 24.

Pattern: `(?:[0-9a-fA-F]{16}|[0-9a-fA-F]{20}|[0-9a-fA-F]{24})`

Required: Yes

DukptKeyDerivationType

The key type derived using DUKPT from a Base Derivation Key (BDK) and Key Serial Number (KSN). This must be less than or equal to the strength of the BDK. For example, you can't use AES_128 as a derivation type for a BDK of AES_128 or TDES_2KEY

Type: String

Valid Values: TDES_2KEY | TDES_3KEY | AES_128 | AES_192 | AES_256

Required: No

DukptKeyVariant

The type of use of DUKPT, which can be for incoming data decryption, outgoing data encryption, or both.

Type: String

Valid Values: BIDIRECTIONAL | REQUEST | RESPONSE

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DukptEncryptionAttributes

Parameters that are required to encrypt plaintext data using DUKPT.

Contents

KeySerialNumber

The unique identifier known as Key Serial Number (KSN) that comes from an encrypting device using DUKPT encryption method. The KSN is derived from the encrypting device unique identifier and an internal transaction counter.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 24.

Pattern: `(?:[0-9a-fA-F]{16}|[0-9a-fA-F]{20}|[0-9a-fA-F]{24})`

Required: Yes

DukptKeyDerivationType

The key type encrypted using DUKPT from a Base Derivation Key (BDK) and Key Serial Number (KSN). This must be less than or equal to the strength of the BDK. For example, you can't use AES_128 as a derivation type for a BDK of AES_128 or TDES_2KEY

Type: String

Valid Values: TDES_2KEY | TDES_3KEY | AES_128 | AES_192 | AES_256

Required: No

DukptKeyVariant

The type of use of DUKPT, which can be incoming data decryption, outgoing data encryption, or both.

Type: String

Valid Values: BIDIRECTIONAL | REQUEST | RESPONSE

Required: No

InitializationVector

An input used to provide the initial state. If no value is provided, AWS Payment Cryptography defaults it to zero.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `(?:[0-9a-fA-F]{16}|[0-9a-fA-F]{32})`

Required: No

Mode

The block cipher method to use for encryption.

The default is CBC.

Type: String

Valid Values: ECB | CBC

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DynamicCardVerificationCode

Parameters that are required to generate or verify Dynamic Card Verification Value (dCVV).

Contents

ApplicationTransactionCounter

The transaction counter value that comes from the terminal.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

TrackData

The data on the two tracks of magnetic cards used for financial transactions. This includes the cardholder name, PAN, expiration date, bank ID (BIN) and several other numbers the issuing bank uses to validate the data received.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 160.

Pattern: `[0-9a-fA-F]+`

Required: Yes

UnpredictableNumber

A random number generated by the issuer.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 8.

Pattern: `[0-9a-fA-F]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DynamicCardVerificationValue

Parameters that are required to generate or verify Dynamic Card Verification Value (dCVV).

Contents

ApplicationTransactionCounter

The transaction counter value that comes from the terminal.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

CardExpiryDate

The expiry date of a payment card.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9]+`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

ServiceCode

The service code of the payment card. This is different from Card Security Code (CSC).

Type: String

Length Constraints: Fixed length of 3.

Pattern: [0-9] +

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EcdhDerivationAttributes

Parameters required to establish ECDH based key exchange.

Contents

CertificateAuthorityPublicKeyIdentifier

The keyArn of the certificate that signed the client's PublicKeyCertificate.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

KeyAlgorithm

The key algorithm of the derived ECDH key.

Type: String

Valid Values: `TDES_2KEY` | `TDES_3KEY` | `AES_128` | `AES_192` | `AES_256` | `HMAC_SHA256` | `HMAC_SHA384` | `HMAC_SHA512` | `HMAC_SHA224`

Required: Yes

KeyDerivationFunction

The key derivation function to use for deriving a key using ECDH.

Type: String

Valid Values: `NIST_SP800` | `ANSI_X963`

Required: Yes

KeyDerivationHashAlgorithm

The hash type to use for deriving a key using ECDH.

Type: String

Valid Values: SHA_256 | SHA_384 | SHA_512

Required: Yes

PublicKeyCertificate

The client's public key certificate in PEM format (base64 encoded) to use for ECDH key derivation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32768.

Pattern: [^\[\;\>]+

Required: Yes

SharedInformation

A byte string containing information that binds the ECDH derived key to the two parties involved or to the context of the key.

It may include details like identities of the two parties deriving the key, context of the operation, session IDs, and optionally a nonce. It must not contain zero bytes, and re-using shared information for multiple ECDH key derivations is not recommended.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 2048.

Pattern: (?:[0-9a-fA-F][0-9a-fA-F])+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

Emv2000Attributes

Parameters to derive the confidentiality and integrity keys for a payment card using EMV2000 deruv.

Contents

ApplicationTransactionCounter

The transaction counter of the current transaction that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

MajorKeyDerivationMode

The method to use when deriving the master key for the payment card.

Type: String

Valid Values: `EMV_OPTION_A` | `EMV_OPTION_B`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN). Typically 00 is used, if no value is provided by the terminal.

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9] +

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EmvCommonAttributes

Parameters to derive the confidentiality and integrity keys for an Emv common payment card.

Contents

ApplicationCryptogram

The application cryptogram for the current transaction that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 16.

Pattern: [0-9a-fA-F]+

Required: Yes

MajorKeyDerivationMode

The method to use when deriving the master key for the payment card.

Type: String

Valid Values: EMV_OPTION_A | EMV_OPTION_B

Required: Yes

Mode

The block cipher method to use for encryption.

Type: String

Valid Values: ECB | CBC

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN). Typically 00 is used, if no value is provided by the terminal.

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

PinBlockLengthPosition

Specifies if PIN block length should be added to front of the pin block.

If value is set to `FRONT_OF_PIN_BLOCK`, then PIN block padding type should be `ISO_IEC_7816_4`.

Type: String

Valid Values: `NONE` | `FRONT_OF_PIN_BLOCK`

Required: Yes

PinBlockPaddingType

The padding to be added to the PIN block prior to encryption.

Padding type should be `ISO_IEC_7816_4`, if `PinBlockLengthPosition` is set to `FRONT_OF_PIN_BLOCK`. No padding is required, if `PinBlockLengthPosition` is set to `NONE`.

Type: String

Valid Values: `NO_PADDING` | `ISO_IEC_7816_4`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: `[0-9]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EmvEncryptionAttributes

Parameters for plaintext encryption using EMV keys.

Contents

MajorKeyDerivationMode

The EMV derivation mode to use for ICC master key derivation as per EMV version 4.3 book 2.

Type: String

Valid Values: EMV_OPTION_A | EMV_OPTION_B

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN). Typically 00 is used, if no value is provided by the terminal.

Type: String

Length Constraints: Fixed length of 2.

Pattern: [0-9]+

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN), a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9]+

Required: Yes

SessionDerivationData

The derivation value used to derive the ICC session key. It is typically the application transaction counter value padded with zeros or previous ARQC value padded with zeros as per EMV version 4.3 book 2.

Type: String

Length Constraints: Fixed length of 16.

Pattern: `[0-9a-fA-F]+`

Required: Yes

InitializationVector

An input used to provide the initial state. If no value is provided, AWS Payment Cryptography defaults it to zero.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `(?:[0-9a-fA-F]{16}|[0-9a-fA-F]{32})`

Required: No

Mode

The block cipher method to use for encryption.

Type: String

Valid Values: ECB | CBC

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EncryptionDecryptionAttributes

Parameters that are required to perform encryption and decryption operations.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Asymmetric

Parameters for plaintext encryption using asymmetric keys.

Type: [AsymmetricEncryptionAttributes](#) object

Required: No

Dukpt

Parameters that are required to encrypt plaintext data using DUKPT.

Type: [DukptEncryptionAttributes](#) object

Required: No

Emv

Parameters for plaintext encryption using EMV keys.

Type: [EmvEncryptionAttributes](#) object

Required: No

Symmetric

Parameters that are required to perform encryption and decryption using symmetric keys.

Type: [SymmetricEncryptionAttributes](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Ibm3624NaturalPin

Parameters that are required to generate or verify Ibm3624 natural PIN.

Contents

DecimalizationTable

The decimalization table to use for IBM 3624 PIN algorithm. The table is used to convert the algorithm intermediate result from hexadecimal characters to decimal.

Type: String

Length Constraints: Fixed length of 16.

Pattern: [0-9]+

Required: Yes

PinValidationData

The unique data for cardholder identification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: [0-9]+

Required: Yes

PinValidationDataPadCharacter

The padding character for validation data.

Type: String

Length Constraints: Fixed length of 1.

Pattern: [0-9A-F]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Ibm3624PinFromOffset

Parameters that are required to generate or verify Ibm3624 PIN from offset PIN.

Contents

DecimalizationTable

The decimalization table to use for IBM 3624 PIN algorithm. The table is used to convert the algorithm intermediate result from hexadecimal characters to decimal.

Type: String

Length Constraints: Fixed length of 16.

Pattern: [0-9]+

Required: Yes

PinOffset

The PIN offset value.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 12.

Pattern: [0-9]+

Required: Yes

PinValidationData

The unique data for cardholder identification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: [0-9]+

Required: Yes

PinValidationDataPadCharacter

The padding character for validation data.

Type: String

Length Constraints: Fixed length of 1.

Pattern: `[0-9A-F]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Ibm3624PinOffset

Parameters that are required to generate or verify Ibm3624 PIN offset PIN.

Contents

DecimalizationTable

The decimalization table to use for IBM 3624 PIN algorithm. The table is used to convert the algorithm intermediate result from hexadecimal characters to decimal.

Type: String

Length Constraints: Fixed length of 16.

Pattern: [0-9]+

Required: Yes

EncryptedPinBlock

The encrypted PIN block data. According to ISO 9564 standard, a PIN Block is an encoded representation of a payment card Personal Account Number (PAN) and the cardholder Personal Identification Number (PIN).

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: [0-9a-fA-F]+

Required: Yes

PinValidationData

The unique data for cardholder identification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: [0-9]+

Required: Yes

PinValidationDataPadCharacter

The padding character for validation data.

Type: String

Length Constraints: Fixed length of 1.

Pattern: [0-9A-F]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Ibm3624PinVerification

Parameters that are required to generate or verify Ibm3624 PIN verification PIN.

Contents

DecimalizationTable

The decimalization table to use for IBM 3624 PIN algorithm. The table is used to convert the algorithm intermediate result from hexadecimal characters to decimal.

Type: String

Length Constraints: Fixed length of 16.

Pattern: [0-9]+

Required: Yes

PinOffset

The PIN offset value.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 12.

Pattern: [0-9]+

Required: Yes

PinValidationData

The unique data for cardholder identification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: [0-9]+

Required: Yes

PinValidationDataPadCharacter

The padding character for validation data.

Type: String

Length Constraints: Fixed length of 1.

Pattern: `[0-9A-F]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Ibm3624RandomPin

Parameters that are required to generate or verify Ibm3624 random PIN.

Contents

DecimalizationTable

The decimalization table to use for IBM 3624 PIN algorithm. The table is used to convert the algorithm intermediate result from hexadecimal characters to decimal.

Type: String

Length Constraints: Fixed length of 16.

Pattern: [0-9]+

Required: Yes

PinValidationData

The unique data for cardholder identification.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: [0-9]+

Required: Yes

PinValidationDataPadCharacter

The padding character for validation data.

Type: String

Length Constraints: Fixed length of 1.

Pattern: [0-9A-F]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

IncomingDiffieHellmanTr31KeyBlock

Parameter information of a TR31KeyBlock wrapped using an ECDH derived key.

Contents

CertificateAuthorityPublicKeyIdentifier

The keyArn of the certificate that signed the client's PublicKeyCertificate.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

DerivationData

The shared information used when deriving a key using ECDH.

Type: [DiffieHellmanDerivationData](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

DeriveKeyAlgorithm

The key algorithm of the derived ECDH key.

Type: String

Valid Values: `TDES_2KEY | TDES_3KEY | AES_128 | AES_192 | AES_256 | HMAC_SHA256 | HMAC_SHA384 | HMAC_SHA512 | HMAC_SHA224`

Required: Yes

KeyDerivationFunction

The key derivation function to use for deriving a key using ECDH.

Type: String

Valid Values: NIST_SP800 | ANSI_X963

Required: Yes

KeyDerivationHashAlgorithm

The hash type to use for deriving a key using ECDH.

Type: String

Valid Values: SHA_256 | SHA_384 | SHA_512

Required: Yes

PrivateKeyIdentifier

The keyARN of the asymmetric ECC key pair.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

PublicKeyCertificate

The client's public key certificate in PEM format (base64 encoded) to use for ECDH key derivation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32768.

Pattern: `[^\\[;\\<>]+`

Required: Yes

WrappedKeyBlock

The WrappedKeyBlock containing the transaction key wrapped using an ECDH derived key.

Type: String

Length Constraints: Minimum length of 56. Maximum length of 9984.

Pattern: `[0-9a-zA-Z]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

IncomingKeyMaterial

Parameter information of the incoming WrappedKeyBlock containing the transaction key.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

DiffieHellmanTr31KeyBlock

Parameter information of the TR31WrappedKeyBlock containing the transaction key wrapped using an ECDH derived key.

Type: [IncomingDiffieHellmanTr31KeyBlock](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

KekValidationRequest

Parameter information for generating a KEK validation request during node-to-node initialization.

Contents

DeriveKeyAlgorithm

The key derivation algorithm to use for generating a KEK validation request.

Type: String

Valid Values: TDES_2KEY | TDES_3KEY | AES_128 | AES_192 | AES_256 | HMAC_SHA256 | HMAC_SHA384 | HMAC_SHA512 | HMAC_SHA224

Required: Yes

RandomKeyMaxLength

The maximum length of the random key to generate for a KEK validation request.

Type: String

Valid Values: BYTES_8 | BYTES_16 | BYTES_24

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

KekValidationResponse

Parameter information for generating a KEK validation response during node-to-node initialization.

Contents

RandomKeySend

The random key send value received from the initiating node to generate a KEK validation response.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 48.

Pattern: `(?:[0-9a-fA-F]{16}|[0-9a-fA-F]{32}|[0-9a-fA-F]{48})`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

MacAlgorithmDukpt

Parameters required for DUKPT MAC generation and verification.

Contents

DukptKeyVariant

The type of use of DUKPT, which can be MAC generation, MAC verification, or both.

Type: String

Valid Values: BIDIRECTIONAL | REQUEST | RESPONSE

Required: Yes

KeySerialNumber

The unique identifier known as Key Serial Number (KSN) that comes from an encrypting device using DUKPT encryption method. The KSN is derived from the encrypting device unique identifier and an internal transaction counter.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 24.

Pattern: (?:[0-9a-fA-F]{16}|[0-9a-fA-F]{20}|[0-9a-fA-F]{24})

Required: Yes

DukptDerivationType

The key type derived using DUKPT from a Base Derivation Key (BDK) and Key Serial Number (KSN). This must be less than or equal to the strength of the BDK. For example, you can't use AES_128 as a derivation type for a BDK of AES_128 or TDES_2KEY.

Type: String

Valid Values: TDES_2KEY | TDES_3KEY | AES_128 | AES_192 | AES_256

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

MacAlgorithmEmv

Parameters that are required for EMV MAC generation and verification.

Contents

MajorKeyDerivationMode

The method to use when deriving the master key for EMV MAC generation or verification.

Type: String

Valid Values: EMV_OPTION_A | EMV_OPTION_B

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: [0-9] +

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN), a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9] +

Required: Yes

SessionKeyDerivationMode

The method of deriving a session key for EMV MAC generation or verification.

Type: String

Valid Values: EMV_COMMON_SESSION_KEY | EMV2000 | AMEX |
MASTERCARD_SESSION_KEY | VISA

Required: Yes

SessionKeyDerivationValue

Parameters that are required to generate session key for EMV generation and verification.

Type: [SessionKeyDerivationValue](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

MacAttributes

Parameters that are required for DUKPT, HMAC, or EMV MAC generation or verification.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Algorithm

The encryption algorithm for MAC generation or verification.

Type: String

Valid Values: ISO9797_ALGORITHM1 | ISO9797_ALGORITHM3 | CMAC | HMAC | HMAC_SHA224 | HMAC_SHA256 | HMAC_SHA384 | HMAC_SHA512 | AS2805_4_1

Required: No

DukptCmac

Parameters that are required for MAC generation or verification using DUKPT CMAC algorithm.

Type: [MacAlgorithmDukpt](#) object

Required: No

DukptIso9797Algorithm1

Parameters that are required for MAC generation or verification using DUKPT ISO 9797 algorithm1.

Type: [MacAlgorithmDukpt](#) object

Required: No

DukptIso9797Algorithm3

Parameters that are required for MAC generation or verification using DUKPT ISO 9797 algorithm3.

Type: [MacAlgorithmDukpt](#) object

Required: No

EmvMac

Parameters that are required for MAC generation or verification using EMV MAC algorithm.

Type: [MacAlgorithmEmv](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

MasterCardAttributes

Parameters to derive the confidentiality and integrity keys for a Mastercard payment card.

Contents

ApplicationCryptogram

The application cryptogram for the current transaction that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 16.

Pattern: `[0-9a-fA-F]+`

Required: Yes

MajorKeyDerivationMode

The method to use when deriving the master key for the payment card.

Type: String

Valid Values: `EMV_OPTION_A` | `EMV_OPTION_B`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN). Typically 00 is used, if no value is provided by the terminal.

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9] +

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

OutgoingKeyMaterial

Parameter information of the outgoing TR31WrappedKeyBlock containing the transaction key.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Tr31KeyBlock

Parameter information of the TR31WrappedKeyBlock containing the transaction key wrapped using a KEK.

Type: [OutgoingTr31KeyBlock](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

OutgoingTr31KeyBlock

Parameter information of the TR31WrappedKeyBlock containing the transaction key wrapped using a KEK.

Contents

WrappingKeyIdIdentifier

The keyARN of the KEK used to wrap the transaction key.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PinData

Parameters that are required to generate, translate, or verify PIN data.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

PinOffset

The PIN offset value.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 12.

Pattern: [0-9]+

Required: No

VerificationValue

The unique data to identify a cardholder. In most cases, this is the same as cardholder's Primary Account Number (PAN). If a value is not provided, it defaults to PAN.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 12.

Pattern: [0-9]+

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PinGenerationAttributes

Parameters that are required for PIN data generation.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Ibm3624NaturalPin

Parameters that are required to generate or verify Ibm3624 natural PIN.

Type: [Ibm3624NaturalPin](#) object

Required: No

Ibm3624PinFromOffset

Parameters that are required to generate or verify Ibm3624 PIN from offset PIN.

Type: [Ibm3624PinFromOffset](#) object

Required: No

Ibm3624PinOffset

Parameters that are required to generate or verify Ibm3624 PIN offset PIN.

Type: [Ibm3624PinOffset](#) object

Required: No

Ibm3624RandomPin

Parameters that are required to generate or verify Ibm3624 random PIN.

Type: [Ibm3624RandomPin](#) object

Required: No

VisaPin

Parameters that are required to generate or verify Visa PIN.

Type: [VisaPin](#) object

Required: No

VisaPinVerificationValue

Parameters that are required to generate or verify Visa PIN Verification Value (PVV).

Type: [VisaPinVerificationValue](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PinVerificationAttributes

Parameters that are required for PIN data verification.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Ibm3624Pin

Parameters that are required to generate or verify Ibm3624 PIN.

Type: [Ibm3624PinVerification](#) object

Required: No

VisaPin

Parameters that are required to generate or verify Visa PIN.

Type: [VisaPinVerification](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ReEncryptionAttributes

Parameters that are required to perform reencryption operation.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Dukpt

Parameters that are required to encrypt plaintext data using DUKPT.

Type: [DukptEncryptionAttributes](#) object

Required: No

Symmetric

Parameters that are required to encrypt data using symmetric keys.

Type: [SymmetricEncryptionAttributes](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SessionKeyAmex

Parameters to derive session key for an Amex payment card.

Contents

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: [0-9]+

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder. A PAN is a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SessionKeyDerivation

Parameters to derive a session key for Authorization Response Cryptogram (ARQC) verification.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

Amex

Parameters to derive session key for an Amex payment card for ARQC verification.

Type: [SessionKeyAmex](#) object

Required: No

Emv2000

Parameters to derive session key for an Emv2000 payment card for ARQC verification.

Type: [SessionKeyEmv2000](#) object

Required: No

EmvCommon

Parameters to derive session key for an Emv common payment card for ARQC verification.

Type: [SessionKeyEmvCommon](#) object

Required: No

Mastercard

Parameters to derive session key for a Mastercard payment card for ARQC verification.

Type: [SessionKeyMastercard](#) object

Required: No

Visa

Parameters to derive session key for a Visa payment cardfor ARQC verification.

Type: [SessionKeyVisa](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SessionKeyDerivationValue

Parameters to derive session key value using a MAC EMV algorithm.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

ApplicationCryptogram

The cryptogram provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 16.

Pattern: [0-9a-fA-F]+

Required: No

ApplicationTransactionCounter

The transaction counter that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 4.

Pattern: [0-9a-fA-F]+

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SessionKeyEmv2000

Parameters to derive session key for an Emv2000 payment card for ARQC verification.

Contents

ApplicationTransactionCounter

The transaction counter that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder. A PAN is a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: `[0-9]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SessionKeyEmvCommon

Parameters to derive session key for an Emv common payment card for ARQC verification.

Contents

ApplicationTransactionCounter

The transaction counter that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder. A PAN is a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: `[0-9]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SessionKeyMastercard

Parameters to derive session key for Mastercard payment card for ARQC verification.

Contents

ApplicationTransactionCounter

The transaction counter that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: `[0-9]+`

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder. A PAN is a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: `[0-9]+`

Required: Yes

UnpredictableNumber

A random number generated by the issuer.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9a-fA-F]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SessionKeyVisa

Parameters to derive session key for Visa payment card for ARQC verification.

Contents

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN).

Type: String

Length Constraints: Fixed length of 2.

Pattern: [0-9]+

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder. A PAN is a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SymmetricEncryptionAttributes

Parameters required to encrypt plaintext data using symmetric keys.

Contents

Mode

The block cipher method to use for encryption.

Type: String

Valid Values: ECB | CBC | CFB | CFB1 | CFB8 | CFB64 | CFB128 | OFB

Required: Yes

InitializationVector

An input used to provide the initial state. If no value is provided, AWS Payment Cryptography defaults it to zero.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: (?:[0-9a-fA-F]{16}|[0-9a-fA-F]{32})

Required: No

PaddingType

The padding to be included with the data.

Type: String

Valid Values: PKCS1 | OAEP_SHA1 | OAEP_SHA256 | OAEP_SHA512

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TranslationIsoFormats

Parameters that are required for translation between ISO9564 PIN block formats 0,1,3,4.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

As2805Format0

Parameters that are required for AS2805 PIN format 0 translation.

Type: [TranslationPinDataAs2805Format0](#) object

Required: No

IsoFormat0

Parameters that are required for ISO9564 PIN format 0 translation.

Type: [TranslationPinDataIsoFormat034](#) object

Required: No

IsoFormat1

Parameters that are required for ISO9564 PIN format 1 translation.

Type: [TranslationPinDataIsoFormat1](#) object

Required: No

IsoFormat3

Parameters that are required for ISO9564 PIN format 3 translation.

Type: [TranslationPinDataIsoFormat034](#) object

Required: No

IsoFormat4

Parameters that are required for ISO9564 PIN format 4 translation.

Type: [TranslationPinDataIsoFormat034](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TranslationPinDataAs2805Format0

Parameters that are required for translation between AS2805 PIN format 0 translation.

Contents

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder. A PAN is a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9] +

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TranslationPinDataIsoFormat034

Parameters that are required for translation between ISO9564 PIN format 0,3,4 translation.

Contents

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder. A PAN is a unique identifier for a payment credit or debit card and associates the card to a specific account holder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9] +

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TranslationPinDataIsoFormat1

Parameters that are required for ISO9564 PIN format 1 translation.

Contents

The members of this exception structure are context-dependent.

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ValidationExceptionField

The request was denied due to an invalid request error.

Contents

message

The request was denied due to an invalid request error.

Type: String

Required: Yes

path

The request was denied due to an invalid request error.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VisaAmexDerivationOutputs

The attributes values used for Amex and Visa derivation methods.

Contents

AuthorizationRequestKeyArn

The keyArn of the issuer master key for cryptogram (IMK-AC) used by the operation.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

Required: Yes

AuthorizationRequestKeyCheckValue

The key check value (KCV) of the issuer master key for cryptogram (IMK-AC) used by the operation.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F] +`

Required: Yes

CurrentPinPekArn

The keyArn of the current PIN PEK.

Type: String

Length Constraints: Minimum length of 70. Maximum length of 150.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:key/[0-9a-zA-Z]{16,64}`

Required: No

CurrentPinPekKeyCheckValue

The key check value (KCV) of the current PIN PEK.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VisaAttributes

Parameters to derive the confidentiality and integrity keys for a Visa payment card.

Contents

ApplicationTransactionCounter

The transaction counter of the current transaction that is provided by the terminal during transaction processing.

Type: String

Length Constraints: Fixed length of 4.

Pattern: `[0-9a-fA-F]+`

Required: Yes

AuthorizationRequestKeyIdentifier

The keyArn of the issuer master key for cryptogram (IMK-AC) for the payment card.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 322.

Pattern: `arn:aws:payment-cryptography:[a-z]{2}-[a-z]{1,16}-[0-9]+:[0-9]{12}:(key/[0-9a-zA-Z]{16,64}|alias/[a-zA-Z0-9/_-]+)$|^alias/[a-zA-Z0-9/_-]+`

Required: Yes

MajorKeyDerivationMode

The method to use when deriving the master key for the payment card.

Type: String

Valid Values: `EMV_OPTION_A` | `EMV_OPTION_B`

Required: Yes

PanSequenceNumber

A number that identifies and differentiates payment cards with the same Primary Account Number (PAN). Typically 00 is used, if no value is provided by the terminal.

Type: String

Length Constraints: Fixed length of 2.

Pattern: [0-9]+

Required: Yes

PrimaryAccountNumber

The Primary Account Number (PAN) of the cardholder.

Type: String

Length Constraints: Minimum length of 12. Maximum length of 19.

Pattern: [0-9]+

Required: Yes

CurrentPinAttributes

The encrypted pinblock of the old pin stored on the chip card.

Type: [CurrentPinAttributes](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VisaPin

Parameters that are required to generate or verify Visa PIN.

Contents

PinVerificationKeyIndex

The value for PIN verification index. It is used in the Visa PIN algorithm to calculate the PVV (PIN Verification Value).

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 6.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VisaPinVerification

Parameters that are required to generate or verify Visa PIN.

Contents

PinVerificationKeyIndex

The value for PIN verification index. It is used in the Visa PIN algorithm to calculate the PVV (PIN Verification Value).

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 6.

Required: Yes

VerificationValue

Parameters that are required to generate or verify Visa PVV (PIN Verification Value).

Type: String

Length Constraints: Minimum length of 4. Maximum length of 12.

Pattern: `[0-9]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VisaPinVerificationValue

Parameters that are required to generate or verify Visa PVV (PIN Verification Value).

Contents

EncryptedPinBlock

The encrypted PIN block data to verify.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 32.

Pattern: `[0-9a-fA-F]+`

Required: Yes

PinVerificationKeyIndex

The value for PIN verification index. It is used in the Visa PIN algorithm to calculate the PVV (PIN Verification Value).

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 6.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

WrappedKey

Parameter information of a WrappedKeyBlock for encryption key exchange.

Contents

WrappedKeyMaterial

Parameter information of a WrappedKeyBlock for encryption key exchange.

Type: [WrappedKeyMaterial](#) object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

KeyCheckValueAlgorithm

The algorithm that AWS Payment Cryptography uses to calculate the key check value (KCV). It is used to validate the key integrity.

For TDES keys, the KCV is computed by encrypting 8 bytes, each with value of zero, with the key to be checked and retaining the 3 highest order bytes of the encrypted result. For AES keys, the KCV is computed using a CMAC algorithm where the input data is 16 bytes of zero and retaining the 3 highest order bytes of the encrypted result.

Type: String

Valid Values: CMAC | ANSI_X9_24 | HMAC | SHA_1

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

WrappedKeyMaterial

Parameter information of a WrappedKeyBlock for encryption key exchange.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

DiffieHellmanSymmetricKey

The parameter information for deriving a ECDH shared key.

Type: [EcdhDerivationAttributes](#) object

Required: No

Tr31KeyBlock

The TR-31 wrapped key block.

Type: String

Length Constraints: Minimum length of 56. Maximum length of 9984.

Pattern: [0-9a-zA-Z]+

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

WrappedWorkingKey

The parameter information of the outgoing wrapped key block.

Contents

KeyCheckValue

The key check value (KCV) of the key contained within the outgoing TR31WrappedKeyBlock.

The KCV is used to check if all parties holding a given key have the same key or to detect that a key has changed. For more information on KCV, see [KCV](#) in the *AWS Payment Cryptography User Guide*.

Type: String

Length Constraints: Minimum length of 4. Maximum length of 16.

Pattern: `[0-9a-fA-F]+`

Required: Yes

WrappedKeyMaterial

The wrapped key block of the outgoing transaction key.

Type: String

Length Constraints: Minimum length of 32. Maximum length of 16384.

Required: Yes

WrappedKeyMaterialFormat

The key block format of the wrapped key.

Type: String

Valid Values: `KEY_CRYPTOGRAM` | `TR31_KEY_BLOCK` | `TR34_KEY_BLOCK`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)