API Documentation

API Documentation

July 21, 2008

Contents

1 Package keyczar

Keyczar Cryptography Toolkit

Collection of tools for managing and using cryptographic keys. Goal is to make it easier for developers to use application-layer cryptography.

Authors: arkajit.dey@gmail.com (Arkajit Dey), steveweis@gmail.com (Steve Weis)

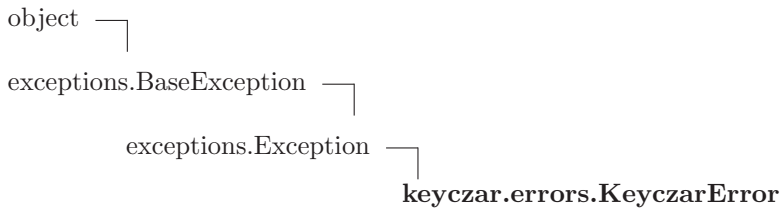
1.1 Modules

2 Module keyczar.errors

Contains hierarchy of all possible exceptions thrown by Keyczar.

Author: arkajit.dey@gmail.com (Arkajit Dey)

2.1 Class KeyczarError



Known Subclasses: keyczar.errors.BadFormatError, keyczar.errors.BadVersionError, keyczar.errors.Base64DecodingError, keyczar.errors.InvalidSignatureError, keyczar.errors.KeyNotFoundError, keyczar.errors.ShortBufferError, keyczar.errors.ShortCiphertextError, keyczar.errors.ShortSignatureError

Indicates exceptions raised by a Keyczar class.

2.1.1 Methods

Inherited from exceptions.Exception

__init__(), __new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

Inherited from object

__hash__(), __reduce_ex__()

2.1.2 Properties

Name	Description
Inherited from exceptions.BaseException args, message	
Inherited from object __class__	

2.2 Class BadVersionError

object
exceptions.BaseException
exceptions.Exception
keyczar.errors.KeyczarError
keyczar.errors.BadVersionError

Indicates a bad version number was received.

2.2.1 Methods

__init__(*self*, *version*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

Inherited from object

__hash__(), __reduce_ex__()

2.2.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

2.3 Class BadFormatError

object
exceptions.BaseException
exceptions.Exception
keyczar.errors.KeyczarError
keyczar.errors.BadFormatError

Indicates a bad format number was received.

2.3.1 Methods

__init__(*self*, *format*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

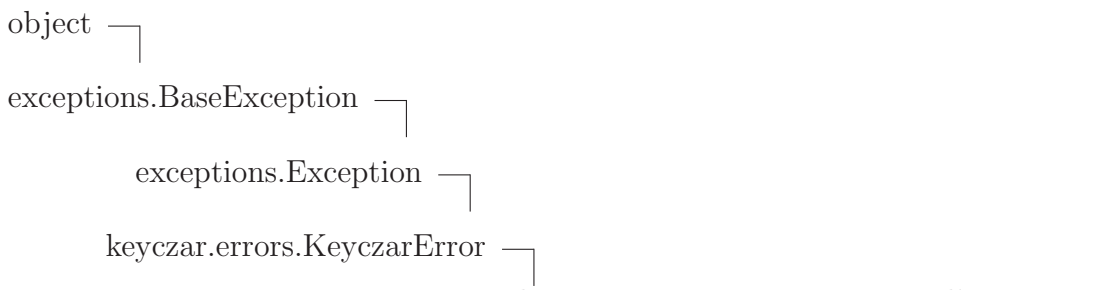
Inherited from object

__hash__(), __reduce_ex__()

2.3.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

2.4 Class Base64DecodingError



Indicates an error while performing Base 64 decoding.

2.4.1 Methods

Inherited from exceptions.Exception

__init__(), __new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

Inherited from object

__hash__(), __reduce_ex__()

2.4.2 Properties

Name	Description
Inherited from exceptions.BaseException args, message	
Inherited from object __class__	

2.5 Class InvalidSignatureError

object
exceptions.BaseException
exceptions.Exception
keyczar.errors.KeyczarError
keyczar.errors.InvalidSignatureError

Indicates an invalid ciphertext signature.

2.5.1 Methods

__init__(*self*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

Inherited from object

__hash__(), __reduce_ex__()

2.5.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

2.6 Class KeyNotFoundError

object
exceptions.BaseException
exceptions.Exception
keyczar.errors.KeyczarError
keyczar.errors.KeyNotFoundError

Known Subclasses: keyczar.errors.NoPrimaryKeyError

Indicates a key with a certain hash id was not found.

2.6.1 Methods

__init__(*self*, *hash*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

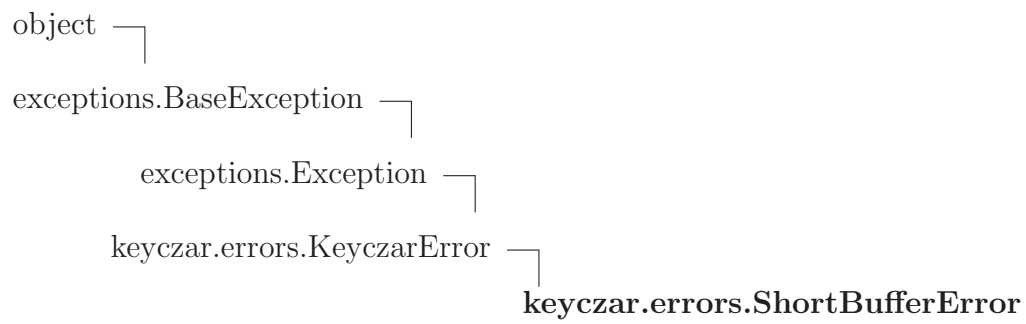
Inherited from object

__hash__(), __reduce_ex__()

2.6.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

2.7 Class ShortBufferError



Indicates a buffer with insufficient capacity.

2.7.1 Methods

__init__(*self*, *given*, *needed*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

Inherited from object

__hash__(), __reduce_ex__()

2.7.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

2.8 Class ShortCiphertextError

object
exceptions.BaseException
exceptions.Exception
keyczar.errors.KeyczarError
keyczar.errors.ShortCiphertextError

Indicates a ciphertext too short to be valid.

2.8.1 Methods

__init__(*self*, *length*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

Inherited from object

__hash__(), __reduce_ex__()

2.8.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

2.9 Class ShortSignatureError

object
exceptions.BaseException
exceptions.Exception
keyczar.errors.KeyczarError
keyczar.errors.ShortSignatureError

Indicates a signature too short to be valid.

2.9.1 Methods

__init__(*self*, *length*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

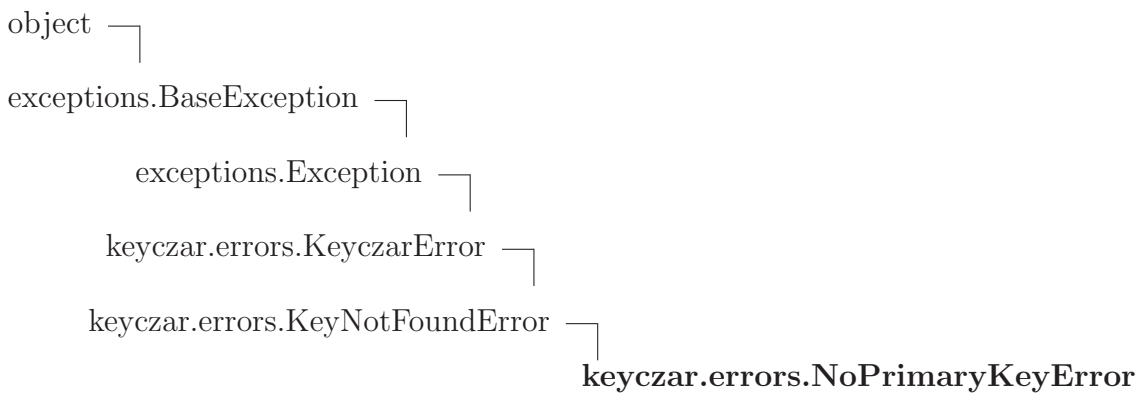
Inherited from object

__hash__(), __reduce_ex__()

2.9.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

2.10 Class NoPrimaryKeyError



Indicates missing primary key.

2.10.1 Methods

__init__(*self*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from exceptions.Exception

__new__()

Inherited from exceptions.BaseException

__delattr__(), __getattribute__(), __getitem__(), __getslice__(), __reduce__(), __repr__(), __setattr__(), __setstate__(), __str__()

Inherited from object

__hash__(), __reduce_ex__()

2.10.2 Properties

Name	Description
Inherited from exceptions.BaseException	
args, message	
Inherited from object	
__class__	

3 Module keyczar.keyczar

Collection of all Keyczar classes used to perform cryptographic functions: encrypt, decrypt, sign and verify.

Authors: arkajit.dey@gmail.com (Arkajit Dey), steveweis@gmail.com (Steve Weis)

3.1 Variables

Name	Description
VERSION	**Value:** `1`
FORMAT	**Value:** `1`
KEY_HASH_SIZE	**Value:** `4`
HEADER_SIZE	**Value:** `6`

3.2 Class Keyczar

object
└
keyczar.keyczar.Keyczar

Known Subclasses: keyczar.keyczar.Encrypter, keyczar.keyczar.GenericKeyczar, keyczar.keyczar.Verifier

Abstract Keyczar base class.

3.2.1 Methods

__**init**__(*self*, *reader*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

__**str**__(*self*)

str(x)

Overrides: object.__str__ extit(inherited documentation)

Read(*location*)

Return a Keyczar object created from FileReader at given location.

Parameters

`location:` pathname of the directory storing the key files

(type=string)

Return Value

a Keyczar to manage the keys stored at the given location

(type=`Keyczar`)

IsAcceptablePurpose(*self*, *purpose*)

Indicates whether purpose is valid. Abstract method.

GetKey(*self*, *id*)

Returns the key associated with the given id, a hash or a version.

Parameters

`id:` Either the hash identifier of the key or its version.

(type=string or `keydata.KeyVersion`)

Return Value

key associated with this id or None if id doesn't exist.

(type=`keys.Key`)

Raises

`KeyNotFoundError` if key with given id doesn't exist

AddVersion(*self*, *status*, *size*=`None`)

Adds a new key version with given status to key set.

Generates a new key of same type (repeated until hash identifier is unique) for this version. Uses supplied key size (if provided) in lieu of the default key size. If this is an unacceptable key size, uses the default key size. Uses next available version number.

Parameters

`status`: the status of the new key to be added

(type=`keyinfo.KeyStatus`)

`size`: size of key in bits, uses default size if not provided.

(type=integer)

Raises

`KeyczarError` if key type unsupported

Promote(*self*, *version_number*)

Promotes the status of key with given version number.

Promoting ACTIVE key automatically demotes current PRIMARY key to ACTIVE.

Parameters

`version_number`: the version number to promote

(type=integer)

Raises

`KeyczarError` if invalid version number or trying to promote a primary key

Demote(*self*, *version_number*)

Demotes the status of key with given version number.

Demoting PRIMARY key results in a key set with no primary version.

Parameters

`version_number`: the version number to demote

(type=integer)

Raises

`KeyczarError` if invalid version number or trying to demote a key scheduled for revocation, use `Revoke` instead.

Revoke(*self*, *version_number*)

Revokes the key with given version number if scheduled to be revoked.

Parameters

`version_number`: integer version number to revoke
(type=integer)

Raises

`KeyczarError` if invalid version number or key is not scheduled for revocation

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

3.2.2 Properties

Name	Description
versions	List of versions in key set.
primary_key	The primary key for this key set.
Inherited from object	
__class__	

3.3 Class GenericKeyczar

To be used by Keyczart.

3.3.1 Methods

Read(*location*)

Return a GenericKeyczar created from FileReader at given location.

Parameters

`location:` pathname of the directory storing the key files

Return Value

a Keyczar to manage the keys stored at the given location

(type=`Keyczar`)

Overrides: keyczar.keyczar.Keyczar.Read

IsAcceptablePurpose(*self*, *purpose*)

All purposes ok for Keyczart.

Overrides: keyczar.keyczar.Keyczar.IsAcceptablePurpose

PublicKeyExport(*self*, *destination*)

Export the public keys corresponding to our key set to destination.

Inherited from keyczar.keyczar.Keyczar(Section 3.2)

AddVersion(), Demote(), GetKey(), Promote(), Revoke(), __init__(), __str__()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

3.3.2 Properties

Name	Description
Inherited from keyczar.keyczar.Keyczar (Section 3.2) primary_key, versions	
Inherited from object __class__	

3.4 Class Encrypter

object
keyczar.keyczar.Keyczar
keyczar.keyczar.Encrypter

Known Subclasses: keyczar.keyczar.Crypter

Capable of encrypting only.

3.4.1 Methods

Read(*location*)

Return an Encrypter object created from FileReader at given location.

Parameters

`location:` pathname of the directory storing the key files

(type=string)

Return Value

an Encrypter to manage the keys stored at the given location and perform encryption functions.

(type=`Encrypter`)

Overrides: keyczar.keyczar.Keyczar.Read

IsAcceptablePurpose(*self*, *purpose*)

Only valid if purpose includes encrypting.

Overrides: keyczar.keyczar.Keyczar.IsAcceptablePurpose

Encrypt(*self*, *data*)

Encrypt the data and return the ciphertext.

Parameters

`data`: message to encrypt

(type=string)

Return Value

ciphertext encoded as a Base64 string

(type=string)

Raises

`NoPrimaryKeyError` if no primary key can be found to encrypt

Inherited from keyczar.keyczar.Keyczar(Section 3.2)

AddVersion(), Demote(), GetKey(), Promote(), Revoke(), __init__(), __str__()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

3.4.2 Properties

Name	Description
Inherited from keyczar.keyczar.Keyczar (Section 3.2) primary_key, versions	
Inherited from object __class__	

3.5 Class Verifier

object

keyczar.keyczar.Keyczar

keyczar.keyczar.Verifier

Known Subclasses: keyczar.keyczar.Signer

Capable of verifying only.

3.5.1 Methods

Read(*location*)

Return a Verifier object created from FileReader at given location.

Parameters

`location`: pathname of the directory storing the key files

(type=string)

Return Value

a Verifier to manage the keys stored at the given location and perform verify functions.

(type=`Verifier`)

Overrides: keyczar.keyczar.Keyczar.Read

IsAcceptablePurpose(*self*, *purpose*)

Only valid if purpose includes verifying.

Overrides: keyczar.keyczar.Keyczar.IsAcceptablePurpose

Verify(*self*, *data*, *sig*)

Verifies whether the signature corresponds to the given data.

Parameters

`data`: message that has been signed with sig

(type=string)

`sig`: Base64 string formatted as Header|Signature

(type=string)

Return Value

True if sig corresponds to data, False otherwise.

(type=boolean)

Inherited from keyczar.keyczar.Keyczar(Section 3.2)

AddVersion(), Demote(), GetKey(), Promote(), Revoke(), __init__(), __str__()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

3.5.2 Properties

Name	Description
Inherited from keyczar.keyczar.Keyczar (Section 3.2) primary_key, versions	
Inherited from object __class__	

3.6 Class Crypter

object
keyczar.keyczar.Keyczar
keyczar.keyczar.Encrypter
keyczar.keyczar.Crypter

Capable of encrypting and decrypting.

3.6.1 Methods

Read(*location*)

Return a Crypter object created from FileReader at given location.

Parameters

`location:` pathname of the directory storing the key files

(type=string)

Return Value

a Crypter to manage the keys stored at the given location and perform encryption and decryption functions.

(type=`Crypter`)

Overrides: keyczar.keyczar.Keyczar.Read

IsAcceptablePurpose(*self*, *purpose*)

Only valid if purpose includes decrypting

Overrides: keyczar.keyczar.Keyczar.IsAcceptablePurpose

Decrypt(*self*, *ciphertext*)

Decrypts the given ciphertext and returns the plaintext.

Parameters

`ciphertext`: Base64 encoded string ciphertext to be decrypted.

(type=string)

Return Value

plaintext message

(type=string)

Raises

`ShortCiphertextError` if length is too short to have Header, IV, Sig

`BadVersionError` if header specifies an illegal version

`BadFormatError` if header specifies an illegal format

`KeyNotFoundError` if key specified in header doesn't exist

`InvalidSignatureError` if the signature can't be verified

Inherited from keyczar.keyczar.Encrypter(Section 3.4)

Encrypt()

Inherited from keyczar.keyczar.Keyczar(Section 3.2)

AddVersion(), Demote(), GetKey(), Promote(), Revoke(), __init__(), __str__()

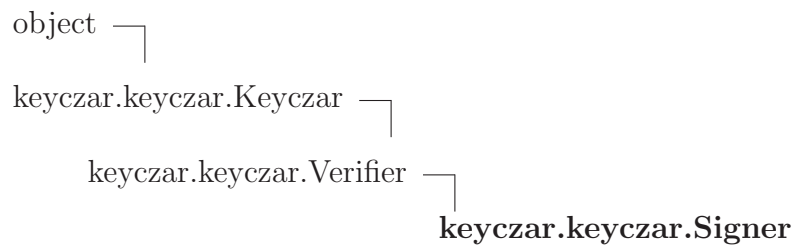
Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

3.6.2 Properties

Name	Description
Inherited from keyczar.keyczar.Keyczar (Section 3.2) primary_key, versions	
Inherited from object __class__	

3.7 Class Signer



Capable of both signing and verifying.

3.7.1 Methods

Read(*location*)

Return a Signer object created from FileReader at given location.

Parameters

`location:` pathname of the directory storing the key files

(type=string)

Return Value

a Signer to manage the keys stored at the given location and perform sign and verify functions.

(type=`Signer`)

Overrides: keyczar.keyczar.Keyczar.Read

IsAcceptablePurpose(*self*, *purpose*)

Only valid if purpose includes signing.

Overrides: keyczar.keyczar.Keyczar.IsAcceptablePurpose

Sign(*self*, *data*)

Sign given data and return corresponding signature.

Parameters

`data:` message to be signed

(type=string)

Return Value

signature on the data encoded as a Base64 string

(type=string)

Inherited from keyczar.keyczar.Verifier(Section 3.5)

Verify()

Inherited from keyczar.keyczar.Keyczar(Section 3.2)

AddVersion(), Demote(), GetKey(), Promote(), Revoke(), __init__(), __str__()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

3.7.2 Properties

Name	Description
Inherited from keyczar.keyczar.Keyczar (Section 3.2) primary_key, versions	
Inherited from object __class__	

4 Module keyczar.keyczart

Keyczart(ool) is a utility for creating and managing Keyczar keysets.

Author: arkajit.dey@gmail.com (Arkajit Dey)

4.1 Functions

usage()

main(*argv*)

4.2 Class KeyczarTool

5 Module keyczar.keydata

Encodes the two classes storing data about keys:

- KeyMetadata: stores metadata
- KeyVersion: stores key strings and types

Authors: arkajit.dey@gmail.com (Arkajit Dey), steveweis@gmail.com (Steve Weis)

5.1 Class KeyMetadata

object
└ **keyczar.keydata.KeyMetadata**

Encodes metadata for a keyset with a name, purpose, type, and versions.

5.1.1 Methods

__init__(*self*, *name*, *purpose*, *type*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

__str__(*self*)

str(x)

Overrides: object.__str__ extit(inherited documentation)

AddVersion(*self*, *version*)

Adds given version and returns True if successful.

Parameters

`version`: version to add

(type=`KeyVersion`)

Return Value

True if version was successfully added (i.e. no previous version had the same version number), False otherwise.

(type=boolean)

RemoveVersion(*self*, *version_number*)

Removes version with given version number and returns it if it exists.

Parameters

`version_number`: version number to remove

(type=integer)

Return Value

the removed version if it exists or None.

(type=`KeyVersion`)

GetVersion(*self*, *version_number*)

Return the version corresponding to the given version number.

Parameters

`version_number`: integer version number of desired version

(type=integer)

Return Value

the corresponding version if it exists

(type=`KeyVersion`)

Raises

`KeyczarError` if the version number is non-existent.

Read(*json_string*)

Return KeyMetadata object constructed from JSON string representation.

Parameters

`json_string`: a JSON representation of a KeyMetadata object

(type=string)

Return Value

the constructed KeyMetadata object

(type=`KeyMetadata`)

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

5.1.2 Properties

Name	Description
versions	
Inherited from object __class__	

5.2 Class KeyVersion

object
└
keyczar.keydata.KeyVersion

5.2.1 Methods

__init__(*self*, *v*, *s*, *export*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

__str__(*self*)

str(x)

Overrides: object.__str__ extit(inherited documentation)

Read(*version*)

Return KeyVersion object constructed from dictionary derived from JSON.

Parameters

`version:` a dictionary obtained from a JSON string representation

(type=dictionary)

Return Value

constructed KeyVersion object

(type=`KeyVersion`)

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

5.2.2 Properties

Name	Description
status	
Inherited from object __class__	

6 Module keyczar.keyinfo

Defines several 'enums' encoding information about keys, such as type, status, purpose, and the cipher mode.

Authors: arkajit.dey@gmail.com (Arkajit Dey), steveweis@gmail.com (Steve Weis)

6.1 Functions

GetType(*name*)

GetStatus(*value*)

GetPurpose(*name*)

GetMode(*name*)

6.2 Variables

Name	Description
AES	**Value:** `KeyType("AES", 0, [128, 192, 256], 0)`
HMAC_SHA1	**Value:** `KeyType("HMAC_SHA1", 1, [256], 20)`
DSA_PRIV	**Value:** `KeyType("DSA_PRIV", 2, [1024], 48)`
DSA_PUB	**Value:** `KeyType("DSA_PUB", 3, [1024], 48)`
RSA_PRIV	**Value:** `KeyType("RSA_PRIV", 4, [2048, 1024, 768, 512], 256)`
RSA_PUB	**Value:** `KeyType("RSA_PUB", 4, [2048, 1024, 768, 512], 256)`
types	**Value:** {`"AES": AES, "HMAC_SHA1": HMAC_SHA1, "DSA_PRIV": DSA_PRIV...`
PRIMARY	**Value:** `KeyStatus("primary", 0)`
ACTIVE	**Value:** `KeyStatus("active", 1)`
SCHEDULED_FOR_REVOCATION	**Value:** `KeyStatus("scheduled_for_revocation", 2)`
statuses	**Value:** {`"PRIMARY": PRIMARY, "ACTIVE": ACTIVE, "SCHEDULED_FOR_REV...`
DECRYPT_AND_ENCRYPT	**Value:** `KeyPurpose("crypt", 0)`

continued on next page

Name	Description
ENCRYPT	**Value:** `KeyPurpose("encrypt", 1)`
SIGN_AND_VERIFY	**Value:** `KeyPurpose("sign", 2)`
VERIFY	**Value:** `KeyPurpose("verify", 3)`
purposes	**Value:** {"DECRYPT_AND_ENCRYPT": DECRYPT_AND_ENCRYPT, "ENCRYPT": E...
CBC	**Value:** `CipherMode("CBC", 0, True, lambda b, i:(i/ b+ 2)* b)`
CTR	**Value:** `CipherMode("CTR", 1, True, lambda b, i: i+ b/ 2)`
ECB	**Value:** `CipherMode("ECB", 2, False, lambda b, i: b)`
DET_CBC	**Value:** `CipherMode("DET_CBC", 3, False, lambda b, i:(i/ b+ 1)* b)`
modes	**Value:** {"CBC": CBC, "CTR": CTR, "ECB": ECB, "DET_CBC": DET_CBC}

6.3 Class KeyType

object

keyczar.keyinfo._NameId

keyczar.keyinfo.KeyType

Encodes different key types and their properties:

- AES
- HMAC-SHA1
- DSA Private
- DSA Public
- RSA Private
- RSA Public

6.3.1 Methods

__init__(*self*, *name*, *id*, *sizes*, *output_size*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

IsValidSize(*self*, *size*)

Inherited from keyczar.keyinfo._NameId

__str__()

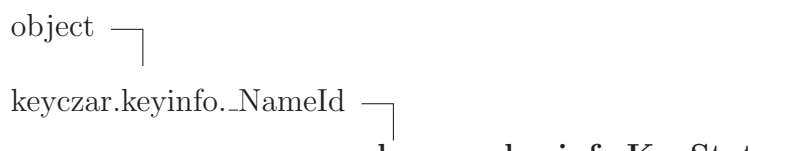
Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

6.3.2 Properties

Name	Description
sizes	List of valid key sizes for this key type.
Inherited from object	
__class__	

6.4 Class KeyStatus



Encodes the different possible statuses of a key:

- Primary: can be used to encrypt and sign new data
- Active: can be used to decrypt or verify data signed previously
- Scheduled for Revocation: can do the same functions as an active key, but status indicates that it is about to be revoked

6.4.1 Methods

Inherited from keyczar.keyinfo._NameId

__init__(), __str__()

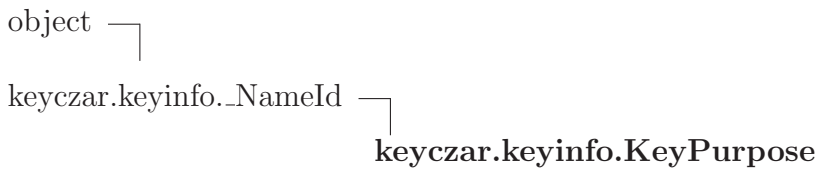
Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

6.4.2 Properties

Name	Description
Inherited from object	
__class__	

6.5 Class KeyPurpose



Encodes the different possible purposes for which a key can be used:

- Decrypt and Encrypt
- Encrypt (only)
- Sign and Verify
- Verify (only)

6.5.1 Methods

Inherited from keyczar.keyinfo._NameId

__init__(), __str__()

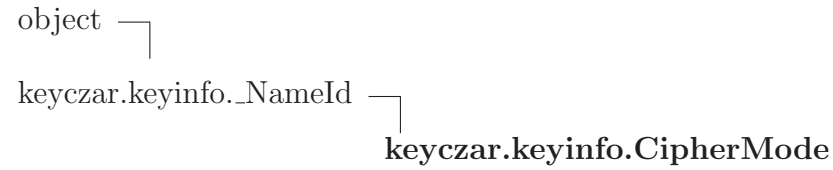
Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

6.5.2 Properties

Name	Description
Inherited from object	
__class__	

6.6 Class CipherMode



Encodes the different possible modes for a cipher:

- Cipher Block Chaining (CBC)
- Counter (CTR)
- Electronic Code Book (ECB)
- Cipher Block Chaining without IV (DET-CBC)

6.6.1 Methods

__init__(*self*, *name*, *id*, *use_iv*, *OutputSizeFn*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from keyczar.keyinfo._NameId

__str__()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

6.6.2 Properties

Name	Description
Inherited from object	
__class__	

7 Module keyczar.keys

Represents cryptographic keys in Keyczar.

Identifies a key by its hash and type. Includes several subclasses of base class Key.

Authors: arkajit.dey@gmail.com (Arkajit Dey), steveweis@gmail.com (Steve Weis)

7.1 Functions

GenKey(*type*, *size*=`None`)

Generates a key of the given type and length.

Parameters

`type`: the type of key to generate

*(type=**keyinfo.KeyType**)*

`size`: the length in bits of the key to be generated

(type=integer)

Return Value

the generated key of the given type and size

Raises

`KeyczarError` if type is a public key or unsupported.

ReadKey(*type*, *key*)

Reads a key of the given type from a JSON string representation.

Parameters

`type`: the type of key to read

*(type=**keyinfo.KeyType**)*

`key`: the JSON string representation of the key

(type=string)

Return Value

the key object read from the JSON string

Raises

`KeyczarError` if type is unsupported

7.2 Class Key

object
└
keyczar.keys.Key

Known Subclasses: keyczar.keys.SymmetricKey, keyczar.keys.AsymmetricKey

Parent class for Keyczar Keys.

7.2.1 Methods

__init__(*self*, *type*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

Header(*self*)

Return the 6-byte header string including version, format, and hash.

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__(), __str__()

7.2.2 Properties

Name	Description
hash	The hash id of the key.
size	The size of the key in bits.
key_string	The key as a Base64 string.
key_bytes	The key as bytes.
Inherited from object __class__	

7.3 Class SymmetricKey

object
keyczar.keys.Key
keyczar.keys.SymmetricKey

Known Subclasses: keyczar.keys.AesKey, keyczar.keys.HmacKey

Parent class for symmetric keys such as AES, HMAC-SHA1

7.3.1 Methods

__**init**__(*self*, *type*, *key_string*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from keyczar.keys.Key(Section 7.2)

Header()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__(), __str__()

7.3.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object __class__	

7.4 Class AsymmetricKey

object
keyczar.keys.Key
keyczar.keys.AsymmetricKey

Known Subclasses: keyczar.keys.PrivateKey, keyczar.keys.PublicKey

Parent class for asymmetric keys.

7.4.1 Methods

__**init**__(*self*, *type*, *params*)
x.__init__(...) initializes x; see x.__class__.__doc__ for signature
Overrides: object.__init__ extit(inherited documentation)

Inherited from keyczar.keys.Key(Section 7.2)

Header()

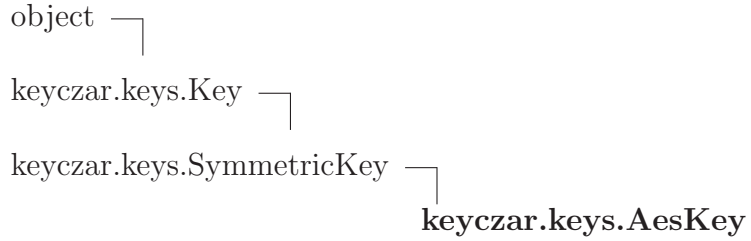
Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__(), __str__()

7.4.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object __class__	

7.5 Class AesKey



Represents AES symmetric private keys.

7.5.1 Methods

__init__(*self*, *key_string*, *hmac_key*, *size*=128, *mode*=CipherMode("CBC", 0, True, lambda b, i:(i/ b+ 2)* b))

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

__str__(*self*)

str(x)

Overrides: object.__str__ extit(inherited documentation)

Generate(*size*=128)

Return a newly generated AES key.

Parameters

`size`: length of key in bits to generate

(type=integer)

Return Value

an AES key

(type=`AesKey`)

Read(*key*)

Reads an AES key from a JSON string representation of it.

Parameters

`key`: a JSON representation of an AES key

(type=string)

Return Value

an AES key

(type=`AesKey`)

Encrypt(*self*, *data*)

Return ciphertext byte string containing Header|IV|Ciph|Sig.

Parameters

`data`: plaintext to be encrypted.

(type=string)

Return Value

raw byte string ciphertext formatted to have Header|IV|Ciph|Sig.

(type=string)

Decrypt(*self*, *input_bytes*)

Decrypts the given ciphertext.

Parameters

`input_bytes`: raw byte string formatted as Header|IV|Ciph|Sig where Sig is the signature over the entire payload (Header|IV|Ciph).

(type=string)

Return Value

plaintext message

(type=string)

Raises

`ShortCiphertextError` if the ciphertext is too short to have IV & Sig

`InvalidSignatureError` if the signature doesn't correspond to payload

Inherited from keyczar.keys.Key(Section 7.2)

Header()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.5.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object	

continued on next page

Name	Description
__class__	

7.6 Class HmacKey

object
└
keyczar.keys.Key
└
keyczar.keys.SymmetricKey
└
keyczar.keys.HmacKey

Represents HMAC-SHA1 symmetric private keys.

7.6.1 Methods

__init__(*self*, *key_string*, *size*=256)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

__str__(*self*)

str(x)

Overrides: object.__str__ extit(inherited documentation)

Generate(*size*=256)

Return a newly generated HMAC-SHA1 key.

Parameters

`size`: length of key in bits to generate

(type=integer)

Return Value

an HMAC-SHA1 key

(type=`HmacKey`)

Read(*key*)

Reads an HMAC-SHA1 key from a JSON string representation of it.

Parameters

`key`: a JSON representation of an HMAC-SHA1 key

(type=string)

Return Value

an HMAC-SHA1 key

(type=`HmacKey`)

Sign(*self*, *msg*)

Return raw byte string of signature on the message.

Parameters

`msg`: message to be signed

(type=string)

Return Value

raw byte string signature

(type=string)

Verify(*self*, *msg*, *sig_bytes*)

Return True if the signature corresponds to the message.

Parameters

`msg`: message that has been signed

(type=string)

`sig_bytes`: raw byte string of the signature

(type=string)

Return Value

True if signature is valid for message. False otherwise.

(type=boolean)

Inherited from keyczar.keys.Key(Section 7.2)

Header()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.6.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object __class__	

7.7 Class PrivateKey

object
└
keyczar.keys.Key
└
keyczar.keys.AsymmetricKey
└
keyczar.keys.PrivateKey

Known Subclasses: keyczar.keys.DsaPrivateKey, keyczar.keys.RsaPrivateKey

Represents private keys in Keyczar for asymmetric key pairs.

7.7.1 Methods

__init__(*self*, *type*, *params*, *pkcs8*, *pub*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

__str__(*self*)

str(x)

Overrides: object.__str__ extit(inherited documentation)

Inherited from keyczar.keys.Key(Section 7.2)

Header()

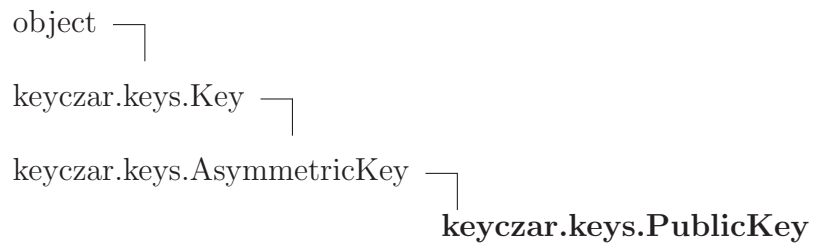
Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.7.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object __class__	

7.8 Class PublicKey



Known Subclasses: keyczar.keys.DsaPublicKey, keyczar.keys.RsaPublicKey

Represents public keys in Keyczar for asymmetric key pairs.

7.8.1 Methods

__init__(*self*, *type*, *params*, *x509*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

__str__(*self*)

str(x)

Overrides: object.__str__ extit(inherited documentation)

Inherited from keyczar.keys.Key(Section 7.2)

Header()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.8.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2)	
hash, key_bytes, key_string, size	
Inherited from object	
__class__	

7.9 Class DsaPrivateKey

object
keyczar.keys.Key
keyczar.keys.AsymmetricKey
keyczar.keys.PrivateKey
keyczar.keys.DsaPrivateKey

Represents DSA private keys in an asymmetric DSA key pair.

7.9.1 Methods

__init__(*self*, *params*, *pkcs8*, *pub*, *key*, *size*=1024)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

Generate(*size*=1024)

Return a newly generated DSA private key.

Parameters

`size`: length of key in bits to generate

(type=integer)

Return Value

a DSA private key

(type=`DsaPrivateKey`)

Read(*key*)

Reads a DSA private key from a JSON string representation of it.

Parameters

`key`: a JSON representation of a DSA private key

(type=string)

Return Value

an DSA private key

(type=`DsaPrivateKey`)

Sign(*self*, *msg*)

Return raw byte string of signature on the message.

Parameters

`msg`: message to be signed

(type=string)

Return Value

signature formatted as r|s where r and s are the long ints in the DSA signature tuple (r,s).

(type=string)

Verify(*self*, *msg*, *sig*)

See Also: `DsaPublicKey.Verify`

Inherited from keyczar.keys.PrivateKey(Section 7.7)

__str__()

Inherited from keyczar.keys.Key(Section 7.2)

Header()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.9.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2)	
hash, key_bytes, key_string, size	

continued on next page

Name	Description
Inherited from object	
__class__	

7.10 Class RsaPrivateKey

object
keyczar.keys.Key
keyczar.keys.AsymmetricKey
keyczar.keys.PrivateKey
keyczar.keys.RsaPrivateKey

Represents RSA private keys in an asymmetric RSA key pair.

7.10.1 Methods

__init__(*self*, *params*, *pkcs8*, *pub*, *key*, *size*=2048)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

Generate(*size*=2048)

Return a newly generated RSA private key.

Parameters

`size`: length of key in bits to generate

(type=integer)

Return Value

a RSA private key

(type=`RsaPrivateKey`)

Read(*key*)

Reads a RSA private key from a JSON string representation of it.

Parameters

`key`: a JSON representation of a RSA private key

(type=string)

Return Value

a RSA private key

(type=`RsaPrivateKey`)

Encrypt(*self*, *data*)

See Also: `RsaPublicKey.Encrypt`

Decrypt(*self*, *input_bytes*)

Decrypts the given ciphertext.

Parameters

`input_bytes`: raw byte string formatted as Header|Ciphertext.

(type=string)

Return Value

plaintext message

(type=string)

Sign(*self*, *msg*)

Return raw byte string of signature on the message.

Parameters

`msg`: message to be signed

(type=string)

Return Value

string representation of long int signature over message

(type=string)

Verify(*self*, *msg*, *sig*)

See Also: `RsaPublicKey.Verify`

Inherited from keyczar.keys.PrivateKey(Section 7.7)

__str__()

Inherited from keyczar.keys.Key(Section 7.2)

Header()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.10.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object __class__	

7.11 Class DsaPublicKey

Represents DSA public keys in an asymmetric DSA key pair.

7.11.1 Methods

__**init**__(*self*, *params*, *x509*, *key*, *size*=`1024`)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

Read(*key*)

Reads a DSA public key from a JSON string representation of it.

Parameters

`key`: a JSON representation of a DSA public key

(type=string)

Return Value

a DSA public key

(type=`DsaPublicKey`)

Verify(*self*, *msg*, *sig*)

Return True if the signature corresponds to the message.

Parameters

`msg`: message that has been signed

(type=string)

`sig`: raw byte string of the signature formatted as r|s

(type=string)

Return Value

True if signature is valid for message. False otherwise.

(type=boolean)

Inherited from keyczar.keys.PublicKey(Section 7.8)

__str__()

Inherited from keyczar.keys.Key(Section 7.2)

Header()

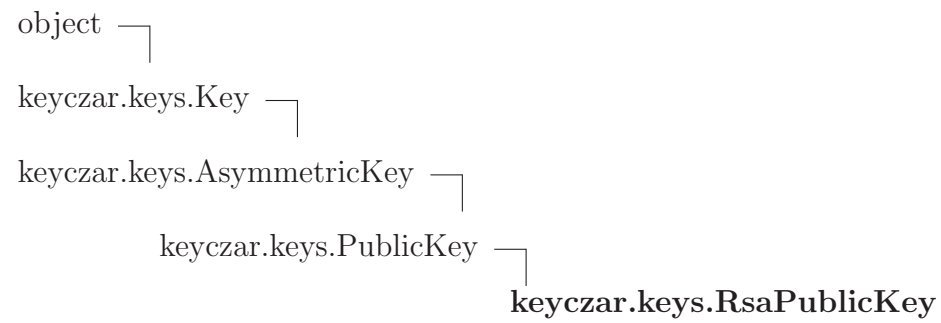
Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.11.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object __class__	

7.12 Class RsaPublicKey



Represents RSA public keys in an asymmetric RSA key pair.

7.12.1 Methods

__init__(*self*, *params*, *x509*, *key*, *size*=2048)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

Read(*key*)

Reads a RSA public key from a JSON string representation of it.

Parameters

`key`: a JSON representation of a RSA public key

(type=string)

Return Value

a RSA public key

(type=`RsaPublicKey`)

Encrypt(*self*, *data*)

Return a raw byte string of the ciphertext in the form Header|Ciph.

Parameters

`data`: message to be encrypted

(type=string)

Return Value

ciphertext formatted as Header|Ciph

(type=string)

Verify(*self*, *msg*, *sig*)

Return True if the signature corresponds to the message.

Parameters

`msg`: message that has been signed

(type=string)

`sig`: string representation of long int signature

(type=string)

Return Value

True if signature is valid for message. False otherwise.

(type=boolean)

Inherited from keyczar.keys.PublicKey(Section 7.8)

__str__()

Inherited from keyczar.keys.Key(Section 7.2)

Header()

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__()

7.12.2 Properties

Name	Description
Inherited from keyczar.keys.Key (Section 7.2) hash, key_bytes, key_string, size	
Inherited from object __class__	

8 Module keyczar.readers

A Reader supports reading metadata and key info for key sets.

Authors: arkajit.dey@gmail.com (Arkajit Dey), steveweis.gmail.com (Steve Weis)

8.1 Class Reader

object
└ **keyczar.readers.Reader**

Known Subclasses: keyczar.readers.FileReader

Interface providing supported methods (no implementation).

8.1.1 Methods

GetMetadata(*self*)

Return the KeyMetadata for the key set being read.

Return Value

JSON string representation of KeyMetadata object

(type=string)

GetKey(*self*, *version_number*)

Return the key corresponding to the given version.

Parameters

`version_number`: the version number of the desired key

(type=integer)

Return Value

JSON string representation of a Key object

(type=string)

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __init__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__(), __str__()

8.1.2 Properties

Name	Description
Inherited from object	
__class__	

8.2 Class FileReader

object
keyczar.readers.Reader
keyczar.readers.FileReader

Reader that reads key data from files.

8.2.1 Methods

__init__(*self*, *location*)

x.__init__(...) initializes x; see x.__class__.__doc__ for signature

Overrides: object.__init__ extit(inherited documentation)

GetMetadata(*self*)

Return the KeyMetadata for the key set being read.

Return Value

JSON string representation of KeyMetadata object

(type=string)

Overrides: keyczar.readers.Reader.GetMetadata extit(inherited documentation)

GetKey(*self*, *version_number*)

Return the key corresponding to the given version.

Parameters

`version_number`: the version number of the desired key

Return Value

JSON string representation of a Key object

(type=string)

Overrides: keyczar.readers.Reader.GetKey extit(inherited documentation)

Inherited from object

__delattr__(), __getattribute__(), __hash__(), __new__(), __reduce__(), __reduce_ex__(), __repr__(), __setattr__(), __str__()

8.2.2 Properties

Name	Description
Inherited from object	
__class__	

9 Module keyczar.util

Utility functions for keyczar package.

Author: arkajit.dey@gmail.com (Arkajit Dey)

9.1 Functions

ParsePkcs8(*pkcs8*)

ExportRsaPkcs8(*params*)

ExportDsaPkcs8(*params*)

ParseX509(*x509*)

ExportRsaX509(*params*)

ExportDsaX509(*params*)

BinToBytes(*bits*)

Convert bit string to byte string.

BytesToBin(*bytes*)

Convert byte string to bit string.

IntToBin(*n*)

IntToBytes(*n*)

Return byte string of 4 big-endian ordered bytes representing n.

RandBytes(*n*)

Return n random bytes.

Hash(*inputs*)

Return a SHA-1 hash over a list of inputs.

Encode(*s*)

Return Base64 encoding of s. Suppress padding characters (=).

Uses URL-safe alphabet: - replaces +, _ replaces /. Will convert s of type unicode to string type first.

Parameters

`s`: string to encode as Base64

(type=string)

Return Value

Base64 representation of s.

(type=string)

Decode(*s*)

Return decoded version of given Base64 string. Ignore whitespace.

Uses URL-safe alphabet: - replaces +, _ replaces /. Will convert s of type unicode to string type first.

Parameters

`s`: Base64 string to decode

(type=string)

Return Value

original string that was encoded as Base64

(type=string)

Raises

`Base64DecodingError` If length of string (ignoring whitespace) is one more than a multiple of four.

9.2 Variables

Name	Description
RSA_OID	**Value:** `ObjectIdentifier('1.2.840.113549.1.1.1')`
RSA_PARAMS	**Value:** `['n', 'e', 'd', 'p', 'q', 'dp', 'dq', 'invq']`
DSA_OID	**Value:** `ObjectIdentifier('1.2.840.10040.4.1')`
DSA_PARAMS	**Value:** `['p', 'q', 'g']`

Index