Module sui::ecdsa_r1

Error if the public key cannot be recovered from the signature.

Error if the signature is invalid.

Hash function name that are valid for ecrecover and secp256k1_verify.

@param signature: A 65-bytes signature in form (r, s, v) that is signed using Secp256r1. Reference implementation on signature generation using RFC6979: https://github.com/MystenLabs/fastcrypto/blob/74aec4886e62122a5b769464c2bea5f803cf8ecc/fastcrypto/src/secp256r1/mod.rs The accepted v values are {0, 1, 2, 3}. @param msg: The message that the signature is signed against, this is raw message without hashing. @param hash: The u8 representing the name of hash function used to hash the message when signing.

If the signature is valid, return the corresponding recovered Secpk256r1 public key, otherwise throw error. This is similar to ecrecover in Ethereum, can only be applied to Secp256r1 signatures. May fail with EFailToRecoverPubKey or EInvalidSignature .

@param signature: A 64-bytes signature in form (r, s) that is signed using Secp256r1. This is an non-recoverable signature without recovery id. Reference implementation on signature generation using RFC6979: https://github.com/MystenLabs/fastcrypto/blob/74aec4886e62122a5b769464c2bea5f803cf8ecc/fastcrypto/src/secp256r1/mod.rs @param public_key: The public key to verify the signature against @param msg: The message that the signature is signed against, this is raw message without hashing. @param hash: The u8 representing the name of hash function used to hash the message when signing.

If the signature is valid to the pubkey and hashed message, return true. Else false.

Constants

Error if the public key cannot be recovered from the signature.

```bash
```

Error if the signature is invalid.

```bash
```

Hash function name that are valid for ecrecover and secp256k1_verify.

```bash
```

```bash
```

@param signature: A 65-bytes signature in form (r, s, v) that is signed using Secp256r1. Reference implementation on signature generation using RFC6979: https://github.com/MystenLabs/fastcrypto/blob/74aec4886e62122a5b769464c2bea5f803cf8ecc/fastcrypto/src/secp256r1/mod.rs The accepted v values are {0, 1, 2, 3}. @param msg: The message that the signature is signed against, this is raw message without hashing. @param hash: The u8 representing the name of hash function used to hash the message when signing.

If the signature is valid, return the corresponding recovered Secpk256r1 public key, otherwise throw error. This is similar to ecrecover in Ethereum, can only be applied to Secp256r1 signatures. May fail with EFailToRecoverPubKey or EInvalidSignature .

```bash
```

```bash
```

@param signature: A 64-bytes signature in form (r, s) that is signed using Secp256r1. This is an non-recoverable signature without recovery id. Reference implementation on signature generation using RFC6979: https://github.com/MystenLabs/fastcrypto/blob/74aec4886e62122a5b769464c2bea5f803cf8ecc/fastcrypto/src/secp256r1/mod.rs @param public_key: The public key to verify the signature against @param msg: The message that the signature is signed against, this is raw message without hashing. @param hash: The u8 representing the name of hash function used to hash the message when signing.

If the signature is valid to the pubkey and hashed message, return true. Else false.

```bash

```

```bash

```

Function

@param signature: A 65-bytes signature in form (r, s, v) that is signed using Secp256r1. Reference implementation on signature generation using RFC6979: https://github.com/MystenLabs/fastcrypto/blob/74aec4886e62122a5b769464c2bea5f803cf8ecc/fastcrypto/src/secp256r1/mod.rs The accepted v values are {0, 1, 2, 3}. @param msg: The message that the signature is signed against, this is raw message without hashing. @param hash: The u8 representing the name of hash function used to hash the message when signing.

If the signature is valid, return the corresponding recovered Secpk256r1 public key, otherwise throw error. This is similar to ecrecover in Ethereum, can only be applied to Secp256r1 signatures. May fail with EFailToRecoverPubKey or EInvalidSignature .

```bash

```

```bash

```

@param signature: A 64-bytes signature in form (r, s) that is signed using Secp256r1. This is an non-recoverable signature without recovery id. Reference implementation on signature generation using RFC6979: https://github.com/MystenLabs/fastcrypto/blob/74aec4886e62122a5b769464c2bea5f803cf8ecc/fastcrypto/src/secp256r1/mod.rs @param public_key: The public key to verify the signature against @param msg: The message that the signature is signed against, this is raw message without hashing. @param hash: The u8 representing the name of hash function used to hash the message when signing.

If the signature is valid to the pubkey and hashed message, return true. Else false.

```bash

```

```bash

```

Function

@param signature: A 64-bytes signature in form (r, s) that is signed using Secp256r1. This is an non-recoverable signature without recovery id. Reference implementation on signature generation using RFC6979: https://github.com/MystenLabs/fastcrypto/blob/74aec4886e62122a5b769464c2bea5f803cf8ecc/fastcrypto/src/secp256r1/mod.rs @param public_key: The public key to verify the signature against @param msg: The message that the signature is signed against, this is raw message without hashing. @param hash: The u8 representing the name of hash function used to hash the message when signing.

If the signature is valid to the pubkey and hashed message, return true. Else false.

```bash

```

```bash

```