Spécifications pour le Composant de Récupération de la Clé Publique d'une Signature ECDSA

Auteur : Giovanni AMOUSSOU

Historique des versions

Version 1.0 (28 mai 2023) : Première version du document

Table des matières

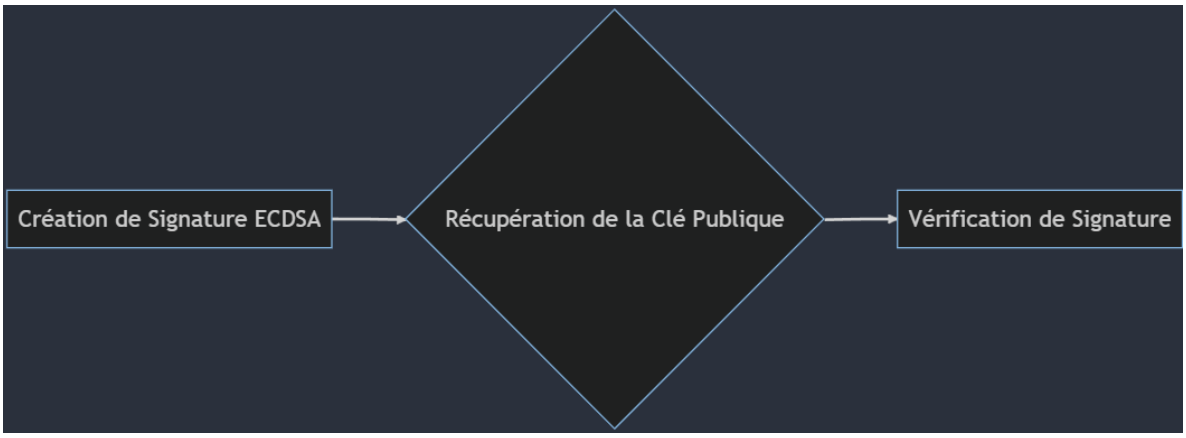
I. Description....2
1. Contexte :....2
2. Schéma bloc incluant les composants connexes :....2
3. Interface et interaction avec chaque autre composant :....2
4. Cas d'erreurs :....2
II. Test....3
1. Plan de test :....3
2. Programme de test :....3
3. Mode d'emploi :....3

I. Description

1. Contexte :

La récupération de la clé publique d'une signature ECDSA est un processus crucial dans la vérification de l'intégrité et de l'authenticité d'un message numérique. Ce composant facilite cette tâche en fournissant une interface simple pour extraire la clé publique à partir d'une signature ECDSA donnée.

2. Schéma bloc incluant les composants connexes :



3. Interface et interaction avec chaque autre composant :

Le composant reçoit une signature ECDSA de la part du module de création de signatures.

Le composant fournit la clé publique extraite au module de vérification de signatures.

```
def recover_public_key(signature: bytes) -> bytes:
    """
    Récupère la clé publique à partir d'une signature ECDSA.

    :param signature: La signature ECDSA.
    :return: La clé publique.
    :raises ValueError: Si la signature est invalide.
    """
```

4. Cas d'erreurs :

Si la signature fournie est invalide, le composant lève une exception ValueError.

II. Test

1. Plan de test :

Le composant sera testé en utilisant un ensemble de signatures ECDSA et de clés publiques connues. Pour chaque paire de clés, le composant doit récupérer avec succès la clé publique à partir de la signature.

2. Programme de test :

```python
def test_recover_public_key():
    # Créez une paire de clés ECDSA (privée et publique)
    private_key, public_key = create_ecdsa_keypair()

    # Créez une signature avec la clé privée
    signature = create_ecdsa_signature(private_key, message)

    # Récupérez la clé publique à partir de la signature
    recovered_public_key = recover_public_key(signature)

    # Vérifiez que la clé publique récupérée correspond à la clé publique originale
    assert recovered_public_key == public_key

```

3. Mode d'emploi :

Pour exécuter le programme de test, lancez simplement la fonction *test_recover_public_key().* Si la fonction s'exécute sans lever d'exception, cela signifie que le composant fonctionne correctement. Sinon, si une exception est levée, le composant a échoué au test.