**Document des spécifications**

**ECDSA signifie « [Elliptic Curve Digital Signature Algorithm](http://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm) »**

**Réalisé par : Samar RHILANE – Luiz – Taoufik**

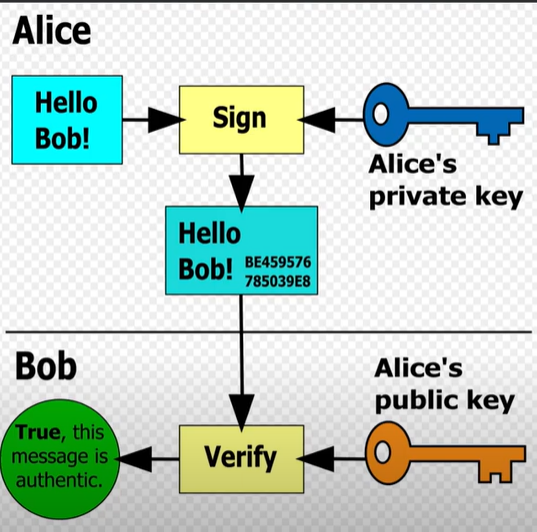
1. **Description**
   1. **Contexte**

**Qu’est-ce que l’ECDSA ?**

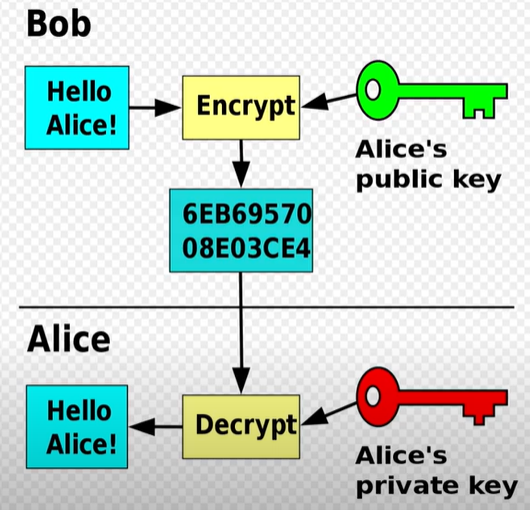
ECDSA est utilisé pour créer une signature numérique de données (un fichier par exemple) afin de nous permettre de vérifier leur authenticité sans compromettre leur sécurité. Pensons-nous comme une vraie signature, nous pouvons reconnaître la signature de quelqu’un, mais nous ne pouvons pas la falsifier sans que les autres le sachent. La différence entre une signature ECDSA et une signature réelle est qu’il est tout simplement impossible de falsifier la signature ECDSA.

**La différence entre le cryptage/chiffrage et la signature**

ECDSA ne crypte pas ou n’empêche pas quelqu’un de voir ou d’accéder aux données, cependant, il les protège, c’est de s’assurer que les données n’ont pas été falsifiées.



**Signature et vérification d’authenticité**



**Cryptage et décryptage**

Le but n'est pas de rendre le message super secret mais plutôt de vérifier que le message provient de la bonne destination

* 1. **Schéma bloc incluant les composants connexes**
  2. **Interface et interaction avec chaque autre composant**
  3. **Résumé: déclarations de fonctions python d’interface et leurs arguments**
  4. **Cas d’erreurs**

1. **Tests**

Reference: [Understanding How ECDSA Protects Your Data. : 15 Steps - Instructables](https://www.instructables.com/Understanding-how-ECDSA-protects-your-data/)