**Documentazione Keyring**

Il Keyring è una classe innestata della classe User, in maniera tale

Che uno User può avere un solo Keyring (pattern Singleton)

Lo user viene caratterizzato dal suo nominativo e al momento

Dell’istanza dello user viene creato il Keyring, completo delle chiavi private

e pubblica di cifratura e firma, simmetriche ed asimmetriche, codificate in un file cifrato.

Lo User è in grado di sbloccare il file cifrato (Keyring) tramite la sua password,

che supponiamo essere nota solo allo stesso User.

Lo User è anche in grado di aggiungere password per siti web al keyring,

accessibile in lettura e scrittura nuovamente solo con la password.

Le password sono memorizzate in maniera sicura all’interno del keyring,

per evitare che in caso di rottura del Keyring stesso l’attaccante possa risalire alle

password: infatti la password del generico sito web inserita dall’utente viene concatenata

ad un salt randomico e poi ne viene calcolato l’hash tramite SHA-512, ed è questa

informazione, insieme al nome del sito web corrispondente, che verrà scritta nel

keyring.