La complexité des mots de passe Qubes est évaluée en termes de résistance à une attaque en force brute contre le hash du mot de passe, exprimée sous la forme d'un nombre de « bits » de complexité.

Un mot de passe de force N bits sera cassable en O(2^N) tentatives, ainsi une force 20 est environ 1000 fois plus résistante qu'une force 10. Il est recommandé une force de 60 bits ou plus (environs 10^18 tentatives).

La métrique suivante est utilisée

- une sous-chaine présente parmi les 10000 mots de passes les plus fréquents est comptabilisée pour 4.9 bits environ (par occurrence complète)
- un charactère alphabétique compte pour 4.7 bits
- un caractère numérique compte pour 3.3 bits
- une caractère ni-numérique ni alphabétique compte pour 4.9 bits

La prise en compte des mots de passe fréquents permet une évaluation plus réaliste de la complexité que des critères plus naïfs basés sur la longueur ou les caractères présents. Un exemple typique étant celui de mots de passes constitués de séquences comme « azerty » ou « 1234 ».

Pour Qubes 2016 – 2020, l'algorithme de hachage est PBKDF2-SHA2 avec 20000 tours.

A partir de Qubes v9.22.1.18 une option de renforcement du sel de 72bits supplémentaires est disponible.