CipherShed - Task #9

Create check-list of features to be tested

07/31/2014 05:36 PM - Bill Cox

Status:	New	**Start date:**	07/31/2014
Priority:	Normal	**Due date:**	
Assignee:	Pier-Luc Caron St-Pierre	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.7.3 Alpha	**Spent time:**	0.00 hour

Description

We should start a check-list for features to be tested before releases, such as full-disk-encryption on Windows and upgrading from TrueCrypt on all platforms.

History

#1 - 07/31/2014 07:44 PM - Bill Cox

- Tracker changed from Bug to Task

- Assignee set to Bill Cox

#2 - 07/31/2014 08:08 PM - Bill Cox

- Target version set to 0.7.3 Alpha

#3 - 07/31/2014 10:36 PM - Bill Cox

- Assignee deleted (Bill Cox)

#4 - 08/01/2014 10:47 AM - Pier-Luc Caron St-Pierre

- Assignee set to Pier-Luc Caron St-Pierre

#5 - 09/21/2014 04:44 AM - Pier-Luc Caron St-Pierre

- Operating system * Windows * Windows XP * Windows Vista * Windows 7 * Windows 8 * Linux * Debian * Fedora * Arch * OS X * 10.9

Encryption algorithms * Algorithms * AES * Serpent * Twofish * AES-Twofish * AES-Twofish-Serpent * Serpent-AES * Serpent-Twofish-AES * Twofish-Serpent * Encryption Test Vectors * XTS mode * Encrypt * Decrypt * Auto-Test All * Reset * Benchmark * Buffer size * 1024 KB * 5.0 MB * 10.0 MB * 50.0 MB * 100 MB * 200 MB * 500 MB * 1024 MB

Hash algorithms * RIPEMD-160 * SHA-512 * Whirlpool
Filesystems Options * FAT * Ext2 * Ext3 * Ext4 * Quick format * Cross-Platform Support

Volume format * Random pool from computer activity * Do not show keys * Aborting volume format

Note * When required, CipherShed asks for the user password for operations that required elevated privileges.

- Volume creation * Volume location history * Show history * Never save history * Encrypted file container * Standard volume * Hidden volume * Volume within a partition * Standard volume * Hidden volume * Volume Size * KB * MB * GB * Password * Display password * Select keyfiles * Validation and confirmation of easy password

- Key files * Key file generator * Algo * RIPEMD-160 * SHA-514 * Whirlpool * Default keyfiles * Add files * Add path * Add token files

- Manage security token keyfiles
- Close all security token session
- PKCS#11 Library path * Close token session after a volume is successfully mounted

- Volume mounting * Selecting a mounting slot * Select a file * Select a device * 'Never save history' * Mount volume as read-only * Mount partition using system encryption (preboot authentication) * Hidden volume protection * Do not mount filesystem
- Volume dismouting

- Auto-mount all devices-hosted volumes
- Dismount all volumes

- Change volume password
- Change header key deviation algorithm
- Add/Remove key file to/from volume
- Backup volume header
- Restore volume header

- Favorites * Add selected volume to favorite * Add all mounted volume to favorite * Organize favorite * Mount volume favorite

- Wipe cache

All those options are configurable:

- Preserve modification timestamp of file containter
- Password cache * Wipe after CipherShed window has been closed
- Mount options * Mount volumes as read-only * Cache passwords in memory * Mount options
- Background task * Enabled * Exit when there no mounted volumes
- Task icon menu item (enabled action are configurable) * Mount favorites volumes * Open mounted volumes * Dismount mounted volumes
- Open explorer window for succesfully mounted vlume
- Use kernel cryptographic service
- Accelerate AES encryption/decryption by using the AES instructions of the processor

All created partiton, key file, container should be compatible between OS and with TrueCrypt version 7.1a unless explicitely specified.