

SafeTok InfoShow – Multi Media User Interface.



Each SafeTok drive (biometric or non biometric) incorporates a multi media enabled, dashboard style, user interface which runs automatically when the drive is inserted into a USB port on a Windows PC or laptop.



The user interface displays html files which are stored in a read only partition on the SafeTok drive and which cannot be deleted by the user. In addition to storing static text, images and hyperlinks to both internal and external web pages the interface can display and run multi media files which can also be stored securely and locally and run offline or stored remotely and streamed to the user via an internet connection. The UI is completely customisable for the service provider, the internally stored content is auto updatable and links to specific content whether internally stored or on line can auto run.



The user interface is integrated with SafeTok protection against key stroke loggers, man in the middle attacks and phishing attempts. The SafeTok device is used to authenticate the user to the service providers' website.

The SafeTok user interface is https enabled allowing users to move safely through all stages of the sale and connect securely, via https to an online donation page or a shopping cart.

Transaction confirmation messages, receipts or thank you letters can be delivered electronically directly to either the public or private (encrypted) partition of the users SafeTok device.



A typical example might look something like the following:



A user logs into their PC using SafeTok Biometric for Windows login and Windows 7 BitLocker authentication.

Once an internet connection is established SafeTok checks for any updates and/or any new content, files or messages.

Content can be "pushed" directly to the user from any web based source such as the SafeTok media server, a service providers own servers or from third party multi media content hosting providers such as YouTube.

SafeTok dynamically apportions secure storage space. If a video file is downloaded to a drive for viewing offline and the file size is larger than the available storage space then SafeTok can “overflow” partial or complete files either to another removable storage device or to a hard disk drive.

Complex file structures are maintained and download automatically resumes if the connection is interrupted or lost.



In this example the service provider is a charity and is asking for donations to help the survivors of a natural disaster.

The news is just hours old so the charity at this point is relying on aggregated third party content from news media, twitter and YouTube postings.

A video announcing the appeal is prepared and uploaded to the either the service providers own servers or the SafeTok media server.

As SafeTok users log in their SafeTok device requests any new content from the server. In this case there is a new streaming video available. They are notified of the appeal and the video is delivered to them via the SafeTok user interface.



The appeal asks for donations and directs users to a secure donations page. SafeTok is used to authenticate the user to the donations site, protects them from keystroke loggers and man in the middle attacks. Once a donation has been made an electronic transaction confirmation is delivered directly to the donors SafeTok device.

New multi media content can be made available at any time as news is updated and new appeals are launched.