

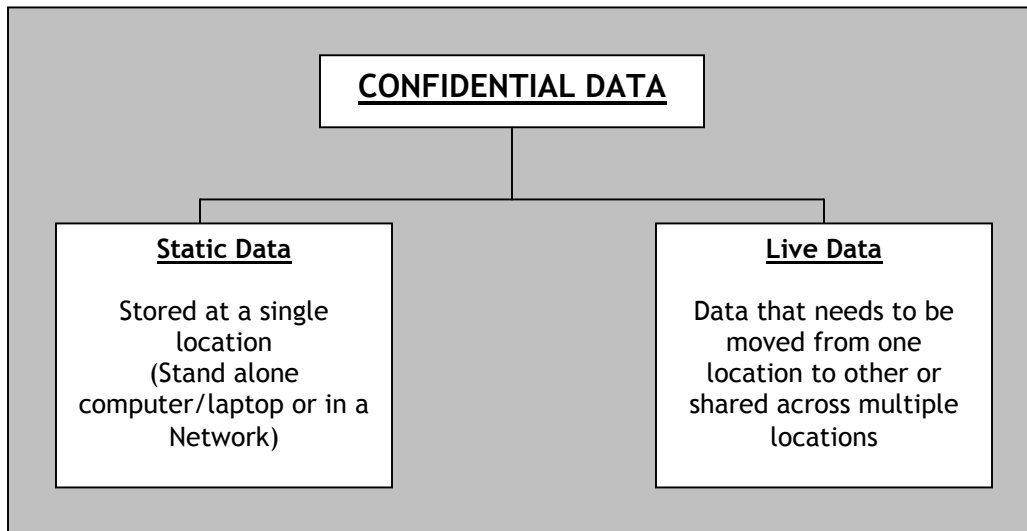
## **Biometric Document Exchange System**

'Effective Communication' is undoubtedly the single most significant cornerstone of the IT revolution. Exchange of information, quickly and effectively, has become a necessity rather than a luxury, as a result of almost every corporate having multiple office locations.

Tutis Biometric Logon (TBL 3.0) gives you end-to-end security for your data as well as network resources and applications. TBL 3.0 enables verifiable & secure transfer of information between two or more parties, each having access to the biometric identity verification system.

### **Data Security with TBL3.0**

Data can be classified as follows



Tutis Biometric Logon not only secures your data, but also enables you to ensure 100 % secure data transactions via email, Internet or network connection. This essentially means that TBL 3.0 protects your data from theft or access by unauthorized personnel during the process of data exchange across different locations. It also helps you protect the critical data on your laptop/computer/network against theft or misuse.

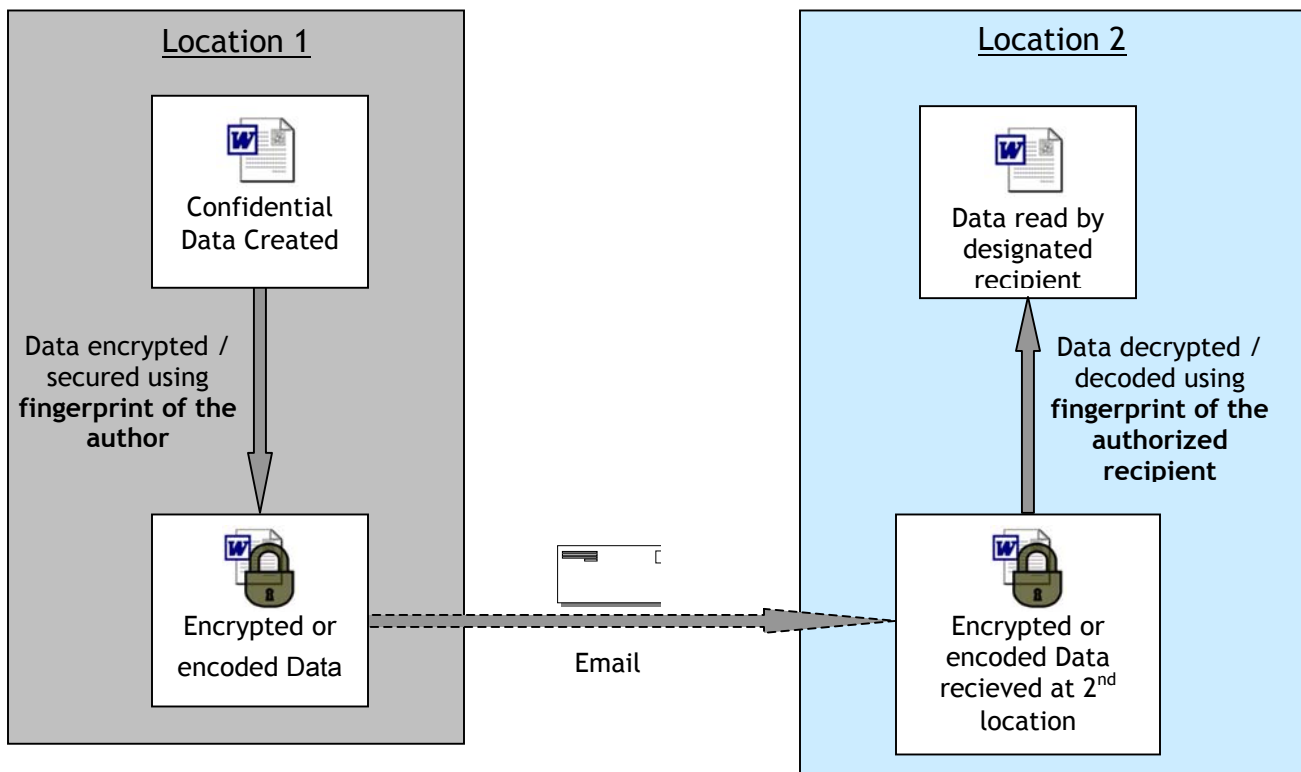
Data transaction can be of the following four types

- Exchange of data via Email
- Sharing of data in a connected Network (LAN / WAN / VPN)
- Data sharing on the Internet
- Physical transfer of data using Flash Drives and other storage devices

Let us look at how TBL ensures maximum security for your data in each of these transaction scenarios

### Secure data exchange using Email

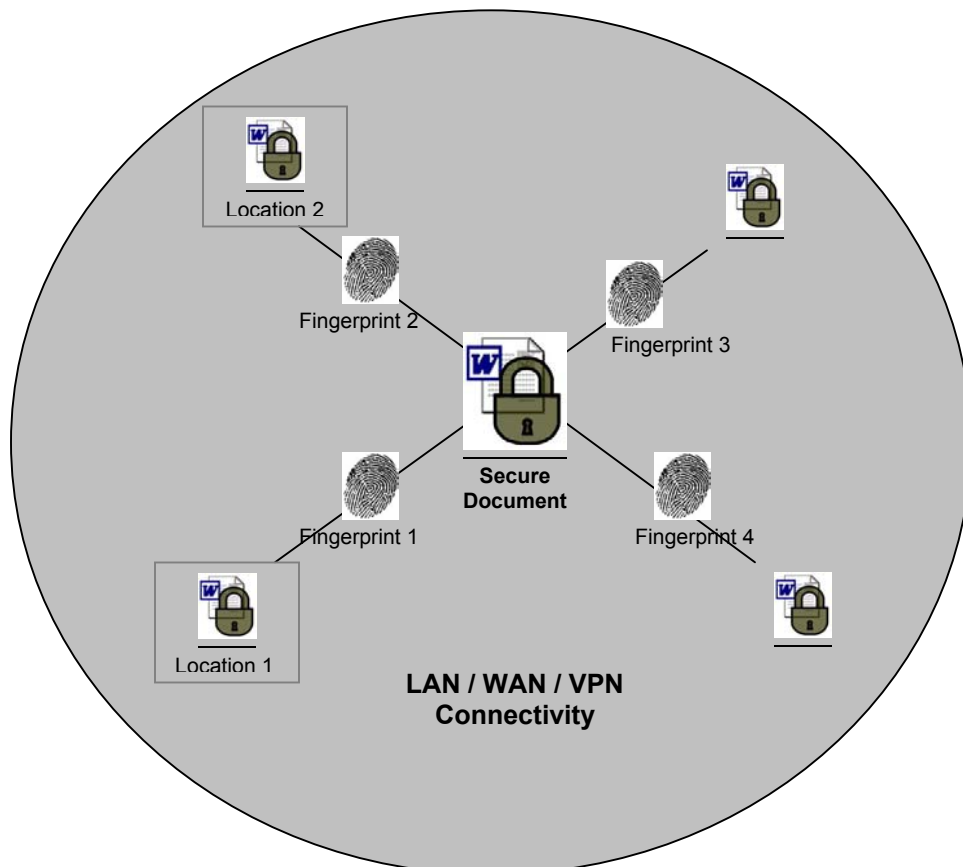
Tutis enables you to send and receive confidential information via Email under totally secure conditions. The flowchart shown below illustrates the process.



As seen from the flowchart, the author using his fingerprint can secure any confidential file. A process called 'Encryption' which is similar to the data being coded secures data. Tutis enables you to encrypt any file such that it can be decrypted or decoded using only the fingerprint of the author, thus ensuring that only an authorized receiving party gains access to the secured information.

This encrypted file can be mailed to a 2<sup>nd</sup> location, where the designated personnel (who is authorized to view this file) can decrypt the file using his fingerprint.

### Secure sharing of data in a connected Network (LAN / WAN / VPN)



With state-of-the-art connectivity technologies, world around us has shrunk to a mere table space. Any data can be made available anywhere in a mouse click, enabling easier information exchange in a jiffy. But along with technology there is a constant fear of breach of

networks not only from the external sources & but as well as internal social engineering. This in itself is a direct application area for Biometric Technology.

Tutis equips network users to securely exchange important data file by encrypting these files in a proprietary 128-bit encryption that uses your fingerprint impression to encrypt the data. In case you want to share a file with someone in the network and that someone is the part of your domain, you can simple add this user as an AFID (Additional Finger Print Identity) and send this file to the intended recipient. The recipient in turn decrypts the file using his own fingerprint eliminating the need of a physical messenger to solicit the service and important information can be shared as and when required.

Apart from faster information exchange, Tutis Biometric Logon software takes away the management in the entire process and enhances information flow across networks.

### **Secure sharing of data using Internet**

Internet being the mother of all networks connects the entire globe through its reach and ease of usage. But then, the Internet as a medium also possesses serious threats to security of data. As it is a highway of connectivity, verifying credentials of users hooked on to the Internet is a voluminous challenge.

Tutis Biometric Logon solution guarantees secure information exchange even on the Internet. For this you are required to simply install Tutis Fingerprint Database on your web server. This database securely stores the fingerprint data of all the key people. Any authorized user who wishes to exchange information can utilize the fingerprint data and add this fingerprint as AFID (Additional Finger Print Identity) and share important files over the Internet as well. It is very important here to understand that the intended recipient needs to be physically present when the file is being decrypted. In other words the person who either encrypts or decrypts the data do so after they confirm their credentials physically and are eligible to execute the said processes.

### **Secure sharing of data without Connectivity**

Consider a case where files have to be shared without direct connectivity. Email transaction is on email clients is a classic example for these kind of file exchanges. In cases where file transactions happen over emails; data theft is a common occurrence. Unauthorized miscreants can intercept emails and data can be stolen.

Tutis Biometric Logon solution addresses this problem via fingerprint sharing facility. Your intended recipient can send you his fingerprint via email and the same can be added as AFID for encrypting files that have to be sent through emails. After the recipient receives this file he can decrypt the data for usage.

Even if the email is intercepted in between, it is useless as data cannot be deciphered unless you have a valid fingerprint to decrypt the file.