Storage of private key

Sl. No	Storage media	Advantages	Disadvantages
1.	Computer Hard Disk	Easiest	1. Computer must be maintained in a secure fashion (access should be restricted etc.) 2. Any backups taken must also be protected is a similar way as they will contain a copy of the private key.
2.	Floppy	1. Easy to use 2. Can be carried on person	1. Private key can be taken out of the floppy. 2. Floppy may get corrupted. 3. The device does not contain any cryptographic module built into it to enable the creation of secure digital signature. 4. In case of Floppy the private key can be overwritten.
3.	CD-R/RW	1. Easy to use 2. Can be carried on person	1. Private key can be taken out of the CD-R/RW. 2. CD-R/RW may get corrupted. 3. The device does not contain any cryptographic module built into it to enable the creation of secure digital signature. 4. In case of CD-RW the private key can be overwritten.
4.	Pen Drives/USB Drives/Flash Drives	1. Easy to use 2. Can be carried on person	1. Private key can be taken out of the USB drive. 3. The device does not contain any cryptographic module built into it to enable the creation of secure digital signature. 4. In case of USB Drive the private key can be overwritten.
5.	Smart Cards	1. Once generated on the smart card **the private key does not come out of the device in its original form**. 2. The smart card has **a chip built into it, which has crypto modules** to enable the signing/encryption/decryption operation to happen in the card itself.	1. Requires a smart card reader to be attached to the computer. 2. Cost is more.
6.	USB Crypto Tokens	1. Once generated on the USB crypto token **the private key does not come out of the device in its original form**. 2. The USB crypto token **has crypto modules** to enable the signing/encryption/decryption operation to happen in the token itself. 3. Does not require any special reader, can be used on any machine since USB ports are available on almost all PCs.	1. Cost is more.

The Gazette Notification 735(E) dated 24th October 2004, contains the Rules to be read in conjunction with section 16 of the IT Act 2000. It defines the Secure Electronic Record to be one that has been authenticated by means of a Secure Digital Signature. To create a Secure Digital Signature **a smart card or hardware token with cryptographic module** has be used to create the key pair. The **private key remains in the device** at any point in time. The content to be signed should go from the host system to the smart card/hardware token and the signed content to be returned to the host system. The cryptographic modules must follow FIPS 140-1 level 3 standard as stipulated in the Regulations 4. (1)(d). As per the notification, in the above table, only No.5 and No.6 can be used to create Secure Electronic Records and Secure Digital Signatures.