

# DECIDING ON A CRYPTOCARD TOKEN – Which Type Do I Want?

Currently, there are 4 types of CRYPTOCARD Token to choose from. How do you decide which type you want?

## The 4 types of CRYPTOCARD Tokens:

**RB-1** (*Hardware*-based Token which is metal-encased and about the size of a credit-card)

**KF-1** (*Hardware*-based Token which is metal-encased and hangs on a key-chain)

**ST-1** (*Software*-based Token application for Windows/Unix/Linux-based systems)

**PT-1** (*Software*-based Token application for PalmPilots)

### TOKEN

### PROS

### CONS

#### **RB-1**

(Hardware-based; credit-card sized)

- Easily portable for use from many machines.

- Can physically *forget* it and leave it behind;  
- Can be physically damaged by dropping, crushing, or sitting on it, by bending, twisting or carrying in hip pocket wallet, by immersing in water, by exposing it to extreme heat/cold, by dismantling it or by placing heavy objects on it.

#### **KF-1**

(Hardware-based; hangs on key-chain)

- Easily portable for use from many machines;  
- If attached to a key-chain, user less likely to *forget* it and leave it behind;  
- A bit less susceptible to physical damage than the RB-1 token since it can hang from a key-chain vs. attempting to carry in hip pocket wallet against vendor's recommendations.

- If user's token falls out of synch (which may happen occasionally) user CANNOT bring into synchronization themselves but instead must physically bring to Password Office to re-synch;  
- Currently, user cannot change their PIN on their own;  
- Although potentially less susceptible to physical damage than the RB-1, the KF-1 can *still* be damaged by dropping, crushing, or sitting on it, by bending or twisting, by immersing in water, by exposing it to extreme heat/cold, by dismantling it or by placing heavy objects on it.

#### **ST-1**

(Software-based for Windows, Unix, Linux)

- When application is loaded on a Windows, Solaris and/or Redhat Linux machine, user has no need to carry a physical token;  
- User can load software token application on more than one machine and more than one *type* of machine (i.e., can load on Windows machine AND on SUN Solaris machine AND on Redhat Linux machine);  
- When troubleshooting a token, Password Office can re-issue a new token without user needing to physically appear at Password Office.

- Argued to be slightly less secure than a hardware-version token since the 'something you have' aspect of strong authentication no longer has a true physical aspect to it (more on that at [http://www.bnl.gov/cybersecurity/strong\\_auth.htm](http://www.bnl.gov/cybersecurity/strong_auth.htm));  
- Software token application may not be available for certain computer platforms (i.e., VMS);

#### **PT-1**

(Software-based for PalmPilot)

- When Palm Pilot Token application loaded on user's Palm Pilot, no need for user to carry an additional physical device for authentication (i.e., an RB-1 or KF-1);  
- When troubleshooting a Palm token, Password Office can re-issue a new token without user needing to physically appear at Password Office.

- As with the ST-1 software token, Palm token is argued to be slightly less secure than a true hardware-version token;  
- If the user's PalmPilot crashes or otherwise causes Palm token program to disappear, Palm Pilot Token application has to be reinstalled.