Confirm that your data is

encrypted by ensuring a symbol

of a lock appears at the bottom

right hand corner of the browser

**•** Check your last sign-in date

and time (at the top of the

screen) whenever you sign into

Internet Banking to make sure it

is correct

**•** Always check your statements

for any transactions that look

suspicious

**•** Always select Sign Out from

the Internet Banking menu when

you complete your banking

**•** Close your internet browser

after signing out at the end of

each Internet Banking session

**•** Always memorise your

password; use a number or word

that you can easily remember,

but which is difficult for others

to guess

15.61 Following should be covered as part of penetration tests / vulnerability tests: -

1. Check for following common vulnerabilities :

- IP Spoofing

- Buffer overflows

- Session hijacks

- Account spoofing

- Frame spoofing

- D-DoS attacks

- Caching of web pages

- Cross-site scripting

- Cookie handling

2. As per RBI’s guidelines PKI (Public Key Infrastructure) is the most favoured

technology for secure Internet banking services. Since Government & RBI is in the

process of identifying a PKI service provider, it may take some time to implement

PKI in all the Banks. However, as it is not yet commonly available, does the bank

use the following alternative system during the transition, until the PKI is put in

place:

- A static ID and password login process.

- Usage of SSL (Secured Socket Layer), which ensures server authentication and

use of client side certificates issued by the Banks themselves using a Certificate

Server.

- The use of at least 128-bit SSL for securing browser to web server

communications and, in addition, encryption of sensitive data like passwords in

transit within the enterprise itself.