ipsa
Independent Parliamentary
Standards Authority

RSA Main Issues

Authentication Problems

The user may have made one of the following errors:

- The user made too many failed logon attempts, causing the device to go into next token code mode (detailed below). This can also cause the account to be ‘locked out’, however, this gets reset every seven minutes.
- The user attempted to authenticate before creating the PIN.
- The user entered an incorrect user name when logging into the system.
- The user has forgotten their pin, request a RSA Pin Reset to info@parliamentarystandards.org.uk.
- The user entered an incorrect PIN or entered the PIN in the wrong location.
- The user may be using the incorrect token; for example, the MP may be trying to authenticate using their proxies intended device.
- Other authentications issues can occur if the user sets a pin which starts with a leading ‘0’ or if it isn’t unique; for instance, it has to be a combination that they haven’t used before.

Error Messages

If any of the following error messages occur, the user must contact IPSA on 020 7811 6400:

- Token not intended for this device. Token import failed.
- Token expired. Request a replacement token.
- Token install failed.

Software doesn’t load saying Qcore4.dll missing

The file is in c:\program files\rsa secured token common and needs copying to c:\program files\rsa secured software token.

The Next Token Code Prompt

On occasion, even after you type your passcode correctly, the system may ask you to enter the next token code (the six numbers displayed on your token). It does this in order to confirm your possession of the token.

When this happens, do the following:

- Wait until the token code changes, and then type the new one. Do NOT enter the PIN, only the token code.
- Click on OK or press the Enter key.

If you are not granted access after correctly entering the next token code, please call 020 7811 6400 for the token to be resynchronised.

Security Precautions

If an unauthorised person learns your PIN or obtains your RSA SecurID software token, this person can assume your identity. Any action this intruder takes is attributed to you in the system's security log.

For your own protection and for that of the system, always take the following precautions:

- Never reveal your PIN to anyone.
- Do not write your PIN down anywhere near your device.
- Log off at the end of your session. Failure to logoff properly can create an unshielded route for another user to access the system.