

Electronic Online Filing Security Recommendations

The following points should be considered by all customers using EPO Online Services software, particularly when implementing the network client:

- We recommend that you always use the User Management function of the software and ensure your users choose complex passwords which are changed regularly.
- Please note communication between the thin client and the client application server is not encrypted; it is therefore necessary to ensure the installation is protected.
- Customers using the Patent Management System Gateway into EPO Online Services should note:
 - An encrypted connection (via SSL) between your Patent Management System and EPO Online Services can be enabled by setting “PMSSSL=1” in the FMI.INI file.
 - The pin number for the smartcard is stored in a configuration file on your server; access to the server should therefore be restricted.