

# **ELECTRONIC COMMUNICATIONS ACT 2000**

---

## **EXPLANATORY NOTES**

### **BACKGROUND**

3. The Government's policy is to facilitate electronic commerce. It has also set itself targets for making Government services available electronically: all schools and libraries to be connected to the internet by 2002, with 100% of all government services to be deliverable online by 2005. The Government has also set a target for 90% of its routine procurement of goods to be done electronically by 2001.
4. The Government's general policy towards electronic communications and information technology is set out in:
  - the Cabinet Office's Paper on "E-Government – A strategic framework for public services in the Information Age" – April 2000 ([www.iagchampions.gov.uk/strategy.htm](http://www.iagchampions.gov.uk/strategy.htm))
  - the Performance and Innovation Report "e-commerce@its.best.uk" published in September 1999 (available on the Cabinet Office website at: [www.cabinet-office.gov.uk/innovation/1999/ecommerce](http://www.cabinet-office.gov.uk/innovation/1999/ecommerce));
  - the Modernising Government White Paper (Cm 4310) published in March 1999 (available on the Cabinet Office website: [www.cabinet-office.gov.uk/moderngov/1999/whitepaper/index.htm](http://www.cabinet-office.gov.uk/moderngov/1999/whitepaper/index.htm));
  - the Competitiveness White Paper (Cm 4176) published in December 1998 (available on the DTI website: [www.dti.gov.uk/com/competitive](http://www.dti.gov.uk/com/competitive)); and
  - the Government's policy statement "Our Information Age: The Government's Vision" (URN 98/677; 4-98) (a summary can be found on the Number 10 website: [www.number-10.gov.uk/public/info/index.html](http://www.number-10.gov.uk/public/info/index.html)).

Electronic commerce is developing quickly, as is Government policy on it. Useful sources of up to date information include the websites of the e-envoy ([www.e-envoy.gov.uk](http://www.e-envoy.gov.uk)), which includes a monthly progress report to the Prime Minister, the Cabinet Office Central IT Unit ([www.citu.gov.uk](http://www.citu.gov.uk)) and the DTI ([www.dti.gov.uk](http://www.dti.gov.uk)).

5. Cryptography and electronic signatures are important for electronic transactions.
  - *Cryptography* is the science of codes and ciphers. Cryptography has long been applied by banks and government and is an essential tool for electronic commerce. Cryptography can be used as the basis of an electronic signature.
  - *Encryption* is the process of turning normal text into a series of letters and/or numbers which can only be deciphered by someone who has the correct password or key. Encryption is used to prevent others reading confidential, private or commercial data (for example an e-mail sent over the internet or a file stored on floppy disk).
  - An *electronic signature* is something associated with an electronic document that performs similar functions to a manual signature. It can be used to give the recipient

confirmation that the communication comes from whom it purports to come from (“authenticity”). Another important use of electronic signatures is establishing that the communication has not been tampered with (“integrity”).

- *Public key cryptography* is a form of cryptography that uses two distinct, but related, keys (known as a key pair): one key for “locking” a document, and a separate key for “unlocking” it. These keys are both large numbers with special mathematical properties.
  - Public key cryptography can be used to provide an electronic signature: the *private key* (which is only known to its owner) is used as the “lock” to transform the data, by scrambling the information contained in it. The transformed data is the electronic signature, which can be verified by “unlocking” it with the *public key* of the person who signed it. Anyone with access to the public key can check the signature, so verifying that it was signed by someone with access to the private key and also verifying that the content of the document had not been changed.
  - Public key cryptography can also be used to keep a communication secret: in this case the keys are used the other way round. The person sending the message would use the public key of the intended recipient to “lock” the message. Now only the corresponding private key can be used to “unlock” the message. This is what the intended recipient would use to read it. A third party would not be able to read the message without access to the intended recipient’s private key.
6. Various organisations provide cryptography services, which include certifying the public key of an individual, managing encryption keys and time stamping electronic signatures. There is a need for the public to be able to have confidence that these services are secure and not open to fraud; and for people to be free from unnecessary restrictions in their use of new technology.
  7. The main purpose of the Act is to help build confidence in electronic commerce and the technology underlying it by providing for:
    - an approvals scheme for businesses and other organisations providing cryptography services, such as electronic signature services and confidentiality services;
    - the legal recognition of electronic signatures and the process under which they are verified, generated or communicated; and
    - the removal of obstacles in other legislation to the use of electronic communication and storage in place of paper.
  8. The Act also contains provisions to update procedures for modifying telecommunications licences.
  9. The Act is in three parts.
    - **Part I, Cryptography Service Providers.** This concerns the arrangements for registering providers of cryptography support services, such as electronic signature services and confidentiality services.
    - **Part II, Facilitation of Electronic Commerce, Data Storage etc.** This makes provision for the legal recognition of electronic signatures and the process under which they may be generated, communicated or verified. It will also facilitate the use of electronic communications or electronic storage of information, as an alternative to traditional means of communication or storage.
    - **Part III, Miscellaneous and Supplemental.** This Part amends sections 12 and 46B of the Telecommunications Act 1984 and inserts a new section 12A into that Act. The new provisions are concerned with the modification of telecommunication licences otherwise than in pursuance of a reference to the Competition Commission.

*These notes refer to the Electronic Communications Act  
2000 (c.7) which received Royal Assent on 25 May 2000*

This Part also concerns matters such as general interpretation, the short title, commencement and territorial extent of this Act.