Identification, trust and privacy.
How biometrics can aid certification of digital signatures

John Huntley, Michael Bromby - Glasgow Caledonian University
Ron Aitken, & Steve Arnott - Serendipity Interactive Ltd. Glasgow

Abstract
Public Key Infrastructure (PKI) enables the secure and private exchange of data using an unsecure public network, such as the Internet. The use of paired private and public keys, issued by a trusted third-party authority, enables documents to be transferred securely and for the sender to be authenticated.

Biometrics offer the potential to enhance considerably the PKI model in restricting the use of your private key for encryption and decryption. The use of a fingerprint, for example, can provide a higher level of confidence than the traditional password / PIN model. This provides the additional level of individual or personal authentication should a group of people have access to one key.

The authentication of data, or a document, is often physically remote from the owner, especially for Internet-based communications. Conversely, traditional biometric usage has been to identify the physical presence of a person for secure entry, the receipt of information, or indeed goods.

Within the EU, the European Electronic Signature Standardisation Initiative (EESSI) has led to a plethora of standards covering PKI, electronic signature algorithms, electronic signature formats, time stamping, the provision of certification services, information security and the preservation of evidence. This paper illustrates how a legally compliant and secure framework for the verification and non-repudiation of digital technology can be established using PKI and biometric technologies. In particular, the legal requirements for digital signatures and their certification must be defined, especially with reference to biometric methods for certificate protection and access.