

# Biometric Signatures

-v-

## PPK Digital Signatures

### 1 What they have in common

#### 1.1 Purpose

Both Biometric and Public/Private Key (PPK) signatures aim to provide a link between a dataset (e.g. a document or a transaction) in the electronic domain and its originator or authorizer. For the sake of simplicity, we will refer to the dataset as a "document", while admitting that such a document might well be little more than a short string of numbers.

It is helpful to note that there are two links, logically speaking: a link from the signature to the document of which it is a signature; and a link from the signature to the originator of the document.

#### 1.1 Mechanisms

Both types of signature employ one-way hashing techniques to establish the link to the document. It is accepted that if such techniques are used, then the integrity of this link can be mathematically proved with a very high degree of probability. The degree of probability is itself demonstrable mathematically.

#### 1.1 Danger of Interception

Both types of signature are effected ultimately through some kind of human interaction with the computer system. In the case of biometric signatures, the biometric data must be sampled by some kind of peripheral which provides an input to the computer system. In the case of PPK signatures, either the key itself or some kind of input which unlocks or decrypts the key can likewise be intercepted. The technologies available to overcome this problem are equally applicable to both types of signature.

#### 1.1 Danger of falsification

Both types of signature, viewed purely as electronic data, are *prima facie* prone to fraudulent modification. However, both may be protected by the use of check information and redundancy. In the case of PenOp, integrity can be guaranteed by employing a password key which is used at signature capture time to generate an integrity hash of the biometric token. The integrity key does not itself form part of the biometric token.

### 1 Digital Signatures

Digital signatures use a cryptographic technique to establish the validity of the link between the signature and its originator. In essence, PPK cryptography uses the

mechanism of a pair of encryption keys, let us say K1 and K2, such that K1 can be used to encrypt a message which can be decrypted only by K2, or to decrypt only messages encrypted by K2; and K2 can be used to decrypt only messages encrypted with K1, or to encrypt messages which can be decrypted only by K1. Given that a message can be decrypted with K2, the probability of that message having been encrypted with K1 can be demonstrated mathematically; such probability being (as with one-way hashing) exceedingly high.

Typically, K2 is made public so that in principle anyone may decrypt the signature. It therefore follows that anyone possessing K2 may verify that the originator held K1.

## **1.1 PPK and the standard of proof**

The link between a digital signature and its originating key is subject to mathematical demonstration. This is because the link itself lies wholly within the same domain, namely, the electronic domain. Essentially, what is mathematically provable is the connexion between K1 and K2, and nothing else.

We may make the philosophical point that mathematical demonstrations are available only when the problem domain is itself describable using symbols which can be mathematically manipulated.

## **1.1 PPK and evidence**

### **1.1.1 Evidence as to the owner of K1**

Digital signatures do not of themselves provide evidence about the identity of the authorized holder ("owner") of K1. In order to answer this deficit, it is proposed that Key Certification Authorities (CAs) be set up.

A CA would assure itself by traditional evidential means that the owner had K1 in his possession and would receive from that owner a copy of K2, and would then verify that the keys did indeed make a pair. (This can be verified by encrypting a secret message with K2, transmitting it to K1's owner, who decrypts it and re-encrypts it with K1; the result is then retransmitted to the CA, which can verify that only K1 could have generated the response.) Once the CA has assured itself as to the ownership of K1, it can serve as an authentication agency.

### **1.1.1 Evidence as to the user of K1**

However, a CA cannot give evidence as to the user of K1. It can give evidence only as to the owner. Given that a public key K1 is typically a large data item, it is not considered practicable that it be memorized by human beings. Consequently, PPK encryption keys have to be stored on electronic media (e.g. disks, cards or tapes). It follows that evidence whether the user of K1 is the owner of K1 lies outside the domain of proof which links K1 to K2. For example, if K1 is stored on a magnetic card, the evidence whether that card was in the possession of the owner is extrinsic to the digital signature and to the electronic domain.

### **1.1.1 Evidential Value of CAs**

We may summarize the evidential question as: "was this message originated by the authorized originator?". CAs can answer only the question "was this message originated by someone claiming to be the authorized originator?". In other words, a CA can not say who *was* signing, only who was *supposed* to be signing. Given a

satisfactory answer to the first question, an answer to the second is redundant. In the absence of a satisfactory answer to the first question, an answer to the second is of no value. Therefore, the evidence provided by a CA is either redundant or of no value.

### **1.1 PPK and onus**

The solution to the evidential lack is to make a presumption that the possessor of the secret key is in fact the legal owner, and to place the burden of securing the secret key upon the owner. Until an owner contacts the CA to revoke his certificate, therefore, he will be legally responsible for all transactions effected with his private key. The CA performs an administrative, not an evidential, role.

## **1 Biometric Signatures**

Biometric signatures consist in a digital recording of a physical interaction with the computer system. Given that they record an event in the physical domain, which is a multi-dimensional continuum, biometric techniques can measure each dimension using a variety of metrics. In theory, an impostor is presented with a multi-dimensional problem.

### **1.1 Biometrics and the standard of proof**

Using statistical or pattern-recognition techniques, biometric verification systems claim to discriminate between the performance of a given individual and the rest of the population.

Because biometric data are real-world data and are somewhat variable, all biometric tests are prone to two kinds of error - false acceptance and false rejection. The lower the threshold for false rejection (i.e. the higher the probability of false rejection), the higher the threshold for false acceptance, and vice-versa. The equal error rate is therefore the key figure for evaluation of biometric authentication mechanisms; most biometric techniques are now subject to equal error rates around 1%. Although some vendors of signature verification methods quote equal error rates, these are less meaningful than for purely physiological biometrics, since the meaning of an error rate is entirely dependent on the set of data used to procure it. Until a standard has been published for testing error rates, therefore, it will always be open to providers to quote figures based on a dataset which is favourable to their own product.

While it is clear that the error rates of biometric techniques could never approach those of the PPK system, it is essential to remember that the domain of proof is not the same, in that biometrics purport to provide evidence of real-world states of affairs. For example, ordinary visual recognition is assumed to be reliable, but mathematical proofs of its reliability would be very difficult to construct.

### **1.1 Biometrics and evidence**

Biometric signatures contain an electronic analogue of the interaction of the human signatory with the computer system, which thus effectively acts as a digital recording device. Digital recordings are already accepted both in forensic and in everyday life as a valid type of identifying evidence.

### **1.1 The status of biometric verification systems**

The accuracy with which a given set of biometric tests can discriminate between authentic and inauthentic data, while important, is nevertheless irrelevant to the issue of the evidential value of the data themselves. For example: given any highly reliable mechanism for biometric authentication operating upon highly reliable biometric data, it is always possible to construct a far less reliable system which operates on the same data.

It may be that a jurisdiction decides to accord some status to the results of a given signature verification system; however, this would be by way of *fiat* and would be entirely independent of the evidential value of the signature data.

## 1 Summary

PPK signatures establish an extremely reliable (and mathematically provable) link between the signature and the *purported* signatory. However, they contain *no* evidence as to the link between the purported signatory and the actual signatory. Such evidence, where available, will be *extrinsic* to the PPK signature and will not participate in the mathematical reliability of the PPK technique itself.

Biometric signatures establish an evidential link between the signature and the *actual* signatory. There is no need for a mechanism to authenticate the claimed signatory. To the extent that biometric verification systems perform reliably in tests, they may be regarded as a useful objective indicator of the strength of this link. The evidence as to authenticity is *intrinsic* to the biometric signature.