Keep Your Originals For Sentimental Purposes Only!

For practical consideration your scanned or printed copy can be authenticated for its contents and its writer. if.π would also provide non-repudiation (the writer falsely denying he wrote this document).

Digital Signatures are recognized as a binding legal commitment in the US and in most advanced countries. But so far, they applied to forms filled in electronically. Paper documents are still authenticated with an old fashioned pen-scribbled signature.

Like in the good old times… Only that back then fraudsters did not have graphic software that makes it so easy to lift a signature from one document and plant it into another. In the good old times, as much as today, if a scribbled signature is challenged, it's quite a task to find hand-writing experts to testify (and they often disagree).

Today, corporate offices, financial institutions, government bureaucracies are overburdened with hard-to-manage filing cabinets loaded with paper stuffed files. And if a single document is misplaced -- good luck!

if.π stands to relieve these suffering secretaries, clerks, managers, and bureaucrats with its new technology that makes every copy of a document as valid and as trustworthy as the original.

Imagine the relief!

How does **if.π** work?

Before explaining the **if.π** solution let's understand why digital signatures so far have by-passed the paper document. A digital signature is a small binary string that is derived from a large string. The mathematics, known as "hash", is such that no matter how long the large string, if even one bit in it flips -- the resulting signature (the small string) would be completely different. To sign an electronic document (the large string) the signer would generate the hash, encrypt it with his private key and attach the encrypted hash to the signed file. Anyone can verify that the file was signed by the professed signer, and

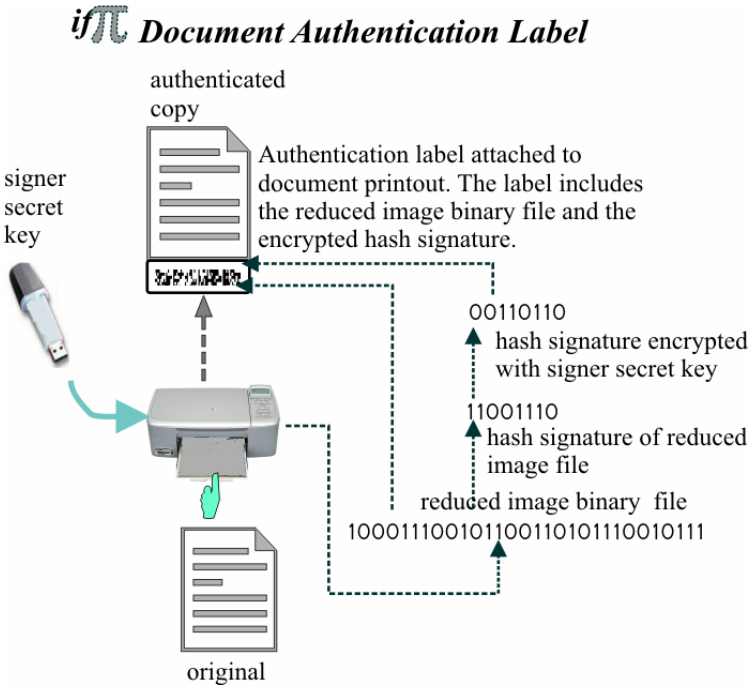
that the contents have not changed, by applying the signer's public key to the encrypted hash, extracting the hash, and comparing it with a processed hash of the available file. If the two hash files disagree, something is wrong.

All that is standard and works pretty smoothly with electronic files. What happens when you deal with a physical paper document? You scan it, and generate an electronic version thereof. Albeit, if you re-scan it, with the paper positioned however slightly different, then the electronic version would be different. If the paper attracted some specs of dust, a coffee stain, a stapler hole, a crease, or if the scanner is of different resolution -- the result would be a different electronic file. When the various electronic files are translated to viewable images they all look similar, but it's impossible to sign these files, using the hashing method because each scan will have a different signature.

And so, despite the advances in cryptography, paper-laden file cabinets are pestering office dwellers around the globe, holding on to originals, relying on the iffy determination that a scribbled signature is authentic.

Enter **if.π**

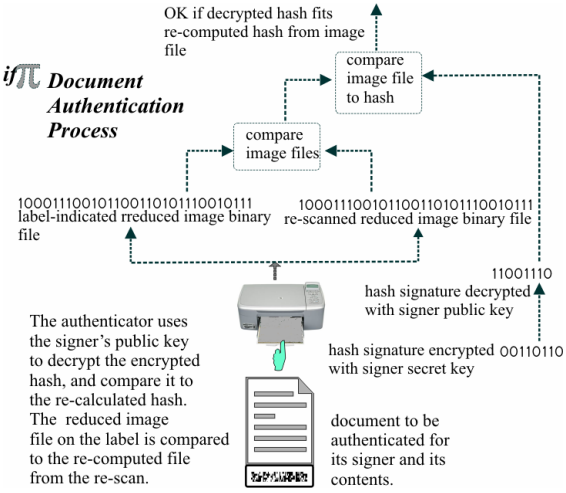
Simply put: **if.π** is an innovative technology that translates a paper image into the same long string of bits (electronic file) regardless of the scanner's resolution, oblivious to normal stains, despite foldings, regardless of tears and holes. **if.π** issues a sticker that contains a reduced image of the page (the long string), and its signed hash. Anyone can use the signer public key, extract the unencrypted hash and thereby validate the long string (the reduced image string). That string can be recomputed from a newly scanned image of the paper. If the two image strings agree, the verifier knows that this image (and the corresponding paper) were signed by the person who is identified on the paper as the writer, and at the same time verify that nobody tampered with the contents of that letter: Double hit: the signer and his letter are both authenticated.



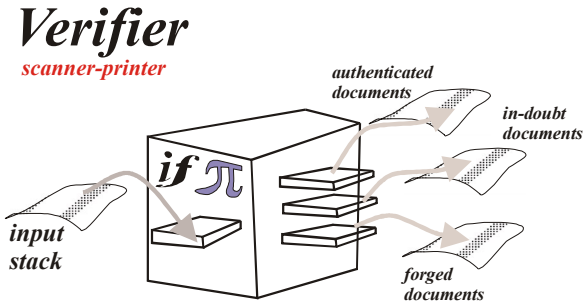
Since this is image based authentication, there is no advantage to the original over a copy. As long as the reduced image string and its encrypted hash are attached, the document is verifiable, and will also withstand false repudiation.

The **if.π** technology can be used for passing paper documents among untrustworthy strangers. Each copy, will be equipped with the sticker. The sticker would feature the long and short strings through two-dimensional bar-code. Any PC system equipped with the **if.π** software would be able to scan the copy and the sticker, and verify the signer and the contents.

Copies would be kept in a searchable database along with their **if.π** strings, and this by itself means a dramatic saving in intensive labor. Think of how many hours office workers waste chasing a misplaced document, or hunting for one, in a distant, hard-to- access archive. All that would change in a jiffy. Paper storage would be fully computerized -- compact and searchable. The last argument in favor of paper media -- the scribbled signature, is now overturned. *Welcome to tomorrow's office!*



A closing note: **if.π** is image oriented and hence it would work with hand written documents, drawings, art-work, photographs -- anything that goes on paper. You can mark ownership for anything visual by taking a picture thereto, and if.π-ing its paper image.



This innovation was developed using "The Innovation Turing Machine", available on Amazon.com