

# Now or Later?

## When should you authenticate your documents?

There are two philosophies of signature authentication for documents. The first is:

- Authenticate the signature instantly at the time of signing.
- Affix a token to the document that includes the time, date, and reason for signing; a flag indicating whether or not the document has been altered since signing; and the fact that the signature has been authenticated; but NOT the signer's biometric information.

The second is:

- The biometric information should be part of the process of creating the document and as such attached to each document, so that authentication of the document author is a separate process that can be done later.

Before choosing which method is best for any application, several issues must be taken into consideration.

One reason to sign a document is to take responsibility for the information filled in on the document in the case of an application form, a report, and similar documents. Another reason to sign is to agree to an obligation, as in the case of a contract or credit card receipt. If the signer is authenticated instantly, the signer is taking responsibility for the information, or for the obligation, from the moment s/he signs.

If, on the other hand, biometric information is attached to the document with the plan to authenticate it some time in the future, many factors can intervene to render the document useless. A few examples include the signer's death, dismemberment, or an illness that alters the ability to sign. Beyond that, the signer might have moved or is otherwise not available.

Another consideration is why the presenter of the document would want to take on an obligation. If the presenter accepts an obligation from another, if the document might in the future be found invalid because the presenter was not able to sign again. Going one step further, suppose the signer is alive, available, and healthy, but no longer wants to honor the obligation previously entered into. The signer might then intentionally sign with his/her signature and claim it was not his/her signature in the first place.

One other issue is privacy. If biometric information is attached to every copy of the document, then that information may be available to people the signer did not intend and would not approve. If it becomes known that one's unauthenticated biometric information is attached to your document, people will refuse to sign your documents simply because of privacy concerns.

The conclusion is that before choosing the best method of signature authentication for each application, the designer should consider whether the purpose of the document is to create an obligation or to submit information. If either is the case, then the designer should consider whether his/her company is willing to accept the risk of the document being declared invalid at a future date, and whether the company's customers might have privacy concerns. If the company does not wish to assume such risk, or if the company's customers might have concerns about privacy, then choose Cyber SIGN.