

**SYSTEM AND METHOD FOR VERIFYING DIGITAL SIGNATURES ON
CERTIFICATES**

ABSTRACT

A system and method for verifying a digital signature on a certificate, which may be used in the processing of encoded messages. In one embodiment, when a digital signature is successfully verified in a signature verification operation, the public key used to verify that digital signature is cached. When a subsequent attempt to verify the digital signature
5 is made, the public key to be used to verify the digital signature is compared to the cached key. If the keys match, the digital signature can be successfully verified without requiring that a signature verification operation in which some data is decoded using the public key be performed.

Fig. 8B