DIGITAL-SIGNED DIGITAL DOCUMENT EXCHANGE SUPPORTING METHOD AND INFORMATION PROCESSOR

ABSTRACT

In response to a sign request including a digital document from a document-creating device 10, a digital-signed-document exchange supporting server 30 canonicalizes the digital document , calculates a digest value thereof and returns the digest value to the document creating device. When the document-creating device transmits a digital sign created by encrypting the digest value to the digital-signed-digital document exchange-supporting server 30, the digital-signed-digital document exchange-supporting server 30 creates a digital-signed document from the digital sign and the digital document and returns the document to the document-creating device. On the other hand, in response to a validation request including a digital-signed-digital document and a public key from a sign validating device 20, the digital-signed-digital document exchange supporting server 30 compares a value resulting from the decryption of the digital sign with the public key and a digest value of the digital document canonicalized and returns the result to the sign validating device.

Figure 1