19 SEP 2006

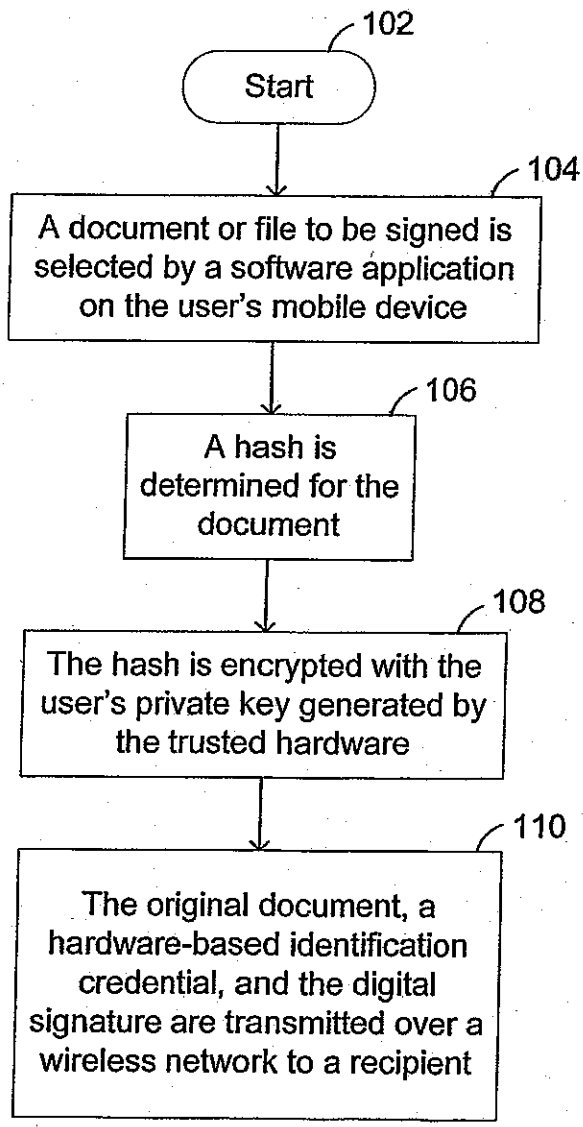


FIG. 1

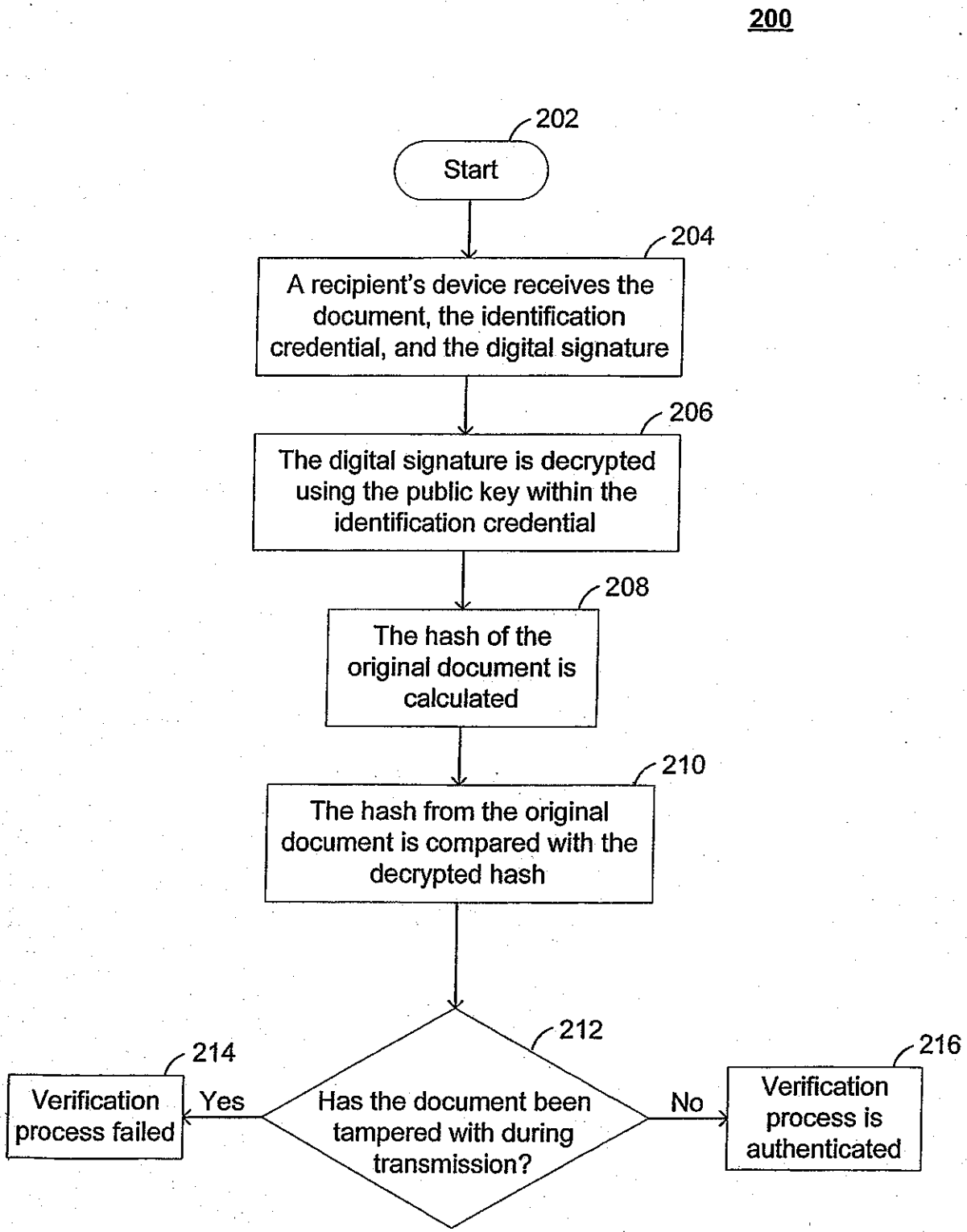

200
202
Start
204
A recipient's device receives the document, the identification credential, and the digital signature
206
The digital signature is decrypted using the public key within the identification credential
208
The hash of the original document is calculated
210
The hash from the original document is compared with the decrypted hash
212
Has the document been tampered with during transmission?
Yes
214
Verification process failed
No
216
Verification process is authenticated

FIG. 2

300

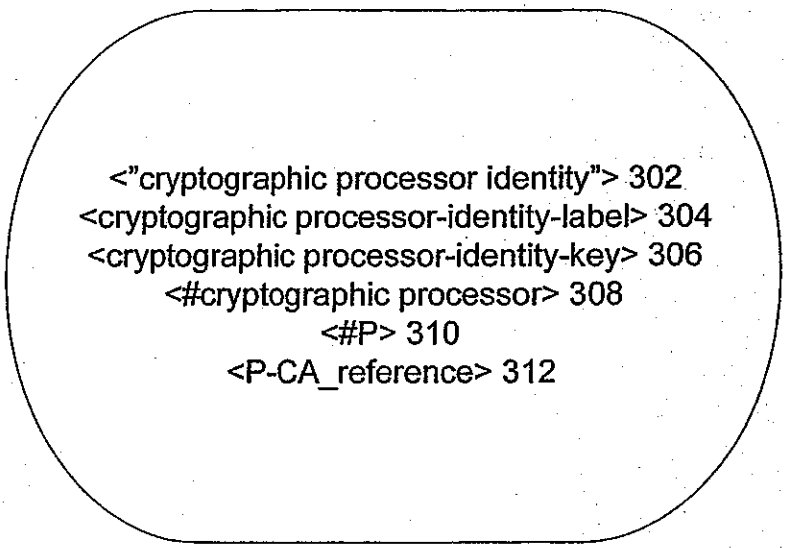

<"cryptographic processor identity"> 302
<cryptographic processor-identity-label> 304
<cryptographic processor-identity-key> 306
<#cryptographic processor> 308
<#P> 310
<P-CA_reference> 312

FIG. 3

400

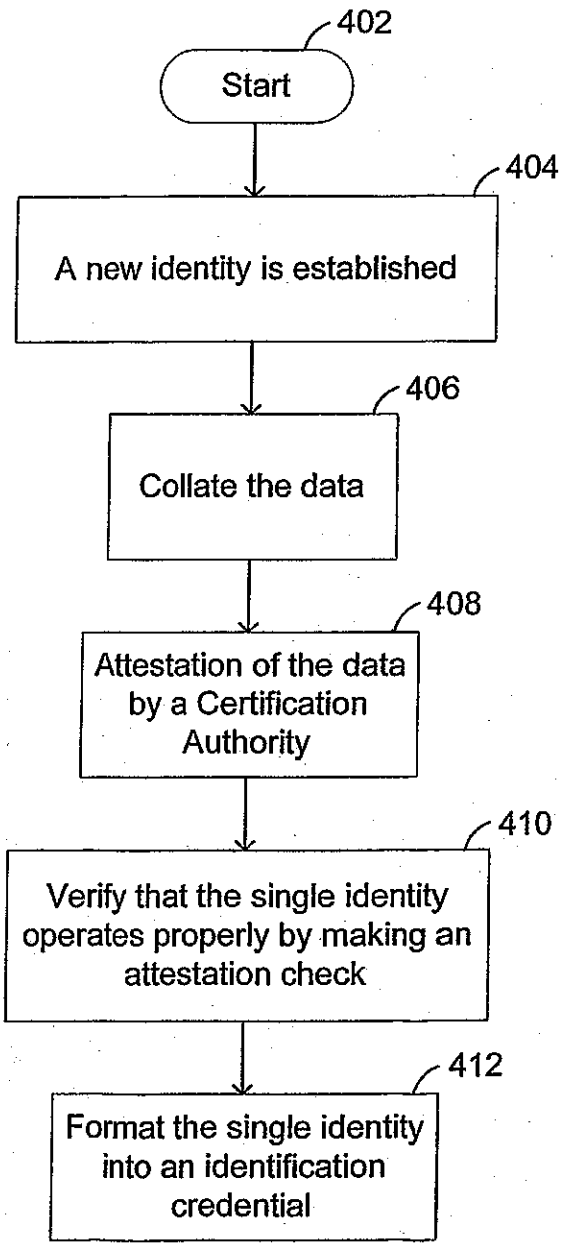

402
Start
404
A new identity is established
406
Collate the data
408
Attestation of the data by a Certification Authority
410
Verify that the single identity operates properly by making an attestation check
412
Format the single identity into an identification credential

FIG. 4