The RSA public-key cryptosystem can be used to authenticate or identify another person or entity. The reason it works well is because each entity has an associated private key which (theoretically) no one else has access to. This allows for positive and unique identification.

Suppose Alice wishes to send a signed message to Bob. She applies a hash function to the message to create a message digest, which serves as a "digital fingerprint" of the message. She then encrypts the message digest with her private key, creating the digital signature she sends to Bob along with the message itself. Bob, upon receiving the message and signature, decrypts the signature with Alice's public key to recover the message digest. He then hashes the message with the same hash function Alice used and compares the result to the message digest decrypted from the signature. If they are exactly equal, the signature has been successfully verified and he can be confident the message did indeed come from Alice. If they are not equal, then the message either originated elsewhere or was altered after it was signed, and he rejects the message. Anybody who reads the message can verify the signature. This does not satisfy situations where Alice wishes to retain the secrecy of the document. In this case she may wish to sign the document, then encrypt it using Bob's public key. Bob will then need to decrypt using his private key and verify the signature on the recovered message using Alice's public key. Alternately, if it is necessary for intermediary third parties to validate the integrity of the message without being able to decrypt its content, a message digest may be computed on the encrypted message, rather than on its plaintext form.

In practice, the public exponent in the RSA algorithm is usually much smaller than the private exponent. This means that verification of a signature is faster than signing. This is desirable because a message will be signed by an individual only once, but the signature may be verified many times.