Smart card

Il sistema per la creazione e la verifica di firme digitali sfrutta le caratteristiche dei sistemi crittografici a due chiavi.
Un sistema crittografico garantisce la riservatezza del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso di una "chiave" (intesa secondo la definizione crittologica) per interpretarli.
Nei sistemi crittografici a due chiavi, detti anche a chiave pubblica o asimmetrici, ogni utente ha una coppia di chiavi: una chiave privata, da non svelare a nessuno, con cui può decodificare i messaggi che gli vengono inviati, e una chiave pubblica, che altri utenti utilizzano per codificare i messaggi da inviargli.
Per ogni utente, le due chiavi vengono generate da un apposito algoritmo con la garanzia che la chiave privata sia la sola in grado di poter decodificare correttamente i messaggi codificati con la chiave pubblica associata.
Lo scenario in cui un mittente vuole spedire un messaggio ad un destinatario in modalità sicura è il seguente: il mittente utilizza la chiave pubblica del destinatario per la codifica del messaggio da spedire, quindi spedisce il messaggio codificato al destinatario; il destinatario riceve il messaggio codificato e adopera la sua chiave privata per ottenere il messaggio "in chiaro".
Grazie ad un'ulteriore proprietà delle due chiavi, inversa rispetto a quella descritta, un sistema di questo tipo è adatto anche per ottenere dei documenti firmati, infatti: la chiave pubblica di un utente è la sola in grado di poter decodificare correttamente i documenti codificati con la chiave privata di quell'utente.
Se un utente vuole creare una firma per un documento, procede nel modo seguente: con l'ausilio di una funzione hash ricava l'impronta digitale del documento, il message digest, un file di dimensione fissa che riassume le informazioni contenute nel documento, dopodiché utilizza la propria chiave privata per codificare quest'impronta digitale: il risultato di questa codifica è la creazione di una firma.
La funzione hash, è fatta in modo da rendere minima la probabilità che da testi diversi si possa ottenere il medesimo valore dell'impronta, inoltre è one-way, a senso unico, questo significa che dall'impronta è pressoché impossibile ottenere nuovamente il testo originario. La firma prodotta dipende dall'impronta digitale del documento e, quindi, dal documento stesso, oltre che dalla chiave privata dell'utente. A questo punto la firma viene allegata al documento.
Chiunque può verificare l'autenticità di un documento: per farlo, decodifica la firma del documento con la chiave pubblica del mittente, ottenendo l'impronta digitale del documento, e poi confronta questa con quella che si ottiene applicando la funzione hash pubblica, al documento; se le due impronte sono uguali, l'autenticità del documento è garantita.