Fondazione Bruno Visentini

DECRETO PNRR, LA FIRMA DIGITALE PER ORA È ASSENTE NELL'IT-WALLET

di **Valentina Garilli** e **Alfonso Papa Malatesta**

—Continua da pagina 29

Dal punto di vista tecnologico, infatti, la firma digitale utilizza la crittografia a chiavi asimmetriche per la generazione di una coppia di chiavi numeriche (chiave privata e chiave pubblica), diverse tra loro, la cui relazione matematica fa sì che un messaggio cifrato con la chiave privata (che rimane segreta) possa essere decifrato e verificato solo con la correlata chiave pubblica (che può essere invece distribuita). Le chiavi, però, sono dei semplici numeri in codice binario; la loro relazione assicura soltanto che è il possessore della chiave privata ad aver generato una certa chiave pubblica e cifrato un certo messaggio, mentre nulla dice circa l'identità del possessore. Anche conoscendo la chiave pubblica non conosciamo ancora l'identità del titolare della coppia di chiavi. È qui che entrano in gioco i certificati di firma rilasciati dai fiduciari qualificati. Essi attestano che una certa chiave pubblica appartiene ad un soggetto identificato, e sono acclusi in ogni operazione di firma.

Oggi, per firmare, occorre dotarsi (sempre per il tramite di fiduciari qualificati e, di solito, a pagamento) di un apposito strumento (di regola contenuto in una smart card o chiavetta Usb) che conservi in modo sicuro i dati di firma, ovvero le chiavi, e il certificato di firma.

Con le novità dell'Eidas 2, rispettati precisi standard di sicurezza, i dati di firma potranno essere conservati direttamente nel dispositivo dove è installato l'Ediw (ad esempio, nello smartphone), il quale si trasformerebbe così in vero e proprio strumento per la firma digitale con "passaporto europeo". L'obiettivo è dotare i cittadini di una firma digitale accessibile e versatile, oltre che gratuita. I possibili utilizzi vanno oltre quelli tradizionali. S'avverte infatti sempre più l'esigenza di stabilire l'autenticità dei contenuti digitali, specie al cospetto della loro creazione e diffusione, su larga scala, da parte di macchine, come consente l'Ia. Secondo alcuni, la crittografia a chiavi asimmetriche può offrire valide soluzioni per garantire autenticità e provenienza dei contenuti online (tra le iniziative in materia, si segnala quella della "Coalition for content provenance and authenticity", C2pa).

In tale contesto si inserisce il nostro Dl 19/2024 con l'It-wallet, il quale, già nel nome, opportunamente richiama che è ancora lo Stato, e non l'Ue, a riconoscere l'identità personale. Tuttavia, perché l'It-wallet possa anche essere qualificato come Ediw occorre che offra tutte le funzionalità essenziali previste dell'Eidas 2, inclusa la firma digitale.

Il Dl 19/2024, in attesa di conversione in legge (atto Camera n. 1752), riguarda l'identità digitale e le attestazioni elettroniche di attributi, ma nulla dice in merito alla firma digitale. Trattandosi di funzionalità essenziale dell'Ediw, sarebbe dunque opportuno che in sede di conversione in legge essa fosse prevista come necessaria per l'It-wallet.

Certo, le successive linee guida dell'Agid (Agenzia per l'Italia digitale, *ndr*) potrebbero includere la firma tra i servizi disponibili nell'It-wallet, ma la rilevanza dello strumento per il cittadino, anche nel contesto dell'esercizio delle proprie libertà nella Unione europea , sembra meritare l'attenzione della norma primaria, quale diritto sancito da legge dello Stato.

Osservatorio Fondazione Bruno Visentini

IL DL 19
Il decreto legge in attesa di conversione riguarda le attestazioni elettroniche di attributi

USO OLTRECONFINE
Eidas 2 consente al portafoglio digitale di essere utilizzato per i servizi nei vari Stati membri