DeepL

Abbonati a DeepL Pro per tradurre file di maggiori dimensioni.
Per ulteriori informazioni, visita www.DeepL.com/pro.

Progetto FoC 2024-25

Server di firma digitale

Un'organizzazione implementa un servizio di firma digitale (DSS), una terza parte fidata che crea coppie di chiavi pubbliche e private, le archivia e genera firme digitali per conto dei dipendenti dell'organizzazione.

I dipendenti dell'organizzazione sono registrati off-line. Al momento della registrazione, un dipendente riceve la chiave pubblica del DSS e una password che deve essere modificata al primo accesso. Il dipendente mantiene la chiave pubblica del server.

Dopo essersi connesso in modo sicuro al DSS, l'utente può invocare la seguente richiesta di operazioni.

- **CreateKeys** che crea e memorizza una coppia di chiavi private e pubbliche per conto dell'utente invocante. Se per l'utente esiste già una coppia di chiavi, l'operazione non ha alcun effetto.
- **SignDoc** che restituisce la firma digitale sul documento specificato come argomento. Il servizio firma digitalmente il documento per conto dell'utente che lo invoca e gli restituisce la firma digitale ottenuta.
- **GetPublicKey** che restituisce la chiave pubblica dell'utente specificato come argomento.
- **DeleteKeys** che cancella la coppia di chiavi dell'utente che la invoca. Dopo la cancellazione di una coppia di chiavi, un utente non può crearne una nuova, a meno che non si registri nuovamente (off-line).

Gli utenti interagiscono con il DSS attraverso un canale sicuro che deve essere stabilito prima di emettere operazioni. Un utente si autentica al servizio tramite la chiave pubblica del servizio. L'utente si autentica al servizio tramite la sua password. Il canale sicuro deve soddisfare i requisiti di perfect forward secrecy (PFS), integrità, no-replay e non-malleabilità.

Il server memorizza le chiavi private degli utenti in forma criptata. La relazione

sul progetto deve contenere:

- Specifiche e scelte progettuali con particolare riferimento all'autenticazione
  protocollo tra un utente e il servizio.
- Formato di tutti i messaggi scambiati.
- Diagrammi di sequenza di ogni protocollo di comunicazione utilizzato (livello di applicazione).