MOSTsecurity Module

Features di MOSTsecurity

- Autenticazione
- Crittografia campi del DB
- Crittografia di documenti
- Firma di documenti
- Archiviazione sostitutiva

Infrastruttura di security

- Evoluzione del sistema di autenticazione e crittografia basato su chiavi asimmetriche:

  il proprietario ha la chiave privata,
  chiunque può avere la chiave pubblica

- Gestione sul client di archivi protetti di chiavi private
- Gestione sul client di dispositivi hardware di firma, crittografia, e autenticazione

Autenticazione user+password vs PKI

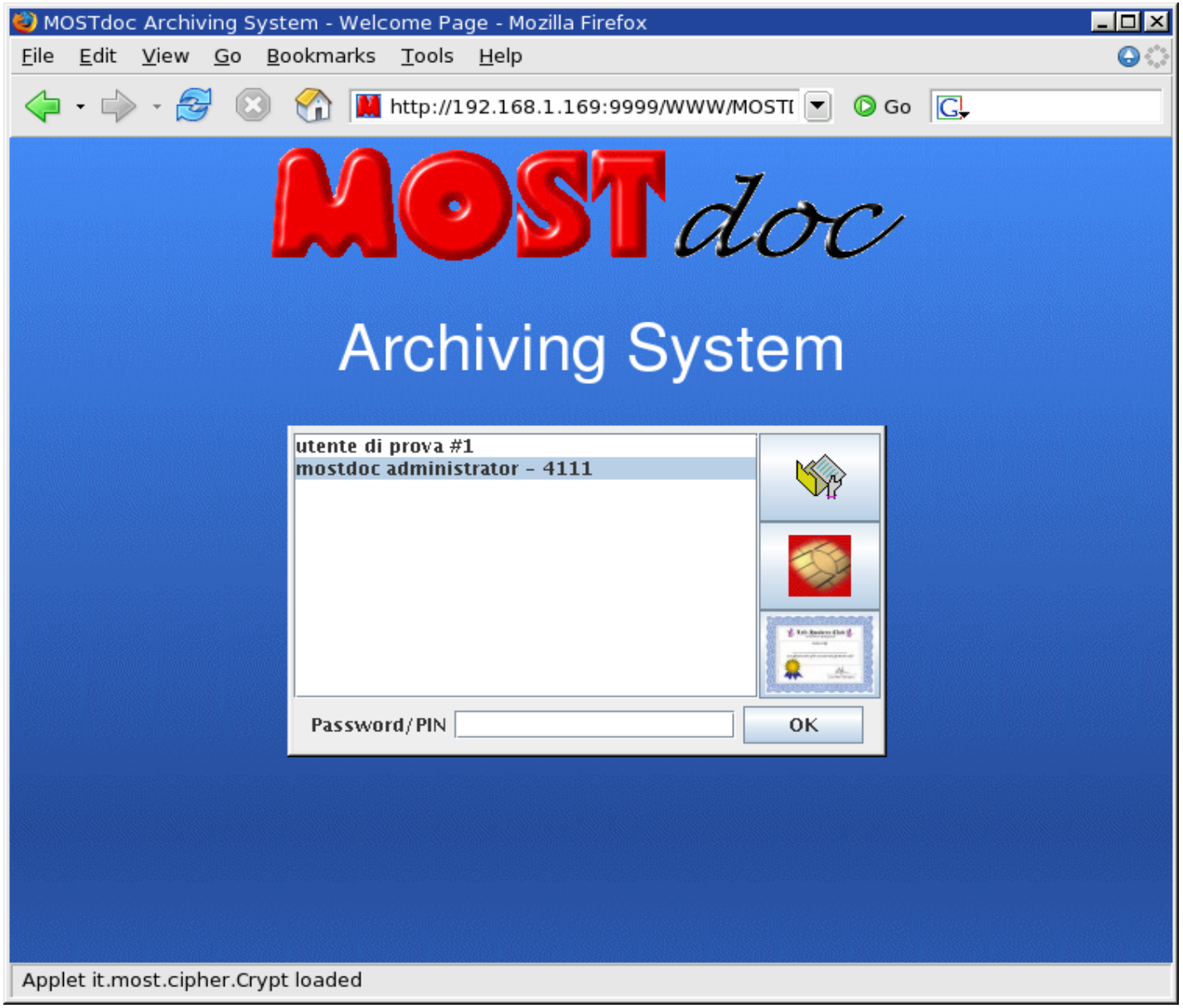
- L'autenticazione tradizionale non dà garanzie sulle reali credenziali dell'utente
- L'uso di dispositivi fisici riduce l'uso non personale delle utenze
- La soluzione con certificati permette l'uso di credenziali riconosciute ufficialmente anche per legge

Autenticazione user+password vs PKI

- L'autenticazione con user+pass richiede la gestione sul server della password utente (anche se in forma non reversibile)

- La soluzione con certificati può appoggiarsi a servizi di validazione pubblici (Certification Authority)

Interfaccia di autenticazione



Modulo di Crittografia

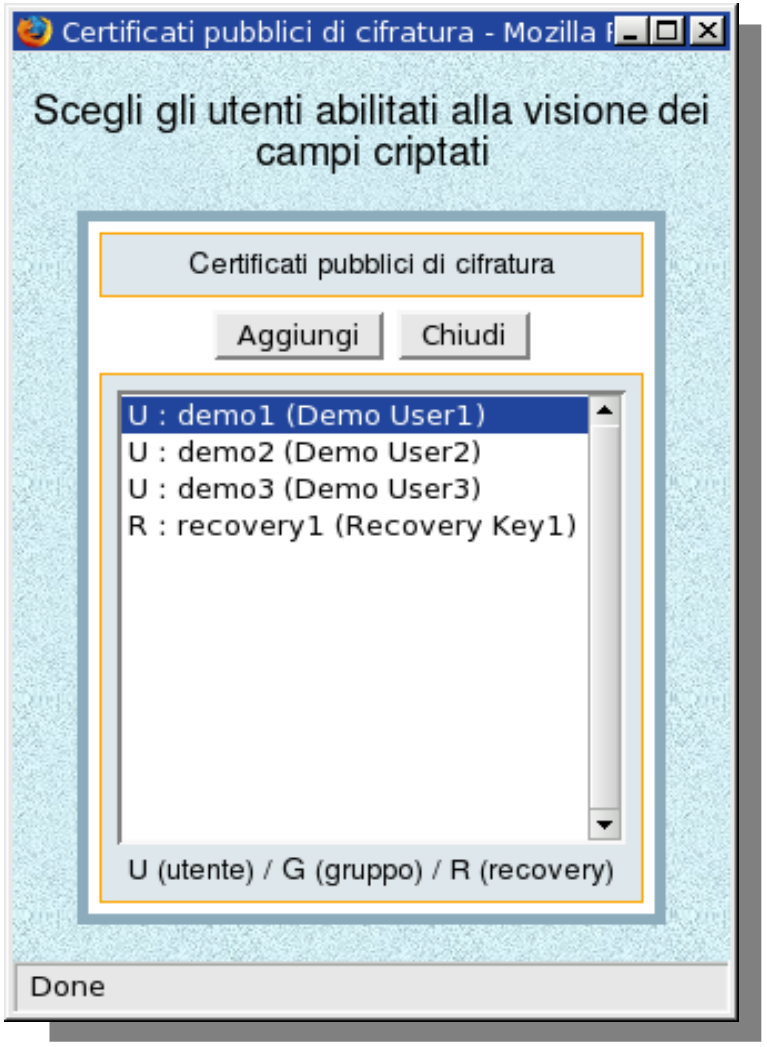
- Anche la crittografia è basata sull'uso di certificati con chiavi asimmetriche
- Solo la crittografia sul client permette la ***vera*** garanzia di sicurezza: i dati sensibili o riservati non arrivano mai in chiaro sul server
- Anche gli amministratori dei sistemi non hanno alcuna possibilità di accesso ai dati criptati come richiesto dal D.L. 196/2003 per il trattamento dei dati sensibili

Modulo di Crittografia

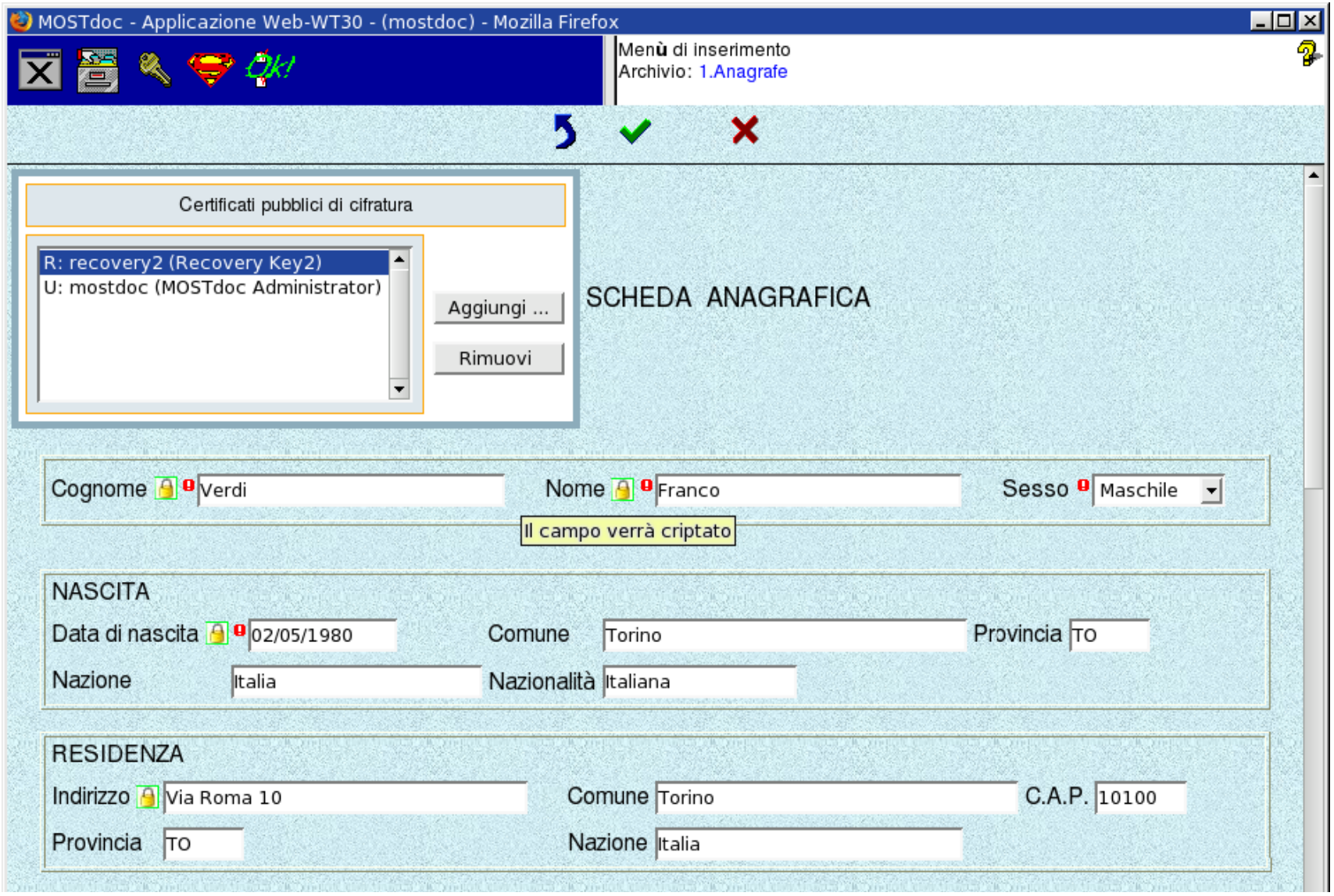
- I documenti criptati sono memorizzati nello storage in formato standard (pkcs#7)
- Una crittografia standard permette l'utilizzo di molteplici sistemi di visualizzazione:
  - qualunque software di gestione file criptati a chiave pubblica,
  - modulo web di crittografia MOSTsec,

Modulo di Crittografia

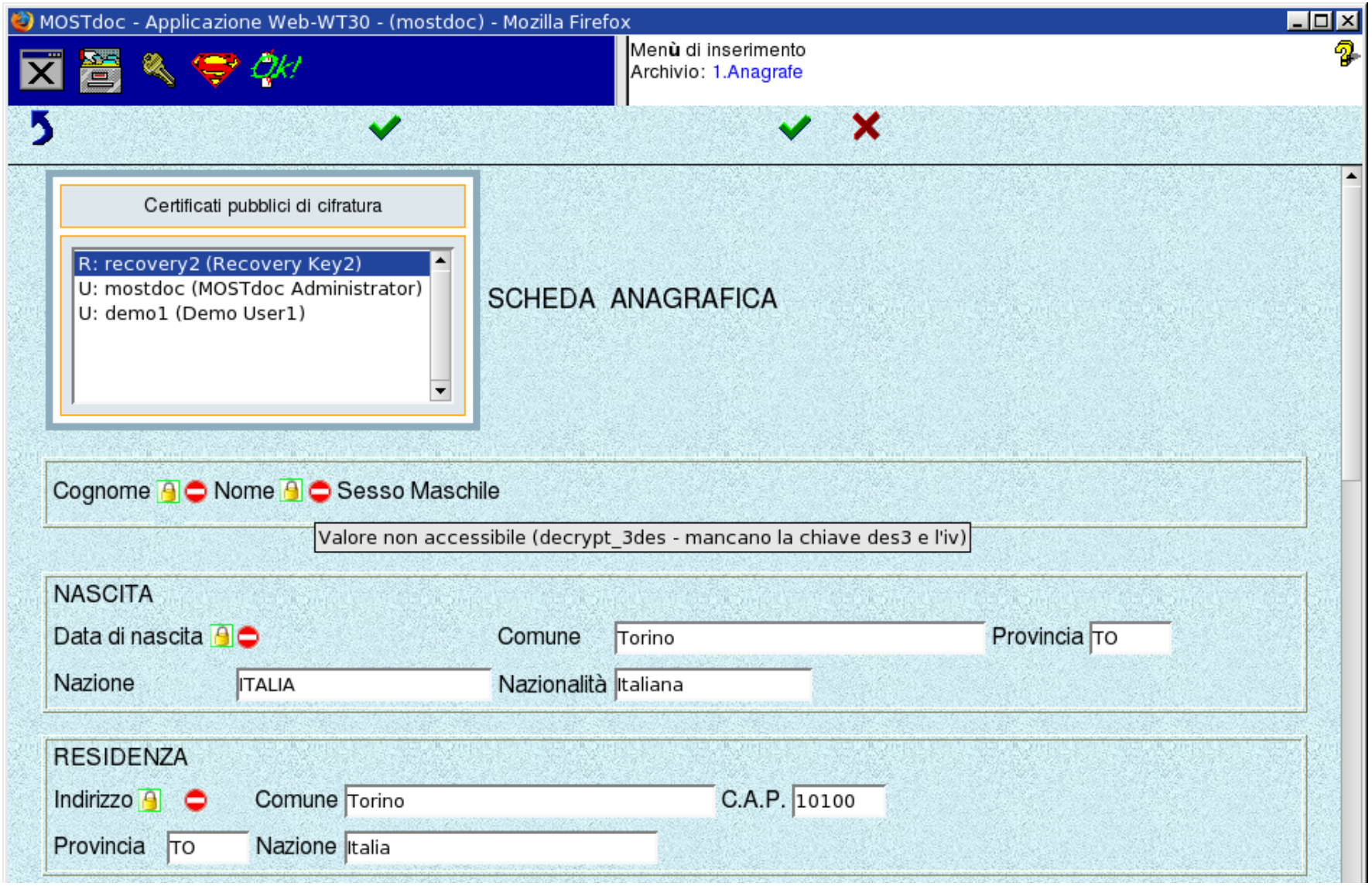
- In inserimento/modifica è possibile scegliere l'elenco degli utenti abilitati alla visualizzazione
- Gli utenti abilitati alla visione dei dati criptati posso *"estendere"* a posteriori il diritto di accesso ad altri utenti



Una cartella clinica
es. di sicurezza su dati sensibili



Una cartella clinica
es. di dati sensibili non accessibili

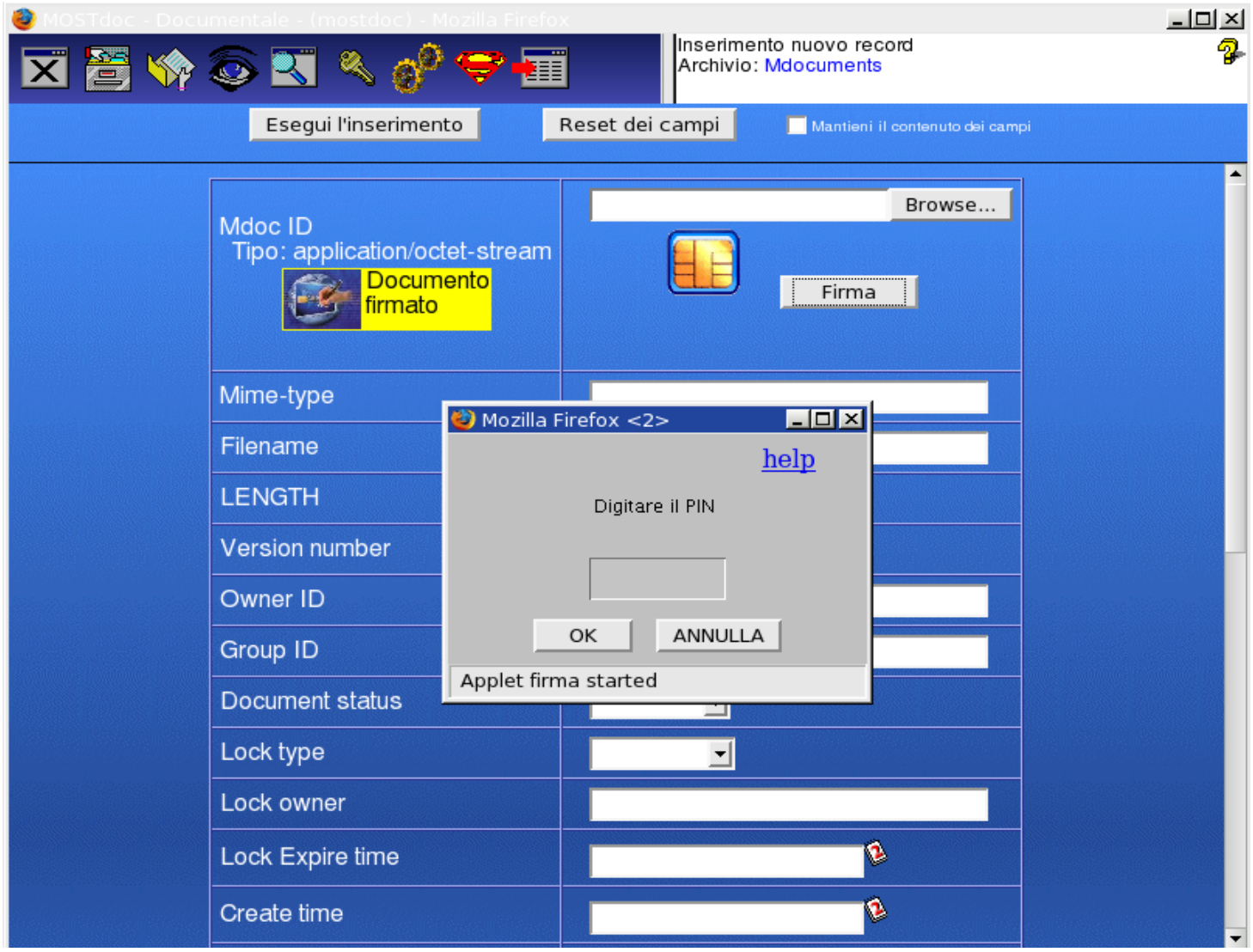


Ricerca su archivio con e senza accesso ai dati criptati

Modulo di Firma

- Apposizione della firma secondo le regole definite di "*firma forte*"
- Firma dei singoli documenti
- Firma dei supporti di memorizzazione per archiviazione sostitutiva
- Verifica di validità dei certificati rispetto agli elenchi pubblici (CRL) e apposizione di marca temporale ufficiale (timestamping)

Firma del singolo documento



Firma di chiusura di un CD