

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

MOST

The screenshot shows a Mozilla Firefox browser window titled "MOSTdoc Archiving System - Welcome Page - Mozilla Firefox". The address bar contains the URL "http://192.168.1.169:9999/WWW/MOSTI". The main content area has a blue background with the "MOSTdoc Archiving System" logo and text. A central dialog box displays the following information:

utente di prova #1	
mostdoc administrator - 4111	
<input type="text"/>	
Password/PIN <input type="text"/>	
<input type="button" value="OK"/>	

At the bottom of the browser window, a status bar indicates "Applet it.most.cipher.Crypt loaded".

Modulo di Crittografia

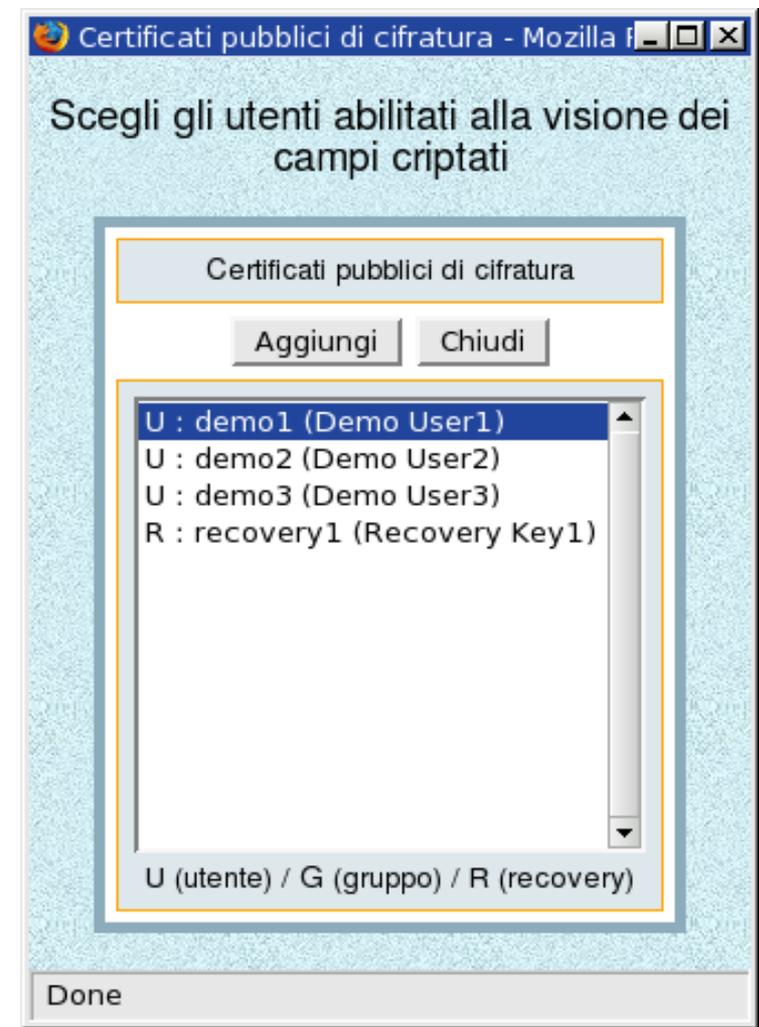
- Anche la crittografia è basata sull'uso di certificati con chiavi asimmetriche
- Solo la crittografia sul client permette la **vera** garanzia di sicurezza: i dati sensibili o riservati non arrivano mai in chiaro sul server
- Anche gli amministratori dei sistemi non hanno alcuna possibilità di accesso 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

MOSTdoc - Applicazione Web-WT30 - (mostdoc) - Mozilla Firefox

Menù di inserimento
Archivio: 1.Anagrafe

↩ ✓ ✗

Certificati pubblici di cifratura

R: recovery2 (Recovery Key2)
U: mostdoc (MOSTdoc Administrator)

Aggiungi ...
Rimuovi

SCHEDA ANAGRAFICA

Cognome   Verdi Nome   Franco Sesso  Maschile

Il campo verrà criptato

NASCITA

Data di nascita   02/05/1980 Comune Torino Provincia TO

Nazione Italia Nazionalità Italiana

RESIDENZA

Indirizzo  Via Roma 10 Comune Torino C.A.P. 10100

Provincia TO Nazione Italia

Una cartella clinica es. di dati sensibili non accessibili

MOSTdoc - Applicazione Web-WT30 - (mostdoc) - Mozilla Firefox

Menù di inserimento
Archivio: 1.Anagrafe

← ✓ → ✓ ✗

Certificati pubblici di cifratura

- R: recovery2 (Recovery Key2)
- U: mostdoc (MOSTdoc Administrator)
- U: demo1 (Demo User1)

SCHEDA ANAGRAFICA

Cognome Nome Sesso

Valore non accessibile (decrypt_3des - mancano la chiave des3 e l'iv)

NASCITA

Data di nascita Comune Provincia

Nazione Nazionalità

RESIDENZA

Indirizzo Comune C.A.P.

Provincia Nazione

Ricerca su archivio con e senza accesso ai dati criptati

MOSTdoc - Applicazione Web-WT30 - (mostdoc) - Mozilla Firefox

Ricerca semplice
Archivio: 1.Anagrafe

2 record trovati 2 record per pagina dal 1 al 2

<input checked="" type="checkbox"/>	Identificatore	Cognome	Nome	Sesso	Data di nascita	Provincia	Indirizzo	Comune	Telefoni	Nazionalità
<input type="checkbox"/>	___TOMBBCN	Verdi	Franco	Maschile	02/05/1980	TO	Via Roma 10	Torino	011-0000000 348-000000000	Italiana
<input type="checkbox"/>	___MBBCO	Rossi	Mario	Maschile	01/05/2005	MI	Via di Rossi	Rho	Tel di Rossi	Italiana

MOSTdoc - Applicazione Web-WT30 - (mostdoc) - Mozilla Firefox

Ricerca semplice
Archivio: 1.Anagrafe

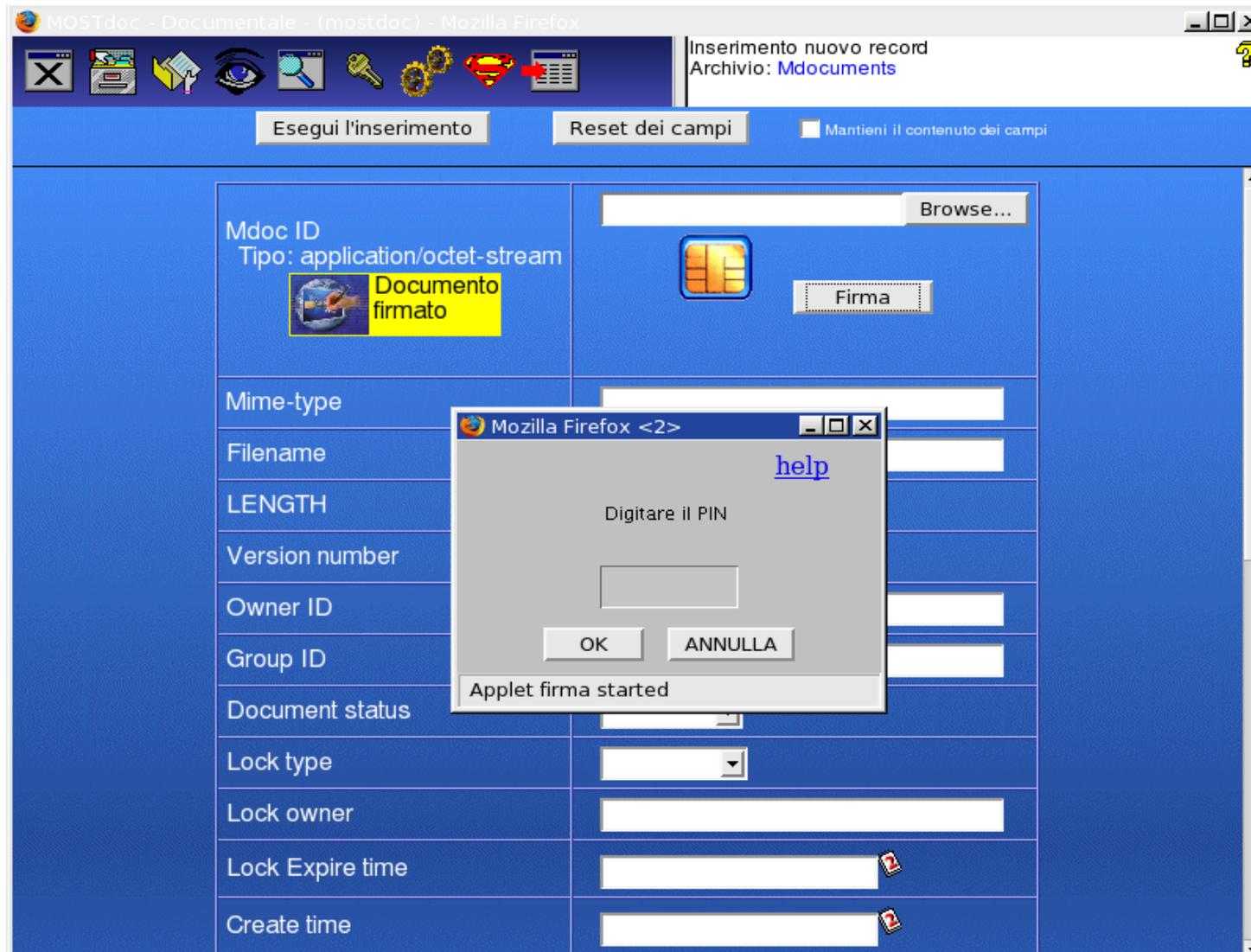
2 record trovati 2 record per pagina dal 1 al 2

<input checked="" type="checkbox"/>	Identificatore	Cognome	Nome	Sesso	Data di nascita	Provincia	Indirizzo	Comune	Telefoni	Nazionalità
<input type="checkbox"/>	___TOMBBCN			Maschile		TO		Torino		Italiana
<input type="checkbox"/>	___MBBCO			Maschile		MI		Rho		Italiana

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

Mozilla Firefox <2>

Procedura di firma del CD

File di chiusura da firmare

Firma

Procedi con la generazione del CD Chiudi

Done

Mozilla Firefox <3>

[help](#)

Digitare il PIN

OK ANNULLA

Applet firma started

Mozilla Firefox

Gestione CD

Owner	Label	n° CD	Applicazione	Data	CD da firmare	Stato di produzione	Azione	File di log
mostdoc	4292E3EEA9147009	1	EPROC	24/05/2005 10:21:02-10:21:02	<input checked="" type="checkbox"/>	Processo interrotto (Preparazione dei contenuti)	Rimozione dei LOG	Mostra il LOG
mostdoc	4292E416A9157404	1	EPROC	24/05/2005 10:21:42-10:22:26	<input checked="" type="checkbox"/>	CD in attesa di firma		Mostra il LOG

Aggiorna Torna al menù principale Chiudi

Done