



DISPONIBILE LA RELEASE 3.0

INTRODUZIONE

La release 3.0 di Cryptodocs comporta importanti modifiche ed estensioni. Tali requisiti si riferiscono in particolare a quanto segue:

- revisione della logica di gestione del processo di cifratura dei documenti, sia a livello utente che di gruppo, specie in presenza di documenti con versioni multiple
- possibilità di assegnare attributi di DRM ai documenti, specificatamente le autorizzazioni di stampa, copia, consultazione offline degli stessi.

Le estensioni in oggetto riguarderanno quindi, come di seguito descritto, un'estensione/revisione dei componenti di cifratura e il potenziamento dei moduli (sia lato cliente che lato server) di gestione degli attributi DRM. Sebbene quest'ultima funzionalità sia disponibile nella versione corrente del prodotto, la dipendenza da moduli di terze parti ne rende complesso ed oneroso per il cliente l'effettivo utilizzo. Le estensioni hanno appunto l'obiettivo di rimuovere questa dipendenza.

Infine la release 3.0 predispone l'applicazione alla realizzazione dei web services di cifratura.

SPECIFICHE FUNZIONALI

Sottosistema di cifratura

Allo scopo di rispondere al requisito di una semplificazione della gestione delle ACL di accesso/decifratura del documento, il flusso di esecuzione di Cryptodocs è stato rivisto secondo le logiche descritte qui di seguito. Si noti che tale flusso presuppone l'utilizzo del sistema documentale tramite interfaccia web (CyberDOCS / DM WebTop). L'implementazione dei componenti di interfaccia è stata progettata in modo da essere quanto meno possibile invasiva rispetto il codice standard, essendo prevista la realizzazione di moduli indipendenti e facilmente integrabili in versioni successive del prodotto OpenText. L'utilizzo della soluzione Cryptodocs con PowerDOCS o DM Extensions non è al momento previsto.

- Il documento viene inserito nel sistema documentale (check-in) tramite le consuete operazioni. La trasmissione al server avviene su canale sicuro (HTTPS). La copia locale (o residente in una cartella di rete) del documento appena caricato viene gestita dall'utente. La cosa più ragionevole è che questa venga cancellata. Le successive modifiche passeranno infatti per il sistema documentale dove il documento è conservato cifrato.
- Non appena il servizio di cifratura di Cryptodocs riconosce l'avvenuta indicizzazione del documento da parte del servizio di indicizzazione, procede con la cifratura dello stesso utilizzando solo ed esclusivamente la chiave pubblica del Master Certificate. Quest'ultimo viene definito in fase di setup di Cryptodocs. E' comunque un aspetto parametrico modificabile anche in seguito.
- In caso di compromissione di un Master Certificate (in altre parole, la sua revoca perché ritenuto non più sicuro), sarà possibile sostituirlo. A tal fine sarà necessario configurare il nuovo certificato, procedere con la decifrazione massiva dei documenti della/e libreria/e coinvolta/e e infine risottomettere i documenti al servizio di cifratura.

Allo scopo di ridurre l'impatto di tale operazione sulla disponibilità del sistema, è possibile definire un Master Certificate diverso per ogni libreria documentale. È comunque da tenere in considerazione il fatto che anche il master certificate ha una scadenza e che quindi si dovrà procedere in prossimità della stessa alla configurazione di un nuovo Master Certificate. L'operazione di decifrazione del documento avviene correttamente, anche se il certificato è scaduto.

Nota: la perdita (cancellazione o illeggibilità) del Master Certificate comporta necessariamente l'impossibilità di decifrare i documenti con esso cifrati. E'

fondamentale mantenere in luoghi sicuri copie di sicurezza di questo certificato.

- Lo store dove è mantenuto il Master Certificate, e la sua chiave privata, è individuato in prima istanza essere lo store Utente di sistema. Questo di fatto garantisce che solo l'utente che esegue queste operazioni (quello che esegue il servizio di DM Server) abbia accesso ai contenuti cifrati. E' d'altro canto vero che un amministratore di dominio potrebbe modificare la password dell'utente Cryptodocs per poi accedere tramite di essa allo store in cui è mantenuto il certificato. Allo scopo di ridurre questo rischio è possibile ipotizzare il mantenimento del certificato su un dispositivo hardware sicuro.
- In fase di consultazione o modifica (visualizzazione, get-copy, check-out) il documento viene decifrato, utilizzando la chiave privata del Master Certificate, e ri-cifrato con la chiave pubblica dell'utente collegato. Durante questa operazione, che si svolge interamente in memoria, non è salvato in alcuna locazione sul server il documento in chiaro.
- Prima di procedere all'operazione di cifratura per il destinatario del documento viene controllata la validità e l'eventuale revoca del certificato del destinatario. Non è consentito inviare un documento ad un destinatario, che pur avendo i diritti (ACL) di accesso al documento non sia in possesso di un certificato valido.
- Il documento viene spedito cifrato al client mediante HTTP (essendo cifrato non è necessario avvalersi di HTTPS).
- Una volta sul client il documento viene decifrato utilizzando il Cryptodocs Client e visualizzato con l'applicazione nativa (es: Acrobat Reader).

Vantaggi derivanti dal nuovo modello di gestione della cifratura dei documenti

L'elemento qualificante nella logica di cifratura sopra descritta è certamente riconducibile al processo di generazione dinamica (a runtime) di una "istanza" del documento decifrabile dal solo richiedente (se questo dispone dei diritti di accesso al documento stesso, ovviamente). Ciò semplifica di gran lunga la problematica relativa alla riassegnazione dei diritti di accesso ai documenti, sia a livello di utenti che di gruppi, anche rispetto le singole versioni. La logica originale di Cryptodocs comportava infatti necessariamente una operazione di decifratura/cifratura del documento in corrispondenza di una modifica delle ACL con la corrispondente rigenerazione della busta contenente le content encryption keys associate agli utenti abilitati alla lettura. In caso di versioni multiple, sarebbe stato necessario effettuare questa operazione su tutte le versioni del documento. La nuova logica evita questa operazione proprio grazie alla generazione dinamica che del documento cifrato basata sulle ACL correnti.

Considerazioni sui tempi di elaborazione

Come detto, al momento della consultazione, il documento viene decifrato e ri-cifrato. Bisogna quindi considerare un certo tempo di latenza dovuto a queste operazioni (che avvengono esclusivamente sul server). Indicativamente su una macchina con processore da 1,8 GHz e 1 GB di memoria RAM tale elaborazione con un documento da 10 MB impiega circa 3 secondi. A questo tempo va poi aggiunto quello di download che dipende però da diversi fattori (es: velocità della rete, interfaccia di rete, proxy, firewall, sub-net...) non valutabili a priori.

Accesso alle chiavi pubbliche, CRL, CSL

Le chiavi pubbliche necessarie alla cifratura sono in condizioni normali scaricate dal server LDAP. Ne viene comunque anche mantenuta una copia locale sul server Cryptodocs allo scopo di permettere l'operatività di Cryptodocs anche in assenza di connettività con il server LDAP (la copia verrà aggiornata periodicamente con un processo di sincronizzazione batch).. Le liste di revoca e sospensione dei certificati sono invece sempre consultate direttamente da LDAP per garantire il massimo dell'aggiornamento. Se un certificato è revocato o sospeso non è possibile procedere alle operazioni di cifratura e decifratura.

Sottosistema di DRM

Gli obiettivi che si è inteso perseguire con l'implementazione di questo sotto sistema sono stati quelli non solo di controllare che un documento sia fruibile da una determinata persona o da un gruppo di persone, cosa che si realizza con la combinazione dei diritti assegnati al documento nel sistema documentale (ACL) e la crittografia, ma anche di controllare altri fattori quali, ad esempio, se il destinatario può o meno produrre la stampa del documento, se ne può salvare una copia, se può accedere al documento solamente se on line o anche off line, se solo dal computer dal quale ha operato la richiesta o anche da un altro computer.

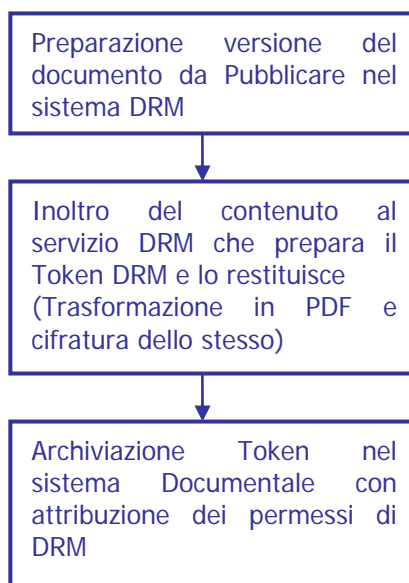
Tali obiettivi comportano quindi la necessità di aggiungere alla normale definizione di accesso ai documenti (ACL) i diritti DRM. Tali diritti possono essere espressi sia a livello di documento che di singola versione dello stesso (è possibile definire impostazioni di default a livello di documento che potranno essere rimpiazzate a livello di singola versione). Questo permette all'applicativo documentale di costruire le versioni appropriate per ciascuna lista di distribuzione e di assegnare a ciascuna di esse i diritti DRM voluti.

Il sistema DRM di DocFlow non manipola il contenuto del documento al fine di oscurare o meno zone dello stesso in funzione dei permessi di visibilità che si vogliono attribuire, ma applica i permessi DRM a una specifica Versione.

Il contenuto DRM ottenuto è inviato al client che lo richiede come un qualsiasi altro documento. L'applicazione DRM Client viene attivata e ricevuto il contenuto DRM si preoccupa di contattare il Server e di controllare i diritti che vengono assegnati al destinatario. Ne attiverà l'effettiva accessibilità secondo i criteri impostati.

Un contenuto DRM fa riferimento a un Token calcolato in fase di pubblicazione DRM di un determinato documento. Si noti che il documento vero e proprio in questa fase viene convertito in un formato protetto PDF o TIFF, in modo da poter consentire al client di lavorare su formati conosciuti.

Di seguito è descritto uno schema logico delle operazioni che debbono essere svolte per la pubblicazione di un documento nel sistema DRM.

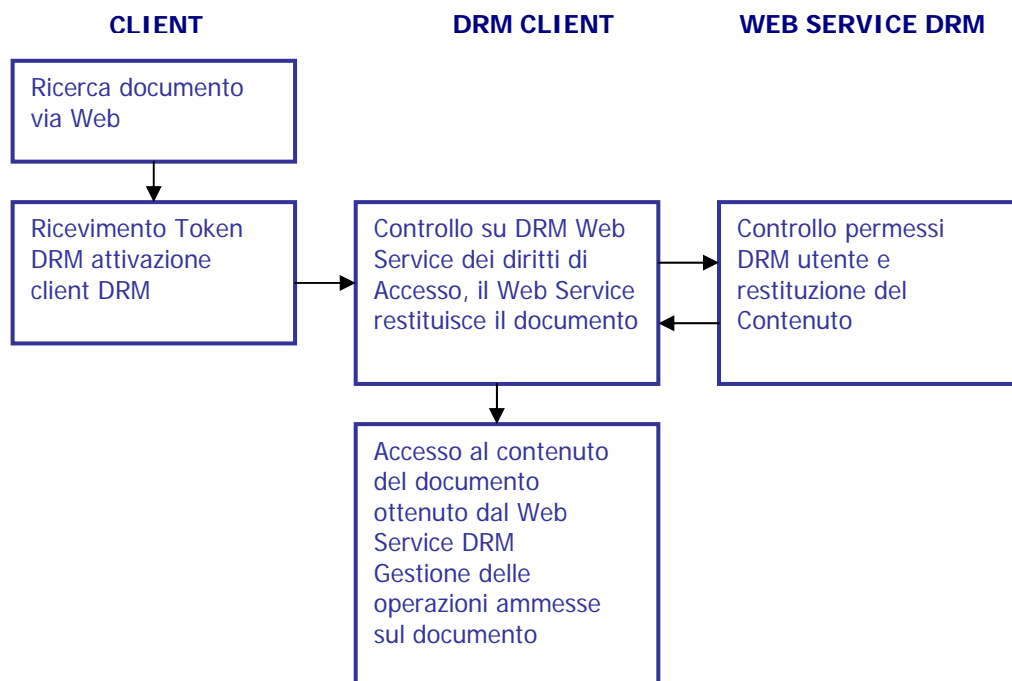


Il contenuto DRM può essere inviato al client come un qualsiasi altro tipo di documento in quanto non contiene il documento vero e proprio ma i riferimenti necessari all'individuazione dello stesso una volta che il client DRM contatterà il Server per ottenerlo.

Con questa tecnica non ci si deve preoccupare del fatto che a questo Token ci sia un accesso indesiderato, in quanto sarebbe fine a se stesso, non contiene informazioni sul contenuto del documento, solo un client autorizzato potrà utilizzarlo per ottenere il documento stesso.

Qualora dopo il primo accesso il client autorizzato abbia il diritto di consultazione off-line, verrà calcolato un contenuto protetto cui il client stesso avrà accesso anche in modalità off-line.

Di seguito è descritto lo schema logico delle operazioni che vengono svolte per la consultazione di un documento protetto con il sistema DRM di DocFlow.



Durante le operazioni di produzione del contenuto DRM è possibile produrre un Watermark sul documento.

Il DRM Client, integra le funzionalità del Client per i documenti cifrati e può opzionalmente includere la capacità di verifica di eventuali contenuti firmati in formato pkcs7 (.p7m).

DRM e ciclo di vita del documento

Dal punto di vista dell'utilizzo del sistema di DRM nell'ambito del ciclo di vita del documento, lo scenario che ci pare possa essere applicato ad un tipico utilizzo è il seguente.

- Completato il processo di creazione e revisione, viene generata la versione PDF del documento ed ad essa viene apposta la firma. Di fatto si può parlare di questa come di versione pubblicata.
- Raggiunto questo stato nel ciclo di vita del documento, viene attivata la funzione di "Pubblicazione DRM". Grazie ad essa l'utente può assegnare i diversi diritti DRM a utenti e gruppi. I diritti DRM della versione considerata possono essere ereditati da una configurazione di default associata alla libreria, al document type o al profilo documentale.

3. Struttura del sistema

Il sistema si compone dei seguenti elementi

Sottosistema di cifratura

- Modifica alla procedura di upload dei documenti

Nel caso sia stata richiesta la cifratura del documento, la routine di upload copia il file sul document server (opzionalmente configurato come encrypted file system) accessibile al servizio di indicizzazione del DM

- Servizio di cifratura

Monitora le librerie documentali in attesa di documenti "marcati" per la cifratura. Procede con la cifratura degli stessi con la chiave pubblica del Master Certificate non appena riconosciuta l'avvenuta indicizzazione.

- Modifica alla procedura di download dei documenti

In seguito ad una richiesta di un utente per operazione di visualizzazione, get-copy o check-out, la procedura di download esegue le seguenti operazioni:

- o Effettua la lettura delle ACL documentali
- o Se l'utente è abilitato all'accesso, reperisce la sua chiave pubblica sul server LDAP (o su cache locale se il primo non è accessibile)
- o Effettua la verifica delle revocation lists
- o Decifra il documento utilizzando la chiave privata del Master Certificate e lo ricifra utilizzando la chiave pubblica del destinatario.
- o Trasmette il documento al richiedente

- Client di decifratura

Si tratta di un plug-in di Internet Explorer. Viene attivato non appena un documento cifrato è scaricato dall'interfaccia utente. Verifica la disponibilità del certificato corrispondente e procede con la decifratura in memoria del documento.

- Utility di amministrazione del sistema di cifratura

Permette:

- o La gestione dei Master Certificate: associazione di certificato a libreria, mantenimento su storage sicuro
- o la decifratura massiva dei documenti di una libreria
- o la configurazione delle regole di accesso al server LDAP
- o la configurazione della copia periodica delle chiavi pubbliche degli utenti su cache locale

Sottosistema DRM

- Funzione applicativa di gestione della pubblicazione DRM

Si tratta di una estensione all'interfaccia utente richiamabile da menu standard di gestione del documento. Una volta richiamata, permette all'utente di:

- Determinare la versione da pubblicare
- Specificare i diritti di accesso/utilizzo (stampa, copia, visualizzazione offline) del documento per utenti e gruppi

La funzione effettua poi la conversione in PDF del documento e la generazione del token DRM

- *Client di visualizzazione*

Si tratta di fatto dello stesso client di decifratura (plug-in di Internet Explorer) sopra descritto, a cui sono aggiunte estensioni utili ad interpretare il contenuto del token DRM ed ad attivare le operazioni ammesse per il documento.

- *Web service per il colloquio del client DRM con il server*

Permette al client di interagire con il server per ottenere dinamicamente informazioni relative alle operazioni ammesse per il documento