UNIVERSITÀ DEGLI STUDI DI BOLOGNA
FACOLTÀ DI INGEGNERIA
Corso di Laurea Magistrale in Ingegneria Informatica

Attività Progettuale di Sicurezza dell'Informazione M

Librerie per la Firma Digitale di documenti PDF

Attività Progettuale di:

Francesco Ongaro

Professore:

Prof.ssa Ing. Rebecca Montanari

Tutor:

Dott.ssa Ing. Anna Riccioni

Anno Accademico 2010 - 2011

Indice

Introduzione....5

Capitolo 1. La firma digitale....6

Capitolo 2. La busta crittografica....7

Capitolo 3. Il formato PDF....8

3.1 Il formato PAdES e CAdES....8

Capitolo 4. Creazione della firma digitale....10

4.1 L'Oggetto Signature Dictionary....10

4.1.1 Il ByteRange....12

4.1.2 Il Contents....13

4.2 Workflow....14

4.3 Algoritmi....15

4.4 Metodi di verifica....15

4.5 Marcatura temporale....16

4.6 Verifica a lungo termine....18

4.6.1 PAdES-LTV....19

4.6.2 PDF/A....22

Capitolo 5. Strumenti utilizzati....24

5.1 Ambiente di sviluppo....24

5.2 Librerie iText....24

5.3 Certificato e Servizi di revoca....24

5.4 Time Stamp Service....25

Capitolo 6. Il codice....26
6.1 Firma di un documento PDF....26
6.1.1 Operazioni preliminari di firma....26
6.1.2 Generazione del digest....29
6.1.3 Recupero informazioni sullo stato di revoca....30
6.1.3.1 OCSP....30
6.1.3.2 CRL....31
6.1.4 Time Stamping....31
6.1.5 Autenticazione degli attributi....32
6.1.6 Firma esterna degli attributi....33
6.1.6.1 Firma interna degli attributi....34
6.1.7 Creazione dell'oggetto PKCS7....34
6.1.8 Verifica dello spazio per contenere la firma....35
6.1.9 Inserimento dell'oggetto PKCS7 nel Contents....35
6.1.10 Firma di un generico input....37
6.2 Firme multiple....40
6.2.1 Verifica livello di certificazione del documento....42
6.2.2 Estrazione di una revisione dal documento....43
6.3 Verifica di un documento PDF....44
6.3.1 Integrità e copertura della firma....44
6.3.2 Verifica stato di revoca tramite lista CRL....47
6.3.3 Verifica stato di revoca tramite richiesta OCSP....49
6.3.4 Output della verifica....50
6.3.5 Recupero allegati di un documento firmato....52
Capitolo 7. Conclusioni e sviluppi futuri....53
Riferimenti Bibliografici....55

Introduzione

L'attività progettuale in oggetto verte sulla realizzazione di librerie Java per la firma digitale, e attività connesse, di documenti in formato PDF.

L'implementazione di tale attività si è appoggiata alle librerie iText, attualmente tra le più interessanti per la gestione e manipolazione di documenti in formato PDF.

Inoltre per poter gestire correttamente alcuni algoritmi avanzati di generazione del digest e della firma digitale, è stato necessario appoggiarsi alle librerie di sicurezza Bouncy Castle.

Aspetto fondamentale è stato quello di cercare di realizzare il progetto in modo da essere in linea con i vincoli imposti dalla nostra normativa italiana [DLB1], la quale a sua volta è basata sulle specifiche tecniche europee ETSI [ETSI1] che forniscono importanti profili per l'implementazione della firma digitale nei documenti PDF, in accordo con lo standard internazionale ISO/IEC 32000 e successivi.

Per capire come sia possibile firmare e verificare digitalmente documenti, si è partiti andando a vedere come questo formato sia strutturato all'interno, spiegando in dettaglio la parte relativa alla firma digitale. Inoltre si è cercato di fornire dettagli al contorno utili all'effettiva realizzazione e test dell'attività progettuale.

Si è voluto inoltre dare un quadro generale sui principi alla base della firma digitale e delle attività connesse per la realizzazione e la verifica delle stessa, nonché dettagli per la realizzazione di documenti che possano essere verificati anche a lungo termine.

Tutta l'attività progettuale ha preso come documentazione normativa di riferimento la Deliberazione CNIPA N.45 del 21/05/09 e come documentazioni tecniche le varie specifiche rilasciate dall'organismo europeo ETSI nonché standard ISO e RFC. Si è cercato di inserire scrupolosamente ogni riferimento a tali documentazioni