



DocFlow adotta le nuove regole per la firma digitale

Milano, settembre 2010

Lo scorso 3 settembre sarebbero dovute entrare in vigore le nuove regole per il riconoscimento e la verifica dei documenti informatici. Tali regole prevedevano alcune modifiche agli algoritmi ed ai certificati per la generazione delle firme elettroniche.

Il 28 luglio è stato **rinvio il termine per l'adeguamento al 31 dicembre**, con un provvedimento che introduce ulteriori modifiche agli algoritmi. Le smartcard (e gli altri dispositivi di firma), in ogni caso, resteranno validi fino alla loro scadenza naturale.

DocFlow ha predisposto le modifiche ai programmi per l'apposizione e la verifica delle firme e delle marche temporali richieste dalle nuove regole, adeguandosi anche alle regole in fase di emanazione da parte della Comunità Europea.

Dal punto di vista degli utenti tutte le modifiche sono trasparenti, questi continueranno ad apporre le firme e le marche temporali nello stesso modo, saranno i programmi a gestire le nuove richieste. In tal modo i clienti DocFlow non saranno costretti ad investire altro tempo per la formazione degli utenti.

Le nuove regole sono state emanate per incrementare il livello di sicurezza, infatti è stata incrementata la lunghezza minima della chiave di crittografia (da 1024 a 2048) ed è stato modificato il

DocFlow

DocFlow Italia SpA
Centro Direzionale Milanofiori
Strada 4 Palazzo Q8
20089 Rozzano MILANO

Tel 02 57503366
Fax 02 57503369
marketing@docflow.it

www.docflow.com

Le modifiche incrementano notevolmente il livello di sicurezza delle firme apposte

calcolo dell'impronta da SHA-1, che prevede la generazione di un'impronta (hash) di 160 bit (20 caratteri), a SHA-256, che porta la lunghezza dell'impronta a 256 bit (32 caratteri).

Le due modifiche incrementano notevolmente il livello di sicurezza delle firme apposte, la chiave più lunga rende enormemente più lunga un eventuale operazione di forzatura della chiave, mentre l'aumento della lunghezza dell'impronta porta la probabilità di individuare un testo che generi la stessa impronta da 15 preceduto da 47 zeri a 115 preceduto da 75 zeri. Un eventuale malintenzionato che volesse provare a "violare" una firma digitale avrebbe la vita ancora più dura di quanto non lo sia oggi.

Le tecnologie attuali non permettono di falsificare una firma digitale già con le vecchie regole. La modifica è stata fatta, in considerazione della diffusione della firma, per permettere anche alle generazioni future di poter mantenere la validità dei documenti informatici firmati digitalmente oggi.



Le regole tecniche impongono anche modifiche agli attributi contenuti nei certificati di firma, in modo da adeguarsi, in anticipo, alla imminente direttiva europea sulla firma digitale che serve a uniformare le leggi dei singoli Stati componenti la Comunità Europea, i nuovi attributi permetteranno di validare in ogni Paese della Comunità Europea le firme apposte con un certificato emesso da una Certification Authority di un Paese diverso.

Oggi il riconoscimento, seppur ammesso giuridicamente, dal punto di vista tecnico ha notevoli difficoltà. In questo modo si risolveranno gran parte delle incompatibilità.

DocFlow

DocFlow Italia SpA
Centro Direzionale Milanofiori
Strada 4 Palazzo Q8
20089 Rozzano MILANO

Tel 02 57503366
Fax 02 57503369
marketing@docflow.it

Per informazioni: www.docflow.com

<http://blog-conservazione-sostitutiva.docflow.com>

www.docflow.com