

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 625 di venerdì 20 settembre 2002

Attenzione al formato dei documenti digitali "firmati"!

Vulnerabilit  in un software di firma digitale di un ente certificatore italiano.

La notizia giunge dalla rivista telematica InterLex. Il software DiKe di firma digitale di Infocamere, ente certificatore italiano, consentirebbe di apporre la firma digitale su un documento in Microsoft Word, con particolari caratteristiche, e successivamente visualizzare il documento stesso modificato senza che il processo di verifica della firma si accorga della modifica.

Il problema   stato rilevato nella gestione dei documenti Word contenenti campi dinamici, cio  configurabili tramite variabili (un esempio di campo variabile   la data).

Dalle prove effettuate da Interlex emerge che " se si usano alcuni di questi campi in un documento Word, il destinatario verificher  correttamente la firma, ma il contenuto dei campi potr  cambiare in funzione delle variabili d'ambiente presenti sul suo computer."

Il programma di firma funziona correttamente, "infatti se si prova a modificare il contenuto dei campi su un file firmato, la firma non viene pi  verificata come valida".

I problemi sono nel software di verifica che "nel momento di visualizzare il documento ricalcola il valore dei campi e li mostra modificati"

Infocamere ha affermato di essere a conoscenza del problema, ma non lo ritiene rilevante in quanto i documenti Word , resi "firmabili" in un secondo tempo, su richiesta degli utenti, non possono essere usati per firmare documenti a "valore legale".

...ma la scritta "verifica completata correttamente", che appare sul documento word firmato pu  trarre in inganno...