Il formato del messaggio che i gruppi devono scambiare è il seguente

f	$Sig(k^{s}_{pr,M}(File))$	$Enc(k^{e}_{pub,D}(k_{sk}))$	IV	$Enc(k_{sk}, File)$

f è un flag di un byte (dettagli in seguito)

$k^{s}_{pr,M}$ è la chiave privata di firma del mittente

$k^{e}_{pub,D}$ è la chiave pubblica di cifratura del destinatario

k_{sk} è la chiave segreta con cui è stato cifrato il documento File

IV è il vettore di inizializzazione del cifrario a blocchi

La firma potrebbe avere una dimensione variabile poiché è codificata in ASN.1.

Se non riuscite a implementare il formato del messaggio richiesto, inserire la firma in un file a parte che avrà lo stesso nome del messaggio ed estensione .sig. Il flag f indica se la firma del documento è in un file a parte (in questo caso il primo byte del messaggio è settato a 0x01). Se il flag f è settato a 0x00 i byte successivi rappresentano i byte della firma.