DIREZIONE DEGLI ARMAMENTI NAVALI

Trasmissione documentazione per offerta di gara

Oggetto: descrizione della procedura adottata dalla Direzione per la trasmissione della documentazione di un'offerta di gara.

Generalità

La metodologia di seguito esposta si basa sulla creazione di un file contenitore avente la funzione di "busta crittografica" (indicato di seguito come "busta principale"), nel quale devono essere inseriti i file da trasmettere (nel caso specifico questi file sono suddivisi in due altre buste crittografiche).
La tecnica utilizzata è quella della crittografia simmetrica.
La busta principale, così predisposta, deve poi essere trasmessa da indirizzo pec/rem all'indirizzo pec della Direzione, entro il termine dalla stessa stabilito.
Decorso tale termine e sempre entro successiva data stabilita dalla Direzione, il mittente deve inviare, stesso mezzo, la chiave di crittografia necessaria ad aprire la busta principale precedentemente spedita.
Le altre due chiavi saranno comunicate su richiesta della Direzione.
Il mittente è responsabile della corretta creazione delle buste (file contenitori), dell'adeguatezza delle chiavi di crittografia simmetrica utilizzate, dell'inserimento nelle buste di tutti i file necessari ed eventualmente della corretta apposizione di firme elettroniche e delle marche temporali sui file stessi.
Più specificamente è necessario poi attenersi ai dettagli tecnici riportati di seguito.

Schema temporale della procedura

Fase1

Scelta delle chiavi crittografiche a cura del mittente (ciascuna chiave dovrà essere una stringa alfanumerica di almeno 15 caratteri contenente almeno un carattere speciale ed una lettera maiuscola)
es: Agjt51ytr9$rf56Yh
Creazione del file container (busta) *es: busta_per_documenti.hc*
Inserimento dei file nella busta principale (nel caso specifico altre due buste contenenti i documenti).
Spedizione pec/rem - pec della busta principale.
(NB le buste NON devono essere firmate elettronicamente o altrimenti alterate, i file contenuti nelle buste possono invece avere firma elettronica).

Fase 2

Invio pec/rem - pec in chiaro della chiave crittografica necessaria per aprire la busta principale.

Elementi tecnici

Software di crittografia da utilizzare: ***VeraCrypt*** - *ultima versione stable disponibile*

free open source disk encryption software for Windows, Mac OSX and Linux.

https://www.veracrypt.fr/en/Home.html

Elementi per la creazione del file container:

Creazione di un encrypted file container - Standard VeraCrypt Volume

Algoritmo di crittografia: ***AES***

Algoritmo di hash: ***SHA-512***

Filesystem type*: **NTFS / FAT32***

Crittografia: ***password (no PIM o keyfile)***

Si consiglia l'aggiunta di un'estensione .hc al file

Sul sito di riferimento del software è presente anche un beginner's tutorial che riporta un esempio, step by step, della creazione di un file container (con alcune differenze rispetto agli elementi sopra indicati)

Dimensione massima del file: ***30 MB (no dynamic container)***

(in caso di assoluta necessità, per numero notevole di allegati, possono essere inviati più file container in email separate)

Note finali

L'indirizzo pec della Direzione è : ***navarm@postacert.difesa.it***

La funzione della busta con crittografia simmetrica è quella di separare temporalmente il momento della sua ricezione da parte del destinatario da quello della conoscibilità del relativo contenuto.

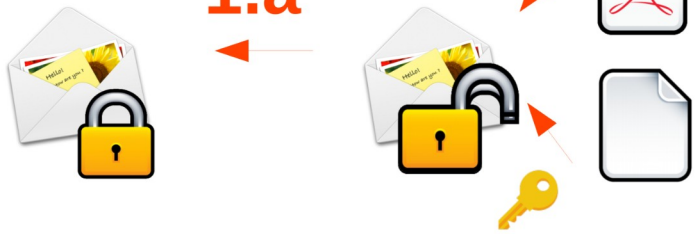
L'utilizzo dell'invio pec/rem – pec ha la finalità di assicurare le consegne della busta e della password (chiave crittografica) nei tempi stabiliti.

Alla firma elettronica e alla marca temporale dei file contenuti nella busta è invece demandata la caratteristica del non ripudio e datazione certa del documento.

Formazione e trasmissione di un plico di offerta

Creazione della **busta A** con chiave simmetrica specifica. La chiave sarà inviata, alla stazione appaltante, solo in un secondo momento.

1.a



3 file container crittografati
e
3 chiavi simmetriche

2

3

Chiusura ed invio plico offerta tramite **PEC** alla stazione appaltante

4

Creazione di un file container crittografato, con funzione di **plico di offerta**, ed inserimento dei 2 file container (buste)

La password (chiave simmetrica) usata per la creazione del file container (plico di offerta) sarà inviata alla stazione appaltante solo in un secondo momento

Creazione della **busta B** con chiave simmetrica specifica. La chiave sarà inviata, alla stazione appaltante, solo in un secondo momento.

1.b

Schema logico di trattazione di documenti informatici inviati alla Direzione tramite buste crittografate (leggibilità differita dei documenti)

Mittente

Creazione di un file container crittografato (busta) ed inserimento file

Chiusura del file container crittografato (busta)

Invio per pec del file container crittografato (busta)

La password (chiave simmetrica) usata per la creazione del file container (busta) viene mantenuta dal mittente e solo in un secondo momento spedita

Invio per pec della password

Destinatario