MANUALE ATTIVAZIONE SOFTWARE GPG4WIN

1. PREMESSA

L'art. 32 del GDPR impone alle aziende ed alle organizzazioni un innalzamento dei livelli di sicurezza al fine di una adeguata protezione dei dati personali e precisamente:

"1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto ***misure tecniche e organizzative adeguate*** *a garantire un livello di* ***sicurezza adeguato al rischio****, che comprendono, tra le altre, se del caso:*

a) *la pseudonimizzazione e* ***la cifratura dei dati personali****;*
b) *etc…"*

A tale proposito ricordiamo che ormai è assodato che il canale mail tradizionale non garantisce purtroppo un adeguato livello di protezione su nessuna delle seguenti direttrici che compongono la cifra di sicurezza di una informazione:

- Non sulla confidenzialità in quanto le mail tradizionali "viaggiano" in chiaro (plain text) per cui chiunque possegga uno "sniffer" della rete può leggerli
- Non sulla integrità in quanto qualcuno potrebbe anche intercettare la mail, sostituire il contenuto e inoltrarlo modificato (impersonando il mittente originale)
- Non sulla autenticità in quanto, come accennato al punto precedente, con un minimo di abilità è possibile impersonare soggetti diversi (ne sono testimonianza le mail di phishing che sono falsificate per far credere di essere inviate "con lo stesso account" del destinatario

Questo livello poi di adeguatezza è decisamente non solo carente ma insufficiente se la mail contiene:

- Dati personali particolari/sensibili/giudiziari
- Informazioni strettamente riservate (relative al business, alle scelte strategiche di una azienda, a progetti importanti e confidenziali etc…)

2. CONSEGUENZA

Al fine di potere usare ancora lo strumento mail diviene quindi indispensabile corredarlo di un "add-on" che permetta per le comunicazioni con i contenuti informativi "riservati" sopra descritti di aggiungere:

- Elementi certi di confidenzialità e riservatezza
- Elementi certi di autenticità del mittente

In pratica usare un add-on in grado di cifrare e firmare le mail.

Questo add-on fortunatamente esiste ed è gratuito.: si tratta di un plug-in chiamato GPG4WIN (per Outlook ma anche per Thunderbird e compatibile con simile strumento PGPMail di Mac, anche se a pagamento): GPG4WIN (https://www.gpg4win.org/).

Cosa è GPGP4WIN? Direttamente dal sito degli ideatori:

Gpg4win enables users to securely transport emails and files with the ***help of encryption and digital signatures. Encryption protects the contents against an unwanted party reading it. Digital signatures make sure that it was not modified and comes from a specific sender****.*

COMPET-E SRL - Via San Pietro, 26/A 12030 Cavallermaggiore (CN)
Tel: 0172-382763 Fax: 0172-1832072 www.compet-e.it - info@compet-e.it

UNI/PdR 43:2018 — UNI CEI EN ISO/IEC 27001:2017 ISO/IEC 27017:2015 e ISO/IEC 27018:2019

Gpg4win supports both relevant cryptography standards, ***OpenPGP and S/MIME (X.509),*** *and is the official GnuPG distribution for Windows. It is maintained by the developers of GnuPG. Gpg4win and the software included with Gpg4win* ***are Free Software*** *(Open Source; among other things free of charge for all commercial and non-commercial purposes).*

Creation of Gpg4win was supported by the German Federal Office for Information Security (BSI).

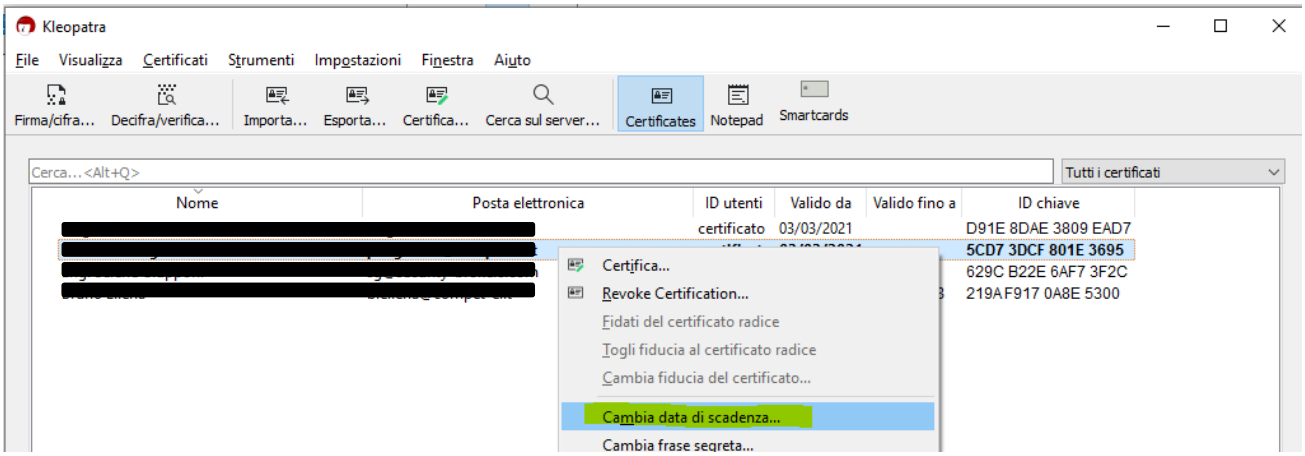
Tale sistema quindi presenta una serie di vantaggi:

- Compatibilità con diversi client di posta (Outlook, Thunderbird, etc..)
- Non vincolo esclusivo di adozione di tecnologia proprietaria (Microsoft)

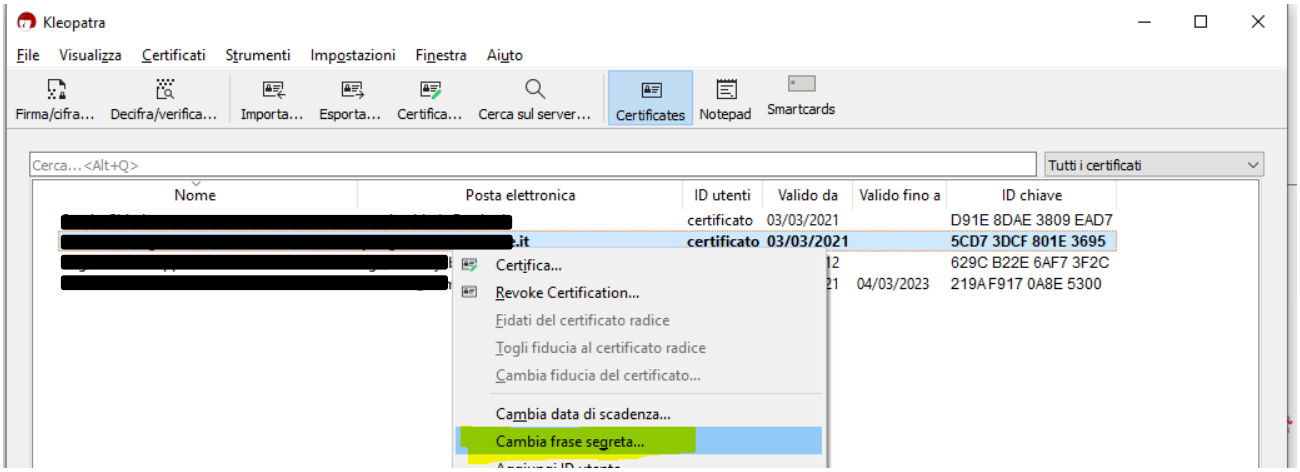
3. CONCLUSIONI

L'installazione del plug-in avviene secondo i seguenti passi:

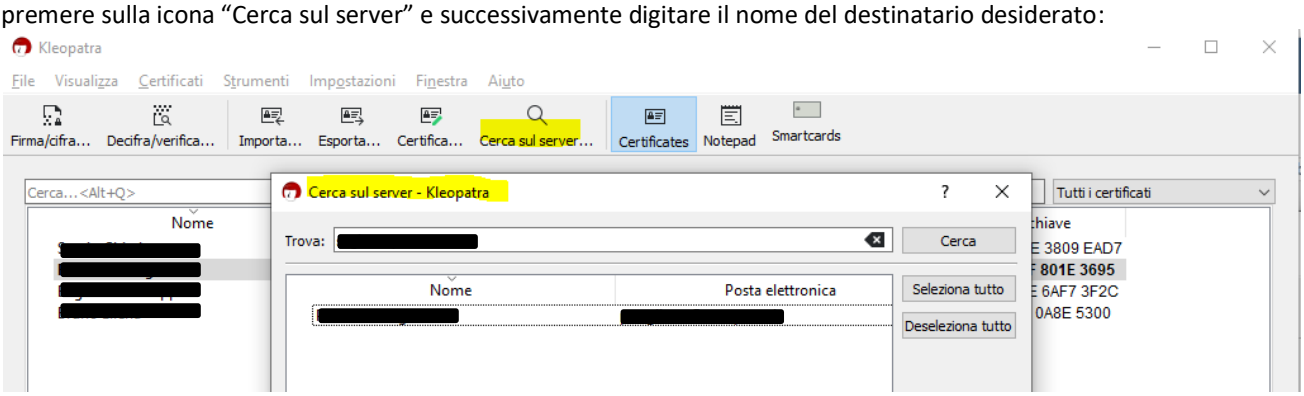
- Scaricare il software da installare dal seguente sito https://www.gpg4win.org/get-gpg4win.html
- Chiudere Outlook o il client di posta prima di lanciare l'installazione
- Lanciare l'installazione con diritti di amministratore
- Appena installato deve essere lanciato il software installato (si chiama Kleopatra) e deve essere generata la coppia chiave pubblica e privata. La generazione deve avvenire non impostando una data di scadenza:



Dal menu soprastante, al passo successivo, scegliere come data scadenza: MAI. Si suggerisce di proteggere ancora le chiavi con una pass-key lunga almeno 10 caratteri:

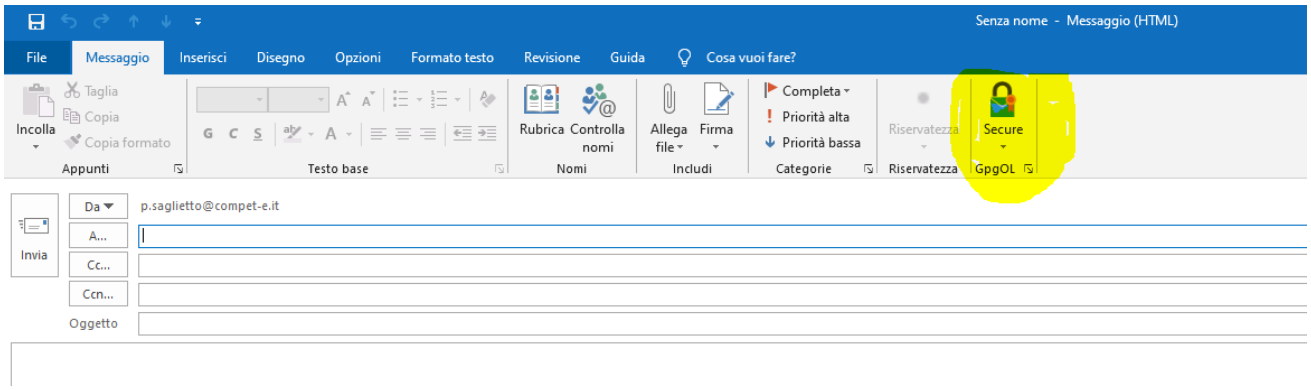


- Le chiavi (privata e pubblica) poi devono essere salvate in un luogo sicuro e fatto un backup in luogo sicuro
- A questo punto importare la chiave pubblica del destinatario/destinatari con cui si vuole colloquiare. Per fare questo premere sulla icona “Cerca sul server” e successivamente digitare il nome del destinatario desiderato:

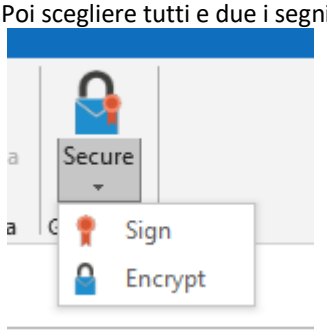


Selezionare la riga della persona ricercata e premere Importa (a questo punto il certificato pubblico del destinatario è importato e si potrà cominciare a scambiare mail in modo sicuro con lui come più sotto indicato).

- Quando fatto, fare un test di invio e ricezione di mail in modalità criptata e firmata. Per fare questo (ad esempio su Outlook) premere l’usuale tasto di nuova mail e premere sulla nuova icona a destra evidenziata nell’immagine sottostante:



Poi scegliere tutti e due i segni di spunta sotto per cifrare e firmare la mail.



Scrivere la mail, allegare i file necessari ed inviare come di solito (se viene chiesta la password immettere quella scelta in precedenza).