MANUALE ATTIVAZIONE SOFTWARE FLOWCRYPT

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 add on alla web mail di Gmail chiamato FlowCrypt

Cosa è FlowCrypt? Direttamente dal sito degli ideatori:

è un add on che si installa sul browser Chrome (ma qui https://flowcrypt.com/download vi sono gli add on anche per installarlo su altri browser quali Firefox) che permette di scambiare mail cifrate firmate digitalmente con interlocutori dotati di medesimi strumenti (basati su tecnologia OpenPGP).

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

Per gli utilizzi con feature base (ma già adatti nel l90% dei casi) è un add-on gratuito. Queste sono le differenze tra la versione free e quella a pagamento:

FlowCrypt Pricing

FlowCrypt Free Forever will always stay feature rich. See for yourself:

WHAT CAN YOU DO	FREE FOREVER	ADVANCED
Send encrypted messages to any recipient	✓	✓
Send encrypted attachments to any recipient	✓	✓
Get messages + files through encrypted contact page	✓	✓
Choose when password encrypted messages expire		✓
Recipients can securely reply without any plugin		✓
Add attachments larger than 5MB (up to 25MB)		✓
Use a custom email footer		✓
If you decide to renew after free trial	**free**	**$5 monthly**

Tale sistema, quindi, presenta una serie di vantaggi:

- Compatibilità con diversi piattaforme/browser
- Non vincolo esclusivo di adozione di tecnologia proprietaria

Di seguito alcune note su altri sistemi che svolgono le medesime funzionalità che possono essere usati come alternative:

Platform	Email provider	Software	Cost	Setup, Use	Our notes
Apple Mail	Any	GPG Suite	Paid (low)	medium, easy	Inexpensive, well s ported and feature- MacOS only.
Outlook App	Any	gpg4o	Paid (medium)	medium, medium	Excellent support i experience Pro-active approac ensure compatibilit
Web Android, iOS	ProtonMail	ProtonMail	Free + paid	easy, easy	Good if you want tc change your email vider. OpenPGP support ited but improving. by many.
Thunderbird	Any	Enigmail	Free OSS	hard, medium	Mature and battle t software Your IT staff should with setup and sup
Outlook Web Yahoo Web	Outlook, Yahoo, ...	Mailvelope	Free OSS	medium, medium	Battle tested. Diffic with attachments, s incompatibility. Free, well maintain and works with mai email providers.

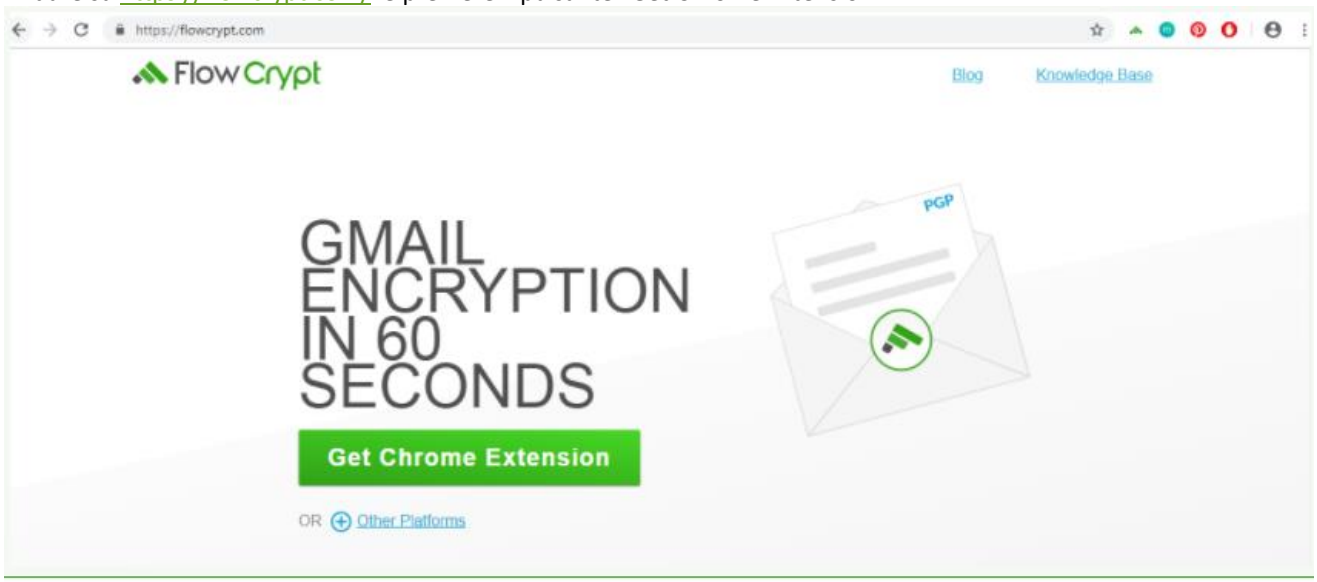
Inoltre, sulla pagina https://flowcrypt.com/docs/technical/other-platforms.html sono presenti eventuali aggiornamenti di compatibilità e di prodotti similari che il mercato o gli sviluppatori open source rilasciano sul tema.

Un'altra pagina molto completa che fornisce tutti i prodotti (free e a pagamento) disponibili sulle varie piattaforme (IOS, Android, linux, etc..) compatibili con sistema di cifratura openPGP è la seguente: https://www.openpgp.org/software/

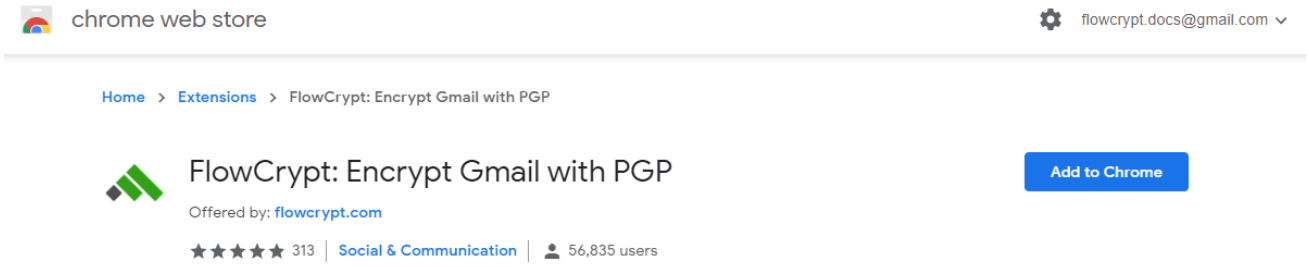
3. CONCLUSIONI

L'installazione di tale add-on avviene secondo i seguenti passi:

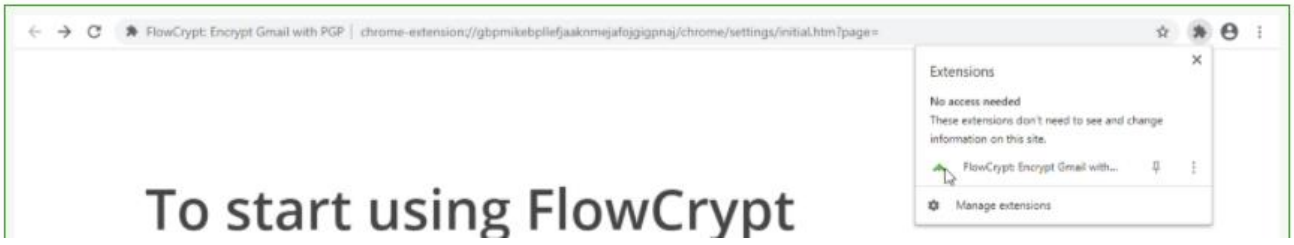
- Andare su https://flowcrypt.com/ e premere il pulsante "Get Chrome Extension"



Si verrà ridirezionati alla seguente pagina:

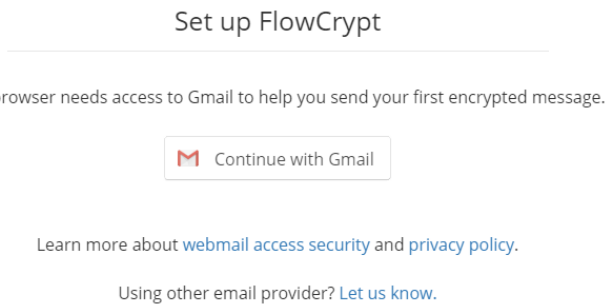


- Premere il pulsante Add to Chrome per avviare l'installazione
- A questo punto l'estensione si troverà installata in Chrome negli appositi spazi dedicati alle estensioni:

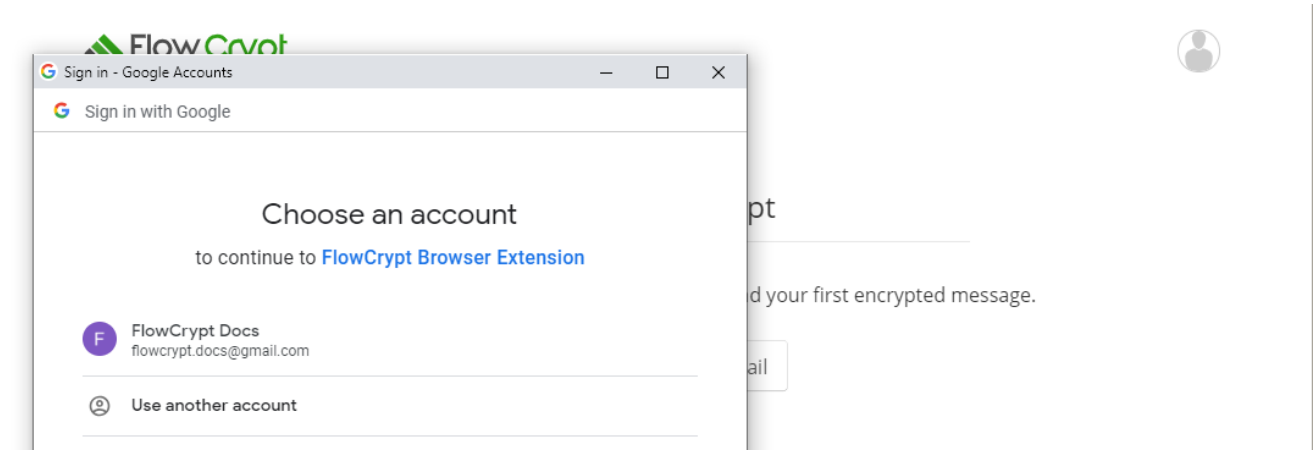


- Se si vuole che l'estensione sia sempre visibile occorre fissare l'opzione selezionata in giallo nell'elenco delle estensioni di Chrome.

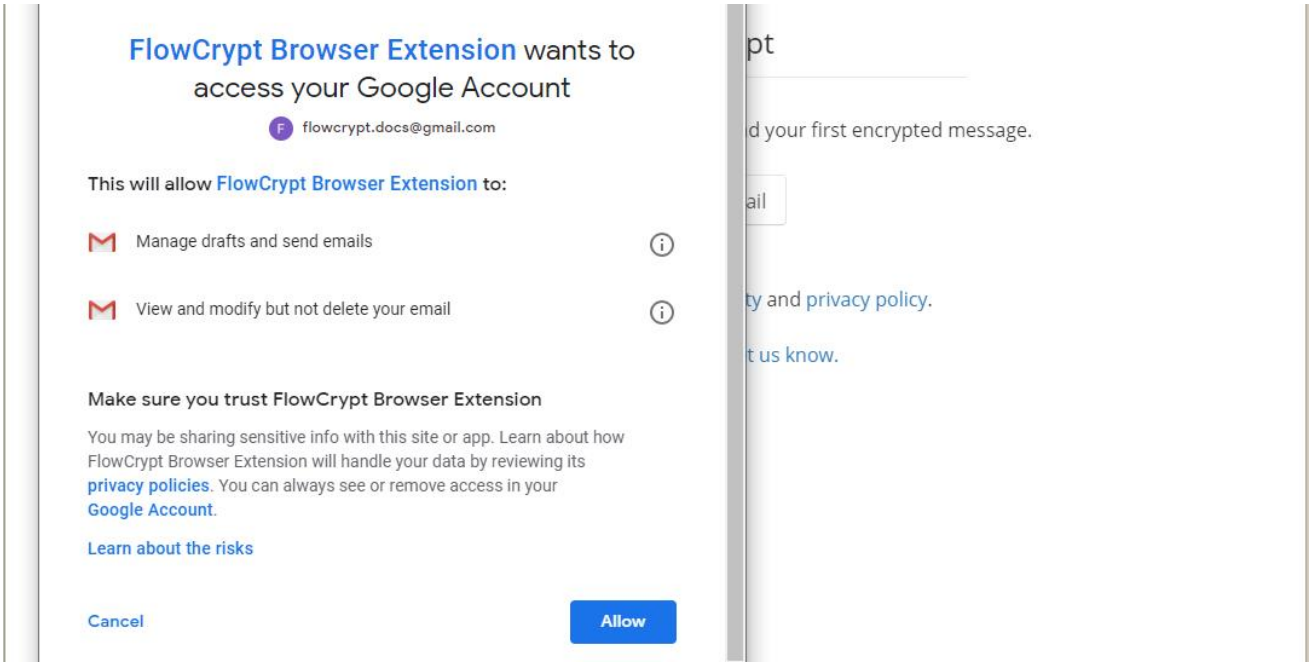
- Dopo l'installazione se l'estensione è attivata comparirà la seguente videata:



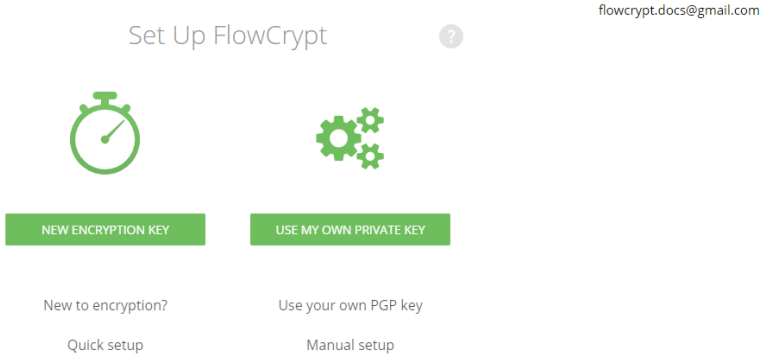
- Premendo su "Continue con Gmail" il sistema chiederà di selezionare un account di Gmail a cui associare l'add-on di cifratura:



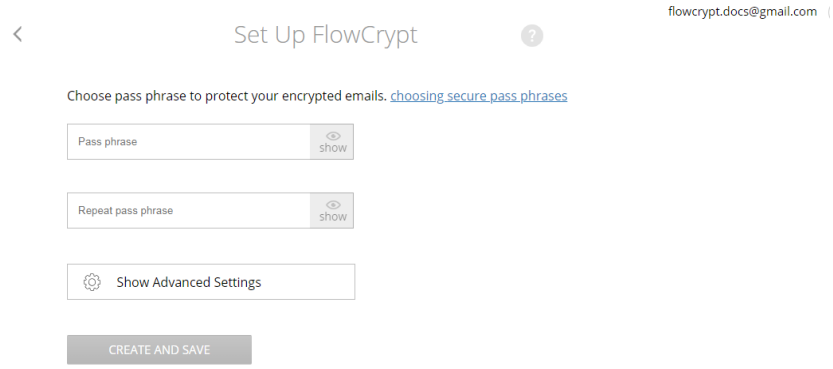
- Premendo su "Continue con Gmail" il sistema chiederà di selezionare un account di Gmail a cui associare la cifratura:



- A questo punto l'estensione è attiva sull'account Gmail e la cosa da fare (una tantum) è la generazione della coppia di chiavi (privata e pubblica) "Premendo New Encryption Key".

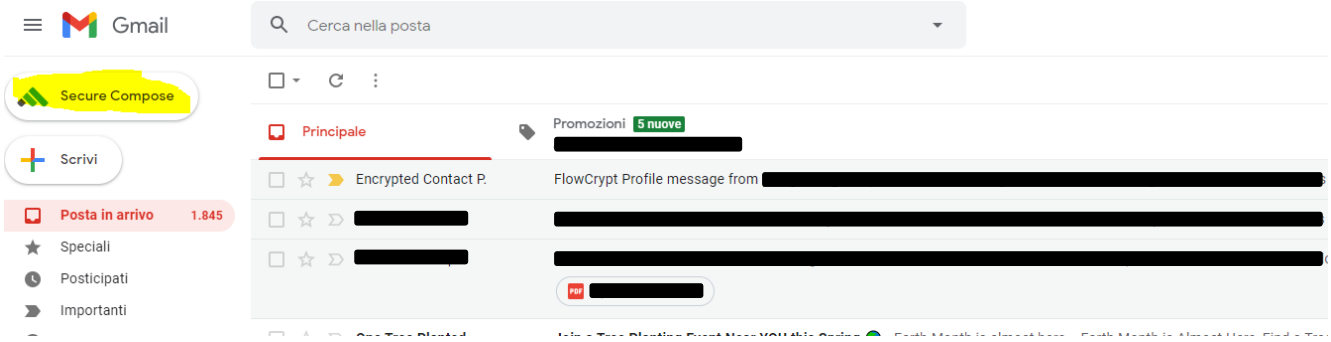


- I parametri richiesti per generare la chiave sono i seguenti:



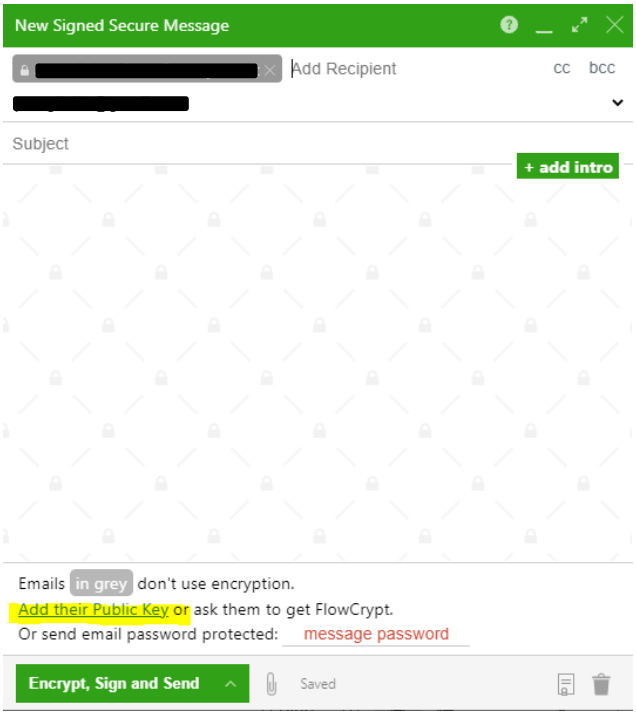
  - ✓ Dove la pass phrase è la parola segreta che si consiglia di essere almeno 10 caratteri.
  - ✓ Verrà visualizzata la chiave generata che si consiglia di salvare in un luogo sicuro. La chiave pubblica deve poi essere inviata ai propri interlocutori (anche solo via mail, tanto è la parte pubblica che quindi non ha vincoli di segretezza).

- A questo punto è possibile cominciare a scambiare mail cifrate con gli interlocutori. Per fare questo premere il pulsante sotto evidenziato "Secure Compose":



- Dopo la pressione del pulsante di cui sopra verrà aperta la finestra —per scrivere le mail cifrate (molto simile alle usuali finestre di composizione mail)

- Digitando nel campo Add Recipient (campo TO) la mail del destinatario se di questo non è stata ancora importata la chiave pubblica ci sarà un messaggio che avvisa che deve essere fatto questo passaggio



- Cliccando Add Their Public key si potrà importare la chiave che l'utente con cui si vuole scambiare mail deve avere mandato come file o come stringa: