# OpenPGP e Crittografia

Linux Day 2025 – Francesco Valentini

# LICENZA

# ~$ whoami

Sono uno studente di informatica, appassionato di cybersecurity, reti informatiche e telecomunicazioni.

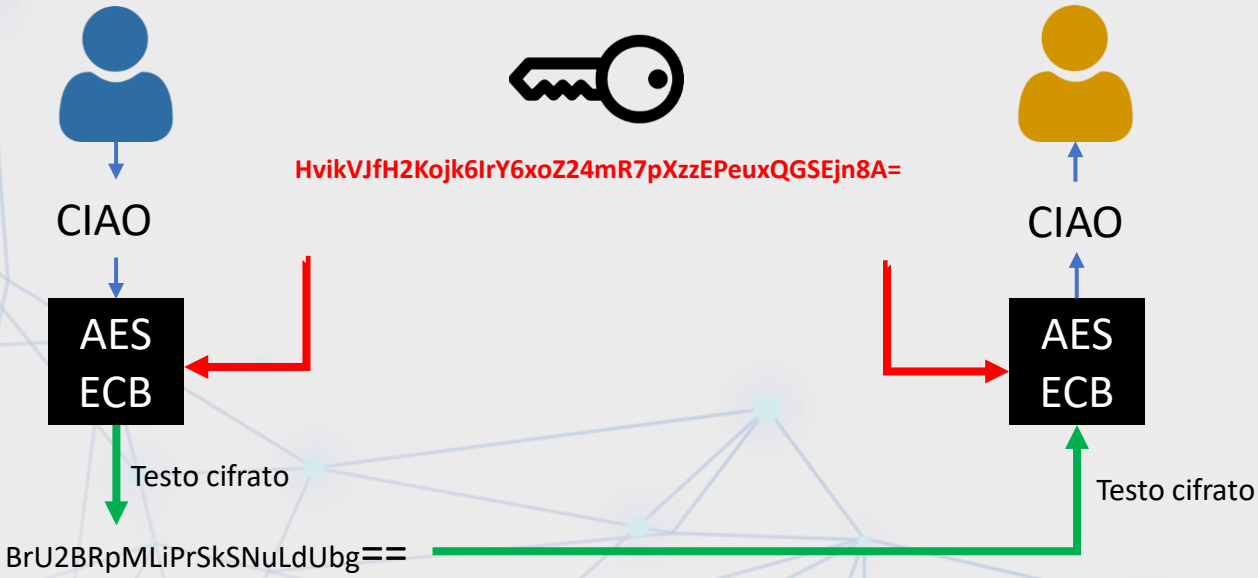
**Formazione:**

- **Diploma di perito informatico**
  **(I. I. S. "Enrico Mattei" di Recanati – 100/100)**
- **Bronzo alle Olimpiadi Nazionali della CyberSecurity (2021)**
- **Corso di laurea L-31 Informatica (Università di Camerino)**

**https://francescovalentini.github.io**

# CRITTOGRAFIA SIMMETRICA

- Tutti hanno la stessa chiave (segreto condiviso).
- La stessa chiave viene utilizzata sia per cifrare che per decifrare.
- La chiave deve essere protetta e scambiata tramite canali sicuri (o trasferita a mano).



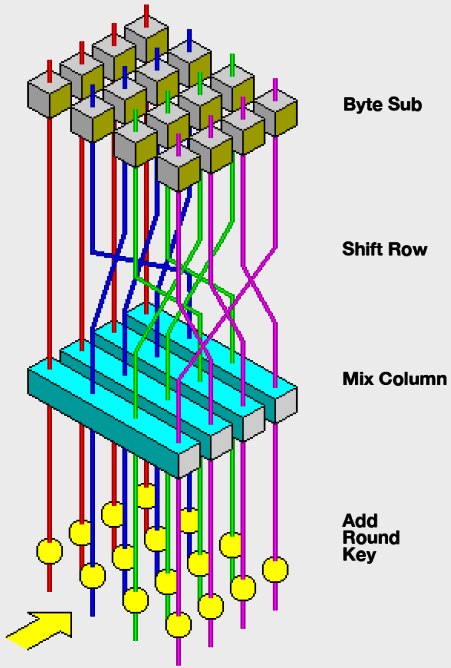
# AES

**AES (Advanced Encryption Standard)** è un algoritmo di cifratura a chiave simmetrica standardizzato dal NIST nel 2001, ad oggi **è tra gli algoritmi più sicuri che esistano!**

**Dimensioni delle chiavi:** 128 bit, 192 bit, 256 bit

**Standardizzazione:**

- È stato standardizzato dal NIST (FIPS-197)
- È **approvato dalla NSA per la protezione di materiale classificato negli USA**.

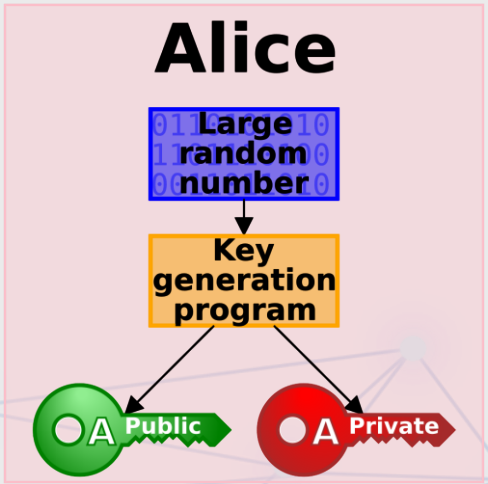



By John Savard - https://www.eng.tau.ac.il/~yash/crypto-netsec/rijndael.htm, CC0, https://commons.wikimedia.org/w/index.php?curid=103718081

# CRITTOGRAFIA ASIMMETRICA

Ogni utente ha una coppia di chiavi:

- **Chiave privata:** Deve essere mantenuta **STRETTAMENTE SEGRETA**
- **Chiave pubblica:** Deriva dalla privata e può essere condivisa con chiunque

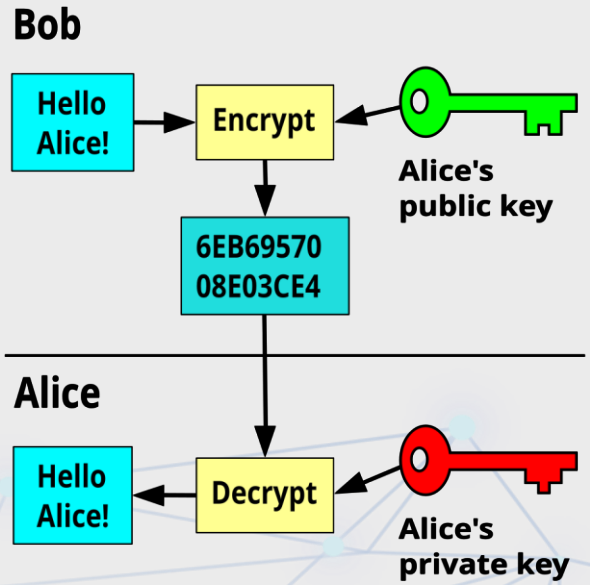



By KohanX (talk) - Own work (Original text: I (KohanX (talk)) created this work entirely by myself.), Public Domain, https://commons.wikimedia.org/w/index.php?curid=24325809

# CRITTOGRAFIA ASIMMETRICA

**Cifratura:**

- ciò che viene **cifrato con la chiave pubblica** può essere **decifrato solo dalla rispettiva chiave privata**.

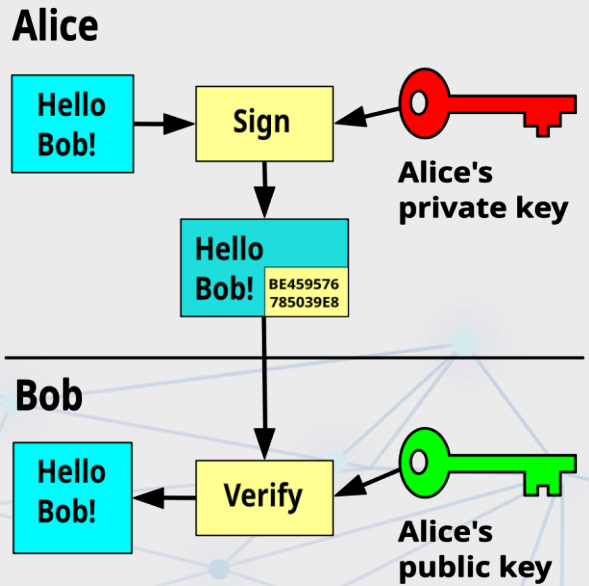



By Davidgothberg - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=1028460

# CRITTOGRAFIA ASIMMETRICA

**Firma digitale:** Il processo può essere usato al contrario ottenendo la Firma Digitale

- **Cifra con chiave privata:** Si cifra l'hash del messaggio con la propria chiave privata e si ottiene un "risultato unico"
- **Verifica con chiave pubblica:** Chi verifica la firma con la chiave pubblica ha la certezza matematica che il messaggio è stato generato dalla rispettiva chiave privata.




By FlippyFlink - Combined changed the image https://en.wikipedia.org/wiki/File:Public_key_encryption.svg from encryption to signing., CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=78867393

# RSA & ECC

RSA (Rivest–Shamir–Adleman): è il più "vecchio" sistema ancora in uso per la crittografia asimmetrica

- Sviluppato da Ron **Rivest**, Adi **Shamir**, Leonard **Adleman** nel 1977 per conto del **GCHQ**
- **Declassificato nel 1997**

Supporta diverse dimensioni di chiave, le più comuni sono:

- 2048 bit
- 3072 bit
- 4096 bit

I sistemi ECC (Elliptic-curve cryptography)

- **Approccio** più moderno alla crittografia asimmetrica
- Consente di avere chiavi più corte con sicurezza equivalente ad RSA

**Alcune curve ECC standard:**

- **NIST P-256 (256 bit)**
- NIST P-384 (384 bit)
- NIST P-512 (512 bit)
- **Curve25519 (256 bit)**

# SHA-2

Le SHA-2 sono una famiglia di funzioni di **HASHING**:

- **Sviluppate nel 2001 dalla NSA, sono ad oggi considerate le più sicure**
- **Standardizzate dal NIST** (FIPS 180-4 Secure Hash Standard )
- Garantiscono **SOLO** l'integrità di un messaggio

SHA-256("CIAO"):

- 6613DDD54D6DB890EC06519714257DD4C2ABE8080229C86C900B57FA7552A8EC

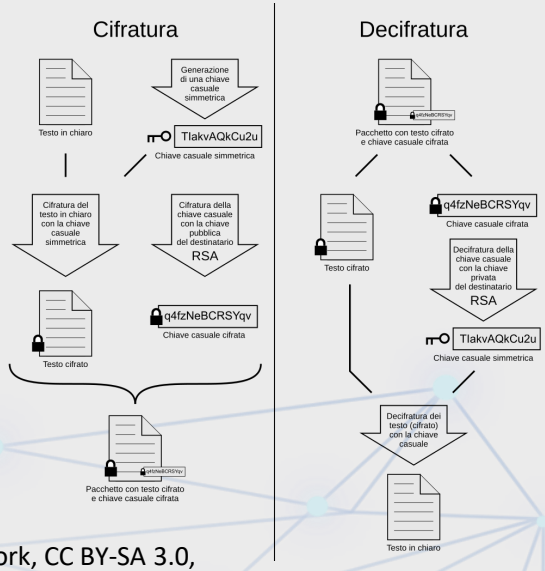
SHA-256("CIAA"):

- 13F3EE5BFFC6CC8F6C9003B0CD9D71E680E4883075FB36F692407AE53A8B8841

# PGP - Pretty Good Privacy

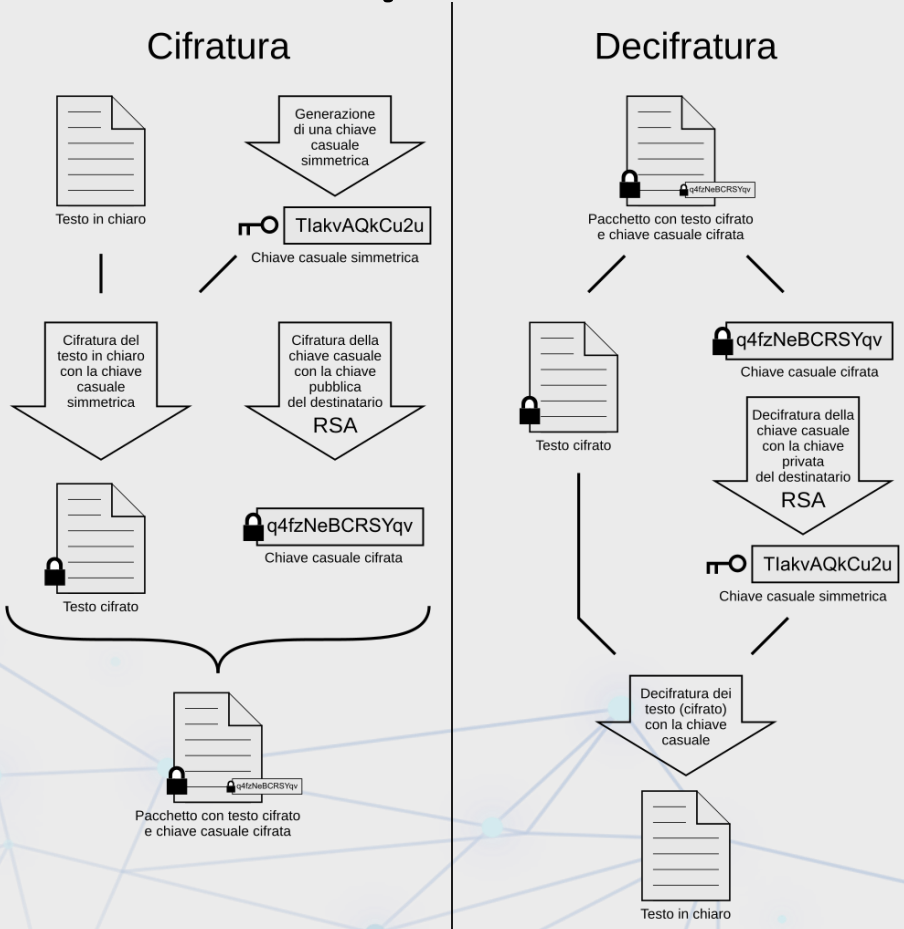
Sviluppato da Phil Zimmermann nel 1991 come software di crittografia per email e file, **utilizza un modello ibrido**: **crittografia simmetrica per i dati + asimmetrica per la chiave.**

Tra il 1997 e il 2007 Zimmermann lavora con la IETF per lo sviluppo di uno standard aperto "OpenPGP" (RFC 4880)




By Aldolat - Own work, CC BY-SA 3.0,
https://commons.wikimedia.org/w/index.php?curid=149423774

# PGP - Pretty Good Privacy



# Problema della fiducia

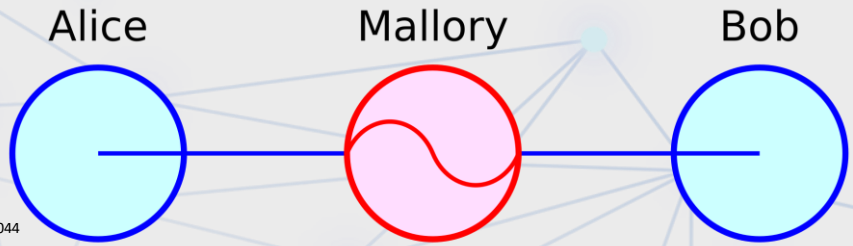
**È necessario fidarsi della chiave pubblica** per evitare attacchi Man-in-the-Middle (MiTM).

**Attacco MiTM:**

- Alice e Bob vogliono comunicare, ma Eve intercetta le comunicazioni e impersona entrambi.
- Alice e Bob pensano di cifrare l'uno per l'altro mentre in realtà cifrano per Eve
- Eve può decifrare e leggere i messaggi, poi cifrarli di nuovo per l'altro.

**Una possibile soluzione:**

- Utilizzare un ente certificatore centralizzato che verifica l'identità di Alice e Bob.
- Questo ente firma le loro chiavi pubbliche, assicurando che appartengano davvero a loro.



# Web Of Trust

È un approccio alternativo a quello dell'ente certificatore centralizzato, è supportato da tutte le implementazioni conformi ad OpenPGP.

**Certificato PGP:**

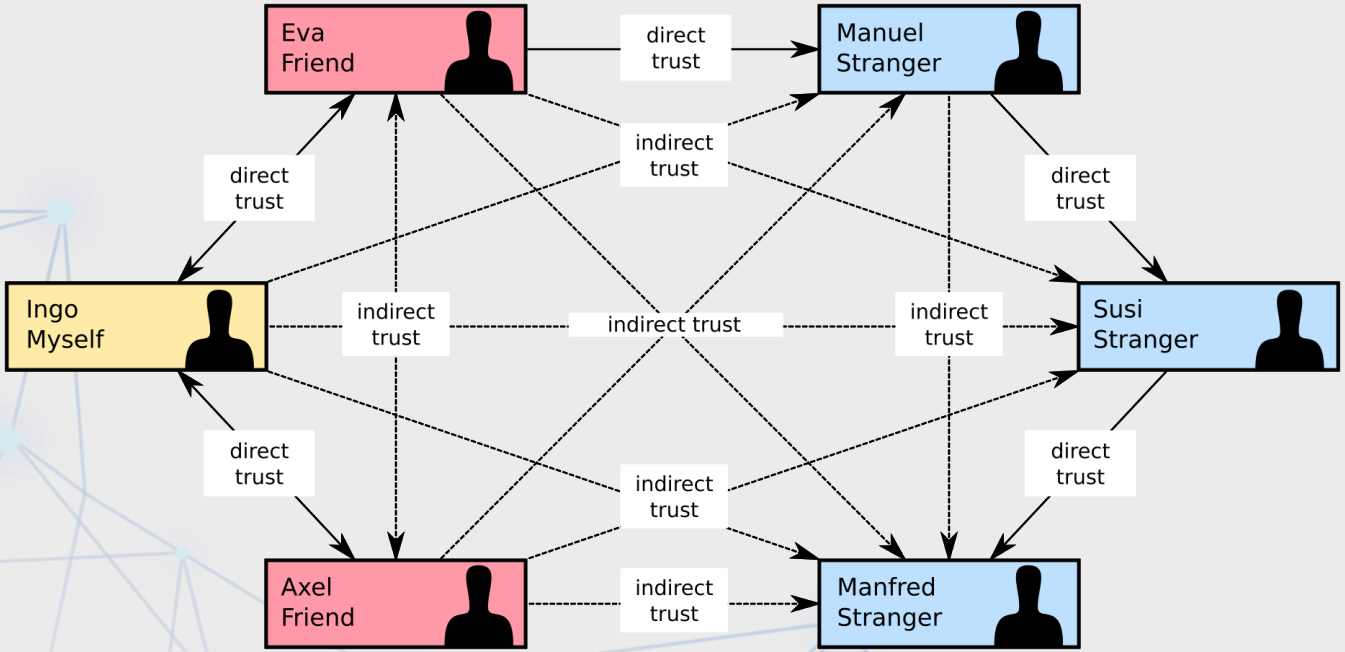
- Include la chiave pubblica e informazioni sul proprietario (nome, email, commento, data di scadenza, ecc.).
- Può essere firmato da altri utenti che attestano l'associazione tra chiave pubblica e persona fisica

**Key Signing Party**:

- riunioni fisiche dove i partecipanti possono firmare le chiavi altrui

Esistono anche le Trust Signatures che consentono a OpenPGP di operare in modo simile alle Certification Authority

# Web Of Trust




By Kku - Own work, CC BY-SA 4.0,
https://commons.wikimedia.org/w/index.php?curid=80652637

# PGP o GPG

PGP è un prodotto commerciale:

- Nel 2010, la PGP Corporation viene acquisita da Symantec.
- Nel 2019, Broadcom acquisisce la divisione Symantec Enterprise Security, che include anche PGP.

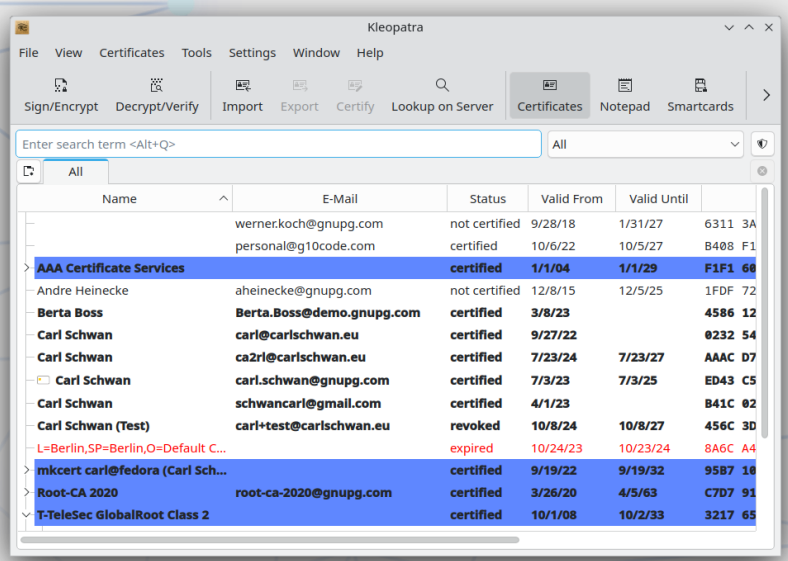
GPG (GNU Privacy Guard) è un'implementazione conforme allo standard **OpenPGP**:

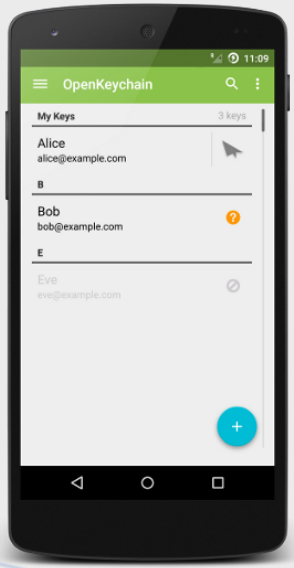
- Creato nel 1997, è ad oggi l'implementazione più completa dello standard disponibile.
- Supporta molteplici sistemi operativi ed è spesso pre-installato.
- GPG è fondamentale nei sistemi che utilizzano APT come gestore dei pacchetti per il corretto funzionamento di "secure apt" (or "apt-secure").

# Software

GnuPG è il software principale spesso già installato, a questo possono aggiungersi altri strumenti che semplificano l'uso:

- **Kleopatra**
- **OpenKeyChain**



# PGP – Non solo software

Le operazioni crittografiche, la generazione e l'archiviazione delle chiavi possono essere delegate a dispositivi hardware come Smart Card, HSM, …


**Smart card comune**

Di Werner Koch - Opera propria, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=36808159


**Lettore di smart-card formato SIM**

Di Ale2006 - Opera propria, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=75206857

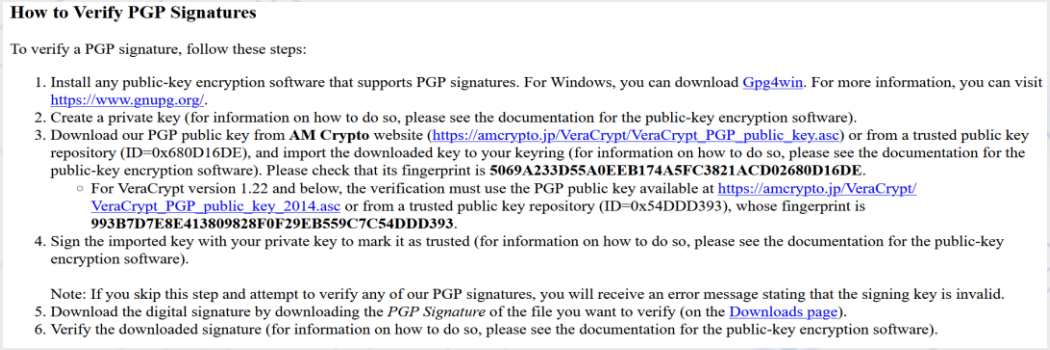
**Progetti interessanti: NitroKey, YubiKey**

# PGP – Casi d'uso

**Firma digitale:**

- Una software-house vuole distribuire il suo software e permettere all'utente finale di verificare autonomamente e offline l'integrità dell'installer scaricato.
- L'azienda **distribuisce il software con le chiavi pubbliche** per la verifica **e i file di firma**.
- Il cliente può verificare la validità del file prima di eseguire l'installer.


Eseguibili + firma




Istruzioni di verifica

# PGP – Casi d’uso

**Cifratura:** Un ente pubblico deve condividere dati riservati via email.

- Con PGP, è possibile cifrare il contenuto solo per i diretti interessati, la cui chiave pubblica è presente nel keystore (archivio delle chiavi fidate).
- In caso di errore nell'invio a un indirizzo non autorizzato, il contenuto resta illeggibile, proteggendo così il dato e l'ente pubblico da possibili sanzioni per data breach.

**Soluzioni:**

- Già integrato nei client mail (Thunderbird)
- Disponibile come estensione (GpgOL per Microsoft Outlook)
- Per webmail esistono estensioni browser come Mailvelope (https://mailvelope.com)

# PGP – Casi d'uso

**Quando NON utilizzare PGP (o certificati X.509 auto firmati)**

- **Per documenti che richiedono FEA o FEQ nei contesti di pubblica amministrazione**
  - Firme o file cifrati con PGP potrebbero non essere nemmeno validabili (oltre che prive di valore legale)
  - Firme CMS con certificati x.509 auto firmati daranno sicuramente errori nei software di validazione

**Quando UTILIZZARE PGP (o certificati X.509 auto firmati)**

- Documenti per cui non sono necessarie le garanzie legali di FEA e FEQ (documenti informali, personali, interni)
- Quando è necessario proteggere informazioni particolarmente sensibili in modo rapido semplice e affidabile

# Chiavi pubbliche e private

**Chiave privata: inizia sempre con**

-----BEGIN PGP PRIVATE KEY BLOCK-----

**LA CHIAVE PRIVATA DEVE RESTARE SEGRETA!**

**Chiave pubblica: inizia sempre con**

-----BEGIN PGP PUBLIC KEY BLOCK-----

**LA CHIAVE PUBBLICA PUÒ ESSERE CONDIVISA CON CHIUNQUE**