Verschlüsselung - PGP vs. S/MIME

Ralf Becker
Geschäftsführer, EGroupware GmbH

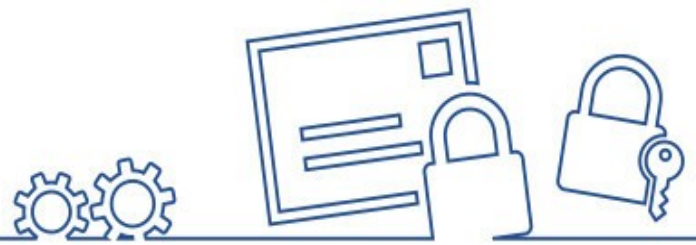
Hadi Nategh
Softwareentwickler, EGroupware GmbH

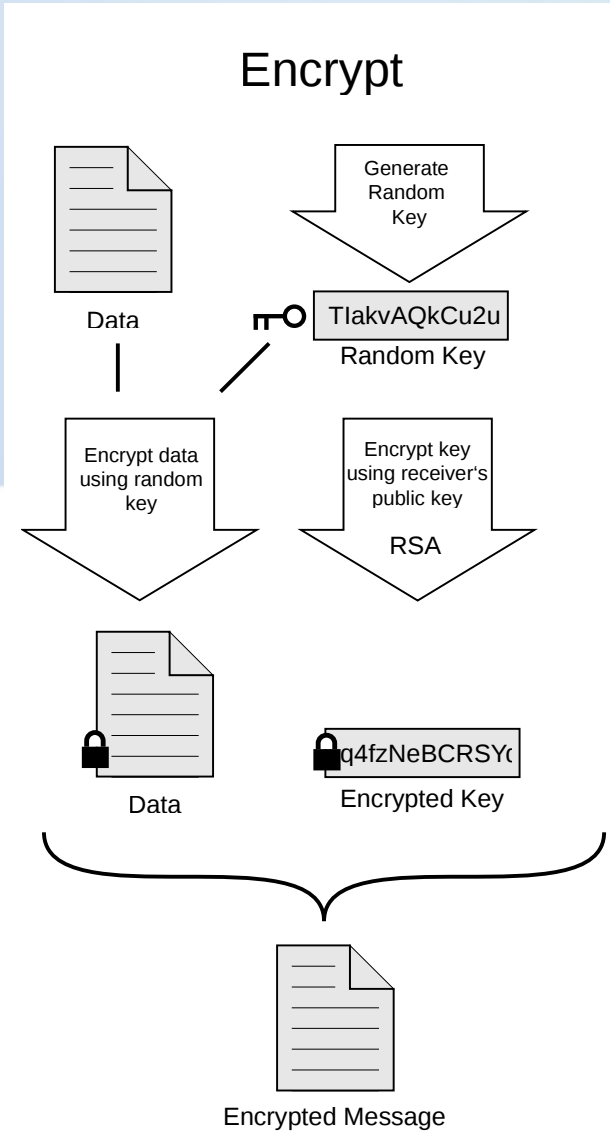
PGP

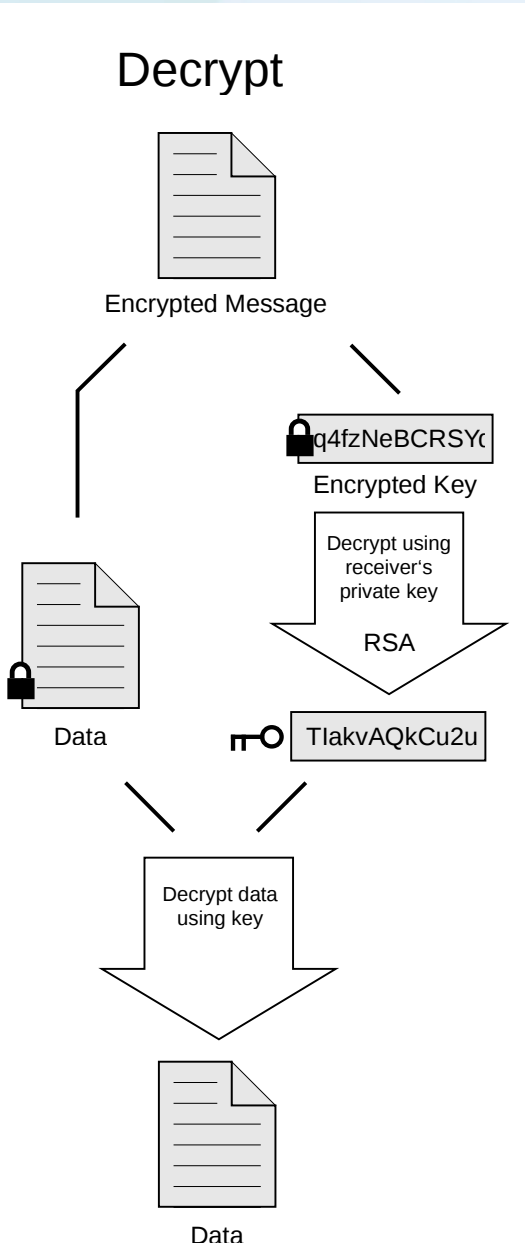
PGP (Pretty Good Privacy) is an encryption protocol which provides cryptographic privacy and authentication. PGP can sign, encrypt and decrypt data.

PGP's Features:

- Confidentiality (Encryption)
- Digital signatures (Authentication)







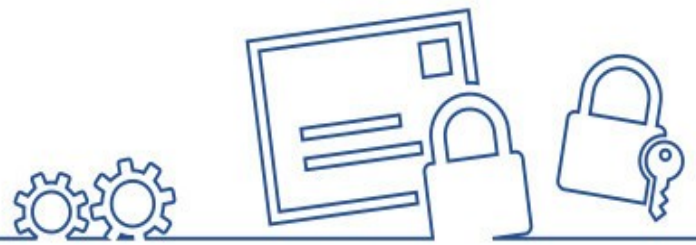
https://en.wikipedia.org/wiki/Pretty_Good_Privacy

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol for sending signed and encrypted messages. S/MIME helps to digitally sign and encrypt a message and make sure the received message is originated from the sender.

Basically, S/MIME provides two main services:

- Digital signature
- Message encryption



S/MIME

- **Digital signatures**

  Digital signatures are equivalent digital version of traditional signature on paper document.

  Digital signatures provide three security features:

  - Authentication: To validate an identity

  - Non-repudiation: The uniqueness of a signature

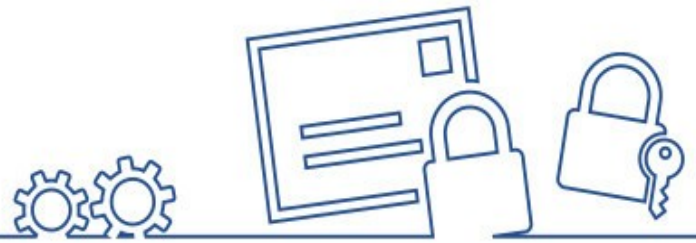
  - Data integrity: To make sure received data has not been tempered

S/MIME

- **Message Encryption**

  S/MIME encryption provides two features:

  - Confidentiality
  - Data integrity



S/MIME

- Digital signatures:

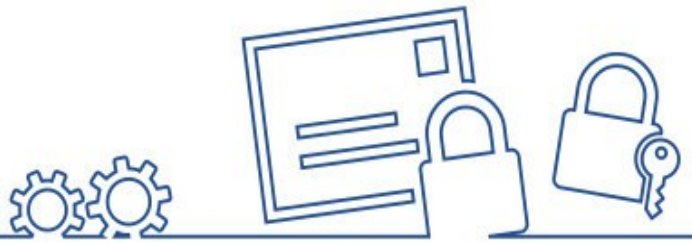
  Digital signatures are equivalent digital version of traditional signature on paper document.

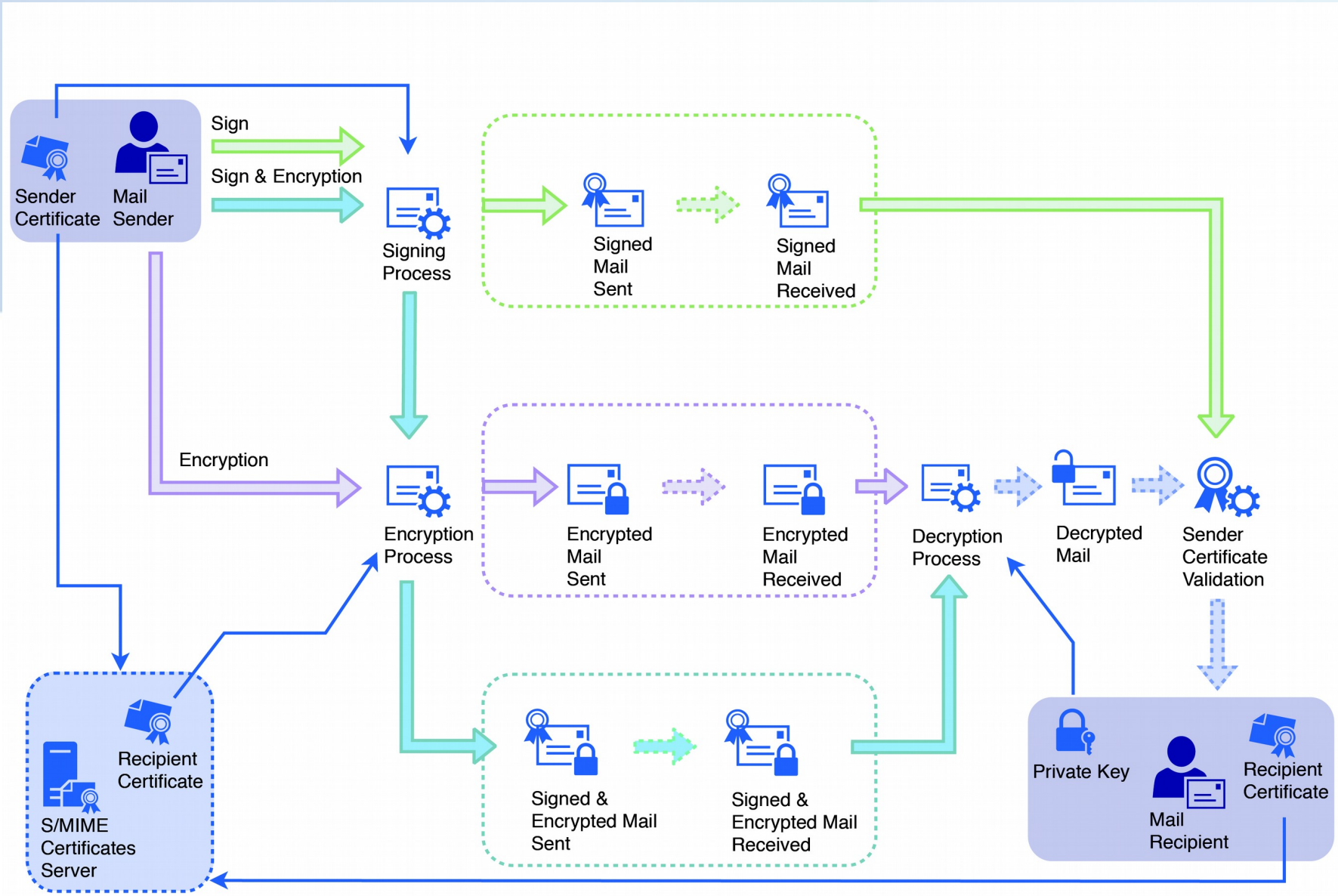
  Digital signatures provide three security features:

  - Authentication: To validate an identity

  - Non-repudiation: The uniqueness of a signature

  - Data integrity: To make sure received data has not been tempered




Sender Certificate
Mail Sender
Sign
Sign & Encryption
Signing Process
Signed Mail Sent
Signed Mail Received
Encryption
Encryption Process
Encrypted Mail Sent
Encrypted Mail Received
Decryption Process
Decrypted Mail
Sender Certificate Validation
Recipient Certificate
S/MIME Certificates Server
Signed & Encrypted Mail Sent
Signed & Encrypted Mail Received
Private Key
Mail Recipient
Recipient Certificate

PGP vs S/MIME

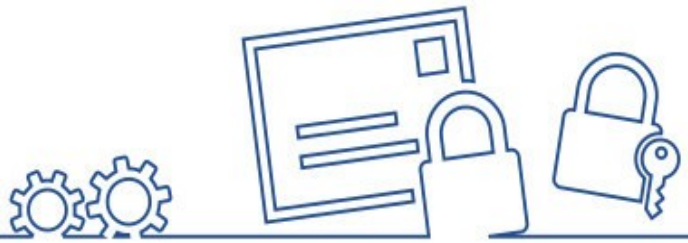
Similar features – what are the differences?

PGP

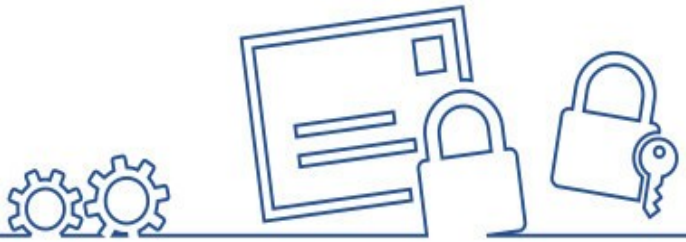
+ Private key stays in browser
+ More secure solution
- Key exchange & validation
- Browser plugin (Mailvelope) needed
- Client support specially mobile

S/MIME

+ Wide client support
+ Ease of use & deployment
+ Key exchange & validation via CA
- Security of CA infrastructure
- Security relies trust in server



THANK YOU!



Verschlüsselung - PGP vs. S/MIME

Bei Fragen sprechen Sie uns gerne an!

If you have any questions, please feel free to contact us!

Ihr EGroupware Team

info@egroupware.org

0631 31657-0