



E-Mail, e-mail, email, eMail, ...

- alt, kaputt, aber trotzdem geil -

Marcel Schmidt, 07.11.2019



Agenda

- Was ist das?
- Wie fing es an?
- Warum immer noch?
- Was läuft schief?
- Wie retten wir die Mail?
- Verschlüsselung mit PGP
- Digitale Signatur
- Wie?



„Mail“ by [Alexander Hauser](#) is licensed under CC-BY-NC-ND 2.0



Was ist das?

- Asynchrones Kommunikationsmedium
- Neben dem WWW immer noch einer der wichtigsten Dienste im Internet

	2015	2016	2017	2018	2019
Worldwide Email Accounts (M)	4,353	4,626	4,920	5,243	5,594
<i>%Growth</i>		6%	6%	7%	7%
Worldwide Email Users* (M)	2,586	2,672	2,760	2,849	2,943
<i>% Growth</i>		3%	3%	3%	3%
Average Accounts Per User	1.7	1.7	1.8	1.8	1.9

Table 1: Worldwide Email Accounts and User Forecast (M), 2015–2019



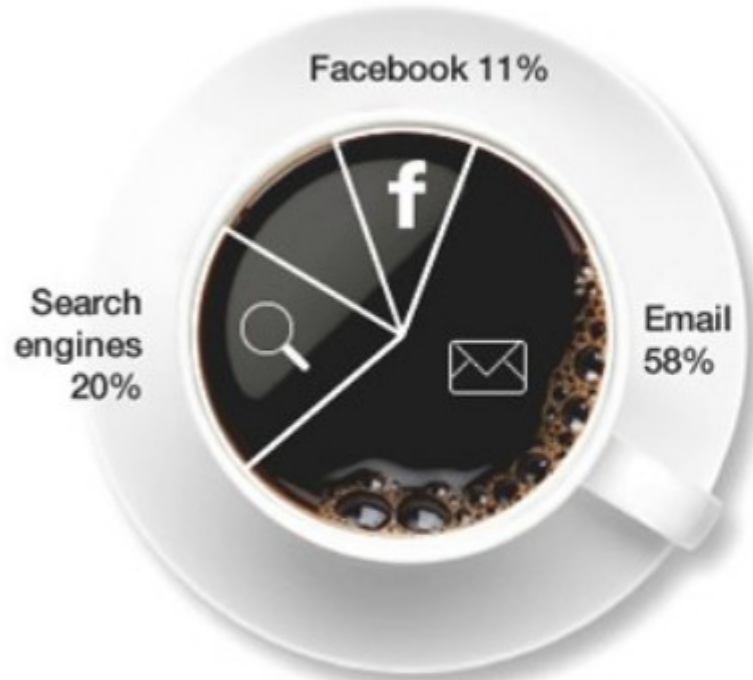
Wie fing es an?

- Mail-Befehl wurde 1964/65 von Glenda Schroeder, Louis Pouzin und Pat Crisman als Erweiterung für Multics vorgeschlagen
- 1971: erste E-Mail (@) durch Ray Tomlinson
und Diskussion eines Protokolls in RFC 196
- 1973: RFC 561 (vorgeschlagener Name XMAIL)
- 1977: RFC 733
- 1982: RFC 822 | 2001: RFC 2822 | 2008: RFC 5322



Warum immer noch?

...oder warum wir nicht davon los kommen.





Warum immer noch?

...oder warum wir nicht davon los kommen.

- Höchster Verbreitungsgrad unter den persönlichen elektronischen Kommunikationsdiensten
- Sowohl im privaten als auch geschäftlichen Bereich akzeptiert
- Authentifikation für viele weitere Dienste/Plattformen erfordern häufig eine Email-Adresse
- Erweiterbar
 - Neben plain Text auch html möglich
 - Anhänge mit beliebigen Dateien
- Geräte/Betriebssystem unabhängig
 - Computer
 - Smartphones
 - Alarmanlagen/Türschlösser
 - Geräte der Netzwerkinfrastruktur wie Router und Switches
 - Glühlampen
 - Sextoys



Warum immer noch?

...oder warum wir nicht davon los kommen.
und warum wir das auch nicht wollen.

Dezentralität

- Keine zentrale Infrastruktur wie bei weit verbreiteten Instant-Messengern oder großen Plattformen im WWW
- Jeder kann einen eigenen Mailserver betreiben ohne bei jemandem um Erlaubnis zu fragen



Was läuft schief?

- Transport ist nicht zwingend und nicht automatisch verschlüsselt
- Mails liegen auf den Servern im Klartext vor
- Fehlender Integritäts- und Authentizitätsnachweis
- Durch Erweiterungen (z.B. html) anfällig für Angriffe



Wer rettet die Mail für uns?

- 2011
- Hat sich nicht durchgesetzt
- Eine De-Mail kostete 30-40ct
- Eingebaute Schnüffelschnittstelle





Müssen wir die Mail retten?

Alles weiter wie bisher,
denn Niemand braucht Verschlüsselung.

bis 2013



Müssen wir die Mail retten?

Alles weiter wie bisher,
denn Niemand braucht Verschlüsselung.

bis 2013 →





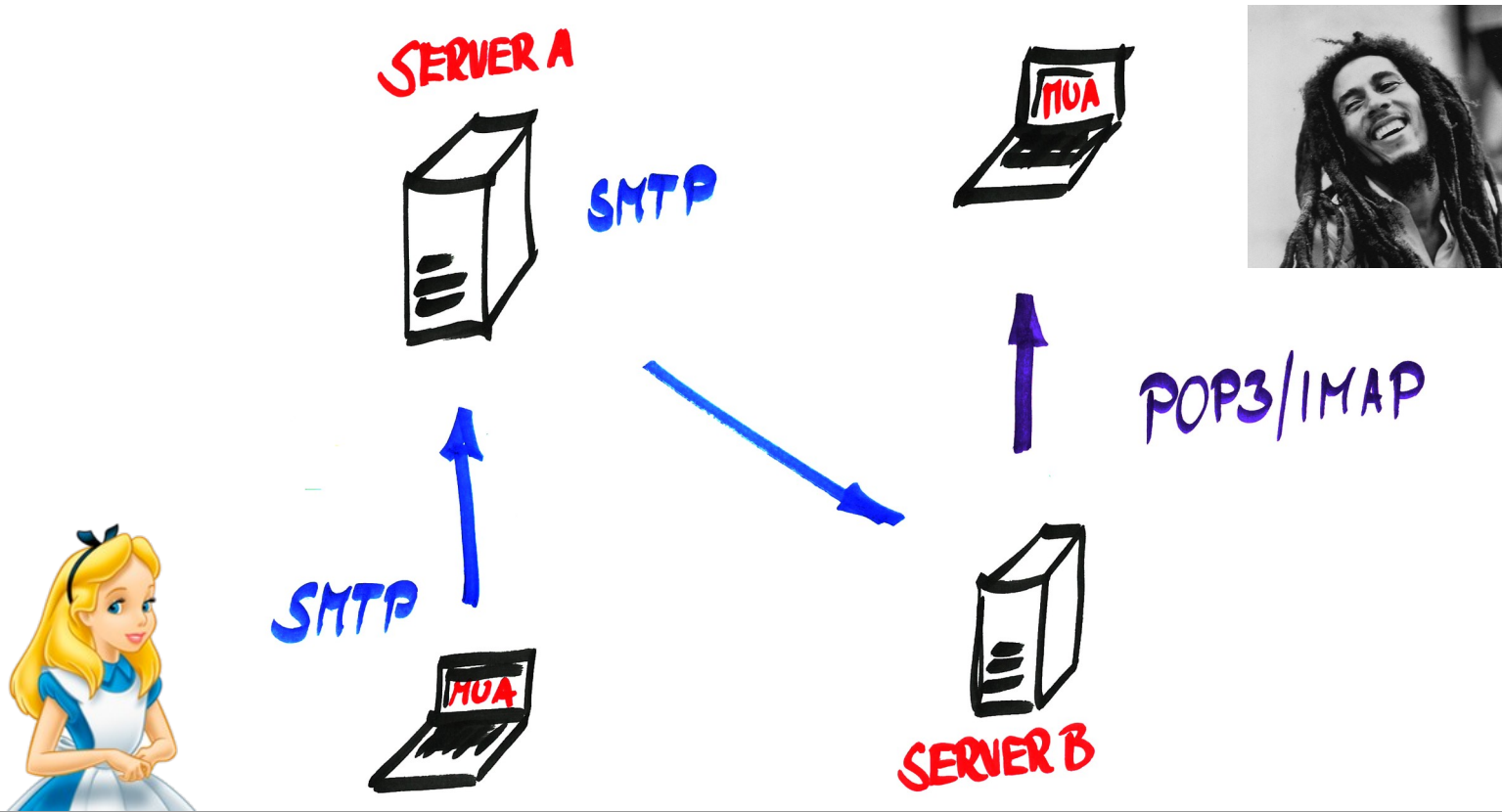
Wer rettet die Mail das 2. Mal für uns?

- 2013: Viele deutsche Mailanbieter schalten jetzt erstmals TLS zwischen ihren Servern ein
- Immer noch kein flächendeckender Zwang für TLS zwischen Client und Server
- Mails liegen auf den Servern weiterhin im Klartext vor oder sind bestenfalls in einer Form verschlüsselt, die es dem Anbieter erlaubt, sie weiterhin lesen zu können



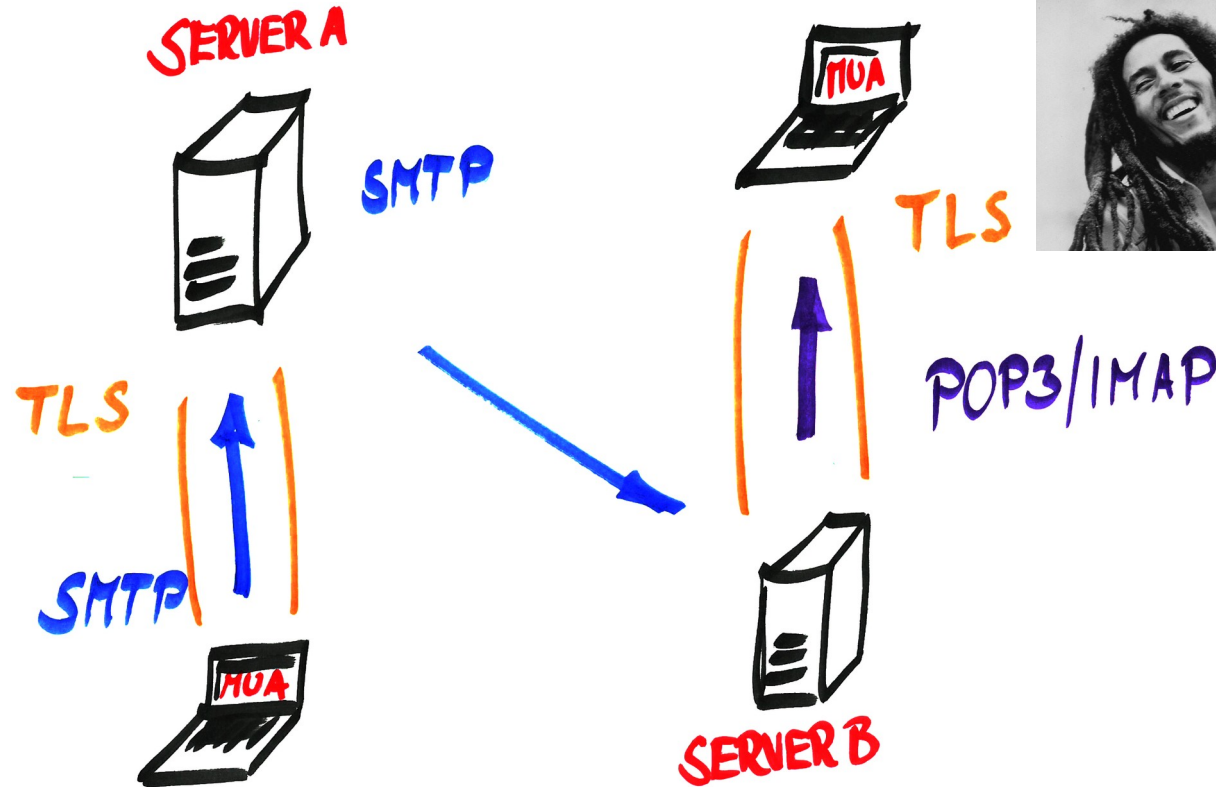


Postauslieferung :(





Postauslieferung :|





Verschlüsselung mit PGP

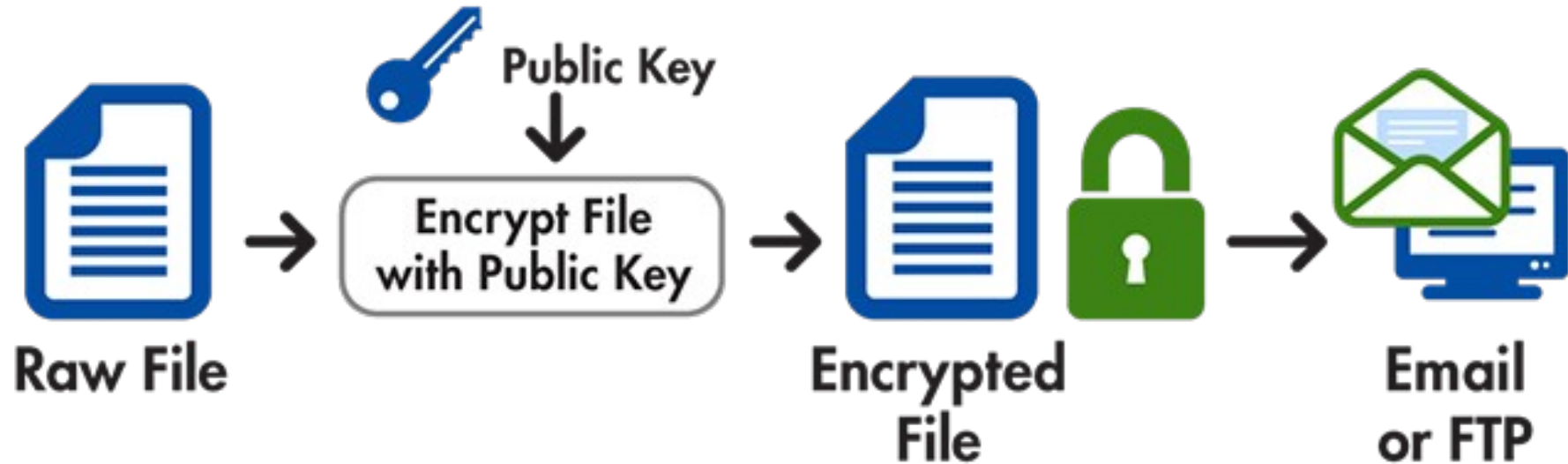
Asymmetrisches Verfahren

- Schlüsselpaar bestehend aus:
öffentlichem und privatem (geheimen) Schlüssel
- Mit dem öffentlichen Schlüssel verschlüsselte Daten lassen sich nur mit dem zum selben Paar gehörigen privaten Schlüssel entschlüsseln
- Mittels der aus den Daten und dem privaten Schlüssel erzeugten Signatur, lässt sich mittels des öffentlichen Schlüssels die Urheberschaft und Integrität der Nachricht/Datei nachprüfen



Verschlüsselung mit PGP

Encryption Process





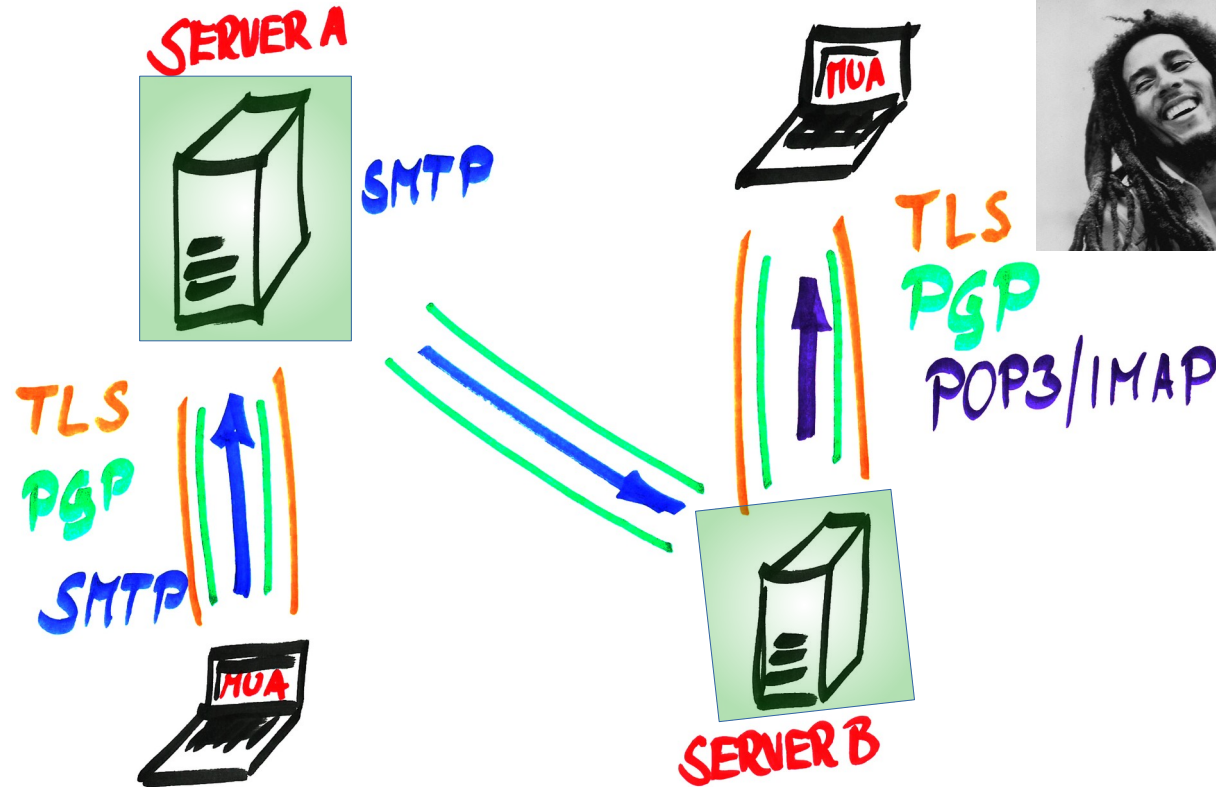
Verschlüsselung mit PGP

Decryption Process



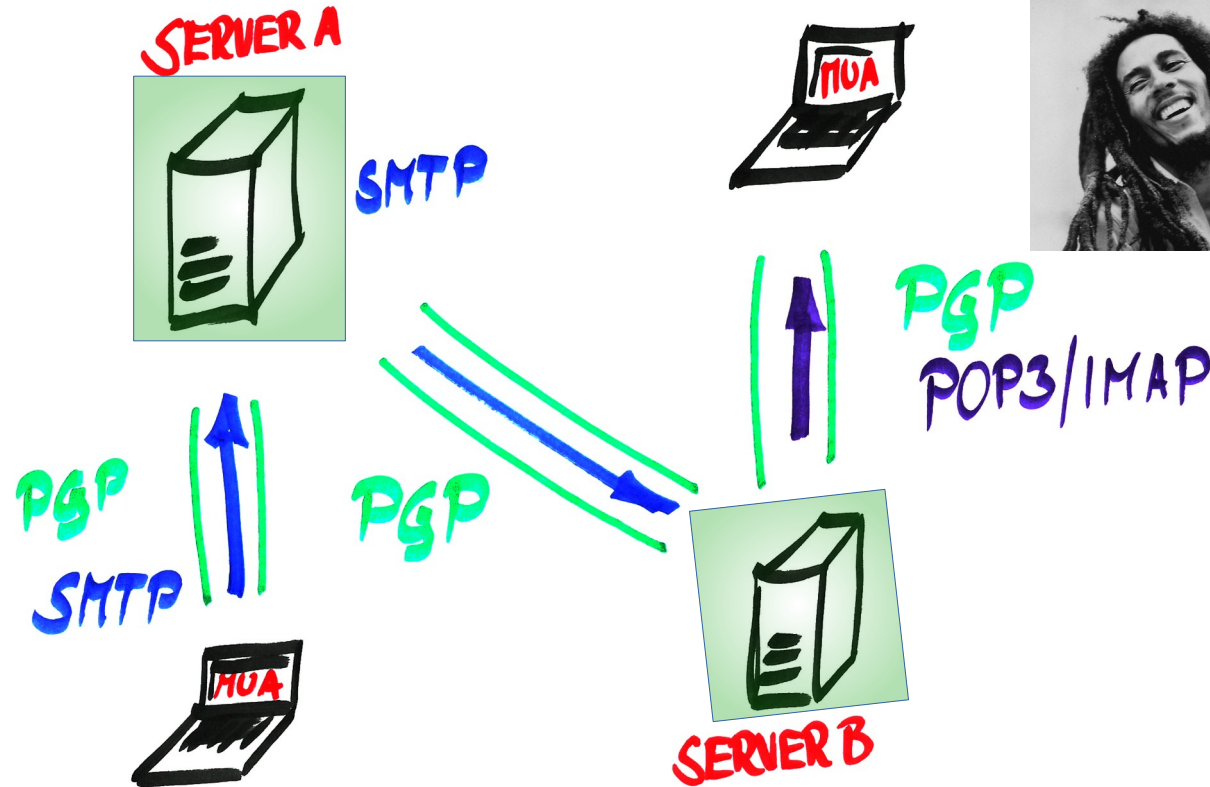


Postauslieferung :)





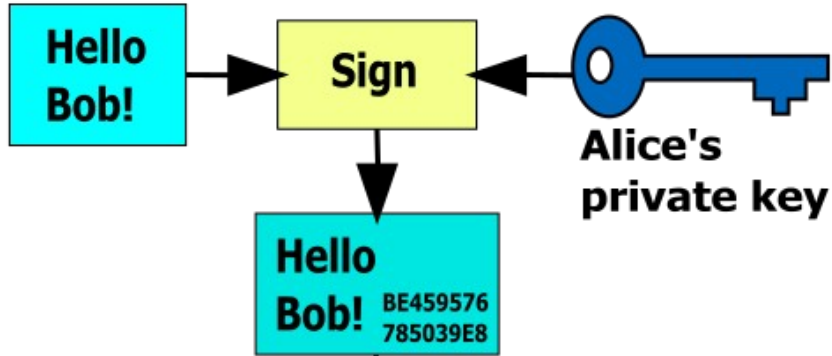
Postauslieferung :)



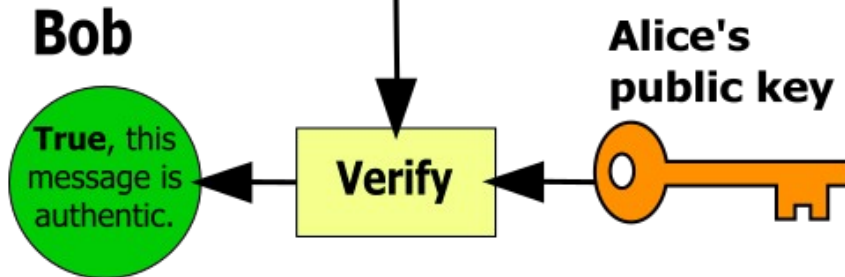


Digitale Signatur

Alice



Bob

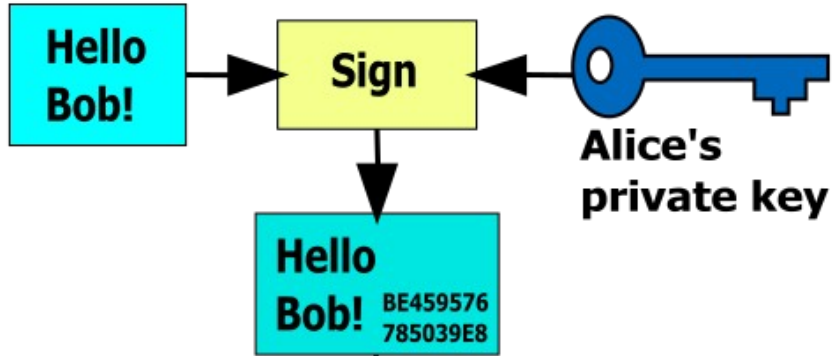


„Illustration of digital signature“ from Wiki-Commons by FlippyFlink is licensed under CC-BY SA

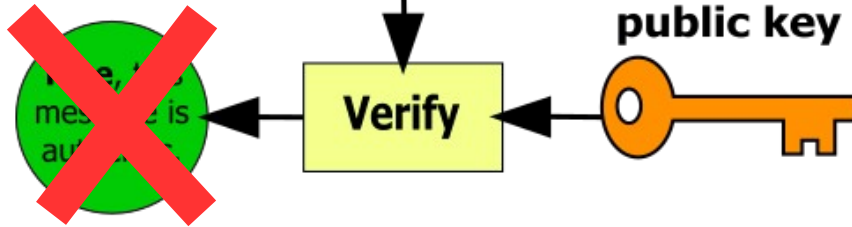


Digitale Signatur

Alice



Bob

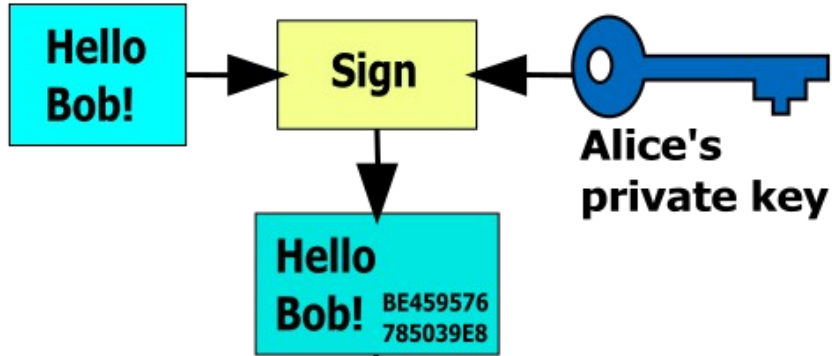


„Illustration of digital signature“ from Wiki-Commons by FlippyFlink is licensed under CC-BY SA

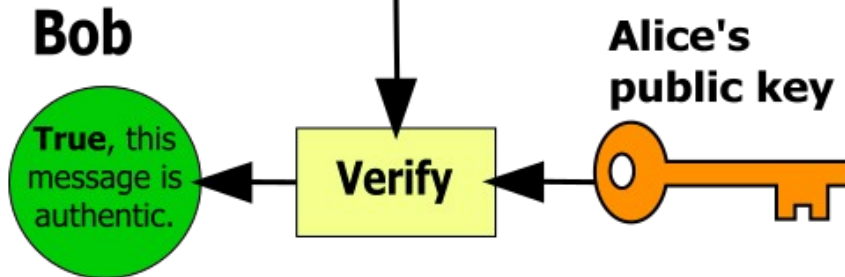


Digitale Signatur

Alice



Bob



„Illustration of digital signature“ from Wiki-Commons by FlippyFlink is licensed under CC-BY SA



Wie?

Windows	Linux	Mac
eM Client EverDesk The Bat! Outlook: gpg4o Gpg4win p≡p Thunderbird: Autocrypt Enigmail	Evolution: Seahorse Kmail: Kleopatra Mutt Thunderbird: Autocrypt Enigmail	Apple Mail: GPGTools Canary Mail Mutt Thunderbird: Autocrypt Enigmail