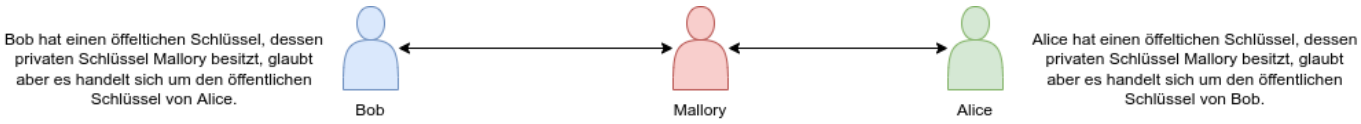
Authentizität

Ein wesentliches Ziel kryptographischer Verfahren ist **Authentizität** - man möchte sicher stellen, dass man tatsächlich mit dem richtigen Kommunikationspartner kommuniziert. Ist diese Verifizierung nicht möglich, kann ein Angreifer, der sich in einem günstigen Moment in den Kommunikationsvorgang einschaltet, mit einem Man in the Middle Angriff (MITM) die scheinbar perfekt verschlüsselte Kommunikation mitlesen und sogar verändern.

Es ist wichtig zu verstehen, dass man wirklich sicher sein muss, dass ein öffentlicher Schlüssel, den man besitzt wirklich dem Kommunikationspartner gehört, den man als Besitzer betrachtet.

(A1)

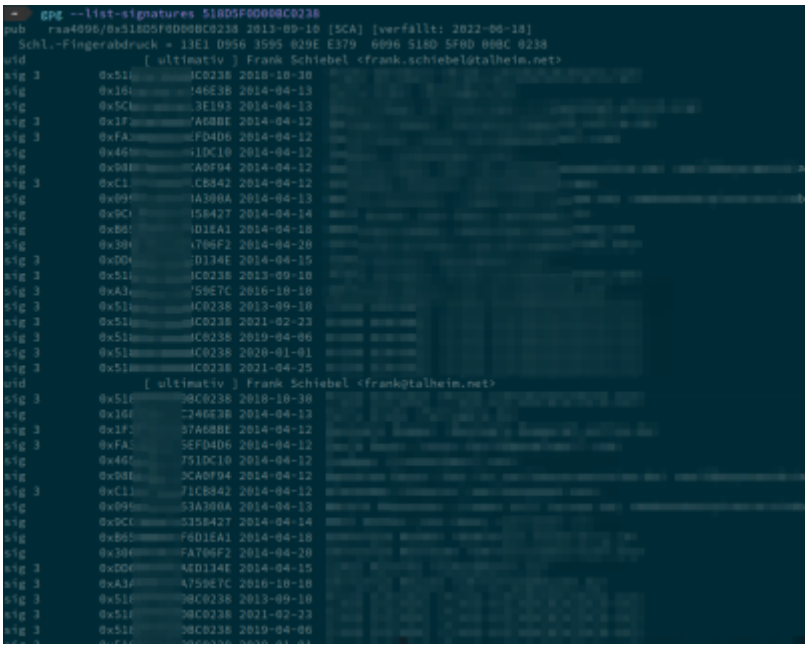
Eine solche Situation kann beispielsweise eintreten, wenn man sich öffentlich Schlüssel von sogenannten "Keyservern" holt - man kann dann nicht mit Sicherheit sagen, ob ein öffentlicher Schlüssel der Person gehört, die dort angegeben ist.



- Was bedeutet in diesem Zusammenhang die Aussage "dieser öffentliche Schlüssel gehört Alice"?
- Welche Folgen hat die im Schaubild dargestellte Situation für die Vertraulichkeit der Kommunikation?
- In welcher Weise sind digitale Signaturen von dieser Situation betroffen?

Web of trust

GnuPG verfolgt zur Lösung des Authentizitätsproblems einen dezentralen Ansatz, das sogenannte Web-of-Trust. Dabei werden nach eingehender Prüfung der Identität mit einem Ausweisdokument die öffentlichen Schlüssel von Personen, die man beispielsweise auf einer Cryptoparty trifft von weiteren Schlüsselbesitzern mit deren privatem Schlüssel signiert.



Die Hoffnung ist, dass man auf diese Weise irgendwann in der Liste der Signaturen für einen Schlüssel auf Menschen trifft, die man tatsächlich kennt und denen man vertraut - auf diese Weise kann man dann annehmen, dass der Schlüsselbesitzer tatsächlich derjenige ist, wer er (oder sie) vorgibt zu sein.

Alternativ kann man bei bilateralen Kommunikationsvorgängen Out-of-band den Fingerabdruck des Schlüssels gegenseitig kontrollieren, um die Authentizität bei dezentral verwalteten Schlüsseln sicherzustellen.

```
~ gpg --list-signatures 518D5F0D00BC0238
pub   rsa4096/0x518D5F0D00BC0238 2013-09-10 [SCA] [verfällt: 2022-06-18]
  Schl.-Fingerabdruck = 13E1 D956 3595 029E E379  6096 518D 5F0D 00BC 0238
```