

# Authentizität

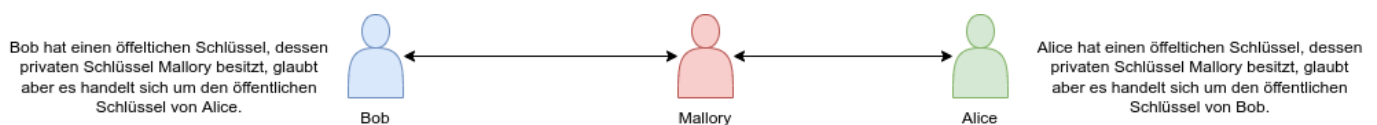
Ein wesentliches Ziel kryptographischer Verfahren ist **Authentizität** - man möchte sicher stellen, dass man tatsächlich mit dem richtigen Kommunikationspartner kommuniziert. Ist diese Verifizierung nicht möglich, kann ein Angreifer, der sich in einem günstigen Moment in den Kommunikationsvorgang einschaltet 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.

```
-- GPG --list-signatures 51805F00008C0238
pub rsa4096/8x51805F00008C0238 2013-09-10 [SCA] [verfällt: 2022-06-18]
    Schl.-Fingerabdruck = 13E1 D956 3595 019E E379 6896 5180 5F00 008C 0238
uid          [ ultimativ ] Frank Schiebel <frank.schiebel@talheim.net>
sig 3 0x51805F00008C0238 2018-10-30
sig 3 0x1680734663B 2014-04-13
sig 3 0x5C80003E193 2014-04-13
sig 3 0x1F8000A588E 2014-04-12
sig 3 0xFA8000F0406 2014-04-12
sig 3 0x46800010C16 2014-04-12
sig 3 0x988000CA0F94 2014-04-12
sig 3 0xC180001C842 2014-04-12
sig 3 0x9980001A380A 2014-04-13
sig 3 0x9C8000158427 2014-04-14
sig 3 0xB68000101EA1 2014-04-18
sig 3 0x3880001706F2 2014-04-20
sig 3 0xDD80001D114E 2014-04-15
sig 3 0x51805F00008C0238 2013-09-10
sig 3 0xA380001759E7C 2016-10-10
sig 3 0x51805F00008C0238 2013-09-10
sig 3 0x51805F00008C0238 2021-02-23
sig 3 0x51805F00008C0238 2019-04-06
sig 3 0x51805F00008C0238 2020-01-01
sig 3 0x51805F00008C0238 2021-04-25
uid          [ ultimativ ] Frank Schiebel <frank@talheim.net>
sig 3 0x51805F00008C0238 2018-10-30
sig 3 0x1680734663B 2014-04-13
sig 3 0x1F8000A588E 2014-04-12
sig 3 0xFA8000F0406 2014-04-12
sig 3 0x46800010C16 2014-04-12
sig 3 0x988000CA0F94 2014-04-12
sig 3 0xC180001C842 2014-04-12
sig 3 0x9980001A380A 2014-04-13
sig 3 0x9C8000158427 2014-04-14
sig 3 0xB68000101EA1 2014-04-18
sig 3 0x3880001706F2 2014-04-20
sig 3 0xDD80001D114E 2014-04-15
sig 3 0xA380001759E7C 2016-10-10
sig 3 0x51805F00008C0238 2013-09-10
sig 3 0x51805F00008C0238 2021-02-23
sig 3 0x51805F00008C0238 2019-04-06
```

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.

From:  
<https://info-bw.de/> -

Permanent link:  
<https://info-bw.de/faecher:informatik:oberstufe:kryptographie:authentizitaet:start?rev=1648748702>

Last update: **31.03.2022 17:45**

