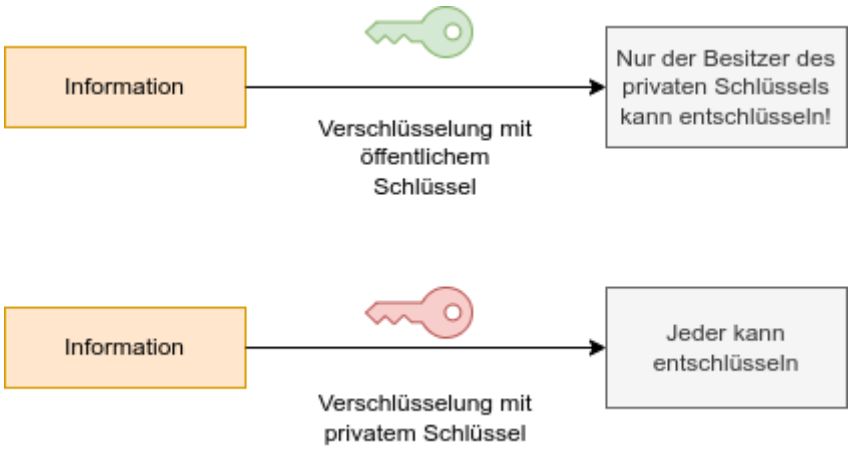
Digitale Signaturen

Asymmetrische Verfahren wie RSA funktionieren meist spiegelbildlich: Informationen, welche mit dem öffentlichen Schlüssel verschlüsselt werden, können mit dem privaten Schlüssel entschlüsselt werden. Es ist aber auch möglich, eine Information mit dem privaten Schlüssel zu verschlüsseln - diese Information kann dann jeder, der den öffentlichen Schlüssel besitzt wieder entschlüsseln. Was soll das bringen?



Wenn ich eine Nachricht mit einem öffentlichen Schlüssel entschlüsseln kann, kann ich mir sicher sein, dass der Sender im Besitz des dazu gehörigen privaten Schlüssels ist.

Ein digitale Signatur funktioniert nun folgendermaßen - wir verwenden ein Zeugnis im PDF-Format als Beispiel, das von der ausstellenden Schule digital signiert werden soll.

Unterschreiben

- Zunächst wird eine Prüfsumme des Dokumententeils erzeugt, welcher die Zeugnisinformationen enthält. Hier kommt meist ein geeignetes Hash-Verfahren zum Einsatz. Wird das Zeugnis nachträglich verändert, ändert sich der Hashwert.
- Den berechneten Hashwert verschlüsselt die Schule jetzt mit ihrem privaten Schlüssel, auf den nur autorisierte Personen Zugriff haben. Der verschlüsselte Hashwert wir dem Dokument hinzugefügt, ohne den Bereich der Zeugnisdaten zu verändern.
- Das Dokument enthält jetzt also die Zeugnisdaten und die verschlüsselte Prüfsumme dieser Zeiugnisdaten

Unterschrift prüfen

Ein Empfänger, der die Korrektheit der Informationen prüfen möchte, geht folgendermaßen vor

- Zuerst wird wieder Prüfsumme des Dokumententeils erzeugt, welcher die Zeugnisinformationen enthält - so wie sie beim Empfänger angekommen sind. Wenn die Daten zwischenzeitlich

verändert wurde, erhält der Empfänger jetzt eine andere Prüfsumme wie der Sender. Wenn das Dokument unverändert ist, erhält er dieselbe Prüfsumme.

- Dann wird mit dem öffentlichen Schlüssel der Schule die verschlüsselt übermittelte Prüfsumme des Senders entschlüsselt. Jetzt weiß man bereits, dass der Sender im Besitz des passenden geheimen Schlüssels war, es sich im Idealfall also wirklich um die Schule handelte, die das Zeugnis unterschrieben hat.
- Abschließend wird die selbst berechnete Prüfsumme mit der verschlüsselt übermittelten Prüfsumme verglichen. Weichen die beiden voneinander ab, wurde das Dokument verändert, andernfalls ist die Signatur gültig.