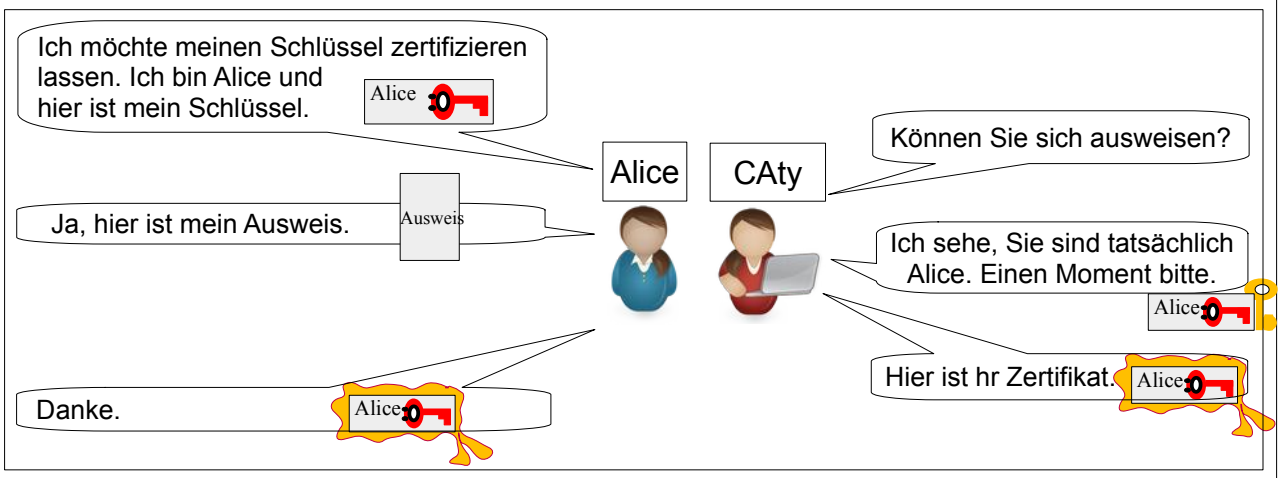
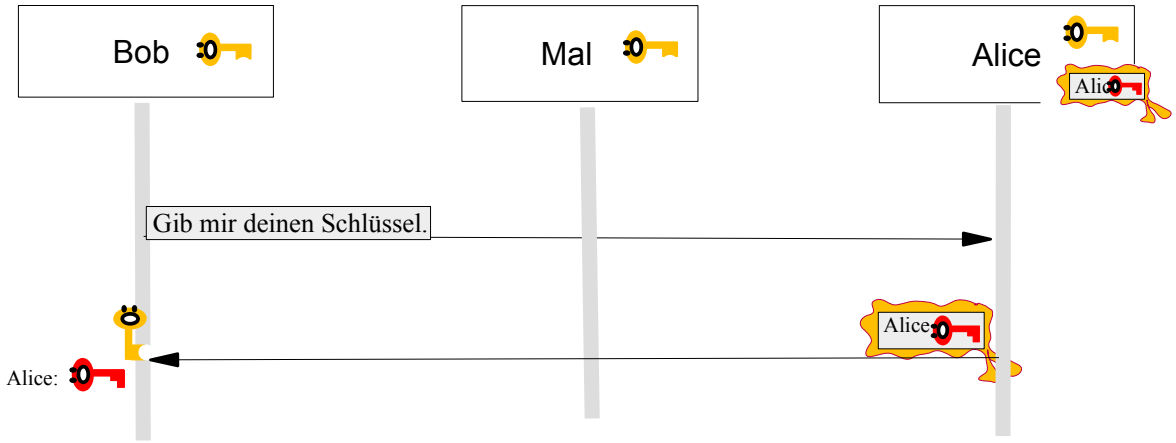
IuD: Zertifikat

Die Einheit aus dem Namen des Schüsseleigentümers und dem öffentlichem Schlüssel, verschlüsselt mit dem privaten Schlüssel der Zertifizierungsinstanz, nennt man Zertifikat.

Die Zertifikate werden von Zertifizierungsstellen, Certification Authoritys (CA), ausgestellt..

Tatsächlich beantwortet die Zertifizierungsstelle nicht jede einzelne Schlüsselanfrage, sondern stellt für Alice ein Zertifikat aus, wendet darauf den privaten Schlüssel der Zertifizierungsstelle an und übergibt es Alice. Alice schickt dieses signierte Zertifikat an ihre Kunden. Um sicher zu sein, dass Alice wirklich Alice ist, muss Alice persönlich bei der Zertifizierungsstelle erscheinen und sich ausweisen.





Damit nicht alle Kunden bei der Zertifizierungsstelle nach deren öffentlichem Schlüssel anfragen müssen, ist der öffentliche Schlüssel der Zertifizierungsstelle direkt im Browser eingetragen.

Es gibt nicht nur eine einzelne CA für die ganze Welt, sondern mehrere, die hierarchisch gegliedert sind und sich gegenseitig vertrauen.

Aufgabe

1. Sicherer Schlüsselaustausch (Aufgabe mit Chat-Tool)

Startet wieder pro Gruppe einmal das Programm ChatServerGUI.jar und startet den Server. Dann startet jeder das Programm ChatClient.jar. Jeder wählt einen kurzen Namen und verbindet sich mit dem Server.

Mindestens zwei Personen wollen vertraulich miteinander kommunizieren. Sie erzeugen dazu ein Schlüsselpaar (Schlüssel noch nicht versenden!). Eine dritte Person, Mal, der Man-in-the-Middle, verbindet sich ebenfalls mit dem Server und erzeugt ein Schlüsselpaar.

In dieser Aufgabe werden die Schlüssel vor dem Versenden von der Zertifizierungsstelle auf den Namen des Schlüsselbesitzers zertifiziert. Klicke dazu im Schlüsselspeicher mit der rechten Maustaste (Schlüssel-Name-Paar zertifizieren).

Der Man-in-the-Middle versucht, wie in der letzen Aufgabe, den Schlüsselaustausch zu manipulieren und seinen öffentlichen Schlüssel als Alice Schlüssel oder als Bobs Schlüssel auszugeben. Hat er eine Chance?