So unterscheiden sich Clientzertifikate von Serverzertifikaten

In Zeiten von DevOps hat man als Entwickler immer mehr mit Zertifikaten zu tun. In meiner Laufbahn als Consultant habe ich bemerkt, dass es hierbei immer wieder zu den grössten Verwirrungen kommt. Ich möchte daher mein heutiges TechUp diesem Thema widmen.

Zuerst ein paar Grundbegriffe

SSL (Secure Socket Layer)

SSL ist ein von Netscape entwickeltes Verschlüsselungsprotokoll, welches 1994 in der Version 1.0 erstmalig erschien. 1995 wurde SSL 2.0, und nur ein Jahr später SSL 3.0 veröffentlich. Alle diese Versionen sind aber heute nicht mehr zulässig. 1996 hat Netscape die Versionskontrolle zur Entwicklung eines Internet-Standards an die IETF (Internet Engineering Task Force), übergeben.

TLS (Transport Layer Socket)

Nach der Übergabe entwickelte die IETF auf Basis von SSL 3.0 das verbessertes Protokoll TLS in der Version 1.0, welches 1999 erschien. Auch dieses wird mittlerweile aber nicht mehr unterstützt, weil es unter anderem nicht mehr dem Zahlungsverkehr-Standard (PCI DSS) entspricht. 2006 wurde die Version 1.1 von TLS herausgebracht. Da hier aber SHA-1 für die Signaturerstelllung verwendet wird, wird von der Nutzung abgeraten. 2008 wurde dann die noch heute gültige TLS 1.2 veröffentlicht. Seit 2018 gibt es aber mittlerweile auch schon TLS 1.3 welche neue Anforderungen für TLS 1.2 enthält.

Cipher Suites

Eine Cipher (Chiffre) ist einfach ein Algorithmus, oder eine Sammlung von Schritten, um mathematische Berechnungen durchzuführen (RSA). Anhand dieses Algorithmus werden die Nachrichten verschlüsselt. Es gibt für TLS 1.2 derzeit 37 Ciphers und für TLS 1.3 fünf Ciphers. Als Cipher Suite bezeichnet man eine Kombination von Chiffren. Es gibt vier verschiedene Arten von Chiffren:

- Key Exchange Algorithms (RSA, DH, ECDH, DHE, ECDHE, PSK)
- Authentication/Digital Signature Algorithm (RSA, ECDSA, DSA)
- Bulk Encryption Algorithms (AES, CHACHA20, Camellia, ARIA)
- Message Authentication Code Algorithms (SHA-256, POLY1305)

Eine Cipher Suite sieht nun beispielsweise so aus:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS ist das Protokoll.
- ECDHE (Elliptic Curve Diffie Hellman) ist eine Chiffre, mit welcher während des Handshake die

Keys ausgetauscht werden.
- RSA ist der Authentifizierungsmechanismus.
- AES_128_GCM Ist der Bulk-Verschlüsselungsmechanismus (also die Verschlüsselung der Daten).
- SHA256 ist der Hashing Algorithmus.