4.4 Digitale Zertifikate

Zertifikate sind so etwas ähnliches wie Ausweise. Die wesentlichen Inhalte eines solchen Zertifikates sind der Zertifikatsinhaber, deren Authentizität durch diesen Ausweis bestätigt wird, deren *Public-Key*, die Zertifizierungsstelle und deren digitale Unterschrift über das Zertifikat. Der Aufbau von Zertifikaten ist standardisiert (siehe Abbildung 1)[1].

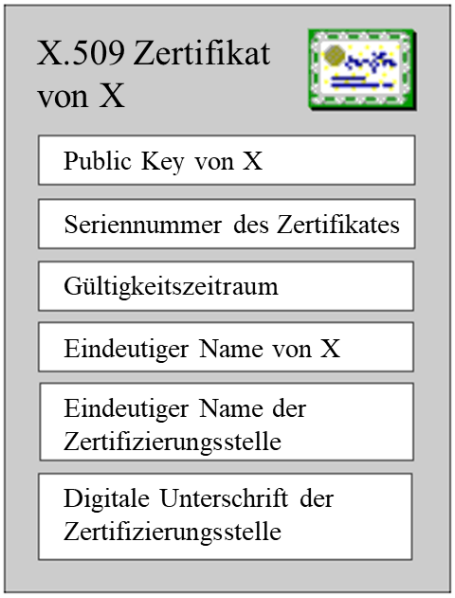

Abbildung 1: Wesentliche Inhalte eins *X.509* Zertifikates, wobei *X* der Zertifikationsinhaber ist

Die Aufgabe, die ein Zertifikat erledigt, ist die eindeutige Zuordnung eines *öffentlichen Schlüssels* zu einer bestimmten Institution X (siehe Abbildung 1). Dass diese Zuordnung korrekt ist und dass die Institution, die den passenden *privaten Schlüssel* besitzt, tatsächlich existiert, dafür verbürgt sich die ausstellende *Zertifizierungsstelle (*engl. ***C****ertification* ***A****uthority*, kurz *CA)*. Diese fügt dem ausgestellten Zertifikat seine digitale Unterschrift hinzu, wodurch es für Dritte ohne die Kenntnis des *privaten Schlüssels* der Zertifizierungsstelle unmöglich wird, das Zertifikat zu verändern. *CAs* sind allgemeine Anbieter für Vertrauensdienste, Berufsverbände (z.B. Wirtschaftsprüfer, Notare usw.), Personal und IT-Abteilungen von Unternehmen, Behörden.

[1] Siehe: X.509 – Wikipedia

