

Aufgabe 6:

DRM, TCPA und NGSCB

Begriffe wie *Digital Rights Management*, *Trusted Computing Platform Alliance* und *Next-Generation Secure Computing Base* (ehemals *Palladium*) halten sich nun schon seit 1999 recht hartnäckig in den Medien, werden hier und da hoch gelobt und vermutlich noch wesentlich häufiger kritisiert und zerrissen. Warum eigentlich? Was kann TCPA, was kann es nicht? Schränkt es den Computerbenutzer ein oder ist es ein Werkzeug von vielen?

Gehen Sie in Ihrer Ausarbeitung insbesondere auf kryptographische Gesichtspunkte von TCPA ein: Sind die eingesetzten Algorithmen zeitgemäß und unbedenklich? Wie funktioniert das Schlüssel-Management? Ist das Vorgehen aus kryptographischer Sicht vertretbar? Wie sind die Verfahren implementiert und in Computer integriert? Welche Probleme ergeben sich daraus?