Schlüsselaustausch und Policy Enforcement bei zweckgebundener Datenübermittlung

Kai Wagner

Wirtschaftswissenschaftliche Fakultät
Universität Regensburg
93040 Regensburg
kai.wagner@gmx.de

Abstract: Im beschriebenen Szenario überlässt ein Betroffener verschiedenen Datenverarbeitern unter dem Gebot strikt zweckgebundener Nutzung eine anlassbezogene Auswahl seiner Daten. Zum Zeitpunkt der Datenhinterlegung und Policy-Formulierung kennen sich Betroffener und potentieller Verarbeiter nicht. Sie nutzen zwei weitere Parteien als Vermittlungsdienst, die über die Einhaltung der Policies wachen, ohne sie selbst interpretieren zu können. Es wird gezeigt, wie die Vermittler ihre Rolle wahrnehmen, und dabei nahezu keine Informationen über den Datenaustausch erhalten. Die Realisierung des Policy-Abgleichs nutzt einen One-Time-Pad-basierten asynchronen Schlüsselaustausch zwischen Betroffenem und Verarbeiter, in den die Vermittler einbezogen werden, wiederum ohne zusätzliche Kenntnisse über Art und Inhalt der Kommunikation zu erwerben.