Projekt DaPriM (Data Privacy Management) der FH Münster.

In der jüngeren Vergangenheit sorgen „Datenpannen“ für eine öffentliche Diskussion über die Durchsetzung des Datenschutzes: Prominente Fälle waren *T-Mobile*, die im Jahr 2006 mehr als 17 Millionen Kundendatensätze verloren hat, und die Universität Göttingen, die im Jahr 2008 einräumen musste, dass die Daten von 26.000 Studenten ungeschützt auf einem Internetserver zugänglich waren.
Diese Datenschutzskandale zeigen den Bedarf an datenschutzfördernden Technologien, die einen wirksamen Schutz der Daten auch bei Fehlverhalten der Benutzer ermöglichen.

Unser Konzept nutzt einen irreversiblen Datenverschluss, so dass sensible Rohdaten innerhalb des Systems verschlüsselt gespeichert werden, niemand aber – auch kein Administrator – einen Zugriff auf diese erhält. Dies wird durch das Einbinden eines TPM-Modules erreicht, das zusammen mit Software-Komponenten sicherstellt, dass sich das System in einem sicheren Zustand befindet und nur dann den internen Zugriff auf die Schlüssel gemäß einer maschinenlesbaren Rechtebeschreibung freigibt. Änderungen am System bleiben möglich, sind aber mit der Löschung des Datenbestandes verbunden.

Da sich Anforderungen in einer Organisation ändern können, müssen die Regeln, mit denen auf diese Daten zugegriffen wird, in Grenzen anpassbar sein. Eine Anpassung wird systemseitig aber nur in soweit zugelassen, dass ein Zugriff auf die Rohdaten bzw. die rechnerische Ermittlung der Rohdaten anhand von Abfrageergebnissen nicht möglich ist.

Es gibt zwei natürliche Angriffwege auf ein solches System: Ein identifizierter Remote-Exploit (beispielsweise beim Zugriff über eine Webschnittstelle) kann das System kompromittieren; das Design sieht daher eine möglichst geringe Angriffsfläche vor, indem angreifbare Komponenten weitesgehend außerhalb des Verschlusses angesiedelt werden und nur ein minimaler Kanal ins Innere existiert. Ein Angriff auf die Hardware (z. B. auf das gespeicherte Schlüsselmaterial) ist ebenfalls denkbar; hierbei müssen Speicherdirektzugriffe (DMA), Seitenkanäle und physikalischer Zugriff auf RAM-Bausteine berücksichtigt werden.