Archivierung

Das Forschungsprojekt „Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente (ArchiSig)“ hat über die Aufbewahrung einfacher elektronischer Dokumente hinaus ein Verfahren entwickelt, wie auch elektronisch signierte Dokumente langfristig aufbewahrt und zur Erhaltung ihres Beweiswerts bei Bedarf automatisiert neu signiert werden können.

Verfahrensbeschreibung

Die aufzubewahrenden signierten Dokumente werden bei der Aufnahme in das Archivsystem auf ihre Integrität und Authentizität überprüft. Die für eine langfristige Signatur- und Authentizitätsprüfung erforderlichen Verifikationsdaten (insb. Zertifikate und Gültigkeitsabfragen) werden beschafft. Die elektronischen Dokumente werden verschlüsselt auf Langfristspeichermedien gespeichert. Die Verifikationsdaten und die Signaturen der Dokumente und Zertifikate werden in einem getrennten System für die Signaturerneuerung gespeichert. Werden bestimmte Algorithmen und Parameter von der Regulierungsbehörde nicht mehr für die folgenden sechs Jahre als sicher prognostiziert, stößt das Verfahren automatisch eine Erneuerung der betroffenen Signaturen an. Diese erfolgt im Regelfall ohne Zugriff auf die elektronischen Dokumente. Vielmehr werden viele Signaturen zusammengefasst und jeweils mit einem Zeitstempel, der eine qualifizierte Signatur trägt, erneut signiert.

Datenverarbeitung

Für die Signaturerneuerung ist ein Zugriff auf die personenbezogenen Daten in den elektronischen Dokumenten im Regelfall nicht erforderlich. Dies wird erst dann notwendig, wenn die verwendeten Hashverfahren unsicher werden. Ein Zugriff auf die signierten Dokumente im Klartext ist jedoch auch hier nicht zwingend notwendig. Dies gilt zumindest dann, wenn sie nach der Signaturerstellung unter Einbeziehung aller Signaturen und gegebenenfalls aller erforderlichen Verifikationsdaten verschlüsselt und dann nochmals gehasht und signiert werden. Für die Signaturerneuerung sind dann nur noch die verschlüsselten Daten maßgeblich. Das auf dem Konzept der Hashwertbäume basierende Verfahren ermöglicht auch, für die langfristig aufbewahrten Dokumente einzelne Dokumentteile, Daten und Signaturen zu berichtigen, zu löschen und zu sperren, ohne dabei die Beweiskraft der anderen erneuerten Signaturen anzugreifen.

Datenschutzrechtliche Bewertung

Die langfristig aufbewahrten personenbezogenen Daten (in den Dokumenten und den Zertifikaten) können trotz der Notwendigkeit einer in Abständen erforderlichen Neusignierung durch Verschlüsselung geschützt werden. Die bei der Neusignierung zu verarbeitenden Signatur- und Hashwerte sind keine personenbezogenen Daten. Durch diese Verfahren können auch besonders schützenswerte Daten für die langfristige Aufbewahrung und Neusignierung an fremde Dienstleister übermittelt werden. Sie erlauben auch, die Rechte der Betroffenen auf Sperrung und Löschung umzusetzen, ohne die Beweisqualität der Signaturen zu gefährden.

Projektverantwortung

Konsortialführer:
PERGIS Systemhaus GmbH

Andreas Bess
Rheinuferstr. 9
67061 Ludwigshafen
eMail: Andreas.Bess@pergis.de.

Datenschutzrecht:
Stefanie Fischer-Dieskau
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Universität Kassel
Mönchebergstr. 21a
34109 Kassel
Telefon: 0561/804-3079
EMail: s.fischer-dieskau@uni-kassel.de