Fragen aus dem Chat zur Sitzung „eIDAS-basierte Beglaubigung und Validierung“, mit Antworten von HS Harz netlab, 13.04.2022

Kontakt: netlab@hs-harz.de, hstrack@hs-harz.de

Hinweis: Sofern die Fragen nicht direkt von Seiten der HS Harz beantwortet sind, ist dies entsprechend kenntlich gemacht.

1. Jana Witthein: Wird eIDAS für das digitale Zeugnis (OZG Leistung digitales Schulzeugnis) genutzt?

Zu 1.: **Antwort erfolgt durch Sachsen-Anhalt:**
Im Rahmen des Proof-of-Concept wurde auch die Signatur der Zeugnisse und der im Zeugnis enthaltenen maschinenlesbaren Daten vorgenommen. Dabei wurde zunächst das XML im ELMO-Format mit einer X509-Signatur signiert, anschließend in die PDF integriert und abschließend das PDF-Zeugnis mit den eingebetteten Daten erneut mit der X509-Signatur signiert. Das hierbei getestete Vorgehen hat bereits die Anforderungen der eIDAS-Verordnung mit berücksichtigt.

Die Anforderungen, die sich aus der eIDAS-Verordnung ergeben, sind eine wesentliche Anforderung, die im Rahmen der Umsetzung eines Referenzsystems berücksichtigt werden.

---

2. Martin Baudach: Wie ist der Zusammenhang zwischen Beglaubigung und digitalem Schulzeugnis (z.B. Abiturzeugnis)? Konkreter: Benötigt man bei digital signierten Dokumenten denn überhaupt "Beglaubigungen"?

Zu 2.: Signaturen und andere Krypto-Funktionen (wie Hash-Funktionen, auch Blockchain/DLT) aus der angewandten Kryptographie sind grundsätzlich zunächst nur befristet valide nutzbar, und benötigen daher einerseits ein aktives Kryptomanagement, andererseits Ergänzungen zur langfristigen Beweiswerterhaltung im Signaturbereich mit Standards wie BSI TR ESOR. (Zusätzlich sind für den operativen Krypto-Einsatz geschützte Systemumgebungen notwendig, z.B. für den Schutz von Secret Keys.) Ein hohes Sicherheitsniveau wird mit qualifizierten Signaturen/Siegeln nach eIDAS-Standards erreicht, und daher vom Gesetzgeber als Schriftformersatz anerkannt und gleichzeitig für digitale Beglaubigungen vorgesehen (Verwaltungsverfahrensgesetze Bund/Länder §33). Vgl.:
https://www.gesetze-im-internet.de/vwvfg/__33.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR-ESOR-LEIT.pdf

Unser eNotar-Verfahren mit digitaler (Quellen-)Beglaubigung per qualifizierter Signatur (eIDAS, Standards) ist entsprechend den Verwaltungsverfahrensgesetzen von Bund und Ländern §33 bereits hybrid für verschiedene Ausgangsfälle samt deren Migration aufgestellt auch für unterschiedliche Zeugnisformen derzeitig/zukünftig. Verschiedene Ausgangsfälle, Optionen und Szenarien sind Original-Papierzeugniswesen (derzeit) mit ergänzenden digitalen „Zeugnis-Kopien/Beglaubigungen“ (auch Hybridformate) sowie Übergänge zur (ggf. nur Papierform ergänzenden) Zeugnisdigitalisierung als auch für die Sicherung der digitalen Zeugnis-Zugänge/Zugriffe bzw. -Transferdienste samt Optionen für gesicherte Langzeitspeicherung nach eIDAS-Standards (inkl. Standard BSI TR ESOR), bei Bedarf.
Unser Verfahren bietet gleichzeitig Lösungen für dieses mehrstellige Anforderungsspektrum, dabei mit Standards (eIDAS, auch EU-weit), hoher Sicherheit und rechtlicher Anerkennung per Schiftformersatz. Ein unspezifisch signiertes digitales Zeugnisdokument oder gar eine 2 Blockchain-Speicherung würden die gleichzeitigen Anforderungen nach Standards, hoher nachgewiesener Sicherheit und Vertrauenswürdigkeit (inkl. für zugeordnete Erteilungen/ Zugänge/Dienste/Widerrufe für Zeugnisse/Beglaubigungen), Effizienz und Optionen für wirksame und vertrauenswürdige Langzeitgültigkeit samt voller rechtlicher Anerkennung als Schriftformersatz dagegen so nicht erfüllen können. Über den Beglaubigungsprozess mittels eNotar wird durch Prüfen der Übereinstimmung der Daten zwischen „Original-Schulzeugnis“-Quellen (papiergebunden oder digital) und „digitaler Kopie“ durch die Amtsperson und dem anschließenden Erstellen der Qualifizierten elektronische Signatur für die digitale Kopie eine beglaubigte digitale Kopie des Schulzeugnisses erstellt (mit QeS-Signatur, nach eIDAS-

Standards), dabei zusätzlich gesichert mit Zugang/Transfer nur für Berechtigte per OZG- oder eIDAS-Konten. (siehe auch §33 VwVfG).

---

3. Frank Pfotenhauer: Basiert die Zeugnissignierung auf dem Piloten der OZG Arbeitsgruppe Sachsen-Anhalt mit der Bundesdruckerei?

Zu 3.: **Antwort erfolgt durch Sachsen-Anhalt:**
Nein. Bei dem Projekt der Hochschule Harz handelt es sich um ein eigenständiges Projekt, das nicht in Verbindung mit dem OZG-Projekt „Digitales Schulzeugnis“ steht, welches in der Zusammenarbeit mit der govdigital und der Bundesdruckerei das Proof-of-Concept zur Zeugniserstellung umgesetzt haben.

---

4. Anna Lisa Wienke: Wie verbreitet ist das Verfahren für die beglaubigte Zeugniskopie schon? Können auch Absolvent*innen solche beglaubigte Kopien nach einem Zeitraum X noch bei der ausstellenden Stelle anfordern?

Zu 4.: Qualifizierte Signaturen von Beglaubigungen können mit gängigen Tools aus dem Office-Umfeld geprüft werden (auch ganz unabhängig von OZG). Die rechtlichen und technischen Ausstattungen dazu gibt es grundsätzlich bereits seit vielen Jahren. Entsprechend gesicherte Zugänge und Applikationen über OZG-Nutzerkonten sind in Versuchsreihen erprobt, das OZG-Massenrollout steht nach den allgemeinen OZG-Timelines sicherlich jedoch noch bevor. Das eNotar-Verfahren der Hochschule Harz steht zurzeit als produktiver Prototyp zur Verfügung, dieser wurde produktiv erprobt in ausgewählten kleineren Versuchsreihen. Die Anforderung und Ausstellung einer digitalen beglaubigten Kopie ist auch nach einem Zeitraum X noch möglich. Begrenzungen ergeben sich hier nur durch die Aufbewahrungszeiten bei dem jeweiligen Amt. Ggf. auch mittels Amtsübergreifender Infrastrukturen für gesicherte und standardisierte Langzeitspeicherungen (nach Standards BSI TR ESOR bzw. eIDAS Preservation TS) können auch längere Zeiträume abgedeckt werden.

---

5. Frank Pfotenhauer: Was ist mit dem XSchule-Standard? Wird der auch unterstützt?

Zu 5.: Wir verfolgen und unterstützen die Entwicklungen im Bereich des XHochschule- und XSchule-Standards aktiv, als Community-Mitglied. Eine Unterstützung von Dokumenten, die nach den XHochschule bzw. XSchule-Standard erstellt wurden, ist bereits jetzt gegeben.

---

6. Arn Waßmann: Welche Kosten entstehen pro qualifizierte elektronische Signatur?

Zu 6.: Wir sehen uns hier im Bereich „Kosten“ nicht als die richtigen Ansprechpartner und verweisen bei dieser (auch politischen) Frage auf zuständige höhere Verwaltungen und Ministerien (Bund/Land). Nur soviel: nach unseren Erfahrungen im technischen Forschungsumfeld spielen die Signaturkosten selbst eher eine untergeordnete Rolle, auch im OZG-Umfeld. Zu Kostenfinanzierungs/verteilungs-Modellen (inkl. möglichen Förderungen zur Entlastung) gibt es sowohl bzgl. Anwendungen/Tools des IT-Planungsrat als auch bzgl. OZG-Umsetzungen bekannte Regelungen und Vorgehensweisen im Bereich der höheren Verwaltungen und Ministerien (Bund/Länder). Eher um Größenordnungen deutlich höhere (Folge-)Kosten werden dagegen erwartet durch Nutzung nicht standardisierter Herstellerlösungen einerseits (wie Vendor-Lockin) oder durch nicht-digitalisierte Verwaltungen andererseits.

---

7. Martin Baudach: Die Frage nach den "laufenden Kosten" (Wie hoch? Für wen?) bei elektronischen Signaturen (z.B. digit. Zeugnisse) und die Frage nach der Haftung bei techn. oder Eingabe-Fehlern bleibt wichtig - für Schule, Hochschule und Privatpersonen...

zu 7.: Zu Kostenfragen: siehe zu 6. Für rechtliche Fragen verweisen wir auf zuständige Behörden bzw. Juristen (für signaturbezogene Fragen (eIDAS TS) ist die zuständige Behörde die Bundesnetzagentur im Geschäftsfeld des BMWK und des BMDV, für Sicherheitsfragen ist das Bundesamt für Sicherheit in der

Informationstechnik (BSI) die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland, im Geschäftsbereich des BMIH). Die Haftung von CA/PKI-Zertifizierungsstellen für eIDAS-Vertrauensdienste ist nach Vertrauensdienstegesetz/ -verordnung geregelt. Weiterführende Links: https://www.bundesnetzagentur.de/EVD/DE/Verbraucher/Fragen/FAQ-node.htmlhttps://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/moderner-staat_node.html

---

8. Anna Lisa Wienke: Und welche Ausgabedatei erhält man bei der beglaubigten eZeugniskopie? PDF? PDF + XML?

Zu 8.: Bisher arbeiten wir bei der eNotar-Anwendung mit pdf-Kopien und detached qualified Signatures oder alternativ mit Hybriden Formaten wie ELMO (XML und PDF) oder auch Europass EDCI (weiter mit den nach eIDAS TS zulässigen Formaten wie zip), weitere Formate sind integrierbar.

---

9. Hans Pongratz: Welche Einrichtungen ""akzeptieren"" denn die elektronisch beglaubigten Nachweise schon? Das wäre ja der ""Lackmustest"". Also Ausstellen ist das ein, aber dann akzeptieren anstelle von Papier die aus meiner Sicht größere Herausforderung für die Verwaltungen.

Zu 9.: Auch sogar mit kostenfreien und (auch bei Behörden) verbreiteten Tools sind Prüfungen qualifizierter Signaturen seit Längerem möglich. Gerade bei IST-SOLL-Fragen im Behördenbereich ist die Perspektive der „Akzeptanz“ nur eine mögliche, andere sind z.B. Umsetzung von „Strategien zur Digitalisierung“ oder „Verpflichtungen“, insbesondere nach der Corona-Pandemie. Es gibt klare gesetzliche Verpflichtungen zur Anerkennung qualifizierter Signaturen EU-weit (eIDAS-Verordnung 2014 ff, gültig in allen EU-Mitgliedsstaaten). Weiter gibt es für Behörden in Deutschland die klare gesetzliche Verpflichtung entsprechende Zugänge für die Einreichung qualifiziert signierter Dokumente anzubieten (z.B. per E-Governmentgesetzen Bund/Länder), s. am Beispiel Bund „Übersicht zu Umsetzungsverpflichtungen aus dem E-Government-Gesetz”: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/umsetzungsverpflichtung-egov.pdf;jsessionid=0D8048AAD423517B4804E4A6D71273AC.2_cid364?__blob=publicationFile&v=4
//www.heise.de/news/Digitales-Unterschreiben-boomt-wegen-Corona-4891881.html

Beispiel Land NRW: §3 E-Government-Gesetz, vgl. https://recht.nrw.de/lmi/owa/br_vbl_detail_text?anw_nr=6&vd_id=15719&vd_back=N551&sg=0&menu=1

Insoweit hierzu immer noch Vollzugsdefizite vorkommen sollten, wären hier sicherlich entsprechende Maßnahmen bzw. Nachsteuerungen der zuständigen Organe aus Executive, Justiz und Gesetzgebung gefragt. Corona und Verbreitung qualifizierter Signaturen vgl.: https://www.heise.de/news/Digitales-Unterschreiben-boomt-wegen-Corona-4891881.html

---

10. Barbara Rehr: Inwieweit sind die einzelnen Bereiche über Prototypen hinaus, wo sind sie realisiert.

Zu 10.: Fundamentale Bausteine unserer eNotar-Lösung (wie eID-Online-Ausweis-Funktion und qualifizierte Signaturen inkl. Fernsignaturen nach eIDAS-Standards) werden von entsprechenden eIDAS-Service-Anbietern in Deutschland und Europa produktiv angeboten, vgl. https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/technik/eID-service/eid-service-node.htmlhttps://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/DEDie Lösung selber ist im Rahmen von Forschungsprojekten als Prototyp mit produktiven Real-Tests entstanden und wurde/wird in Projekten in Kooperation mit Wirtschaft und Verwaltung weiterentwickelt bzw. integriert (z.B. Prototyp KOLIBRI zur Nationalen Bildungsplattform (BMBF), von Bechtle, dataport, univention, Hochschule Harz), welche den Weg für entsprechende Produkt-Umsetzungen und ein Massenrollout durch Wirtschaft und Verwaltung vorbereiten.

---

11. Martin Windolph: Können einzelne Nachweise kurzfristig widerrufen werden, z.B. aufgrund eines erkannten Betrugs? Wie lang sind Signaturzertifikate gültig und müssen Nachweise regelmäßig neu signiert werden?

Zu 11.: eIDAS-basierte Trustservices (z.B. Signaturen/Siegel) erlauben integrierte standardisierte Verfahren für Widerrufe (entsprechend Gültigkeitsmodellen). Grundsätzlich sind Verfahren der angewandten Kryptographie stets nur befristet gültig, also auch Signaturzertifikate (letztere oft 2 bis 3 Jahre). Für Langzeitsicherungen gibt es hierzu jedoch standardisierte Verfahren mit automatisiert integrierten „krypto-graphischen Erneuerungen“ wie „PKI-Übersignaturen/Zeitstempel“ (eIDAS Preservation Standards, BSI TR ESOR). Vgl.: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR-ESOR-LEIT.pdf

---

12. Barbara Rehr: Wie sieht es mit der Signaturprüfung aus? Manuell pro eingereichtem Zeugnis? Digital möglich?

Zu 12.: PKI-Signaturen (auch QeS) können lokal oder remote mit Tools oder Diensten geprüft werden, dabei auch automatisiert bzw. anwendungsintegriert für größere Anzahlen von Zeugnisbeglaubigungen (vgl. Standards für eIDAS Validation Services).

---

13. Jana Witthein: Gibt es Schnittstellen für die Schulverwaltungsprogramme damit die Zeugnisse automatisch erstellt werden?

Zu 13.: Das eNotar-System arbeitet auf Basis von Standards (Protokolle, Formate), enthält weiter Rollen-Optionen für die Ankopplung an Schul-/Hochschul-Systeme einerseits als auch an eIDAS-Infrastrukturen andererseits, und ist damit an bestehende Systeme koppelbar. Die Signatur-Optionen können weiter mit den zugelassenen Möglichkeiten für „Massen-Signaturen“ kombiniert werden.

---

14. Irina Ullrich: Kann die Nutzung auch für duale Studien (Praktika) für Vertrage genutzt werden?

Zu 14.: Das eNotar-Verfahren kann auch für andere Dokumente (Verträge) genutzt werden. Für das Praktikummanagement wurde eigens das Verfahren zu „eInternship“ erweitert.

---

15. Christiane Schiltz: Wie verknüpft man vorhandene Schüler/Studentendaten mit einer eID?

Zu 15.: Hierzu wurden verschiedene Komponenten bzw. Services entwickelt:

- „YourCredentials“-Service zur Beglaubigung und vertrauenswürdiger Kopplung verschiedener digitaler Identitäten einer einzigen Person für verschiedene Bildungsphasen/Bildungsträgersysteme, in Erweiterung dann auch für ID-Kopplungen verschiedener Personen wie „Elternteil-Kind“.
- Hybride Nutzerkonten „eProSecal“, welche vorhandene Legacy-Identitäten mit eID/eIDAS-Identitäten direkt koppeln, als auch indirekt mit OZG-Nutzerkonten (Land/Bund). Damit sind entsprechende Anpassungen und System-integrationen je nach Rolloutstand/Migration im OZG-Bereich möglich.