Umweltfreundliche Bildungsnachweise: Systementwurf und Erfahrungen mit elektronischen Kurszertifikaten

T. Kiertscher, R. U. Franz
Technische Hochschule Brandenburg, Deutschland

Abstract: Wenn Studierende an Online-Kursen einer Hochschule teilnehmen, erhalten sie nach Bestehen oft ein Kurszertifikat, welches Kursinhalt, Umfang in ECTS und Note ausweist.

Die gewohnte Praxis, Kurszertifikate handschriftlich zu unterschreiben und postalisch zu versenden, wird bei sehr vielen Kursteilnehmern zu aufwändig; insbesondere, wenn die Kurse weltweit angeboten werden. Ein elektronisches Kurszertifikat kann den zeitlichen, materiellen und finanziellen Aufwand für die Hochschule deutlich reduzieren und zusätzlich Mehrwerte schaffen. Eine langfristig verfügbare Echtheitsprüfung spiegelt dabei den Wert des Kursabschlusses wider.

Um die Erstellung und Verifikation der Kurszertifikate optimal in die Verwaltung der Online-Kurse integrieren zu können, wurde ein eigenes System entwickelt, welches die Digitalisierungsstrategie der Hochschule innovativ unterstützt und durch Prozessoptimierungen deutlich nachhaltiger arbeitet. In diesem Beitrag wird der Systementwurf vorgestellt und einige wichtige Entwurfsentscheidungen erläutert. Ein Rückblick auf drei Jahre im Betrieb erlauben die Bewertung des Systems hinsichtlich Aufwandseinsparung.

Keywords: Online-Lehre, Kurszertifikat, Nachhaltigkeit, Digitale Prozesse

1. Einführung

In der heutigen Bildungslandschaft stehen Studierende vor dem anspruchsvollen Ziel ihre akademische Ausbildung abzuschließen und möglichst gut für den späteren Berufseinstieg vorbereitet zu sein. Um dieses Ziel zu erreichen, bietet unsere Hochschule Online-Kurse an, die sowohl akademische Inhalte vermitteln, aber gleichzeitig auch auf die Berater-Zertifikatsprüfungen der SAP vorbereiten. Die Zertifikate der SAP sind praxisnah aber die vom Unternehmen zur Vorbereitung ausgegebenen Schulungsunterlagen sind nicht akademisch aufgebaut, sondern zielen inhaltlich direkt auf die Prüfungen. Sie bieten den Studierenden eine Dokumentation praxisrelevanter Kenntnisse, die sich eng an den Anforderungen der Wirtschaft orientiert und sind damit besonders wertvoll für Studierende, die sich auf eine Karriere in der Wirtschaft vorbereiten. Allerdings werden sie in vielen Hochschulen nicht anerkannt, da sie keine Note enthalten, der Arbeitsumfang nicht ersichtlich ist und sie nicht auf wissenschaftlichen Grundlagen basieren.

Im Gegensatz dazu werden Hochschulzertifikate von akkreditierten Hochschulen vergeben, enthalten eine Note, dokumentieren akademische Inhalte und sind in der Regel mit der Anrechnung von ECTS-Leistungspunkten verbunden. Dies macht sie nicht nur in der akademischen Welt anerkannt, sondern ermöglichen auch die Anrechnung im Rahmen von Studienprogrammen.

Alle von unserer Hochschule angebotenen Online-Kurse im Themengebiet *Enterprise Ressource Planning* (ERP) schließen bei erfolgreichem Bearbeiten und Bestehen mit einem

Hochschulzertifikat ab. Auf Wunsch können die Studierenden im Anschluss an der Prüfung für das zugehörige SAP-Zertifikat teilnehmen. Da es sehr hohe Teilnehmerzahlen bei diesen Online-Kursen mit Studierenden aus aller Welt gibt, war der Aufbau eines Online-Zertifikatssystems notwendig.

2. Stand der Technik

Zertifikate von Hochschulen wurden in der Vergangenheit üblicherweise in Papierform mit einem Siegel und handschriftlichen Unterschriften ausgegeben. Dabei weist das Siegel nach, dass die Urkunde tatsächlich von der Hochschule stammt, indem der physische Zugriff auf das Siegel durch geeignete Maßnahmen auf einen bestimmten Personenkreis beschränkt ist. Die Unterschriften erhöhen die Fälschungssicherheit durch ihre individuelle Linienführung. Die Fälschungssicherheit einer Unterschrift, besonders wenn diese in einer großen Zahl von Urkunden verbreitet wird, ist zwar weiterhin anerkannt, jedoch nicht unanfechtbar (Yeung et. al., 2004).

Wenn ein bisher in Papierform erstelltes Zertifikat in eine elektronische Form überführt wird, z. B. in das *Portable Document Format* (PDF), gehen Merkmale an Siegel und Unterschrift verloren, die von einem Experten genutzt werden können, um die Echtheit zu überprüfen. Siegel und Unterschrift werden in einem PDF auf eine Pixel- oder Vektorgrafik mit begrenzter Auflösung reduziert. Diese lässt nicht nur viele Details vermissen. Sie kann auch verlustfrei kopiert und in anderen Dokumenten wiederverwendet werden.

Elektronische Dokumente sind ohne weiteres nicht vor Manipulationen geschützt. Der Inhalt von PDF-Dateien lässt sich mit einer großen Auswahl an Programmen beliebig verändern. Die Integrität, die ein Blatt Papier bietet, indem es die einmal aufgedruckten und handschriftlich geschriebenen Inhalte zu einer Einheit verbindet, ist bei einer PDF-Datei nicht gegeben.

Um die Echtheit von digitalen Dokumenten sicherzustellen, haben sich die folgenden drei Verfahren etabliert: Elektronische Unterschrift, Digitale Signatur und Verifikations-URL.

Die **elektronische Unterschrift** ist nicht mehr als das Erfassen einer handschriftlichen Unterschrift mit einem digitalen Eingabegerät wie Maus oder Touch-Pad als Vektorgrafik. Diese wird dann als grafisches Element in die PDF-Datei eingefügt. Nicht nur verändert das digitale Eingabegerät die Linienführung der Unterschrift zum Teil erheblich, die erzeugte Vektorgrafik bildet, mit der ursprünglichen PDF-Datei keine untrennbare Einheit. Deshalb kann der übrige Inhalt der PDF-Datei verändert werden, ohne die Unterschrift zu berühren.

Aufgrund seines geringen Aufwandes und dem aktuellen Rechtsrahmen findet diese schwache Methode eines Authentizitätsnachweises dennoch häufig Anwendung und wird auch von Softwareherstellern als sinnvolle Praxis propagiert. Darunter z. B. Adobe, das Unternehmen welches das PDF entwickelt hat, mit der *E-Signatur*[10] oder Stefan Ziegler als Teil der *PDF24 Tools*[11].

Die **digitale Signatur** ist eine informationstechnische Lösung, welche eine mathematische Prüfsumme über die Daten des Dokuments bildet und diese mit Hilfe von asymmetrischer Kryptografie verschlüsselt. Dadurch entsteht eine digitale Unterschrift, die an das Dokument

[10] https://www.adobe.com/de/sign/electronic-signatures.html
[11] https://tools.pdf24.org/de/pdf-unterschreiben

angefügt wird (Bertsch, 2002; Pelzl & Paar, 2016). Für das asymmetrische Verschlüsseln und den Identitätsnachweis des Unterzeichners ist ein digitales Zertifikat erforderlich. Das Vertrauen in ein digitales Zertifikat wird durch eine *Public Key Infrastructure* (PKI) hergestellt. Digitale Signaturen sind eine sichere Methode des Authentizitätsnachweises, solange die genutzten kryptografischen Algorithmen nicht angreifbar werden, die Algorithmen korrekt implementiert wurden und die privaten Schlüssel der Vertrauensstellen und des Unterzeichners geheim gehalten werden. Da eine PKI mit technischem Aufwand verbunden ist, sind digitale Zertifikate für den Unterzeichner i. d. R. nicht kostenfrei. Der PDF-Standard umfasst digitale Signaturen und viele Anbieter, u. a. Adobe[12], bieten diese als Dienstleistung an. Die Verwendung von digitalen Signaturen ist in der EU durch die eIDAS-Verordnung geregelt (eIDAS VO (EU) 910/2014). Das *Deutsche Forschungsnetz* (DFN) stellt eine PKI für digitale Signaturen zur Verfügung (Gröper, 2022).

Bei der **Verifikations-URL** wird in das Dokument eine URL als Hyperlink oder als Text eingefügt, welche den Aufruf einer Webseite auf einem Verifikationsserver erlaubt. Diese zeigt dann i. d. R. jene Informationen an, die unverfälscht im Zertifikat stehen sollten. Ein Abgleich der Informationen aus dem Dokument mit denen auf der Webseite offenbart zuverlässig Manipulationen am Dokument. Der Verifikationsserver muss dafür die wesentlichen Informationen von allen ausgegebenen Dokumenten vorhalten. Ein Beispiel für eine etablierte Nutzung dieser Technik, sind die Kurszertifikate der Online-Lern-Plattform Coursera[13], welche u. a. den Namen des Lernenden, den Kursnamen, die Unterschrift der Lehrkraft als Grafik (s. *Elektronische Unterschrift*) und die Verifikations-URL enthalten.

3. Anforderungen

An ein System zur Ausstellung und Verifikation von Kurszertifikaten an unserer Hochschule werden die folgenden Anforderungen gestellt. **Betriebssicherheit:** Mit der Betriebssicherheit ist hier vornehmlich die Resilienz gegen illegale Zugriffe über das Internet, aber auch aus dem Intranet der Hochschule gemeint. Die Sicherheit muss langfristig gewährleistet werden. **Fälschungssicherheit:** Es muss mit erheblichem Aufwand verbunden oder theoretisch unmöglich sein, gefälschte Zertifikate auszustellen, oder manipulierte Zertifikate unter Anwendung der Verifikationsmöglichkeiten als echt erscheinen zu lassen. **Erweiterbarkeit:** Das System muss an eine zunehmend digitalisierte Infrastruktur angepasst und in teilautomatisierte Arbeitsabläufe integriert werden können. Ein für die Hochschule quelloffenes System ist dabei sehr hilfreich. **Abhängigkeiten:** Das System soll weitgehend unabhängig von externen Dienstleistern und auch unabhängig von den Dienstleistungen des DFN betrieben werden können. Das System soll auch unabhängig vom zentralen *Hochschulinformationssystem* (HIS) der Hochschule betrieben werden können, da die Verwaltung der Online-Kurse in einem spezialisierten System erfolgt. **Funktionalität:** Authentifizierung von Unterzeichnern am System mit dem zentralen Hochschul-Account; Verifikation ausgedruckter Zertifikate; Zertifikate in mehreren Sprachen; Verwaltung für grafische Vorlagen; Online-Editor für das Platzieren und Formatieren von Freitext und Datenfeldern; Import der Datensätze über ein verbreitetes Datenformat (z. B. CSV); Korrektur und Widerruf von ausgestellten Zertifikaten. **Rechtlicher Rahmen:** Das System muss den

[12] https://www.adobe.com/de/sign/digital-signatures.html
[13] https://www.coursera.support/s/article/208280196-Course-Certificates

aktuell geltenden rechtlichen Bestimmungen, insbesondere der DSGVO entsprechen (DSGVO (EU) 2016/679).

4. Systementwurf

In diesem Abschnitt wird der Entwurf des Zertifikatssystems beschrieben. Zunächst wird kurz die Wahl der Authentifizierungsmethode begründet. Dann wird die grobe Architektur vorgestellt, und das Konzept für die Integritätssicherung der Zertifikatsdaten erläutert. Nach einer Beschreibung des Ablaufs zur Verifikation eines ausgestellten Zertifikats, werden einige technologische Entscheidungen erläutert.

4.1. Authentifizierungsmethode

Eine grundlegende Entscheidung, die im Entwicklungsprozess getroffen wurde, ist die Authentifizierungsmethode für die Zertifikate. Die elektronische Unterschrift wurde als ungenügend bewertet, um die Anforderung der Fälschungssicherheit zu erfüllen. Die digitale Signatur würde Abhängigkeiten zu externen Dienstleistern mit sich bringen, die vermieden werden sollen. Übrig bleibt das Konzept der Verifikations-URL.

4.2. Architektur

Das System ist in zwei Komponenten gegliedert: Den *Manager* und den *Verifikator*. Beide haben eine eigene Datenbank. Der Manager stellt eine Verwaltungsoberfläche im Intranet der Hochschule bereit. Er speichert Zertifikatsvorlagen und Zertifikatsdatensätze in einer Datenbank und ermöglicht den Versand von ausgestellten Zertifikaten über den E-Mail-Server der Hochschule. Beim Ausstellen eines Zertifikats schreibt der Manager einen verschlüsselten Verifikationsdatensatz in die Datenbank des Verifikators. Der Verifikator hat nur lesenden Zugriff auf seine Datenbank. Die Komponenten und ihre Nutzer sind in Abb. 1 dargestellt.

Die Trennung des Systems in Manager und Verifikator hat einige Vorteile im Vergleich mit einem monolithischen System:

- Die Angriffsfläche aus dem Internet wird minimiert. Angriffe auf den öffentlich erreichbaren Server treffen zunächst nur den Verifikator.
- Der Verifikator besitzt nur sehr wenig Funktionalität, was seine Komplexität verringert und so weiter die Angriffsfläche minimiert.
- Gelingt einem Angreifer aus dem Internet der Einbruch in den Verifikator, erlangt er nur lesenden Zugriff auf verschlüsselte Datensätze.
- Verwaltungsfunktionen und Mechanismen zur Integritätssicherung der Datenbank des Managers können unabhängig vom Verifikator aktualisiert werden.
- Der Manager kann bei Wartung oder, langfristig gedacht, auch bei Stilllegung des Systems abgeschaltet werden, ohne die Funktionalität des Verifikators zu beeinträchtigen.

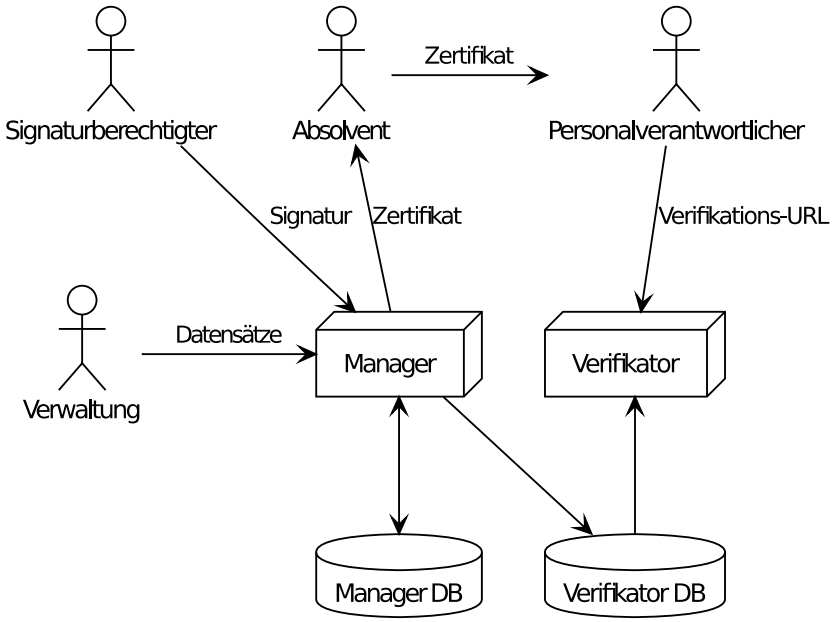

Abb. 1: Systemübersicht

4.3. Integritätssicherung

Die Integritätssicherung der Zertifikatsdatensätze soll langfristig sicherstellen, dass die zugrunde liegenden Daten von ausgestellten Zertifikaten nicht nachträglich in der Datenbank des Managers manipuliert werden können. Die Maßnahmen zur Integritätssicherung sind für den Fall vorgesehen, dass ein Angreifer schreibenden Zugriff auf die Datenbank des Managers erlangt hat.

Als Sicherungsmaßnahme wird eine Kette von digitalen Signaturen verwendet. Der Unterzeichner verwendet dabei ein selbst-signiertes digitales Zertifikat, welches nicht durch eine PKI, sondern durch ein starkes Passwort gesichert ist. Die Manipulation eines einzelnen Datensatzes oder das böswillige Hinzufügen eines Datensatzes könnte auch ohne eine Kette aufgedeckt werden. Sie dient jedoch dem Zweck, dass auch das Löschen von Datensätzen nachweisbar wird. Wird ein Angriff aufgedeckt, muss die Datenbank aus einer Sicherungskopie wiederhergestellt werden.

4.4. Zertifikatsausstellung und Widerruf

Das System sieht vier Rollen für Benutzer vor: Administrator, Sachbearbeiter, Signaturberechtigter und Prüfer. Ein **Administrator** weist anderen Benutzern die übrigen Rollen im Zertifikatssystem zu. Ein **Sachbearbeiter** legt Zertifikatsvorlagen an, importiert Datensätze, ordnet Zertifikatsvorlagen zu und stellt *Signaturanfragen* für einen oder mehrere Datensätze.

Ein **Signaturberechtigter** legt sich ein Siegel an (selbst-signiertes digitales Zertifikat); und prüft und bewilligt Signaturanfragen. Das System sieht neben Signaturanfragen auch Widerrufs- und Korrekturanfragen vor. Wird eine Widerrufsanfrage bewilligt, legt das System einen signierten Widerrufsdatensatz an, der den Zertifikatsdatensatz des widerrufenen Zertifikats referenziert. Eine Korrektur erzeugt einen Widerrufsdatensatz gefolgt von einem neuen Zertifikatsdatensatz.

Ein **Prüfer** hat lesenden Zugriff auf Datensätze, Zertifikatsdatensätze und Widerrufsdatensätze und hat die Möglichkeit einen Integritätsprüflauf auszulösen.

Durch die Trennung der Rollen Sachbearbeiter und Signaturberechtigter, kann das System das Vier-Augen-Prinzip effektiv umsetzen; welches optional durch die Rolle des Prüfers um eine dritte Partei erweitert werden kann.

Wird ein Zertifikatsdatensatz in der Datenbank des Managers angelegt, wird eine zufällige aber in der Datenbank eindeutige ID und ein zufälliger symmetrischer Schlüssel als Teil des Zertifikatsdatensatzes erzeugt. Aus der ID, dem Schlüssel und der Internetadresse des Verifikationsservers, kann später die Verifikations-URL gebildet werden. Anschließend wird in der Datenbank des Verifikators unter Verwendung von ID und Schlüssel ein verschlüsselter Verifikationsdatensatz angelegt. Wird ein Widerrufsdatensatz in der Datenbank des Managers angelegt, wird der referenzierte Verifikationsdatensatz gelöscht. Die Datenbank des Verifikators kann jederzeit, mit Hilfe der Kette von Zertifikats- und Widerrufsdatensätzen aus der Datenbank des Managers, auf Integrität überprüft und auch vollständig wiederhergestellt werden.

4.5. Verifikationsablauf

Der Verifikator stellt eine einfache Webseite im Internet bereit, auf welche die Verifikations-URL verweist. Sie zeigt bei einem gültigen Zertifikat den zugehörigen Datensatz an. Dazu extrahiert der Verifikator den Verifikations-Code aus der URL und ruft mit der ID den Verifikationsdatensatz ab. Er entschlüsselt diesen mit dem Schlüssel und zeigt die enthaltenen Informationen an. Die Webseite des Verifikators kennt nur zwei Anzeigezustände:

- *Der Verifikations-Code ist ungültig:* Entweder wurde kein verschlüsselter Datensatz für die ID gefunden, oder der Versuch der Entschlüsselung mit dem Schlüssel aus dem Code war nicht erfolgreich.
- *Der Verifikations-Code ist gültig:* Der Datensatz wird angezeigt und der Benutzer muss die Informationen zwischen Webseite und Zertifikat vergleichen, um festzustellen, ob das Zertifikat unverändert und damit echt ist.

4.6. Technologische Entscheidungen

Zur Implementierung wurden die folgenden Technologien gewählt: Java und JavaScript (Programmiersprachen), Spring Boot (Application Framework), MySQL (Datenbank), Bouncy Castle (Programmierbibliothek für Kryptografie), Apache PDFbox (Programmierbibliothek für PDF-Erstellung und Manipulation), RSA-Signaturen. Auswahlkriterien waren dabei hauptsächlich Verbreitung und langfristige Verfügbarkeit von Sicherheits-Updates.

Der Verifikations-Code soll möglichst leicht fehlerfrei abzuschreiben sein. Der Code ist an die *Bubble-Babble*-Kodierung angelehnt und besteht aus fünf 5er-Gruppen (Huima, 2011). Das verwendete Alphabet und die erlaubten Wechsel von Konsonanten und Vokalen weichen vom Standard ab, um die Kapazität zu erhöhen; verzichtet dabei aber auf die Prüfsummenfunktion. Die ID nimmt die ersten zwei Gruppen ein (Entropie ≈ 41 Bits). Das erlaubt bis zu 2,2E+12 Zertifikate auf einem Verifikationsserver. Bei einer Hochschule mit 10 000 ausgestellten Zertifikaten/Jahr und einer Betriebszeit über 100 Jahren, werden lediglich 0,000 05% des verfügbaren ID-Raumes genutzt. Der Schlüssel nimmt die übrigen drei Gruppen ein (Entropie ≈ 61 Bits).

Ein Verifikations-Code könnte wie folgt aussehen: „abeci-dofug-omnip-sefgo-ijaku“

Eine Zertifikatsvorlage besteht aus einer PDF-Datei als grafischer Hintergrund, Freitext- und Datenfeldern, dem Hyperlink für die Verifikations-URL und optional einem *QR-Code*[14].

Um den Ressourcenbedarf zu minimieren, werden Zertifikate dynamisch beim Versenden aus Zertifikatsvorlage und -datensatz generiert und nicht als Datei auf dem Server gespeichert.

5. Evaluierung

Das primäre Ziel der Einführung der elektronischen Kurszertifikate war die Reduzierung des Aufwands. Tab. 1 stellt ihn nach Papiermenge, Kosten und Zeit dar. Bei den Portokosten wurden Einsparungen bereits dadurch erlangt, dass Sammelsendungen an ausländische Partneruniversitäten geschickt wurden. Der Aufwand für die Systementwicklung belief sich auf 4 Monate Vollzeit für einen akademischen Mitarbeiter mit abgeschlossenem Informatikstudium.

Tab. 1: Aufwände

Form	Material/Kostenart	Ø Papier/Jahr	Ø Kosten/Jahr	Rolle	Ø Zeit/Jahr
Papier	Versandtaschen	240 kg	401 €	Unterzeichner	40 h
	Zertifikate/Druck	50 kg	704 €	Verwaltung	200 h
	Porto		3 015 €		
	Summe	**290 kg**	**4 120 €**		**240 h**
Elektr.	Material	0 kg	0 €	Unterzeichner	5 h
	Betrieb		150 €	Verwaltung	15 h
				Entwickler	10 h
	Summe	**0 kg**	**150 €**		**30 h**

Für den Betrieb wird eine VM mit 2 CPUs, 3 GB RAM und 32 GB SSD-Speicher benötigt. Die Kosten dafür sind auf 150€/Jahr geschätzt. Eine vergleichbare VM als Amazon AWS EC2, kostet zum Zeitpunkt der Drucklegung 0,04$/h und damit 320€/Jahr, oder 185€/Jahr über drei Jahre.

Mit dem Zertifikatsystem wurden bisher 21 647 Zertifikate ausgestellt und versendet. In Tab. 2 sind die ausgestellten korrigierten und widerrufenen Zertifikate je Semester gelistet. Tab. 3 enthält die Verzögerungen, mit der Widerrufe oder Korrekturen durchgeführt wurden. Eine Analyse des Zugriffsprotokolls des Verifikators über 4 Monate hat die Statistik in Tab. 4 ergeben.

Tab. 2: Zertifikate nach Semestern

Semester	ausgestellt	korrigiert	widerrufen
SS 2020	3107	5	2
WS 2020/21	3144	36	2
SS 2021	2625	16	1
WS 2021/22	2199	6	0
SS 2022	2137	1	4
WS 2022/23	2064	5	0
SS 2023	1819	6	0
WS 2023/24	2161	13	0

[14] https://www.denso-wave.com/en/technology/vol1.html

Tab. 3: Korrekturen und Widerrufe

Verzögerung	Anteil
gleicher Tag	3
gleiche Woche	48
gleicher Monat	27
gleiches Halbjahr	11
gleiches Jahr	2
später	1

Tab. 4: Anfragen an den Verifikator in 4 Monaten

Ergebnis	Anfragen	Kommentar
Gültig	16 015	ID bekannt, nicht widerrufen, Schlüssel OK
Nicht gefunden	1	ID unbekannt
Widerrufen	21	ID bekannt, widerrufen
Ungültig	1	ID bekannt, Schlüssel ungültig
Exploits	1 006	Nicht vorgesehene URL-Parameter
Summe	**17 042**	

6. Zusammenfassung

Die Entwicklung und Einführung eines Systems für die Ausstellung von elektronischen Zertifikaten für Online-Kurse hat in unserer Hochschule für eine deutliche Reduzierung von monetärem und zeitlichem Aufwand geführt und spart eine große Menge an Papier ein. Der wegfallende internationale Versand ist deutlich nachhaltiger. Das System bietet eine hohe Betriebssicherheit und benötigt auch bei langfristigem Betrieb wenige Ressourcen.

Zukünftig ist die direkte Anbindung an die Online-Kursverwaltung mit automatischem Transfer der Datensätze für Kursabschlüsse und eine Modernisierung der Integritätssicherungsmaßnahmen durch den Wechsel von RSA auf ED25519 geplant.

7. Literaturverzeichnis

Bertsch, Andreas: Digitale Signaturen. In: *Digitale Signaturen*. Berlin, Heidelberg : Springer, 2002 — ISBN 978-3-642-56304-1, S. 7–65

DSGVO (EU) 2016/679: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

eIDAS VO (EU) 910/2014: Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

Gröper, Ralf: Technische und rechtliche Aspekte bei Dokumentensignaturen. — URL https://doku.tid.dfn.de/_media/de:dfnpki:dokumentensignatur_2022.pdf

Huima, Antti: The Bubble Babble Binary Data Encoding. — URL http://web.mit.edu/kenta/www/one/bubblebabble/spec/jrtrjwzi/draft-huima-01.txt

Pelzl, Jan ; Paar, Christof: Einführung in die asymmetrische Kryptografie. In: *Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender*. Berlin, Heidelberg : Springer, 2016 — ISBN 978-3-662-49297-0, S. 173–198

Yeung, Dit-Yan ; Chang, Hong ; et. al.: SVC2004: First international signature verification competition. In: *Biometric Authentication: First International Conference*, ICBA 2004, Hong Kong, China, Juli 15-17, 2004. Proceedings : Springer, 2004, S. 16–22