1 Bezeichnung der Verarbeitungstätigkeit

Zugangsverfahren für das Serviceportal für Studierende der Hochschule Landshut unter der Nutzung einer App bzw. spezialisierter Hardware

2 Name und Kontaktdaten des Verantwortlichen

2.a Datenschutzrechtlich Verantwortlicher

Verantwortlich für die Datenerhebung ist die Hochschule für angewandte Wissenschaften Landshut, Am Lurzenhof 1, 84036 Landshut,

Tel. +49 (0)871 - 506 0 Fax. +49 (0)871 - 506 506

E-Mail: info@haw-landshut.de

Verantwortlich für den App-Store ist der jeweilige Betreiber.

2.b Fachlich zuständige Stelle

IT-Abteilung der Hochschule Landshut

Frau Grabsch: E-Mail: Ljupka.Grabsch@haw-landshut.de Tel.: +49 (0) 871 506 151

Herr Stark: E-Mail: Thomas.Stark@haw-landshut.de Tel: .: +49 (0) 871 506 254

3 Kontaktdaten des Datenschutzbeauftragten

Hochschule Landshut, Am Lurzenhof 1, 84036 Landshut

E-Mail: datenschutz@haw-landshut.de

4 Zweck, Art, Umfang und Rechtsgrundlage

4.a Zweck, Art und Umfang

Da das Zugangsverfahren zugleich eine technische Maßnahme gemäß Art. 32 DSGVO zum Schutz der personenbezogenen Daten des Portals ist, ist es geboten, hier diese Maßnahme darzulegen und auch auf Risiken einzugehen.

4.a.1 Personenbezogene Daten

Accountname, Schlüssel („shared secret“, private key) und generierte Passwörter sind einer natürlichen Person, dem Studierenden, der sich anmelden will, zugeordnet und somit personenbezogene Daten (Art. 4 Nr. 1 DSGVO). Der sich Anmeldende ist der „Betroffene“ im Sinne des Datenschutzrechts.

Für den sog. öffentlichen Schlüssel im U2F Security Key – Verfahren, einem Challenge-Response-Verfahren, ist dies nicht der Fall, da der öffentliche Schlüssel nicht rückfahrbar auf den Security Key, eine Hardware, ist und nicht rückführbar ist auf die Person, den Studierenden, die den Security Key benutzt.

Personenbezogene Daten sind auch die Daten, die in Logs über den Sender, den sich anmeldenden Nutzer und sein System erhoben werden, wie die IP-Adresse, Zeit der Nutzung der IP-Adresse technische Daten über Browser und Betriebssystem, Art der Kommunikation (Anmeldung, Übersendung eines Passworts, Anforderung einer Challenge etc.)

Solche Logs werden auf der Ebene des Betriebssystems geführt aber auch als Audit-Log im sogenannten Authentikator (hier die Open Source Software privacyIDEA auf einem Server der Hochschule Landshut).

4.a.2 Erhebung

Erheben ist das Beschaffen von Daten beim Betroffenen. Erhoben werden nur Passwörter und technische Einstellungen (z.B. Passwortlänge) vom Betroffenen. Dabei kommt es nicht darauf an, ob die Daten vom Nutzer eingegeben werden oder von seinen Systemen übermittelt werden. Es kommt auch nicht darauf an, ob der Nutzer die Daten frei wählen kann.

Das Dauerpasswort („klassisches Passwort“) gibt der Nutzer nach seinem Wunsch ein. Zeitabhängige Passwörter werden auf einem System des Nutzers (Smartphone) generiert und von ihm übermittelt, können aber nicht frei gewählt werden. Ein öffentlicher Schlüssel wird von einem System des Nutzers generiert und übermittelt. Alle anderen Daten werden vom System (der Hochschule Landshut) generiert.

4.a.3 Authentifizierung

Authentifizierung ist der Nachweis der Identität, d.h. der Nachweis, dass die Person, die einen Zugang zu einem System verlangt, eine bestimmte Ressource begehrt, oder eine bestimmte Information gibt oder zu erhalten wünscht, auch diejenige Person ist, als die sie sich ausgibt. Unter „System“ wird eine Kombination von Software und Hardware verstanden. Im hiesigen Fall ist dies das „Portal“, das Studierenden und Beschäftigten gewisse Dienste als sogenannte Webanwendung zur Verfügung stellt. Man geht davon aus, dass der Browser genügt, um diese Dienste auf einem Endgerät in Anspruch zu nehmen, d.h. es ist keine Installation von Software erforderlich. Für die Inanspruchnahme wird angenommen, dass der Studierende einen Desktop (und kein Smartphone[1],[2]) als Endgerät nutzt.

Tatsächlich wird nicht die „bürgerliche Identität“ des Nutzers geprüft, sondern, ob er gewisse Authentisierungsmittel (wie Passwörter) vorweisen kann.

Authentifizierung kann also für beliebige Operationen durchgeführt werden. In diesem Kontext geht es um die Anmeldung am System und daher sprechen wir im Folgenden nur von der Anmeldung und meinen die Anmeldung im „Portal“.

Da über den Begriff immer wieder Streit besteht, hier eine Differenzierung:

Authentifizierung ist in enger Bedeutung: der Vorgang, in dem ein System prüft, ob die Mittel, die ein Nutzer vorweist, ihn als Berechtigten ausweisen. Beispiel: Es wird geprüft, ob der analoge Schlüssel zum Schloss passt. Beispiel: Das System liest mit dem Sensor die Daten der Chipkarte und prüft anhand der Daten, ob der Nutzer berechtigt ist.

Authentifizierung ist in weiter Bedeutung: Vorgang wie (1) und Vorgang, in dem der Nutzer Mittel benutzt, um seine Berechtigung zu zeigen, d.h. der Begriff in der weiten Bedeutung kennzeichnet den gesamten Vorgang.

Anmerkung: Das BSI macht den Unterschied zwischen Authentifizierung und Authentisierung.

Nachfolgend wird der Begriff in seiner weiten Bedeutung verwandt, weil dies auch dem gesetzlichen Sprachgebrauch (z.B. im BayHSchG) entspricht. Die Webseite der Hochschule Landshut verwendet jedoch beides.

4.a.4 Rollen

Für die Authentifizierung nehmen die beteiligten Personen bzw. Systeme bestimmte Rollen ein:

Endbenutzer: Person, die den Zugang begehrt. (Kurz: Nutzer)

User Agent: System, dessen sich der Endbenutzer auf seiner Seite bedient, um den Zugang zu erlangen, in der Regel „Browser“.

Prover: Teil-System auf Seiten des Benutzers, das Passwörter generiert. Es will den Beweis der Identität führen.

Authentikator: Teil des Systems, zu dem der Nutzer den Zugang begehrt, und zwar der Teil des Systems, der die Authentisierungsmittel prüft, die der Nutzer vorweist. (synonym: Verifikator, Validator, Validierer).

Diese Rolle spielt hier die Open Source Software „privacyIDEA“ zusammen mit der Infrastruktur, auf der sie läuft.

Identitätsmanagement: Teil des Systems, zu dem der Nutzer den Zugang begehrt, der die Nutzer verwaltet.

System, im Kontext das System zu dem der Nutzer den Zugang begehrt.

Im Folgenden wird kontextabhängig auch von Sender und Empfänger gesprochen.

---

[1] Dies ist eine Einschränkung, die gegenwärtig nach Aussage der IT-Abteilung besteht. Aus logischer Sicht, sollte völlig gleichgültig sein, ob Sie als Nutzer das Portal mit dem Browser eines Desktops oder eines Smartphone aufrufen.

[2] Auf einem Smartphone wäre denkbar, dass, anstatt das Portal als Webanwendung mit einem Browser vom Smartphone aus aufzurufen, man das Portal als native App auf dem Smartphone installieren kann. Dies wäre für eine mobile Anwendung das zeitgemäße, ist aber (noch) nicht vorgesehen.

4.a.5 2-Faktoren-Authentifizierung

Die 2-Faktoren-Authentifizierung ist ein Unterfall einer sog. „starken Kundenauthentifzierung“. Die „Faktoren“ entsprechen den „Elementen“ im nachfolgenden Zitat aus BaFin; Rundschreiben 4/2015 (BA) - Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI):

„Starke Kundenauthentifizierung ist im Sinne dieses Rundschreibens ein Verfahren, das auf der Verwendung zweier oder mehrerer der folgenden Elemente basiert, die als Wissen, Besitz und Inhärenz kategorisiert werden:

i) etwas, das nur der Nutzer weiß, z. B. ein statisches Passwort, ein Code, eine persönliche Identifikationsnummer,

ii) etwas, das nur der Nutzer besitzt, z. B. ein Token, eine Smartcard, ein Mobiltelefon, iii) eine Eigenschaft des Nutzers, z. B. ein biometrisches Charakteristikum, etwa ein Fingerabdruck.

Außerdem müssen die gewählten Elemente unabhängig voneinander sein, d. h. die Verletzung eines Elements darf keinen Einfluss auf das andere bzw. die anderen haben. Mindestens eines der Elemente sollte nicht wiederverwendbar und nicht reproduzierbar (die Inhärenz ausgenommen) sein und nicht heimlich über das Internet entwendet werden können. Das starke Authentifizierungsverfahren sollte so gestaltet sein, dass die Vertraulichkeit der Authentifizierungsdaten gewahrt bleibt.“

4.a.6 1. Faktor

Erster Faktor ist ein auf Dauer durch den Nutzer (hier: Studierenden) gewähltes Passwort. Es muss gewissen Bedingungen genügen (z.B. nicht ein Wort sein, das man in einem Lexikon nachschlagen kann) und es wird nach dem Stand der Technik in einer gesicherten Form gespeichert, - nämlich konkateniert mit einem Account-spezifischen sog. „Salt“ und in dieser Kombination in einen Hashwert umgerechnet und als solcher gespeichert. Das verwendete Verfahren ist ein Hashverfahren wie HMAC-SHA-2 und aufwärts.

4.a.7 2. Faktor: Prinzip

Der zweite Faktor ist hier kein biometrischer, sondern ein weiteres, allerdings nur einmal verwendbares Passwort. Die Forderung ist, dass die Gewinnung dieses Passworts den Besitz eines Gegenstands voraussetzt.

4.a.7.1 Einmal-Passwort

Die den hier gewählten Verfahren zugrundeliegende Idee ist die des Einmal-Passworts, die durch den Einsatz kryptologischer Verfahren realisiert wird.

Eigenschaften des Einmal-Passworts:

- Jedes Passwort ist nur einmal verwendbar, d.h. für einen Zugangsvorgang.
- Jedes Passwort ist nur eine sehr kurze Zeitspanne gültig, d.h. für einen Zugangsvorgang verwendbar
- Das Passwort ist nur in dieser Zeitspanne verfügbar, es wird weder beim dem, der es vorlegt (Prover), noch beim Authentikator auf Vorrat gespeichert.

Vorteil: Ein Angreifer hat nur begrenzte Zeit das Passwort zu entwenden[3] oder ein von ihm generiertes Passwort vorzulegen[4]. Ein Angreifer kann auch ein entwendetes Passwort nicht mehrfach verwenden, in dem er es später nochmals „einspielt“.

Wie und wann der Angreifer aber Passwörter errechnet, bleibt ihm überlassen, d.h. er könnte auch auf Vorrat Passwörter erzeugen, die er vorlegen will. Es wäre ein Missverständnis anzunehmen, dass der Angreifer in seiner Arbeit immer auf die Spanne der Gültigkeit des Passworts beschränkt wäre. Falls das Passwort aufgrund einer zufälligen Information zustande käme, d.h. in seine Berechnung noch eine zufällige Information eingehen würde, die der Angreifer nicht vorhersehen kann, erschwert dies den Angriff.

Herausforderung: Der Empfänger des Passworts muss eine Möglichkeit der Verifikation (oft auch syn: Validierung) haben, d.h. er muss für jeden Zugangsvorgang prüfen können, ob das Passwort auch vom Berechtigten stammt. Dies muss geschehen, ohne dass das Passwort selbst vorab zwischen den Beteiligten ausgetauscht wurde, d.h. hier unterscheidet sich der Vorgang vom klassischen Passwortverfahren.

Lösungsidee: Die Zugang begehrende und dazu das Passwort vorlegende Instanz (Prover - eine Person, ein Rechenprozess) und die validierende Instanz (Authentikator, Validator) müssen zum Zeitpunkt eines Zugangsvorgangs ein koordiniertes „Wissen“ darüber haben, welches oder welche Passwörter gültig sind. Die validierende Instanz muss dieses Wissen haben, ohne dass ihr vorab das Einmal-Passwort bekannt gemacht wurde.

Für jeden Zugangsvorgang wird vom Sender aus einem Klartext eine Kennung (Zeichenfolge) berechnet. Man könnte die Kennung als eine Art elektronische Unterschrift ansehen. Der Klartext wechselt je Zugangsvorgang. Die Kennung ist spezifisch für den Klartext und die Verbindung Sender-Empfänger, d.h. für andere Klartexte ist die Kennung in der Regel eine andere. Für andere Sender-Empfänger-Paare wird die Kennung so berechnet, so dass sie selbst für denselben Klartext in der Regel eine andere ist[5].

Der Empfänger hat in jedem Zugangsvorgang den Klartext und die zugehörige Kennung und kann somit prüfen, ob die Kennung tatsächlich vom Berechtigten stammt, d.h. ob der Sender der Berechtigte ist. Klartext und Kennung zusammen haben die Funktion des Passworts.

Der Empfänger kann entweder den Klartext in gleicher Weise wie der Sender aus einer Information ableiten, über die beide verfügen, z.B. aus der Uhrzeit des Zugangsvorgangs, oder der Sender hat den Klartext ohnedies vom Empfänger erhalten, oder der Sender sendet den von ihm gewählten Klartext mitsamt der Kennung.

Kennt der Empfänger bereits den Klartext (z.B. Uhrzeit), dann genügt es, wenn nur die Kennung versandt wird – sie ist dann das Passwort. Im Folgenden wird immer die Kennung als Passwort bezeichnet – wohl wissend, dass in manchen Fällen der Sender auch noch den Klartext mitsenden muss.

---

[3] durch Beobachtung oder gezielten Angriff

[4] zu raten oder systematisch zu erzeugen

[5] Dies sind wichtige Forderungen, die sich auch formaler darstellen lassen. Problematisch ist der „Weichmacher“ „in der Regel“. Dies deutet darauf hin, dass theoretisch diese unerwünschten Situationen eintreten können, praktisch aber nie. Letztlich geht es um statistische Aussagen. Ein gutes Beispiel für die Natur solcher Aussagen liefet das Geburtstagsexperiment: Wieviele Personen muss man in einem Raum versammeln, damit die Wahrscheinlichkeit, dass es mindestens zwei Personen darunter gibt, die am gleichen Tag Geburtstag haben, eine gewisse vorgegebene Wahrscheinlichkeit übersteigt? (Man findet Literatur dazu auch unter dem irreführenden Namen „Geburtstagsparadoxon“).

4.a.7.1.1 Herkunft des Passworts

Das Einmal-Passwort wird durch eine kryptologische Operation auf einer Quelle (syn. Basis) gewonnen, die im Folgenden als Klartext bezeichnet wird.

4.a.7.1.2 Passwort aus Klartext mit Zeitstempel

Der Sender (=Zugang begehrende Person und IT-System auf ihrer Seite) generiert für jeden Zugangsvorgang den Klartext und sendet Klartext und daraus ermitteltes Passwort. Um die Gültigkeitsdauer zu begrenzen, muss er aber den Klartext mit einer Zeitangabe ergänzen, die mit in die Berechnung des Passworts eingeht. Die Zeitangabe ist Teil des Klartextes.

Damit wird verhindert, dass ein Paar „Klartext mit Passwort“ abgefangen und außerhalb der Gültigkeitsdauer wiederverwendet wird.

4.a.7.1.3 Passwort aus einem Zähler

Sender und Empfänger einigen sich zur Bestimmung des Klartexts darauf, dass ein Zähler, den man nach jedem erfolgreichen Zugangsversuch weiterzählt, verwandt wird. Beide Partner haben synchron laufende Zähler. Die Zählerstände selbst müssen nicht ausgetauscht werden, d.h. jeder Partner kennt den „aktuellen“ und daher relevanten Zählerstand.

4.a.7.1.4 Passwort aus einem Zeitstempel

Sender und Empfänger einigen sich zur Bestimmung des Klartexts darauf, einen aus der aktuellen Uhrzeit gewonnenen Zeitstempel zu verwenden, wobei sie ihre Uhren synchronisieren und ein diskretes Zeitraster (time step) wählen (etwa alle 30 sec). Der Zeitstempel muss dann zwischen Sender und Empfänger ausgetauscht werden. Beispiel: Sendet der Sender um 17:03:45 sec so nimmt er 17:03:30 als Zeitstempel, sendet er um 17:04:15 so nimmt er 17:04:00 als Zeitstempel. Der Empfänger verfährt zum Zeitpunkt, in dem er das Passwort erhält, für dessen Prüfung genauso, d.h. ermittelt die relevanten Zeitstempel (und ist dabei kulant, in dem er auch benachbarte Zeitstempel heranzieht. Dies gleicht Verzögerungen und leichte Asynchronität aus). Ein solches Verfahren ist unter dem Namen Time Based One Time Passwort – TOTP- normiert und verfügbar.

4.a.7.1.5 Challenge-Response

Der Empfänger sendet dem Sender für jeden Zugangswunsch einen Klartext als Frage, den der Sender innerhalb einer vorgegebenen Frist mit der Zusendung des Passworts beantwortet (Challenge Response - CR). Es ist sinnvoll, dass die Challenge einmalig und ein Zufallswert ist.

4.a.7.2 Kryptographische Algorithmen

Der Sender muss also zum aktuellen Klartext das Passwort berechnen und der Empfänger muss für jedes Paar (Klartext, Passwort) prüfen können, ob das Passwort korrekt ist, d.h. zum Klartext passt. Da das Passwort auch spezifisch für den Sender ist, kann der Empfänger im Fall eines korrekten Passworts auf die Authentizität des Senders schließen: Kein anderer Sender sollte in der Lage sein, aus demselben Klartext ein identisches Passwort zu produzieren.

Erreicht wird dies dadurch, dass der Sender ein nur ihm und dem Empfänger bekanntes Geheimnis verwendet (shared secret, geheimer symmetrischer Schüssel) oder ein nur dem Sender bekanntes Geheimnis. Im ersten Fall verwendet der Empfänger das gemeinsame[6] Geheimnis zur Prüfung. Im letzten Fall muss der Sender den Empfänger mit einem besonderen Mittel, einem sog. öffentlichen

Schlüssel ausstatten, mit dem er die Kennung prüfen kann (asymmetrisches Verschlüsselungsverfahren, vgl. die Gleichungen im Glossar zu „Schlüssel, asymmetrisch“).

Für die Berechnung und Prüfung gibt es also folgende Varianten:

4.a.7.2.1 Hashverfahren mit symmetrischem Schlüssel

Um ein **schlüsselabhängiges Hashverfahren** zu erhalten, wird auf sogenanntes **schlüsselunabhängiges Hashverfahren** zurückgegriffen wie z.B. SHA-1 oder Nachfolgeverfahren.

Diese Verfahren werden, um sie an den zu Authentifizierenden zu binden, mit einem Schlüssel versehen, d.h. in die Berechnung des Hashwerts geht ein Schlüssel ein. Damit wird also ein sog. „schlüsselabhängiges Hashverfahren“ genutzt.

Solche Verfahren könnten einfach dadurch gewonnen werden, dass man an den Klartext noch den Schlüssel anhängt, bevor der Hashwert ermittelt wird. Ein solches „naives“ Verfahren ist jedoch angreifbar.

Besser ist es den sog. HMAC zu verwenden, der den Schlüssel und den Klartext in sehr spezieller Weise mit der schlüsselunabhängigen Hashfunktion kombiniert.

4.a.7.2.2 Digitale Signatur

Die digitale Signatur ist ein Spezialfall der elektronischen Signatur.

Für die Elektronische Signatur wird der Klartext signiert, d.h. es ist ihm eine Signatur beigefügt. Die Signatur ist eine aus dem Klartext errechnete Zeichenfolge, die spezifisch für den Klartext **und** den Sender ist. Der Empfänger erhält den Klartext und Signatur.

Für die digitale Signatur errechnet man aus dem Klartext einen sog. Fingerabdruck (finger print). Der Fingerabdruck ist der Hashwert, der sich durch Anwendung eines schlüsselunabhängigen Hash-Verfahrens aus dem Klartext ergibt. Anschließend wird ein asymmetrisches Verschlüsselungsverfahren eingesetzt: Der Fingerabdruck wird mit dem privaten Schlüssel des Senders (hier des sich anmeldenden Endnutzers) verschlüsselt. Das Ergebnis ist die Digitale Signatur. Sie hat hier die Funktion des Passworts. Ist der Klartext nur einmal zu verwenden, hat man damit ein Einmal-Passwort.

Der Empfänger (hier der Authentikator) berechnet ebenfalls einen Fingerabdruck (nach dem gleichen Verfahren wie der Sender) aus dem Klartext. Er entschlüsselt mit Hilfe des öffentlichen Schlüssels des Senders den erhaltenen verschlüsselten Fingerabdruck. Sind beide Fingerabdrücke gleich, kann der Empfänger von der Authentizität der Nachricht, d.h. des signierten Klartextes, ausgehen.

4.a.7.2.3 Anforderungen an die Algorithmen

4.a.7.2.3.1 Perspektive des Angreifers

Die oben angesprochenen Verfahren sollten mindestens gegen einen Angreifer sicher sein, der die Kommunikation nur beobachtet und dann mit Rechnerunterstützung das Verfahren brechen will, in dem er Schwächen eines Algorithmus nutzt. Man wünscht also mindestens eine gewisse „mathematische“ Sicherheit. Es sind also Angriffe zu unterscheiden, die immer und gegen jedes

[6] im deutschen Sprachgebrauch heißt dies auch oft ein „geteiltes Geheimnis“ im Sinne eines Teilens mit einem anderen.

System durchführbar sind, als „unspezifisch“ sind, von solchen, die Schwachstellen der Algorithmen ausnutzen. Das Beobachten und Einspielen beobachteter Passwörter ist ein unspezifischer Angriff.

Ein Angreifer kann im hier vorliegenden Szenario unterschiedliche Ziele haben:

(1) Im Idealfall kann er selbst zu beliebigen Klartexten Passwörter erzeugen, d.h. je nach Verfahren zu beliebigen Zählerständen, Zeitstempeln, Challenges. Damit ist er Herr des Verfahrens.

Der Angreifer kann auch bescheidener sein:

(2) Annahme: Der Angreifer kennt ein Paar, bestehend aus Klartext und Passwort. Dies könnte er durch Beobachtung erlangt haben. Wenn es ihm gelingt einen weiteren Klartext zu finden, der zum selben Passwort führt (Kollision), so kann er daraus bereits einen Vorteil ziehen. Er dann dieses Passwort im Kontext des zweiten Klartextes verwenden, um dem Empfänger zu suggerieren, es gehöre zum diesem, dem zweiten Klartext.

Es mag für den Angreifer eine Herausforderung sein, für einen gegebenen Klartext einen weiteren zu konstruieren, der zum gleichen Passwort führt. Der Angreifer kann aber noch bescheidener sein:

(3) Falls es ihm gelingt zwei Klartexte zu finden, die zum selben Passwort führen (Kollision), so kann er daraus bereits einen Vorteil ziehen.

Der Angreifer kann den Berechtigten beobachten, wie er aus dem einen Klartext das Passwort produziert, kann dieses Passwort für sich notieren und dann dieses Passwort im Kontext des zweiten Klartextes verwenden, um dem Empfänger zu suggerieren, es gehöre zum diesem, dem zweiten Klartext.

Beispiel: Falls der Angreifer zwei Zeitstempel, und damit Zeitpunkte kennen würde, denen dasselbe Passwort zugeordnet würde, so kann er den ersten dieser Zeitpunkte abpassen, das vom Berechtigten dort verwendete Passwort beobachten und notieren und dann anschließend zum zweiten Zeitpunkt – er liege später - sich selbst als Berechtigter generieren, indem er das notierte Passwort dem Empfänger zum zweiten Zeitpunkt zukommen lässt. Eine bessere Position hat der Angreifer, wenn er nicht nur auf eine Beobachtung angewiesen ist, sondern, wenn er den Berechtigten veranlassen kann, das Passwort zum einem der beiden Klartexte zu bilden. Dann kann er das Passwort „abzweigen“ und mit „seinem“ Klartext verwenden.

Es muss nochmals betont werden, dass der Angreifer in diesen Szenarien (2) und (3) selbst nicht in der Lage ist, das Passwort aus dem Klartext so zu berechnen, wie der Berechtigte, sondern darauf angewiesen ist, dass der Berechtigte die Berechnung sozusagen „für ihn“ durchführt.

4.a.7.2.3.2 Brute Force Angriff

Der Angriff hat das Ziel, sich durch Ausprobieren Kenntnis davon zu verschaffen, welche Klartexte auf vorgegebene Passwörter abgebildet werden. Der Angriff dient damit der Entdeckung der Umkehrfunktion. Im Speziellen findet der Angreifer dadurch Kollisionen.

Der Angreifer kann für das Probieren den Berechtigten einsetzen, indem er ihn veranlasst, aus Klartexten Passwörter zu erzeugen. Der Angreifer kann auch selbst diese Berechnung vornehmen, da der Algorithmus bekannt ist, muss aber dann den zu verwendenden Schlüssel „raten“. (Zur Erinnerung: Es geht immer ein geheimer Schlüssel in die Berechnung ein.) Das Verfahren ist aufwendig, da alle Klartexte „probiert“ werden müssen. Der Angreifer wird dies dadurch optimieren, indem er sich alle relevanten Passwörter bzw, alle möglichen Passwörter besorgt. Bei jedem Test sieht der Angreifer nach, welchen Treffer er in der Menge der möglichen Passwörter findet – es kann nur einen geben.

Wählt der Angreifer nur ein „Sample“ möglicher Klartexte anstatt Klartexte systematisch „auszuprobieren“, so führt er einen sog. „Geburtstagsangriff“ durch.

Wie erwähnt müsste der Angreifer dieses Ausprobieren aller Klartexte für jeden Schlüssel durchführen. Kennt er den Schlüssel, kommt es für den Aufwand nur auf die Größe der Klartextmenge an.

4.a.7.2.3.3 Geburtstagsangriff

Der Begriff stammt aus der folgenden Fragestellung: Wie viele Personen müssen in einem Raum versammelt sein, dass mit einer gewissen Mindest-Wahrscheinlichkeit (z.B. ½) mindestens zwei Personen am gleichen Tag Geburtstag haben.

Dem entspricht: Wie viele Klartexte sind nötig, dass mit einer gewissen Mindest-Wahrscheinlichkeit (z.B. ½) mindestens zwei Klartexte auf dasselbe Passwort abgebildet werden, d.h. zu einer Kollision führen?

Die Zahl möglicher Passwörter, die Zahl der Klartextwahlen und die Wahrscheinlichkeit von Kollisionen hängen zusammen.

Ziel der Abwehr von Angriffen ist es die Zahl möglicher Passwörter so einzurichten, dass auch die Kollisions-Wahrscheinlichkeit von ½ (also wie ein Münzwurf) nur mit einer extrem hohen Zahl an zufällig gewählten Klartexten erreicht werden kann.

4.a.7.2.3.4 Abgeleitete Anforderungen

Die Anforderungen an das Verfahren korrespondieren mit Zielen des Angreifers. Eine „starke“ Forderung blockiert auch Angriffe, für die der Angreifer wenig Anstrengungen unternehmen muss.

(1) Der Angreifer darf praktisch nicht in der Lage sein, ohne Kenntnis des Schlüssels aus einem Klartext das Passwort zu errechnen.

(zu „praktisch in der Lage sein“ siehe unten).

(2) („One-Way“)

Es ist zu fordern, dass es praktisch nicht möglich ist, aus einem beliebigen vorgegebenen Passwort die Klartexte zu errechnen, die in der Berechnung zu diesem Passwort als Ergebnis führen.

Könnte der Angreifer bei gegebenem Passwort den zugehörigen Klartext oder die zugehörigen Klartexte ermitteln, sind alle Wünsche des Angreifers zur Ermittlung von Kollisionen erfüllt: Dabei ist es nicht wichtig, dass er den Klartext in Erfahrung bringt, denn es geht hier nicht um die Sicherung der Vertraulichkeit des Klartexts. Kann der Angreifer aber alle Klartexte zu einem Passwort ermitteln, kann er damit auch Kollisionen ermitteln und nutzen (siehe oben).

Aber selbst, wenn dies gewährleistet ist, könnte es dennoch eine Möglichkeit für den Angreifer geben, Kollisionen zu konstruieren. Daher:

(3) („schwache Kollisionsresistenz“)

Man muss fordern, dass es dem Angreifer praktisch nicht möglich ist, zu einem vorgelegten Klartext einen anderen Klartext zu finden, der zum selben Passwort führt.

Aber selbst, wenn dies gewährleistet ist:

(4) („starke Kollisionsresistenz“)

Man muss weiter fordern, dass es dem Angreifer praktisch nicht möglich ist, zwei Klartexte zu finden, die zum selben Passwort führen.

Alle diese Forderungen müssen erfüllt sein.

4.a.7.2.3.5 „Praktisch nicht möglich“

„Praktisch nicht möglich“ heißt, dass es dem Angreifer nicht möglich ist, mit vertretbarem Aufwand mit ausreichend hoher Wahrscheinlichkeit sein Angriffsziel zu erreichen. Dies ist eine statistische Aussage (vgl. Geburtstagsangriff).

4.a.7.2.3.6 Wahl von Parametern

Die IT-Abteilung als fachlich zuständige Abteilung muss Parameter des Verfahrens so wählen, dass spezifische Angriffe praktisch ausgeschlossen sind.

4.a.7.3 Kombinationen von Passwortgewinnung und Berechnung

Die Herkunft der Klartextes eines Passworts (d.h. ob dies eine frei gewählte Zeichenkette ist, die mit einem Zeitstempel versehen wurde, oder ein Zähler, ein Zeitstempel oder eine freigewählte Zeichenkette ist, die beantwortet werden muss), ist unabhängig von der Frage mit welchem Verschlüsselungsverfahren das Passwort gewonnen wurde und wie es dann zu validieren ist.

Daher lassen sich Verfahren auch kombinieren.

(vgl. Sciarerreta G. et.al. Formal Analysis of Mobile Multi-Factor Authentication with Single Sign On, in:ACM Transactions on Privacy and Security Vol. 23, No.3 Article 12,page 13:5 “and the prover answers with a valid response obtained by performing an established operation (such as hashing the challenge with a secret or applying a private key operation).”

Dies gilt nicht nur für CR sondern für jedes Passwort, das aus einem Klartext berechnet wird. Man beachte allerdings, dass man für das TOTP-Verfahren eben einen symmetrischen Schlüssel verwendet.

	Symmetrisch (shared secret)	Asymmetrisch (public/private key)
Klartext mit Zeitstempel		
Zählerbasiert (Hashbased One Time Password - HOTP)		
Zeitbasiert (Time based One Time Password - TOTP)	HS LA	
Frage-Antwort (Challenge Response -CR)		HS LA

Es könnte also auch ein Zeitstempel mit einer digitalen Signatur „unterschrieben“ werden – aber dieses Verfahren ist nicht üblich. Üblich ist der Einsatz der Digitalen Signatur für ein Challenge Response Verfahren. Möglich wäre aber, dass der Prover Klartexte zufällig generiert, mit Zeitstempel versieht und dann digital signiert oder (nur) mit einem Hashverfahren verarbeitet.

4.a.7.4 Phasenmodell

Initialisierung

Beweisführender (Prover) und Authentifizierer müssen sich auf ein Authentisierungsverfahren verständigen und für das Verfahren nötige Information auf Dauer austauschen. Diese Phase der Verständigung ist die „Initialisierung“ (enrollment).

Zugangsvorgänge

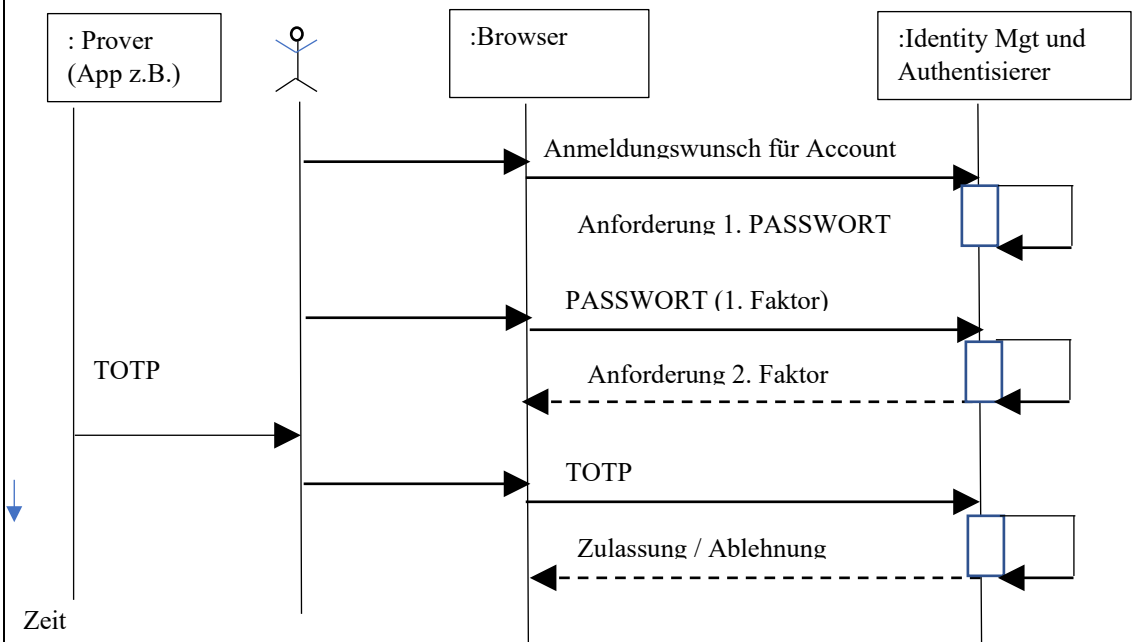
Die Phase der Authentifizierungen (Plural!) zerfällt in Aktivitäten, in denen der Client jeweils einen Zugang bzw. Zugriff begehrt (hier: Anmeldung, allgemein: Zugriff auf ein Betriebsmittel, Information etc.) und jeweils seine Identität nachweisen muss. Es kann sehr unterschiedliche Arten von Zugriffen geben. Gemeinsam ist allen hier betrachteten Zugriffen, dass sie eine Authentifizierung voraussetzen. Zugriffe, die ohne Authentifizierung erlaubt sind, kann es auch geben, aber sie sind für die Anmeldungssituation nicht relevant.

4.a.7.4.1.1 TOTP – Initialisierung

Es muss das gemeinsame Geheimnis („shared secret“) ausgetauscht werden. Der Authentikator generiert das shared secret und sendet es an den Nutzer (User agent). Es muss dem Prover zum Zweck der Generierung von Passworten zu Verfügung gestellt werden.

4.a.7.4.2 TOTP - Zugangsvorgang

Ablauf bei TOTP (nur Zugangsvorgang)



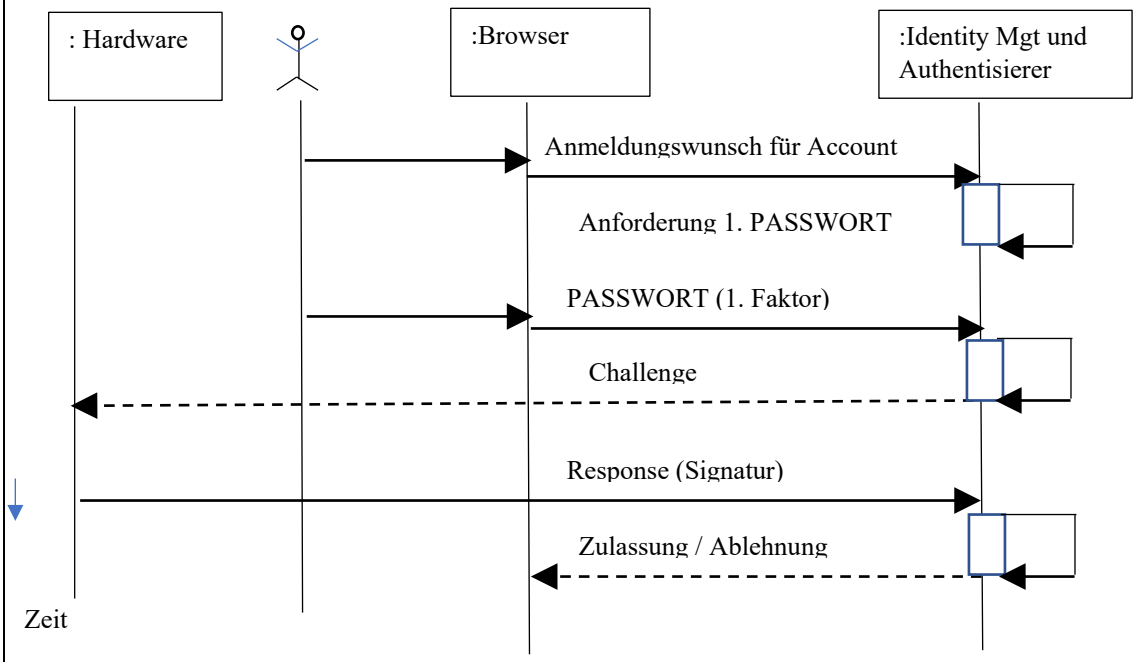
Besonderheit: Der Nutzer selbst muss das Passwort (TOTP) ablesen und eingeben.

4.a.7.4.2.1 CR – Initialisierung

Auf Seite des Nutzers wird ein Schlüsselpaar generiert. Der private Schlüssel verbleibt beim Nutzer. Der öffentliche Schlüssel wird (als Zertifikat) dem Authentikator mitgeteilt.

4.a.7.4.2.2 CR - Zugangsvorgang

Ablauf bei CR (nur Zugangsvorgang)



4.a.8 Praxis der Hochschule Landshut

Die 2-Faktor-Authentisierung ist ein Verfahren zur Identitätsbestätigung, welches sich, dem Namen entsprechend, zweier Faktoren bedient:

1. Faktor - Wissen: Benutzername und Passwort Ihres Hochschulaccounts.
2. Faktor - Besitz: Sie verfügen entweder über ein Mobiltelefon, auf welchem sich eine App befindet, mit der Sie Ihnen zugesandte sogenannte „Tokens“ scannen können oder Sie erwerben ein sogenanntes Hardware-Token, in unserem Fall einen Yubico-Security Key (U2F-Security-Key) oder eine in der Funktion vergleichbare Hardware.

Anmerkung: Da das App-Verfahren nicht an ein bestimmtes Smartphone gebunden ist, lässt sich daran zweifeln, ob dies wirklich ein Faktor des „Besitzes“ ist.

Beide Verfahren dienen dazu den zweiten Faktor der Authentifizierung zu sichern:

(1) TOTP:

Die Applikation „HAW LA TOTP“ (im Folgenden als „App“ bezeichnet) wurde entwickelt zum Scan von QR-Codes und der daraus resultierenden Erzeugung eines Authentisierungstokens. Bestandteil des Authentisierungstokens ist das „zeitbasierte Einmalpasswort“ („TOTP“, en.: „Time-Based One-Time Password“).

Um das Verfahren der Zwei-Faktoren-Authentifizierung in der digitalen Form durchzuführen, benötigen Sie ein Smartphone. Sie müssen eine App, die von der Hochschule Landshut bereitgestellt wird aus einem Appstore auf Ihr Smartphone herunterladen. Alternativ sind die Apps FreeOTP oder GoogleAuthenticator zu empfehlen.

Die App wird im Android App Store (Google Play Store) oder im Apple App Store zur Verfügung gestellt.

Rechtlicher Hinweis: Die Nutzung der Stores unterliegt der Vereinbarung zwischen den Store-Betreibern und Ihnen. Die Hochschule Landshut ist nicht Partei einer solchen Vereinbarung und hat keinen Einfluss auf die Datenverarbeitung seitens der Stores.

Als zweiten Faktor nutzt sie in einem Verfahren ein Zeitabhängiges Einmal-Passwort (Time-Based One-Time Password - TOTP), das der Nutzer nach der Anmeldung mit dem klassischen Passwort vorweisen muss. Der Konstruktion dieses Passworts liegt ein gemeinsames Geheimnis (s.u) zugrunde. Das Einmal-Passwort wird mittels einer App berechnet, die der Nutzer auf sein Smartphone laden muss. Die Anmeldung selbst erfolgt mit dem Personal Computer (auch Desktop, Laptop)

(2) U2F mit Security Key (Security Key)
Dieses Verfahren (kurz: U2F Security Key) arbeitet nach der FIDO 2 Spezifikation, indem serverspezifisch mit der Security Key-Hardware ein Schlüsselpaar, bestehend aus private und public key generiert wird, wobei der private key in der Hardware geschützt gespeichert wird.
Der Server erhält den öffentlichen Schlüssel.

4.a.8.1 Eingesetzte Software

PrivacyIDEA: „privacyIDEA“ ist eine Software, die auf einem LINUX-Rechner der HS LA läuft (genauer: eine Software-Instanz der Open Source Software privacyIDEA auf einem (virtualisierten) Server mit dem Betriebssystem LINUX, der im RZ der HS LA installiert ist).

Shibboleth ist das implementierte Identitätsmanagementsystem (Identity Provider).

Für die Kommunikation mit dem Yubico-Security Key wird in Shibboleth, dem an der Hochschule eingesetzten Identitätsmanagementsystem, ein Plug-In eingesetzt.

4.a.8.2 Begriff des „Token“

Die Hochschule Landshut lässt die beiden genannten Verfahrenstypen „TOTP“ und „U2F mit Security Key“ zu.

Will man ein Verfahren eines bestimmten Typs anwenden, benötigt man für die Durchführung gewisse Daten, z.B. einen Schlüssel und die Festlegung, wie lange ein Passwort gültig sein soll und vieles mehr. Diese Daten werden in einer Datenstruktur verpackt, die man „Token“ (auch: „Authentisierungstoken“) nennt. Man erhält einen strukturierten Wert.

Der Begriff Token wird in IT-Texten oftmals auch noch für anderes verwandt, aber wir nehmen ihn für die Datenstruktur, wenn wir nichts anderes sagen. Daher verwenden wir folgenden Tokenbegriff: Wenn im Folgenden von einem Token die Rede ist, so ist damit ein strukturierter Wert gemeint.

4.a.8.2.1 Tokenarten

Unterschiedliche Verfahren verlangen Token einer unterschiedlichen Art. Die Tokenarten unterscheiden sich in der Struktur. Hier gibt es Registrierungstoken, TOTP-Token und U2F-Token.

4.a.8.2.1.1 Registrierungstoken

Dieser Token wird nur für die erstmalige Anmeldung benötigt. Es wird per Mail zugesandt und ist nur einmal benutzbar.

4.a.8.2.1.2 TOTP-Token

Will man TOTP erzeugen, benötigt man ein sog. TOTP-Token. Das TOTP-Token steuert die Generation der TOTP, d.h. zu einem TOTP-Token gehört, wenn die Erzeugung der TOTP läuft, zu jedem Zeitpunkt ein TOTP. Man kann sich die App auf dem Smartphone als Maschine vorstellen, die gesteuert von einem TOTP-Token ständig TOTPs erzeugt, sagen wir alle 30 sec oder 60 sec ein neues TOTP. Man sieht dann auf der App ein Fenster mit ständig (alle 30 sec oder 60 sec) wechselndem TOTP.

Hat man mehrere TOTP-Token auf das Smartphone übertragen, dann wird die App für alle TOTP-Token permanent TOTPs erzeugen. Annahme: Wir hätten drei TOTP-Token. Man sieht dann drei Fenster, in denen ständig neue TOTP erscheinen.

Eingabe des TOTP erfolgt in den Browser am Desktop.

Zur Anmeldung muss man jetzt ein TOTP eingeben, das man vom Smartphone abliest. Man sollte natürlich nicht zu lange warten, denn nach 30 sec oder 60 sec wird das TOTP ungültig. Hat man nur ein TOTP-Token auf dem Smartphone, dann muss man das eine angezeigte TOTP nehmen.

Irgendetwas anderes einzugeben, führt zum Fehlschlag der Anmeldung.

Hat man mehrere TOTP Token, so hätte man die Auswahl zwischen den, sagen wir, drei TOTP. Es ist völlig gleichgültig, welches man nimmt – eines von den dreien muss es sein. Es sollte allerdings nur ein TOTP von einem noch aktiven TOTP-Token sein.

4.a.8.2.1.3 U2F-Token

Will man mit dem Security Key arbeiten, dann benötigt man ein U2F-Token.

4.a.8.2.1.4 Andere Token

Für andere Verfahren benötigt man Token einer anderen Art.

4.a.8.3 Token-Liste und Tokenprofil

Da man sowohl mit TOTP- als auch mit U2F-Security Key - Verfahren arbeiten kann, kann es dazu kommen, dass man einen Token-Mix aus Token diverser Arten anhäuft, z.B. einige TOTP-Token, ein U2F-Token und das Registrierungstoken. Damit man da nicht verwirrt wird, kann man in seinem Token-Profil nachsehen, welche Token man hat und von welcher Art diese sind. Das Tokenprofil eines Nutzers ist eine Liste der Token, die er hat. Jedes Token hat seine Identifikation. Die Tokenliste bekommt man vom Authentikator bei der Anmeldung. Es kann darunter Token geben, die schon deaktiviert sind.

Ein Tokenprofil könnte so aussehen:
REG012345678
TOTP34567865

TOTP567875657
U2F5654578888

4.a.8.4 Token-Liste auf der App

Die App führt alle aktuellen TOTP-Token. Andere machen auf der App keinen Sinn. Die iOS-App verfügt über keine Auflistung, da lediglich ein einziger Token gespeichert wird.

4.a.8.5 Registrierung

Gleichgültig, welches Verfahren Sie einsetzen, besteht folgende Schwierigkeit: Bei der ersten Anmeldung haben sie keine Token (siehe oben). Sie benötigen für die erste Anmeldung ein sog, Registrierungstoken. Es wird Ihnen via e-mail zugesandt. Sie müssen ein 24-stelliges Passwort bei der Anmeldung als 2. Faktor eingeben.

4.a.8.6 Zugangs-Variante mit Einsatz einer App

Das Verfahren ist ein zeitbasiertes Verfahren (nach rfc6228: Time based One Time Password - TOTP und rfc 4226 HMAC based One Time Password), in dem mittels eines Hashverfahrens (HMAC) verschlüsselt („gehasht“) werden, und zwar einerseits von der App auf Ihrem Smartphone und andererseits vom Server (der HS Landshut). Der Server überprüft die ihm gesandten Hashes von Zeitpunkten durch eigene Hashes und prüft damit die Authentizität.

Beim diesem „Hashing“ wird ein geheimer Schlüssel benutzt, d.h. das Ergebnis, die erzeugten Hashes, hängt von diesem Schlüssel ab.

Also:

hash(time, key) ist das Ergebnis, der sogenannte Hashwert (auch „Hashcode“),

time ist die aktuelle Zeit (aus einem diskreten Zeitraster),

key ist der geheime Schlüssel.

App und Server teilen sich das Geheimnis, d.h. sie nutzen beide den gleichen geheimen Schlüssel (shared secret). Diesen Schlüssel mussten sie vorher ausgetauscht haben.

Solange sie das gleiche Geheimnis nutzen, erzeugen App und Server für den gleichen Zeitstempel den gleichen Hashwert. Darauf beruht die Authentifizierung: Bekommt der Server für den Zeitpunkt, sagen wir t1, den Hashwert von der App, den er selbst für diesen Zeitpunkt t1 errechnet, dann kann er sicher sein, dass die App mit dem gleichen Geheimnis gerechnet hat wie er selbst. Da die App also das Geheimnis kennt, wird sie für authentisch gehalten.

Dass ein Hashverfahren zur Verschlüsselung benutzt wird, ist entscheidend für die Sicherheit.

Das Hashverfahren sichert, dass bei Verwendung eines anderen Schlüssels für den gleichen Zeitstempel auch mit hoher Wahrscheinlichkeit ein anderer Hashwert erzeugt wird. Einen Schlüssel zu konstruieren, der für einen Zeitstempel zum gleichen Hashwert führt, ist nicht mit vertretbarem Aufwand möglich (Näheres findet man in der Literatur zum Stichwort „Kollisionsfreiheit“)

App und Server müssen dazu zeitlich synchronisiert werden. Damit das Verfahren funktioniert, legt man ein diskretes Zeitraster zugrunde, z.B. schaltet die Zeit alle 30 sec fort. Der Server prüft auch nicht nur gegen einen Zeitpunkt, sondern gegen die Hashcodes unmittelbar zurückliegender Zeitpunkte.

4.a.8.6.1 Initialisierung

Das Geheimnis wird in einer Initialisierungsphase vom Nutzer angefordert, indem dieser ein neues TOTP-Token anfordert. Vorsorglich sei nochmals erwähnt, dass das TOTP-Token nicht mit dem TOTP selbst verwechselt werden sollte.

Das TOTP-Token wird vom Authentikator übertragen. Es kann intern als Zeichenkette codiert werden.

Es wird am Bildschirm als QR-Code dargestellt.

Der Nutzer teilt dieses Geheimnis der App mittels einer Aufnahme durch die Smartphone-Kamera mit.

Die App führt eine Plausibilitätsprüfung des QR-Codes durch, rekonstruiert das TOTP-Token und extrahiert die wichtigen Bestandteile.

Obwohl das TOTP-Token, das das shared secret enthält unterschiedlich dargestellt (syn. „codiert“) wird, ist es nicht verschlüsselt. Jeder, der die Struktur des Tokens kennt, kann diese unterschiedlichen Darstellungen nutzen, um sich in den Besitz des shared secret zu bringen.

4.a.8.6.2 Zugangsvorgang

Der Authentifizierungsvorgang läuft wie folgt:

Für jedes auf der Android-App befindliche TOTP-Token:

- Jedes TOTP-Token ist als eine Maschine zu sehen, die fortlaufend neue TOTP (Passwörter) generiert. Die App nimmt dazu aktuelle Zeit und bildet daraus den Hashwert mit Hilfe des HMAC-<Basis>-Verfahrens unter zu Hilfenahme aller Parameter des TOTP-Tokens. Tatsächlich ist das TOTP ein strukturierter Wert, der auch Angaben über seine Generierungszeit (generated) und seine Gültigkeit (expires) enthält. Jedem TOTP-Token ist also zu einem Zeitpunkt ein aktuelles TOTP zugeordnet und eine Timer, der zeigt, wie lange dieses TOTP noch gültig ist. Der Timer wird abwärts gezählt, bis das TOTP wechselt. <Basis> meint das zugrundeliegende schlüsselunabhängige Hashverfahren.

Der Nutzer kann nun eines der TOTP nehmen, die er auf seinem Smartphone in der App sieht. Es kann sein, dass er mehrere Token hat und damit mehrere TOTP sieht (Anmerkung: in der iOS-Version der App wird lediglich ein einziges TOTP-Token gespeichert). Wichtig ist, dass der Nutzer nun eines der TOTP nehmen kann und am Personal Computer eingeben kann – er war ja aufgefordert ein TOTP zu nennen.

Der Desktop/Browser sendet diesen Hashwert an den Server. Der Authentikator (hier: privacyIDEA) empfängt den Hashwert, bildet seinerseits den Hashwert der aktuellen Zeit (wir nehmen an, dass er auch die aktuelle Zeit hat). Auch er nutzt das gemeinsame Geheimnis. Dann werden die beiden Hashwerte verglichen. Falls diese identisch sind, hat der Server die Gewissheit, dass die App das gleiche Geheimnis verwendet hat.

4.a.8.7 Zugangs-Variante U2F-Security-Key

Der Security Key ist Hardware, die am Rechner eingesteckt wird (wie ein USB-Stick).

4.a.8.7.1 Initialisierung

Der Security Key generiert ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel bleibt in der Hardware verborgen.

Der Server erhält den öffentlichen Schlüssel.

4.a.8.7.2 Zugangsvorgang

Die Authentifizierung findet über ein Challenge-Response Verfahren statt, in dem der Server eine Zufallszahl generiert, diese an den Security Key sendet, dieser die Zahl mit Hilfe des privaten Schlüssels signiert („unterschreibt“), die signierte Zahl zurücksendet und der Server die Signatur mit Hilfe des öffentlichen Schlüssels prüft.

Es ist allerdings eine Nutzer-Interaktion nötig, d.h. der Nutzer muss den Security Key durch einen Tastendruck veranlassen, die Antwort auf die Challenge zu generieren.

Wenn die Signaturprüfung erfolgreich war, dann kann der Server davon ausgehen, dass der private Schlüssel des Senders (bzw. seines Security Key) zum öffentlichen Schlüssel passt. Damit ist derjenige, der den öffentlichen Schlüssel vorgewiesen hat, authentifiziert.

Der Vorgang „Digitale Signatur“ in einem Public-Key-System wird vielfach in Lehrbüchern beschrieben und ist dort nachlesbar. Gleiches gilt für „Zertifikate“. Es werden also Standardverfahren eingesetzt. Die Besonderheit hier ist das Challenge-Response-Verfahren und die Verwendung von Hardware zur Schlüsselgenerierung.

4.a.8.8 Schwachstellen und Risiken

4.a.8.8.1 Kryptographische Algorithmen

Obwohl die verwandten Algorithmen im Prinzip eine mathematisch sichere Verarbeitung gestatten, hängt die Sicherheit

(a) von der Korrektheit der math. Modelle

(b) Korrektheit der Implementierung der Algorithmen

(c) richtiger Wahl der Parameter

ab.

Dies verantwortet die IT-Abteilung der Hochschule Landshut. Eine Zertifizierung von math. Modellen und Implementierung fand nicht statt.

zu a) Es wird für das TOTP-Verfahren, soweit die Android-App der Hochschule Landshut verwendet wird, kein HMAC-SHA-1 zugelassen, da die Kollisionsresistenz von SHA-1 nicht gegeben ist. Die iOS-Version der App verwendet ausschließlich HMAC-SHA-1.

Das shared secret wird als Zufallszahl erzeugt.

Die Challenge des U2F-Verfahrens ist eine Zufallszahl.

zu c) Es sei darauf hingewiesen, dass die Sicherheit von der Wahl der Parameter abhängt, wie z.B.

- Länge der generierten Passwörter
- Länge des „shared secret“ (mindestens: 128)
- Länge von private und public key
- Länge des Zeitintervalls
- Zahl tolerierter Fehlversuche

- Fensterbreite für TOTP-Test

4.a.8.8.2 Mangelnder Schutz des Registrierungstokens

Das Registrierungstoken wird durch ungeschützte Mail übertragen und ist daher für Angreifer leicht zugänglich.

4.a.8.8.3 Kein Besitz im Fall der App-Variante

Da die App nicht an das Smartphone gebunden ist, auf dem sie installiert ist und auch jede beliebige andere Implementierung des TOTP-Generierungsverfahrens genutzt werden kann, besteht keine Abhängigkeit von einem Gegenstand im Besitz des Nutzers. Das shared secret ist nicht auf einem gesonderten Gerät geschützt.

4.a.8.8.4 Mangelnder Schutz des „shared secret“

Das shared secret kann durch Angriffe auf die Kommunikation Authenticator – Browser gewonnen werden.

Das shared secret kann durch Angriffe auf den Browser gewonnen werden.

Das shared secret wird als QR-Code am Bildschirm sichtbar und kann auch von einem Angreifer fotografiert werden.

Wer das shared secret kennt, kann beliebig wie ein Berechtigter agieren.

4.a.8.8.5 Freie Wahl von Parametern durch den Nutzer

Der Nutzer kann das Intervall (time step), die Länge des Passworts und das Basishashverfahren für den HMAC wählen.

4.a.8.8.6 Freigabe der Kamera für die App

Wie jegliche Kamerafreigabe an eine App, schafft auch diese das Risiko, dass auch andere Apps zugreifen bzw. auch für andere Apps freigegeben wird oder die Freigabe nicht mehr zurückgenommen wird.

4.a.8.8.7 Keine Unabhängigkeit des Authentisierungsmittel in der App-Variante

Das wesentliche Element der 2-Faktoren-Authentisierung, die Unabhängigkeit der Faktoren ist hier nicht gegeben. Ein Angreifer, der Herrschaft über den Personal Computer des Nutzers erlangt, hat den 1. Faktor wie auch den zweiten Faktor (in Form des shared secret) zur Verfügung. Diese Situation besteht bei Einsatz eines Hardware-Token nicht.

4.a.8.8.8 Möglichkeit der Software-Manipulation

Weder die Server-Software (privacyIDEA) noch die herunterzuladende App sind gegen Manipulation von außen geschützt.

4.a.8.8.9 Usability/Benutzerfreundlichkeit

Wie bei allen 2-Faktorenlösungen steigt der Aufwand für den Nutzer.

4.a.8.8.10 Fazit

Während die Hardware-Lösung sicher erscheint, ist der Gewinn an Sicherheit durch die App-Lösung mäßig. Dies wirft die Frage nach der Zweckmäßigkeit der Lösung auf, die aber nicht aus Sicht des Datenschutzes zu beantworten ist.

4.b Rechtsgrundlage

4.b.1 Verarbeitung der Daten durch die Hochschule Landshut

4.b.1.1 Personenbezogene Daten (Art. 4 Nr. 1, EG 26 DSGVO)

4.b.1.1.1 Daten des Portals

Das Zugangsverfahren dient dem Schutz personenbezogener Daten, die der Studierende aus dem Portal abrufen kann.

4.b.1.1.2 Daten des Zugangsverfahrens

Personenbezogene Passwörter und Schlüssel und nicht-personenbezogene Klartexte wie Uhrzeiten oder Zählerstände, sowie Challenges werden verarbeitet.

4.b.1.1.3 Technische Daten der Kommunikation

Es werden die IP-Adresse und der Zeitpunkt ihrer Nutzung, sowie technische Daten des Desktops (Betriebssystem, Browsereinstellungen) an die Hochschule übertragen.

4.b.1.2 Rechtsgrundlage

Rechtsgrundlage ist Art. 6 Abs. 1 Buchstabe e, Abs. 2 und 3 DSGVO iVm Art. 32 DSGVO in Verbindung mit Art. 4 Abs. 1 BayDSG in Verbindung mit der Aufgabenstellung der Hochschule. Hierzu gehört die Organisation der Kommunikation mit den Studierenden und damit das Anmeldeverfahren zum Portal. Die Verarbeitung ist ein angemessenes Mittel zum Schutz der personenbezogenen Daten des Portals (Art. 32 DSGVO):

4.b.2 nachrichtlich: Verarbeitung personenbezogener Daten im Appstore

Diese Verarbeitung liegt außerhalb der Verantwortung der Hochschule Landshut.

Art und Umfang der Verarbeitung personenbezogener Daten durch den Appstore-Betreiber werden in der Nutzungs-Vereinbarung zwischen Appstore-Betreiber und dem Betroffenen, der die App der Hochschule aus dem Appstore herunterlädt, geregelt.

Rechtsgrund für diese Datenverarbeitung kann sein Art. 6 Absatz 1 Buchstabe b DSGVO (Vertrag) oder, falls eine Einwilligung eingeholt wird, Art. 6 Absatz 1 Buchstabe a DSGVO oder ein gem. Art. 6 Abs. 1 Buchstabe f , ein berechtigtes Interesse des Appstore-Betreibers. Das Nähere ergibt sich aus den Geschäftsbedingungen des Appstore-Betreibers.

5 Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

Die spezifisch für den Zugang erhobenen und generierten Daten erhält ausschließlich die Hochschule Landshut bzw. deren Systeme, soweit die Daten überhaupt den Herrschaftsbereich des Betroffenen verlassen. „Private Schlüssel“ verbleiben beim Betroffenen. Die App erhält im Rahmen des Zugangsverfahrens weder über ein Netz von der Hochschule Daten des Betroffenen noch übermittelt sie an die Hochschule Daten des Betroffenen. Falls der Betroffene allerdings Informationen mit Hilfe der App von der Hochschule anfordert (wie z.B. Datenschutzhinweise), so wird in der üblichen Weise eine Verbindung zur Hochschule etabliert. Bei der Anmeldung am Desktop werden neben Passwörtern Daten an die Hochschule übertragen, wie sie der Einsatz des Protokolls TCP/IP verlangt. Die Hochschule setzt im Rahmen des Zugangsverfahrens nur Cookies im Browserspeicher des Betroffenen, die für die Funktion des Zugangs notwendig sind.

Die Hochschule Landshut setzt keine Auftragsverarbeiter ein. Der Betreiber des Appstores (wie z.B. Google Playstore, Apple-Appstore) ist kein Auftragsverarbeiter der Hochschule Landshut. Die Hochschule Landshut sieht sich auch nicht in einer gemeinsamen Verantwortung (Art. 26 DSGVO) mit dem Betreiber des Appstore und sieht keine Ähnlichkeit der hiesigen Sachverhalts mit dem vom EuGH in der Rechtssache „Facebook-Fanpage“ entschiedenen.

6 Übermittlung von personenbezogenen Daten an ein Drittland

Weder in Registrierungsphase, Initialisierungsphasen noch bei den Zugangsvorgängen findet eine Übertragung seitens des Verantwortlichen von personenbezogenen Daten des Betroffenen in ein Drittland statt, ausgenommen der Betroffene versucht den Zugang zum Portal aus einem Drittland zu erlangen.

7 Dauer der Speicherung personenbezogener Daten

Die personenbezogenen Daten des Zugangsverfahren werden maximal für die Dauer der Mitgliedschaft zur Hochschule, d.h. während der Zeit, in der der Studierende eingeschrieben ist, zuzüglich einer Karenzzeit von maximal 6 Monaten gespeichert.

8 Rechte des Betroffenen

Nach der Datenschutz-Grundverordnung stehen Ihnen folgende Rechte zu:

- Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Art. 15 DSGVO).

- Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Art. 16 DSGVO).

- Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18 und 21 DSGVO).

- Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DSGVO).

- Sollten Sie von Ihren oben genannten Rechten Gebrauch machen, prüft die öffentliche Stelle, ob die gesetzlichen Voraussetzungen hierfür erfüllt sind.

- Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz:

Postfach 22 12 19, 80502 München

Wagmüllerstraße 18, 80538 München

Tel.: 089 212672-0

Fax.: 089 212672-50

Mail: poststelle@datenschutz-bayern.de

9 Widerrufsrecht bei Einwilligung

Soweit wir Ihre personenbezogenen Daten aufgrund Ihrer Einwilligung verarbeiten, haben Sie nach Art. 7 Abs. 3 DSGVO das Recht Ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

10 Pflicht zur Bereitstellung der Daten

Die Nutzung des von der Hochschule vorgesehenen Zugangsverfahrens in einer der Alternativen ist verpflichtend. Insoweit sind der Hochschule Daten (wie Passwörter) zur Verfügung zu stellen. Es besteht jedoch keine Verpflichtung zur Nutzung eines Appstores. Eine solche Verpflichtung, die mit dem Abschluss einer Vereinbarung mit einem Appstore-Betreiber einhergeht, als Voraussetzung für den Zugang zu einem Hochschulportal für Studierende wäre rechtlich nicht zulässig. Ein solcher Zwang wäre auch datenschutzrechtlich bedenklich.

11 Anhang I: Abkürzungsverzeichnis

2FA	**2**-**F**aktoren-**A**uthentifizierung
BayDSG	**Bay**erisches **D**aten**s**chutz**g**esetz
BayHSchG	**B**ayerisches **H**ochschulgesetz
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
CR	**C**hallenge **R**esponse
CVE	**C**ommon **V**ulnerabilities and **E**xposures
DSGVO	**D**aten**s**chutz**g**rund**ver**o**r**dnung
GDPR	**G**eneral **D**ata **P**rotection **R**egulation (vgl. DSGVO)
HMAC	Keyed-**H**ash **M**essage **A**uthentication **C**ode
HOTP	**H**MAC-Based **O**ne-**T**ime **P**assword
IDP	**Id**entity **P**rovider
IP	**I**nternet **P**rotocol
JSON	**J**ava**S**cript **O**bject **N**otation
MAC	**M**essage **A**uthentication **C**ode
MFA	**M**ulti-**F**aktoren-**A**uthentifizierung
OTP	**O**ne-**T**ime **P**assword
RSA	**R**ivest **S**hamir **A**dleman Verfahren
SHA	Secure **H**ash **A**lgorithm
SP	**S**ervice **P**rovider – Dienstbereitsteller
TCP	**T**ransport **C**ontrol **P**rotocol
TOM	**T**echnisch **o**rganisatorische **M**aßnahme
TOTP	**T**ime-**B**ased **O**ne-**T**ime **P**assword
U2F	**U**niversal **S**econd **F**actor

12 Anhang II: Glossar

Abbildung – hier synonym zu „Berechnung“: „Das Urbild wird auf einen Wert abgebildet“ ist gleichbedeutend mit „Der Wert wird aus dem Urbild berechnet“. Verschlüsselung und Hashing sind Abbildungen, die im hiesigen Zusammenhang von Bedeutung sind.

Android – Smartphone-Betriebssystem (alle außer Apple).

App – Applikation, syn. Anwendungsprogramm; Begriff wird vorwiegend für Programme auf einem Smartphone gebraucht.

Art.29-Gruppe – Arbeitsgruppe der EU zum Datenschutz entsprechend der EU-Datenschutzrichtlinie; veröffentlichte viele auch für die Auslegung der DSGVO relevante Arbeitspapiere („Working Papers“)

Auftragsverarbeiter - Art. 4 Nr. 8.

[Im Sinne dieser Verordnung bezeichnet der Ausdruck] „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Authentifikation – Online-Duden: „Identitätsprüfung eines Benutzers, einer Benutzerin als Zugangs- und Rechtekontrolle für ein System (z.B. durch Passwort)“. In diesem Sinn verwendet den Begriff: Claudia Eckert, IT-Sicherheit, 10.Auflage, Kapitel 10 „Authentifikation“. Es ist immer zu beachten, dass die Identitätsprüfung des Nutzers von der Annahme ausgeht, dass die Anwendung gewisser Mittel die Identität nachweist.

Beispiel: Es wird davon ausgegangen, dass die Person die den Personalausweis „Max Mustermann“ vorzeigt, auch die bürgerliche Identität „Max Mustermann“ hat, wenn das Lichtbild mit der Person übereinstimmt.

Beispiel: Es wird von der Annahme ausgegangen, dass die Person, die das Passwort vorweist, auch die Person ist, die das Passwort als ihr persönliches Geheimnis generiert hat und dass diese Person tatsächlich die Person ist, der man den Zugang zum System mit Hilfe eines persönlichen Geheimnisses geben will. Das System muss aber über die „bürgerliche Identität“ dieser Person nichts wissen. Es mag sein, dass die Person nur dadurch identifiziert ist, dass sie eine bestimmte e-mail-Adresse hat und darauf reagiert, in dem sie einen Link anklickt. Eventuell hat sie zusätzlich ein übermitteltes Passwort erhalten und wieder eingegeben. Dann besteht die Vermutung: Kommunikationspartner ist eine Person, die diese e-mail-Adresse hat und den Teilnehmeranschluss hat. Es besteht weiter die Vermutung, dass dann diese Person ein Passwort wählt. Zwingend ist das alles aber nicht. Welche „bürgerliche Identität“ diese Person hat, ist offen. Die e-mail-Adresse muss kein Klarnamen sein. Wir haben eine Kette von Vorgängen, bei denen wir hoffen, dass am Anfang die Feststellung der bürgerlichen Identität steht.

damit syn. zu „Authentifizierung“ in der weiten Bedeutung.

Authentifizierung –

(1) enge Bedeutung: der Vorgang, in dem ein System prüft, ob die Mittel, die ein Nutzer vorweist, ihn als Berechtigten ausweisen. Beispiel: Es wird geprüft, ob der analoge Schlüssel zu Schloss passt. Beispiel: Das System liest mit dem Sensor die Daten der Chipkarte und prüft anhand der Daten, ob der Nutzer berechtigt ist.

(2) weite Bedeutung: Vorgang wie (1) und Vorgang, in dem der Nutzer Mittel benutzt, um seine Berechtigung zu zeigen (vgl. Authentisierung (1)), d.h. der Begriff in der weiten Bedeutung kennzeichnet den gesamten Vorgang.

Anmerkung: Das BSI macht den Unterschied zwischen Authentifizierung und Authentisierung.

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei_Faktor-Authentisierung.html

(letzter Abruf 1.9.2020)

„Was ist der Unterschied zwischen Authentisierung und Authentifizierung? Die Begriffe Authentisierung und Authentifizierung werden im allgemeinen Sprachgebrauch oft synonym verwendet, beschreiben aber verschiedene Teilprozesse z.B. eines Anmeldevorgangs. Ein Benutzer AUTHENTISIERT sich an einem System mittels eindeutiger Anmeldeinformationen (z.B. Passwort oder Chipkarte). Das System überprüft daraufhin die Gültigkeit der verwendeten Daten, es AUTHENTIFIZIERT den Nutzer oder die Nutzerin."

Der Begriff wird aber überwiegend in der weiten Bedeutung gebraucht und ist dann synonym zum ebenfalls üblichen, aber selteneren Gebrauch des Begriffs der Authentisierung in der weiten Bedeutung.

Das bay. Hochschulgesetz verwendet den Begriff „Authentifizierung" in der weiten Bedeutung in Art. 61 Abs. 10 BayHSchG.

Zitat

Bayerisches Hochschulgesetz (BayHSchG) vom 23. Mai 2006 (GVBl. S. 245, BayRS 2210-1-1-WK), das zuletzt durch § 1 des Gesetzes vom 24. Juli 2020 (GVBl. S. 382) geändert worden ist

Art. 61 (10) [1]Zur Erprobung neuer oder effizienterer Prüfungsmodelle kann das Staatsministerium durch Rechtsverordnung vorsehen, dass Prüfungen, die ihrer Natur nach dafür geeignet sind, in elektronischer Form und ohne die Verpflichtung durchgeführt werden können, persönlich in einem vorgegebenen Prüfungsraum anwesend sein zu müssen. [2]In der Rechtsverordnung sind insbesondere Bestimmungen zu treffen

1. zur Sicherung des Datenschutzes,

2. zur Sicherung persönlicher Leistungserbringung durch den zu Prüfenden während der gesamten Prüfungsdauer,

3.zur eindeutigen Authentifizierung des zu Prüfenden,

4. zur Verhinderung von Täuschungshandlungen,

5. zum Umgang mit technischen Problemen.

[3]Im Übrigen bleiben Art. 12 Abs. 3 Nr. 6 und Art. 61 Abs. 3 Nr. 8 unberührt. [4]Das Staatsministerium evaluiert diese Bestimmung sowie die darauf aufbauenden Prüfungsregelungen spätestens zum Jahresende 2024 und berichtet hierzu dem Landtag.

Zitatende

Der führende Kommentar zur DSGVO, Simitis et. al, Datenschutzrecht, 1. Auflage, 2019 verwendet ebenfalls den Begriff in der weiten Bedeutung (vgl. Stichwortverzeichnis).

Es macht daher Sinn, den Begriff „Authentifizierung" zu verwenden, wenn man den gesamten Vorgang meint. Dies ist kein falscher Sprachgebrauch.

Authentisierung –

(1) enge Bedeutung: der Vorgang, in dem der Nutzer Mittel benutzt, um seine Berechtigung zu zeigen Beispiel: der Nutzer nutzt den analogen Schlüssel. Beispiel: Der Nutzer hält die Chipkarte an einen Sensor.

(2) weite Bedeutung: Vorgang wie (1), aber auch wie Authentifizierung (1).

Authentisierer (syn zu Authentikator)

Authentifikator (syn zu Authentikator)

Authentikator – Teilsystem, das die Vorgänge der Authentifikation auf der Seite des Systems, zu dem Zugang begehrt wird, abwickelt.

Autorisierung – Nachweis, dass ein Nutzer, dessen Identität geklärt ist, eine Berechtigung für bestimmte Operationen hat.

Beweisführender – syn Prover, dasjenige Teilsystem auf Seiten des Nutzers, das die Authentisierungsmittel berechnet. Im Speziellen: Einheit aus Hardware und Software, die in der Lage ist, Passwörter zu berechnen, die der Nutzer dem Authentikator vorweisen kann.

Codierung - Die Codierung ist ein Wechsel in der Darstellung einer Information, gegebenenfalls zu Hinzufügung von Prüfinformation, die gestattet zu prüfen, ob die Originalinformation verändert wurde oder sogar gestattet, das Original wieder zu rekonstruieren. Typische Codierungen sind die Codierung einer ASCII-Zeichenfolge (Zeichen aus dem ASCII-Vorrat) als Folge von Binärzeichen (als Binärzahl) oder die Darstellung einer Zeichenfolge als QR-Code.

Eine Codierung ist keine Verschlüsselung. Ihr Zweck ist nicht die Sicherung der Vertraulichkeit. Es ist daher irreführend, eine Codierung als Verschlüsselung zu bezeichnen. Die QR-Codierung ist keine Verschlüsselung. Ein QR-Code kann aber genutzt werden, um einen Schlüssel darzustellen.

Datum -Darstellung von Information

Daten: mehrere Darstellungen von Information

Datenstruktur – ein Wert, der in sich strukturiert ist. Beispiel: („Max“, „Mustermann“,1953); Beispiel: [1, 4711, 12] Beispiel: (reg4111,……), (TOTP412,….)

Jede Datenstruktur hat einen bestimmten Typ, den Datentyp (syn: ist von einem bestimmten Datentyp).

Unterscheide die Datenstruktur vom „Datentyp“

Einmal-Passwort – One-Time Password – OTP, technisch gesehen: eine Datenstruktur eines bestimmten Typs.

Endgerät – System, das der Nutzer benutzt, um sich anzumelden. Das Endgerät kommuniziert mit dem Server.

Geburtstagsangriff – Ein Angriff, um Klartexte aus einer vorgegebenen Menge zu finden, die zum selben Passwort führen (syn. auf dasselbe Passwort abgebildet werden), d.h. zum Finden von Kollisionen. Die interessante Frage ist, wie viele Klartexte man wählen muss, damit man mit einer gewissen Wahrscheinlichkeit mindestens eine Kollision findet. Dem entspricht: Wieviele Personen muss man versammeln, damit man in der Menge der Personen mindestens zwei mit dem gleichen Geburtstag findet?

Hashing - Hashing ist das Berechnen eines Werts (Hashwerts) vorgegebener fester Länge aus einer Zeichenfolge beliebiger Länge, dem Urbild (auch „Original“). Formulierungen, die den Berechnungsvorgang beschreiben, sind: „Das Urbild führt zu einem Hashwert“. „Das Urbild wird auf den Hashwert abgebildet.“ Beim hier wichtigen kryptographischen Hashing darf es nicht möglich sein, aus dem Hashwert auf das Urbild zurückzuschließen. Es darf auch nicht mit vertretbarem Aufwand möglich sein, ein anderes Urbild zu konstruieren, dass den gleichen Hashwert ergibt wie das ursprüngliche Urbild. Es darf auch nicht möglich sein, mir vertretbarem Aufwand zwei Urbilder zu konstruieren, die den gleichen Hashwert haben.

Hashing, schlüsselabhängiges (keyed hashing)

Falls in die Berechnung des Hashwerts auch ein Schlüssel eingeht, handelt es sich um eine spezielle Form des Hashings, das sog. Schlüsselabhängige Hashing (keyed hashing). In der Regel wird der

Schlüssel geheim gehalten. Während der Schlüssel fest bleibt, werden mit ihm unterschiedliche Eingaben gehashed. Die Hashwerte hängen von Eingabe und Schlüssel nahezu eindeutig ab, d.h. ohne Kenntnis des Schlüssels lassen sich die dieselben Hashwerte nicht effizient für gleiche Eingaben erzielen.

Hash - (syn.Hashwert)

Hashverfahren – (syn. Hashing)

Hashwert – Ergebnis der Anwendung des Hashverfahrens

iOS – Smartphone-Betriebssystem (Apple)

Identität –

(1) bürgerliche Identität

(2) Identität als Artefakt

Keyed Hash Message Authentication Code –Klasse spezieller schlüsselabhängiger Hashverfahren, abgekürzt mit HMAC-<Basisverfahren>, wobei das Basisverfahren ein nicht-schlüsselabhängiges Hashverfahren ist. Kennzeichen der Konstruktion ist, dass die Eingabe in spezieller Weise mit dem Schlüssel kombiniert wird und darauf dann das Basisverfahren angewandt wird.

Key –

(1) siehe: Schlüssel

(2) Bezeichnung von Hardware, die zur Authentisierung benutzt wird: Beispiel „Security Key“ (dies ist zugleich ein Produktname der Fa.Yubico)

Kollision – Vorkommen zweier verschiedener Klartexte, die zum selben Hashwert führen

Kollisionsresistenz – eines Hashverfahrens:

schwache – Dem Angreifer ist es praktisch unmöglich, zu einem vorgegebenen Klartext einen anderen Klartext zu finden, der mit dem Hashverfahren zum selben Passwort führt.

starke - Dem Angreifer ist es praktisch unmöglich, zwei Klartexte zu finden, die mit dem Hashverfahren zum selben Passwort führen.

Kryptosystem, mathematisches Modell, jeweils nach Verwendung der Schlüssel bezeichnet

symmetrisches

asymmetrisches

Linux - Betriebssystem

one-way – Bezeichnung für eine Funktion, deren Umkehrfunktion praktisch nicht zu ermitteln ist

Identity Provider – Identity Manager

Identity Manager – System, das Nutzer verwaltet.

Infrastruktur – auch IT-Infrastruktur Rechnerhardware zusammen mit dem Betriebssystem und eventuelle sog. Middleware.

personenbezogenes Datum:

Art. 4 Nr. 1 [Im Sinne dieser Verordnung bezeichnet der Ausdruck]: Leerzeichen „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare

natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

EG 26 Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

privacyIDEA Name eines Open Source Werkzeugs

Protokoll – Man beachte die homonyme Verwendung:

(1) Im Sinne der Netzwerktechnik: Technisches Regelwerk, das festlegt nachdem Daten übertragen werden. Festgelegt werden Datenformate und Prozesse der Verarbeitung. Beispiel Transport C Protocol, IP : Internet Protocol

(2) Aufzeichnung über Vorgänge

Prover – siehe Beweisführender

Verschlüsselung - Die Verschlüsselung hat das Ziel unter Einsatz eines Verschlüsselungs-Schlüssels (einer speziellen Zeichenkette) aus einem Input (einer Zeichenkette) einen Output (eine Zeichenkette) derart zu erzeugen, dass ohne Kenntnis des Entschlüsselungs-Schlüssels der Input nicht aus dem Output hergestellt werden kann. Im Falle symmetrischer Verfahren sind beide Schlüssel identisch, im Falle asymmetrischer Verfahren sind sie nicht identisch, stehen aber in einer mathematischen Beziehung. Da Schlüssel auch nur Zeichenketten sind, können auch sie wieder verschlüsselt werden, d.h. eine Verschlüsselung „zweiter Stufe“ ist möglich.

technisch-organisatorische Maßnahmen – Art. 32 DSGVO

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. […]

Token – Der Begriff des Tokens wird (von IT-Personal) derart vielfältig und undifferenziert verwandt, dass beim Lesen eines jeden Textes eine sehr sorgfältige Ermittlung der Bedeutung notwendig ist.

(1) Hardware, die für Zwecke der Authentisierung eingesetzt wird

(2) Software: Apps wie TOTP-Apps, welche auch als „Software-Token“ bezeichnet werden.

(3) Datenstruktur: Ein strukturierter Wert, der die nötige Information zur Durchführung eines bestimmten Verfahrens der Authentisierung enthält. Diese Datenstrukturen kann man nach dem Typ des Tokens (Tokentyp) unterscheiden. Z.B. gibt es TOTP-Token, ein U2F-Token usf. Diese Datenstruktur (TOTP-Token) kann auch innerhalb einer App (s. (2)) gespeichert werden.

(4) Wert, der vorzuweisen ist, um einen Zugang zu bzw. Zugriff auf eine Ressource zu erlangen. Dieser Wert kann in sich strukturiert sein oder einfach sein. Im Zugangsprotokoll OAuth 2.0 ist dies die Bedeutung von „Token“.

(5) synonym zu „Passwort“. Dieser Gebrauch des Begriffs „Token“ sollte vermieden werden, weil er in der Beschreibung von Verfahren zur Verwirrung führt.

(4) Verfahrensbestandteil:

Tokenliste: eine Datenstruktur in Form einer Liste; die Einzelelemente stellen Token im Sinne der Definition (3) dar.. Diese Liste kann sich auch auf dem Server befinden, kann übertragen werden und dem Nutzer durch seinen Browser präsentiert werden. TOTP-Token können als Liste auch auf dem Smartphone mit der App dargestellt werden.

Rivest **S**hamir **A**dleman Verfahren - Verschlüsselungsverfahren mit asymmetrischen Schlüsseln

shared secret – sog. geteiltes (syn. gemeinsames) Geheimnis; Es handelt sich in der Regel um einen symmetrischen Schlüssel

Server – Teil des Gesamtsystems, Einheit aus Hardware und Software, Bereitsteller von Diensten, wie einem Serviceportal. Der Server ist in Bezug auf die Kommunikation Sender und Empfänger von Nachrichten.

Shibboleth – spezielles Identitätsmanagementsystem

Signatur -

digitale

Verfahren der elektronischen Signatur mit Verwendung eines asymmetrischen Kryptosystems

Ergebnis des vorgenannten Verfahrens, das einem Dokument zugefügt wird

elektronische

Verfahren zur Sicherung von Integrität und Authentizität von Dokumenten oder Nachrichten

Ergebnis des Verfahrens**, das einem Dokument zugefügt wird**

Bem.: nicht als Synonym zu digitale Signatur verwenden

Dies ist Sprachgebrauch des § 126 a BGB und des Signaturgesetzes – SigG.

Signaturverfahren, Signierungsverfahren – wie „elektronische Signatur“

Schlüssel –

Eingabe in Verschlüsselungs- bzw. Hashverfahren

symmetrischer : Schlüssel, der sowohl von Sender als auch Empfänger genutzt wird

asymmetrischer: Schlüssel, der nur von einem Partner der Kommunikation genutzt wird. Es kann der private bzw. der öffentliche Schlüssel sein. Welcher Schlüssel in welcher Rolle genutzt wird, hängt von dem Zweck ab, zu dem der Schlüssel benutzt wird.

Zweck kann sein:

(a) die Sicherung der Vertraulichkeit durch Verschlüsselung

(b) die Sicherung der Integrität und Authentizität eines Dokuments durch eine digitale Signatur.

Maßgebend ist, dass

(a) dec(private_key,enc(public_key,m)=m bzw.

(b) dec(public_key,enc(private_key,m))=m

wobei enc die Entschlüsselung und dec die Verschlüsselung und m die zu verschlüssselnde Nachricht bezeichnet.

(a) betrifft die Sicherung der Vertraulichkeit (b) die Sicherung der Integrität und Authentizität.

In (a) verschlüsselt der Sender mit dem öffentlichen Schlüssel des Empfängers, und der Empfänger entschlüsselt mit seinem privaten Schlüssel; in (b) signiert der Sender mit Hilfe seines privaten Schlüssels und der Empfänger prüft mit dem öffentlichen Schlüssel des Senders. Allerdings ist m in diesem Fall in der Regel nicht unmittelbar das Dokument, sondern ein aus der Nachricht durch eine Hashverfahren gewonnener Fingerabdruck.

Service Provider - Der Teil des Gesamtsystems, der einen Dienst bereitstellt. ImI beschriebenen Fall ist es das Serviceportal, bei dem sich der Nutzer anmelden will.

System – Gesamtheit aus Rechnerhardware, Betriebssystem und Anwendungssoftware

Universal Second Factor – normiertes Verfahren der Authentisierung unter Einsatz eines asymmetrischen Kryptosystems

Validierung

im Zusammenhang mit Authentifizierung: Vorgang der Prüfung des Authentisierungsmittels

Bemerkung: Die Verwendung des Begriffs „Validierung“ bei Passwortprüfung ist technisch falsch, aber in Tools wie privacyIDEA üblich. Der Begriff „Verifikation“ hierfür wäre korrekt.

Verantwortlicher – Art.4 Nr. 7 DSGVO

[Im Sinne dieser Verordnung bezeichnet der Ausdruck] „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

Verifikation - im Zusammenhang mit Authentifizierung: Vorgang der Prüfung des Authentisierungsmittels

Verletzung Art. 4 Nr. 12 DSGVO

[Im Sinne dieser Verordnung bezeichnet der Ausdruck] „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Verschlüsselung – siehe „Schlüssel“

Wert, einfacher Zahlen diverser Zahlensysteme, Zeichen, Zeichenketten, Wahrheitswerte.

Wert, strukturierter – ein Wert, der sich aus anderen Werten zusammensetzt. Beispiel („Max“, „Mustermann“, 65) Rekursiver Aufbau ist möglich. Typischerweise wählt man normierte Darstellungen wie JSON - JavaScript Object Notation oder XML.

13 Anhang III: Literatur (Auswahl)

Claudia Eckert; IT-Sicherheit, 10. Auflage, 2018, insbes: Kapitel 10 „Authentifikation“

Ralf Küsters, Thomas Wilke; Moderne Kryptographie -Eine Einführung,1. Auflage, 2011

Stephan Spitz, Michael Pramateftakis, Joachim Swoboda; Kryptographie und IT-Sicherheit Grundlagen und Anwendungen, 2.Auflage,2011

Dietmar Wätjen, Kryptographie, - Grundlagen, Algorithmen, Protokolle, 3. Auflage, 2018

Zeitschrift: Datenschutz und Datensicherheit – DuD, Heft 4/2016 mit Schwerpunkt „Authentifikation“.

Technische Spezifikationen:

rfc 6238:TOTP: Time-Based One-Time Password Algorithm, May 2011

rfc4226 HOTP: An HMAC-Based One-Time Password Algorithm, Dec 2005
