**Maßnahmen zur Sicherstellung der Authentizität und Non-Repudiation**

Version 1.1

Datum: 03.02.2022

David Nguyen

Klasse: 5bWI

Inhalt

[Aufgabenstellung 3](#_Toc94865247)

[Authentizität und Non-Repudiation 3](#_Toc94865248)

[Technische Maßnahmen 4](#_Toc94865249)

[Signierung 4](#_Toc94865250)

[Hashing 4](#_Toc94865251)

[TLS-Verschlüsselung 5](#_Toc94865252)

[Confidential Printing 5](#_Toc94865253)

[Zugangskontrollkonzeption 6](#_Toc94865254)

[Weisungshandbuch/Arbeitsanweisungen 6](#_Toc94865255)

[Organisatorische Maßnahmen 6](#_Toc94865256)

[Monitoring und Logging Systeme 6](#_Toc94865257)

[Device Management 7](#_Toc94865258)

[System-Audits 7](#_Toc94865259)

[Schulung und Awareness der Benutzer 8](#_Toc94865260)

[Handbuch/Systemdokumentation 8](#_Toc94865261)

# Aufgabenstellung

Maßnahmen zur Sicherstellung der Authentizität und Non-Repudiation

Erhebe und beschreibe technische und organisatorische Maßnahmen zur Sicherstellung der Authentizität und Non-Repudiation von IV-Systemen.

Beispielhaft:

technisch: Signierung, Hashing, TLS-Verschlüsselung, Confidential Printing, Zugangskontroll-Konzeption, Weisungshandbuch, Arbeitsanweisungen

organisatorisch dazu: Monitoring und Logging Systeme, Device Management, System-Audits, Schulung und Awareness der Benutzer, Handbuch/Systemdokumentation, Testkonzepte, ...

# Authentizität und Non-Repudiation

Die lückenlose Nachvollziehbarkeit Themenblock der Revision. Änderungen der Daten können lückenlos nachvollzogen werden und somit von auch den Verarbeitungssysteme. Wesentliche Grundlagen für die Authentizität sind im IT-Sicherheitsgesetz zu finden in der DSVGO, TKG, KRITIS. Als Grundsatz kann man sich merken wer darf von wo was wie zugreifen. Wer ist dabei wichtig. Systeme sind entweder authentisch oder nicht authentisch. Im Internet gibt es eine vierstufige Architektur das ist aber laut Herr Hallinger Blödsinn, man kann entweder ein System prüfen oder nicht prüfen. Entweder sind die Informationen da oder nicht.

Authentizität wird als Unterklasse der Integrität behandelt. Dabei geht es bei Integrität um Systeme, Informationen, Verarbeitungssysteme und ob sie integer sind, also nach Vollziehbarkeit und Transparent. Bei Authentizität geht es um die Person, die eine Information bereitstellt, dass man nachträglich beweisen kann, wer die Information bearbeitet hat.

Echtheit, Überprüfbarkeit und Vertrauen der Person und die nicht abstreitbarkeit. Die Verarbeitung von Informationen ist lückenlos unveränderbar den Arbeiter zuweisbar das braucht man bei der Integrität nicht und die Daten können jederzeit zwischen den Zwischenschritten hin bis zur Quelle zurückverfolgt werden

Unter Authentizität versteht man sowohl einen Identitätsnachweis als auch die Authentizität der eigentlichen Daten. Bei ersterem möchte man sicherstellen, dass der Kommunikationspartner auch der ist, für den man ihn hält. Dafür soll eine Instanz einer anderen ihre Identität nachweisen können, ohne dass es Zweifel gibt. Bei der Authentizität der Daten geht es dann noch darum, dass die erhaltenen Daten auch tatsächlich von der authentisierten Instanz stammen. Die Authentizität wird oft auch als übergeordnetes Schutzziel angesehen, da die anderen Schutzziele sonst wertlos sind, wenn man nicht sicher sein kann, ob man mit dem tatsächlichen gewünschten Kommunikationspartner kommuniziert oder mit einem unbekannten Dritten.

Unter der Authentizität eines Objekts bzw. Subjekts wird die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts verstanden, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar sind.

## Technische Maßnahmen

### Signierung

Unabdingbar bei der Übermittlung elektronischer Daten und Dokumente ist die Möglichkeit, die Authentizität des Verfassers nachprüfen zu können. Nichts wäre schlimmer, als wenn zum Beispiel bei wichtigen Verträgen eine andere Person als die angegebene ihre „Unterschrift“ leistet.

Als Identifikationsnachweis gelten traditionell Wissen, Besitz und Eigenschaften, wobei im besten Fall alle drei angesprochenen Punkte bei einer Überprüfung zur Geltung kommen. Bei heutigen PIN-Abfragen wird beispielsweise nur das Wissen überprüft, eine zum Beispiel in der Hand gehaltene EC-Karte könnte als Nachweis des Besitzes dienen, während der Fingerabdruck eine typische Eigenschaft darstellt. Die Nutzung einer Signaturkarte in Verbindung mit einer PIN-Nummer integriert immerhin schon zwei dieser Nachweismöglichkeiten.

Unabdingbar bei der Übermittlung elektronischer Daten und Dokumente ist die Möglichkeit, die Authentizität des Verfassers nachprüfen zu können. Nichts wäre schlimmer, als wenn zum Beispiel bei wichtigen Verträgen eine andere Person als die angegebene ihre „Unterschrift“ leistet.

Als Identifikationsnachweis gelten traditionell Wissen, Besitz und Eigenschaften, wobei im besten Fall alle drei angesprochenen Punkte bei einer Überprüfung zur Geltung kommen. Bei heutigen PIN-Abfragen wird beispielsweise nur das Wissen überprüft, eine zum Beispiel in der Hand gehaltene EC-Karte könnte als Nachweis des Besitzes dienen, während der Fingerabdruck eine typische Eigenschaft darstellt. Die Nutzung einer Signaturkarte in Verbindung mit einer PIN-Nummer integriert immerhin schon zwei dieser Nachweismöglichkeiten.

Ein Hauptanliegen der digitalen Signatur ist die zweifelsfreie Identifizierung des Absenders.

Für die Umsetzung der Verschlüsselung bzw. der digitalen Signaturen existieren mehrere Möglichkeiten, die sich vor allem in ihrer Komplexität und ihren Einsatzmöglichkeiten unterscheiden. Diese werden auf den folgenden Seiten näher beschrieben.

Genauso gibt es nur einige Formate und Programme, mit denen sich die digitale Signatur verwirklichen lässt. Diese werden ebenfalls dargestellt, inklusive ihrer Nutzbarkeit und Nachteile.

### Hashing

Hashing bezeichnet einen kryptografischen Prozess, der dazu genutzt werden kann, die Authentizität und Integrität diverser Datentypen zu validieren. Hashfunktionen kommen vor allem in Authentifizierungssystemen zur Anwendung - hier bieten sie den Vorteil, dass keine Passwörter im Plaintext-Format gespeichert werden müssen. Werden Hashfunktionen falsch eingesetzt, können schwerwiegende Datenlecks die Folge sein. Schlimmer ist nur, wenn Hashing überhaupt nicht zum Einsatz kommt.

Die Internet Engineering Taskforce (IETF) empfiehlt in einem aktuellen Entwurf für die Speicherung von Passwörtern den Einsatz folgender Hashing-Algorithmen:

* Argon2
* Bcrypt
* Scrypt
* PBKDF2

Neben dem Algorithmus kommt es jedoch auch auf andere Faktoren an. Zum Beispiel die Passwortlänge: Ein Minimum von acht Zeichen ist beispielsweise wichtig, weil so Dictionary-Angriffe wesentlich schwieriger werden.

Jede Hashfunktion kann darüber hinaus so implementiert werden, dass der Hashing-Algorithmus mehrfach auf das Passwort angewendet wird ("Work Factor"). Das sorgt für höhere Sicherheit, benötigt aber auch mehr Rechenpower. Für die Wahl des richtigen "Work Factor" gibt es laut OWASP keine goldene Regel: "Die Wahl des idealen 'Work Factor' hängt von der Performance des Servers und der Zahl der Nutzer auf der Applikation ab. Um ihn zu ermitteln, sind Tests mit verschiedenen Servern nötig. Als Faustregel lässt sich festhalten, dass die Berechnung eines Hashwertes nicht länger als eine Sekunde in Anspruch nehmen sollte - in Umgebungen mit hohem Traffic noch wesentlich weniger."

### TLS-Verschlüsselung

Transport Layer Security (TLS, englisch für Transportschichtsicherheit), auch bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

TLS besteht aus den beiden Hauptkomponenten TLS Handshake und TLS Record. Im TLS Handshake findet ein sicherer Schlüsselaustausch und eine Authentisierung statt. TLS Record verwendet dann den im TLS Handshake ausgehandelten symmetrischen Schlüssel für eine sichere Datenübertragung – die Daten werden verschlüsselt und mit einem MAC gegen Veränderungen geschützt übertragen.

Für den Schlüsselaustausch sind in den älteren TLS-Versionen verschiedene Algorithmen mit unterschiedlichen Sicherheitsgarantien im Einsatz. Die neueste Version TLS 1.3 verwendet allerdings nur noch das Diffie-Hellman-Schlüsselaustausch Protokoll (DHE oder ECDHE). Dabei wird für jede Verbindung ein neuer Sitzungsschlüssel (Session Key) ausgehandelt. Da dies ohne Verwendung eines Langzeitschlüssels geschieht, erreicht TLS 1.3 Perfect Forward Secrecy. Mit dem Key kann man davon ausgehen, dass die richtige Person Zugriff auf die Daten bekommt und diese auch bearbeiten kann.

### Confidential Printing

Druckprotokolle, Kundendatenlisten, die auf einen Drucker liegen, entspricht den Alltag in einer Praxis, aber so sollte es in Theorie nicht sein. Beispiel: Man sitzt in einem Büro mit einem Gemeinschaftsdrucker und danach schickt man einen Druckauftrag. Auf dem Weg zum Drucker wird man noch abgelenkt und vergeudet Zeit, redet noch mit seinen Kollegen und währenddessen liegen die Dokumente beim Drucker und dann kommt die Mittagspause man vergisst, dass man etwas ausgedruckt hat. Wie kann man sowas verhindern, die Funktion dahinter nennt sich Confidential Printing, wenn man einen Druckauftrag abschickt, muss man dann einen PIN-Code mitgeben und wenn man dann druckt, gibt man den PIN-Code ein und erst dann kommt der Ausdruck raus oder mit einer Karte. Dass erst wenn man die Karte an den Drucker ranhält, dass der Ausdruck rauskommt. Das Problem ist, dass in der Drucker Warteschlange die ganzen Kundendaten gespeichert werden, so können andere Personen und Netzwerk Administratoren auf diese Daten zugreifen.

Durch Confidential Printing, wird sichergestellt, dass nur die Personen Zugriff auf die Daten haben und diese auch bearbeiten können.

### Zugangskontrollkonzeption

Zugangskontrolle verwehrt Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird. So wird sichergestellt, dass z. B. ein Rechner nur mit berechtigten Nutzern kommunizieren kann. Es wird zwischen Zugangskontrolldiensten, zur Realisierung der Zugangskontrolle, und zugangskontrollierten Diensten, die erst nach erfolgreicher Zugangskontrolle genutzt werden können, unterschieden. Bis 2018 wurde der Aspekt des Zutritts zu (Zutrittskontrolle) und der Nutzung von Datenverarbeitungsanlagen (Zugangskontrolle in einem engeren Sinne) im deutschen Recht unterschieden, während heute sowohl der Zugang zu Grundstücken und Räumen, einschließlich aller Datenverarbeitungsanlagen neben deren informationstechnischer Nutzungsmöglichkeit nur noch vom Zugang zu den von einer Zugangsberechtigung umfassten Daten unterschieden wird. Letztere abgestufte Inanspruchnahme von Betriebsmitteln wird als Zugriffskontrolle bezeichnet.

Zuerst muss die Identität des Kommunikationspartners erfragt werden. Dabei können auch Pseudonyme zugelassen sein. Nur bei erfolgreicher Prüfung der Identität (Authentifizierung) wird die Kommunikationsbeziehung fortgesetzt. Ein Mensch kann von einem Rechner auf Grund seiner biologischen Merkmale (Biometrie), seines Wissens (z. B. Benutzername mit Passwort) und seines Besitzes (z. B. Ausweis, Smartcard) erkannt werden. Ein Mensch kann sich vor einem Rechner absichern, indem er ihn an Äußerlichkeiten (z. B. Gehäuse, Hologramm, Verunreinigungen), seinem Wissen oder seinem Standort identifiziert. Rechner können sich untereinander nur durch ihr Wissen und eventuell durch die Herkunft der Leitung erkennen. Die Prüfung der Identität kann entweder am Anfang oder dauerhaft, während der gesamten Kommunikation, erfolgen.

Bei der technischen Umsetzung sind insbesondere die Schutzinteressen der Teilnehmer (eventuell vertreten durch ihre Endgeräte) und des Anbieters der zugangskontrollierten Dienste zu berücksichtigen. Für den Teilnehmer können dies zum Beispiel sein:

* Vertraulichkeit (z. B. Vermeidung unnötiger Protokolldaten), Anonymität
* Erreichbarkeit

Zugangskontrolldienste werden in der Regel in Verbindung mit kryptografischen Systemen (Verschlüsselung, Authentifikation) realisiert, um die Sicherheit gegen Angriffe zu erhöhen.

### Weisungshandbuch/Arbeitsanweisungen

In Banken nennt man das Weisungshandbuch in Unternehmen Arbeitsanweisungen. Diese Arbeitsanweisungen sind für die Mitarbeiter verbindlich

## Organisatorische Maßnahmen

### Monitoring und Logging Systeme

Jeder weiß, dass Protokolle in der IT-Branche eine wichtige Rolle spielen. Protokolle werden für verschiedene Zwecke verwendet, z. B. für den IT-Betrieb, die System- und Anwendungsüberwachung, Geschäftsanalysen, Sicherheit und Compliance und vieles mehr.

Ein zentralisiertes Protokollierungssystem macht Entwicklern das Leben leicht, insbesondere wenn es darum geht, Fehler in der Anwendung zu beheben, Probleme zu erkennen, die Anwendung aufgrund unerwarteter Zugriffe auf Dienste zu sichern oder die Leistung der Anwendung zu überprüfen usw. Einige der großartigen Eigenschaften eines zentralisierten Protokollierungssystems sind seine kostengünstige Wartung, die einfache Suche nach Protokollen, die grafische Benutzeroberfläche usw.

Splunk ist ein zentralisiertes Log-Analyse-Tool für maschinell erzeugte Daten, unstrukturierte/strukturierte und komplexe mehrzeilige Daten, das folgende Funktionen bietet: einfache Suche/Navigation, Echtzeit-Sichtbarkeit, historische Analysen, Berichte, Alarme, Dashboards und Visualisierung.

Splunk mit einem zentralen Login Server und mit entsprechenden Agents auf den einzelnen dezentralen Systemen die entsprechend mitprotokollieren woher kommen die Daten wie wurden sie verändert und so weiter.

### Device Management

Wenn eine Information über USB-Schnittstelle hereingekommen ist, dann ist es schwer zu beweisen wer sie auch reingesteckt hat

Unter Gerätemanagement versteht man den Prozess der Verwaltung der Implementierung, des Betriebs und der Wartung eines physischen und/oder virtuellen Geräts. Es ist ein weit gefasster Begriff, der verschiedene Verwaltungswerkzeuge und -prozesse für die Wartung und Instandhaltung eines Computers, Netzwerks, mobilen und/oder virtuellen Geräts umfasst

Das Gerätemanagement hat im Allgemeinen folgende Aufgaben:

Installation von Geräte- und Komponententreibern und zugehöriger Software

Konfiguration eines Geräts, damit es mit dem gebündelten Betriebssystem, des Geschäfts/Arbeitsablaufs-Software und/oder mit anderen Hardware-Geräten die erwartete Leistung erbringt. Implementierung von Sicherheitsmaßnahmen und -prozessen.

Geräte beziehen sich in der Regel auf physische/Hardware-Geräte wie Computer, Laptops, Server, Mobiltelefone und andere. Es kann sich aber auch um virtuelle Geräte handeln, wie z. B. virtuelle Maschinen oder virtuelle Switches. In Windows ist die Geräteverwaltung auch ein Verwaltungsmodul, das zur Verwaltung oder Konfiguration der physischen Geräte, Anschlüsse und Schnittstellen eines Computers oder Servers dient.

### System-Audits

Wann immer ein Verstoß vorliegt, ist es für die Datenintegrität entscheidend, die Quelle aufzuspüren. Oft als Audit-Trail bezeichnet, bietet dies einem Unternehmen die Möglichkeit, die Ursache des Problems genau zu lokalisieren. Dabei sollten Audit Trails folgende Merkmale aufweisen:

* Audit Trails müssen automatisch generiert werden können
* Nutzer dürfen keine Möglichkeit haben, den Audit Trail zu manipulieren
* Jedes Ereignis (Erstellen, Löschen, Lesen, Ändern) wird erfasst und aufgezeichnet
* Bei jedem Ereignis wird der entsprechende Benutzer erfasst, um festzustellen, wer auf die Daten (auf welche Weise) zugegriffen hat
* Jedes Ereignis wird mit einem Zeitstempel versehen, so dass Sie wissen, wann das Ereignis stattgefunden hat.

Ein Systemaudit ist eine systematische, strukturierte und dokumentierte Untersuchung der Wirksamkeit eines Managementsystems. Zum Beispiel ist das Einführen und Aufrechterhalten eines Qualitätsmanagementsystems im Unternehmen heutzutage unabdingbar für den Erfolg eines Unternehmens. Dabei muss das Qualitätsmanagementsystem wirksam umgesetzt und ständig weiterentwickelt werden, um einen anhaltenden Effekt zu erzielen.

Damit dies sichergestellt ist, werden Managementsysteme vor Ort einer regelmäßigen Überprüfung unterzogen – dem internen Systemaudit. Das interne Systemaudit stellt eine große Chance für ein Unternehmen dar. Es unterstützt Sie bei der Analyse und bei der Bewertung des Managementsystems und eröffnet neue Möglichkeiten, Ihr Qualitätsmanagementsystem kontinuierlich zu verbessern.

### Schulung und Awareness der Benutzer

Durch Schulungen können die Benutzer auf allgegenwertige sowie leicht vermeidbare Fehler hingewiesen werden, wodurch der Großteil der Korrektheit ausgebügelt wäre. Die Mitarbeiter/innen können bei Fragen und Unklarheiten mit dem Umgang mit Daten ein Verständnis entwickeln und die Folgen des Schadens verstehen die, damit entstehen würden. Bei der Schulung lernen die Benutzer wie mit Daten umzugehen ist und wie man die Richtigkeit der Daten behält.

### Handbuch/Systemdokumentation

Aufstellung der Software mit Schnittstellen mit Funktionen. Im Handbuch bzw. der Dokumentation stehen die Vorschriften für den Umgang von Daten. Worauf soll man achten groß/klein Schreibung, Kommasetzung bei Beträgen. Das Handbuch soll den Mitarbeiter/innen einen Leitfaden geben, um die einfachen Fehler zu vermeiden und somit die Integrität der Daten zu gewähren.

Die Dokumentation soll auch protokollieren wer war wann wofür zuständig. So kann man wieder auf die Lückenlosigkeit zurückgreifen, in dem man immer sieht wer hat was geändert. Damit die Dokumentation auch nutzbar ist muss sie authentisch sein. Also man muss sie prüfen können. Eine Dokumentation die Fehler beinhaltet oder nicht vollständig kann man nicht gebrauchen, da sie nicht authentisch ist.