Erläuterungen und Hinweise zum Umgang mit elektronischen Signaturen bei der digitalen Prüfung von bautechnischen Nachweisen

1. Einleitung

Im Oktober 2019 hatte die ARGEBAU Änderungen der MBO und der MbauVorlVO zur Erleichterung digitaler bauaufsichtlicher Verfahren in die Verbändeanhörung gegeben. Zielstellung war, die MBO und die MBauVorlVO einerseits von zahlreichen Schriftformerfordernissen zu befreien und andererseits die elektronische Übermittlung von Anträgen, Anzeigen und Mitteilungen als den zukünftigen Regelfall zu definieren [1].

Die BVPI hat sich im Rahmen des Anhörungsverfahrens ausdrücklich dafür ausgesprochen, die Schriftform für die von Prüfingenieuren zu erstellenden bauaufsichtlichen Prüfungen und deren Dokumente zu erhalten bzw. deren Ersatz durch die elektronische Form zu ermöglichen.

In den vergangenen Wochen haben bereits erste Bundesländer begonnen, die von der ARGEBAU geplanten Änderungen von MBO und MBauVorlV in Landesrecht umzusetzen (z.B. Niedersachsen).

Neben den Änderungen von MBO, MBauVorlV und den entsprechenden Länderregelungen stellt auch die Umsetzung des Online Zugangsgesetzes (OZG) die Prüfingenieure bei der Prüfung von bautechnischen Nachweisen vor neue Herausforderungen.

Digital eingereichte bautechnische Nachweise (i.d.R. im pdf–Format) sollen ohne Medienbruch digital geprüft werden. Am Ende des digitalen Prüfvorgangs müssen Prüfberichte sowie die geprüften bautechnischen Nachweise digital signiert werden. Der digitale Signaturprozess übernimmt somit zunächst die gleiche Aufgabe wie vergleichbar die handschriftliche Signatur des Prüfingenieurs bei der ursprünglichen Unterzeichnung auf Papier. Digitale Signaturprozesse leisten darüber hinaus aber auch weitere Zusatzfunktionen.

Diese Erläuterungen und Hinweise des Arbeitskreises Digitalisierung des BVPI soll einen Einstieg in elektronische Signaturen für Prüfingenieure erleichtern und diesbezügliche Empfehlungen abgeben.

2. Rechtliche Situation / Quellen

[1] Anhörungsverfahren zur Änderung der MBO und der MBauVorlV zur Erleichterung digitaler bauaufsichtlicher Verfahren; ARGEBAU vom 02.10.2019

[2] eIDAS-VOVerordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt; vom 23. Juli 2014; (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices)

[3] Technische Richtlinie TR – 03107-1 Elektronische Identitäten und Vertrauensdienste im E- Government; Bundesamt für Sicherheit in der Informationstechnik (BSI); Version 1.1.1; vom 07.05.2019

[4] Technische Richtlinie TR – 03125 (Anhang TR-ESOR) Beweiswerterhaltung kryptographisch signierter Dokumente; Bundesamt für Sicherheit in der Informationstechnik (BSI); Version 1.2.2; vom 02.07.2019

[5] Musterbauordnung (MBO) zuletzt geändert 27.09.2019

[6] Muster einer Verordnung über Bauvorlagen und bauaufsichtliche Anzeigen (Musterbauvorlagenverordnung MBauVorlV); Fassung Februar 2007

3. Begriffsbestimmungen

Elektronische Signatur (ES)
Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden, und die der Unterzeichner zum Unterzeichnen verwendet, werden elektronische Signatur (ES) genannt.

„Fortgeschrittene elektronische Signatur“ (AdES) ist eine **ES**, die folgende, weitere Anforderungen erfüllt:

- Sie ist eindeutig dem Unterzeichner zugeordnet,
- sie ermöglicht die Identifizierung des Unterzeichners,
- sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann,
- sie ist mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Datenerkannt werden kann.

  „Elektronische Signaturerstellungsdaten“ sind eindeutige Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden.

„Qualifizierte elektronische Signatur“ (QES) ist eine **AdES**, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

„Elektronische Signaturerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird.

„Qualifizierte elektronische Signaturerstellungseinheit“ ist eine elektronische Signaturerstellungseinheit, die besondere Anforderungen des Anhangs II der eIDAS- VO [2] erfüllt.

„Zertifikate für elektronische Signaturen“ sind elektronische Bescheinigungen, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt. Zertifikate verfügen i.d.R. über ein Gültigkeitsdatum.

„Qualifiziertes Zertifikat für elektronische Signaturen“ ist ein von einem qualifizierten Vertrauensdienstanbieter ausgestelltes Zertifikat für elektronische Signaturen, das bestimmte Anforderungen nach eIDAS -VO erfüllt.

„Vertrauensdienst“ ist ein elektronischer Dienst, der i.d.R. gegen Entgelt erbracht wird und u.a. aus Folgendem besteht: Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, Diensten für die Zustellung elektronischer Einschreiben sowie diese Dienste betreffende Zertifikate.

„Qualifizierter Vertrauensdienst“ ist ein Vertrauensdienst, der die einschlägigen Anforderungen der eIDAS-VO erfüllt. Da es sich bei der eIDAS-VO um eine europäische Verordnung handelt, werden qualifizierte Vertrauensdienste von einer Vielzahl von Anbietern innerhalb der EU Staaten gegen Entgelt angeboten. (Link zu den europäischen Anbietern am Ende der Technischen Mitteilung)

„Gesetzliches Schriftformerfordernis“ ist ein gesetzlich angeordnetes Formerfordernis, das insbesondere eine eigenhändige Unterschrift unter ein Dokument verlangt. Die grundlegende Regelung dazu findet sich in § 126 BGB. Die Schriftformerfordernis kann durch eine qualifizierte digitale Signatur ersetzt werden (§ 126a BGB). § 3a Verwaltungsverfahrensgesetz (VwVfG) sieht weitere Möglichkeiten zum Ersatz des Schriftformerfordernisses über digitale Wege vor.

„Gesetzliches Textformerfordernis“ ist ein gesetzlich angeordnetes Formerfordernis, das eine lesbare, aber nicht unterschriebene Erklärung verlangt.

„Integrität“ bezeichnet die Sicherheit, dass die Gültigkeit der elektronischen Signatur nur dann erhalten bleibt, wenn das Dokument nicht verändert wurde. Wird der Inhalt eines signierten elektronischen Dokumentes verändert, wird durch Überprüfung die Signatur automatisch im Dokument für ungültig erklärt.

„Identität / Authentizität“ bezeichnet die eindeutige Identifizierbarkeit des Autors des digitalen Signaturprozesses. Das Datum der Erstellung der Signatur, sowie der Inhalt müssen für den Empfänger authentisch belegbar sein.

4. Erläuterungen

a) Einordnung in den Rechtsrahmen und Verfahren

Mit der eIDAS-VO [2] der EU wird seit Mitte 2016 ein einheitlicher, europaweit gültiger, rechtlicher und organisatorischer Rahmen für einen vertrauenswürdigen elektronischen Geschäftsverkehr festgelegt. Damit sollen sichere und nahtlose digitale Transaktionen zwischen Unternehmen, Bürgern und Behörden anhand von elektronischen Signaturen ermöglicht werden.

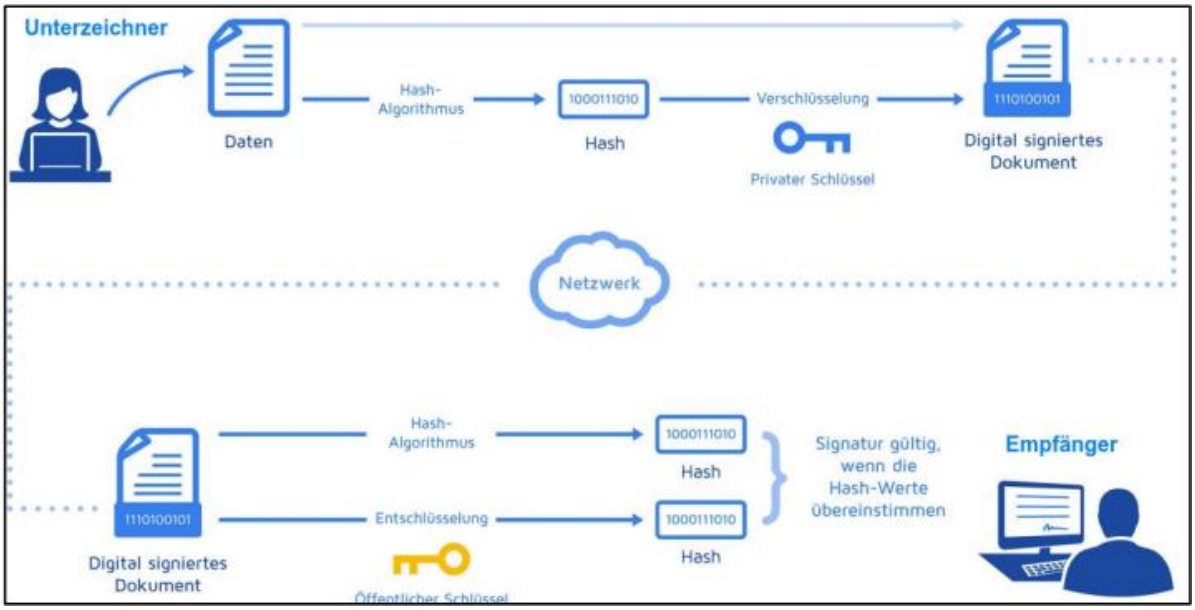
Als eIDAS-VO konforme Signaturen werden die fortgeschrittene elektronische Signatur (AdES) und die qualifizierte elektronische Signatur (QES) eingesetzt. Die qualifizierte elektronische Signatur gewährleistet die Authentizität des elektronischen Dokuments, d.h. der Unterzeichnende kann darüber eindeutig identifiziert und die Herkunft der Daten bestimmtwerden. Außerdem stellt sie die Integrität der übermittelten Daten sicher, indem jede Veränderung der ursprünglichen Daten kenntlich gemacht werden kann.

b) Ablauf eines digitalen Signaturprozesses

Eine Person erhält von dem Anbieter **elektronischer Vertrauensdienste** ihrer Wahl ein Zertifikat mit einem s.g. „Schlüsselbund“. Der „Schlüsselbund“ besteht aus einem geheimen privaten Schlüssel und einem öffentlichen Schlüssel. Vor Herausgabe des Zertifikates und „Schlüsselbundes“ hat der Anbieter die Identität der anfragenden Person in geeigneter Form festgestellt. Je höher der Anspruch auf Vertrauen, desto höher wird der Anspruch auf eine rechtssichere Identitätsfeststellung sein. Nach dem Identifikationsverfahren „vertraut“ der Vertrauensdienstanbieter somit der Person.

Beim elektronischen Signaturvorgang wird durch die verwendete Soft- und Hardware sowie Technologien aus der Kryptographie ein s.g. Hashwert des elektronischen Dokumentes gebildet, der mit dem geheimen, privaten Schlüssel verschlüsselt wird. Dieser verschlüsselte Hashwert ist wie ein elektronischer Fingerabdruck zum Zeitpunkt der Signatur zu verstehen und eindeutig einem Dokument zuzuordnen. Der verschlüsselte Hashwert und der öffentliche Teil des „Schlüsselbundes“ werden automatisch zum Bestandteil des signierten Dokumentes und beim Versand z.B. einer signierten pdf-Datei mit diesem versendet.

Soll ein signiertes elektronisches Dokument auf **Integrität** geprüft werden, wird mit dem gleichen mathematischen Verfahren der Hashwert des Dokumentes durch die Software des Empfängers erneut gebildet. Weiterhin wird mit dem mitgelieferten öffentlichen „Schlüssel“ der mitgelieferte Hashwert des Dokumentes, der zum Zeitpunkt der Signatur entstanden ist, entschlüsselt. Die beiden Hashwerte werden automatisch verglichen. Ist der Hashwert unverändert geblieben, ist die Integrität des Dokumentes sichergestellt („Fingerabdruck“ zum Zeitpunkt der Signatur ist identisch mit dem „Fingerabdruck“ zum Zeitpunkt der Dokumentenkontrolle – Das Dokument ist unverändert).



Dieser mathematische Teil zur Dokumentenüberprüfung zur Integrität wird von den elektronischen Systemen automatisch angewendet. Da jede nachträgliche Veränderung an elektronischen Dokumenten den Hashwert zum Zeitpunkt der Prüfung verändert, kann mit diesem Vergleichsverfahren jede nachträgliche Veränderung am Dokument erkennbar gemacht werden.

Der geheime private Teil des „Schlüsselbundes“ ist kennwortgeschützt und verbleibt immer bei der signierenden Person auf gesicherten Speichermedien.

Ein Außenstehender, der die Autorenschaft des Signierenden überprüfen möchte, muss darauf vertrauen können, dass der mit dem Dokument automatisch mitgelieferte öffentliche Schlüssel auch tatsächlich zu der im Schlüssel benannten Person gehört.

Ab genau diesem Punkt unterscheiden sich fortgeschrittene und qualifizierte Signaturen voneinander.

- **Fortgeschrittene Signatur (AdES):**

  Bei der fortgeschrittenen Signatur muss das ausgestellte Zertifikat inkl. des zugehörigen „Schlüsselbundes“ nicht von einem **qualifizierten Vertrauensdienstanbieter** erstellt sein. Jeder Anbieter der nach eIDAS VO [2] nicht als „qualifiziert“ gilt, kann das zuvor genannte Schlüsselpaar erstellen. Diese Möglichkeit ist unter anderem auch in einigen verfügbaren pdf-Programmen vorgesehen.

  Weiterhin sind hierfür Vertrauensdienstanbieter denkbar, welche die hohen Kriterien an qualifizierte Anbieter eIDAS-VO nicht erfüllen können oder wollen. Auch bei der AdES werden wie o.g. Schlüsselpaare erstellt, die ebenso kennwortgeschützt sind, sodass der Signierende sich durch diese eigenen Zertifikate und das nur ihm bekannte Kennwort authentifiziert.

  Ein öffentlicher Teil des Zertifikates, der zur Überprüfung der Signatur bei einem Empfänger erforderlich ist (Wurzelzertifikat), kann als Datei exportiert und den potenziellen

Empfängern von elektronischen Dokumenten zur Verfügung gestellt werden. Diese Empfänger binden sich das Wurzelzertifikat, welches die Identität des Signierenden durch den Anbieter des Vertrauensdienst bestätigt, z.B. in den lokalen Zertifikatspeicher als vertrauenswürdig ein und können damit in Zukunft die Authentizität eines vom Unterzeichner erstellten Dokumentes überprüfen.
Damit der Empfänger - nach erfolgreicher technischer Überprüfung der Signatur – auch tatsächlich von der **Authentizität** bezüglich des Absenders überzeugt sein kann, muss der öffentliche Teil des Wurzelzertifikates ihm vorher auf sicherem Wege übermittelt werden. Diese Übermittlung geschieht z.B. durch persönliche Übergabe – oder besser, von öffentlich zugänglicher authentifizierter Website oder über einen vertrauenswürdigen Verzeichnisdienst.

Die fortgeschrittene Signatur kann nach eIDAS-VO - insbesondere bei der Kommunikation mit zuvor nicht bekannten Parteien - keine eindeutig gesicherten Rückschlüsse auf den tatsächlichen Autor liefern, solange das Vertrauen des Empfängers zu dem Anbieter des Vertrauensdienstes und seinem Wurzelzertifikat nicht vollständig geklärt ist.

In einigen Bundesländern bieten die hier zuständigen Bewertungs- und Verrechnungsstellen (BVS) Vertrauensdienste für Prüfingenieure an und reichen nach erfolgreicher Identifikation den Prüfingenieuren Zertifikate für fortgeschrittene elektronische Signaturen aus. Das i.d.R. auf den BVS Homepages öffentliche BVS Wurzelzertifikat kann von jedem Empfänger signierter Dokumente auf seinem PC als „vertrauenswürdige Stammzertifizierungsstelle“ gespeichert werden und somit zur lokalen Identitätsprüfung herangezogen werden. In den Bundesländern, wo diese Regelung Anwendung findet, vertrauen die Empfänger von mitttels **AdES** signierten Dokumenten somit der jeweiligen BVS als Anbieter von Vertrauensdiensten und damit den in dieser Form elektronisch signierten Dokumenten.

- **Qualifizierte elektronische Signatur (QES):**

  Bei der qualifizierten elektronischen Signatur werden dezidierte Anforderungen an die Anbieter von Vertrauensdiensten sowie an die verwendete Signatur-Hard- und -Software gestellt. Diese Anbieter müssen die vorgegebenen Standards nachweislich einhalten und diesbezüglich nach den Vorgaben der eIDAS-VO zertifiziert sein.

  Dies beginnt damit, dass das zur Signierung verwendete Schlüsselpaar eindeutig der signierenden Person zugeordnet wird. Dies geschieht i.d.R. indem eine rechtlich anerkannte Identitätsprüfung dieser Person vorgenommen wird. Weiterhin ist die sichere Aufbewahrung und Verwendung des kennwortgeschützten privaten Schlüssels über eine entsprechend zertifizierte Hard- und Software (d.h. Signaturkarten, Kartenleser, Signatursoftware usw.) zu gewährleisten.

  Der Empfänger von mittels **QES** signierten Dokumenten kann die **Identität** des Signierenden sofort mit seiner Software überprüfen, da die Wurzelzertifikate qualifizierter Vertrauensdienstanbieter öffentlich zugänglich sind bzw. bereits in den lokalen Zertifikatspeichern am PC eingelesen wurden. Eine manuelle Übermittlung von Wurzelzertifikaten kann bei **QES** entfallen.

- **Elektronische Siegel:**

  Mit der eIDAS-VO sind auch elektronische Siegel (Organisationszertifikate) möglich, welche als **QES** dienen. Diese neuen elektronische Siegel können als digitaler Firmenstempel und gleichzeitig als Integritätsschutz für Dokumente eingesetzt werden. Inhaber des "E-Siegels" sind juristische Personen. Eine Organisation erhält so die Möglichkeit, ihre zeichnungspflichtigen Geschäftsunterlagen im Namen der Organisation zu unterschreiben. Damit ist der Ursprung beziehungsweise der Absender des Dokuments eindeutig identifizierbar. Elektronische Unterlagen können so mit einem Integritätsschutz versehen werden. Die Siegelerzeugung erfolgt dabei automatisiert und fördert so den Abbau von Papierarchiven.

- **Fernsignaturen:**

  Auf Grundlage der eIDAS-VO sind weiterhin auch Fernsignaturen möglich welche als **QES** dienen. Alternativ zur Signaturkarte sollen Fernsignaturen die Möglichkeit bieten, qualifizierte Signaturen mit Hilfe des Mobiltelefons zu erzeugen. Dabei kann auf die zusätzliche Infrastruktur für Signaturkarten und Lesegeräte verzichtet werden.

- **Einfache elektronische Signatur (ES):**

  Mit der einfachen elektronischen Signatur (z.B. eMail-Signatur oder eingescannte Unterschrift) kann die Authentizität und Integrität eines Dokumentes nicht sichergestellt werden.

5. Rechtswirkungen

Hinsichtlich der Rechtswirkung einer elektronischen Signatur wird im Artikel 25 der eIDAS-VO Folgendes festgelegt:

- Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift.

- Eine qualifizierte elektronische Signatur, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Signatur anerkannt.

6. Empfehlungen

a) Bei vorliegender Schriftformerfordernis wird für die Signierung elektronischer Dokumente die Anwendung der qualifizierten elektronischen Signatur (**QES**) empfohlen.

   Hierzu sucht man sich aus den innerhalb der EU nach eIDAS-VO gelisteten qualifizierten Vertrauensdienstanbietern einen Partner aus

   Alle nach eIDAS-VO gelisteten Anbieter erzeugen am Ende des Prozesses eine qualifizierte elektronische Signatur.

(https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home)

Die jeweiligen Anbieter unterscheiden sich stark in den anfallenden Kosten für die Dienstleistung, den jeweiligen Gültigkeitsdauern der Signatur-Zertifikate, Verwahrungsorte der privaten Schlüssel, Handhabung der zugehörigen Signaturhardware und Signatursoftware und im Einzelfall auch in den angesprochenen Zielgruppen. Es wird empfohlen, mindestens bzgl. der o.g. Kriterien Vergleiche bei mehreren Anbietern durchzuführen.

b) Der Umfang an Unterlagen, welche im Rahmen der Prüfung durch den Prüfingenieur durch **QES** zu signieren ist, richtet sich nach den länderspezifischen gesetzlichen Grundlagen. Diese können den LBO´s, und den zugehörigen Landesprüfverordnungen, welche den Ablauf der Prüfung der bautechnischen Nachweise regeln, entnommen werden. In der Regel sind bei vorliegendem Schriftformerfordernis mindestens die Prüfberichte, die bautechnischen Nachweise, die Ausführungsunterlagen (falls diese Prüfgegenstand sind), Überwachungsberichte sowie ggf. landesspezifische Formulare am Ende der Prüftätigkeit mit **QES** zu signieren.

c) Vor dem Erstellen einer Signatur wird empfohlen, das geprüfte elektronische Dokument durch einen geeigneten „Prüfstempel“ und ein „Unterschriftenbild“ zu kennzeichnen. Diese können in den meisten pdf-Editoren grafisch individuell vorbereitet und abgespeichert werden. Empfehlenswert ist weiterhin, beim Signaturvorgang automatisiert einen sichtbaren Datumsstempel (lokales Signaturdatum) auf dem digitalen Dokument zu verorten.

Die Empfehlungen unter c) sind für wirksame und gültige **QES** formal nicht erforderlich. Jedoch schaffen diese Maßnahmen, insbesondere in Übergangsphasen, ein in der Welt des Bauens vertrautes und allgemein bekanntes Layout einer durch den Prüfingenieur geprüften Unterlage.

Beispiele für Prüfstempel zur Verortung von Unterschriftenbildern von elektronischen Signaturen:

d) Durch QES signierte elektronische Dokumente, die nicht schreibgeschützt wurden, können durch pdf-Editoren im Nachhinein verändert werden. Das ggf. versehentliche Einfügen eines einzigen Punktes verändert das elektronische Dokument, verändert somit den Hashwert und würde eine elektronische Signatur brechen und dieses bei einer Integritätsprüfung der pdf-Software erkennbar machen. Zur Vermeidung von versehentlichen Änderungen am

elektronisch signierten Dokument und dem damit verbundenen Brechen der QES wird empfohlen, die Dokumente beim Signaturvorgang im pdf-Editor mit einem Schreibschutz zu versehen.

Hinweis: Im Einzelfall kann es erforderlich sein, dass weitere Ergänzungen in vom Prüfingenieur geprüften bautechnischen Nachweisen erforderlich werden. (z.B. werden in einigen Bundesländern weitere Ergänzungen durch Bauaufsichtsbehörden an geprüften Unterlagen vorgenommen oder im Falle von Mehrfachprüfinstanzen im Ingenieurbau). In diesem Falle ist auf einen Schreibschutz der geprüften elektronischen Unterlagen zu verzichten

e) Jede elektronische Signatur ist mit einem „lokalen“ Zeitpunkt des PC´s verbunden, auf welchem die Signatur erstellt wurde. Diese lokale Zeitangabe kann aus unterschiedlichen Gründen von dem realen Zeitpunkt abweichen, an welchem tatsächlich signiert wurde. Ein plausibles, einfaches Beispiel hierfür wäre u.a., dass der lokale PC, mit welchem signiert wird, fehlerhafte Zeiteinstellungen in der Systemsteuerung besitzt. Diese lokalen Einstellungen sind vom Empfänger nicht einsehbar.

   Um zusätzliches Vertrauen in den gespeicherten Signaturzeitpunkt zu erlangen, wird daher wird empfohlen, einer elektronischen Signatur einen Zeitstempel eines unabhängigen Zeitservers hinzuzufügen. Diesen zusätzlichen Dienst bieten einige qualifizierte Vertrauensdienstanbieter an.

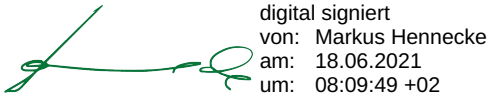
f) In den Bundesländern, die eine BVS als vertrauenswürdigen Vertrauensdienstanbieter anerkennen, kann die **AdES** – der BVS ebenso verwendet werden.

7. Weiterführende Links

https://www.elektronische-vertrauensdienste.de/cln_131/EVD/DE/Verbraucher/Vertrauensdienste/Signatur/Signatur-start.html

8. Signaturbeispiele mit Unterschriftenbild:

QES (D-Trust) Hennecke:



QES (A-Trust) Duensing:

AdES (BVS- BB) Hamann: