Die digitale Signatur in der Schweiz.
Grundlagen. Kommerzielle Nutzungsanforderungen.

Bedürfnisse und Handlungsempfehlungen zur Förderung der breiten geschäftlichen Anwendung.

Masterarbeit Digitale Transformation am Institut für Innovation und Entrepreneurship, Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)

Autor: Michael Sieber
QuoVadis Trustlink Schweiz AG

Betreuerin: Dr. Carmen Kobe
Institut für Innovation und Entrepreneurship, ZHAW

Koreferent: Reto Scagnetti
QuoVadis Trustlink Schweiz AG

Buchackern, 22.06.2021

Vorwort

Die Themenauswahl zu dieser Masterarbeit fiel mir sehr leicht. Nahezu meine gesamte berufliche Karriere verbrachte ich im Umfeld der digitalen Transformation, seit 2017 als Head of Sales & Marketing und Mitglied der Geschäftsleitung bei QuoVadis Trustlink Schweiz AG. QuoVadis bietet ihren Kunden kryptografische Services wie Gesamtkonzepte, Anwendungen und Toolkits für den Einsatz von digitalen Zertifikaten und elektronischen Signaturen an.

Digital Signing auf Basis von PKI (Public Key Infrastructure) ist eine QuoVadis Kernkompetenz und fasziniert mich seit meiner ersten Berührung mit diesem Fachgebiet. Seit nun vier Jahren beschäftige ich mich intensiv und mit voller Passion mit der digitalen Signatur im Kontext der geschäftlichen Verwendung. Die Passion beruht einerseits auf der Komplexität und Vielschichtigkeit des elektronischen Unterschreibens. So ergeben sich bei dieser kryptografischen Dienstleistung Berührungspunkte und Anforderungen aus gesetzlichen, technischen und prozessualen Bereichen. Andererseits habe ich viele Kundensituationen angetroffen, wo zwar bereits ein hoher Digitalisierungsgrad vorhanden war, jedoch für die Unterschrift von Dokumenten noch häufig auf Stift und Papier ausgewichen worden ist, wobei mein «Digitalisierungsherz» blutete.

Ich fragte mich, weshalb Digital Signing im Schweizer Geschäftsalltag noch keine dominierende Rolle spielt, obschon die gesetzliche Grundlage und Lösungen dazu bereits seit geraumer Zeit bestehen. Des Weiteren habe ich die vergangenen Jahre immer wieder die Erfahrung gemacht, dass Geschäftskunden mit der komplexen Thematik von Digital Signing (rechtlich, technisch, prozessual) überfordert waren.

Diese Masterarbeit soll eine kompakte und leichte Einführung für Unternehmensentscheider ermöglichen, welche sich mit einer Investition in Digital Signing beschäftigen. Weiter möchte ich mit dieser Masterarbeit die Anforderungen von ausgewählten Personen für eine breite geschäftliche Nutzung der digitalen Signatur erörtern. Die dabei gewonnenen Erkenntnisse und abgeleiteten Handlungsempfehlungen sollen zu einer Förderung der geschäftlichen Verwendung der digitalen Signatur beitragen.

Management Summary

Die digitale Transformation ist im Schweizer Unternehmensmarkt längst Realität. Geschäftsprozesse werden zugunsten maximaler Effizienz digitalisiert. Digitale Arbeitsprozesse ermöglichen schnelle und kostengünstige administrative Durchlaufzeiten. Geschäfte sollen jederzeit und von überall her komfortabel und digital abgeschlossen werden können. Die digitale Signatur unterstützt diese Prozessdigitalisierung und ermöglicht, anstelle der traditionellen Handunterschrift, eine gegenseitige geschäftliche Übereinkunft vollständig digital zu erzielen.

Diese Masterarbeit untersucht, welche Anforderungen ausgewählte Vertreter von Schweizer Unternehmen an eine breite geschäftliche Verwendung der digitalen Signatur stellen. Für die wichtigsten aus aktueller Angebotsperspektive nicht oder nur teilweise erfüllbaren Anforderungen werden Handlungsempfehlungen zugunsten der Förderung der breiten geschäftlichen Verwendung der digitalen Signatur abgeleitet.

Im Hauptteil I werden die Grundlagen rund um die digitale Signatur in der Schweiz erarbeitet als auch die theoretischen User-Anforderungen auf Basis systematischer Literaturrecherche vorgestellt. Um ein möglichst umfassendes Bild der Anforderungen zu erhalten, werden zusätzlich im Hauptteil II mittels qualitativen Interviews auch praxisorientierte Anforderungen erhoben.

Die aus der Theorie abgeleiteten User-Anforderungen liessen sich grösstenteils durch die Interviews (Praxis) bestätigen und erweitern. Einen grossen Fokus legten die Gesprächspartner auf ein schnelles, einfaches und vor allem vollständig digitales User-Onboarding, also der Befähigung eines Users um die digitale Signatur überhaupt nutzen zu können. Auch an den Funktionsumfang einer digitalen Signierlösung wurden starke Anforderungen gestellt: die Digital Signing Lösung soll cloudbasiert sein, individualisierbare Workflowkomponenten wie z. B. das Einladen von externen Unterzeichnern zulassen, geräteunabhängig funktionieren, Schnittstellen zu Drittapplikationen unterstützen und schlussendlich einen intuitiven Signaturprozess ermöglichen. Ebenfalls zeigten sich signifikante Erwartungen an eine exklusive Datenhaltung in der Schweiz und an höchste IT-Security Standards. Im Rahmen der geführten Gespräche ergab sich zudem eine klare Favorisierung der höchsten Schweizer Signaturstufe, der qualifizierten elektronischen Signatur.

Obschon sich viele der gestellten Anforderungen bereits mit den aktuell vorhandenen Angeboten an Digital Signing Lösungen erfüllen lassen, wurden auch Erwartungen

identifiziert, welche heute noch nicht oder nur teilweise erfüllt werden können. Als grössten noch ungelösten Schmerzpunkt wurde die noch nicht digitale, sondern physisch notwendige User-Identifikation für die Ausstellung einer qualifizierten elektronischen Signatur, festgemacht. Dieser derzeitige regulatorische Umstand zeigte sich als klarer Bremsfaktor in der Skalierung der digitalen Signatur in der Schweizer Geschäftswelt.

Wie allerdings der Ausblick dieser Masterarbeit aufzeigt, wurden bereits Massnahmen initiiert, welche die Akzeptanz einer digitalen User-Identifikation für die Ausstellung von Schweizer qualifizierten elektronischen Signaturen erreichen sollen.

Keywords: Digitale Signatur Schweiz, ZertES, qualifizierte elektronische Signatur, Prozessdigitalisierung

Hinweis

Zugunsten einer optimalen Lesbarkeit wurde in dieser Masterarbeit auf eine gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet. Die verwendeten Personenbezeichnungen richten sich immer an alle Geschlechter.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

CA	Certificate Authority
CRM	Customer Relationship Management (Tool)
CSP	Certification Service Provider
eIDAS	Europäische Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93 EG
ESIGN Gesetz	US-amerikanisches Gesetz «Electronic Signatures in Global and National Commerce Act»
FES	Fortgeschrittene elektronische Signatur
GUI	Graphical User Interface
HSM	Hardware Security Module
OR	Schweizerische Obligationenrecht
PKI	Public Key Infrastructure
QES	Qualifizierte elektronische Signatur
SLA	Service Level Agreement
TAV	Technische und Administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate
VZertES	Schweizer Verordnung über die elektronische Signatur

ZertES	Schweizer Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur)

Glossar

Digital Signing	Im Kontext dieser Masterarbeit wird damit die elektronische Signatur für natürliche Personen für die digitale Signierung von Dokumenten verstanden.
Hashwert	Ein Hashwert ist eine Art digitaler Fingerabdruck eines Dokumentes. Eindeutig und einmalig, jedoch mit dem Vorteil, dass ein Hashwert keinen Rückschluss auf Dokumentinhalte zulässt (1&1 IONOS SE, 2020).
Public Key Infrastructure	Eine Public Key Infrastruktur wird im Fachgebiet der Kryptologie angewendet. Basierend auf dieser Infrastruktur können digitale Zertifikate ausgestellt, verteilt und überprüft werden. Diese Technologie wird für das digitale Signieren von Dokumenten eingesetzt (Luber & Schmitz, 2018).
Strukturierte Daten	Strukturierte Daten sind so organisiert und aufbereitet, sodass sie für eine effiziente weitere IT-Verarbeitung und Analyse genutzt werden können (Redaktion ComputerWeekly.de, 2020).

EINLEITUNG

1. Einführung

1.1. Ausgangslage

Die digitale Transformation ist im Schweizer Unternehmensmarkt längst Realität. Geschäftsprozesse werden zugunsten maximaler Effizienz digitalisiert. Digitale Arbeitsprozesse ermöglichen schnelle und kostengünstige administrative Durchlaufzeiten sowie *strukturierte Daten* und damit datengetriebene Entscheidungsgrundlagen. Geschäfte sollen jederzeit (7x24), von überall aus (standortunabhängig), hochsicher und komfortabel digital abgeschlossen werden können.

Die digitale Signatur unterstützt diese Prozessdigitalisierung und ermöglicht - anstelle der traditionellen, analogen Handunterschrift, welche einen teuren Medienbruch bedeutet - eine gegenseitige geschäftliche Übereinkunft vollständig digital zu erzielen. In der Schweiz sind die technischen Möglichkeiten und gesetzlichen Rahmenbedingungen (Bundesgesetz über die elektronische Signatur, ZertES (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 2016)) dazu bereits vorhanden.

1.2. Problemstellung

Obschon die Prozessdigitalisierung sowohl auf Anbieter- (z. B. Bank) als auch Nachfragerseite (z. B. Neukunde einer Bank) gefordert ist, wird für die Unterschrift von Dokumenten der digitale Pfad noch häufig verlassen (Jaeggi & Bollhalder, 2019, S. 2), (Kühn, 2016), (Schneeberger, 2018). Dokumente werden weiterhin häufig ausgedruckt (Papier- und Druckkosten), via Post von der einen Partei zur anderen Partei versendet (teure Wartezeiten, Porto), von Hand unterschrieben und schlussendlich wieder via Scanprozessen (Personalaufwand) aufwändig den digitalen Unternehmenssystemen zugeführt. Weshalb wird diese letzte Meile nicht auch digitalisiert und damit der beschriebene, teure Medienbruch verhindert? Technische Lösungen und eine gesetzliche Grundlage (ZertES, erstmalig 2003 in Kraft getreten) rund um Digitales Signieren gibt es schon seit geraumer Zeit, jedoch werden Dokumente trotzdem weiterhin mehrheitlich von Hand unterschrieben.

Für den an *Digital Signing* interessierten Unternehmensentscheider fehlt es derzeit an einer kompakten, aktuellen Übersicht und Einführung in das komplexe Themenumfeld

der elektronischen Signatur in der Schweiz (technische, regulatorische, rechtliche und prozessuale Anforderungen, Ökosystem).

Die skizzierte Problemstellung erfährt eine hohe Relevanz, da in sämtlichen Unternehmen, unabhängig der Industrie oder Grösse, eine Vielzahl an Dokumenten unterschrieben werden und damit Digital Signing ein wertschöpfendes Digitalisierungspotential darstellen kann. Durch die aktuelle Corona-Pandemie und die den damit grösstenteils verbundenen Homeoffice-Modus (Der Bundesrat, 2021) wird die beschriebene Relevanz noch akzentuiert: Dokumente mit geforderten Mehrfachunterschriften von Repräsentanten einer Unternehmung können nicht mehr unmittelbar und zentral am Firmensitz unterzeichnet werden, sondern müssen einzeln zwischen den dezentral verteilten Unterzeichnern zirkuliert werden.

1.3. Forschungsfrage und Zielsetzung

Basierend auf der geschilderten Problemstellung möchte diese Masterarbeit herausfinden, welche Anforderungen ausgewählte Personen von Schweizer Unternehmen an eine breite geschäftliche Nutzung von Digital Signing stellen. Aufgrund der gewonnenen Erkenntnisse sollen aus heutiger Perspektive nicht oder nur teilweise erfüllbare Ansprüche identifiziert und Handlungsempfehlungen zur Förderung der geschäftlichen Nutzung der digitalen Signatur abgeleitet werden. Es ist beabsichtigt, die festgestellten Herausforderungen (aktuell nicht erfüllbare Anforderungen) ganzheitlich zu erfassen, womit sich die daraus abgeleiteten Handlungsempfehlungen an unterschiedliche Adressaten richten können.

Weiter soll diese Masterarbeit für den an Digital Signing interessierten Unternehmensentscheider eine noch nicht vorhandene, aktuelle und kompakte Übersicht auf das komplexe Schweizer Ökosystem der elektronischen Signatur bieten.

Die Hauptforschungsfrage lautet: «Was sind die Anforderungen von ausgewählten Vertretern von Schweizer Unternehmen zugunsten einer breiten geschäftlichen Nutzung der digitalen Signatur?»

Die Nebenfragestellung lautet: «Was sind notwendige Optimierungsmassnahmen (zuhanden verschiedener Adressaten) zugunsten einer Förderung der breiten kommerziellen Nutzung der digitalen Signatur in der Schweiz?»

1.4. Forschungsstand

Es wurde eine umfangreiche Literaturrecherche zum Themenbereich «Kommerzielle Anforderungen und Anwendung der digitalen Signatur im Rechtsraum Schweiz» betrieben.

Als Resultat war festzustellen, dass das Thema Digitale Signatur und deren kommerzielle Nutzung (als auch Anforderungen), dediziert für den Schweizer Rechtsraum, bisher wenig aktuell und ausführlich erforscht wurde. Zwar gibt es zahlreiche Literatur zur Kryptografie (als Beispiele können die Werke «Kryptografie verständlich» von Christof Paar und Jan Pelzl oder «Einführung in die Kryptographie» von Johannes Buchmann genannt werden), welche die technische Basis einer digitalen Signatur bildet, allerdings fehlen ausführliche und aktuelle Forschungsgrundlagen zu der kommerziellen Anwendung (und User-Bedürfnissen) der digitalen Signatur in der Schweiz. Der explizite Bezug zum Schweizer Rechtsraum ist für diese Masterarbeit zentral, da die Schweiz ein eigenes, anderes Gesetz für die digitale Signatur (ZertES) als z. B. Europa (eIDAS (Europäisches Parlament, 2014)) in Kraft hat und damit auch andere gesetzliche Anforderungen berücksichtigt werden müssen. Im Rahmen der Literaturrecherche bildeten gerade diese gesetzlichen und regulatorischen Grundlagen (Details in Kapitel 2.3.1) einen signifikanten Anteil.

Während der Literaturrecherche war zudem auffällig, dass zum Thema Digitale Signatur vor allem Informationen auf Internetplattformen zu finden sind, was logisch begründbar ist, da die digitale Signatur ja gerade die Alternative zu Papierprozessen (und damit Literatur auf Papier) bilden möchte.

Mit dieser Masterarbeit möchte der Autor die beschriebene Forschungslücke schliessen und auch die Perspektive von Unternehmensentscheidern und kommerziellen Anwendern zur Nutzung der digitalen Signatur im Rechtsraum Schweiz berücksichtigen.

1.5. Vorgehensweise

Im **Hauptteil I** werden die Grundlagen für die digitale Signatur in der Schweiz aufgearbeitet. Dabei werden schwerpunktmässig die rechtlichen und regulatorischen Rahmenbedingungen, heute verfügbare technische Möglichkeiten und die Key Player im Ökosystem als eine Art Bestandesaufnahme erarbeitet. Eine gründliche und systematische Literaturrecherche bildet die Grundlage für diesen theorielastigen Hauptteil I, insbesondere für die gesetzlichen und technischen Rahmenbedingungen. Ebenfalls fliessen Erkenntnisse aus der Literaturrecherche über die Digitalisierung von

Geschäftsprozessen ein, wobei die digitale Signatur eine mögliche Form darstellen kann.

Im **Hauptteil II** werden mittels empirischer Forschung die Bedürfnisse von ausgewählten Vertretern von Schweizer Unternehmen zugunsten eines breiten geschäftlichen Einsatzes der digitalen Signatur erhoben als auch die daraus gewonnenen Resultate präsentiert. Anschliessend werden Handlungsempfehlungen zugunsten einer Förderung der breiten Nutzung der digitalen Signatur im Schweizer Unternehmensmarkt abgeleitet und die Forschungsfragen beantwortet.

Der **Schlussteil** rundet die Masterarbeit mit einer kritischen Würdigung und einem Ausblick ab.

1.6. Aufbau der Arbeit

In der **Einleitung** zu dieser Masterarbeit werden insbesondere die **Ausgangslage, Problemstellung und daraus abgeleitete Forschungsfragen sowie die Vorgehensweise zur Beantwortung der Forschungsfragen** reflektiert.

Im **Hauptteil I (Kapitel 2.)** werden die **Grundlagen für die digitale Signatur in der Schweiz** erarbeitet. Dieser Teil gliedert sich in sechs Kapitel. Im Kapitel 2.1. «Definition» werden die Begrifflichkeiten «digitale Signatur» und «elektronische Signatur» beleuchtet und ein Definitionsversuch unternommen. Das Kapitel 2.2. «Verwendungszweck & Leistungsversprechen» ergründet die Vorteile bei der geschäftlichen Verwendung der digitalen Signatur. Das Kapitel 2.3. «Rechtliche und regulatorische Rahmenbedingungen» beantwortet, wie der Schweizer Gesetzgeber die digitale Signatur regelt und welche Anforderungen er an Anbieter und Anwender stellt. Eine Übersicht der relevanten Akteure im Schweizer Ökosystem der digitalen Signatur wird in Kapitel 2.4 «Marktakteure» vorgestellt. Im Kapitel 2.5. gilt der Fokus dem «Technischen Ablauf eines Signaturprozesses». Schlussendlich schliesst der Hauptteil I mit dem Kapitel 2.6. «Angebotsübersicht», welches die aktuell wichtigsten verfügbaren Digital Signing Angebote in der Schweiz aufzeigt.

Im **Hauptteil II (Kapitel 3., 4., 5., 6.) werden die Anforderungen an Digital Signing aus der Perspektive von ausgewählten Vertretern von Schweizer Unternehmen erhoben und ausgewertet.** Während im Kapitel 3. «Erhebung Anforderungen an Digital Signing im Geschäftsumfeld» die Rahmenbedingungen rund um die Erhebung der Anforderungen mittels qualitativer Befragung abgesteckt werden, konzentriert sich das Kapitel 4. «Ergebnisse Anforderungen an Digital Signing im Geschäftsumfeld» auf die

Resultate der Befragungen. Dabei werden die wichtigsten Erkenntnisse erarbeitet und vorgestellt. Im Kapitel 5. «Handlungsempfehlungen» werden für die erhobenen und aktuell nicht oder nur teilweise erfüllbaren Anforderungen Handlungsempfehlungen zur Förderung der geschäftlichen Verwendung der digitalen Signatur erarbeitet. Der Hauptteil II schliesst mit der Beantwortung der Forschungsfragen (Kapitel 6.).

Der Schlussteil (Kapitel 7.) rundet die Masterarbeit mit einer **kritischen Reflexion** und **einem Ausblick** ab.

1.7. Zielgruppe

Diese Masterarbeit soll einen Mehrwert für Unternehmensentscheider bieten, welche sich mit der Einführung der digitalen Signatur im Rechtsraum Schweiz beschäftigen. Des Weiteren sollen die erarbeiteten Handlungsempfehlungen die adressierten Marktakteure wie Anbieter von Digital Signing Lösungen oder Vertreter der regulatorischen Rahmenbedingungen (z. B. Schweizer Gesetzgeber für die elektronische Signatur) motivieren, Massnahmen zur Förderung der kommerziellen Nutzung der digitalen Signatur umzusetzen.

1.8. Abgrenzung

Im Hauptteil I dieser Masterarbeit wird eine Bestandesaufnahme der digitalen Signatur im Rechtsraum Schweiz erarbeitet. Die digitale Signatur ist stark von rechtlichen und technischen Rahmenbedingungen abhängig. Es ist nicht der Anspruch, in diesen zwei Fachbereichen eine zu hohe Detailtiefe zu erreichen, sondern vielmehr die wichtigsten Zusammenhänge für den an Digital Signing interessierten Unternehmensentscheider verständlich darzustellen.

Das Schweizer Bundesgesetz über die elektronische Signatur regelt sowohl elektronische Signaturen von natürlichen Personen als auch von juristischen Personen. Diese Masterarbeit konzentriert sich dabei ausschliesslich auf die geschäftliche Verwendung von elektronischen Signaturen von natürlichen Personen.

Ebenfalls gilt es festzuhalten, dass sich die rechtlichen und technischen Anforderungen an eine digitale Signatur je nach Rechtsraum unterscheiden können. So hat z. B. der Rechtsraum Europa ein eigenes Gesetz über die elektronische Signatur (eIDAS), welches sich von der Schweizer Gesetzeslage (ZertES) unterscheidet. Diese Masterarbeit fokussiert sich explizit auf die digitale Signatur im Rechtsraum Schweiz.

Das E-ID-Gesetz (Schweizerische Eidgenossenschaft, 2021), über welches die Schweizer Stimmberechtigten am 07. März 2021 abgestimmt und dieses abgelehnt hatten, wird nur im Ausblick (Kapitel 7.2.) thematisiert. Die Gründe dafür liegen einerseits in der Ablehnung des Gesetzes und andererseits darin, dass selbst bei einer Annahme eine notwendige Konkretisierung in Bezug auf die Personenidentifikation zur Befähigung einer digitalen Signatur erst noch hätte ausgearbeitet werden müssen.

Die im Hauptteil II erhobenen Anforderungen an Digital Signing aus geschäftlicher User-Perspektive und daraus abgeleiteten Handlungsempfehlungen zugunsten einer Förderung der kommerziellen Nutzung der digitalen Signatur sind nicht repräsentativ, sondern haben lediglich Gültigkeit für die interviewten Personen. Eine Überprüfung der gewonnenen Erkenntnisse auf eine Allgemeingültigkeit für entsprechende Unternehmensgrössen und -industrien oder Funktionen der Anwender ist nicht Teil dieser Masterarbeit, stellt aber einen interessanten Nachfolgeforschungsauftrag dar.

HAUPTTEIL I

2. Die digitale Signatur in der Schweiz: Eine Bestandesaufnahme

In diesem Kapitel werden die wichtigsten Eckpfeiler rund um Digital Signing in der Schweiz erarbeitet. Gestartet mit der Begriffsdefinition der digitalen Signatur (Kapitel 2.1.), wird anschliessend in Kapitel 2.2 Sinn und Zweck erörtert. Das Kapitel 2.3. fokussiert sich auf die Gesetzeslage und regulatorischen Anforderungen rund um die digitale Signatur in der Schweiz. Während die wichtigsten Marktakteure im Ökosystem in Kapitel 2.4. vorgestellt werden, dokumentiert das Kapitel 2.5. die digitale Signierung eines Dokuments Schritt für Schritt. Den Abschluss bildet das Kapitel 2.6. mit einer Übersicht zu den aktuell verbreitetsten Digital Signing Lösungen in der Schweiz.

Die in diesem Kapitel gewonnenen Erkenntnisse dienen als Grundverständnis, um in den nachfolgenden Kapiteln gewinnbringende Outputs zur Förderung der geschäftlichen Verwendung der digitalen Signatur zu erreichen.

2.1. Definition

In der Praxis werden die Begriffe «elektronische Signatur» und «digitale Signatur» oftmals - zum Teil fälschlicherweise, abhängig von länderspezifischer Gesetzgebung - als Synonym verwendet. Es herrscht zwar ein gemeinsames Verständnis darüber, dass beide Bezeichnungen auf das digitale Äquivalent zur analogen Handunterschrift hindeuten sollen, allerdings können länderspezifisch die beiden Benennungen unterschiedliche Ausgestaltungen in den technischen und regulatorischen Anforderungen ausweisen.

Die **elektronische Signatur** ist in vielen Ländern sehr breit gefasst, so bezeichnet z. B. das amerikanische ESIGN Gesetz (U.S. Government, 2000) in der Sec. 106. Definitions. im 5. Absatz die elektronische Signatur «als einen elektronischen Ton, ein elektronisches Symbol oder ein elektronisches Verfahren, das an einen Vertrag oder eine andere Aufzeichnung angehängt oder damit logisch verbunden ist und von einer Person mit der Absicht, die Aufzeichnung zu unterzeichnen, ausgeführt oder angenommen wird». In Konsequenz bedeutet dies, dass eine elektronische Signatur in diesem Kontext auch ein eingetippter Name in einem elektronischen Dokument sein kann, womit weder die Authentizität des Unterzeichners (unbestreitbare Nachvollziehung, wer unterzeichnet hat) noch die Integrität des unterzeichneten

Dokumentes (der Dokumenteninhalt wurde nach der Unterzeichnung nicht mehr verändert) einwandfrei nachvollziehbar sichergestellt sind.

Die praxisbasierte Definition der **digitalen Signatur** ist dabei konkreter, sie stützt sich auf ein *PKI*-basiertes digitales Zertifikat, welches von einer öffentlich anerkannten Zertifizierungsstelle (*CA*) ausgestellt wird (DocuSign Contributor, 2021). Durch dieses eingesetzte Verfahren werden sowohl die Authentizität der unterzeichnenden Personen als auch die Integrität des unterzeichneten Dokuments sichergestellt (eine detailliertere Beschreibung zu diesem Verfahren findet sich in Kapiteln 2.3. und 2.5.). Die digitale Signatur kann damit als eine mögliche Form der elektronischen Signatur angesehen werden (DocuSign Contributor, 2021).

Im **Rechtsraum Schweiz** ist die elektronische Signatur im Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 2016) geregelt. Anders als z. B. das amerikanische ESIGN Gesetz verweist das Schweizer Bundesgesetz über die elektronische Signatur bereits im Titel auf Attribute einer digitalen Signatur wie «Zertifizierungsdienste» oder «digitale Zertifikate». Im 1. Abschnitt «Allgemeine Bestimmungen» wird dann noch konkreter festgehalten, dass dieses Gesetz u. a. «die Anforderungen an die Qualität bestimmter digitaler Zertifikate und an ihre Verwendung (Art. 1 Abs. 1 Bst. a ZertES)» als auch die «Rechte und Pflichten der anerkannten Anbieterinnen von Zertifizierungsdiensten (Art. 1 Abs. 1 Bst. c ZertES)» regelt. **Im Schweizer Gesetzeskontext kann folglich die elektronische Signatur als digitale Signatur verstanden werden,** was das Schweizer Bundesamt für Kommunikation BAKOM in ihrer Definition der elektronischen Signatur unter Nennung von Eigenschaften einer digitalen Signatur unterstreicht (Bundesamt für Kommunikation BAKOM, 2020): «Die elektronische Signatur ist ein technisches Verfahren zur Überprüfung der Echtheit eines Dokuments, einer elektronischen Nachricht oder anderer elektronischer Daten sowie der Identität des Unterzeichnenden. Sie basiert auf einer Zertifizierungsinfrastruktur, die von vertrauenswürdigen Dritten verwaltet wird: den Anbieterinnen von Zertifizierungsdiensten.» Diese Masterarbeit fokussiert sich auf die digitale Signatur im Schweizer Rechtsraum auf Basis von PKI-basierten Zertifikaten einer öffentlich anerkannten Zertifizierungsstelle. Obschon wie erläutert im Schweizer Gesetzeskontext die elektronische und digitale Signatur als Synonym benutzt werden können, verwendet der Autor fortfolgend mehrheitlich den Begriff «digitale Signatur», da sich dieser international für PKI-basierte Signaturen durchgesetzt hat.

Im Schweizer Bundesgesetz über die elektronische Signatur werden im Art. 2 verschiedene Signaturtypen festgehalten, wobei u. a. zwischen Signaturen von natürlichen Personen (die Signatur wird einer natürlichen Person zugeordnet) und von juristischen Personen (die Signatur wird einer juristischen Person zugeordnet, unterschrieben wird mit sogenannten Firmensiegeln) unterschieden wird. Da sich diese Masterarbeit ausschliesslich mit der geschäftlichen Verwendung der digitalen Signatur von natürlichen Personen beschäftigt, werden nachfolgend die wichtigsten im ZertES festgehaltenen digitalen persönlichen Signaturtypen vorgestellt:

Signaturbezeichnung ZertES	**Zertifikatsbasis**	**Sicher-stellung Authentizität des Unter-zeichners**	**Sicher-stellung Integrität des unter-schrieb-enen Doku-mentes**	**Der eigen-händigen Unterschrift gesetzlich gleich-gestellt**	**Für natürliche Personen**
Fortgeschrittene elektronische Signatur (FES)	Ja, digitales Zertifikat	Ja	Ja	Nein	Ja
Geregelte elektronische Signatur	Ja, geregeltes Zertifikat	Ja	Ja	Nein	Ja
Qualifizierte elektronische Signatur (QES)	Ja, qualifiziertes Zertifikat. Verwendungszweck ausschliesslich für die elektronische Signatur*. **: rein technisch kann z. B. eine FES nicht nur zum Signieren von Dokumenten, sondern auch für Loginzwecke (Authentisierung) genutzt werden. Bei der QES wird die Verwend-ung gesetzlich auf die elektronische Signatur eingeschränkt.*	Ja	Ja	**Ja,** **Art. 14 Abs. 2bis OR**	Ja

Tabelle 1 Ausgewählte digitale persönliche Signaturtypen gemäss ZertES

Quelle: eigene Darstellung

Das Schweizer Bundesgesetz über die elektronische Signatur hält fest, dass eine **qualifizierte elektronische Signatur,** welche als einzige der Handunterschrift gesetzlich gleichgestellt ist (Art. 14 Abs. 2bis OR), **auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten** beruhen muss (Art. 2 Bst. e, g, h ZertES). Diese zertifizierten Dienstleister bestätigen durch auf Basis ihrer ausgestellten Zertifikate erzeugten Signaturen die Authentizität des Unterzeichners und stellen durch das technische Signaturverfahren (Details dazu in Kapitel 2.5.) die Integrität des unterzeichneten Dokumentes sicher. Die Schweizerische Akkreditierungsstelle SAS publiziert hierzu auf ihrer Website (Schweizerische Akkreditierungsstelle SAS, 2021) die aktuell anerkannten Anbieterinnen, welche in Kapitel 2.4 «Marktakteure» dieser Masterarbeit näher vorgestellt werden.

Es gilt als bemerkenswert festzuhalten, dass das Schweizer Bundesgesetz über die elektronische Signatur zwar mehrere digitale persönliche Signaturtypen definiert (Details in Tabelle 1), allerdings nicht, in welchen Fällen diese verwendet werden können. Dazu nimmt dann das Schweizerische Obligationenrecht (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 2021) Stellung und definiert, welche Verträge Schriftlichkeit (Art. 11 Abs. 1 OR) und eine Unterzeichnung der verpflichtenden Personen (Art. 13 Abs. 1 OR) verlangen. Dort, wo eine Unterzeichnung verlangt ist, verweist der Art. 14 Abs. 1 OR, dass die Unterschrift eigenhändig zu schreiben ist und Art. 14 Abs. 2bis OR setzt der eigenhändigen Unterschrift die qualifizierte elektronische Signatur in Kombination mit einem qualifizierten Zeitstempel gleich. Als Konsequenz daraus lässt sich ableiten, dass von den im Schweizer Bundesgesetz über die elektronische Signatur definierten digitalen persönlichen Signaturen einzig die qualifizierte elektronische Signatur explizite gesetzliche Verwendung findet und für die anderen Typen (z. B. fortgeschrittene elektronische Signatur) keine gesetzliche Verwendung vorgesehen ist.

Wie die digitale Signatur im Geschäftsalltag verwendet werden kann und welche Vorteile damit einhergehen sollen, wird im nächsten Kapitel thematisiert.

2.2. Verwendungszweck und Leistungsversprechen

Nachdem im Kapitel 2.1. ein Definitionsversuch für die digitale Signatur und eine erste Einordnung in den Rechtsraum Schweiz erarbeitet wurde, soll in diesem Kapitel der beabsichtigte Verwendungszweck und das Leistungsversprechen, quasi die Daseinsberechtigung für die digitale Signatur, erörtert werden.

Die digitale Signatur soll die traditionelle, analoge Handunterschrift vorteilhaft ersetzen. Unzählige, ehemals analoge Unternehmensprozesse, sind bereits durch digitalisierte Abläufe wertschöpfend ersetzt worden. So findet heute beispielsweise die schriftliche geschäftliche Kommunikation dominierend digital per E-Mail statt, was gegenüber dem früheren analogen Postversand deutliche Schnelligkeits- und Kostenvorteile mit sich bringt. Als ein anderes Beispiel kann die digitalisierte Kundenkartei in Form eines *CRM*-Systems genannt werden, welches sämtliche Kundenberührungspunkte und Aktivitäten erhebt, verwaltet und übersichtlich auf Knopfdruck anzeigen kann. Trotz all dieser digitalen Errungenschaften greifen Unternehmen im Rahmen von Unterzeichnungsprozessen noch häufig auf die analoge Handunterschrift zurück (Jaeggi & Bollhalder, 2019, S. 2), (Kühn, 2016), (Schneeberger, 2018) und torpedieren damit vorgängig erreichte digitale Vorteile: zu unterzeichnende Dokumente werden ausgedruckt (Papier- und Druckkosten), zur Unterschrift postalisch versendet (Versandkosten, Wartezeit) und nach erfolgter Unterzeichnung wieder via Scanprozessen (manueller Aufwand) den Unternehmenssystemen zugeführt. Diese im Zusammenhang mit der analogen Unterzeichnung von Dokumenten beschriebenen Nachteile sollen mit der digitalen Signatur gelöst werden.

- Die elektronische Signatur soll diese «letzte Meile» eines Prozesses ebenfalls digitalisieren und einen **teuren Medienbruch verhindern.** Medienbrüche innerhalb einer Customer Journey (z. B. wenn ein Hypothekenangebot vom Interessenten zwar vollständig digital verglichen und ausgesucht werden kann, jedoch der finale Vertragsabschluss via Handunterschrift auf Papier verlangt wird) sollten grösstmöglich reduziert werden, da jeder Medienbruch das Risiko eines potentiellen Kundenabsprunges erhöht und auch die Fehlerquote (Informationen gehen verloren, falsche Übertragung) steigt (Feldbrügge & Brecht-Hadraschek, 2008, S. 45).
- Da dadurch Dokumente nicht mehr ausgedruckt werden müssen, werden nicht nur die **Papier- und Druckkosten gesenkt,** sondern auch die **ökologische Effizienz optimiert.**
- Dass der Austausch von Dokumenten zur elektronischen Signierung ebenfalls digital erfolgen kann (z. B. via E-Mail) und damit auf einen postalischen Versand verzichtet werden kann, trägt ebenfalls zur Verbesserung der Nachhaltigkeit und zu **Kostenersparnissen (Porto)** bei. An dieser Stelle tritt allerdings noch ein wichtigerer Vorteil ein, nämlich die **Zeitersparnis** (keine Versandwartezeiten) und die **Erfüllung des Kundenanspruches nach individuell präferierten Geschäftsabschlusszeiten. Geschäftsabschlüsse mit** der Notwendigkeit von

Unterschriften sollen zu **jederzeit** und von **überall** aus, ohne Wartezeiten und bevorzugt via Mobile (Rieber, 2017, S. 2) getätigt werden können. Dies kann gut im Rahmen einer Bankkontoeröffnung illustriert werden: ein Bankneukunde kann dabei zu seiner präferierten Zeit, z. B. am Samstagnachmittag («jederzeit», keine Rücksicht auf Banköffnungszeiten) bequem vom Sofa aus («überall», keine Notwendigkeit eines Filialbesuches, was in Zeiten der aktuellen Corona-Pandemie ebenfalls vorteilig ist) mittels Digital Signing (und vorausgegangener Videoidentifikation des Neukunden) ein Bankkonto eröffnen.

- Eine **digitale und medienbruchfreie Customer-Journey** ermöglicht das **Erkennen von Kunden- und Nutzungsdaten** (Appelfeller & Feldmann, 2018, S. 39), welche **wertschöpfend verwertet werden können.** Zum Beispiel kann eine Bank so Rückschlüsse gewinnen, an welchen Wochen- und Tageszeiten Neukunden schwergewichtig Konten eröffnen und entsprechend Marketingaktivitäten daraufhin bündeln. Des Weiteren wird damit der **Anspruch der Generationen Y und Z,** welche für Unternehmen eine ernstzunehmende Zielgruppe und Kaufkraft darstellen, nach digitalen Kundenbeziehungen (Kleinjohann & Reinecke, 2020, S. 5) ebenfalls **erfüllt**.
- Die manuelle Rückführung von unterschriebenen Papierdokumenten in die IT-Systemlandschaft eines Unternehmens ist nicht mehr nötig. **Die elektronisch unterzeichneten Dokumente liegen bereits vollständig digital vor,** was wiederum eine **Zeit- und Kostenersparnis** (manuelle Scanprozesse mit entsprechendem Personalaufwand werden reduziert) erwirkt.
- Durch den durchgehend digitalen Prozess liegen **strukturierte Daten** vor, was die Weiterverarbeitung von Nachfolgeprozessen stark optimiert. Während z. B. bei einem eingescannten Dokument die Suchfunktion nach Stichworten innerhalb des Dokumentes eingeschränkt ist, kann ein vollständig digitales Dokument, welches auf strukturierten Daten beruht, einfach und effizient nach Keywords durchsucht werden.
- Während eine Handunterschrift leicht gefälscht werden kann (wer hat noch nie die Unterschrift der Eltern für eine schlechte Schulbenotung gefälscht?) stellt das technische Verfahren einer zertifikatsbasierten digitalen Signatur die **Dokumentenintegrität** (der Dokumenteninhalt wurde nach der Unterzeichnung nicht mehr verändert) und die **Authentizität des Unterzeichners** (es kann zweifelsfrei festgestellt werden, wer ein Dokument signiert hat) sicher. Die Authentizität des Unterzeichners wird durch die vorgängig erfolgte Personenidentifikation (Details in Kapitel 2.3.2) sowie einer der Signatur vorausgehenden starken 2-Faktor-Authentisierung des Users gewährleistet. Die

Integrität wird durch den Vergleich der *Hashwerte* (Hashwert des Dokuments vor und nach der Signatur) sichergestellt. Details zu diesem Verfahren finden sich in Kapitel 2.5.

- Selbst der Schweizer Gesetzgeber erachtet die qualifizierte elektronische Signatur als derart sicher, dass er hierzu im Gegensatz zur Handunterschrift mittels Art. 59a[22] Abs. 1 und 2 OR sogar die **Umkehr der Beweislast** ermöglicht.

In jeder Unternehmensindustrie werden Dokumente unterzeichnet, vom Arbeitsvertrag über die Auftragsbestätigung bis hin zur Spesenabrechnung. Je höher das Signaturvolumen desto höher wiegen die Nachteile der traditionellen Handunterschrift. Die folgenden Kundenindustrien und Anwendungsbereiche können als gute Beispiele mit hohen Signaturvolumen herangezogen werden:

- **Finanzindustrie** (z. B. Bankkontoeröffnung oder Hypothekengeschäfte)
- **Treuhandwesen** (z. B. Revisionsberichte)
- **Rechtswesen** (z. B. Anträge, Urteile)
- **Versicherungsindustrie** (z. B. Policen)
- **Gesundheitssektor** (z. B. Diagnosen oder Rezepte)
- **Immobiliensektor** (z. B. Mietverträge)
- **Automobilindustrie** (z. B. Kauf- oder Leasingverträge)
- **Personaldienstleister** (z. B. Arbeitsverträge)

In den aufgeführten Anwendungsfällen liegen häufig sensible (z. B. vertrauenswürdige, haftungsrelevante) Inhalte vor, wo man mittels einer Unterschrift zu einem bestimmten Zeitpunkt vorliegende und von den Vertragsparteien zugestimmte Inhalte zweifelsfrei festhalten möchte.

2.3. Rechtliche und regulatorische Rahmenbedingungen

Nachdem im vorherigen Kapitel die Vorteile von Digital Signing präsentiert wurden, untersucht dieses Kapitel, wie die digitale Signatur in der Schweiz gesetzlich geregelt ist.

Vorab gilt es festzuhalten, dass nur in sehr wenigen und im Schweizerischen Obligationenrecht definierten Verträgen Schriftlichkeit (Art. 11 Abs. 1 OR) und die Unterzeichnung der verpflichtenden Personen (Art. 13 Abs. 1 OR) gesetzlich gefordert sind. Als Beispiel hierzu kann das Schenkungsversprechen (Art. 243 Abs. 1 OR) genannt werden. Trotzdem werden im Geschäftsalltag viele Dokumente (einige Beispiele sind im

Kapitel 2.2 genannt), auch solche bei welchen das Gesetz keine Schriftlichkeit und Unterschrift verlangt, schriftlich festgehalten und von den Vertragsparteien unterzeichnet. Die Vertragsparteien verschaffen sich damit die Sicherheit, dass in einem potenziellen Streitfall die Vertragskonditionen als auch die Willensbekundung der Vertragsteilnehmer durch die Unterzeichnung nachweisbar festgehalten sind. Wie dieses komfortable Gefühl der Sicherheit auch in Form von digitalen Signaturen gesetzlich geregelt ist, ergründen die nachfolgenden Kapitel.

2.3.1. Die rechtlichen und regulatorischen Quellen

Um ein Verständnis für die Regulierung der elektronischen Signatur in der Schweiz zu erhalten, gilt es im Wesentlichen die folgenden Bestimmungen zu berücksichtigen:

- **OR** Schweizerisches Obligationenrecht (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 2021)
- **ZertES** Schweizer Bundesgesetz über die elektronische Signatur (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 2016)
- **VZertES** Schweizer Verordnung über die elektronische Signatur (Schweizerische Bundesrat, 2016)
- **TAV** Technische und Administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesamt für Kommunikation BAKOM, 2016)

Eine zentrale Bedeutung nimmt das **Schweizerische Obligationenrecht OR** ein, welches die Gleichstellung der qualifizierten elektronischen Signatur zur Handunterschrift regelt. Art. 14 Abs. 2^{bis} OR hält dazu fest: «Der eigenhändigen Unterschrift gleichgestellt ist die mit einem qualifizierten Zeitstempel verbundene qualifizierte elektronische Signatur gemäss Bundesgesetz vom 18. März 2016 über die elektronische Signatur.». Eine weitere wichtige Bestimmung findet sich im Art. $59a^{30}$ Abs. 1 OR: «Der Inhaber eines kryptografischen Schlüssels, der zur Erzeugung elektronischer Signaturen oder Siegel eingesetzt wird, haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf ein gültiges geregeltes Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 18. März 2016 über die elektronische Signatur verlassen haben.» Der Gesetzgeber anerkennt damit die qualifizierte elektronische Signatur als derart sicher, dass er die Umkehr der Beweislast ermöglicht. In einem allfälligen Streitfall über die Frage, ob ein gültig unterzeichneter Vertrag vorliegt oder nicht, muss der Kläger, sofern qualifizierte elektronische Signaturen verwendet wurden, nicht nachweisen, dass der Vertrag gültig unterzeichnet worden ist, sondern die Gegenpartei muss beweisen, dass dies nicht der Fall ist.

Das **Schweizer Bundesgesetz über die elektronische Signatur (ZertES)** regelt das digitale Äquivalent zur Handunterschrift und u.a. die Anforderungen an die Ausstellung einer qualifizierten elektronischen Signatur, auf welche sich das Schweizerische Obligationenrecht in der Gleichstellung zur eigenhändigen Unterschrift bezieht. Die wichtigsten Bestimmungen werden nachfolgend vorgestellt:

- Im **1. Abschnitt «allgemeine Bestimmungen»** definiert der Art. 2 ZertES verschiedene elektronische Signaturtypen als auch, auf welcher technischen Basis (Zertifikat) diese erstellt werden dürfen, u.a.:
    - Die qualifizierte elektronische Signatur muss gemäss Art. 2 Bst. e ZertES auf einem qualifizierten Zertifikat beruhen.
        - Das referenzierte qualifizierte Zertifikat ist «ein geregeltes Zertifikat, das die Anforderungen nach Artikel 8 erfüllt» (Art. 2 Bst. h ZertES). Der erwähnte Artikel 8 wird nachfolgend unter dem 4. Abschnitt noch genauer vorgestellt.
        - Das erwähnte geregelte Zertifikat ist «ein digitales Zertifikat, das die Anforderungen nach Artikel 7 erfüllt und von einer nach diesem Gesetz anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt wurde (Art. 2 Bst. g ZertES). Der referenzierte Artikel 7 wird nachfolgend unter dem 4. Abschnitt noch genauer vorgestellt.
        - Die genannte Anbieterin von Zertifizierungsdiensten wird im Art. 2 Bst. k ZertES wie folgt beschrieben: «Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt.» Entsprechende Anbieterinnen müssen anerkannt werden, wozu nachfolgend die Anforderungen unter dem 2. Abschnitt vorgestellt werden.
    - Der im Art. 14 Abs. 2^{bis} OR bzgl. der Gleichstellung zur eigenhändigen Unterschrift in Kombination mit der qualifizierten elektronischen Signatur verlangte qualifizierte elektronische Zeitstempel wird im Art. 2 Bst. j ZertES definiert. Der qualifizierte elektronische Zeitstempel darf nur von einer anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt werden und bestätigt damit unbestreitbar, dass bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen sind.
    - Abschliessend kann zum Art. 2 ZertES festgehalten werden, dass zwar verschiedene elektronische persönliche Signaturtypen deklariert sind,

sich das ZertES allerdings über deren Rechtswirkungen in der Verwendung ausschweigt.

- Im **2. Abschnitt «Anerkennung der Anbieterinnen von Zertifizierungsdiensten»** wird deklariert, unter welchen Voraussetzungen sich Anbieterinnen von Zertifizierungsdiensten (welche dann wiederum bemächtigt sind, ZertES-konforme elektronische Zertifikate und Signaturen auszustellen) anerkennen lassen können. Dabei stechen die folgenden Anforderungen wesentlich heraus:
    - Fähigkeit (z. B. Informatiksysteme und Fachpersonal), qualifizierte Zertifikate gemäss den gestellten Anforderungen auszustellen und zu verwalten (Art. 3 Abs. 1 Bst. b, c, d ZertES).
    - Verfügbarkeit über ausreichende Finanzmittel- oder garantien (Art. 3 Abs. 1 Bst. e ZertES). Eine Konkretisierung dazu findet sich in der Verordnung über die elektronische Signatur in Art. 2 Abs. 1, wo verlangt wird, dass eine anerkannte Anbieterin zur Deckung ihrer Haftung eine Versicherung von mindestens CHF 2 Mio. pro Versicherungsfall und CHF 8 Mio. pro Versicherungsjahr abschliessen muss.
    - Darüber hinaus verweist der Art. 5 Abs. 2 ZertES, dass die zuständige Akkreditierungsstelle der Öffentlichkeit eine Liste mit anerkannten Anbieterinnen von Zertifizierungsdiensten zur Verfügung stellen muss. Diese Liste ist über die Website der Schweizerischen Akkreditierungsstelle SAS abrufbar und die aktuellste Form vom März 2021 im Anhang dieser Masterarbeit verfügbar.
- Der **3. Abschnitt widmet sich der «Generierung, Speicherung und Verwendung kryptografischer Schlüssel».**
    - Im Art. 6 Abs. 1 ZertES sichert sich der Bundesrat das grundsätzliche Recht zu, konkrete Anforderungen zur Generierung, Speicherung und Verwendung kryptografischer Schlüssel zu regeln. Diese Konkretisierung findet schlussendlich in der Verordnung des ZertES und den TAV statt.
    - Im Art. 6 Abs. 2 ZertES sind minimale Anforderungen zur Generierung, Speicherung und Verwendung kryptografischer Schlüssel festgehalten, insbesondere dass die Schlüssel einmalig und nicht ableitbar sein müssen.

- Der **4. Abschnitt** definiert die Anforderungen an **«geregelte Zertifikate»** und qualifizierte Zertifikate.
    - Der Art. 7 Abs. 2 ZertES regelt, welche Angaben ein geregeltes Zertifikat enthalten muss, u.a.:
        - «den Hinweis, dass es sich um ein geregeltes Zertifikat handelt» (Bst. b)
        - «den Namen oder die Bezeichnung der Inhaberin oder des Inhabers des zugehörigen privaten kryptografischen Schlüssels; besteht eine Verwechslungsmöglichkeit, so ist der Name oder die Bezeichnung mit einem unterscheidenden Zusatz zu versehen» (Bst. c)
        - «den öffentlichen kryptografischen Schlüssel» (Bst. f)
        - «die Gültigkeitsdauer» (Bst. g)
        - «den Namen, den Niederlassungsstaat und das geregelte elektronische Siegel der Anbieterin von Zertifizierungsdiensten, die das Zertifikat ausstellt.» (Bst. h)
    - Der Art. 8 ZertES regelt dann die zusätzlichen Anforderungen an qualifizierte Zertifikate, welche die Basis für die Ausstellung von qualifizierten elektronischen Signaturen darstellen.
        - Während ein geregeltes Zertifikat auch auf eine Unternehmung ausgestellt werden kann, ist die Ausstellung eines qualifizierten Zertifikates nur für natürliche Personen erlaubt (Abs. 1).
        - Der Verwendungszweck des qualifizierten Zertifikates wird eingeschränkt und kann ausschliesslich für die elektronische Signatur verwendet werden (Abs. 2).
        - Es muss im Zertifikat ausgewiesen sein, dass es sich um ein qualifiziertes Zertifikat handelt (Abs. 3).

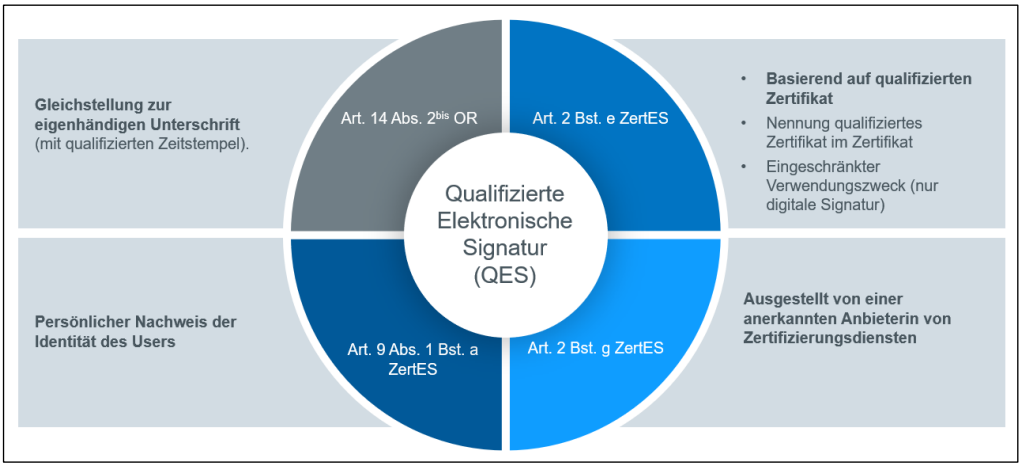


Abbildung 1 Wichtigste Eigenschaften QES

Quelle: eigene Darstellung

- Im **5. Abschnitt** werden die «**Pflichten anerkannter Anbieterinnen von Zertifizierungsdiensten»** festgehalten. Dabei werden insbesondere im Art. 9 ZertES die Anforderungen an die Identifikation von Antragsstellern für ein geregeltes Zertifikat festgelegt. Der Autor erachtet diese Voraussetzungen als derart wichtig und erfolgskritisch für den Durchbruch von Digital Signing, dass er diesem Thema ein eigenes Kapitel 2.3.2. widmet.
- Die weiteren Abschnitte 6. «Aufsicht über die anerkannten Anbieterinnen von Zertifizierungsdiensten», 7. «Haftung», 8. «Internationale Abkommen» und 9. «Schlussbestimmungen» werden im Kontext auf diese Masterarbeit als weniger relevant erachtet und nicht weiter vertieft.

Die **Verordnung über die elektronische Signatur, VZertES,** konkretisiert die Ausführungen des ZertES in vielen Bereichen. Die wichtigsten Konkretisierungen finden sich dabei in den Artikeln 5 «Ausstellung geregelter Zertifikate auf natürliche Personen» und 7 «Befreiung von der Pflicht des persönlichen Erscheinens», welche in direktem Zusammenhang mit den Anforderungen an die Identifizierung eines Antragsstellers für eine qualifizierte elektronische Signatur stehen. Da dies für die Förderung der geschäftlichen Verwendung der digitalen Signatur erfolgskritisch erscheint, wird die User-Identifikation separat im Kapitel 2.3.2 aufgearbeitet.

Die **technischen und administrativen Vorschriften (TAV) über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate** konkretisieren die in ZertES und VZertES definierten Anforderungen an Anbieterinnen von Zertifizierungsdiensten für die Ausstellung von qualifizierten Zertifikaten weiter. Dabei stützt sich das TAV-Regelwerk

grösstenteils auf bereits bestehende internationale Normen. Nebst grundlegenden Anforderungen über die Organisation und operativen Grundsätze von anerkannten Anbieterinnen von Zertifizierungsdiensten wird Fokus auf die folgenden Anforderungen gelegt:

- Verwaltung der Schlüssel: ein qualifiziertes Zertifikat beruht auf kryptografischen Dienstleistungen. Dabei werden digitale Schlüssel geschaffen, zu deren Generierung und Verwaltung das TAV-Regelwerk Anforderungen für die Anbieterinnen von Zertifizierungsdienstleistungen vorschreibt, z. B. welche Anforderungen eine Signaturerstellungseinheit (Hardware wie HSM) erfüllen muss.
- Verwaltung geregelter Zertifikate: in diesem TAV-Kapitel wird u.a. behandelt, wie die Ungültigkeitserklärung für geregelte Zertifikate gehandhabt werden muss und welche Attribute das technische Format eines geregelten Zertifikats ausweisen muss. Dabei kommt dem qualifizierten Zertifikat, welches die Grundlage für die qualifizierte elektronische Signatur bildet, die Besonderheit zu, dass der Hinweis «qualified certificate» im Zertifikatsinhalt ausgewiesen werden muss.

Auf eine Vertiefung dieser TAV-Anforderungen und referenzierten internationaler Normen wird im Rahmen dieser Masterarbeit und entsprechender Umfang-Anforderung bewusst verzichtet.

Zusammenfassend kann festgehalten werden, dass im Schweizer Rechtsraum einzig die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gesetzlich via dem Schweizer Obligationenrecht gleichgestellt ist. Die Anforderungen an die Ausstellung einer qualifizierten elektronischen Signatur werden im Schweizer Bundesgesetz über die elektronische Signatur (ZertES) dargestellt und in der Verordnung (VZertES) und den Technischen und Administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (TAV) konkretisiert. Die qualifizierte elektronische Signatur darf ausschliesslich von anerkannten Anbietern von Zertifizierungsdienstleistungen ausgestellt werden.

Abbildung 2 Gesetzeshierarchie qualifizierte elektronische Signatur

Quelle: (QuoVadis Trustlink Schweiz AG (intern))

2.3.2. Identifikation von Antragsstellern für die qualifizierte elektronische Signatur

Mit der qualifizierten elektronischen Signatur können Dokumente wie Verträge vollständig digital und rechtsgültig - der eigenhändigen Unterschrift gleichgestellt - unterzeichnet werden. Entsprechend unabdingbar gilt es sicherzustellen, dass die digitale Signatur der «korrekten» natürlichen Person zugewiesen ist und auch ausschliesslich von ihr ausgelöst werden kann. Das ZertES regelt dazu im Art. 9 Abs. 1 Bst. a sinngemäss, dass Antragssteller auf ein geregeltes Zertifikat (welches mit zusätzlichen Attributen (qualifiziertes Zertifikat) die Basis für die qualifizierte elektronische Signatur bildet) persönlich bei einer anerkannten Anbieterin von Zertifizierungsdiensten zwecks einer Identifikationsbestätigung erscheinen müssen. Art. 9 Abs. 6 ZertES ermöglicht es den anerkannten Anbieterinnen von Zertifizierungsdiensten allerdings, diese persönliche Identifikationsprüfung von Antragstellern auch an Dritte zu delegieren, allerdings bleiben sie dabei weiterhin für die korrekte Ausführung der Aufgabe haftbar.

Die Verordnung zum ZertES erlaubt im Artikel 7 im Rahmen der Nachweiserbringung der Identität eines Antragsstellers für die Ausstellung eines geregelten Zertifikates unter bestimmten Umständen eine Befreiung der Pflicht des persönlichen Erscheinens. Absatz 1 hält dazu fest, dass die Identität einer Person, die ein geregeltes Zertifikat beantragt, auch auf Distanz festgestellt werden kann, sofern eine Konformitätsbewertungsstelle bestätigt hat, dass das verwendete Verfahren zur Personenidentifikation eine

gleichwertige Sicherheit zum persönlichen Erscheinen bietet. Im Kontext der Befähigung zur qualifizierten elektronischen Signatur muss die Schweizerische Akkreditierungsstelle SAS diese ebenbürtige Sicherheit bestätigen, was bisher noch zu keinem alternativen Identifikationsverfahren gemacht wurde.

Art. 7 Abs. 2 VZertES ermöglicht eine Ausnahme für Schweizer Finanzintermediäre: Sinngemäss wird dabei erlaubt, dass anerkannte Anbieterinnen von Zertifizierungsdiensten geregelte Zertifikate auch im Rahmen eines Verfahrens zur Personenidentifikation mittels audiovisueller Kommunikation in Echtzeit (Echtzeit Identifikation auf Distanz via Videokonferenz) ausstellen können, sofern das Verfahren den Anforderungen des Geldwäschereigesetzes entspricht. Der Zusatz, dass die so ausgestellten Zertifikate nur im Rahmen der Beziehungen zwischen deren Inhaberinnen und Inhaber und den Finanzintermediären, die ihre Identität überprüft haben, verwendet werden dürfen, verweist auf die Einschränkung dieser Möglichkeit der Personenidentifikation auf Distanz für ausschliesslich Finanzintermediäre.

Eine userfreundliche, effiziente und vollständig digitale Identifikation von Antragsstellern («Onboarding») auf eine qualifizierte elektronische Signatur ist für die breite geschäftliche Nutzung von Digital Signing essenziell. Kunden stellen heute eine «Ich-Alles-Überall-Sofort-Erwartung» (Rusnjak & Schallmo, 2018, S. 101). Sobald also die Befähigung für die an einem Digital Signing Prozess beteiligten Personen aufwendig wird, z. B. mit dem verlangten persönlichen Erscheinen zwecks Identifikationsbestätigung (Nicht-Erfüllung von «Überall» und «Sofort»), sinkt die Attraktivität des Verfahrens und erhöht sich das Absprungrisiko. In diesem Kontext lässt sich die aktuelle Regulierung für die Beantragung einer qualifizierten elektronischen Signatur als theoretische Schwachstelle im Gesamtprozess von Digital Signing erkennen, wozu im Hauptteil II dieser Masterarbeit auch die Praxisperspektive untersucht wird. Das Europäische Signaturgesetz eIDAS erlaubt in diesem Punkt eine attraktivere und vollständig digitale Kundenerfahrung: es ermöglicht grösstenteils (länderspezifisch) die Videoidentifikation für Antragssteller auf eine qualifizierte elektronische Signatur uneingeschränkt und nicht wie in der Schweizer Regulierung nur für Finanzintermediäre (Fitzer & Kraul, 2019, S. 17).

Weiter erwähnenswert ist, dass im ZertES zwar verschiedene persönliche digitale Signaturtypen aufgelistet sind (eine Übersicht bietet die Tabelle 1) allerdings in Bezug auf die User-Identifizierung nur auf geregelte Zertifikate eingegangen wird. Für bspw. die fortgeschrittene elektronische Signatur finden sich keine User-Identifikationsanforderungen. Vermutlich liegt die Begründung dafür im Umstand, dass

auch nur die qualifizierte elektronische Signatur im Schweizerischen Obligationenrecht als digitale Alternative zur eigenhändigen Unterschrift akzeptiert ist und es über die Verwendung der fortgeschrittenen elektronischen Signatur im OR ebenfalls keine Erwähnung gibt. Eine Empfehlung, wie die verschiedenen Signaturtypen trotz zum Teil fehlender gesetzlicher Grundlagen verwendet werden können, wird im nachfolgenden Kapitel präsentiert.

2.3.3. Welche elektronische Signatur wird benötigt?

Wie das Kapitel 2.3. aufzeigt, gibt es in der Schweiz nur sehr wenige Verträge, welche eine Schriftlichkeit und Unterschrift der Vertragsparteien gesetzlich vorschreiben. Wird eine Unterschrift benötigt oder gewünscht, kann die Fragenstellung, in welchem Anwendungsfall welche Art von elektronsicher Signatur eingesetzt werden soll, aus dreierlei Perspektiven beantwortet werden.

- Wenn gesetzlich eine Schriftlichkeit und die Unterschrift der verpflichtenden Personen verlangt ist, wird die eigenhändige Unterschrift oder das digitale Pendant, die qualifizierte elektronische Signatur, gefordert (Art. 13 Abs. 1 OR, Art. 14 Abs. 1 und 2^{bis} OR).
- Weiter gilt es die gestellten Anforderungen an die Rechtsverbindlichkeit und das Haftungsrisiko zu beurteilen. Je höher das potenzielle Haftungsrisiko eines Geschäftsabschlusses, desto höher der Anspruch an die höchstmögliche Rechtsverbindlichkeit der geleisteten Signatur, um im Streitfall die Zustimmung zu einer Vereinbarung einwandfrei feststellen zu können. Je stärker der Anspruch an eine Rechtsverbindlichkeit einer Signatur desto höher die Anforderungen an die einmalige vorgelagerte Identifikationsbestätigung des Signaturinhabers.
- Zum anderen gilt es auch, den Signaturtyp entsprechend den gemäss Gerichtsstand länderspezifischen gesetzlichen Anforderungen zu wählen. Ist z. B. in einem digital signierten Vertrag der Gerichtsstand für allfällige Streitfälle in der Schweiz, gilt entsprechend die Schweizer Gesetzeslage, welche für die höchste Rechtsverbindlichkeit einer digitalen Unterschrift die qualifizierte elektronische Signatur nach ZertES verlangt. Wäre der Gerichtsstand in Europa, müsste eine rechtsverbindliche digitale Unterschrift nach den Standards von eIDAS verwendet werden.

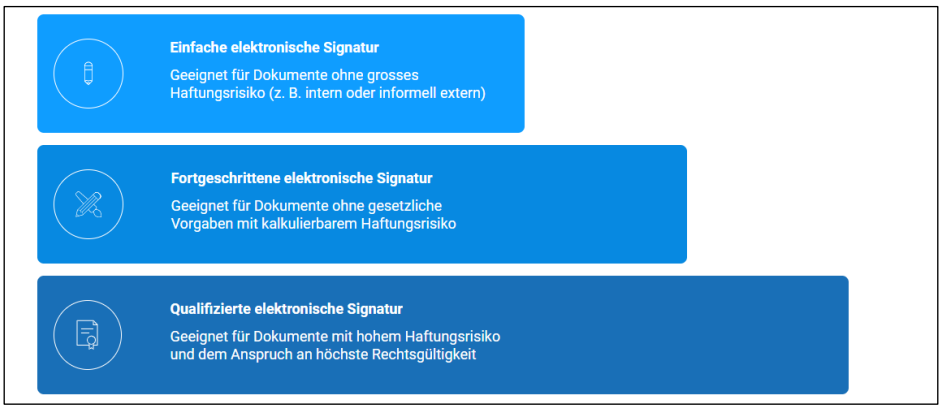


Abbildung 3 Empfehlung digitaler Signaturtypen nach Use-Cases
Quelle: (QuoVadis Trustlink Schweiz AG, kein Datum)

2.4. Marktakteure

Die in Kapitel 2.2 aufgezeigten Verwendungszwecke und Leistungsversprechen werden im Zusammenspiel verschiedener Marktteilnehmer erbracht. Die nachfolgende Grafik hält die relevanten Akteure im Schweizer Digital Signing Markt fest:

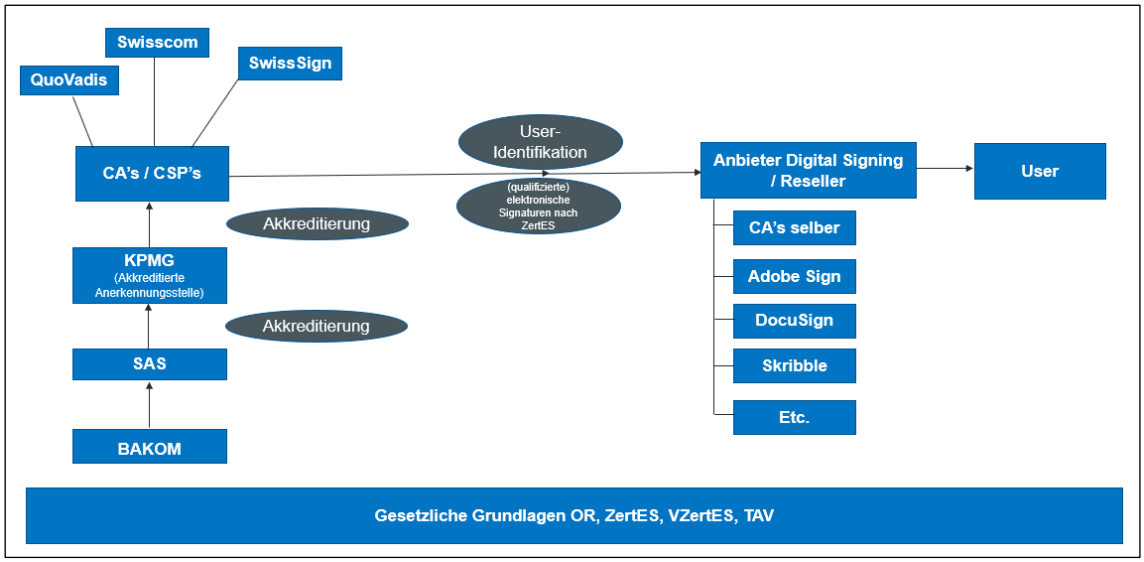


Abbildung 4 Marktakteure Digital Signing Schweiz

Quelle: eigene Darstellung

Das **BAKOM (Bundesamt für Kommunikation)** als für das ZertES zuständige Bundesamt beauftragt die **Schweizerische Akkreditierungsstelle (SAS)** zur Akkreditierung von Anerkennungsstellen.

Aktuell fungiert nur **KPMG** als **akkreditierte Anerkennungsstelle** (Schweizerische Akkreditierungsstelle SAS, 2021)**.** Die KPMG kontrolliert und akkreditiert *CSP's* auf deren Erfüllung der ZertES-Anforderungen.

Die **CA's (Certificate Authorities),** im Schweizer Kontext auch **CSP's (Certification Service Provider)** genannt, sind akkreditiert, elektronische Signaturen gemäss dem Schweizer Signaturrecht ZertES auszustellen. Für das höchste Signaturlevel, der qualifizierten elektronischen Signatur, sind per Stand März 2021 die folgenden Unternehmungen zugelassen (Schweizerische Akkreditierungsstelle SAS, 2021):

- Swisscom (Schweiz) AG
- QuoVadis Trustlink Schweiz AG
- SwissSign AG
- (Bundesamt für Informatik und Telekommunikation)

Das Bundesamt für Informatik und Kommunikation ist zwar als CSP für die Ausstellung von qualifizierten elektronischen Signaturen aufgeführt, bestätigte allerdings auf Anfrage, dass sie nicht als Anbieter im Markt auftritt und ihre Leistungen nur den Ämtern der Bundesverwaltung zugänglich macht. Die CA's müssen in jährlichen Audits die Erfüllung der Anforderungen als CSP nachweisen. Damit die CA's überhaupt qualifizierte elektronische Signaturen ausstellen können, müssen sie den Antragssteller gemäss den regulatorischen Anforderungen (Details dazu in Kapitel 2.3.2) vorab erfolgreich identifizieren. Es kann festgehalten werden, dass die Anzahl an akkreditierten Herausgebern (CA's) für elektronische Signaturen höchster Güte mit drei Anbietern sehr überschaubar ist.

Gerade weil die Hürden zur Anerkennung eines CSP's sehr hoch sind und es entsprechend wenige akkreditierte Herausgeber gibt, treten im Markt auch **Anbieter für Digital Signing Lösungen** auf, die selber nicht als CA akkreditiert sind, jedoch die entsprechende Zertifikate als **Reseller** von einer anerkannten Stelle beziehen. Diese nicht anerkannten Anbieter fokussieren sich dabei in ihrer Angebotsentwicklung vor allem auf die Signingapplikation, was dem User eine attraktive und effiziente Anwendung seiner elektronischen Signatur ermöglichen soll. Das einer elektronischen Signatur zugrundeliegende Zertifikat wird dabei mehr als Mittel zum Zweck verstanden, was von einer akkreditierten Stelle eingekauft und von dieser z. B. via Schnittstelle in der Lösung des nicht anerkannten Anbieters zur Verfügung gestellt wird.

Basierend auf den Erfahrungen des Autors sind vor allem die nachfolgenden Unternehmen im Schweizer Digital Signing Markt vertreten, welche digitale Signierlösungen anbieten:

- Die CA's selber (Swisscom, QuoVadis, SwissSign)
- Adobe Sign*
- DocuSign*
- Skribble*
- Individualisierte Kundenlösungen durch Softwareentwicklungsunternehmen wie z. B. Appway AG, Rockon Digital Evolution oder ti&m AG*
- * = nicht selber akkreditierte CSP's, sondern beziehen die öffentlich anerkannten Zertifikate von akkreditierten CA's

Die **User** sind im Kontext dieser Masterarbeit natürliche Personen, welche die elektronische Signatur für geschäftliche Zwecke verwenden.

Die **gesetzlichen Grundlagen** definieren die Rahmenbedingungen für die Ausstellung von elektronischen Signaturen (Details in Kapitel 2.3).

Nun wo die wichtigsten Marktakteure bekannt sind gibt das Kapitel 2.5. einen Einblick in den technischen Ablauf eines digitalen Signaturprozesses, wobei die vorgestellten Marktakteure wichtige Rollen einnehmen.

2.5. Technischer Ablauf eines digitalen Signaturprozesses

Um Missbrauch zu verhindern, werden hohe Sicherheitsanforderungen an die (qualifizierte) elektronische Signatur gestellt. Dabei gilt es einerseits die Integrität eines unterschriebenen Dokumentes zu gewährleisten, sodass zweifelsfrei festgehalten werden kann, dass das unterschriebene Dokument nach der digitalen Signatur keine inhaltlichen Veränderungen mehr erfahren hat. Andererseits soll auch unbestreitbar sichergestellt werden, welche Person das Dokument digital signiert hat, was mit dem Nachweis der Authentizität erbracht wird.

Diese Anforderungen werden durch ein kryptografisches Verfahren sichergestellt. Als eine Hauptaufgabe der Kryptografie kann die Absicherung von Daten genannt werden (Paar & Pelzl, 2016, S. 2).

Als Untergebiet der Kryptografie tritt ein Konzept mit asymmetrischen (Public Key) Algorithmen, welches ursprünglich von Whitfield Diffie, Martin Hellman und Ralph

Merkle 1976 eingeführt wurde, hervor (Paar & Pelzl, 2016, S. 3). Bei diesem kryptografischen Verfahren wird mit einem elektronischen Schlüsselpaar gearbeitet, welches sich einerseits aus einem geheimen, persönlichen Schlüssel und einem öffentlichen Schlüssel zusammensetzt (Paar & Pelzl, 2016, S. 3). Die nachfolgende Abbildung und dazugehörende Prozessbeschreibung veranschaulicht den Einsatz des Schlüsselpaares im Kontext von digitalen Signaturen, welche als eine der wichtigsten Anwendungen im Gebiet der asymmetrischen Kryptografie angesehen wird (Paar & Pelzl, 2016, S. 297).

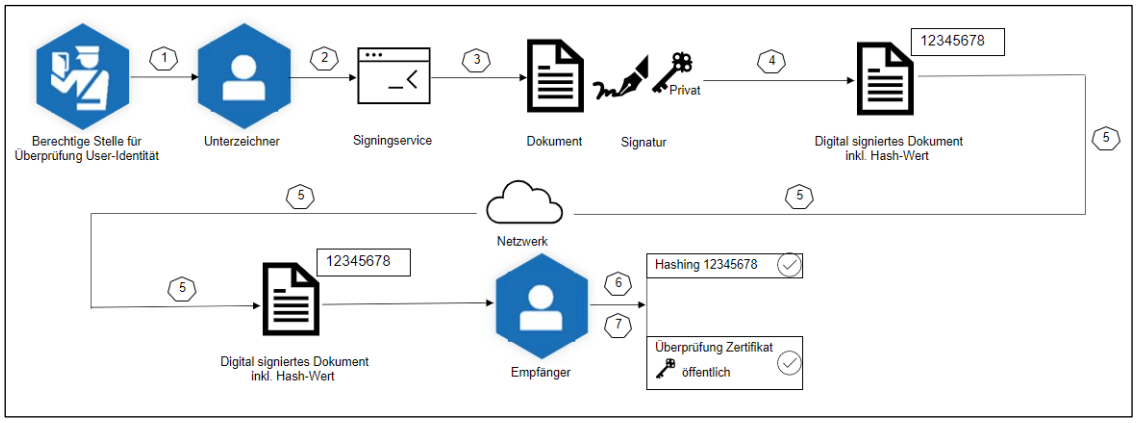


Abbildung 5 Technischer Ablauf digitaler Signaturprozess mit QES

Quelle: Eigene Darstellung in Anlehnung an *(DocuSign Contributor, 2021)*

1. Eine berechtigte Stelle bestätigt einmalig die Identifikation einer natürlichen Person (späterer Unterzeichner).
2. Die natürliche Person (späterer Unterzeichner) erwirbt sich einen digitalen Signingservice. Eine Übersicht zu den aktuell verfügbaren Angeboten an Digital Signing Lösungen ist in Kapitel 2.6. abgebildet. Sie sollte dabei einen zertifikatsbasierten Signaturservice berücksichtigen, womit ihr ein öffentlich anerkanntes Zertifikat von einer berechtigen Stelle (CSP) ausgestellt wird, sodass ihre elektronische Signatur auch anerkannt wird (z. B. qualifizierte elektronische Signatur).
3. Der Unterzeichner signiert ein Dokument mit seiner elektronischen Signatur. Während dem Signaturvorgang wird das Dokument gehasht, was einem eindeutig identifizierbaren Fingerabdruck des Dokuments gleichkommt. Sobald sich der Inhalt des Dokumentes verändert, würde damit auch der Hashwert des Dokuments verändert. Mittels des privaten Schlüssels des Zertifikatsinhabers aktiviert der Unterzeichner sein Zertifikat und signiert das Dokument. Der Signaturprozess ist durch eine starke 2-Faktorenauthentifizierung (der Nutzer

wird durch eine Kombination zweier unabhängiger Komponenten (Faktoren, z. B. Wissen, Besitz, Biometrie) authentifiziert) abgesichert, sodass nur der Zertifikatsinhaber selbst die Signatur auslösen kann. Das zugrundeliegende Zertifikat kann dabei entweder beim User lokal (z. B. auf einem USB-Stick) oder auch auf einem HSM im Rechenzentrum des CSP's (Remote Signing) gespeichert sein.

4. Das Endergebnis ist ein digital signiertes Dokument inklusive eines eindeutigen Hashwertes.
5. Das digital signierte Dokument kann nun beliebig einem Empfänger gesendet werden, z. B. via E-Mail oder durch Upload auf eine Plattform.
6. Der Empfänger des digital signierten Dokumentes hasht das Dokument, mit demselben Hash-Algorithmus wie der Unterzeichner verwendet hatte, erneut. Dabei wird überprüft, ob der Empfänger denselben Hashwert des Dokumentes kalkuliert. Wenn ja, ist damit sichergestellt, dass das Dokument nach der Signatur des Unterzeichners inhaltlich nicht mehr verändert worden ist. Wenn nein, wurden inhaltliche Veränderungen am Dokument vorgenommen. Dieses Verfahren wird automatisch von der Signingsoftware, z. B. vom Acrobat Reader, durchgeführt und gewährleistet die Erkennung der Integrität.
7. Der Empfänger hat nebst der Sicherstellung der Integrität des Dokumentes auch ein Interesse, die Authentizität des Unterzeichners zu überprüfen. Er will sich vergewissern, dass auch tatsächlich die diejenige Person digital unterzeichnet hat, welche das digital signierte Dokument vorgibt. Der öffentliche Schlüssel des Zertifikatsinhabers wird in den Zertifikatsinformation im digital signierten Dokument mitgeliefert. Mittels dieses öffentlichen Schlüssels kann die Signatursoftware nachvollziehen, ob die Signatur auf einem gültigen und anerkannten Zertifikat einer berechtigen Stelle basiert. Ist dies der Fall, z. B. mit einem gültigen qualifizierten Zertifikat, kann sich der Empfänger damit auf die vorgelagerte, erfolgreiche Identifikation des Unterzeichners verlassen.

Damit das asymmetrische Public Key Verfahren und die damit beabsichtigte Sicherstellung der Authentizität gewährleistet sind, darf der geheime, private Schlüssel ausschliesslich vom Inhaber (Unterzeichner) aktiviert werden können. Ebenso darf vom öffentlich verfügbaren Schlüssel kein Rückkalkulierung auf den geheimen, privaten Schlüssel geschehen können (Bundesamt für Sicherheit in der Informationstechnik, 2020, S. 27). Je grösser die Schlüssellänge desto höher die Sicherheit, dass auf Basis des öffentlich bekannten Schlüssels der geheime, private Schlüssel nicht rekonstruiert werden kann. Allerdings gilt es zu beachten, dass je grösser die Schlüssellänge ist auch

desto höhere IT-Ressourcen von denjenigen Applikationen abverlangt werden, welche diese kryptografischen Verfahren anwenden (z. B. Digital Signing Applikation). Aktueller Standard ist bereits seit längerer Zeit immer noch eine 2048 Bit Verschlüsselung (Freist, 2014).

Das nächste Kapitel zeigt nun auf, wie die Gültigkeit einer elektronischen Signatur, welche auf Basis des hier veranschaulichten Prozesses ausgestellt wurde, überprüft werden kann.

2.5.1. Prüfung einer qualifizierten elektronsichen Signatur

Die Überprüfung, ob ein Dokument mit einer gültigen qualifizierten elektronischen Signatur unterzeichnet worden ist, kann einerseits in den Zertifikatsdetails im signierten Dokument selbst und andererseits über einen Webservice der Schweizerischen Bundesverwaltung nachvollzogen werden.

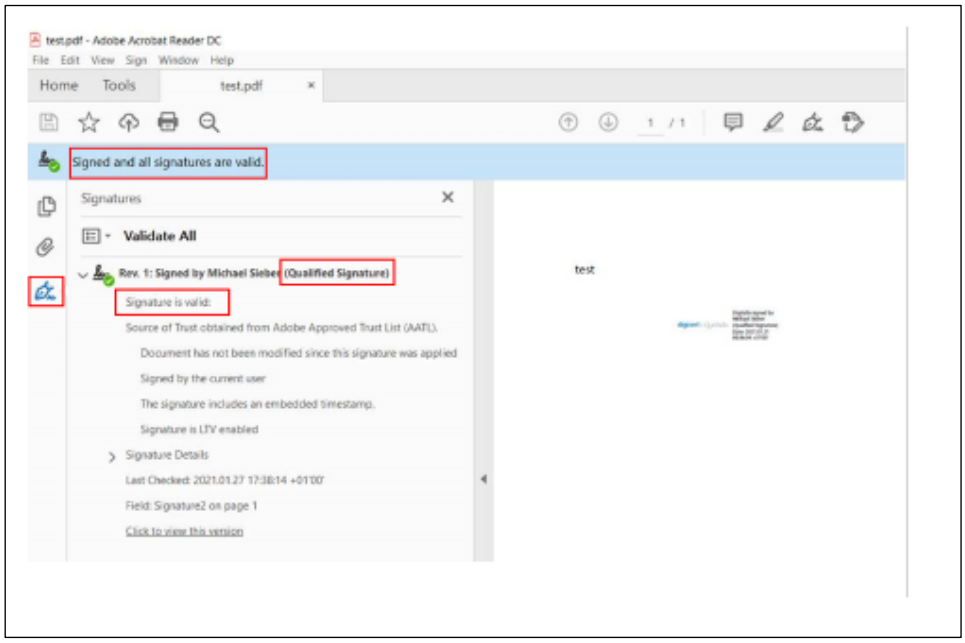


Abbildung 6 Signatur- und Zertifikatsdetails über signiertes Dokument I

Quelle: Printscreen aus Acrobat Reader

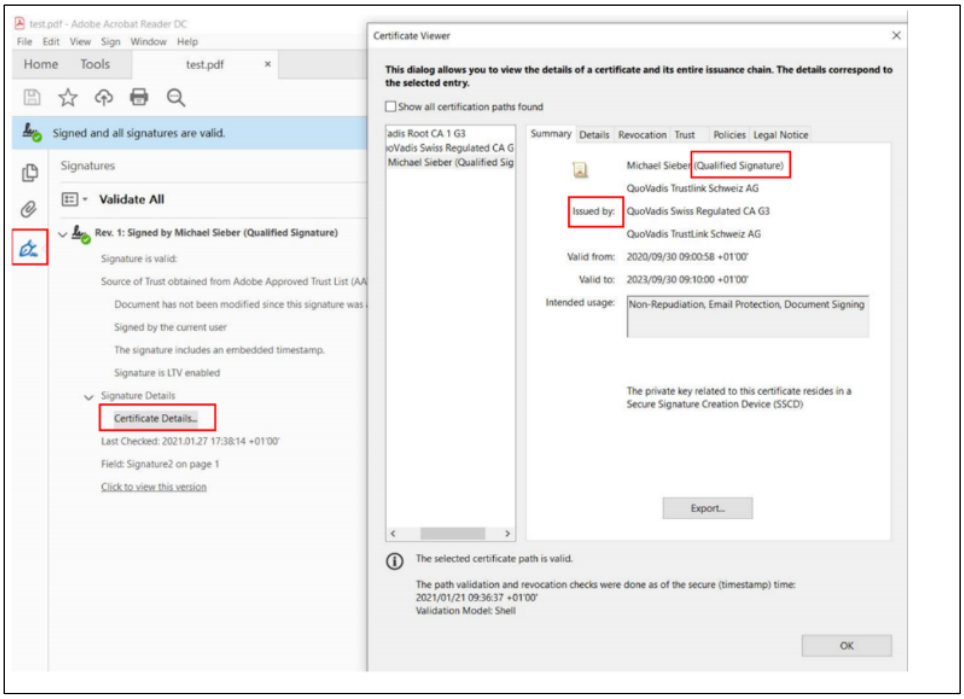


Abbildung 7 Signatur- und Zertifikatsdetails über signiertes Dokument II

Quelle: Printscreen aus Acrobat Reader

Über www.validator.ch, ein Service der Schweizerischen Bundesverwaltung, kann in wenigen Schritten ein mit einer elektronischen Signatur unterschriebenes Dokument auf Gültikgeit und Art der Signatur überprüft werden. Im ersten Schritt wird angegeben, auf welchen Signaturtyp (z. B. qualifizierte elektronsiche Signatur gemäss ZertES) ein Dokument überprüft werden soll. In einem zweiten Schritt wird das entsprechende Dokument hochgeladen und im dritten Schritt via dem Befehl «Dokument prüfen» der Prüfvorgang gestartet. Die nachfolgende Abbildung zeigt ein Beispiel eines erfolgreichen Prüfberichtes:

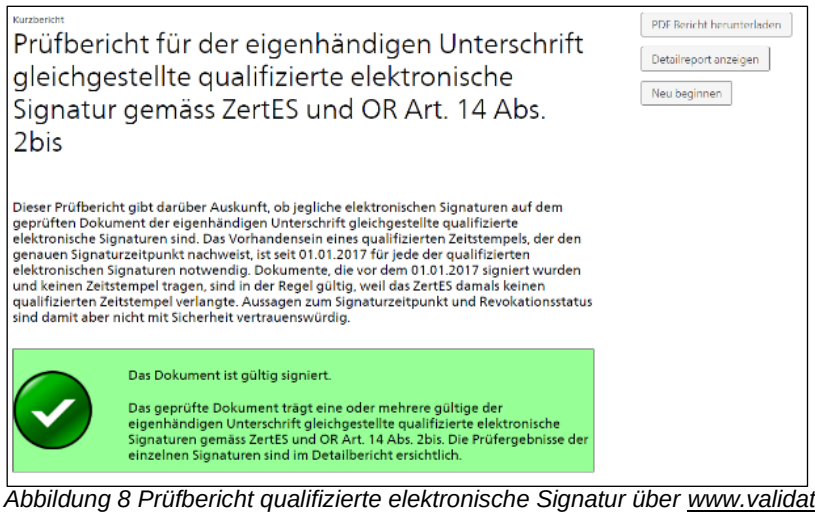


Abbildung 8 Prüfbericht qualifizierte elektronische Signatur über www.validator.ch

Quelle: (Bundesbehörden der Schweizerischen Eidgenossenschaft, kein Datum)

2.6. Angebotsübersicht

Zum Abschluss des Hauptteils I werden die Angebote gemäss der in Tabelle 2 aufgeführten relevanten Digital Signing Anbieter für den Markt Schweiz präsentiert. Als Angebotskriterien wurden die folgenden Attribute ausgewählt, welche für eine breite geschäftliche Verwendung erfolgskritisch erscheinen:

- **Digital Signing Service:** kann ein Kunde allein mit der angebotenen Lösung die digitale Signatur userfreundlich und effizient einsetzen oder bedarf es dazu weitere Zusatzservices? Als Hauptkomponenten für die erfolgreiche Verwendung einer digitalen Signatur wird einerseits das «nackte» technische Zertifikat, worauf eine elektronische Signatur basiert, andererseits die «Verpackung», also die Signingapplikation, worin das Zertifikat und digitale Signatur verwendet werden können, benötigt. Die Signingapplikation wird in der Tabelle 2 in die Komponenten «Frontend» und «Workflow» unterteilt. Das Frontend bietet dem User die grafische Bearbeitungsoberfläche und mit einem Workflow lassen sich individuelle Signaturprozesse gestalten (z. B. Unterzeichnungsparteien einladen, Erinnerungsfunktion bei säumigen Unterzeichnern, gewünschte Signierreihenfolge festlegen usw.). Ist die Signingapplikation nicht im Angebot enthalten, so muss der User sich selbst eine Signingapplikation beschaffen, welche mit dem gewählten Zertifikatsdienst kompatibel ist.
- **Angebotsvielfalt:** Bietet ein Lieferant verschiedene Digital Signing Lösungen und Ausführungen an? Basieren z. B. die angebotenen Lösungen auf Komponenten, die lokal vom Kunden installiert werden müssen oder wird ein reiner Cloud-Ansatz angeboten?
- **Signaturtypen:** Zum einen stellt sich die Frage, ob die Anbieterin selbst als öffentlich anerkannte Anbieterin von Zertifizierungsdiensten operiert oder nicht. Falls nicht und die Zertifikate von Dritten eingekauft werden, kann das ein potenzielles Risiko bedeuten, da Abhängigkeiten zum anerkannten CSP bestehen. Zum anderen gilt die angebotene Vielfalt an Signaturtypen als erfolgskritisch, da spezifisch je Use-Case von den Kunden verschiedene Signaturtypen verwendet werden möchten.

- **IT-Infrastruktur Anforderungen und Vorlaufzeit:** Welche Anforderungen werden an die Kunden-IT-Infrastruktur für die Einführung der Digital Signing Lösung gestellt? Wie lange ist die benötigte Vorlaufzeit, um Digital Signing operativ einzuführen?
- **Preis:** Unternehmen, die sich mit der Einführung von Digital Signing beschäftigen, werden die Investition schlussendlich auch aufgrund der kommerziellen Konditionen beurteilen. Gerade bei potenziellen Neueinsteigern kann ein zu hoher Investitionsaufwand als Hürde wirken.
- **Hash Signing / Besonderheiten:** Im Hinblick auf Datentransfer im eher konservativen Schweizer Unternehmensmarkt kann **Hash Signing** ein erfolgskritisches Unterscheidungsmerkmal darstellen. Bei einem Ansatz mit Hash Signing wird nicht das (lesbare) Dokument selbst, sondern nur der (unlesbare) Hashwert eines Dokuments, was mit einem Fingerabdruck eines Dokuments verglichen werden kann, mit dem Signaturanbieter geteilt. Der Hashwert wird beim Zertifikatsdienstleister signiert und zurück in die Kundenumgebung gesendet, wo der signierte Hashwert wieder lokal mit dem Dokument verbunden wird. Damit kann eine vollständige Dokumentenhoheit beim Kunden sichergestellt werden.

Angebotskriterium / Anbieter	Digital Signing Service	Angebotsvielfalt	Signaturtypen	IT Infrastruktur Anforderungen und Vorlaufzeit	Preis	Hash-Signing / Besonderheiten
Adobe Sign	• Frontend: JA • Workflow: JA • Anerkannte Signaturen: JA, Bezug durch Dritte (öffentlich anerkannte CA's)	• Mehrere Lösungen: NEIN, eine Lösung (Adobe Sign) • Cloud: JA • On Premise: NEIN (keine Angaben)	• Einfach: JA • Fortgeschritten (FES): JA • CH Qualifiziert (QES): geplant • Bezug von FES und QES durch Dritte (öffentlich anerkannte CA's)	• IT Infrastruktur Anforderungen: keine (Plattform) • Vorlaufzeit: Schnell («innerhalb von Stunden / wenigen Tagen»)	• Ab CHF 11.65.– pro User und Monat*	• Hash-Signing: NEIN (keine Angaben) • Verschiedene Preismodelle (Adobe Acrobat Pro DC mit E-Signaturen und Adobe Acrobat PDF Pack mit E-Signaturen) • Lösung kombinierbar mit anderen Acrobat Adobe Lizenzmodellen
BIT	Das BIT trifft nicht auf dem Privatmarkt auf und bietet seine Lösungen nur den Ämtern der Bundesverwaltung an**.					
DocuSign	• Frontend: JA • Workflow: JA • Anerkannte Signaturen: JA, Bezug durch Dritte (öffentlich anerkannte CA's)	• Mehrere Lösungen: JA, Cloud und Hybrid Cloud Varianten • Cloud: JA • On Premise: NEIN, aber Hybrid Cloud Variante («Signing Appliance Installation hinter Firewall»)	• Einfach: JA • Fortgeschritten (FES): JA • CH Qualifiziert (QES): JA • Bezug von FES und QES durch Dritte (öffentlich anerkannte CA's)	• IT Infrastruktur Anforderungen: Abhängig von gewählter Lösung, bei Cloud/SaaS-Variante keine Softwareinstallation notwendig, bei Hybrid Cloud Lösung Software-installation notwendig • Vorlaufzeit: Keine Angaben, bei Cloud/SaaS-Variante -> Annahme schnell	• Ab EUR 9.-- pro User und Monat inkl. 5 Dokumenten-sendungen*	• Hash-Signing: JA • Verschiedene Preismodelle (Personal, Standard, Business Pro) • Wenig konkrete Informationen zur Funktionsweise des Hybrid Cloud Modell • Starke US Verbreitung da US-ESIGN-Gesetz keine qualifizierten Zertifikate verlangt • Cloud SaaS Fokus
QuoVadis	• Frontend: JA, (Fremdlösung Ascertia SigningHub) • Workflow: JA, (Fremdlösung Ascertia SigningHub) • Anerkannten Signaturen: JA, Ausstellung über eigene öffentlich anerkannte CA	• Mehrere Lösungen: JA, QuoVadis Signing Service, DSS Engine, DSS Workflow • Cloud: JA • On Premise: Nein, aber Hybrid Cloud Variante (Signingapplikation on premise, Zertifikate bei QuoVadis (Fernsignatur))	• Einfach: JA • Fortgeschritten: JA • CH Qualifiziert: JA • Ausstellung über eigene öffentlich anerkannte CA	• IT-Infrastruktur-Anforderungen: Abhängig von gewählter Lösung, bei Cloud/SaaS-Variante keine Softwareinstallation notwendig, bei Hybrid Cloud Lösungen Software-installation notwendig • Vorlaufzeit: für Cloud/Saas-Variante: schnell («innerhalb von wenigen Tagen»)	• Ab CHF 350.– pro User inkl. unlimitiertes Signingvolumen (mit qualifizierter Signatur) für 3 Jahre	• Hash-Signing: JA • Ausstellung der Zertifikate über eigene öffentlich anerkannte CA • Verschiedene Signing Lösungen nach Use-Cases im Angebot
Skribble	• Frontend: JA • Workflow: JA • Anerkannte Signaturen: JA, Bezug durch Dritte (öffentlich anerkannte CA's)	• Mehrere Lösungen: NEIN, eine Lösung (Skribble Plattform) • Cloud: JA • On Premise: NEIN (keine Angaben)	• Einfach: JA • Fortgeschritten (FES): JA • CH Qualifiziert (QES): JA • Bezug von FES und QES durch Dritte (öffentlich anerkannte CA's)	• IT Infrastruktur Anforderungen: keine (Plattform) • Vorlaufzeit: Keine Angaben, da aber Plattform-basiert -> Annahme schnell	• EUR 1.10 pro Einfache Signatur • EUR 1.90 pro Fortgeschrittene Signatur • EUR 2.40 pro Qualifizierte Signatur	• Hash-Signing: NEIN (keine Angaben) • Verschiedene Preismodelle (Fair Flat, Business, Enterprise)
Swisscom	• Frontend: JA (durch Fremdlösungen wie Skribble oder Ajila) • Workflow: JA (durch Fremdlösungen wie Skribble oder Ajila) • Anerkannte Signaturen: JA, Ausstellung über eigene öffentlich anerkannte CA	• Mehrere Lösungen: JA, All-in Signing Service und SwissTrustRoom • Cloud: JA • On premise: NEIN, aber Hybrid Cloud Variante (Signingapplikation on premise, Zertifikate bei Swisscom (Fernsignatur))	• Einfach: NEIN (keine Angaben) • Fortgeschritten: JA • CH Qualifiziert: JA • Ausstellung über eigene öffentlich anerkannte CA	• IT-Infrastruktur-Anforderungen: Abhängig von gewählter Lösung, bei Cloud/SaaS-Variante keine Softwareinstallation notwendig, bei Hybrid Cloud Lösungen Software-installation notwendig • Vorlaufzeit: Keine Angaben, bei Cloud/SaaS-Variante -> Annahme schnell	• SwissTrustRoom: ab CHF 5.– pro User und Monat plus CHF 1.00 pro Fortgeschrittene oder qualifizierte elektronische Signatur • All-in Signing Service: Jährliche Basis-Fee CHF 2'400.— plus CHF 1.– pro qualifizierte Signatur oder CHF 0.50 pro Fortgeschrittene Signatur	• Hash-Signing: JA • Ausstellung der Zertifikate über eigene öffentlich anerkannte CA
SwissSign	• Aktuell kein Angebot	• Aktuell kein Angebot	• Aktuell kein Angebot	• Aktuell kein Angebot	• Aktuell kein Angebot	• Aktuell kein Angebot

*: keine Angabe wie viele und welche Art Signaturen im Preis inkludiert sind

**: Quelle: Schriftliche Auskunft Mitarbeiter BIT

Restliche Quellen: Adobe Sign, DocuSign, QuoVadis, Skribble, Swisscom, SwissSign: abgerufen von den jeweiligen Websites am 07.06.2021

Selektive Auswahl der bekanntesten Anbieter, Aufführungen nicht abschliessend

Tabelle 2 Angebotsübersicht Digital Signing Schweiz

Quelle: Eigene Darstellung

Die in der Tabelle 2 berücksichtigten Kriterien sollen nicht als abschliessend verstanden werden. Je nach individueller Ausgangslage eines Unternehmens, welches Digital Signing einführen will, können weitere Attribute relevant sein, z. B.:

- **Datenhaltung:** welche Daten werden wo, wie und für wie lange gespeichert?
- **Gerätunabhängigkeit:** kann der Digital Signing Service geräteunabhängig, also via Desktop-Computer und Mobile genutzt werden? Gibt es Einschränkungen bezüglich der verwendeten Betriebssysteme der Kunden?
- **Schnittstellenverfügbarkeit:** kann der Digital Signing Service mit Drittapplikationen (z. B. CRM-System, z. B. ERP-System) via Schnittstellen interagieren?
- **User-Onboarding:** Wie wird das User-Onboarding (u.a. User-Identifikation) vom Anbieter gelöst? Wie erläutert, bildet das User-Onboarding eine kritische Komponente für den Erfolg einer Digital Signing Lösung.

Ebenfalls zeigte sich in der Angebotsrecherche, dass sich ein Angebotsvergleich zwischen den verschiedenen Lösungen und Lieferanten teilweise als schwierig darstellt: zum einen werden nicht bei allen Anbietern und Lösungen sämtliche relevanten Kriterien transparent und detailliert präsentiert, zum anderen erschweren unterschiedliche und teilweise intransparente Preismodelle den Vergleich.

2.7. Fazit Hauptteil I

Mit dem Abschluss des Hauptteils I kann festgehalten werden, dass die digitale Signatur in der Schweiz gesetzlich geregelt ist und auf Basis von digitalen (und gesetzlich definierten) Zertifikaten beruht. Obschon in der dafür relevanten Gesetzesgrundlage ZertES verschiedene persönliche Signaturtypen festgehalten sind, ist einzig die qualifizierte elektronische Signatur gemäss dem Schweizerischen Obligationenrecht der eigenhändigen Unterschrift gesetzlich gleichgestellt. Die qualifizierte elektronische Signatur für den Schweizer Privatmarkt kann aktuell nur von drei akkreditieren Unternehmen (Anbieterinnen von Zertifizierungsdiensten) ausgestellt werden. Die Anwendung einer anerkannten digitalen Signatur (z. B. QES) erfolgt nach einem kryptografischen Verfahren mit asymmetrischen Public Key Algorithmen und deckt höchste Sicherheitsanforderungen ab, womit die anerkannte digitale Signatur als sicherer als die Handunterschrift beurteilt werden kann. Es konnten viele theoretische Vorteile bei der Verwendung von Digital Signing erörtert werden, welche insbesondere auf vollständig digitale Geschäftsprozesse und die damit verbundenen Effizienz- und Kostenvorteile abzielen. Der aktuell regulatorisch geforderte physische User-

Identifikationsprozess für die Ausstellung einer qualifizierten elektronischen Signatur stellt einen Medienbruch dar, welcher ein Grund für die noch fehlende Marktdurchdringung von Digital Signing darstellen kann. Weiter zeigte sich, dass es eine Handvoll relevanter Digital Signing Anbieter im Schweizer Markt gibt, welche sich aber in ihren Angeboten doch unterscheiden.

Im folgenden Hauptteil II wird eine empirische Forschung (qualitative Befragung) zur Erhebung der Anforderungen von ausgewählten Personen an eine breite geschäftliche Nutzung von Digital Signing vorbereitet, durchgeführt und ausgewertet. Dadurch werden die im Hauptteil I gewonnenen theoretischen Erkenntnisse aus einer Praxisperspektive überprüft. Im Rahmen von Handlungsempfehlungen werden erkannte Optimierungspunkte zur Förderung der geschäftlichen Verwendung der digitalen Signatur in der Schweiz an verschiedene Empfänger adressiert. Den Abschluss des Hauptteils II bildet die Beantwortung der Forschungsfragen.

HAUPTTEIL II

3. Erhebung Anforderungen an Digital Signing im Geschäftsumfeld

In diesem Teil der Masterarbeit werden die Rahmenbedingungen für eine qualitative Befragung von ausgewählten Vertretern von Schweizer Unternehmen zur Erhebung ihrer Anforderungen rund um den geschäftlichen Einsatz der digitalen Signatur festgelegt. Die im Hauptteil I erarbeitete Theorie wird damit auch in die Praxis transferiert.

3.1. Methodisches Vorgehen

Als Forschungsmethode für die Erhebung der Anforderungen wurden qualitative Interviews ausgewählt. Innerhalb der Gattung der qualitativen Interviews hat sich die Form von Leitfadeninterviews (Baur & Blasius, 2014, S. 53), auch semistrukturierte oder halbstrukturierte Interviews genannt, als am geeignetsten erwiesen.

Im semistrukturierten Interview werden im Vorfeld Leitfragen festgelegt. Die Reihenfolge, in welcher diese Leitfragen dann gestellt werden, kann flexibel aufgrund des Gesprächsverlaufes definiert werden (Hussy, Schreier, & Echterhoff, 2013, S. 225). Das individuelle und flexible Ergänzen von Fragen (Ad-hoc Fragen (Hussy, Schreier, & Echterhoff, 2013, S. 226)) ist dabei ebenfalls vorgesehen und trägt dazu bei, das Momentum bei wertvollen Inputs des Interviewpartners zu nutzen und das Gespräch zu vertiefen.

Die gewählte Forschungsmethode zeigte sich für die Beantwortung der offenen Forschungsfrage («Was sind die Anforderungen von ausgewählten Vertretern von Schweizer Unternehmen zugunsten einer breiten geschäftlichen Nutzung der digitalen Signatur?») am passendsten, da sich das qualifizierte, semistrukturierte Interview ebenfalls durch seine offene, aber gleichzeitig auch standardisierte Gestaltung, charakterisiert. Die Vorteile liegen einerseits in der offenen Struktur, womit auch situativ Freiraum für das Gewinnen von zusätzlichen wertvollen Informationen vorhanden ist. Andererseits helfen die vorbereiteten Leitfragen das Interview trotzdem in die richtige Richtung zu lenken und den Fokus nicht zu verlieren.

3.2. Untersuchungsziel

Das Ziel dieser qualitativen Befragung ist es, die Anforderungen von ausgewählten Vertretern von Schweizer Unternehmen an eine breite geschäftliche Verwendung von Digital Signing zu erheben und damit die Hauptforschungsfrage (Kapitel 1.3.) zu beantworten. Aus den daraus gewonnenen Erkenntnissen werden in Kapitel 5. Handlungsempfehlungen erarbeitet, um den breiten geschäftlichen Einsatz der digitalen Signatur zu fördern und damit auch die Nebenfragenstellung (Kapitel 1.3.) zu beantworten.

3.3. Untersuchungsobjekte

Insgesamt wurde mit fünf Interviewpartnern zwischen April und Mai 2021 ein qualitatives Interview geführt, wobei die folgenden Kriterien in der Auswahl der Gesprächspartner berücksichtigt wurden:

- **Unternehmensindustrie:** Da in jedem Unternehmen Dokumente - heute hauptsächlich noch via Handunterschrift - unterzeichnet werden, wurden auch absichtlich Vertreter von unterschiedlichen Unternehmensindustrien befragt, um eine möglichst breite Rückmeldung zu erhalten.
- **Unternehmensgrösse:** Ebenfalls absichtlich variierten die Unternehmensgrössen, um auch in diesem Kriterium ein breites Spektrum zu berücksichtigen.
- **Unternehmenstätigkeit im Schweizer Markt:** Alle Interviewpartner arbeiten bei Unternehmen, welche dominierend im Schweizer Rechtsraum operieren. Dies galt als Pflichtvoraussetzung, da diese Masterarbeit die digitale Signatur in der Schweiz untersucht.
- **Funktionen der Gesprächspartner:** Es wurden Gesprächspartner ausgesucht, die in ihrem Geschäftsalltag regelmässig Dokumente signieren, unabhängig ob bereits digital oder noch analog. Ebenfalls sollten nicht nur Anwender befragt werden, sondern auch Personen, welche die Anforderungen an Digital Signing insbesondere auch aus einer kommerziellen und gesamtunternehmerischen Investitionsperspektive betrachten (Entscheider).
- **Erfahrungsgrad Digital Signing:** Es wurden sowohl Personen befragt, die bisher Digital Signing noch nicht anwenden als auch solche, die schon erste Erfahrungen damit gemacht haben. Auch diese Entscheidung wurde bewusst gefällt, um ein möglichst breites Spektrum an Rückmeldungen zu erhalten. Dasselbe zählt für das Alter der befragten Personen.

Insgesamt kann bei der Auswahl der Gesprächspartner festgehalten werden, dass bewusst eine Mischung von Personen (und Unternehmen) berücksichtigt worden ist, da Digital Signing ein sehr breites Anwendungspotential verspricht (Details dazu auch in Kapitel 2.2.). Lediglich die Kriterien, dass die Vertreter bei Unternehmen arbeiten müssen, welche eine starke Geschäftstätigkeit in der Schweiz betreiben und dass die Gesprächspartner entweder selbst regelmässig im geschäftlichen Umfeld Dokumente signieren oder sich mit der Einführung der digitalen Signatur für ihr Unternehmen beschäftigen, bildeten Muss-Anforderungen.

Kürzel Gesprächspartner	Industrie	Unternehmens-grösse	Funktionen Interviewpartner / Geschlecht / Alter	Anwender	Ent-scheider	Digitale Signatur bereits geschäftlich im Einsatz
GP-1	Wirtschaftsprüfung, Treuhand, Beratung	Ca. 1'450 Mitarbeiter	Leiter IT Transformation & Solutions Männlich, 45 Jahre alt	X	X	X
GP-2	Automobilhandel	Ca. 5’500 Mitarbeiter	Head of Aftersales Männlich, 36 Jahre alt	X	-	- (nicht via öffentlich anerkannten Zertifikaten)
GP-3	Pensionskasse	Ca. 110 Mitarbeiter	Leiter Investment Operations Männlich, 36 Jahre alt	X	X	- (in Beschaffungs-evaluation)
GP-4	Immobilien, Generalunternehmer	Ca. 220 Mitarbeiter	Interne Revision, Compliance Themen, Quali-tätsmanagement, Risikomonitoring Männlich, 57 Jahre alt	X	(X), Beein-flusser	- (in Beschaffungs-evaluation)

GP-5	Sozialversicherungs-anstalt	Ca. 1'000 Mitarbeiter	Leiter IT Service Männlich, 62 Jahre alt	X	X	- (in Beschaffungs-evaluation)

Tabelle 3 Übersicht Interviewpartner

Quelle: eigene Darstellung

3.4. Untersuchungsgrenzen

Die durch die Befragung abgeleiteten Erkenntnisse können nicht als wissenschaftlich repräsentativ betrachtet werden, sondern haben lediglich Gültigkeit für die interviewten Personen. Eine Überprüfung der gewonnenen Erkenntnisse auf eine Allgemeingültigkeit für z. B. Unternehmensgrössen und -industrien oder Funktionen der Interviewpartner ist nicht Teil dieser Masterarbeit, stellt aber einen interessanten Nachfolgeforschungsauftrag dar.

3.5. Interviewsetup

Zu Beginn und vor den ersten Fragenstellungen wurden immer nochmals die Rahmenbedingungen des Interviews, welche bereits bei der initialen Interviewanfrage mitgeteilt worden sind, abgesteckt. Dabei wurde nochmals das Thema des Interviews, den Kontext zu der Masterarbeit sowie das Ziel des Gespräches erläutert. Ebenfalls wurde die ungefähre Interviewzeitdauer von 30 - 60 Minuten mitgeteilt als auch die Zusicherung der Anonymität (Personen- und Unternehmensnamen) bestätigt, von welcher sich eine möglichst hemmungsfreie Gesprächssituation erhofft wurde. Des Weiteren wurden die Gesprächspartner immer vor dem Start der Aufnahme darauf hingewiesen, dass die Interviews ausgezeichnet werden und ihre explizite Zustimmung dazu abgeholt.

Pro Interview wurden zwischen 17 bis 28 Fragen gestellt. Die Fragenstellungen unterteilten sich wie in Leitfadeninterviews üblich in einleitende Fragen, Leitfadenfragen und Ad-hoc-Fragen (Hussy, Schreier, & Echterhoff, 2013, S. 225). Während die einleitenden Fragen Smalltalk-Charakter zugunsten eines angenehmen Gesprächseinstieges hatten, bildete der Interviewleitfaden (Anhang) das Gerüst der Gespräche. Bei passenden Gesprächssituationen, welche das Potential für weitere wertschöpfende Rückmeldungen vermuten liessen, wurden die Gespräche mittels Ad-hoc-Fragen vertieft.

Sämtliche Interviews fanden mündlich und in Schweizerdeutsch statt. Die Interviews wurden auf Distanz via der Videokonferenzlösung Zoom geführt und mit Erlaubnis der Gesprächspartner aufgenommen.

3.6. Transkription

Die aufgenommenen Interviews wurden nachträglich transkribiert und finden sich im Anhang dieser Masterarbeit. Bei der Transkription fand eine Bereinigung statt, d.h. es wurden nur diejenigen Gesprächsinhalte verschriftlicht, welche dem Autor dieser Masterarbeit als relevant für die Beantwortung der Forschungsfragen erschienen. So sind z. B. die einleitenden Smalltalk-Fragen, die Abholung von administrativen Informationen (z. B. Alter, Funktion usw.) als auch die Verdankung des Gesprächs Gespräches am Schluss nicht transkribiert worden. Ebenfalls wurden, wo zwingend nötig, Versprecher und grammatikalisch falsche Satzstellungen - welche sich vor allem durch den Schweizerdeutschen Dialekt ergaben - zugunsten der Lesbarkeit der Verschriftlichung korrigiert. Diese getroffene Auswahl und Korrekturen stellen eine persönliche Interpretation des Autors dar, die allerdings immer unter Prämisse stattfand, die Inhalte der Gespräche sinngemäss und in Relevanz zur Beantwortung der Forschungsfragen wiederzugeben.

Innerhalb der Transkription der Interviews finden sich teilweise die folgenden Klammern, die zur korrekten Deutung nachfolgend erklärt werden:

[…]: Diese Symbolisierung (leere Klammer mit drei Punkten) wurde verwendet, um darzustellen, wenn der Gesprächspartner noch weiteren Inhalt innerhalb seiner Beantwortung der Frage mitteilte, dieser jedoch für die Beantwortung der Forschungsfragen als nicht relevant erschien und deshalb nicht verschriftlicht wurde.

[Text]: Diese Symbolisierung (Klammer mit Text) wurde verwendet, um innerhalb einer Antwort des Gesprächspartners fehlenden Kontext wiederzugeben. Ohne diese Kontext-Anreicherung wäre die Antwort für den Leser nur schwierig nachvollziehbar gewesen. Beispiel: *GP-1: «Gute Frage. Was wir uns erhoffen würden wäre sicher eine Nachverfolgbarkeit, sprich wir haben alle diese Dokumente danach **[nach dem Digital Signing]** alle digital abgelegt.»*

3.7. Kategorisierung und weitere Auswertungskriterien

3.7.1. Kategorisierung

In der Auswertung der Interviews wurde sich an das Modell der strukturierten Inhaltsanalyse von Mayring angelehnt (Mayring, 2015, S. 65). Dabei wurden die Gespräche auf Basis der im Hauptteil I (insbesondere Kapitel 2.2., 2.3.2. und 2.6.) abgeleiteten theoretischen User-Anforderungen an einen breiten geschäftlichen Einsatz von Digital Signing in Form von Kategorien und Codes (deduktive Codes) strukturiert ausgewertet. Ergaben sich in den Interviewauswertungen relevante Aussagen, für welche vorab auf Basis der Theoriearbeit (Hauptteil I) keine Kategorisierungen oder Codes vorgesehen waren, wurden diese nachträglich geschaffen (induktive Codes). Die Auswertung wurde mittels der kostenlosen Software-Probelizenz «MAXQDA 2020» erarbeitet, welche als weit verbreitende Software im Bereich qualitativer Forschung genutzt wird (Verbi GmbH, kein Datum).

Zusammenfassende Kategorien	Codes (deduktiv (d) und induktiv (i))	Muster aus den Interviews
Effiziente, digitale und kosten-günstige Geschäftsprozesse	• Zeitersparnis erreichen (d) • Effizienzsteigerung durch strukturierte Daten (d) • Personalaufwand, verursacht durch manuelle und meist analoge Prozesse, senken (z. B. Eliminierung Dokumente einscannen für Digitalisierung) (d) • Allgemeine Kostensenkung (Druckkosten, Portokosten senken) (d) • Attraktiver Kostenaufwand für Digital Signing (günstig) (d)	*GP-2: «Für mich ist wichtig, dass sie schnell funktioniert. Wenn ich z. B. eine Rechnung kontiere, möchte ich nicht mehr als 30 Sekunden investieren.»* *GP-3: «Es muss immer schnell gehen, je mehr Hürden ich habe, desto weniger mache ich es.»*

User-Onboarding: schnell, einfach, digital und kostengünstig	• einfache, effiziente, günstige und digitale User-Identifikation (intern & extern) (d) • kleinstmögliche Vorlaufzeit / einfaches User-Onboarding (d) • Forderung nach E-ID (i)	*GP-2: «Es muss verständlich und nicht allzu komplex sein. Idealerweise hätte ich diese Vorarbeiten innerhalb einer Viertelstunde erledigt, sodass ich gar nicht viel Zeit investieren muss, bevor es funktioniert.»* *GP-5: «Ja. Es ist unverständlich, dass man bei uns [in der Schweiz] einen Pass oder ID abholen kann, wir aber nicht in der Lage sind, eine digitale ID mitzugeben. Aber wir haben ja erst kürzlich darüber abgestimmt.»*
Funktionsumfang / Varianten Digital Signing Lösung	• Cloudfähigkeit (d) • On Premise (d) • Individualisierbare Workflowkomponenten inkl. Frontend & Dash-board (v. a. Möglichkeit, externe Unterzeichner einfach zum Unter-zeichnungsprozess einzuladen) (d) • Intuitive, einfache Digital Signing Prozesse (d) • Geräteunabhängigkeit (Desktop & Mobile, neutral in Bezug auf Betriebs-systeme) (d) • Schnittstelle / Anbindung an vor- oder nach-gelagerte Applikationen (d) • Single Sign On (i) • Verschiedene Signaturtypen (i)	*GP-5: «Mit der Ortsunabhängigkeit, die ich erwähnt hatte, ist natürlich mitverbunden, dass ich sehr gerne Lösungen hätte, die auch mobile einsetzbar sind.»* *GP-4: «Ich finde das sehr wichtig. Das hilft den Prozess wirklich steuern zu können. Auch dass ich sagen kann, dieser Vertragspartner muss qualifiziert digital unterzeichnen [der Signatur-workflow-Initiant gibt vor, mit welcher Art von digitaler Signatur unterzeichnet werden muss] oder dass er zuerst unterzeichnen muss. Es könnte ja auch noch weitergehen, dass so bald alle unterzeichnet haben mir danach dieser Vertrag automatisch in die richtige Ablage gespeichert werden würde. Ich finde das würde schon enorm viel bringen. […]»*

Befriedigung Zielgruppenansprüche	• Befriedigung Ansprüche bestehender und / oder neuer Zielgruppen (Z. B. Erreichung aller Zielgruppen (auch Y & Z mit digitalen Anforderungen), Erreichung aller Kaufbedürfnisse («hier, jetzt, überall»)) (d)	*GP-1: «Aber wir haben sicher grosse internationale Kunden, wo wir durch das [Digital Signing] sicher einen Vorteil haben, weil wir ganz klar sagen können, wir können digital zusammenarbeiten, inklusive der gesamten digitalen Signierung. Von dem her gesehen gibt es den einen oder anderen Fall, welchen wir dadurch gewonnen hatten.»*
Sicherheitsansprüche	• Sicherstellung Authentizität Unterzeichner (d) • Sicherstellung Dokumentenintegrität (d) • Datenhaltung exklusive in der Schweiz (i) • Höchste IT-Security Standards (v.a. bei Datenhaltung) (i) • Keine Dokumententeilung mit Signaturanbieter / Hash Signing (d) • Notwendigkeit Rechtsverbindlichkeit von Digital Signing (QES) (d)	*GP-2: «Und logischerweise möchte ich nicht, dass jemand anders für mich unterschreiben kann.»* *GP-3: «Sehr wichtig. Anders hätten wir es nicht akzeptiert. Sie müssen sich vorstellen, wenn Sie Verträge über ein paar Milliarden unterschreiben und es gibt daraus ein Problem, ist dann das Erste was der Anwalt sagt, dass die digitale [nicht qualifizierte] Unterschrift nicht rechtsgültig ist.»*
Andere Anforderungen / Varia	• Nutzung Digital Signing ist abhängig vom Alter des Users (i) • Imageaufwertung (d) • Unwissenheit verschiedene Signaturlevels (i) • Unsicherheit Akzeptanz digitale Signatur (i) • Corona-Pandemie erhöht Bedürfnis für Digital Signing (i) • Einfaches Preismodell (i) • QES-Zertifikat übergreifend nutzbar (unabhängig Signinglösung) (i) • Erkennen von Kunden- und Nutzungsdaten zu Marketingoptimierungszwecken (d)	*GP-3: «Wir sind gespannt, wie die Amerikaner reagieren werden, wenn die Formulare von uns digital signiert daherkommen. Gerade Steuerbehörden sind so «tick the box», Hauptsache das Häkchen ist da, ob es stimmt oder nicht, ist egal. […] Die Manager kennen die digitale Signatur schon, bei den Behörden sind wir gespannt, was dort die Rückmeldung sein wird.»* *GP-3: «Der Schmerzensdruck bis anhin war aber noch zu wenig gross. […] Jetzt aber mit dem Homeoffice [durch die Corona-Pandemie] und unserer Policy, dass man Zuhause keine Dokumente ausdrucken darf, hat man gemerkt, dass der Prozess nicht mehr funktioniert.»*

	• Ökologische Effizienz steigern (d)	

Tabelle 4 Strukturierte Inhaltsanalyse, Kategorien & Codes

Quelle: eigene Darstellung

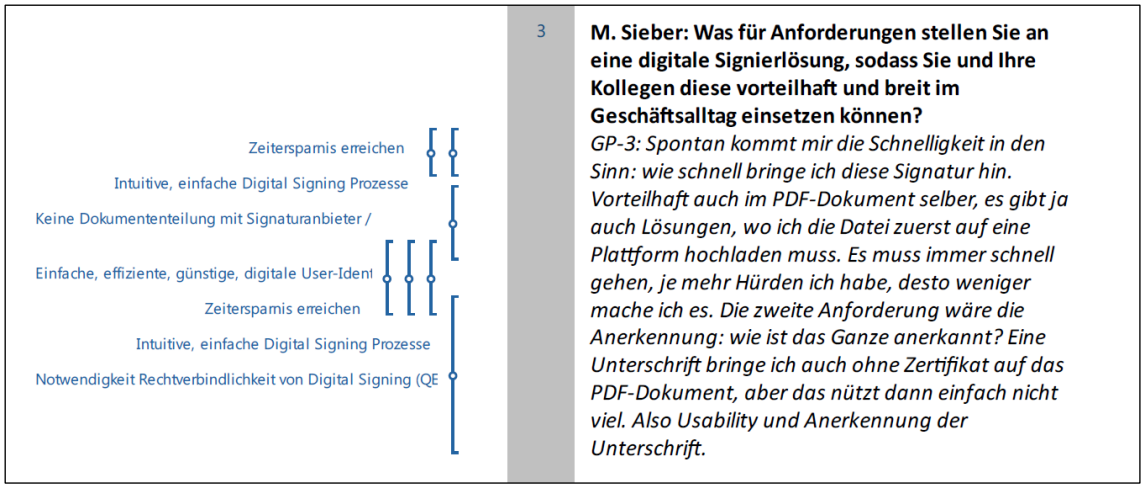


Abbildung 9 Beispiel einer codierten Textpassage aus der Interviewtranskription
Quelle: Printscreen aus kostenloser Software-Probelizenz «MAXQDA 2020»

3.7.2. Weitere Auswertungskriterien

Im Nachfolgenden wird erläutert, unter welchen weiteren Kriterien die Auswertung erarbeitet wurde.

- Bei in der Auswertung (Kapitel 4.) referenzierten Aussagen wird jeweils ein Bezug (Kürzel) zum entsprechenden Interviewpartner dargestellt, womit dessen Perspektive besser nachvollzogen werden kann. Die vergebenen Kürzel sind in der Tabelle 3 ersichtlich.
- Die erhaltenen Antworten wurden mittels der Software MAXQDA 2020 den Codes aus der Tabelle 4 zugeteilt.
    - Zugunsten einer ganzheitlichen Betrachtung wurden je Code sämtliche inhaltlich relevanten Aussagen, wertunabhängig, zugeteilt. D.h. bei der Zuteilung einer Aussage auf einen Code spielte es keine Rolle, ob der Gesprächspartner den entsprechenden Code (Anforderung) befürwortete oder verneinte, sondern nur, dass er sich dazu äusserte. Die Auswertung, ob ein Code befürwortet oder verneint wurde, fand erst in einem zweiten Analyseschritt statt.
    - Zu Beginn (bei einem Interview am Schluss) eines Interviews wurde jeweils eine vollständig ungestützte und offene Frage nach den

Anforderungen des Gesprächspartners zugunsten seiner breiten geschäftlichen Verwendung einer digitalen Signierlösung gestellt. Die vom Gesprächspartner darauf erhaltenen Antworten wurden in der Auswertung mit einer stärkeren Gewichtung (Gewichtung 2) taxiert. Sie rechtfertigen diese höhere Gewichtung da sie den ersten Impuls des Befragten, quasi seine initialen Hauptgedanken zur Fragestellung, widerspiegelten. Z. B.: «*Ganz allgemein gesehen, was stellst du für Anforderungen an eine digitale Signierlösung, sodass du diese im Geschäftsalltag vorteilhaft nutzen und breit einsetzen kannst?» GP-2: «Für mich ist wichtig, dass sie schnell funktioniert. Wenn ich z. B. eine Rechnung kontiere, möchte ich nicht mehr als 30 Sekunden investieren.»*

- Ebenfalls stärker gewichtet (Gewichtung 2) wurden genannte Anforderungen, deren Wichtigkeit die Gesprächspartner deutlich unterstrichen hatten. Z. B. *GP-1: «Sehr sehr wertvoll, definitiv.»*
- Antworten des Interviewpartners konnten auch mehrfach codiert werden, sofern die Aussage Relevanz für mehrere Codierungen hatte.

Das folgende Kapitel 4. zeigt die aus den Interviews gewonnenen und analysierten Erkenntnisse strukturiert auf.

4. Ergebnisse Anforderungen an Digital Signing im Geschäftsumfeld

In diesem Kapitel werden die gewonnenen Ergebnisse aus der Erhebung der Anforderungen für einen breiten geschäftlichen Einsatz der digitalen Signatur präsentiert. Dabei werden zuerst die Erkenntnisse zu den einzelnen Kategorien (Tabelle 4) beleuchtet, wonach eine konsolidierte Betrachtung den Abschluss des Kapitels bildet. Die zugrundeliegenden Interviews und deren Auswertung fanden gemäss den in Kapitel 3. vorgestellten Rahmenbedingungen statt.

4.1. Ergebnisse zu effizienten, digitalen und kostengünstigen Geschäftsprozessen

Dokumentname	Code	Anfang	Ende	Gewicht
Interview mit Gesprächspartner GP1	Allgemeine Kostensenkung (Druckkosten, Portokosten senken)	6	6	0
Interview mit Gesprächspartner GP1	Allgemeine Kostensenkung (Druckkosten, Portokosten senken)	6	6	0
Interview mit Gesprächspartner GP5	Allgemeine Kostensenkung (Druckkosten, Portokosten senken)	7	7	0
Interview mit Gesprächspartner GP1	Attraktiver Kostenaufwand für Digital Signing (günstig)	6	6	0
Interview mit Gesprächspartner GP2	Attraktiver Kostenaufwand für Digital Signing (günstig)	7	7	0
Interview mit Gesprächspartner GP2	Attraktiver Kostenaufwand für Digital Signing (günstig)	8	8	0
Interview mit Gesprächspartner GP3	Attraktiver Kostenaufwand für Digital Signing (günstig)	4	4	0
Interview mit Gesprächspartner GP3	Attraktiver Kostenaufwand für Digital Signing (günstig)	5	5	0
Interview mit Gesprächspartner	**Attraktiver Kostenaufwand für Digital Signing (günstig)**	**4**	**4**	**2**
Interview mit Gesprächspartner GP1	Effizienzsteigerung durch strukturierte Daten	5	5	0
Interview mit Gesprächspartner GP2	Effizienzsteigerung durch strukturierte Daten	9	9	0
Interview mit Gesprächspartner GP2	Effizienzsteigerung durch strukturierte Daten	10	10	0
Interview mit Gesprächspartner	**Effizienzsteigerung durch strukturierte Daten**	**8**	**8**	**2**
Interview mit Gesprächspartner	**Effizienzsteigerung durch strukturierte Daten**	**9**	**9**	**2**
Interview mit Gesprächspartner	**Effizienzsteigerung durch strukturierte Daten**	**24**	**24**	**2**
Interview mit Gesprächspartner GP1	Personalaufwand, verursacht d. man./analoge Prozesse, senken	5	5	0
Interview mit Gesprächspartner GP1	Personalaufwand, verursacht d. man./analoge Prozesse, senken	5	5	0
Interview mit Gesprächspartner GP1	Personalaufwand, verursacht d. man./analoge Prozesse, senken	6	6	0
Interview mit Gesprächspartner GP4	Personalaufwand, verursacht d. man./analoge Prozesse, senken	5	5	0
Interview mit Gesprächspartner GP5	Personalaufwand, verursacht d. man./analoge Prozesse, senken	5	5	0
Interview mit Gesprächspartner GP5	Personalaufwand, verursacht d. man./analoge Prozesse, senken	7	7	0
Interview mit Gesprächspartner	**Personalaufwand, verursacht d. man./analoge Prozesse, senken**	**9**	**9**	**2**
Interview mit Gesprächspartner	**Personalaufwand, verursacht d. man./analoge Prozesse, senken**	**23**	**23**	**2**
Interview mit Gesprächspartner	**Personalaufwand, verursacht d. man./analoge Prozesse, senken**	**24**	**24**	**2**
Interview mit Gesprächspartner GP1	Zeitersparnis erreichen	5	5	0
Interview mit Gesprächspartner	**Zeitersparnis erreichen**	**4**	**4**	**2**
Interview mit Gesprächspartner GP2	Zeitersparnis erreichen	12	12	0
Interview mit Gesprächspartner	**Zeitersparnis erreichen**	**3**	**3**	**2**
Interview mit Gesprächspartner	**Zeitersparnis erreichen**	**3**	**3**	**2**
Interview mit Gesprächspartner GP3	Zeitersparnis erreichen	4	4	0
Interview mit Gesprächspartner GP3	Zeitersparnis erreichen	6	6	0
Interview mit Gesprächspartner	**Zeitersparnis erreichen**	**6**	**6**	**2**
Interview mit Gesprächspartner GP4	Zeitersparnis erreichen	5	5	0
Interview mit Gesprächspartner GP5	Zeitersparnis erreichen	5	5	0
Interview mit Gesprächspartner GP5	Zeitersparnis erreichen	6	6	0
Interview mit Gesprächspartner	**Zeitersparnis erreichen**	**23**	**23**	**2**
Interview mit Gesprächspartner	**Zeitersparnis erreichen**	**24**	**24**	**2**
Total 37 Nennungen				

Abbildung 10 Codierungen Kategorie effiziente, digitale Geschäftsprozesse

Quelle: Eigene Darstellung, abgeleitet aus «MAXQDA 2020»-Software

Einleitung: Insgesamt wurden 37 Passagen aus den Interviewantworten der Kategorie «effiziente, digitale und kostengünstige Geschäftsprozesse» zugeordnet. Die vorab auf Basis der Theorie prognostizierten Anforderungen (deduktive Codes) wurden grösstenteils bestätigt. In dieser Kategorie wurden keine neuen Anforderungen (induktive Codes) durch die Gespräche generiert.

Zeitersparnis erreichen: Jeder Gesprächspartner gab an, dass er beim geschäftlichen Einsatz von Digital Signing eine Zeitersparnis gegenüber dem Verfahren mit der Handunterschrift fordert. Drei der fünf Interviewpartner haben diese Erwartung sogar ungestützt oder als sehr wichtig geäussert. Die Anforderung an eine Zeitersparnis wurde dabei nicht nur im Kontext des beschleunigten Versandes eines zu signierenden Dokumentes (z. B. per E-Mail statt als Papier per Post) verstanden, sondern auch für die eigentliche digitale Signierung eines Dokumentes. Die Erwartungshaltung dazu war, dass ein User eine digitale Signatur ohne viele Schritte schnell und intuitiv auslösen können muss.

GP-1: *«Auf der anderen Seite sicher die Geschwindigkeit. Sprich du unterschreibst das Dokument, versendest oder legst es ab und musst es nicht via interne Post von Niederlassung A nach Niederlassung B senden.»*

GP-3: *«Es muss immer schnell gehen, je mehr Hürden ich habe, desto weniger mache ich es.»*

Effizienzsteigerung durch strukturierte Daten: Drei der fünf Interviewpartner forderten mit dem geschäftlichen Einsatz von Digital Signing eine Effizienzsteigerung durch strukturierte Daten, einer bewertete dies sogar als sehr wichtig. In diesem Zusammenhang wurde vor allem die Erwartung geäussert, dass mit einem digital signierten Dokument eine komplett digitale und strukturierte Datei vorliegt, welche dann nachfolgend wesentlich effizienter nachverarbeitet werden kann, z. B. im Rahmen einer Stichwortsuche. Einige der Gesprächspartner digitalisieren zwar ihre von Hand unterzeichneten Dokumente via Einscannen, erreichen damit aber keine komplett digitale und strukturierte Datei.

GP-5: *«Absolut. Das wäre grossartig, wenn unsere Kunden uns Ihre Dokumente digital übergeben könnten, sodass wir direkt damit arbeiten könnten.»*

Personalaufwand, verursacht durch manuelle und meist analoge Prozesse, senken: Drei der fünf interviewten Personen stellten die Anforderung, dass mit der geschäftlichen Verwendung der digitalen Signatur der Personalaufwand für manuelle Prozesse gesenkt werden können muss. Für eine Interviewperson stellte dies sogar eine sehr wichtige Anforderung dar. Grundsätzlich möchte man mit der digitalen Signatur den mit der Handunterschrift und Papier personalaufwändigen Medienbruch lösen: so soll es mit Digital Signing z. B. nicht mehr notwendig sein, von Hand unterschriebene Dokumente wieder (manuell) einzuscannen und so halbwegs zu digitalisieren.

GP-5: *«Ist natürlich so. Wenn man Papier verwalten muss, hat man all die Nachteile mit dem Papier. Klar, ich kann es einscannen, ich kann mir eine Lösung beschaffen, mit welcher ich die eingescannten Dokumente dann bei mir organsiert abspeichern und wieder finden kann.»*

GP-5: *«Das ist zurzeit unser grosser Pferdefuss innerhalb der Digitalisierung, dass wir immer noch sehr viel Papier entgegennehmen müssen.»*

Allgemeine Kostensenkung (Druckkosten, Portokosten senken): Zwei der fünf interviewten Personen forderten mit der Verwendung der digitalen Signatur eine allgemeine Kostensenkung gegenüber dem analogen Unterzeichnungsprozess zu erreichen. Erstaunlich festzustellen war, dass drei der fünf interviewten Personen die Kostenersparnis nicht explizit als eine zentrale Anforderung an Digital Signing nannten. Allerdings herrschte der allgemeine Tenor – codierungsübergreifend – dass man mit Digital Signing effizientere Geschäftsprozesse schaffen möchte, was implizierend auch einer Kostensenkung gleichgestellt werden kann, denn je effizienter sich ein Prozess gestaltet, desto kostengünstiger ist er.

GP-1: *«Und die Kosten, die wir bezahlen pro Mitarbeiter sind natürlich in keinem Verhältnis zu interner Post vielleicht von Niederlassung zu Niederlassung via Schweizerische Post das Dokument physisch zu verschicken.»*

Attraktiver Kostenaufwand für Digital Signing (günstig): Vier der fünf befragten Personen äusserten sich zum Preis einer digitalen Signaturlösung, wovon lediglich für eine Person ein kostengünstiges Preismodell eine wichtige Anforderung darstellte. Bei einigen Gesprächspartner mag die fehlende Erwartungshaltung darin begründet sein, dass sie selbst nicht für die Prüfung der kommerziellen Konditionen verantwortlich sind. Grundsätzlich spürte man allerdings die Erwartungshaltung, dass eine digitale Signierlösung sicherlich nicht teurer als der Prozess über die Handunterschrift sein darf.

GP-1: *«Wenn ich mal die Kosten aufrechnen würde, ist Digital Signing definitiv effizienter und günstiger.»*

GP-2: «Weil ich mit den Kosten bei uns nicht zu tun habe. Die IT ist bei uns der Gatekeeper und entscheidet, welcher Prozesse und Systemlandschaft implementiert wird.»

GP-3: «Ist nicht so im Vordergrund gestanden, weil in der Finanzbranche nicht dasselbe Denken wie in der Industrie herrscht.»

GP-4: «Der einzige Hinderungsgrund sind die Kosten.»

GP-2: «Wenn ich es richtig im Kopf habe, haben wir viele Systeme, jetzt nicht explizit auf die digitale Signatur bezogen, wo wir zwischen 5-10 Franken pro Monat und User zahlen. Und das sind dann auch Systeme, die man stundenlang pro Tag verwendet. In meinem Verständnis dürfte dann nur eine digitale Signatur nicht teurer sein. Jetzt habe ich im Übrigen die Kosten gerade gefunden: für mich kostet der Adobe Acrobat DC pro Monat 17 Franken. […]»

Zusammenfassung: Wenig überraschend bestätigte sich die Theorie, dass an einen breiten geschäftlichen Einsatz der digitalen Signatur die Erwartung geknüpft wird, dass damit Unterzeichnungsprozesse deutlich effizienter gestaltet werden können müssen. Zeitgewinne (Zeit ist Geld), Effizienzgewinne durch komplett digitale und strukturierte Daten wie auch die Reduzierung von Personalressourcen im Zusammenhang mit Aufgaben bei papierlastigen Handunterschriftsprozessen bildeten Anforderungen der Interviewpartner. Schlussendlich mündet die Erfüllung dieser Anforderungen auch in einer Kostenreduktion der Unterzeichnungsprozesse der Unternehmen. Konkrete Erwartungen an einen günstigen Preis für eine digitale Signierlösung wurden nur einmal explizit gefordert, bei den restlichen Interviewpartnern stand dies aus verschiedenen Gründen nicht im Vordergrund.

4.2. Ergebnisse zu einfaches, digitales User-Onboarding

Dokumentname	Code	Anfang	Ende	Gewicht
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**20**	**20**	**2**
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**22**	**22**	**2**
Interview mit Gesprächspartner GP2	Einfache, effiziente, günstige, digitale User-Identifikation	20	20	0
Interview mit Gesprächspartner GP2	Einfache, effiziente, günstige, digitale User-Identifikation	21	21	0
Interview mit Gesprächspartner GP2	Einfache, effiziente, günstige, digitale User-Identifikation	22	22	0
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**3**	**3**	**2**
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**12**	**12**	**2**
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**13**	**13**	**2**
Interview mit Gesprächspartner GP3	Einfache, effiziente, günstige, digitale User-Identifikation	18	18	0
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**4**	**4**	**2**
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**4**	**4**	**2**
Interview mit Gesprächspartner GP4	Einfache, effiziente, günstige, digitale User-Identifikation	13	13	0
Interview mit Gesprächspartner GP4	Einfache, effiziente, günstige, digitale User-Identifikation	13	13	0
Interview mit Gesprächspartner GP4	Einfache, effiziente, günstige, digitale User-Identifikation	14	14	0
Interview mit Gesprächspartner GP4	Einfache, effiziente, günstige, digitale User-Identifikation	20	20	0
Interview mit Gesprächspartner	**Einfache, effiziente, günstige, digitale User-Identif**	**21**	**21**	**2**
Interview mit Gesprächspartner GP5	Einfache, effiziente, günstige, digitale User-Identifikation	17	17	0
Interview mit Gesprächspartner GP5	Einfache, effiziente, günstige, digitale User-Identifikation	18	18	0
Interview mit Gesprächspartner GP5	Einfache, effiziente, günstige, digitale User-Identifikation	19	19	0
Interview mit Gesprächspartner GP5	Einfache, effiziente, günstige, digitale User-Identifikation	21	21	0
Interview mit Gesprächspartner GP5	Einfache, effiziente, günstige, digitale User-Identifikation	26	26	0
Interview mit Gesprächspartner GP5	Einfache, effiziente, günstige, digitale User-Identifikation	30	30	0
Interview mit Gesprächspartner GP5	Einfache, effiziente, günstige, digitale User-Identifikation	31	31	0
Interview mit Gesprächspartner GP4	Forderung nach E-ID	13	13	0
Interview mit Gesprächspartner GP5	Forderung nach E-ID	20	20	0
Interview mit Gesprächspartner GP5	Forderung nach E-ID	21	21	0
Interview mit Gesprächspartner GP1	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	18	18	0
Interview mit Gesprächspartner GP1	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	21	21	0
Interview mit Gesprächspartner	**kleinstmögliche Vorlaufzeit- / einfaches User-Onb**	**22**	**22**	**2**
Interview mit Gesprächspartner GP2	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	20	20	0
Interview mit Gesprächspartner GP2	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	22	22	0
Interview mit Gesprächspartner	**kleinstmögliche Vorlaufzeit- / einfaches User-Onb**	**12**	**12**	**2**
Interview mit Gesprächspartner	**kleinstmögliche Vorlaufzeit- / einfaches User-Onb**	**13**	**13**	**2**
Interview mit Gesprächspartner	**kleinstmögliche Vorlaufzeit- / einfaches User-Onb**	**4**	**4**	**2**
Interview mit Gesprächspartner	**kleinstmögliche Vorlaufzeit- / einfaches User-Onb**	**4**	**4**	**2**
Interview mit Gesprächspartner GP4	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	12	12	0
Interview mit Gesprächspartner GP4	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	13	13	0
Interview mit Gesprächspartner GP4	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	13	13	0
Interview mit Gesprächspartner GP4	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	14	14	0
Interview mit Gesprächspartner GP4	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	20	20	0
Interview mit Gesprächspartner	**kleinstmögliche Vorlaufzeit- / einfaches User-Onb**	**21**	**21**	**2**
Interview mit Gesprächspartner GP5	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	18	18	0
Interview mit Gesprächspartner GP5	kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	26	26	0
Total 43 Nennungen				

Abbildung 11 Codierungen für einfaches, digitales User-Onboarding

Quelle: Eigene Darstellung, abgeleitet aus «MAXQDA 2020»-Software

Einleitung: Insgesamt wurden 43 Passagen aus den Interviewantworten der Kategorie «User-Onboarding: schnell, einfach, digital und kostengünstig» zugeordnet. Zu dieser Kategorie ergaben sich nach der Kategorie «Funktionsumfang» die meisten Nennungen, was auf ein starkes Bedürfnis der Interviewpartner hinweist. Die vorab auf Basis der Theorie prognostizierten Anforderungen (deduktive Codes) wurden allesamt bestätigt. Innerhalb der geführten Gespräche ergab sich eine weitere Anforderung, welche auf Basis der Theorie nicht vorgesehen war (induktive Codierung): «Forderung nach E-ID».

Einfache, effiziente, günstige und digitale User-Identifikation: Jeder der fünf Gesprächspartner sah einen direkten Zusammenhang zwischen der Art und Weise der notwendigen User-Identifikation und der breiten geschäftlichen Verwendung der digitalen Signatur. Es wurde die klare Forderung nach einer möglichst einfachen, effizienten (und somit günstigen) und vor allem vollständig digitalen User-Identifikation -

unabhängig des Signaturtyps - geltend gemacht. Drei Gesprächspartner bewerteten diese Anforderung als sehr wichtig zugunsten eines breiten geschäftlichen Einsatzes der digitalen Signatur. Grundsätzlich befindet sich der Grossteil der interviewten Personen im Dilemma, dass sie einerseits die höchste digitale Signaturstufe, die qualifizierte elektronische Signatur, einsetzen möchten, diese allerdings eine persönliche face-to-face User-Identifikation bei einer berechtigten Stelle voraussetzt. Solange dies «nur» für die eigenen Mitarbeiter einer Unternehmung gemacht werden muss, wurde dieser User-Identifikationsprozess als einigermassen gangbar angesehen. Sobald allerdings auch externe Vertragsparteien zu einem digitalen Vertragsabschluss eingeladen werden und diese ebenfalls mit der qualifizierten elektronischen Signatur unterzeichnen sollen, wurde ein grosses Abbruchrisiko skizziert. Für die externe Unterschriftspartei, welche vielleicht nur diese eine qualifizierte elektronische Signatur tätigen will oder muss, zeigt sich die physische Vorab-Identifikation bei einer berechtigen Stelle als zu umständlich. Wenn externe Unterzeichner aus den genannten Gründen nur vereinzelt an digitalen Signierungsprozessen partizipieren, reduziert dies die Anwendungsmöglichkeiten für eine Unternehmung stark. So können sie dann nur intern oder gegen extern einseitig (Anwendungsfälle, wo keine Gegensignatur der externen Partei gefordert ist) qualifiziert elektronisch signieren. Ein Interviewpartner stellte zudem die Sicherheit des aktuell notwendigen face-to-face Useridentifikationsprozesses insofern in Frage, ob z. B. der Postbeamte eine Identifikation eines Users tatsächlich seriös überprüft und bestätigt.

GP-1: *«Genau. Das passiert ja heute schon bei gewissen Banken, wo du alles in einem vorgelagerten Prozess schon hochladen kannst, deine ID und ein Foto via Webcam. Das gibt es ja alles schon und da wäre ich definitiv Freund davon [wenn diese digitalisierte User-Identifikationsmethode für die Ausstellung einer qualifizierten elektronischen Unterschrift auch für Nicht-Finanzintermediäre erlaubt wäre].»*

GP-2: *«Ja, würde ich zustimmen. Gerade in der heutigen Zeit [Corona-Pandemie] bin ich vielleicht noch alle drei Wochen einen Tag im Büro. Wenn wir uns jetzt physisch identifizieren lassen liessen, müsste man wieder vor Ort sein und es würde dann drei Wochen dauern. Wenn das jetzt digital, z. B. über einen Videochat möglich wäre, würde ich wieder Zeit gewinnen.»*

GP-3: *«Es muss immer schnell gehen, je mehr Hürden ich habe, desto weniger mache ich es. Ein Bedürfnis ist sicher die [User] Identifizierung über eine Online-Lösung. Davon hat man ja bereits vor Jahren darüber gesprochen. […] Das ist natürlich einfacher, als wenn ich persönlich bei der Post vorbeigehen muss. Das ist ja ohnehin ein bisschen ein*

sinnloser Prozess, denn der Postbeamte schaut mich einmal an und «knallt» den Stempel drauf. Zu ihm könnte ich auch, wenn ich nicht die Person wäre, die ich bin [er würde das nicht bemerken und trotzdem die Identität bestätigen]. Das ist sicher etwas, was man optimieren kann und notwendig ist. […]»

GP-4: *«Darum ist dann die fortgeschrittene elektronische Signatur interessant, wo die Personen nicht noch zuerst mit dem Pass bei der Post [zur User-Identifikation] vorbei gehen müssen. Für viele wäre das [eine einmalige physische User-Identifikation bei einer erlaubten Stelle als Voraussetzung zum Erhalt der qualifizierten elektronischen Signatur] eine extreme Hürde. Dieser Aufwand lohnt sich dann nicht für Verträge wo es um CHF 500.—geht.»*

Forderung nach E-ID: Zwei Personen erachteten bei der Forderung nach einem effizienten User-Onboarding die vom Schweizer Stimmvolk abgelehnte E-ID als wertvollen, aber verpassten Beschleunigungsfaktor. Grundidee dabei wäre gewesen, dass jede Privatperson in der Schweiz nebst dem physischen Identitätsausweis auch standardmässig eine E-ID hätte, womit grundsätzlich jeder Privatperson eine qualifizierte elektronische Signatur ausgestellt werden könnte (sofern die Person über eine E-ID nach höchstem Sicherheitslevel verfügt hätte) und die dafür notwendige (separate) persönliche User-Identifikation entfallen würde.

GP-5: *«Ja. Es ist unverständlich, dass man bei uns [in der Schweiz] einen Pass oder ID abholen kann, wir aber nicht in der Lage sind, eine digitale ID mitzugeben. Aber wir haben ja erst kürzlich darüber abgestimmt.»*

GP-4: *«Oder es müsste halt à la E-ID jede Person vom Bund aus eine Registration haben. […]»*

Kleinstmögliche Vorlaufzeit / einfaches User-Onboarding: Nebst der User-Identifizierung für die Berechtigung einer digitalen Signatur wurde auch das User-Onboarding an sich stark thematisiert. Dabei ist gemeint, welche Schritte der User (nebst der Identifikationsbestätigung) als Vorarbeiten durchlaufen muss, bis er das erste Mal die digitale Signatur auch tatsächlich produktiv nutzen kann. Hier wurden Anforderungen an eine kurze Vorlaufzeit mit möglichst wenigen und vor allem einfach verständlichen Schritten gestellt. Auch hier galt der Tenor, je weniger Hürden das User-Onboarding darstellt, desto breiter würde die digitale Signatur geschäftlich eingesetzt.

GP-4: *« Es darf nicht zu viele Schritte haben. Der User müsste eigentlich mit einem Klick signieren können.»*

GP-2: *«Es muss verständlich und nicht allzu komplex sein. Idealerweise hätte ich diese Vorarbeiten innerhalb einer Viertelstunde erledigt, sodass ich gar nicht viel Zeit investieren muss, bevor es funktioniert.»*

Zusammenfassung: Definitiv als grösste Hürde für eine breite geschäftliche Nutzung der höchsten digitalen Signaturart (QES) stellte sich die derzeit notwendige face-to-face User-Identifikation heraus. Diese aktuelle Regulierung verhindert eine schnelle Skalierung und reduziert die Anwendungsgebiete für die Unternehmen. Auch die anderen genannten Anforderungen (E-ID, kleinstmögliche Vorlaufzeit, Einfachheit) zielen auf ein effizientes, kostengünstiges und digitales User-Onboarding ab, was schlussendlich den breiten geschäftlichen Einsatz fördern sollte. Die Aussage von GP-3 bringt es auf den Punkt: «*[…] Je mehr Hürden ich habe, desto weniger mache ich es.»*

4.3. Ergebnisse zum Funktionsumfang der Digital Signing Lösung

Dokumentname	Code	Anfang	Ende	Gewicht
Interview mit Gesprächspartner GP1	Cloudfähigkeit	15	15	0
Interview mit Gesprächspartner GP1	Cloudfähigkeit	16	16	0
Interview mit Gesprächspartner GP1	Cloudfähigkeit	23	23	0
Interview mit Gesprächspartner GP1	Cloudfähigkeit	27	27	0
Interview mit Gesprächspartner GP2	Cloudfähigkeit	23	23	0
Interview mit Gesprächspartner GP2	Cloudfähigkeit	24	24	0
Interview mit Gesprächspartner GP4	Cloudfähigkeit	11	11	0
Interview mit Gesprächspartner GP1	Geräteunabhängigkeit	27	27	0
Interview mit Gesprächspartner	**Geräteunabhängigkeit**	**6**	**6**	**2**
Interview mit Gesprächspartner GP2	Geräteunabhängigkeit	26	26	0
Interview mit Gesprächspartner GP2	Geräteunabhängigkeit	27	27	0
Interview mit Gesprächspartner GP3	Geräteunabhängigkeit	15	15	0
Interview mit Gesprächspartner GP3	Geräteunabhängigkeit	16	16	0
Interview mit Gesprächspartner	**Geräteunabhängigkeit**	**17**	**17**	**2**
Interview mit Gesprächspartner GP5	Geräteunabhängigkeit	5	5	0
Interview mit Gesprächspartner GP5	Geräteunabhängigkeit	29	29	0
Interview mit Gesprächspartner GP5	Geräteunabhängigkeit	30	30	0
Interview mit Gesprächspartner GP1	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	24	24	0
Interview mit Gesprächspartner GP1	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	25	25	0
Interview mit Gesprächspartner GP1	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	26	26	0
Interview mit Gesprächspartner GP1	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	29	29	0
Interview mit Gesprächspartner	**Indiv. Workflowkomponenten inkl. Frontend & D**	**25**	**25**	**2**
Interview mit Gesprächspartner GP2	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	25	25	0
Interview mit Gesprächspartner GP3	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	18	18	0
Interview mit Gesprächspartner	**Indiv. Workflowkomponenten inkl. Frontend & D**	**3**	**3**	**2**
Interview mit Gesprächspartner	**Indiv. Workflowkomponenten inkl. Frontend & D**	**3**	**3**	**2**
Interview mit Gesprächspartner	**Indiv. Workflowkomponenten inkl. Frontend & D**	**4**	**4**	**2**
Interview mit Gesprächspartner GP4	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	15	15	0
Interview mit Gesprächspartner GP4	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	16	16	0
Interview mit Gesprächspartner	**Indiv. Workflowkomponenten inkl. Frontend & D**	**19**	**19**	**2**
Interview mit Gesprächspartner GP5	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	4	4	0
Interview mit Gesprächspartner GP5	Indiv. Workflowkomponenten inkl. Frontend & Dashboard	28	28	0
Interview mit Gesprächspartner	**Intuitive, einfache Digital Signing Prozesse**	**3**	**3**	**2**
Interview mit Gesprächspartner	**Intuitive, einfache Digital Signing Prozesse**	**3**	**3**	**2**
Interview mit Gesprächspartner	**Intuitive, einfache Digital Signing Prozesse**	**4**	**4**	**2**
Interview mit Gesprächspartner GP4	Intuitive, einfache Digital Signing Prozesse	12	12	0
Interview mit Gesprächspartner	**Intuitive, einfache Digital Signing Prozesse**	**4**	**4**	**2**
Interview mit Gesprächspartner GP4	On Premise Anforderung	11	11	0
Interview mit Gesprächspartner	**On Premise Anforderung**	**27**	**27**	**2**
Interview mit Gesprächspartner GP1	Schnittstelle/Anbindung an vor-/ nachgelagerte Applikat	28	28	0
Interview mit Gesprächspartner GP2	Schnittstelle/Anbindung an vor-/ nachgelagerte Applikat	25	25	0
Interview mit Gesprächspartner GP3	Schnittstelle/Anbindung an vor-/ nachgelagerte Applikat	14	14	0
Interview mit Gesprächspartner GP3	Schnittstelle/Anbindung an vor-/ nachgelagerte Applikat	17	17	0
Interview mit Gesprächspartner GP4	Schnittstelle/Anbindung an vor-/ nachgelagerte Applikat	18	18	0
Interview mit Gesprächspartner	**Schnittstelle/Anbindung an vor-/ nachgelagert**	**4**	**4**	**2**
Interview mit Gesprächspartner	**Schnittstelle/Anbindung an vor-/ nachgelagert**	**27**	**27**	**2**
Interview mit Gesprächspartner GP1	Single Sign On	30	30	0
Interview mit Gesprächspartner GP5	Verschiedene Signaturtypen	14	14	0
Total 48 Nennungen				

Abbildung 12 Codierungen Kategorie Funktionsumfang

Quelle: Eigene Darstellung, abgeleitet aus «MAXQDA 2020»-Software

Einleitung: Insgesamt wurden 48 Passagen aus den Interviewantworten der Kategorie «Funktionsumfang / Varianten Digital Signing Lösung» zugeordnet. Zu dieser Kategorie ergaben sich nebst der Kategorie «User-Onboarding: schnell, einfach, digital und kostengünstig» die meisten Nennungen, was auf einen starken Fokus der Interviewpartner hinweist. Die vorab auf Basis der Theorie prognostizierten Anforderungen (deduktive Codes) wurden allesamt bestätigt. Innerhalb der geführten Gespräche ergaben sich zudem weitere Anforderungen, welche auf Basis der Theorie nicht vorgesehen waren (induktive Codierung): «Single Sign On» und «Verschiedene Signaturtypen».

Cloudfähigkeit oder On Premise Anforderung: Zwei Personen favorisierten klar eine cloud-basierte Digital Signing Lösung. Als Gründe gaben sie einerseits Kostenvorteile, andererseits aber auch die damit nicht in der eigenen Verantwortung liegende Verfügbarkeit der Anwendung an. Eine interviewte Person zeigte sich für beide Szenarien offen. Lediglich eine Person stellte die Anforderung an eine On Premise Lösung.

GP-1: *«Sprich wir sind dabei, alle unsere Prozesse und Software cloudfähig zu machen. […] Wir haben beschlossen, dass wir Ende 2022, spätestens 2023, wann unser heutiges Rechencenter end of life ist, wir möglichst viele Daten nicht mehr selber On Premise haben möchten.»*

GP-2: *«Idealerweise wäre das [die digitale Signaturlösung] auch eine Lösung, die trotzdem weiterläuft, auch wenn man andere Hauptsysteme abstellen müsste.»*

Geräteunabhängigkeit: Alle Interviewteilnehmer sprachen sich für eine Geräteunabhängigkeit aus und stellen damit die Anforderung, dass eine eingesetzte Digital Signing Lösung von allen Geräten (Desktop, Laptop, Tablet, Mobile) und von allen Betriebssystemen (Windows, MAC usw.) aus einsetzbar sein muss. Interessant festzustellen war, dass sich allerdings drei Personen auch skeptisch zeigten, was die eigentliche digitale Signierung vom Mobile aus angeht. Aufgrund des kleinen Bildschirms des Mobilegerätes möchten sie lange, komplexe oder wichtige Verträge dann doch lieber auf einem Desktop Computer oder Laptop überprüfen und signieren.

GP-2: *«In einer perfekten Welt sollte die Gegenpartei dein digital signiertes Dokument erkennen können, egal ob sie dies auf einem Mobile, Tablet oder auf einem Mac oder Windows Computer anschauen.»*

GP-3: *«Wenn ich signiere, hat es meistens einen Grund. Dann möchte ich das Dokument auch noch [gut] durchlesen können. Wenn es vielleicht ein Brief ist [one- pager] – ok. Wenn ich aber z. B. ein 40-seitiges Dokument habe, muss ich schon wissen, um was es genau geht. Vielleicht kommt es ein wenig aufs Dokument drauf an. […] Wenn ich jetzt so mein Telefon mit seiner Bildschirmgrösse anschaue, logge ich mich lieber schnell im Citrix [über Laptop / Desktop] ein, sodass ich dann auch die Unterschrift gut platzieren kann.»*

Individualisierbare Workflowkomponenten inkl. Frontend & Dashboard: Vier von fünf Interviewpartnern genügte die «nackte» digitale Signatur nicht, sie stellten auch

Anforderungen an unterstützende Workflowkomponenten. Von zwei Gesprächspartnern wurde dieses Kriterium sogar als sehr wichtig bewertet. Die Workflowkomponenten sollen es nebst der eigenen Signatur auch erlauben, direkt aus der Digital Signing Lösung heraus weitere (interne und externe) Unterzeichner einzuladen, zu definieren mit welcher Art von digitaler Signatur die eingeladenen Unterzeichner signieren sollen als auch Auswertungsmöglichkeiten bieten (z. B. wer hat wie viele Dokumente signiert, von wem ist das Dokument noch nicht signiert usw.). Lediglich eine Person begnügte sich derzeit mit der blossen digitalen Signatur und fokussierte keine weiteren Funktionen darüber hinaus.

GP-3: *«Persönlich fände ich das spannend. Weil dann kann ich direkt sagen, Manager X und Y, ihr zwei bitte digital signieren.»*

GP-4: *«Und auch komplexe Verträge müssen einfach handelbar sein. Und wir müssen [externe] Dritte einfach in den Signaturprozess integrieren können. Das System funktioniert nur gut, wenn die gesamte Geschäftswelt digital signiert.»*

GP-4: *«Ich finde das sehr wichtig. Das hilft den Prozess wirklich steuern zu können. Auch dass ich sagen kann, dieser Vertragspartner muss qualifiziert digital unterzeichnen [der Signaturworkflow-Initiant gibt vor, mit welcher Art von digitaler Signatur unterzeichnet werden muss] oder dass er zuerst unterzeichnen muss.»*

GP-4: *«Ich finde es noch gut, wenn man alles auswerten kann. Welche Verträge hat wer unterzeichnet.»*

Intuitive, einfache Digital Signing Prozesse: Drei der befragten Personen stellten beim geschäftlichen Einsatz der digitalen Signatur die Anforderung, dass der Signierprozess möglichst einfach und intuitiv gestaltet sein muss. Für diese drei Personen war diese Erwartung nicht nur nice-to-have, sondern signifikant wichtig. Je einfacher und selbstverständlicher der digitale Signierungsprozess gestaltet ist, desto stärker prognostizierten die Interviewpartner die Verwendung.

GP-3: *«Es muss immer schnell gehen, je mehr Hürden ich habe, desto weniger mache ich es.»*

GP-4: *«Sie muss ganz einfach sein [im Handling]. Und ich möchte nicht studieren müssen, ob ich nun mit einer fortgeschrittenen, einer qualifizierten oder einer einfachen elektronischen Signatur unterschreiben soll. Der ganze Prozess sollte ohne Studieren*

vonstattengehen können. Alles andere ist fehleranfällig. Insbesondere auch, wenn er jetzt mal zwei bis drei Monate nichts signiert hatte und er hat dann wieder etwas zu Signieren, dann muss es selbsterklärend sein, sonst verzweifeln die User. […]»

Schnittstelle / Anbindung an vor- oder nachgelagerte Applikationen: Vier der fünf Interviewpartner stellten zugunsten einer breiten geschäftlichen Verwendung der digitalen Signatur die Anforderung, dass die eingesetzte Digital Signing Lösung auch Schnittstellen in bereits im Unternehmen vorhandene Applikationen unterstützen können muss. Als Hintergrund dieser Anforderung können wiederum Effizienzvorteile mittels durchgängigen Geschäftsprozessen verstanden werden, z. B. dass ein signiertes Dokument automatisiert dem ERP System zugeführt wird und dies nicht manuell geschehen muss. Eine befragte Person benötigte diese Funktion nicht und fokussierte ausschliesslich auf einen digitalen 1:1 Ersatz der Handunterschrift.

GP-2: *«Dort wäre es allerdings spannend, wenn es mit einem Vertrags-managementtool verlinkt wäre.»*

GP-5: *«Einen wichtigen Aspekt finde ich auch die Anwendungsübergreifbarkeit. Ich habe gerne Lösungen, die ich nachher überall einsetzen kann. Da kann man bis in Fachanwendungen denken, die wir selbst gebaut haben.»*

Single Sign On und verschiedene Signaturtypen: Eine befragte Person definierte als nice-to-have Anforderung die Möglichkeit nach einer Single Sign On Anmeldung zur Digital Signing Lösung.
Ebenfalls nur von einer Person wurde die Anforderung gestellt, dass die Signinglösung verschiedene digitale Signaturarten unterstützen können muss.

GP-1: *«Und in meiner bescheidenen Welt wäre es cool, dass wenn ich das AD-Passwort wechsle, es mein Passwort vom Zertifikat ebenfalls gleich auch wechseln würde. Ich weiss aber, dass dies technisch nicht geht – es ist eher ein User-Problem. […]»*

GP-5: *«Absolut. Es gibt sehr viele Prozesse, wo man keine qualifizierte elektronische Signatur benötigt. Dort könnten wir uns das sehr gut vorstellen.»*

Zusammenfassung: Die Auswertung dieser Kategorie machte deutlich, dass grösstenteils der blosse digitale 1:1 Ersatz der Handunterschrift nicht ausreicht, sondern von den Unternehmen darüber hinausgehende Anforderungen wie

individualisierbare Workflowkomponenten oder Schnittstellen in andere Applikationen gestellt werden. Ebenfalls auffallend war die Favorisierung nach Cloudlösungen. Auch die Geräteunabhängigkeit als auch einfache und intuitive Signierprozesse zugunsten einer breiten geschäftlichen Verwendung der digitalen Signatur bildeten Anforderungen der interviewten Personen.

4.4. Ergebnisse zur Befriedigung der Zielgruppenansprüche

Dokumentname	Code	Anfang	Ende	Gewicht
Interview mit Gesprächspartner GP1	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	7	7	0
Interview mit Gesprächspartner GP1	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	8	8	0
Interview mit Gesprächspartner GP1	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	9	9	0
Interview mit Gesprächspartner GP1	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	9	9	0
Interview mit Gesprächspartner GP1	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	9	9	0
Interview mit Gesprächspartner GP1	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	19	19	0
Interview mit Gesprächspartner GP2	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	11	11	0
Interview mit Gesprächspartner GP2	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	12	12	0
Interview mit Gesprächspartner GP2	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	13	13	0
Interview mit Gesprächspartner GP3	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	7	7	0
Interview mit Gesprächspartner GP3	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	8	8	0
Interview mit Gesprächspartner GP4	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	7	7	0
Interview mit Gesprächspartner GP4	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	8	8	0
Interview mit Gesprächspartner GP5	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	10	10	0
Interview mit Gesprächspartner GP5	Befriedigung Ansprüche bestehender und/oder neuer Zielgruppen	11	11	0
Total 15 Nennungen				

Abbildung 13 Codierungen Kategorie Zielgruppenansprüche

Quelle: Eigene Darstellung, abgeleitet aus «MAXQDA 2020»-Software

Einleitung: Insgesamt wurden 15 Passagen aus den Interviewantworten der Kategorie «Befriedigung Zielgruppenansprüche» zugeordnet. Die vorab auf Basis der Theorie prognostizierten Anforderungen (deduktive Codes) wurden grösstenteils bestätigt. In dieser Kategorie wurden keine neuen Anforderungen (induktive Codes) durch die Gespräche generiert.

Befriedigung Bedürfnisse bestehender oder neuen Zielgruppen & Zusammenfassung: Obschon sich alle Interviewpartner zu ihren Anforderungen an Digital Signing in Bezug auf ihre bestehenden oder neuen (externen) Zielgruppen wie Kunden oder Partner äusserten, hatte keiner die Befriedigung derer Bedürfnisse als sehr wichtige Anforderung taxiert. Vier der fünf Gesprächspartner berichteten allerdings von Fällen, wo externe Vertragsparteien bei der Unterzeichnung von Dokumenten eine digitale Signatur von ihnen forderten. Ebenfalls war auffallend, dass die Gesprächspartner eine zeitliche Entwicklung feststellten, d.h. früher die Anforderung nach einer digitalen Signatur von ihren externen Vertragsparteien nicht oder nur vereinzelt gestellt wurde, heutzutage jedoch immer häufiger. Die Erwartungshaltung der externen Unterzeichnungsparteien scheint sich auch kundenspezifisch zu unterscheiden. So berichtete eine Interviewperson, dass vor allem internationale Grossunternehmen von ihnen eine digitale Signatur fordern, während andere

Gesprächspartner klare Personengruppen benennen konnten (z. B. Garagisten), für welche dies derzeit gar keine Anforderung darstellt.

GP-1: *«Dannzumal wo wir das eingeführt haben [vor dreieinhalb Jahren], glaube ich, war das noch nicht im Fokus. Aber heute würde ich ganz klar sagen, wir haben gewisse Vorgaben und Richtlinien von der Revisionsaufsichtsbehörde und auch grossen Kunden, die das von uns erwarten. Heute ist die Erwartung [der Kunden] ganz anders, als wo wir es eingeführt hatten.»*

GP-1: *«Könnte ich mir gut vorstellen, vor allem bei grossen internationalen Firmen ist es sicher eher ein Thema. Wir haben aber auch kleine Kunden / KMU's, die in der Digitalisierung noch gar nirgends sind. Wir bekommen immer noch regelmässig [von diesen kleinen Firmen / KMUs] Schuhschachteln mit Belegen zugesendet, die wir danach digitalisieren. [...]»*

GP-2: *«Das Werk [Lieferant] mittlerweile ja. […] Wer aber gar keine digitalen Unterschriften verwendet sind unsere Garagisten, wenn sie mit uns als Importeuer arbeiten. Dort sind wir schon froh, wenn sie es schaffen, ein Dokument einzuscannen. Dort machen wir eigentlich noch fast alles physisch per Post, mit Blut und Schweiss unterschrieben. Wer aber sicher immer mehr nachfragt, um Dokumente digital zu unterschreiben, sind die Endkunden, die beim Garagisten ein Auto kaufen.»*

4.5. Ergebnisse zu Sicherheitsansprüchen

Dokumentname	Code	Anfang	Ende	Gewicht
Interview mit Gesprächspartner	**Datenhaltung exklusive in Schweiz**	**14**	**14**	**2**
Interview mit Gesprächspartner GP2	Datenhaltung exklusive in Schweiz	19	19	0
Interview mit Gesprächspartner	**Datenhaltung exklusive in Schweiz**	**9**	**9**	**2**
Interview mit Gesprächspartner	**Datenhaltung exklusive in Schweiz**	**15**	**15**	**2**
Interview mit Gesprächspartner GP1	höchste IT-Security Standards (v.a. bei Datenhaltung)	10	10	0
Interview mit Gesprächspartner GP1	höchste IT-Security Standards (v.a. bei Datenhaltung)	14	14	0
Interview mit Gesprächspartner GP1	höchste IT-Security Standards (v.a. bei Datenhaltung)	23	23	0
Interview mit Gesprächspartner GP1	höchste IT-Security Standards (v.a. bei Datenhaltung)	23	23	0
Interview mit Gesprächspartner GP2	höchste IT-Security Standards (v.a. bei Datenhaltung)	18	18	0
Interview mit Gesprächspartner GP2	höchste IT-Security Standards (v.a. bei Datenhaltung)	23	23	0
Interview mit Gesprächspartner GP4	höchste IT-Security Standards (v.a. bei Datenhaltung)	10	10	0
Interview mit Gesprächspartner	**höchste IT-Security Standards (v.a. bei Datenl**	**12**	**12**	**2**
Interview mit Gesprächspartner	**Keine Dokumententeilung mit Signaturanbiete**	**17**	**17**	**2**
Interview mit Gesprächspartner GP2	Keine Dokumententeilung mit Signaturanbieter / Hash-	18	18	0
Interview mit Gesprächspartner	**Keine Dokumententeilung mit Signaturanbiete**	**3**	**3**	**2**
Interview mit Gesprächspartner	**Keine Dokumententeilung mit Signaturanbiete**	**10**	**10**	**2**
Interview mit Gesprächspartner	**Keine Dokumententeilung mit Signaturanbiete**	**16**	**16**	**2**
Interview mit Gesprächspartner GP5	Keine Dokumententeilung mit Signaturanbieter / Hash-	27	27	0
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**10**	**10**	**2**
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**12**	**12**	**2**
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**3**	**3**	**2**
Interview mit Gesprächspartner GP3	Notwendigkeit Rechtverbindlichkeit von Digital Signinç	5	5	0
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**11**	**11**	**2**
Interview mit Gesprächspartner GP3	Notwendigkeit Rechtverbindlichkeit von Digital Signinç	19	19	0
Interview mit Gesprächspartner GP3	Notwendigkeit Rechtverbindlichkeit von Digital Signinç	20	20	0
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**2**	**2**	**2**
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**4**	**4**	**2**
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**9**	**9**	**2**
Interview mit Gesprächspartner GP5	Notwendigkeit Rechtverbindlichkeit von Digital Signinç	13	13	0
Interview mit Gesprächspartner	**Notwendigkeit Rechtverbindlichkeit von Digita**	**25**	**25**	**2**
Interview mit Gesprächspartner GP1	Sicherstellung Authentizität des Unterzeichners	5	5	0
Interview mit Gesprächspartner	**Sicherstellung Authentizität des Unterzeichne**	**4**	**4**	**2**
Interview mit Gesprächspartner GP2	Sicherstellung Authentizität des Unterzeichners	5	5	0
Interview mit Gesprächspartner GP3	Sicherstellung Authentizität des Unterzeichners	20	20	0
Interview mit Gesprächspartner GP3	Sicherstellung Authentizität des Unterzeichners	21	21	0
Interview mit Gesprächspartner GP5	Sicherstellung Authentizität des Unterzeichners	18	18	0
Interview mit Gesprächspartner GP2	Sicherstellung Dokumentenintegrität	14	14	0
Interview mit Gesprächspartner GP2	Sicherstellung Dokumentenintegrität	18	18	0
Interview mit Gesprächspartner GP3	Sicherstellung Dokumentenintegrität	21	21	0
Total 39 Nennungen				

Abbildung 14 Codierungen Kategorie Sicherheitsansprüche

Quelle: Eigene Darstellung, abgeleitet aus «MAXQDA 2020»-Software

Einleitung: Insgesamt wurden 39 Nennungen aus den Interviewantworten der Kategorie «Sicherheitsansprüche» zugeordnet. Die vorab auf Basis der Theorie prognostizierten Anforderungen (deduktive Codes) wurden allesamt bestätigt und noch mit zwei weiteren induktiven Codierungen - «Datenhaltung exklusive in der Schweiz» und «höchste IT-Security Standards» - ergänzt.

Datenhaltung exklusive in der Schweiz: drei Gesprächspartner forderten im Rahmen einer Digital Signing Lösung eine exklusive Datenhaltung in der Schweiz. Bei allen drei Personen respektive deren Unternehmungen galt dies als nicht verhandelbare Prämisse und deshalb als besonders wichtige Anforderung. Eine befrage Person thematisierte diese Anforderung nicht und eine weitere Person wusste nicht, wie die Datenhaltungsanforderungen seiner Unternehmung lauten.

GP-1: *«Die Datenhaltung muss in der Schweiz sein.»*

GP-5: *«Absolut, ja. Unsere Vorgabe lautet, dass unsere Daten sicher in der Schweiz gespeichert werden müssen. Und es muss auch gewährleistet sein, dass unsere Daten von dort die Landesgrenzen nicht verlassen können.»*

Höchste IT-Security Standards: Vier der fünf Interviewpartner gaben an, dass bei der geschäftlichen Verwendung einer Digital Signing Lösung höchste IT-Security Standards eine Anforderung darstellen. Die entsprechenden Interviewpersonen zeigten sich allerdings nicht selbst für diesen Fachbereich verantwortlich, sondern verwiesen an ihre hierfür zuständigen internen Fachabteilungen und konnten deshalb nicht weiter ins Detail gehen oder konkrete Anforderungen dazu benennen.

GP-4: *«Die Frage ist natürlich, wie sicher ist es, dass niemand mit meiner persönlichen digitalen Signatur für mich einkaufen geht. Das ist sicher noch eine Sorge, die bei den Leuten im Kopf ist.»*

GP-5: *«Sicherheitsaspekte sind immer das Wichtigste für uns, weil wir schlussendlich mit sehr sensiblen Daten unterwegs sind. Die Gewährleistung des Datenschutzes ist für uns primär, dies sichergestellt zu haben ist das oberste Credo. Und bei Übermittlungen möchten wir sicher sein, dass die Übermittlungskanäle sicher sind.»*

Keine Dokumententeilung mit Signaturanbieter / Hash Signing: Vier der befragten Personen präferierten eine Digital Signing Lösung, mit welcher das zu signierende Dokument nicht mit dem Signaturanbieter geteilt wird (Hash Signing). Für drei dieser Personen stellte dies sogar eine sehr wichtige Anforderung dar. Der Grund dafür liegt auf der Hand: wenn Dokumente signiert werden, betrifft dies in den meisten Fällen wichtige Vereinbarungen, ansonsten das Dokument ja erst gar nicht unterzeichnet werden müsste. Bei solch wichtigen Dokumenten mit teilweise sensiblen Inhalten (z. B. Sozialleistungsanträge) möchte man sicherstellen, dass nur die tatsächlich beteiligten und berechtigten Personen Dokumenteneinsicht haben. In einer ersten Betrachtung kann diese Anforderung als widersprüchlich zur erhobenen Favorisierung von Cloudlösungen verstanden werden. Der goldene Mittelweg scheint der hybride Ansatz von Hash Signing zu bieten, bei welchem der Grossteil der kritischen kryptografischen Operation beim Digital Signing Anbieter geschieht (Erfüllung Cloudanspruch, Reduzierung aufwändiger und komplexer Softwareinstallation beim Kunden, SLA Verantwortung grösstenteils beim Anbieter), allerdings anstelle eines lesbaren Dokuments nur ein nicht auf den Inhalt schliessbarer Hashwert an den Signaturanbieter

übermittelt wird (Erfüllung Dokumenteneinsicht nur für berechtigte Personen, dazu allerdings Softwareinstallation beim Kunden on premise notwendig).

GP-5: «Ja, absolut. Als ich das gesehen habe, fand ich dies sehr smart gelöst, dass ich unser Dokument nirgendwo hochladen muss und dieses bei uns bleibt.»

GP-5: *«Die von euch [QuoVadis] eingesetzte Lösung ist ja hybrid. Die Anwendung geschieht bei euch, aber das Dokument bleibt bei uns. Das ist so sehr smart gelöst für uns.»*

Notwendigkeit Rechtsverbindlichkeit von Digital Signing (QES): Bei dieser Codierung herrschte eine starke Einigkeit. Vier der fünf Interviewpartner formulierten die Anforderung, dass eine geschäftlich verwendete digitale Signatur der Handunterschrift gesetzlich gleichgestellt sein muss, was einzig mit der Verwendung der qualifizierten elektronischen Signatur möglich ist. Für diese vier Personen stellte dies nicht nur eine nice-to-have Anforderung dar, sondern zeigte sich als unabdingbares Kriterium. Lediglich eine befragte Person war sich der verschiedenen digitalen Signaturlevels nicht bewusst und hat dies erst im Rahmen des Interviews erfahren.

GP-1: *«Sicher sehr sehr wichtig. Wir haben mit sehr sensitiven Daten von unseren Kunden zu tun. […] Von dem her gesehen ist das für uns das A und O. Es kann nicht einfach irgendein Produkt sein, welches wir einsetzen. […] Nur schon von den Vorgaben der Finma Gesetzgebung und vom Geldwäschereigesetz her, dürfen wir nur qualifizierte, zertifizierte Lösungen einsetzen. Wir würden uns dadurch [mit einer nicht qualifizierten elektronischen Signatur) auch unglaubwürdig machen und hätten auch rechtliche Probleme.»*

GP-3: *«Sehr wichtig. Anders hätten wir es nicht akzeptiert. Sie müssen sich vorstellen, wenn Sie Verträge über ein paar Milliarden unterschreiben und es gibt daraus ein Problem, ist dann das Erste was der Anwalt sagt, dass die digitale [nicht qualifizierte] Unterschrift nicht rechtsgültig ist.»*

GP-4: *«Sie muss rechtlich verheben. Also eine qualifizierte elektronische Signatur die der Handunterschrift gesetzlich gleichgestellt ist. Ich glaube dies muss der grundsätzliche Anspruch sein.»*

Sicherstellung Authentizität des Unterzeichners und Dokumentenintegrität: Im Rahmen der Sicherheitsbedürfnisse bei der geschäftlichen Verwendung der digitalen Signatur wurden von den Gesprächspartnern auch Anforderungen an die Authentizität des Unterzeichners (Sicherstellung, dass auch tatsächlich zweifelsfrei derjenige unterschrieben hat, dessen Anschein es hat) und an die Dokumentenintegrität (das Dokument wurde nach der Signatur inhaltlich nicht mehr verändert) gestellt. Für die Sicherstellung der Authentizität des Unterzeichners sprachen sich vier Interviewpartner aus, wovon eine Person dieses Kriterium als sehr wichtig bewertete. Die Gewährleistung der Dokumentenintegrität wurde von zwei Personen gefordert.

GP-2: *«Und logischerweise möchte ich nicht, dass jemand anders für mich unterschreiben kann. Da haben wir heute hie und da ein Thema bei Fällen, wo ich meine Unterschrift eingescannt hatte, z. B. bei Massenversänden von Briefen. […] Und nun lese ich immer wieder von Rundschreiben an Händler, wo ich mitunterschrieben haben soll, aber vorab dazu gar nie die Freigabe erteilt habe.»*

GP-2: *«Ich gehe auch davon aus, dass das Dokument nachträglich nicht mehr veränderbar ist. Das würde ich voraussetzen.»*

Zusammenfassung: Die Interviewpartner präferierten für die bei einer digitalen Signatur anfallenden Daten eine exklusive Datenhaltung in der Schweiz. Allgemein zeigten sich hohe IT-Security Anforderungen, da im Rahmen von signierten Dokumenten grösstenteils sensible Inhalte verarbeitet werden, deren Zugriff stark geschützt werden möchte. Entsprechend kann auch die starke Forderung nach Hash Signing interpretiert werden, womit das zu signierende Dokument erst gar nicht mit dem Signaturanbieter geteilt wird. Sämtliche befragten Personen, welche über die verschiedenen digitalen Signaturtypen informiert waren, haben für die Anwendung in ihrem Unternehmen das höchste Level, die qualifizierte elektronische Signatur, gefordert, welche der eigenhändigen Unterschrift gesetzlich gleichgestellt ist.

4.6. Ergebnisse zu anderen Anforderungen / Varia

Dokumentname	Code	Anfang	Ende	Gewicht
Interview mit Gesprächspartner GP2	Corona Pandemie erhöht Bedürfnis für Digital Signing	3	3	0
Interview mit Gesprächspartner GP2	Corona Pandemie erhöht Bedürfnis für Digital Signing	22	22	0
Interview mit Gesprächspartner GP3	Corona Pandemie erhöht Bedürfnis für Digital Signing	2	2	2
Interview mit Gesprächspartner GP3	Corona Pandemie erhöht Bedürfnis für Digital Signing	19	19	0
Interview mit Gesprächspartner GP4	Corona Pandemie erhöht Bedürfnis für Digital Signing	3	3	2
Interview mit Gesprächspartner GP4	Einfaches Preismodell	6	6	0
Interview mit Gesprächspartner GP1	Imageaufwertung	12	12	0
Interview mit Gesprächspartner GP1	Imageaufwertung	13	13	0
Interview mit Gesprächspartner GP1	Imageaufwertung	14	14	0
Interview mit Gesprächspartner GP1	Imageaufwertung	19	19	0
Interview mit Gesprächspartner GP1	Nutzung Digital Signing ist abhängig vom Alter des Users	3	3	0
Interview mit Gesprächspartner GP4	QES-Zertifikat übergreifend nutzbar (unabhängig Signinglösung)	20	20	0
Interview mit Gesprächspartner GP3	Unsicherheit Akzeptanz digitale Signatur	6	6	0
Interview mit Gesprächspartner GP2	Unwissenheit verschiedene Signaturlevels	15	15	0
Interview mit Gesprächspartner GP2	Unwissenheit verschiedene Signaturlevels	16	16	0
Total 15 Nennungen				

Abbildung 15 Codierungen Kategorie andere Anforderungen / Varia

Quelle: Eigene Darstellung, abgeleitet aus «MAXQDA 2020»-Software

Einleitung: Insgesamt wurden 15 Passagen aus den Interviewantworten der Kategorie «Andere Anforderungen / Varia» zugeordnet. Die hier generierten Codierungen wurden grösstenteils nicht im Vorfeld definiert, sondern ergaben sich erst durch die Interviews und gelten somit als induktive Codierungen. Hier wurden nicht nur klassische Anforderungen codiert, sondern auch andere Aussagen, die im Zusammenhang zum Forschungsthema als interessant erschienen.

Corona-Pandemie erhöht Bedürfnis für Digital Signing: Die aktuelle Corona-Pandemie wurde von drei Interviewpartnern proaktiv thematisiert. Sie sahen in dem damit verbundenen Homeoffice-Modus ein klar steigendes Bedürfnis an Digital Signing und damit an der Digitalisierung dieser «letzten Meile».

GP-4: *«Und jetzt, wo wir alle im Homeoffice sind [Corona-Pandemie], haben wir erkannt, dass es immer dringender wird und dass wenn wir von Digitalisierung sprechen, dass man auch digital Signieren muss. […]»*

GP-3: *«Der Schmerzensdruck bis anhin war aber noch zu wenig gross. […] Jetzt aber mit dem Homeoffice [durch die Corona-Pandemie] und unserer Policy, dass man Zuhause keine Dokumente ausdrucken darf, hat man gemerkt, dass der Prozess nicht mehr funktioniert. Es würde bedeuten, dass immer zwei Personen ins Büro fahren müssten, weil wir immer kollektiv unterzeichnen müssen. So haben wir einen Push bekommen, eine digitale Signierlösung einzuführen.»*

Einfaches Preismodell: Ein Interviewpartner bemängelte, dass die Preismodelle für Digital Signing nicht genügend transparent und einfach seien und stellte die Anforderung an ein einfaches Flat-Rate Modell.

GP-4: *«Die Preishöhe ist noch schwierig zu beurteilen. Irgendwie müsste man auf ein Flat Rate Modell kommen können. Also eher die Kosten auf eine Person bezogen, wie ein Mobile-Abonnement. Die aktuelle Schwierigkeit liegt im hin und her rechnen mit den verschiedenen Tarifen zwischen den Signaturtypen und dann kommt noch der Userpreis hinzu, da blickt niemand mehr durch. Ich fände es schön, wenn wir sagen könnten, wir haben 220 Mitarbeiter mal XYZ Kosten pro Person.»*

Imageaufwertung: Diese deduktive Codierung wurde viermal berücksichtigt. In zwei Fällen wurde die Anforderung beschrieben, mit Digital Signing eine Vorbildungsfunktion zu erreichen respektive als innovativer Dienstleister wahrgenommen zu werden. In den anderen zwei Fällen galt der Blick auf das Image vor allem der Befürchtung, dass wenn man nicht die höchste digitale Signaturstufe (QES) verwenden würde, sich dies negativ auf die Reputation auswirken würde.

GP-1: *«Weil wir dort auch eine gewisse Vorbildfunktion gegenüber den Kunden haben.»*

GP-1: *«Wir würden uns dadurch [mit einer nicht qualifizierten elektronischen Signatur] auch unglaubwürdig machen».*

Nutzung Digital Signing ist abhängig vom Alter des Users: Ein Gesprächspartner brachte die Perspektive ein, dass die Nutzung der digitalen Signatur mit dem Alter des Users zusammenhängen könnte, konkret dass ältere User Digital Signing aufgrund der Komplexität weniger nutzen möchten.

GP-1: *«Es gibt sicher die einen oder anderen, welche vielleicht auch etwas älter sind und finden, sie kämen hier nicht draus und dann von Hand unterschreiben.»*

QES-Zertifikat übergreifend nutzbar (unabhängig Signinglösung): Eine befragte Person stellte die Anforderung, dass ein qualifiziertes Zertifikat, welches die Basis für die qualifizierte elektronische Signatur bildet, plattformübergreifend und damit unabhängig vom Anbieter der Digital Signing Lösung, genutzt werden können muss.

GP-4*: «Irgendwie sollte jede Person bereits eine solche Registration [Qualifiziertes Zertifikat] haben, welche auch unabhängig vom Unternehmen gilt. Ob ich nun auf einer*

Swisscom, QuoVadis oder Europäischen Plattform bin, das sollte gar keine Rolle spielen, zumindest innerhalb der Schweiz nicht.»

Unsicherheit Akzeptanz digitale Signatur: Ein Interviewpartner zeigte sich unsicher, ob die amerikanische Steuerbehörde Dokumente akzeptiert, welche neu nicht mehr von Hand unterzeichnet werden, sondern mittels einer Schweizer qualifizierten elektronischen Signatur digital signiert sind.

GP-3: *«Wir sind gespannt, wie die Amerikaner reagieren werden, wenn die Formulare von uns digital signiert daherkommen. Gerade Steuerbehörden sind so «tick the box», Hauptsache das Häkchen ist da, ob es stimmt oder nicht, ist egal. […] Die Manager kennen die digitale Signatur schon, bei den Behörden sind wir gespannt, was dort die Rückmeldung sein wird.»*

Ungewissheit verschiedene Signaturlevels: Lediglich einem der fünf Gesprächspartner war nicht bewusst, dass in der Schweiz ausschliesslich die qualifizierte elektronische Signatur der Handunterschrift gesetzlich gleichgestellt ist. Den anderen interviewten Personen war dieser Umstand nicht nur bewusst, sondern sie haben sich im Rahmen einer Nutzung der digitalen Signatur für ihr Unternehmen sogar klar für die Verwendung der qualifizierten elektronischen Signatur ausgesprochen.

GP-2: *«Ehrlicherweise habe ich zu wenig Wissen diesbezüglich. Ich wüsste nicht, wie so ein digital signiertes Dokument [ein nicht mit einer qualifizierten elektronischen Signatur signiertes Dokument] vor Gericht standhalten würde.»*

GP-2: *«Ich glaube es war bis anhin noch kein Thema, weil wir keinen konkreten Fall hatten, welcher in einer Gerichtsverhandlung geendet ist. Darum war es zumindest mir nicht bekannt. Wenn ich dich richtig verstehe, ist z. B. die Lösung, welche wir nutzen, nicht qualifiziert und rechtssicher?»*

Zusammenfassung: Aus der Kategorie «andere Anforderungen / Varia» stach die dominierende Nennung der Corona-Pandemie heraus, welche aufgrund der Homeoffice Situation das Bedürfnis auf komplett digitale Geschäftsprozesse, inklusive der Unterschrift, stark fördert. Ebenfalls mehrfach erwähnt wurde das Anstreben (Anforderung) eines Images als innovativer und digitaler Dienstleister im Zuge der Nutzung der digitalen Signatur. Hingegen wurden die im Vorfeld aus Basis der Theorie abgeleiteten Anforderungen (deduktive Codes) «Erkennen von Kunden- und

Nutzungsdaten zu Marketingoptimierungszwecken» und «Ökologische Effizienz steigern» von keinem der Interviewpartner erwähnt.

4.7. Konsolidierte Betrachtung geschäftliche Anforderungen an Digital Signing

Insgesamt wurden aus den Antworten der fünf Interviews 197 Anforderungen zugunsten einer breiten geschäftlichen Verwendung der digitalen Signatur auf 30 Codierungen zugeteilt, welche wiederum in sechs Kategorien zusammengefasst wurden.

Die häufigsten genannten Anforderungen betrafen die Kategorien **«Funktionsumfang / Varianten Digital Signing Lösung»** und **«User-Onboarding: schnell, einfach, digital und kostengünstig».** Bei der Kategorie **«Funktionsumfang / Varianten Digital Signing Lösung»** konnte festgestellt werden, dass die meisten Gesprächspartner weitere Funktionen über die reine digitale Signatur hinaus forderten. So sollen Workflowkomponenten (z. B. in einem Unterzeichnungsprozess sogleich die Teilnehmer festlegen und einladen) und auch Schnittstellen der Digital Signing Lösung in bereits bestehende Applikationen (z. B. ERP des Unternehmens) den Signierprozess veredeln und bestmöglich in die Geschäftsprozesse integrieren. Die digitale Signierungslösung wurde als Cloudlösung favorisiert und soll zugunsten einer breiten Verwendung geräteunabhängig funktionieren. Starke Anforderungen wurden auch an die Kategorie **«User-Onboarding: schnell, einfach, digital und kostengünstig»** gestellt, welche gleichzeitig als aktueller Schmerzenspunkt identifiziert werden konnte. Digital Signing kann nur dann maximal wertschöpfend eingesetzt werden, wenn eine Unternehmung als Initiant eines digitalen Signierprozesses auch externe Unterzeichner einfach und in attraktiver Weise für eine digitale Gegensignatur motivieren kann. Gepaart mit der klaren Forderung nach der höchsten digitalen Signaturart (Kategorie **«Sicherheitsansprüche»**) - der qualifizierten elektronischen Signatur - zeigte sich die aktuelle Regulierung mit der verlangten physischen User-Identifikation durch eine berechtigte Stelle als Problem und Konflikt zum Bedürfnis eines attraktiven User-Onboardings. Je einfacher und schneller User für die (höchste) digitale Signatur befähigt und eingerichtet werden können, desto stärker wurde die geschäftliche Verwendung von Digital Signing prognostiziert.

Vier von fünf Gesprächspartnern gaben an, dass sie Anwendungsfälle der geschäftlichen digitalen Signatur haben, bei welchen die Gegenpartei eine digitale Signatur von ihnen fordert (Kategorie **«Befriedigung Zielgruppenansprüche»**). Digital Signing wird damit nicht nur für einsetzende Unternehmung ein

Digitalisierungsinstrument, sondern wird mehr und mehr auch von deren Zielgruppen gefordert.

Im Rahmen der **«Sicherheitsansprüche»** wurde neben der höchsten digitalen Signaturstufe (QES) auch eine exklusive Datenhaltung in der Schweiz dominant gefordert. Die Erwartungen an hohe IT-Security Standards als auch die signifikante Forderung nach Hash Signing zeigten auf, dass im Rahmen von Digital Signing grösstenteils sensible Daten verarbeitet werden, welche bestmöglich geschützt sein möchten.

Eine konstante Anforderung - kategorienübergreifend - war die Erwartung nach zeitsparenden und effizienten als auch intuitiven Digital Signing Prozessen. Ob beim User-Onboarding oder beim eigentlichen digitalen Signieren (Kategorie **«Effiziente, digitale und kostengünstige Geschäftsprozesse»**): je schneller und einfacher der Prozess gestaltet werden kann, desto stärker wurde die Nutzung prophezeit.

Eine interessante Erkenntnis bildeten die Aussagen, dass die aktuelle Corona-Pandemie als Beschleunigungsfaktor zur Einführung einer digitalen Signaturlösung angesehen wird (Kategorie **«Andere Anforderungen / Varia»**). Aus nice-to-have vor der Pandemie wurde in manchen Fällen ein must-have in der Pandemie.

Das nachfolgende Kapitel 5. wird auf Basis der erhobenen Anforderungen derzeitige Schwachstellen der digitalen Signatur identifizieren und Handlungsempfehlungen zur Verbesserung dieser Mängel präsentieren.

5. Handlungsempfehlungen

Zur Beantwortung der Nebenfragenstellung nach notwendigen Optimierungsmassnahmen zur Förderung der breiten kommerziellen Nutzung der digitalen Signatur in der Schweiz werden nachfolgend Handlungsempfehlungen für die wichtigsten erhobenen Anforderungen erarbeitet, welche aus aktueller Marktangebotsperspektive nicht oder nur teilweise erfüllbar sind.

Alle anderen erhobenen Anforderungen können aus aktueller Marktangebotssicht entweder bereits gut erfüllt werden oder wurden als nicht genügend wichtig bewertet, um dafür Handlungsmassnahmen einzuleiten.

5.1. Handlungsempfehlung zugunsten attraktives User-Onboarding

Zugunsten eines breiten geschäftlichen Einsatzes der digitalen Signatur hat sich die attraktive User-Befähigung, das sogenannte User-Onboarding, als erfolgskritische Komponente gezeigt. Die Anforderungen nach «schnell, einfach, digital und kostengünstig» können insbesondere im Rahmen der qualifizierten elektronischen Signatur nicht erfüllt werden, da aktuell eine physische User-Identifikation bei einer berechtigten Stelle verlangt wird. Dieser Umstand erschwert es den Unternehmungen insbesondere externe Unterzeichner in attraktiver Art und Weise in den digitalen Signaturprozess einzubinden und zeigt sich als grosse Hürde der Skalierung von Digital Signing.

Kategorie	Nicht oder nur teilweise erfüllte Anforderungen (Codierungen)	Handlungsempfehlung	Adressat
«User-Onboarding: schnell, einfach, digital und kostengünstig»	• Einfache, effiziente, günstige und digitale User-Identifikation • Kleinstmögliche Vorlaufzeit- / einfaches User-Onboarding	Die für die qualifizierte elektronische Signatur derzeit physisch notwendige User-Identifikation muss digitalisiert werden. Die regulatorische Voraus-setzung ist mit dem Art. 7 Abs. 1 VZertES bereits vorhanden: *«Die Identität einer Person […] kann auf Distanz festgestellt werden, sofern eine Konformitätsbewertungsstelle bestätigt hat, dass das verwendete Verfahren zur Personenidentifikation eine gleichwertige Sicherheit zum persönlichen Erscheinen bietet.»*	• BAKOM als verantwortliche Bundesinstanz für ZertES • Schweizerische Konformitäts-bewertungs-stelle (SAS Schweizerische Akkreditierungs-stelle)

		Anstrengungen für eine Bestätigung dieser gleichwertigen Sicherheit eines digitalisierten User-Identifikations-verfahrens sind bereits im Gange (Details in Kapitel 7.2.). Sobald die vollständig digitale Personenidentifikation zugunsten einer QES ermöglicht wird, kann auch die zweite Anforderung nach einer kleinstmöglichen Vorlaufzeit und einem einfachen User-Onboarding erfüllt werden.	

Tabelle 5 Handlungsempfehlung attraktives User-Onboarding

Quelle: eigene Darstellung

5.2. Handlungsempfehlung zugunsten cloudbasierter Schweizer Signierlösung

Die dominant gestellten Anforderungen nach einer cloudbasierten Signierlösung mit exklusiver Datenhaltung in der Schweiz in Kombination mit Hash Signing werden derzeit noch nicht von allen Anbietern erfüllt. Ebenfalls kann die vielfach geforderte Geräteunabhängigkeit noch nicht vollständig durch alle Anbieter von Digital Signing Lösungen erfüllt werden.

Kategorie	Nicht oder nur teilweise erfüllte Anforderungen (Codierungen)	Handlungsempfehlung	Adressat
«Sicherheits-ansprüche» und «Funktionsumfang / Varianten Digital Signing Lösung»	• Keine Dokumenten-teilung mit Signatur-anbieter / Hash Signing • Datenhaltung exklusive in der Schweiz • Cloudfähigkeit • Geräteunabhängig-keit	Als goldene Kombination zur Erfüllung der Unternehmensansprüche zeigt sich eine cloudbasierte Digital Signing Lösung, wobei eine exklusive Schweizer Datenhaltung sichergestellt wird. Damit die zu signierenden Dokumente erst gar nicht mit dem Signaturanbieter geteilt werden müssen, soll die präf-erierte Lösung auch Hash Signing ermöglichen, was allerdings einen Gegensatz zur favorisierten reinen Cloudlösung darstellt: für die Sicher-stellung von Hash Signing muss eine (kleine) Softwarekomponente bei den Usern lokal (On Premise) installiert werden, welche das Hashing der	Anbieter von Digital Signing Lösungen

		Dokumente und die Kommunikation zu der (in der Cloud betriebenen) Signaturlösung ermöglicht. Dies scheint allerdings verkraftbar zu sein, sofern diese Softwarekomponente schnell und einfach lokal von den Usern in Betrieb genommen werden kann, da die Cloudanforderungen vor allem aus Kosten- und Performance-gewährleistungsgründen gefordert wurden. In diesem Zusammenhang würde man dann von einem hybriden (On Premise (Hash Signing-Komponente) / Cloud (Signierlösung beim Anbieter betrieben)) Ansatz sprechen. Sollte das Handling mit der Hash Signingkomponente nicht einfach möglich sein, geniesst der Cloud-ansatz den Vorzug vor Hash Signing. Sofern die Dokumente über eine Schweizer Cloud gehandelt werden und nach kurzer Zeit vom Signatur-anbieter automatisch gelöscht werden, erfüllt dies die meisten Anforderungen in diesem Kontext ebenfalls. Bzgl. der Geräteunabhängigkeit sollte die optimale Digital Signing Lösung von sämtlichen Geräten und den gängigsten Betriebssystemen aufgerufen und bedient werden können (Desktop Computer, Mobiles, Tablets, Windows, Mac, Android).	

Tabelle 6 Handlungsempfehlung Schweizer Cloud-Lösung & Geräteunabhängigkeit

Quelle: eigene Darstellung

5.3. Handlungsempfehlung Unterstützung Schnittstellen

Um Digital Signing bestmöglich in Geschäftsprozesse zu integrieren wurde die Möglichkeit nach Schnittstellen in Drittapplikationen gefordert. Durch Schnittstellen in (bereits bei den Unternehmungen bestehende) Fremdapplikationen können durchgängige Prozesse ermöglicht und damit manuelle Aufwände zugunsten einer Effizienzsteigerung reduziert werden. So kann z. B. via Schnittstelle ein signiertes Dokument aus der Digital Signing Lösung automatisiert ins Archivsystem der Unternehmung transferiert werden. Aus aktueller Angebotsperspektive unterstützen

noch nicht alle Digital Signing Lösungen diese Möglichkeit nach Schnittstellen in Fremdapplikationen.

Kategorie	Nicht oder nur teilweise erfüllte Anforderungen (Codierungen)	Handlungsempfehlung	Adressat
«Funktionsumfang / Varianten Digital Signing Lösung»	Schnittstelle / Anbindung an vor- oder nachgelagerte Applikationen	Es wird empfohlen, dass die Digital Signing Lösungen die weit verbreitete REST-API (Representational State Transfer (REST) Application Programming Interface (API)) als Standardtechnologie für die Ermöglichung von Schnittstellen in Drittapplikationen unterstützen. REST-API's gelten als einfacher verwendbar als SOAP-APIs (Simple Object Access Protocol (SOAP)) (Red Hat Limited, kein Datum) und sollten daher als Technologiestandard für Schnittstellen von den Digital Signing Anbietern verwendet werden.	Anbieter von Digital Signing Lösungen

Tabelle 7 Handlungsempfehlung Unterstützung Schnittstellen

Quelle: eigene Darstellung

5.4. Handlungsempfehlung QES-Angebot

Die befragten Personen sprachen sich klar für die höchste digitale Signaturstufe, der qualifizierten elektronischen Signatur, aus. Sie möchten in allfälligen Streitfällen, welche vor einem Schweizer Gericht verhandelt werden, auf der sicheren Seite sein und keinen Zweifel an den digital signierten Dokumenten aufkommen lassen. Wie im Hauptteil I aufgezeigt, kann die qualifizierte elektronische Signatur ausschliesslich von dazu akkreditierten Unternehmen ausgestellt werden. Digital Signing Anbieter, welche nicht über diese Akkreditierung verfügen, können die QES allerdings von akkreditierten Unternehmen einkaufen und so ihren Kunden zur Verfügung stellen. Aus aktueller Angebotsperspektive erfüllen noch nicht alle Anbieter von Digital Signing Lösungen diese dominierende Anforderung nach der QES. Dabei geht es nicht nur um die reine Einkaufsmöglichkeit einer QES, sondern auch um die Art und Weise dieser Ermöglichung, welche für den User möglichst standardisiert und einfach ablaufen sollte.

Kategorie	Nicht oder nur teilweise erfüllte Anforderungen (Codierungen)	Handlungsempfehlung	Adressat
«Sicherheits-ansprüche»	Notwendigkeit Rechtverbindlichkeit von Digital Signing (QES)	Es wird empfohlen, dass sämtliche Digital Signing Anbieter ihren Kunden die QES einfach verfügbar machen. Dafür nicht akkreditierte Anbieter können die QES über einen akkreditierten Anbieter einkaufen und ihren Kunden anbieten (Reselling). Es reicht dabei nicht aus, nur eine QES verfügbar zu machen, sondern die Erlangung dieser QES muss für den User so einfach und smart wie möglich gewährleistet sein. Das Interviewzitat «*Es muss immer schnell gehen, je mehr Hürden ich habe, desto weniger mache ich es.*» beschreibt diese Anforderung sehr treffend. Eine jüngst dafür entwickelte Schnittstelle vom Cloud Signature Consortium (CSC) ermöglicht den nicht akkreditierten Anbietern über einen standardisierten Prozess die QES über akkreditierte Anbieter in ihre Digital Signing Lösung zu integrieren und so ihren Usern sehr attraktiv und smart zugänglich zu machen (Cloud Signature Consortium VZW, kein Datum). Nun gilt es diese Schnittstelle von allen Digital Signing Anbieter zu integrieren.	Anbieter von Digital Signing Lösungen

Tabelle 8 Handlungsempfehlung QES-Angebot

Quelle: eigene Darstellung

Mit dem Abschluss dieses Kapitels liegen nun alle Informationen vor, um im nachfolgenden Kapitel 6. die Forschungsfragen abschliessend zu beantworten.

6. Beantwortung Forschungsfragen und Fazit Hauptteil II

6.1. Beantwortung der Forschungsfragen

Für die Beantwortung der **Hauptforschungsfrage «Was sind die Anforderungen von ausgewählten Vertretern von Schweizer Unternehmen zugunsten einer breiten geschäftlichen Nutzung der digitalen Signatur?»** kann auf das Kapitel 4. und im speziellen auf das Kapitel 4.7. verwiesen werden. Die nachfolgende Grafik zeigt, ungeachtet der Anzahl Nennungen oder Wichtigkeit für die befragen Personen, alle im Rahmen der Interviews genannten Anforderungen:

Zusammenfassende Kategorie	Genannte Anforderungen
Effiziente, digitale und kosten-günstige Geschäftsprozesse	• Zeitersparnis erreichen • Effizienzsteigerung durch strukturierte Daten • Personalaufwand, verursacht durch manuelle und meist analoge Prozesse, senken (z. B. Eliminierung Dokumente einscannen für Digitalisierung) • Allgemeine Kostensenkung (Druckkosten, Portokosten senken) • Attraktiver Kostenaufwand für Digital Signing (günstig)
User-Onboarding: schnell, einfach, digital und kostengünstig	• einfache, effiziente, günstige und digitale User-Identifikation (intern & extern) • kleinstmögliche Vorlaufzeit / einfaches User-Onboarding • Forderung nach E-ID
Funktionsumfang / Varianten Digital Signing Lösung	• Cloudfähigkeit • On Premise • Individualisierbare Workflowkomponenten inkl. Frontend & Dash-board (v. a. Möglichkeit, externe Unterzeichner einfach zum Unter-zeichnungsprozess einzuladen) • Intuitive, einfache Digital Signing Prozesse • Geräteunabhängigkeit (Desktop & Mobile, neutral in Bezug auf Betriebssysteme) • Schnittstelle / Anbindung an vor- oder nachgelagerte Applikationen • Single Sign On • Verschiedene Signaturtypen
Befriedigung Zielgruppenansprüche	• Befriedigung Ansprüche bestehender und / oder neuer Zielgruppen

Sicherheitsansprüche	• Sicherstellung Authentizität Unterzeichner • Sicherstellung Dokumentenintegrität • Datenhaltung exklusive in der Schweiz • Höchste IT-Security Standards (v.a. bei Datenhaltung) • Keine Dokumententeilung mit Signaturanbieter / Hash Signing • Notwendigkeit Rechtsverbindlichkeit von Digital Signing (QES)
Andere Anforderungen	• Imageaufwertung • Einfaches Preismodell • QES-Zertifikat übergreifend nutzbar (unabhängig Signinglösung)

Tabelle 9 Anforderungen aus Interviews, ungeachtet Menge der Nennungen

Quelle: eigene Darstellung

Wird die Anzahl der Nennungen und die Wichtigkeit einer Anforderung für die Gesprächspartner berücksichtigt, zeigt sich ein Fokus auf die nachfolgenden Kategorien und Codierungen (Anforderungen):

- **User-Onboarding: schnell, einfach, digital und kostengünstig**
  - einfache, effiziente, günstige und digitale User-Identifikation (intern & extern), insbesondere für QES
  - kleinstmögliche Vorlaufzeit / einfaches User-Onboarding
- **Funktionsumfang / Varianten Digital Signing Lösung**
  - Cloudfähigkeit
  - Individualisierbare Workflowkomponenten inkl. Frontend & Dashboard (v. a. Möglichkeit, externe Unterzeichner einfach zum Unterzeichnungsprozess einzuladen)
  - Intuitive, einfache Digital Signing Prozesse
  - Geräteunabhängigkeit (Desktop & Mobile, neutral in Bezug auf Betriebssysteme)
  - Schnittstelle / Anbindung an vor- oder nachgelagerte Applikationen
- **Sicherheitsansprüche**
  - Datenhaltung exklusive in der Schweiz
  - Höchste IT-Security Standards (v.a. bei Datenhaltung)
  - keine Dokumententeilung mit Signaturanbieter / Hash Signing
  - Notwendigkeit Rechtsverbindlichkeit von Digital Signing (QES)

- Die oberhalb erwähnten besonders im Fokus stehenden Anforderungen an eine breite geschäftliche Verwendung der digitalen Signatur beeinflussen schlussendlich die Kategorie «**Effiziente, digitale und kostengünstige Geschäftsprozesse»** massgeblich.

Die aus der Theorie (Hauptteil I) abgeleiteten Anforderungen liessen sich grösstenteils durch die Interviews (Praxis) bestätigen und erweitern. Einzig die theoretischen Anforderungen nach «Erkennen von Kunden- und Nutzungsdaten zu Marketing-optimierungszwecken» und «Ökologische Effizienz steigern» wurden durch die Praxiserhebung nicht bestätigt.

Die Beantwortung der **Nebenfragestellung «Was sind notwendige Optimierungsmassnahmen (zuhanden verschiedener Adressaten) zugunsten einer Förderung der breiten kommerziellen Nutzung der digitalen Signatur in der Schweiz?»** liefert das Kapitel 5. einen Überblick. Als wichtigste Optimierungs-massnahmen können folgende Handlungsempfehlungen festgehalten werden:

- Digitalisierung der User-Identifikation für die Ausstellung einer QES
- Angebotserweiterung QES inkl. smartem Bezug / Nutzung der User für alle Digital Signing Anbieter
- Angebotserweiterung cloudbasierte Digital Signing Lösung mit exklusiver Datenhaltung in der Schweiz und in Kombination mit Hash Signing (hybrider Ansatz (On Premise (Hash Signing-Komponente) / Cloud (Signierlösung beim Anbieter betrieben))
- Sicherstellung Geräteunabhängigkeit der Digital Signing Lösung
- Ermöglichung von Schnittstellen der Digital Signing Lösung in Drittapplikationen

6.2. Fazit Hauptteil II

Der Hauptteil II zeigte sich in vier Kapitel strukturiert. In Kapitel 3. wurde der Grundstein für die spätere Erhebung der Anforderungen von ausgewählten Vertretern von Schweizer Unternehmungen zugunsten einer breiten geschäftlichen Verwendung der digitalen Signatur gelegt. Dabei hatte sich das qualifizierte, semistrukturierte Interview als optimal erwiesen. In Kapitel 4. fand die eigentliche Erhebung und vor allem die Auswertung der Interviews statt. 197 Anforderungen zugunsten einer breiten geschäftlichen Verwendung der digitalen Signatur wurden auf 30 Codierungen (Anforderungen) zugeteilt, welche wiederum in sechs Kategorien zusammenfasst wurden. Die wichtigsten genannten Anforderungen betrafen ein schnelles, einfaches und

digitales User-Onboarding, Funktionen über die reine digitale Signatur hinaus wie z. B. individualisierbare Workflowkomponenten als auch Bedürfnisse nach einer cloudbasierten Signinglösung in Kombination mit Hash Signing und exklusiver Datenhaltung in der Schweiz. Ebenfalls zeigte sich ein starkes Bedürfnis nach der höchsten digitalen Signatur (QES). Eine ausführliche Zusammenfassung der wichtigsten genannten Anforderungen findet sich in Kapitel 4.7. Das Kapitel 5. identifizierte wichtige Anforderungen der Gesprächspartner, welche aus heutiger Perspektive nicht oder nur teilweise erfüllt werden können und sprach als Lösungsansatz verschiedene Handlungsempfehlungen aus. Die noch nicht digitalisierte User-Identifikation für die Ausstellung einer QES als auch der noch nicht bei allen Anbietern vorhandene hybride (Hash Signing Komponente On Premise, Signierlösung in der Cloud) Ansatz einer Digital Signing Lösung wurden dabei als grösste Schmerzenspunkte erkannt und mit Lösungen versehen. Mit dem Kapitel 6. und der Beantwortung der Forschungsfragen wurde der Hauptteil II abgeschlossen.

Der nachfolgende Schlussteil beendet die Masterarbeit mit einer kritischen Würdigung der Arbeit (Kapitel 7.1.) und einem Ausblick (Kapitel 7.2.).

SCHLUSSTEIL

7. Abschluss

7.1. Kritische Würdigung der Arbeit

Der theorielastige Hauptteil I wurde auf Basis strukturierter und umfangreicher Literaturrecherche erarbeitet. Schwergewichtig dienten dabei die gesetzlichen und regulatorischen Anforderungen in Form des Schweizerischen Obligationenrechtes, des ZertES, der VZertES und den TAV als Literaturquellen. Ausserhalb der gesetzlichen, regulatorischen Quellen fanden sich andere relevante Informationen, z. B. im Kontext zur geschäftlichen Verwendung von Digital Signing, vorwiegend auf Internetplattformen, was logisch begründbar ist, da die digitale Signatur ja gerade die Alternative zu Papierprozessen (und damit Literatur auf Papier) bilden möchte. Die kritische Qualitätsüberprüfung von diesen Internetartikeln wie auch auf eine transparente Quellenangabe zeigte sich in einigen Fällen als herausfordernd. Allgemein ist festzuhalten, dass das Thema Digitale Signatur und deren kommerzielle Nutzung (und Anforderungen), dediziert für den Schweizer Rechtsraum, noch nicht aktuell und ausführlich erforscht wurde und die hier vorliegende Masterarbeit einen wertvollen Beitrag stiften möchte. Trotzdem erwies sich die gründliche Literaturrecherche und Theorieerarbeitung im Hauptteil I als richtig und bildete die Vorbereitung für die empirische Forschung im Hauptteil II.

Die qualitativen Interviews zeigten sich zwar aufwändig in der Auswertung, erwiesen sich jedoch als die richtige Forschungsmethode zur Erhebung der geschäftlichen Anforderungen an Digital Signing. Die semistrukturierten Interviews erlaubten es sowohl den Fokus auf das Untersuchungsziel zu halten, allerdings aber auch den Gesprächspartnern eine Freiheit einzuräumen, die zu wertschöpfenden Gesprächsinhalten führte. Aufgrund der engen Zeitressourcen für diese Masterarbeit konnte nur eine limitierte Anzahl an Interviews geführt werden. Die daraus resultierten Erkenntnisse stellen damit kein wissenschaftlich repräsentatives Resultat dar. Zukünftige weiter darauf aufbauende Forschung kann das gewonnene Fazit auf eine Allgemeingültigkeit hin überprüfen und verfeinern. Innerhalb der fünf geführten qualitativen Interviews konnte eine Lernkurve des Interviewers erreicht werden: Das Führen der Interviews wurde gewohnter und dadurch intuitiver, was die Qualität der Gespräche und gewonnenen Erkenntnisse positiv förderte.

7.2. Zukünftige Forschung und Ausblick

Wie in den Untersuchungsgrenzen in Kapitel 3.4. erläutert, basierten die praxisbezogenen Erhebungen der Anforderungen für einen breiten geschäftlichen Einsatz der digitalen Signatur auf Interviews mit ausgewählten Personen. Eine wissenschaftliche Repräsentativität z. B. für Unternehmensgrössen- oder industrien ist damit nicht gegeben, stellt aber einen interessanten Auftrag für zukünftige Forschung dar.

Das im März 2021 vom Schweizer Stimmvolk abgelehnte E-ID Gesetz (Schweizerische Eidgenossenschaft, 2021) hätte hinsichtlich der innerhalb von Digital Signing erfolgskritischen Identifikationsbestätigung von Usern eine Optimierungsgrundlage darstellen können. Hätte sich eine sichere E-ID etabliert und eine starke Verbreitung gefunden, hätte ein Vorstoss zur Akzeptanz einer E-ID als Alternative zur (separaten) persönlichen, physischen User-Identifikation für die Beantragung einer qualifizierten elektronischen Signatur unternommen werden können. Ein User-Onboarding für eine qualifizierte elektronische Signatur hätte damit für Personen, welche bereits über eine genügende (Hinweis: es waren verschiedene Sicherheitslevels der E-ID vorgesehen) E-ID verfügt hätten, deutlich effizienter, digitaler und attraktiver gestaltet werden können, was die Skalierbarkeit von Digital Signing stark erhöht hätte. Es wird interessant zu beachten sein, wie sich die Thematik einer Schweizer E-ID in Zukunft weiterentwickeln wird und ob allenfalls ein weiterer politischer Vorstoss diesbezüglich unternommen wird.

Ebenfalls zugunsten einer Lockerung der persönlichen, physischen User-Identifikation für die Erlangung einer qualifizierten elektronischen Signatur (und damit einer Förderung der geschäftlichen Verwendung von Digital Signing) kann der Art. 7 Abs. 1 VZertES beitragen, welcher eine (digitale) Alternative zur persönlichen, physischen Identifikation erlaubt, sofern eine Konformitätsbewertungsstelle diese als gleich sicher bestätigt. Dazu sind insofern Aktivitäten im Gange, als dass derzeit die ETSI TS 119 461 Norm (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects) überarbeitet wird und künftig Spezifikationen einer genügend sicheren digitalen User-Identifikation ausweisen soll (ETSI, kein Datum). Sobald die Überarbeitung dieser Norm abgeschlossen und freigegeben ist, kann die Schweizerische Konformitätsbewertungsstelle (SAS Schweizerische Akkreditierungsstelle) diese als ebenbürtig zur persönlichen, physischen User-Identifikation anerkennen und entsprechend die TAV (Technische und Administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer

Anwendungen digitaler Zertifikate) anpassen. Da aber zum aktuellen Zeitpunkt die ETSI TS 119 461 Norm weiterhin erst in Überarbeitung ist, kann mit einer potenziellen Übernahme in die TAV und ersten Anwendungen dieser erleichterten User-Identifikation frühestens innerhalb 2022 gerechnet werden.

Weiter interessant zu beobachten sein wird, wie sich die künftige Entwicklung des Schweizerischen (ZertES) und des Europäischen (eIDAS) Signaturgesetzes gestalten wird. Ist es sinnvoll, in diesen eng miteinander verbundenen Wirtschaftsregionen weiterhin zwei verschiedene Gesetze für Digital Signing aufrecht zu erhalten oder findet künftig eine Annäherung oder gegenseitige Akzeptanz statt?

Im Rahmen der digitalen Transformation von Geschäftsprozessen wird Digital Signing mehr und mehr an Bedeutung gewinnen, um auch die «letzte Meile» der Unterschrift wertschöpfend zu digitalisieren. Entsprechend werden die im Ausblick skizzierten Themen (und weitere!) in den Fokus rücken und diskutiert werden.

Danksagungen

Ich möchte mich herzlich bei meinen Interviewpartnern bedanken, welche es mir durch die spannenden Gespräche ermöglichten, meine erarbeiteten Theorien mit der Praxis zu verknüpfen, zu testen und zu erweitern.

Ebenfalls gebührt meiner Masterarbeitsbetreuerin, Dr. Carmen Kobe, als auch dem Ko-Referenten, Reto Scagnetti, ein grosser Dank. Sie beide waren wichtige Ankerpunkte und Sparringpartner für diese Arbeit und unterstützten mich fachlich und persönlich.

Zu guter Letzt möchte ich auch meiner Frau und Familie danken, welche mir einmal mehr die Zeit und Geduld für diese Weiterbildung ermöglichten.

LITERATURVERZEICHNIS

1&1 IONOS SE. (28. Juli 2020). *Was ist eine Hashfunktion?* Von https://www.ionos.de/digitalguide/server/sicherheit/hashfunktion/ abgerufen

Appelfeller, W., & Feldmann, C. (2018). *Die digitale Transformation des Unternehmens.* Berlin: Springer-Gabler. doi:10.1007/978-3-662-54061-9

Baur, N., & Blasius, J. (2014). *Handbuch Methoden der empirischen Sozialforschung.* Wiesbaden: Springer Fachmedien Wiesbaden GmbH. doi:10.1007/978-3-531-18939-0

Bundesamt für Kommunikation BAKOM. (23. November 2016). *Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate*. Bern: Schweizerische Eidgenossenschaft.

Bundesamt für Kommunikation BAKOM. (02. April 2020). *Elektronische Signtaur*. Von https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2020). *BSI - Technische Richtlinie.* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesbehörden der Schweizerischen Eidgenossenschaft. (kein Datum). *Validator ist ein Service der Bundesverwaltung*. Von https://www.e-service.admin.ch/validator/upload/all/de abgerufen

Cloud Signature Consortium VZW. (kein Datum). *Protocols and API specifications*. Von https://cloudsignatureconsortium.org/resources/ abgerufen

Der Bundesrat. (13. Januar 2021). *Coronavirus: Bundesrat verlängert und verschärft Massnahmen*. Von https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-81967.html abgerufen

Die Bundesversammlung der Schweizerischen Eidgenossenschaft. (18. März 2016). *Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate*. Bern: Schweizerische Eidgenossenschaft.

Die Bundesversammlung der Schweizerischen Eidgenossenschaft. (01. Januar 2021). *Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)*. Bern: Schweizerische Eidgenossenschaft.

DocuSign Contributor. (26. Januar 2021). *Elektronische oder digitale Signatur?* Von https://www.docusign.de/blog/elektronische-oder-digitale-signatur abgerufen

ETSI. (kein Datum). *Specialist Task Force 588: Identiy Proofing for Trust Service Subjects*. Von https://portal.etsi.org/STF/STFs/STF-HomePages/STF588#who abgerufen

Europäisches Parlament. (2014). *Europäische Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93 EG*. Brüssel: Europäisches Parlament.

Feldbrügge, R., & Brecht-Hadraschek, B. (2008). *Prozessmanagement leicht gemacht* (2. Ausg.). München: Redline Wirtschaft, FinanzBuch Verlag GmbH.

Fitzer, K., & Kraul, T. (13. Juni 2019). Identifikationsmittel. *Der Rechtsrahmen von eIDAS und GWG - Rahmenbedingungen oder Hürdenlauf? bitkom eIDAS Summit*. London: Noerr Partnerschaftsgesellschaft mbB.

Freist, R. (06. August 2014). *Verschlüsselung - Was ist noch unknackbar?* Von https://www.pcwelt.de/ratgeber/Verschluesselung_-_Was_ist_noch_unknackbar_-Sicherheits-Check-8845011.html abgerufen

Hussy, W., Schreier, M., & Echterhoff, G. (2013). *Forschungsmethoden in Psychologie und Sozialwissenschaften.* Heidelberg: Springer-Verlag. doi:10.1007/978-3-642-34362-9

Jaeggi, A., & Bollhalder, R. (2019). *EY Legal News April 2019: Elektronische Signatur - ein Überblick.* Basel: Ernst & Young AG.

Kleinjohann, M., & Reinecke, V. (2020). *Marketingkommunikation mit der Generation Z.* Wiesbaden: Springer Gabler. doi:10.1007/978-3-658-30822-3

Kühn, P. (16. November 2016). *Die elektronische Unterschrift*. Von https://www.vischer.com/know-how/blog/die-elektronische-unterschrift-38340/#:~:text=Nach%20unserer%20Einsch%C3%A4tzung%20sind%20gem%C3%A4ss,herk%C3%B6mmlichem%20Weg%20(eigenh%C3%A4ndig)%20unterzeichnet abgerufen

Luber, S., & Schmitz, P. (20. März 2018). *Definition PKI: Was ist eine PKI (Public-Key-Infrastruktur)?* Von https://www.security-insider.de/was-ist-eine-pki-public-key-infrastruktur-a-696659/ abgerufen

Mayring, P. (2015). *Qualitative Inhaltsanalyse* (11. Ausg.). Weinheim: Beltz.

Paar, C., & Pelzl, J. (2016). *Kryptografie verständlich.* Berlin Heidelberg: Springer Vieweg. doi:10.1007/978-3-662-49297-0

QuoVadis Trustlink Schweiz AG (intern). (kein Datum).

QuoVadis Trustlink Schweiz AG. (kein Datum). *Alle Dokumente bereits digital – aber für die Unterschrift brauchen Sie noch Papier?* Von https://signing.quovadisglobal.ch/ abgerufen

Red Hat Limited. (kein Datum). *Was ist eine REST-API und was ist REST (Representational State Transfer)?* Von https://www.redhat.com/de/topics/api/what-is-a-rest-api abgerufen

Redaktion ComputerWeekly.de. (April 2020). *Strukturierte Daten*. Von https://whatis.techtarget.com/de/definition/Strukturierte-Daten abgerufen

Rieber, D. (2017). *Mobile Marketing.* Wiesbaden: Springer Fachmedien Wiesbaden GmbH. doi:10.1007/978-3-658-14777-8

Rusnjak, A., & Schallmo, D. (2018). *Customer Experience im Zeitalter des Kunden.* Wiesbaden: Springer Gabler. doi:10.1007/978-3-658-18961-7

Schneeberger, D. (24. September 2018). *Hürden für die digitale Unterschrift abbauen*. Von https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183814 abgerufen

Schweizerische Akkreditierungsstelle SAS. (4. März 2021). *Public Key Infrastructure (PKI)*. Von https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki1.html abgerufen

Schweizerische Bundesrat. (23. November 2016). *Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate*. Bern : Schweizerische Eidgenossenschaft.

Schweizerische Eidgenossenschaft. (2021). Volksabstimmung 07. März 2021. *Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz)*. Bern: Schweizerische Eidgenossenschaft.

U.S. Government. (30. Juni 2000). *Electronic Signatures in Global and National Commerce Act*. USA: U.S. Government.

Verbi GmbH. (kein Datum). *Was ist MAXQDA?* Von https://www.maxqda.de/was-ist-maxqda abgerufen

ANHANG

Anhang A: Interviewleitfaden

Gedankenstützen für eine erfolgreiche Interviewführung

- Offene Fragen stellen, wenn immer möglich ungestützt
- Wenn das Gespräch nicht so läuft, ankurbeln:
    - Erzählen Sie doch mal…
    - Können Sie sich an eine typische Situation erinnern wo…
    - Können Sie das genauer beschreiben?
    - Inwiefern spielt dabei auch eine Rolle, dass…
- Dem Interviewpartner die grösste Sprechzeit lassen
- Keine Wertung vom Interviewer

Formales vor Start der Fragenstellungen: Setup

- Erläuterung Thema und Ziel des Interviews / Kontext zur Masterarbeit
- Zeitdauer bekannt geben (30 – 60 Minuten)
- Anonymisierung (Personen und Unternehmen) für Verschriftlichung bestätigen
- Hinweis und Zustimmung auf Gesprächsaufnahme abholen

Formales vor Start der Fragestellungen: Smalltalk zum Warmwerden / Fakten Interviewpartner abholen

- Smalltalk: Aktuelle Geschäftslage usw.
- Fakten Interviewpartner:
    - Unternehmung
    - Anzahl Mitarbeiter
    - Geschäftstätigkeit Schweiz
    - Funktion
    - Alter
    - Potenzieller Anwender und/oder Entscheider?
    - Bisheriger Erfahrungsgrad Digital Signing
    - Unterzeichnungs-Use-Cases

Zuallererst ungestützte Hauptfrage

Welche Anforderungen stellen Sie an eine digitale Signierlösung, sodass Sie die digitale Signatur im Geschäftsalltag vorteilhaft und breit einsetzen können/wollen und eine Investition darin befürworten?

Danach Vertiefungsfragen je Kategorie.

Interviewhauptfrage nach Wirkung/Anforderungen auf Geschäftsprozesse

Für Gesprächspartner ohne aktuellen Einsatz von Digital Signing:
Was für eine Wirkung auf Ihre aktuellen Geschäftsprozesse erwarten Sie bei einer allfälligen Einführung von Digital Signing? Was würden Sie erwarten / fordern?

Für Gesprächspartner welche Digital Signing bereits im Einsatz haben:
Wie hat sich die Einführung von Digital Signing auf Ihre Geschäftsprozesse ausgewirkt? Inwiefern konnten Ihre Anforderungen erfüllt / nicht erfüllt werden?

Interviewhauptfrage nach Wirkung/Anforderungen auf Zielgruppen

Für Gesprächspartner ohne aktuellen Einsatz von Digital Signing:
Wie beurteilen Sie eine allfällige Einführung von Digital Signing auf Ihre Bestands- und Neukunden? Was sind Ihre Anforderungen bei einer Einführung von Digital Signing in Bezug auf Ihre Kundenbasis und Verkaufsabschlüsse?

Für Gesprächspartner welche Digital Signing bereits im Einsatz haben:
Wie hat sich die Einführung von Digital Signing auf Ihre Kundenbasis (Bestands- und Neukunden) sowie Verkaufserlöse ausgewirkt? Inwiefern konnten Ihre Anforderungen erfüllt / nicht erfüllt werden?

Interviewhauptfrage nach Wichtigkeit / Relevanz Sicherheitsaspekte

Für Gesprächspartner ohne aktuellen Einsatz von Digital Signing:
Wie wichtig sind für Sie Sicherheitsaspekte rund um eine einzuführende Digital Signing Lösung? An was genau denken Sie da?

Für Gesprächspartner welche Digital Signing bereits im Einsatz haben: *Wie wichtig waren für Sie Sicherheitsaspekte bei der Einführung von Digital Signing? Wie zeigten sich diese Anforderungen dann in der Praxis?*

Interviewhauptfrage nach Anforderungen zum User-Onboarding

Für Gesprächspartner ohne aktuellen Einsatz von Digital Signing: *Wenn Sie daran denken, eine Digital Signing Lösung auf Ihre Mitarbeiter oder auch externe Unterzeichner auszurollen, was ist Ihnen dabei wichtig?*

Für Gesprächspartner welche Digital Signing bereits im Einsatz haben: *Kommen wir zur User-Ausrollung/Befähigung. Was ist Ihnen dabei wichtig und inwiefern konnten Ihre Anforderungen mit der eingesetzten Lösung erfüllt werden?*

Interviewhauptfrage nach Funktionsumfang der Digital Signing Lösung

Kommen wir zum Abschluss ein wenig auf den Funktionsumfang einer Digital Signing Lösung zu sprechen. Also weg von der Frage, welche Art von digitaler Signatur eingesetzt wird, sondern vielmehr WIE Sie sie im Geschäftsalltag wertschöpfend verwenden können. Was für Anforderungen haben Sie hierzu?

Anhang B: Interviewtranskriptionen

Interview mit Gesprächspartner GP-1 am 23.04.2021, 09.00 – 10.00 Uhr

M. Sieber: Wie ich dich ja informiert habe, möchten wir heute darüber sprechen, was du selbst für Anforderungen an Digital Signing in der Nutzung im Geschäftsalltag stellst. Damit wir zuerst auch noch einen besseren Bezug zu eurer Unternehmung erhalten: Ihr habt ja Digital Signing bereits im Einsatz. Kannst du mir kurz ein wenig beschreiben, für welche Use-Cases ihr dies anwendet?
GP-1: Jedes Dokument, welches die Unternehmung verlässt, muss seit 1.5 Jahren digital unterschrieben werden. Von einfachen Offerten für eine Wirtschaftsprüfung bis zu Verträgen und Berichten muss alles zweifach digital von uns unterschrieben werden.

M. Sieber: Das heisst ihr habt gar keine Dokumente mehr, die von Hand unterzeichnet rausgehen?
GP-1: Ich würde jetzt lügen, wenn ich sage «ja das stimmt». Es gibt sicher den einen oder anderen, der sich nicht an diese Abmachung hält. [...] Es gibt sicher die einen oder anderen, welche vielleicht auch etwas älter sind und finden, sie kämen hier nicht draus und dann von Hand unterschreiben. Aber es gibt eine Weisung, von dem her gesehen dürfte man eigentlich nicht [von Hand unterschreiben].

M. Sieber: Als ihr Digital Signing eingeführt habt, habt ihr euch sicher Gedanken gemacht und habt Anforderungen und Erwartungen gehabt, wie sich eure Geschäftsprozesse damit entwickeln werden. Was sind das für Anforderungen gewesen?
GP-1: Das ist eingeführt worden, bevor ich in die Unternehmung gekommen bin. Dementsprechend war ich bei dieser Projekteinführung nicht dabei und kann dir darauf keine Antwort geben. [...]

M. Sieber: Anders gefragt, wenn ihr jetzt noch kein Digital Signing hättet und du würdest es jetzt einführen, was wären dann für dich wichtige Anforderungen die du an die Entwicklung deiner Geschäftsprozesse stellen würdest?
GP-1: Gute Frage. Was wir uns erhoffen würden wäre sicher eine Nachverfolgbarkeit, sprich wir haben alle diese Dokumente danach [nach dem Digital Signing] alle digital abgelegt. Auf der anderen Seite sicher die Geschwindigkeit. Sprich du unterschreibst das Dokument, versendest oder legst es ab und musst es nicht via interner Post von

Niederlassung A nach Niederlassung B senden. [...] Plus was ich super finde, ich kann jederzeit nachvollziehen, wer hat wann was unterschrieben. Das ist sicher ein Mehrwert.

M. Sieber: Du hast jetzt die Kosten nicht genannt. Ist das für dich ein Punkt, wo du sagst, müsste ja logischerweise günstiger sein als der analoge Prozess?
GP-1: Klar ja, würde ich auch so sehen. Die Kosten sind nun für mich nicht gerade im Vordergrund gestanden, aber logisch, du bist natürlich effizienter und schneller. Und die Kosten, die wir bezahlen pro Mitarbeiter sind natürlich logischerweise in keinem Verhältnis zur internen Post oder vielleicht von Niederlassung zu Niederlassung via Schweizerische Post das Dokument physisch zu verschicken. Wenn ich mal die Kosten aufrechnen würde, ist es [Digital Signing] definitiv effizienter und günstiger.

M. Sieber: Gut, das ist interessant. Wenn wir nun mal ein wenig eure Kunden und Partner anschauen, mit welchen ihr Geschäfte betreibt. Die sind ja auch betroffen, wenn ihr Dokumente nicht mehr analog, sondern digital unterschreibt. Was hast du dir gedacht, wie die darauf reagieren? Oder habt ihr das mal auf der Seite gelassen und euch zuerst nur auf euch konzentriert?
GP-1: In erster Linie haben wir ganz klar für uns geschaut. Wir haben vor dreieinhalb Jahren das digitale Kundenportal eingeführt, das heisst wir arbeiten mit unseren Kunden, das sind rund 25'000, nur noch digital zusammen. [...] Wir haben eigentlich auch nie ein schlechtes Feedback vom Kunden erhalten, dass er jetzt gegen die digitale Unterschrift wäre oder das nicht verstehen würde. Insofern haben wir hierzu nur positive Erfahrungen gemacht, aber haben ganz klar in erster Linie auf uns geschaut.

M. Sieber: Hattest du auch den Eindruck, dass gewisse Kunden die digitale Unterschrift fast schon von euch erwartet haben?
GP-1: Dannzumal wo wir das eingeführt haben [vor dreieinhalb Jahren], glaube ich, war das noch nicht im Fokus. Aber heute würde ich ganz klar sagen, wir haben gewisse Vorgaben und Richtlinien von der Revisionsaufsichtsbehörde und auch grossen Kunden, die das von uns erwarten. Heute ist die Erwartung [der Kunden] ganz anders, als wo wir es eingeführt hatten.

M. Sieber: Andersherum gefragt: hast du das Gefühl, dass du aufgrund der digitalen Signatur als Unternehmen mit Kunden zusammenarbeiten kannst, mit welchen ansonsten, wenn ihr noch mit der analogen Unterschrift arbeiten würdet, keine Zusammenarbeit möglich wäre?
GP-1: Könnte ich mir gut vorstellen, vor allem bei grossen internationalen Firmen ist es sicher eher ein Thema. Wir haben aber auch kleine Kunden / KMU's, die in der Digitalisierung noch gar nirgends sind. Wir bekommen immer noch regelmässig [von diesen kleinen Firmen / KMUs] Schuhschachteln mit Belegen zugesendet, die wir danach digitalisieren. [...] Aber wir haben grosse internationale Kunden, wo wir durch das [Digital Signing] sicher einen Vorteil haben, weil wir ganz klar sagen können, wir können digital zusammenarbeiten, inklusive der gesamten digitalen Signierung. Von dem her gesehen gibt es den einen oder anderen Fall, welchen wir dadurch gewonnen hatten.

M. Sieber: Spannend. Wenn wir jetzt etwas auf die Sicherheitsaspekte zu sprechen kommen: Wie wichtig sind dir diese bei einer Digital Signing Lösung und an was denkst du im Speziellen?
GP-1: Wie du weisst, haben wir ein ganzes Security Team, welches sich um solche Themen kümmert. Die hatten dies [Digital Signing] dazumal auch eingeführt, entsprechend kann ich dir darauf fast keine Antwort geben. Für mich persönlich ist es sicher wichtig, dass die Zertifikate sicher validiert sind. Aber ich hätte jetzt nicht den Fokus auf Security gesetzt.

M. Sieber: Vielleicht auch ein wenig aufgrund deiner Funktion [bzw. weil es andere Funktionen gibt, die sich darum zu kümmern haben]?
GP-1: Genau. Ist für mich nicht Daily-Business.

M. Sieber: Ok. Wie du weisst, gibt es in der Schweiz einzig nur die qualifizierte elektronische Signatur, welche gesetzlich auch der Handunterschrift gleichgestellt ist. Das ist auch jene, die ihr im Rahmen eurer eingesetzten Digital Signing Lösung nutzt. Wie wichtig ist das für euch, dass es rechtverbindlich ist?
GP-1: Sicher sehr sehr wichtig. Wir haben mit sehr sensitiven Daten von unseren Kunden zu tun. […] Von dem her gesehen ist das für uns das A und O. Es kann nicht einfach irgendein Produkt sein, welches wir einsetzen. […] Nur schon von den Vorgaben der Finma Gesetzgebung und vom Geldwäschereigesetz her, dürfen wir nur qualifizierte, zertifizierte Lösungen einsetzen. Wir würden uns dadurch [mit einer nicht

qualifizierten elektronischen Signatur) auch unglaubwürdig machen und hätten auch rechtliche Probleme.

M. Sieber: Wahrscheinlich auch ein Imageproblem, oder?
GP-1: Genau. […] Wir sind dabei, mit Microsoft Schweiz die ganzen Cloudthematiken anzuschauen. Und dort musst du eine Bewilligung von der Revisionsaufsichtsbehörde haben, dass du die Daten nicht mehr selbst in deiner eigenen Infrastruktur hast. […] Ein Imageschaden wäre natürlich verheerend.

M. Sieber: Du hast gerade einen spannenden Punkt angesprochen, nämlich Datenspeicherung. Was ist euch dabei wichtig?
GP-1: Die Datenhaltung muss in der Schweiz sein. Es muss eine gewisse Security-Zertifizierung haben. […] Wir haben ein gesamtes Team, welches sich um Datenschutz kümmert, weil wir dort auch eine gewisse Vorbildfunktion gegenüber den Kunden haben. Von dem her gesehen ist es ein sehr interessantes Thema, das auch immer je mehr Stellenwert haben wird.

M. Sieber: Kann ich im Umkehrschluss daraus entnehmen, dass ihr immer eine Datenhoheit bei euch präferiert, quasi On Premise?
GP-1: In der Vergangenheit war das so. […] Unsere Geschäftsleitung hat aber vor einigen Wochen beschlossen, dass das nächste Rechencenter nicht mehr von uns betrieben wird. Sprich wir sind dabei, alle unsere Prozesse und Software cloudfähig zu machen. […] Wir haben beschlossen, dass wir Ende 2022, spätestens 2023, wann unser heutiges Rechencenter end of life ist, wir möglichst vielen Daten nicht mehr selber On Premise haben möchten.

M. Sieber: Wahrscheinlich auch aus Investitions- und Betreuungsgründen?
GP-1: Logisch. Das sind mehrere Millionen, die du damit [On Premise] investierst. Klar du investierst es dann einfach anders, vielleicht etwas günstiger. […]

M. Sieber: Dann ist eigentlich Hash Signing, was ihr bereits einsetzt, genau das Richtige? Einerseits betreibt ihr die Signing Lösung damit nicht bei euch On Premise, andererseits erhält der Signing-Anbieter aber auch kein Dokument von euch.
GP-1: Für uns sehr wertvoll. […]

M. Sieber: Gut. Lass uns ein wenig auf das Thema User-Onboarding kommen. Wie wichtig ist dir das und was sind aus deiner Sicht Anforderungen dazu damit du Digital Signing im Geschäftsalltag wertvoll einsetzen kannst?
GP-1: So wir es heute haben [LRA Delegation] ist es für uns gut. Es ist bei uns ein HR-Prozess, d.h. wenn ein Mitarbeiter eintritt, wird anhand seiner Daten der Prozess gestartet [persönliche face-to-face Identifikation]. […] Das von euch [QuoVadis, Signaturanbieter] zur Verfügung gestellte Formular [Antragsformular für eine qualifizierte elektronische Signatur] mit der Kopie der Identitätskarte wird euch danach zugestellt, wonach wir innerhalb von kürzester Zeit die Zertifikate von euch ausgestellt erhalten. […]

M. Sieber: Du sprichst einen wichtigen Punkt an. Ihr habt die qualifizierte elektronische Signatur im Einsatz, wo die Regularien eine face-to-face Useridentifikation von erlaubten Stellen verlangen. In eurem Fall haben wir das mittels LRA-Delegation an euch ausgelagert, sodass das HR bei euch dies selbst machen kann. Das funktioniert ja, wie von dir beschrieben, für eure eigenen Mitarbeiter gut. Habt ihr auch Fälle, wo ihr von einer externen Vertragspartei eine qualifizierte Signatur einfordert? Dieser müsste sich ja dann auch bei einer erlaubten Stelle face-to-face identifizieren lassen.
GP-1: Bei uns haben wir den Fokus ganz klar auf die Dokumente gelegt, welche die Unternehmung von uns verlassen, die müssen so [digital signiert] sein. Wir lassen immer noch zu, dass eine Offerte von einem Lieferanten nicht digital unterschrieben ist, aber die Offertzusage von unserer Seite muss dann digital unterschrieben sein. Wir haben noch nie solche gehabt, welche die digitale Unterschrift nicht akzeptiert haben. Wir haben sogar schon welche gehabt, welche gesagt haben «hey cool, wie habt ihr das gemacht?» und nachgefragt haben, mit welcher Lösung wir das gemacht haben. Von daher ist der Schweizer Markt auch im Wandel und es wird immer mehr digital unterschrieben.

M. Sieber: Du würdest mir aber zustimmen, dass wenn sich der Umstand ändert, sodass User für eine qualifizierte elektronische Signatur auch automatisierter und digitalisierter geonboardet werden können, dies sehr wertvoll für euch und eure Gegenüber (externe Vertragsparteien) wäre?
GP-1: Sehr sehr wertvoll, definitiv.

M. Sieber: Wenn wir gerade beim Thema User-Onboarding bleiben. Inwiefern ist für dich die Vorlaufzeit wichtig?
GP-1: […] Bis jetzt war es so, dass wir dies jeweils innerhalb von ein paar Tagen [nach Versand Antragsformulare an Signaturlieferant] erhalten haben. […] Meistens hängt es bei den Antragsstellern als beim Zertifikatslieferant. […]

M. Sieber: Auch dort hättest du ja wieder einen Beschleunigungsfaktor, wenn die User-Identifikation und Befähigung digital passieren könnte.
GP-1: Genau. Das passiert heute ja schon bei gewissen Banken, wo du alles in einem vorgelagerten Prozess schon hochladen kannst, deine ID und ein Foto via Webcam. Das gibt es ja alles schon und da wäre ich definitiv Freund davon [wenn diese digitalisierte User-Identifikationsmethode für die Ausstellung einer qualifizierten elektronischen Unterschrift auch für Nicht-Finanzintermediäre erlaubt wäre].

M. Sieber: Wenn wir an die Anforderungen an die IT-Infrastruktur im Rahmen der Einführung von Digital Signing denken, was ist euch dabei wichtig?
GP-1: Gute Frage. Da bin ich recht weit weg. Sicher ist das Thema heute Security, Mehrfachauthentifizierung, ist sie [die Lösung] cloudfähig, wie wird sie betrieben, was für Datenbanken braucht es im Hintergrund ist so, was mir spontan in den Sinn kommt. […]

M. Sieber: Wir haben nun viel darüber gesprochen, welche Art von digitaler Signatur eingesetzt werden soll. Mich interessiert nun auch, *wie* sie deiner Ansicht nach eingesetzt werden soll. Es gibt verschiedene Lösungen mit verschiedenen Funktionsumfängen. Was ist dir dabei für eine breite Einsetzung im Geschäftsalltag wichtig?
GP-1: So wie wir es heute haben [Digitale Signierung direkt aus dem Acrobat Reader, keine Workflowkomponenten]. […] Wir haben eine Vorgabe, die für uns wichtig ist: und zwar die Grösse der Unterschrift. In Adobe kannst du die Grösse der Unterschrift frei definieren. Wir haben Vorgaben bei gewissen Berichten, vor allem Abschlussberichte bei ausserordentlichen oder eingeschränkten Revisionen, wo die Unterschrift eine gewisse Grösse haben muss. Sprich wo im Template, wo wir die Berichte erstellen, eine gewisse Grösse der Unterschrift nicht überschritten werden darf. […] Das ist sicher für uns bei solchen Berichten wichtig, sodass unsere Mitarbeiter dafür mit einem zweiten Produkt, dem Localsigner [weil dies bei der anderen Lösung nicht als unabänderbare Vorlage eingestellt werden kann] unterschreiben. Die beiden Unterschriften sind dann nicht nur gleich gross, sondern sind dann auch schön auf der

gleichen Höhe. […] Das ist einfach ein Feld, welches klar definiert ist und welches auf unser Template für diese Berichte passt.

M. Sieber: Mit der aktuell eingesetzten Lösung müsst ihr ja Dokumente manuell per E-Mail an die nächste Partei versenden, die ebenfalls signieren soll. Dazu gibt es heute auch Lösungen, wo ihr dies direkt alles aus einem Guss und Tool heraus machen könntet. Dann kannst du z. B. direkt innerhalb des Signierworkflows die gewünschten Signierparteien einladen. Ist das etwas, wozu ihr euch auch schon Gedanken macht?
GP-1: Das ist jetzt ein grosser Zufall. Wir haben genau gestern darüber gesprochen. Die Lösung des anderen Anbieters, Localsigner, die ist end of life und wird nicht mehr weiterentwickelt. Und jetzt sind wir auf der Suche nach einer alternativen Lösung. […] Der Projektleiter wird auf dich zukommen, ob du dazu Wissen hast und uns helfen kannst. Und auch andere Lösungen, die du noch im Portfolio hast, auch mit uns anschaust.

M. Sieber: Ich entnehme daraus, dass für euch mittlerweile nach ein paar Jahren Erfahrung mit Digital Signing die Anforderungen auch steigen. Im Sinne von «die Unterschrift ist das eine», aber das Wie rundherum wird auch immer wichtiger. Also eben dass ihr sehr effizient digital signierte Dokumente weiterleiten könnt, dass ihr z. B. Reminderfunktionen nutzen könnt, falls eine Unterzeichnungspartei nicht rechtzeitig signiert. Das ist für euch mittlerweile also auch wichtig?
GP-1: Genau. Das ist definitiv etwas, das kommt. […] Das müssen wir anschauen.

M. Sieber: Wie wichtig ist für dich die Geräteunabhängigkeit? Also dass die digitale Signierlösung sowohl auf Desktop, Mobile und auch betriebssystem-unabhängig läuft?
GP-1: Ist ein Thema, dass immer wieder kommt und dass wir anschauen müssen. […] Mit all diesen Cloud-Themen, mit Office365 welches wir einführen werden, tritt natürlich der Mobile-Aspekt immer mehr in den Mittelpunkt.

M. Sieber: Inwiefern ist es für euch ein Thema, die Signinglösung auch an andere Applikationen anzubinden?
GP-1: Guter Aspekt. […] In der Vergangenheit war immer die Anforderung, der Bericht muss immer schön unterschrieben sein und immer gleich gross. Mit der Zeit kommen immer je mehr Anforderungen dazu. Jetzt ist wohl der Zeitpunkt gekommen, mal eine

Auslegeordnung zu machen, welche Anforderungen haben wir und welche Produkte gibt es auf dem Markt, die uns dabei helfen könnten.

M. Sieber: Wir kommen langsam zum Schluss. Gibt es weitere Bedürfnisse und Erwartungen, die wir bis anhin nicht thematisiert haben, die für dich wichtig für einen erfolgreichen geschäftlichen Einsatz von Digital Signing sind?
GP-1: Ich glaube die Lösung, die wir heute haben, genügt zumindest meinen Anforderungen. […] Es wird jetzt sicher in diesem Projekt [end of life der zweiten eingesetzten Signing Lösung (LocalSigner)] eine gewisse Umfrage geben. Wir müssen natürlich unsere internen Kunden fragen, was ihnen heute fehlt, sodass wir nicht einfach einen 1:1 Ersatz machen, sondern ein wenig über den Tellerrand hinausdenken. […]

M. Sieber: Noch eine letzte Frage. Wenn du an den Einsatz der digitalen Signatur denkst, was ist der grösste «Painpoint» dabei?
GP-1: Wenn ich mein Passwort vom Zertifikat vergesse. Wir haben eine Policy bei uns, dass wir alle 180 Tage das Passwort wechseln müssen und dass dieses eine gewisse Anzahl Zeichen haben muss, weil wir mit sensitiven Daten unterwegs sind. Und dann vergisst man manchmal das Zertifikatspasswort auch zu wechseln. Und in meiner bescheidenen Welt wäre es cool, dass wenn ich das AD-Passwort wechsle, es mein Passwort vom Zertifikat ebenfalls gleich auch wechseln würde. Ich weiss aber, dass dies technisch nicht geht – es ist eher ein User-Problem. […]

M. Sieber: Du meinst Single Sign On im Rahmen der Signaturlösung?
GP-1: Genau.

Interview mit Gesprächspartner GP-2 am 29.04.2021, 08.00 – 09.00 Uhr

M. Sieber: Wie vorinformiert, werden wir heute über deine Anforderungen sprechen, wenn du Digital Signing in deinem Geschäftsalltag verwendest. Am Anfang möchte ich ein bisschen auf eure Unternehmensausgangslage eingehen. Du hast mir im Vorfeld gesagt, dass du bereits regelmässig geschäftlich Dokumente digital signierst. Das ist richtig, oder?
GP-2: Das ist korrekt, ja.

M. Sieber: Kannst du bitte den Use-Case ein wenig skizzieren, in welchem Kontext du Dokumente digital signierst und in welcher Häufigkeit?
GP-2: Es gibt eigentlich zwei Hauptthemen, wo ich die digitale Unterschrift verwende. Das erste ist der Kreditorenworkflow. […] Bis vor der Corona Zeit musste ich Rechnungen immer noch physisch visieren. Dann haben wir das physisch in die interne Post gegeben und so an die Buchhaltung versendet. Mit der Corona Zeit sind wir immerhin so weit gekommen, dass wir auf PDF-Rechnungen eine digitale Unterschrift setzen dürfen. […] Und das zweite Thema sind bei mir Vertragsdokumente oder Vereinbarungen, beispielsweise mit dem Hersteller in Tschechien oder Händlern in der Schweiz, welche wir seit letztem Jahr mit einer physischen Unterschrift [Scan] und einem Adobe Zertifikat digital visieren.

M. Sieber: Ganz allgemein gesehen, was stellst du für Anforderungen an eine digitale Signierlösung, sodass du diese im Geschäftsalltag vorteilhaft nutzen und breit einsetzen kannst?
GP-2: Für mich ist wichtig, dass sie schnell funktioniert. Wenn ich z. B. eine Rechnung kontiere, möchte ich nicht mehr als 30 Sekunden investieren. Das ist z. B. heute ein Thema, dass wenn ich mit Adobe signiere, dies in meinem Verständnis immer noch etwas zu mühsam ist. […] Und logischerweise möchte ich nicht, dass jemand anders für mich unterschreiben kann. Da haben wir heute hie und da ein Thema bei Fällen, wo ich meine Unterschrift eingescannt hatte, z. B. bei Massenversänden von Briefen. […] Und nun lese ich immer wieder von Rundschreiben an Händler, wo ich mitunterschrieben haben soll, aber vorab dazu gar nie die Freigabe erteilt habe.

M. Sieber: Also die haben deine Unterschrift ohne dein Wissen einfach wiederverwendet?
GP-2: Genau. Das ist zwar entgegen internen Richtlinien, […] aber das verselbständigt sich dann einfach.

M. Sieber: Hast du noch andere spontane Anforderungen, bevor wir weiter ins Detail gehen?
GP-2: […] Idealerweise könnte das Zertifikat oder meine Signatur jeder lesen, unabhängig von seinem Gerät. Also nicht, dass dann einer sagt, er könne das nicht lesen, weil er nicht das entsprechende Programm installiert hat.

M. Sieber: Spannend. Danke mal für deine ersten spontanen Anforderungen, die du genannt hast. Ich möchte nun gerne über bestimmte Bereiche noch etwas detaillierter sprechen. Der erste Bereich wäre Geschäftsprozesse. Du hat schon den Faktor Zeit respektive Schnelligkeit als Anforderung beim geschäftlichen Verwenden der digitalen Signatur genannt. Du hast nichts zu den Kosten genannt. Weshalb ist das für dich nicht entscheidend?
GP-2: Weil ich mit den Kosten bei uns nichts zu tun habe. Die IT ist bei uns der Gatekeeper und entscheidet, welche Prozesse und Systemlandschaft implementiert wird. Wir als User abonnieren nur ein zur Verfügung gestelltes System. Bei uns ist das hierfür der Adobe Acrobat Reader DC [Document Cloud]. Ich weiss ehrlich gesagt nicht, was ich für diese Nutzung monatlich an Lizenzgebühren zahlen muss.

M. Sieber: Andersherum gefragt: Was wäre für dich ein fairer Preis für die Nutzung einer digitalen Signatur?
GP-2: Wenn ich es richtig im Kopf habe, haben wir viele Systeme, jetzt nicht explizit auf die digitale Signatur bezogen, wo wir zwischen 5-10 Franken pro Monat und User zahlen. Und das sind dann auch Systeme, die man stundenlang pro Tag verwendet. In meinem Verständnis dürfte dann nur eine digitale Signatur nicht teurer sein. Jetzt habe ich im Übrigen die Kosten gerade gefunden: für mich kostet der Adobe Acrobat DC pro Monat 17 Franken. […]

M. Sieber: Sind für dich auch nachgelagerte Geschäftsprozesse ein wichtiges Thema? Also strukturierte Daten, sodass du mit der digitalen Signatur ein komplett digitales Dokument hast, welches du im Nachgang damit auch komplett digital auswerten und durchsuchen könntest. Ist das etwas was für dich wichtig ist oder mehr nice-to-have?
GP-2: Ist für mich persönlich im heutigen Kontext gar nicht relevant. Ich kann mir aber vorstellen, dass dies z. B. für die Personen in der Buchhaltung relevant sein könnte. Ich visiere zwar das PDF digital, sie können dies dann aber doch wieder nicht automatisiert auslesen, weil ich mir gut vorstellen kann, dass sie es zuerst dann wieder ausdrucken. […] Also ich habe die Vorteile mit dem digitalen Signieren, aber hinten

heraus ist der Prozess bei uns noch überhaupt nicht zu Ende gedacht. Und auf die Verträge bezogen, die wir [via Handunterschrift] unterschreiben: wir haben die meisten als nicht visiertes PDF abgelegt, ich suche dann jeweils dort nach Stichworten oder Formulierungen. Wenn ich ein Dokument hätte, das einerseits digital unterschrieben ist und andererseits die [digitale] Suche zulässt, dann umso besser.

M. Sieber: Das heisst ihr müsst heute beides noch ablegen? Also einerseits die nicht visierte elektronische Form, andererseits der unterschriebene Vertrag in Papierform?
GP-2: Nicht unbedingt in Papierform. Dort sind wir so weit gegangen, dass wenn wir den Vertrag von Hand unterschreiben, dann haben wir ihn einfach eingescannt und das physische Dokument entsorgt. Aber wenn ich dann im Laufwerk bin, habe ich dann meistens zwei Dateien, also 1x visiert und 1x nicht visiert.

M. Sieber: Kommen wir auf eure externen Anspruchsgruppen, wie z. B. Partner und Kunden zu sprechen. Die könnten auch betroffen sein, wenn ihr digital anstelle von Hand Dokumente unterzeichnet. Gibt es dazu Anwendungsfälle bei euch?
GP-2: Sicher mit dem Lieferanten. Mit denen sind wir so weit, dass wir Verträge oder Bonusvereinbarungen digital unterschreiben, d.h. ihnen so digital visiert senden und sie es dann wiederum auch digital gegenzeichnen.

M. Sieber: Hast du das Gefühl, dass sich durch die Nutzung von Digital Signing etwas in der Beziehung zu diesen externen Anspruchsgruppen verändert hat?
GP-2: Es geht halt alles schneller. Das ist aber nicht unbedingt eine Verhaltensänderung, sondern mehr, dass sich der Prozess verändert hat. […]

M. Sieber: Denkst du, dass externe Anspruchsgruppen die digitale Signatur gar fast schon von euch erwarten?
GP-2: Das Werk [Lieferant] mittlerweile ja. […] Wer aber gar keine digitalen Unterschriften verwendet sind unsere Garagisten, wenn sie mit uns als Importeur arbeiten. Dort sind wir schon froh, wenn sie es schaffen, ein Dokument einzuscannen. Dort machen wir eigentlich noch fast alles physisch per Post, mit Blut und Schweiss unterschrieben. Wer aber sicher immer mehr nachfragt, um Dokumente digital zu unterschreiben, sind die Endkunden, die beim Garagisten ein Auto kaufen.

M. Sieber: Thema Sicherheitsanforderungen: Du hast eingangs erwähnt, dass du sicherstellen willst, dass keine andere Person für dich signieren kann. Gibt es noch andere Sicherheitsaspekte, welche dir bei der Nutzung der digitalen Signatur wichtig sind?
GP-2: Ich gehe auch davon aus, dass das Dokument nachträglich nicht mehr veränderbar ist. Das würde ich voraussetzen.

M. Sieber: Ein viel diskutiertes Thema ist immer die Rechtsverbindlichkeit einer digitalen Signatur. Weisst du hierzu schon etwas darüber, wie sich dies in der Schweiz darstellt?
GP-2: Ehrlicherweise habe ich zu wenig Wissen diesbezüglich. Ich wüsste nicht, wie so ein digital signiertes Dokument vor Gericht standhalten würde.

M. Sieber: In der Schweiz ist einzig die sogenannte qualifizierte elektronische Signatur gesetzlich der Handunterschrift gleichgestellt. Einerseits muss diese von einem akkreditierten Anbieter kommen, andererseits muss der User vorab einmalig persönlich, face-to-face, von einer erlaubten Stelle identifiziert worden sein. Ist diese Rechtsverbindlichkeit für euch wichtig?
GP-2: Ich glaube es war bis anhin noch kein Thema, weil wir keinen konkreten Fall hatten, welcher in einer Gerichtsverhandlung geendet ist. Darum war es zumindest mir nicht bekannt. Wenn ich dich richtig verstehe, ist z. B. die Lösung, welche wir nutzen, nicht qualifiziert und rechtssicher?

M. Sieber: Richtig.

M. Sieber: Nehmen wir an, du würdest künftig mit einem akkreditieren Anbieter von digitalen Signaturen zusammenarbeiten, um eben auch die qualifizierte elektronische Signatur zu nutzen. Hättest du dort Anforderungen hinsichtlich wie man mit deinen Daten umgeht, Thema Speicherung von Daten?
GP-2: Ich würde jetzt davon ausgehen, dass dies über eine Blockchain abgesichert ist, sprich nicht veränderbar und auch anonymisiert abgespeichert wird. Sodass aufgrund einer Zertifikatsnummer nicht auf meine Privatadresse geschlossen werden kann. Aber ich habe mir dazu ehrlicherweise noch zu wenig Gedanken gemacht.

M. Sieber: Habt ihr eine Firmenregelung, wo das Daten gespeichert werden müssen respektive wo nicht?
GP-2: Ist mir so nicht bekannt, dass wir definiert hätten, wo das unsere Daten gespeichert sein sollten. Müsste ich weiter abklären.

M. Sieber: Ein weiterer wichtiger Punkt ist die User-Befähigung für eine digitale Signierlösung. Damit meine ich, wie kommt ein User überhaupt an die Lösung, was er muss er vorab einrichten und unternehmen, bevor er überhaupt das erste Mal produktiv signieren kann. Was ist dir dabei wichtig?
GP-2: Es muss verständlich und nicht allzu komplex sein. Idealerweise hätte ich diese Vorarbeiten innerhalb einer Viertelstunde erledigt, sodass ich gar nicht viel Zeit investieren muss, bevor es funktioniert.

M. Sieber: Wir haben ja vorher besprochen, dass du, bevor du eine öffentlich anerkannte digitale Signatur erhalten könntest, einmalig eine Bestätigung deiner Identifikation erbringen müsstest. Bei der qualifizierten elektronischen Signatur müsstest du hierzu eine physische, persönliche Identifikation bei einer erlaubten Stelle durchlaufen. Und nicht nur du, sondern auch deine externen Vertragsparteien, wenn du von ihnen verlangst, dass sie ebenfalls qualifiziert digital signieren. Wie beurteilst du das?
GP-2: Ich würde mir das kompliziert vorstellen. Wenn z. B. unsere Mitarbeiter, lass es uns 500 sein die das benötigen würden, jeder selber eine solch erlaubte Identifikationsstelle aufsucht. Da hätte ich dann eher den Anspruch, dass dies bei uns vor Ort gemacht werden könnte. […] Und etwas Ähnliches würde ich mir auch für die Garagisten vorstellen, d.h. dass der Dienstleister bei ihnen lokal vorbeigeht und diejenigen, die das nutzen möchten, werden dann identifiziert.

M. Sieber: Würdest du mir Recht geben, dass wenn dieses User-Identifikationsverfahren [für die qualifizierte elektronische Signatur] künftig auch vollständig digital funktionieren könnte, dies eine deutliche Erleichterung und einen Vorteil darstellen würde?
GP-2: Ja, würde ich zustimmen. Gerade in der heutigen Zeit [Corona-Pandemie] bin ich vielleicht noch alle drei Wochen einen Tag im Büro. Wenn wir uns jetzt physisch identifizieren lassen liessen, müsste man wieder vor Ort sein und es würde dann drei Wochen dauern. Wenn das jetzt digital, z. B. über einen Videochat möglich wäre, würde ich wieder Zeit gewinnen.

M. Sieber: Was geht dir beim Thema IT-Infrastrukturanforderungen durch den Kopf? Was sind deine Bedürfnisse hierzu?
GP-2: Ich wäre jetzt hier nicht der Entscheidungsträger. Aber so wie ich unsere IT verstehe, würde alles auf Sicherheitsaspekte geprüft werden und es würde eine Ausschreibung als Beschaffungsprozess stattfinden. Seit einem Jahr hatten wir immer wieder mal Cyberattacken. […] Idealerweise wäre das [die digitale Signaturlösung] auch eine Lösung, die trotzdem weiterläuft, auch wenn man andere Hauptsysteme abstellen müsste.

M. Sieber: Du würdest also eine Cloud-Lösung favorisieren, sodass es nicht von euch betriebene Services sind?
GP-2: Genau. Das wäre jetzt meine Präferenz, im Wissen, dass ich hier nichts zum Entscheid herbeiführen kann.

M. Sieber: Wir kommen langsam zum Abschluss. Da würde mich das *Wie* interessieren, also wie möchtest du die digitale Signatur im Geschäftsalltag verwenden. Was sind für dich hierzu wichtige Bedürfnisse, z. B. ein Workflowtool?
GP-2: Also z. B. rund um das Kreditorenthema, wenn ich diese Rechnungen signiere, das ist ja eigentlich hochgradig standardisiert. Darum unbedingt ein Workflowtool, das wäre schon der Anspruch. Mit den Verträgen und Vereinbarungen könnte ich es mir auch vorstellen, ist aber für mich mengenmässig sicher weniger relevant, denn wegen diesen 10 Verträgen im Jahr brauche ich nicht unbedingt ein System, das mir den Workflow vorgibt. Dort wäre es allerdings spannend, wenn es mit einem Vertragsmanagementtool verlinkt wäre. Haben wir heute aber auch nicht.

M. Sieber: Du hattest eingangs auch die Geräteunabhängigkeit genannt.
GP-2: In einer perfekten Welt sollte die Gegenpartei dein digital signiertes Dokument erkennen können, egal ob sie dies auf einem Mobile, Tablet oder auf einem Mac oder Windows Computer anschauen.

M. Sieber: Geht es für dich hier nur um das «Erkennen/Sehen», oder möchtest du auch vom Mobile aus eine digitale Signatur setzen können?
GP-2: Wäre jetzt nicht mein Anspruch. Wenn ich heute Dokumente digital signiere, dann mache ich das ausschliesslich am Desktop. Auch deshalb, weil ich das Dokument vorher «sauber» gelesen haben möchte und das gelingt mir nicht über das Mobile. Darum würde ich dies ausschliesslich mit einem Desktop nutzen.

Interview mit Gesprächspartner GP-3 am 29.04.2021, 10.00 – 11.00 Uhr

M. Sieber: Wie ich Sie ja vorinformiert habe, möchte ich Sie heute zu Ihren Anforderungen rund um die Nutzung der digitalen Signatur im Geschäftsalltag befragen. Zunächst möchten wir aber die Ausgangslage Ihres Unternehmens etwas besser kennen lernen. Wie ich weiss, sind Sie gerade bei der Evaluation und Einführung einer digitalen Signierlösung. Können Sie bitte Ihre Use-Cases beschreiben, wo Sie künftig digital und nicht mehr von Hand unterzeichnen möchten?

GP-3: Ich bin im Bereich Kapitalanlage angehängt. […] Wir haben weltweit viele Mandate mit vielen Managern. Das führt dazu, dass wir bei jeder Mandatsvergabe Vertragsverhandlungen haben, dass es diverse Dokumente gibt, die der Manager aus regulatorischer Sicht benötigt, z. B. eine Erklärung für die Steuerbehörde, eine Erklärung für KYC oder bei Ausschreibungen die NDA's. Wir haben also viele Dokumente, die wir unterzeichnen. Das war eigentlich schon immer ein Problem, denn für die Unterschrift auszudrucken und wieder einzuscannen, war nie sexy. […] Der Schmerzensdruck bis anhin war aber noch zu wenig gross. […] Jetzt aber mit dem Homeoffice [durch die Corona-Pandemie] und unserer Policy, dass man Zuhause keine Dokumente ausdrucken darf, hat man gemerkt, dass der Prozess nicht mehr funktioniert. Es würde bedeuten, dass immer zwei Personen ins Büro fahren müssten, weil wir immer kollektiv unterzeichnen müssen. So haben wir einen Push bekommen, eine digitale Signierlösung einzuführen.

M. Sieber: Was für Anforderungen stellen Sie an eine digitale Signierlösung, sodass Sie und Ihre Kollegen diese vorteilhaft und breit im Geschäftsalltag einsetzen können?

GP-3: Spontan kommt mir die Schnelligkeit in den Sinn: wie schnell bringe ich diese Signatur hin. Vorteilhaft auch im PDF-Dokument selbst, es gibt ja auch Lösungen, wo ich die Datei zuerst auf eine Plattform hochladen muss. Es muss immer schnell gehen, je mehr Hürden ich habe, desto weniger mache ich es. Die zweite Anforderung wäre die Anerkennung: wie ist das Ganze anerkannt? Eine Unterschrift bringe ich auch ohne Zertifikat auf das PDF-Dokument, aber das nützt dann einfach nicht viel. Also Usability und Anerkennung der Unterschrift.

M. Sieber: Ich möchte gerne noch etwas vertiefter auf Ihre Geschäftsprozesse eingehen. Sie haben dazu schon einiges genannt: es soll schneller gehen, ausdrucken soll vermieden werden. Sie haben die Kosten nicht erwähnt. Wollten Sie auch eine Kostensenkung erreichen oder ist dies nicht im Vordergrund gestanden?

GP-3: Ist nicht so im Vordergrund gestanden, weil in der Finanzbranche nicht dasselbe Denken wie in der Industrie herrscht. In der Industrie hat jeder Mitarbeiter seinen Lohn auf die Stunde und dieser wird an die Leistung angerechnet. In der Finanzbranche kennt man dies noch nicht. Wenn ich jetzt viel weniger Zeit benötige [mit der digitalen Signatur], ist es dann mir bewusst und ist definitiv günstiger, wenn wir es digital machen, aber ist noch kein Case, der bei uns gerechnet wird. […]

M. Sieber: Das eine ist ja die Kostensenkung, wenn Sie digital signieren, das andere sind die Kosten der Digital Signing Lösung selbst. Was ist für Sie ein stimmiger Preis für eine digitale Signierlösung?

GP-3: Das Angebot ist ja eingeschränkt, dadurch dass wir die qualifizierte elektronische Signatur wollten [wozu in der Schweiz nur wenige Anbieter akkreditiert sind]. Dann haben wir die verschiedenen Preismodelle angeschaut und einen Business Case ausgerechnet. Da gab es einmal das Flat Angebot von Ihnen [QuoVadis] und die anderen Anbieter haben Kosten pro Unterschrift gehabt. Dann haben wir ausgerechnet ab wie vielen Unterschriften der Break Even bei beiden erreicht ist. Und dann haben wir festgestellt, dass wir vier [Geschäftsleitung, welche die digitale Signatur für sich einführt] viel signieren, wo sich dann die Flat Rate empfohlen hatte. Wir haben es von dieser Seite angegangen, wir sind nicht hingegangen und haben per se gesagt, der Preis pro Signatur ist nicht gut und wir müssen den auf 50 Rappen pro Unterschrift runterbringen.

M. Sieber: Ich möchte noch auf Ihre externen Anspruchsgruppen zu sprechen kommen. Also z. B. Kunden und Partner, die ja auch betroffen sein können, wenn Sie künftig Dokumente digital und nicht mehr von Hand unterzeichnen. Denken Sie, dass es durch die Nutzung von Digital Signig zu einer Veränderung in der Beziehung mit diesen externen Anspruchsgruppen kommt und wenn ja, an was denken Sie?

GP-3: Was sich sicher verbessern wird ist die Geschwindigkeit. […] Die zeitliche Komponente ist die Wichtigste. Wir sind gespannt, wie die Amerikaner reagieren werden, wenn die Formulare von uns digital signiert daherkommen. Gerade Steuerbehörden sind so «tick the box», Hauptsache das Häkchen ist da, ob es stimmt

oder nicht, ist egal. […] Die Manager kennen die digitale Signatur schon, bei den Behörden sind wir gespannt, was dort die Rückmeldung sein wird.

M. Sieber: Haben Sie das Gefühl, dass es im Umkehrschluss sogar externe Anspruchsgruppen gibt, welche die digitale Signatur von Ihnen fordern und erwarten?
GP-3: Könnte ich mir gut vorstellen. Heute wird von uns immer eine Unterschriftsliste verlangt und umgekehrt auch. Man verlangt von den Firmen eine «Authorized Signatory List». Aufgrund der Fluktuation ist diese dann meistens nach einem halben Jahr nicht mehr aktuell. Nun kann man sagen: wenn einer von einer Firma mit einer qualifizierten elektronischen Signatur unterzeichnen kann, dann gehe ich davon aus, dass die Firma ihm diese Signatur auch bewusst gegeben hat. […] Ich glaube, dies ist der grosse Vorteil meiner Meinung nach, dass man annehmen kann, jeder Mitarbeiter der für eine Firma unterschreiben kann, hat die qualifizierte elektronische Signatur, entsprechend brauche ich die «Authorized Signatory List» nicht mehr.

M. Sieber: Inwiefern denken Sie, dass Sie mit Digital Signing auch Zielgruppen erreichen, welche Sie früher aufgrund der Handunterschriftsanforderung nicht erreicht haben? Also solche, denen der Prozess mit Handunterschrift und via Post versenden zu kompliziert war?
GP-3: Was wir bei unseren Versicherungskunden merken: sie fragen selbst immer mehr nach, ob wir Formulare akzeptieren, die digital unterzeichnet sind. […] Ich glaube umgekehrt ist es gar nicht so relevant. Hat aber auch damit zu tun, dass bei uns ein Grossteil der Kunden durch Broker reinkommen. So hat der Endkunde am Anfang kein Direktkontakt mit uns. Zum anderen bieten wir dort, wo wir Interaktionspunkte haben, z. B. bei der Erfassung eines neuen Mitarbeiters, eine digitale Plattform, worin man als Kunde alles selbst machen kann. Diese Firmen sind dann nicht mehr auf uns angewiesen und können sich selbst einloggen, können selbständig Lohn- oder andere Anpassungen machen [die nicht unterschreibungsrelevant sind].

M. Sieber: Sprechen wir noch über Ihre Sicherheitsbedürfnisse bei der Nutzung der digitalen Signatur. Was haben Sie dabei für Sicherheitsanforderungen?
GP-3: Thema Nr. 1: wo werden die Daten gehostet? Wir lassen eigentlich für alle Tools nur die Schweiz zu, ausser es ist ein ganz grosser Player, wo wir nicht gross verhandeln können. […] Das war auch ein grosser Grund, weshalb wir mit Ihnen [QuoVadis] relativ schnell starten konnten, wir musste nicht noch erst eine Due Diligence der IT durchlaufen.

M. Sieber: Weil Hash Signing sicherstellt, dass keine Dokumente zu uns gelangen.
GP-3: Genau.

M. Sieber: Sie haben die Rechtsverbindlichkeit angesprochen. Wie Sie ja bereits wissen, ist nur die qualifizierte elektronische Signatur gesetzlich der Hand-unterschrift gleichgestellt. Wie wichtig ist Ihnen diese Rechtsverbindlichkeit?
GP-3: Sehr wichtig. Anders hätten wir es nicht akzeptiert. Sie müssen sich vorstellen, wenn Sie Verträge über ein paar Milliarden unterschreiben und es gibt daraus ein Problem, ist dann das Erste was der Anwalt sagt, dass die digitale [nicht qualifizierte] Unterschrift nicht rechtsgültig ist. Wir haben jeweils in der Vergangenheit für nicht so relevante Dokumente auch unsere Unterschrift ins PDF getan [eingescannt], war aber nichts Verbindliches.

M. Sieber: Lassen Sie uns ein wenig zur User-Ausrollung und Befähigung kommen. Damit meine ich, wie Sie oder Ihre Kollegen oder irgendwann auch Ihre externen Vertragsparteien überhaupt Zugang zu der digitalen Signatur erhalten. Also was müssen Sie unternehmen und einrichten, bevor Sie das erste Mal produktiv digital signieren können. Was ist Ihnen hierbei wichtig?
GP-3: Ein Bedürfnis ist sicher die [User] Identifizierung über eine Online-Lösung. Davon hat man ja bereits vor Jahren gesprochen. […] Das ist natürlich einfacher, als wenn ich persönlich bei der Post vorbeigehen muss. Das ist ohnehin ein bisschen ein sinnloser Prozess, denn der Postbeamte schaut mich einmal an und «knallt» den Stempel drauf. Zu ihm könnte ich auch, wenn ich nicht die Person wäre, die ich bin [er würde das nicht bemerken und trotzdem die Identität bestätigen]. Das ist sicher etwas, was man optimieren kann und notwendig ist. […]

M. Sieber: Sie haben es eingangs selbst gesagt. Je mehr Hürden Sie haben, desto weniger nutzen Sie es. So wie ich Sie spüre stellt für Sie der aktuelle User-Identifikationsprozess [persönliche User-Identifikation bei einer erlaubten Stelle für eine qualifizierte elektronische Signatur] eine solche Hürde dar?
GP-3: Genau. […]

M. Sieber: Thema Funktionsumfang der digitalen Signaturlösung. Also nicht, welche digitale Signatur Sie einsetzen, sondern vielmehr *wie*. Sie werden eine Lösung einsetzen, mit welcher Sie direkt aus dem PDF-Dokument heraus digital signieren können. Es gibt allerdings auch weiterführende Lösungen, womit Sie mit Signaturworkflows das signierte Dokument anschliessend nicht manuell via E-Mail an andere Parteien weiterversenden müssen, sondern diese Aufgabe bereits im Digital Signing Tool übernommen und gestartet werden kann. Wie wichtig sind Ihnen solche Features und was sind Ihre Bedürfnisse an eine «Verpackung» der digitalen Signatur?
GP-3: Dort wo man den Prozess [zur eingesetzten Lösung] optimieren kann, ist sicher eine Schnittstelle zu meinen Ordnern. […]

M. Sieber: Inwiefern ist für Sie die Geräteunabhängigkeit wichtig? Haben Sie z. B. auch das Bedürfnis, vom Mobile aus Dokumente digital zu signieren?
GP-3: Privat schon. Geschäftlich arbeiten wir auf Citrix. Abgesehen vom Mobile bin also von überall, also ob vom Laptop Zuhause oder im Geschäft, immer in der Citrix Umgebung unterwegs. Sprich dann habe ich diese Funktionen immer verfügbar. Ich wüsste jetzt auch nicht, ob ich auf einem Mobile signieren würde.

M. Sieber: Aus welchem Grund nicht?
GP-3: Wenn ich signiere, hat es meistens einen Grund. Dann möchte ich das Dokument auch noch [gut] durchlesen können. Wenn es vielleicht ein Brief ist [one-pager] – ok. Wenn ich aber z. B. ein 40-seitiges Dokument habe, muss ich schon wissen, um was es genau geht. Vielleicht kommt es ein wenig aufs Dokument drauf an. […] Wenn ich jetzt so mein Telefon mit seiner Bildschirmgrösse anschaue, logge ich mich lieber schnell im Citrix [über Laptop / Desktop] ein, sodass ich dann auch die Unterschrift gut platzieren kann.

M. Sieber: Sie haben noch die Schnittstelle an vor- oder nachgelagerte Applikationen angesprochen. Also dass Sie z. B. direkt aus dem ERP oder CRM heraus digital signieren könnten und nicht zuerst ein PDF downloaden müssten (und später wieder der Applikation zuführen müssten). Wie wichtig ist das für Sie?
GP-3: Ja, genau. Das findet dann vor allem der Rest des Unternehmens wichtig [andere Abteilungen]. Z. B. der Leiter IT wird sich dies dann sicher genau anschauen, wenn sie [Rest der Unternehmung / andere Abteilungen] dann so weit sind. Weil dort

möchte man dann eine andere Durchgängigkeit erreichen. Es muss dann von überall nutzbar sein.

M. Sieber: Ist es für Sie oder Ihre Kollegen wichtig, auch externe Unterzeichner in einem digitalen Signaturprozess einladen zu können? Mit der aktuellen Lösung signieren ja «nur» Sie / Ihre Kollegen einseitig, von Ihrem Unternehmen, aus.
G*P-3: Persönlich fände ich das spannend. Weil dann kann ich direkt sagen, Manager X und Y, ihr zwei bitte digital signieren. Was ich nicht weiss, wie gross dann die Akzeptanz [bei den eingeladenen Personen] ist und wie schnell sich die eingeladenen User hierfür registrieren können. [...]*

M. Sieber: Das heisst im heutigen Prozess unterzeichnet Ihre externe Vertragspartei noch von Hand oder benötigen Sie in den meisten Fällen, wo Sie ein Dokument digital signieren, gar keine Signatur von der anderen, externen Vertragspartei?
G*P-3: Doch, das braucht es schon. Wir erfahren heute eigentlich drei Wege: Diejenigen, die auch mit einem Zertifikat [und damit öffentlich anerkannter digitaler Signatur] arbeiten, dann diejenigen, die ausdrucken, unterschreiben [von Hand] und wieder einscannen und dann noch diejenigen, die selber im PDF-Dokument etwas basteln [nicht zertifikatsbasiert und somit keine öffentlich anerkannte digitale Signatur]. Das ist dann das, was wir nicht akzeptieren können. Da besteht aber schon ein gewisser Druck. Z. B. in London hatten nun viele ihre Offices zu [aufgrund Corona-Pandemie], die nutzen dann viel DocuSign.*

M. Sieber: Die aber grösstenteils keine rechtsgültigen [Schweizer qualifizierte elektronische Signaturen] Signaturen nutzen.
G*P-3: Genau. Dort haben wir dann wieder ein Problem. Dort lassen wir uns dann einfach von der Unternehmung bestätigen, dass dies ok ist [und somit untereinander vereinbart gilt, dass dies als rechtsgültig angesehen wird] und akzeptieren es dann. Man muss aber fairerweise auch sagen, dass wenn jemand von Hand unterzeichnet, ob dann auch immer klar ist, wer tatsächlich unterschrieben hat, ist auch nicht so sicher.*

M. Sieber: Ich entnehme, dass es aber Fälle gibt, wo Ihre externe Vertragspartei von Hand unterzeichnet und dies einscannt. Das hingegen akzeptieren Sie dann, denn eine Handunterschrift wäre ja nur im Original und nicht eingescannt gültig?
GP-3: […] Im Nachgang wird dann das Original noch eingefordert. Wir akzeptieren dies aber auch, weil unsere Haltung dort ist, dass er [die externe Vertragspartei] in einem Streitfall nicht sagen kann, er hätte von nichts gewusst. Weil man hat die E-Mail-Korrespondenz. […] Aber ist ein berechtigter Punkt, ganz sauber ist es natürlich nicht. Aber am Ende des Tages erachte ich eine solche digitale Unterschrift als einiges vertrauenswürdiger als eine Handunterschrift.

Interview mit Gesprächspartner GP-4 am 30.04.2021, 14.00 – 15.00 Uhr

M. Sieber: Wie vorinformiert sprechen wir heute über Ihre Anforderungen an die Verwendung der digitalen Signatur im Geschäftsalltag. Wie ich weiss, beschäftigen Sie sich derzeit stark mit der Einführung der digitalen Signatur für Ihr Unternehmen. Können Sie die Use-Cases beschreiben, in welchen Sie die digitale Signatur angedacht haben und nicht mehr von Hand unterzeichnen möchten?

GP-4: Das Thema ist vor ca. drei Jahren aufgekommen, als wir damit begannen, immer mehr zu digitalisieren. D.h. wir haben unsere ganze Ablagestruktur nun vollständig digital und legen nichts mehr in Papierform ab. Aber wir haben noch eine Regelung, dass ein Vertrag oder Dokument handschriftlich unterzeichnet sein muss. Diese Unterschriften respektive Verträge werden dann in ein PDF-Dokument umgewandelt [eingescannt] und dann so weiterverarbeitet und digital archiviert.

M. Sieber: Was sind das für Dokumente?

GP-4: Querbeet: Protokolle, Briefe, Architektenverträge, Subunternehmerverträge. Es zeigt sich aus der Erfahrung heraus, dass die Qualität von der Vertragsablage, insbesondere dort wo wir klassische Subunternehmerverträge haben, digital in der Tendenz etwas schlechter als in Papierform ist. Denn in der Papierform ist es relativ einfach: dort habe ich einen umfänglichen Vertrag, ca. 200 – 300 Seiten, der ist zusammengebunden im Ordner abgelegt worden. Und den konnte man wieder hervornehmen und hat gesehen, dass er unterschrieben ist. […] Nur jetzt in der digitalen Ablage ist es etwas herausfordernder: ein Subunternehmerwerkvertrag oder auch ein Mietvertrag haben unter Umständen auch Planbeilagen. Das sind dann vielleicht fünf bis sechs Dokumente, die separat unterzeichnet werden müssen, z. B. allgemeine Geschäftsbedingungen oder Sicherheitskonzepte. Wir haben Vertragsdokumente von über 1'000 Seiten oder von 650MB Datenumfang. Und da sieht man, dass das ganze [digitale] Handling nicht ganz so einfach ist. Die Thematik in der heutigen Lösung - also mit der Handunterschrift wo nachträglich ein PDF-Dokument erstellt wird - ist, dass halt am Schluss nur noch eine Unterschriftsseite mit den Unternehmen [Vertragsparteien] hin- und her gesendet wird. Dann werden am Schluss die Verträge wieder zusammengesetzt [vor der elektronischen Archivierung]. Dann sehe ich manchmal, dass die teilweise nicht vollständig sind, d.h. 2-3 Seiten nicht richtig eingescannt wurden oder statt der Unterschriftsseite wird eine leere Seite eingescannt. Dieses Handling ist nicht sehr gut. Und jetzt, wo wir alle im Homeoffice

sind [Corona-Pandemie], haben wir erkannt, dass es immer dringender wird und dass wenn wir von Digitalisierung sprechen, dass man auch digital Signieren muss. […]

M. Sieber: Ganz allgemein und spontan: Was sind Ihre Anforderungen an eine digitale Signierlösung, sodass Sie und Ihre Kollegen diese im Geschäftsalltag vorteilhaft und breit einsetzen können?

G*P-4: Sie muss ganz einfach sein [im Handling]. Und ich möchte nicht studieren müssen, ob ich nun mit einer fortgeschrittenen, einer qualifizierten oder einer einfachen elektronischen Signatur unterschreiben soll. Der ganze Prozess sollte ohne Studieren vonstatten gehen können. Alles andere ist extrem fehleranfällig. Darum favorisiere ich nun auch für unsere Unternehmung, dass jeder Mitarbeiter die qualifizierte elektronische Signatur [höchste Stufe] erhält. Der einzige Hinderungsgrund sind die Kosten. […] Und auch komplexe Verträge müssen einfach handelbar sein. Und wir müssen [externe] Dritte einfach in den Signaturprozess integrieren können. Das System funktioniert nur gut, wenn die gesamte Geschäftswelt digital signiert. Da sind wir aber natürlich noch weit davon entfernt. Jetzt wo wir beginnen, digital zu signieren, müssen wir zusehen, dass wir Hürden bei [externen] Dritten abbauen können, dass wir sie animieren, sodass sie auch digital signieren. Darum ist dann die fortgeschrittene elektronische Signatur interessant, wo die Personen nicht noch zuerst mit dem Pass bei der Post [zur User-Identifikation] vorbei gehen müssen. Für viele wäre das [eine einmalige physische User-Identifikation bei einer erlaubten Stelle als Voraussetzung zum Erhalt der qualifizierten elektronischen Signatur] eine extreme Hürde. Dieser Aufwand lohnt sich dann nicht für Verträge wo es um CHF 500.—geht.*

M. Sieber: Ist für Sie auch eine Kostensenkung im Vergleich zum analogen Signaturprozess mit hin und her senden, warten und wieder einscannen ein Thema?

G*P-4: […] Wir beurteilen, dass dies ein spürbarer Effizienzgewinn darstellen wird. Indem dass wir vor allem Zeit gewinnen, werden die ganzen Prozesse effizienter.*

M. Sieber: Sie haben eingangs die Kosten für Digital Signing genannt. Wie muss für Sie ein Preis für eine digitale Signierlösung sein, sodass er für Sie «stimmig» ist?

G*P-4: Die Preishöhe ist noch schwierig zu beurteilen. Irgendwie müsste man auf ein Flat Rate Modell kommen können. Also eher die Kosten auf eine Person bezogen, wie ein Mobile-Abonnement. Die aktuelle Schwierigkeit liegt im hin und her rechnen mit den verschiedenen Tarifen zwischen den Signaturtypen und dann kommt noch der*

Userpreis hinzu, da blickt niemand mehr durch. Ich fände es schön, wenn wir sagen könnten, wir haben 220 Mitarbeiter mal XYZ Kosten pro Person.

M. Sieber: Lassen Sie uns ein wenig auf Ihre externen Anspruchsgruppen wie Kunden und Partner zu sprechen kommen, welche ja auch betroffen sein können, wenn Sie neu digital anstelle via Handunterschrift signieren. Was für eine Veränderung oder Erwartung mit der Verwendung der digitalen Signatur erwarten Sie in der Geschäftsbeziehung zu diesen externen Anspruchsgruppen?
G*P-4: Dass sie mitmachen. Ich kann noch nicht beurteilen, wie diese Bereitschaft [dass externe Vertragsparteien ebenfalls digital signieren] wirklich ist. Eigentlich haben wir zwei Kategorien von externen Anspruchsgruppen: Privatpersonen - vor allem Wohnungsmieter - und die Geschäftskunden.*

M. Sieber: Inwiefern haben Sie das Gefühl, dass Ihre externen Anspruchsgruppen Digital Signing von Ihnen bereits erwarten?
G*P-4: Ich glaube nicht. Ich glaube, es haben sich alle ein bisschen an den aktuellen Prozess [Handunterschrift, danach einscannen] gewöhnt. Vereinzelt grosse Bauherren wie SBB oder UBS signieren aber bereits vereinzelt digital.*

M. Sieber: Thema Sicherheitsbedürfnisse: Was haben Sie für Anforderungen an die Sicherheitsaspekte bei der Verwendung einer digitalen Signatur?
G*P-4: Sie muss rechtlich verheben. Also eine qualifizierte elektronische Signatur die der Handunterschrift gesetzlich gleichgestellt ist. Ich glaube dies muss der grundsätzliche Anspruch sein.*

M. Sieber: Haben Sie zum Thema Sicherheitsbedürfnisse noch andere Anforderungen? Z. B. an die Speicherung von Daten, also wie geht man mit Daten oder zu signierenden Dokumenten beim Signaturanbieter um?
G*P-4: Die Frage ist natürlich, wie sicher ist es, dass niemand mit meiner persönlichen digitalen Signatur für mich einkaufen geht. Das ist sicher noch eine Sorge, die bei den Leuten im Kopf ist.*

M. Sieber: Nochmals zum Thema Daten.
G*P-4: Also am liebsten habe ich die Daten bei mir in der Unternehmung. Ich bin mir aber bewusst, dass dies in der heutigen Zeit mit all den Cloudlösungen nicht mehr überall machbar ist. Wir haben auch bei uns wichtige Applikationen, deren Daten komplett beim Anbieter sind. Wir wissen, wenn dieser halt ein technisches Problem hat, dann stehen auch wir still. Vielleicht liegt es auch eher daran, dass ich noch ein*

wenig auf der konservativeren Schiene unterwegs bin und die Daten lieber bei mir habe. Ich glaube die moderne Fraktion, die schwört eher auf Cloudlösungen und wollen gar nichts mehr bei sich haben. […] Ich habe keine Bedenken für externe Lösungen, da wird man sich nicht verschliessen können. Und man muss auch vertrauen, dass es sicher abläuft.

M. Sieber: Ein anderer wichtiger Punkt innerhalb der Verwendung einer digitalen Signaturlösung stellt das User-Onboarding dar. Damit meine ich, wie kommen Sie, Ihre Kollegen oder auch externe Unterzeichnungsparteien überhaupt zu der digitalen Signaturlösung. Was müssen für vorgelagerte Schritte unternommen werden, bevor sie überhaupt das erste Mal produktiv signieren können. Was ist Ihnen dabei wichtig?
GP-4: Es darf nicht zu viele Schritte haben. Der User müsste eigentlich mit einem Klick signieren können. Insbesondere auch, wenn er jetzt mal zwei bis drei Monate nichts signiert hatte und er hat dann wieder etwas zu signieren, dann muss es selbsterklärend sein, sonst verzweifeln die User. […]

M. Sieber: Sie haben gesagt, Sie setzen, wenn, dann grösstenteils die qualifizierte elektronische Signatur ein, wofür mit der heutigen Regulierung weiterhin immer noch eine physische, persönliche User-Identifikation bei einer erlaubten Stelle stattfinden muss. Wie beurteilen Sie das?
GP-4: Es ist halt eher umständlich. Eigentlich müsste man die ganze Identifikation auch über Video oder dergleichen machen können. Oder es müsste halt à la E-ID jede Person vom Bund aus eine Registration haben. […] Also für uns als Firma ist ja der Aufwand überschaubar [weil sie dies ja wollen und proaktiv steuern können]. Das Problem ist eher der Prozess, wenn ich eine externe Drittpartei zum Signieren einlade und ich möchte, dass dieser zwingend mit der qualifizierten elektronischen Signatur signieren muss. Dafür müsste er jetzt extra mit seinem Ausweis die Gemeinde oder eine andere berechtigte Stelle aufsuchen. Das ist dann mühsam. Dann ist er vielleicht noch im Urlaub oder hat keine Zeit und dann ruht das zu unterzeichnende Dokument wieder. Das müsste doch alles auch irgendwie online gehen müssen.

M. Sieber: Inwiefern ist für Sie die Vorlaufzeit wichtig? Ich meine dies auf den User bezogen, welchen Sie zu einer digitalen Gegen-Signatur einladen. Was haben Sie für eine zeitliche Erwartung, bis dieser befähigt sein müsste?
GP-4: Schön wäre es, wenn er es mit ein paar Klicks sofort machen kann. Er kriegt die

Einladung, kann einen Link anklicken, dann wird er zur Registrierung [und Identifikation] aufgefordert und er kann dies mit wenigen Klicks machen.

M. Sieber: Lassen Sie uns noch ein wenig vom Funktionsumfang einer digitalen Signierlösung sprechen. Also die «Verpackung» der digitalen Signatur, welche beeinflusst, *wie* Sie die digitale Signatur im Geschäftsalltag einsetzen können. Was haben Sie hierzu für Anforderungen? Sie hatten ja z. B. bereits genannt, dass Sie externe Drittparteien sehr einfach auf einen Signaturprozess einladen möchten. Gibt es da noch andere Funktionsbedürfnisse?
G*P-4: Ich finde es noch gut, wenn man alles auswerten kann. Welche Verträge hat wer unterzeichnet.*

M. Sieber: also Reportingmöglichkeiten?
G*P-4: Genau. Das gibt einfach eine Sicherheit. Durch die ganze Digitalisierung ist alles ein wenig «luftig», jeder macht ein wenig etwas, versendet Daten und wenn man sich dann fragt, ob alles korrekt läuft, hätte man durch ein Reporting eine Möglichkeit dies zu kontrollieren.*

M. Sieber: Inwiefern ist Ihnen eine Geräteunabhängigkeit wichtig? Also dass Sie z. B. nicht nur vom Desktop aus Dokumente digital signieren können, sondern auch vom Mobile aus?
G*P-4: Sehr wichtig. Ich glaube es muss zwingend sein, dass man von allen Geräten aus signieren kann. Es ist mir zwar klar, dass es ambitioniert wäre, einen grossen Vertrag vor der Unterschrift nochmals am Mobile durchzugehen. […]*

M. Sieber: Was denken Sie beim Thema Schnittstellen im Rahmen einer digitalen Signierlösung. Meistens ist das digitale Signieren nur ein Teilprozess, das signierte Dokument geht vielleicht danach in ein Archiv oder ERP System oder wird bereits schon dort erstellt. Ist dies etwas, worüber Sie sich schon Gedanken machen, oder ist der Fokus erstmalig nur auf der reinen digitalen Signatur?
G*P-4: Genau, im Moment ist der Fokus exklusive auf das digitale Signieren. Solche Vollintegrationen sind derzeit noch aussen vor.*

M. Sieber: Wie wichtig sind für Sie Workflowkomponenten innerhalb der digitalen Signaturlösung? Also z. B. dass Sie das Dokument nicht nur digital signieren und dann manuell per E-Mail an eine weitere Partei versenden, sondern dass ein Workflow innerhalb des Signiertools diese Aufgabe übernimmt. Oder z. B. Reminderfunktionen, sodass die eingesetzte Signierlösung automatisch Reminder an Vertragsparteien sendet, die noch nicht signiert haben.
GP-4: Ich finde das sehr wichtig. Das hilft den Prozess wirklich steuern zu können. Auch dass ich sagen kann, dieser Vertragspartner muss qualifiziert digital unterzeichnen [der Signaturworkflow-Initiant gibt vor, mit welcher Art von digitaler Signatur unterzeichnet werden muss] oder dass er zuerst unterzeichnen muss. Es könnte ja auch noch weitergehen, dass so bald alle unterzeichnet haben mir danach dieser Vertrag automatisch in die richtige Ablage gespeichert werden würde. Ich finde das würde schon enorm viel bringen. […]

M. Sieber: Sie haben sich nun intensiv mit der digitalen Signatur und Lösungen dazu auseinandergesetzt. Was ist aktuell für Sie der grösste Schmerzpunkt beim Thema Digital Signing?
GP-4: Die grösste Hemmschwelle ist, dass nicht einfach jede Geschäftsperson eine solche [qualifizierte elektronische Signatur] hat. Ich muss mal zuerst alle Mitarbeiter in meiner Unternehmung registrieren lassen. Dann habe ich aber noch das Thema mit den externen Unterzeichnern, die zu einer Signatur eingeladen werden, die müssen sich dann auch noch zuerst registrieren. Irgendwie sollte jede Person bereits eine solche Registration haben, welche auch unabhängig vom Unternehmen gilt. Ob ich nun auf einer Swisscom, QuoVadis oder Europäischen Plattform bin, das sollte gar keine Rolle spielen, zumindest innerhalb der Schweiz nicht.

M. Sieber: Also das Thema User-Onboarding so einfach wie möglich…
GP-4: Ja, ich glaube, dies ist der entscheidende Knackpunkt damit es sich wirklich durchsetzt.

Interview mit Gesprächspartner GP-5 am 07.05.2021, 11.00 – 12.00 Uhr

M. Sieber: Wie vorinformiert sprechen wir heute über Ihre Anforderungen an die Nutzung der digitalen Signatur im Geschäftsalltag. Vorab möchte ich die Ausgangslage Ihres Unternehmens noch etwas besser kennen lernen. Ich weiss, dass Sie sich intensiv mit der digitalen Signatur im Rahmen der Einführung für eine Abteilung Ihres Unternehmens beschäftigt haben. Bitte erläutern Sie kurz die Use-Cases, für welche diese Abteilung die digitale Signatur einsetzen wird.
GP-5: Dabei geht es um Gerichtseingaben.

M. Sieber: Ist das ein Vorgang, der häufig von dieser Abteilung vorgenommen wird? Von wie vielen Dokumenten sprechen wir hier pro Jahr?
GP-5: Ich würde sagen über 1'000 im Jahr.

M. Sieber: Ganz allgemein gefragt: Was sind Ihre Anforderungen an eine digitale Signaturlösung, sodass Sie und Ihre Kollegen sie vorteilhaft im Geschäftsalltag verwenden können und Sie eine entsprechende Investition darin befürworten können?
GP-5: Grundsätzlich muss sie für die User in der Anwendung einfach sein. Wir setzen die digitale Signatur für die Signierung von PDF-Dokumenten ein. Man kann ja aber – mit einer anderen Lösung – auch E-Mails signieren. Es wäre schön, wenn man eine Lösung für alle Signaturmöglichkeiten hätte. Die digitale Signaturlösung müsste auch überall in den Standard Office Produkten integrierbar sein. Ich glaube die digitale Signaturlösung muss uns «nur» eine digitale Signatur bieten, weiter muss sie nicht gehen, sie muss uns keinen Workflow zur Verfügung stellen. Für diesen sind wir selbst zuständig.

M. Sieber: Nehmen wir etwas mehr Bezug auf Ihre Geschäftsprozesse. Was haben Sie für Anforderungen und Erwartungen bei der Nutzung der digitalen Signatur im Hinblick auf Ihre Geschäftsprozesse?
GP-5: Ortsunabhängigkeit. Vereinfachung von Prozessen durch Digitalisierung.

M. Sieber: Also der Faktor Zeitersparnis…
GP-5: Ganz genau.

M. Sieber: Sie haben das Thema Kostensenkung nicht genannt. Steht das aktuell nicht im Vordergrund für Sie?
GP-5: Hatte ich nun nicht im Fokus. Aber es ist klar, wenn ich einen Prozess effizienter gestalte, dann sinkt auch der Aufwand [und damit die Kosten]. Ich glaube es steht bei uns nicht das Monetäre im Prozess im Vordergrund. Wir sind sehr kostensensitiv, aber die Einsatzmöglichkeiten [der qualifizierten elektronischen Signatur] sind bei uns nicht sehr gross. […] Wir haben nicht viele Verträge, wir sind kein Handels- oder Bauunternehmen, aber unsere Prozesse werden effizienter.

M. Sieber: Spielen für Sie auch nachgelagerte Prozesse eine Rolle? Thema strukturierte Daten: Wenn Sie nun ein digital signiertes Dokument haben, ist dieses ja im Nachgang auch komplett digital durchsuch- und auswertbar. Ist das für Sie im Rahmen der digitalen Signatur ein wichtiges Feature oder mehr nice-to-have?
GP-5: Da würde ich schon einen grossen Vorteil sehen.

M. Sieber: Das heisst, ihr verbringt viel Zeit mit der Suche nach solchen [nicht strukturierten] Dateien?
GP-5: Ist natürlich so. Wenn man Papier verwalten muss, hat man all die Nachteile mit dem Papier. Klar, ich kann es einscannen, ich kann mir eine Lösung beschaffen, mit welcher ich die eingescannten Dokumente dann bei mir organisiert abspeichern und wieder finden kann. […]

M. Sieber: Haben Sie das Gefühl, dass externe Anspruchsgruppen, wie z. B. Kunden und Partner wie die Gerichte, die digitale Signatur sogar von Ihnen fordern?
GP-5: Bis jetzt habe ich dazu noch nichts grossartig mitbekommen. Aber genau in dem Geschäftsbereich, wo wir sie jetzt einsetzen möchten [Gerichtseingaben], dort haben wir die entsprechende Anfrage erhalten.

M. Sieber: Der Treiber für die Einführung der digitalen Signatur war also die Gegenseite, die Gerichte?
GP-5: Es waren beide Seiten. Wir möchten unsere Dossiers und Einsprachen digital übermitteln und die andere Seite sagt ja, dürft ihr, wir sind bereit dafür, aber es braucht noch etwas dazu: die elektronische Signatur. Sonst müsst ihr die Dokumente immer noch parallel senden [handunterschriebene Dokumente physisch per Post]. […] Wir merken aber, gerade auf der Seite der Gerichte, dass der Wandel kommt und wir

unsere Akten digital übermitteln dürfen. Das war lange nicht so. Von dem her gesehen war es gegenseitig gewünscht.

M. Sieber: Spannend. Wie wichtig sind für Sie Sicherheitsaspekte bei der Nutzung einer digitalen Signierlösung? An welche Punkte denken Sie dabei im Speziellen?
GP-5: Sicherheitsaspekte sind immer das Wichtigste für uns, weil wir schlussendlich mit sehr sensiblen Daten unterwegs sind. Die Gewährleistung des Datenschutzes ist für uns primär, dies sichergestellt zu haben ist das oberste Credo. Und bei Übermittlungen möchten wir sicher sein, dass die Übermittlungskanäle sicher sind. Es wir dann aber noch schwieriger, wenn wir noch weiterdenken und überlegen, ob wir auch innerhalb eines [externen] Unternehmens sicherstellen können, dass der Zugriff [auf die signierten und zu signierenden Dokumente] auch nur durch die Personen erfolgen kann, welche die [berechtigten] Empfänger sind.

M. Sieber: Sie haben erwähnt, dass Sie mit den Gerichten die qualifizierte elektronische Signatur einsetzen müssen. Also die höchste digitale Signaturstufe, die auch gesetzlich der Handunterschrift gleichgestellt ist, welche aber auch gewisse Bedingungen voraussetzt. Nämlich, dass sie von einem akkreditierten Anbieter ausgestellt wird und dass der User, der sie einsetzt, sich vorab einmalig face-to-face von einer berechtigten Stelle identifizieren lässt. Wie wichtig war Ihnen diese Rechtsverbindlichkeit?
GP-5: Wir hatten uns das vorher gar nicht überlegt. Wir sind mit dem Wunsch konfrontiert worden, diese digitale Signatur zu erhalten [von der Abteilung, welche die Gerichtseingaben macht. Diese wiederum wurden von Gerichten informiert, dass sie bei einer digitalen Signatur die qualifizierte elektronische Signatur einzusetzen haben]. […]

M. Sieber: Könnten Sie sich auch vorstellen eine niedrigere, nicht rechtsgültige Stufe der digitalen Signatur zu nutzen?
GP-5: Absolut. Es gibt sehr viele Prozesse, wo man keine qualifizierte elektronische Signatur benötigt. Dort könnten wir uns das sehr gut vorstellen.

M. Sieber: Sie hatten den Umgang mit Daten angesprochen. Haben Sie eine Unternehmensregelung, wo Daten gespeichert werden müssen, wenn Sie mit Drittanbietern zusammenarbeiten?
GP-5: Absolut, ja. Unsere Vorgabe lautet, dass unsere Daten sicher in der Schweiz

gespeichert werden müssen. Und es muss auch gewährleistet sein, dass unsere Daten von dort die Landesgrenzen nicht verlassen können.

M. Sieber: Diejenige Signaturlösung, für welche Sie sich entschieden haben, bietet Hash Signing an. Das heisst der Signaturanbieter erhält nicht einmal das zu signierende Dokument, sondern lediglich einen Hashwert. War dies für Sie eine wichtige Anforderung?
GP-5: Ja, absolut. Als ich das gesehen habe, fand ich dies sehr smart gelöst, dass ich unser Dokument nirgendwo hochladen muss und dieses bei uns bleibt.

M. Sieber: Lassen Sie uns als Nächstes über das Thema User-Onboarding sprechen. Damit meine ich, wie Sie, Ihre Kollegen oder vielleicht irgendwann auch einmal externe Signaturparteien überhaupt an die digitale Signaturlösung kommen. Welche Schritte die User vorab unternehmen müssen, bevor sie damit überhaupt das erste Mal produktiv signieren können. Was ist Ihnen dabei für Ihre User wichtig?
GP-5: Schlussendlich natürlich die Einfachheit. Primär, dass die User die Schritte, welche sie unternehmen müssen, einfach verstehen, sodass sie nicht nachfragen müssen.

M. Sieber: Bei der qualifizierten elektronischen Signatur, die Sie aktuell einsetzen, ist bekanntlich vorab die einmalige persönliche User-Identifizierung durch eine berechtigte Stelle notwendig. Wie beurteilen Sie das?
GP-5: Ich empfinde das jetzt nicht als grosse Hürde. Das ist absolut ok, wir sind alle in einem Land, wo alles sehr kleinräumig ist. Mit den vorhandenen berechtigen Stellen kann jeder problemlos in Kontakt treten. Wir haben ja keinen Geschäfts-Use-Case, wo jemand innerhalb einer Stunde digital signieren können muss. Sondern es ist etwas, dass man ganz bewusst angeht und damit eine gewisse Zeit dafür hat. Und es gibt eine Gewährleistung, […] dass es Stellen gibt, die ausserhalb der Unternehmen sind und über die entsprechenden Mittel verfügen, um Personendaten und das Foto des Ausweises mit der Person, die vor einem [zwecks Identifikationsbestätigung] steht, zu prüfen und bestätigen. Ich finde das absolut in Ordnung.

M. Sieber: Etwas anders sieht es aus, wenn Sie sich vorstellen, in Zukunft auch einmal externe Personen in Ihren Signaturprozess einzuladen. Ihr Endkunde ist schlussendlich der private Bürger. Spätestens dort wird es wohl etwas herausfordernd, da dieser wohl kaum, nur weil Sie von ihm eine digitale Signatur wünschen, den Aufwand auf sich nehmen und sich zu solch einer Identifikationsstelle begehen wird?
GP-5: Das ist sicher so, ja. Dann müsste man andere Lösungen haben. Bei unserer Kundschaft müsste man eher auf Bundeslösungen schauen.

M. Sieber: Wie meinen Sie das genau?
GP-5: Dass z. B. mit einer E-ID gearbeitet wird.

M. Sieber: Sodass die Userbefähigung automatisch vorhanden wäre und dieser nicht noch zusätzliche Hürden unternehmen müsste, um mit Ihnen digital zu signieren?
GP-5: Ja. Es ist unverständlich, dass man bei uns [in der Schweiz] einen Pass oder ID abholen kann, wir aber nicht in der Lage sind, eine digitale ID mitzugeben. Aber wir haben ja erst kürzlich darüber abgestimmt.

M. Sieber: Was ja leider nicht angenommen wurde.
GP-5: Ja. […] Unsere allgemeinen Geschäfte sind so, dass die Kunden [private Bürger] den Prozess von aussen auslösen und uns mit einem [von Hand] unterschriebenen Formular den Anstoss geben, ihren Bedarf zu prüfen.

M. Sieber: Das von Hand unterzeichnete Formular, welches ja die Initialzündung darstellt, ist ja somit immer noch ein Papierprozess.
GP-5: Ja. Das ist zurzeit unser grosser Pferdefuss innerhalb der Digitalisierung, dass wir immer noch sehr viel Papier entgegennehmen müssen.

M. Sieber: Es wäre für Sie also sehr wertschöpfend – sofern natürlich Ihre Kunden das auch wünschen – dass Sie von Anfang an den digitalen Weg gehen könnten und kein Medienbruch mit dem Papier und der Handunterschrift mehr hätten?
GP-5: Absolut. Das wäre grossartig, wenn unsere Kunden […] uns Ihre Dokumente digital übergeben könnten, sodass wir direkt damit arbeiten könnten.

M. Sieber: Sie haben als Sozialversicherungsanstalt ja mit sehr sensiblen Daten und Dokumenten zu tun. Dort würden Sie dann wohl auch darauf bestehen, dass wenn diese Dokumente von Ihren Kunden digital signiert werden, dass sie mit der höchsten Stufe [qualifiziert] signiert werden?
GP-5: Das ist so, auf jeden Fall. Man kann sich nicht für eine Sozialleistung anmelden und wir hätten nicht eine entsprechende Gewährleistung, dass die Person, die sich angemeldet hatte, auch die Person ist, die auf dem Formular steht. Entsprechend ist dann die Anforderung an die Unterschrift sehr hoch.

M. Sieber: Ich entnehme, dass so lange nur Ihre Mitarbeiter qualifiziert digital signieren, der Umstand der einmaligen, persönlichen User-Identifikation gangbar ist. Aber richtig wertschöpfend ist es erst, wenn auch der Weg von Ihren externen Kunden zu Ihnen digital wäre und dort hätten wir aber mit dieser notwendigen User-Identifikationsform nicht die gewünschte Skalierung.
GP-5: Ja. Es wäre nicht denkbar, dass wir den Kunden eine Empfehlung abgeben würden, dass sie entsprechend handeln müssten. Da müssten uns dann andere Lösungen dienen.

M. Sieber: Thema IT-Infrastruktur. Was stellen Sie dort für Anforderungen, wenn Sie Lösungen, z. B. für Digital Signing, bei sich im Unternehmen einführen?
GP-5: Grundsätzlich ist bei uns viel vor Ort, also On Premise. Die von euch [QuoVadis] eingesetzte Lösung ist ja hybrid. Die Anwendung geschieht bei euch, aber das Dokument bleibt bei uns. Das ist so sehr smart gelöst für uns. Einen wichtigen Aspekt finde ich auch die Anwendungsübergreifbarkeit. Ich habe gerne Lösungen, die ich nachher überall einsetzen kann. Da kann man bis in Fachanwendungen denken, die wir selbst gebaut haben.

M. Sieber: Sie haben nun eine Lösung gewählt, mit welcher Sie direkt aus dem Acrobat Reader heraus digital signieren können. Sie leiten nach der digitalen Signatur das Dokument selbst und manuell via E-Mail an die gewünschten Empfänger weiter. Heute gäbe es auch Digital Signing Lösungen mit weiteren Funktionen, z. B. mit Workflowkomponenten, wo Sie direkt aus der Signing Applikation weitere Personen zur digitalen Signierung einladen könnten. Oder Reportingmöglichkeiten oder auch Reminderfunktionen, mit welchen Signierparteien erinnert werden, wenn sie noch nicht signiert hätten. Ist dies bei Ihnen auch ein Fokus?
GP-5: Das steht jetzt nicht unbedingt im Fokus. Wir sind da [mit der aktuell

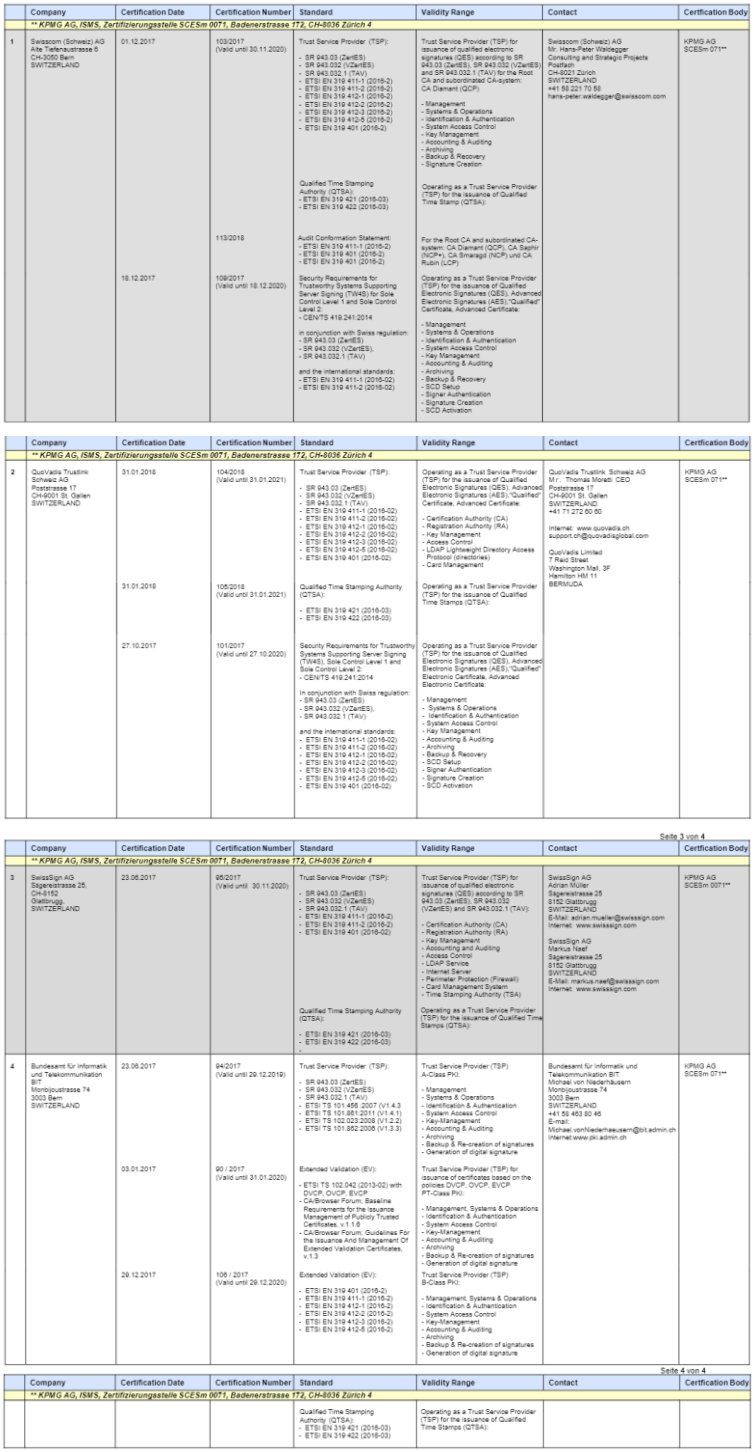
eingesetzten und schlanken Signing Lösung] in einer peripheren Tätigkeit von unseren Prozessen. Wenn wir jetzt tiefer integrieren würden, dann wird es schwieriger. Dann müsste es ganz anders integriert werden.

M. Sieber: Sie hatten auch die Geräteunabhängigkeit angesprochen. Wäre es damit für Sie auch eine Anforderung, vom Mobile aus digital zu signieren?
GP-5: Mit der Ortsunabhängigkeit, die ich erwähnt hatte, ist natürlich mitverbunden, dass ich sehr gerne Lösungen hätte, die auch mobile einsetzbar sind.

M. Sieber: Wir kommen langsam zum Abschluss des Gespräches. Jetzt wo Sie sich mit dem Thema digitale Signatur, deren Nutzung und Anschaffung intensiv beschäftigt haben, wo sehen Sie den grössten Schmerzpunkt?
GP-5: Bei der universellen und breiten Anwendung.

M. Sieber: Mit der breiten Anwendung meinen Sie die einhergehende User-Befähigung, sodass viele User die digitale Signatur einsetzen können?
GP-5: Ja, genau so habe ich die Breite gemeint.

Anhang C: Anerkannte Anbieterinnen von Zertifizierungsdiensten gemäss ZertES



	Company	Certification Date	Certification Number	Standard	Validity Range	Contact	Certfication Body
** KPMG AG, ISMS, Zertifizierungsstelle SCESm 0071, Badenerstrasse 172, CH-8036 Zürich 4							
1	Swisscom (Schweiz) AG Alte Tiefenaustrasse 6 CH-3050 Bern SWITZERLAND	01.12.2017	103/2017 (Valid until 30.11.2020)	Trust Service Provider (TSP): - SR 943.03 (ZertES) - SR 943.032 (VZertES) - SR 943.032.1 (TAV) - ETSI EN 319 411-1 (2016-2) - ETSI EN 319 411-2 (2016-2) - ETSI EN 319 412-1 (2016-2) - ETSI EN 319 412-2 (2016-2) - ETSI EN 319 412-3 (2016-2) - ETSI EN 319 412-5 (2016-2) - ETSI EN 319 401 (2016-2) Qualified Time Stamping Authority (QTSA): - ETSI EN 319 421 (2016-03) - ETSI EN 319 422 (2016-03)	Trust Service Provider (TSP) for issuance of qualified electronic signatures (QES) according to SR 943.03 (ZertES), SR 943.032 (VZertES) and SR 943.032.1 (TAV) for the Root CA and subordinated CA-system: CA Diamant (QCP): - Management - Systems & Operations - Identification & Authentication - System Access Control - Key Management - Accounting & Auditing - Archiving - Backup & Recovery - Signature Creation Operating as a Trust Service Provider (TSP) for the issuance of Qualified Time Stamp (QTSA):	Swisscom (Schweiz) AG Mr. Hans-Peter Waldegger Consulting and Strategic Projects Postfach CH-8021 Zürich SWITZERLAND +41 58 221 70 58 hans-peter.waldegger@swisscom.com	KPMG AG SCESm 071**
			113/2018	Audit Conformation Statement: - ETSI EN 319 411-1 (2016-2) - ETSI EN 319 401 (2016-2) - ETSI EN 319 401 (2016-2)	For the Root CA and subordinated CA-system: CA Diamant (QCP), CA Saphir (NCP+), CA Smaragd (NCP) und CA Rubin (LCP)		
		18.12.2017	109/2017 (Valid until 18.12.2020)	Security Requirements for Trustworthy Systems Supporting Server Signing (TW4S) for Sole Control Level 1 and Sole Control Level 2: - CEN/TS 419 241:2014 in conjunction with Swiss regulation: - SR 943.03 (ZertES) - SR 943.032 (VZertES), - SR 943.032.1 (TAV) and the international standards: - ETSI EN 319 411-1 (2016-02) - ETSI EN 319 411-2 (2016-02)	Operating as a Trust Service Provider (TSP) for the issuance of Qualified Electronic Signatures (QES), Advanced Electronic Signatures (AES) "Qualified" Certificate, Advanced Certificate: - Management - Systems & Operations - Identification & Authentication - System Access Control - Key Management - Accounting & Auditing - Archiving - Backup & Recovery - SCD Setup - Signer Authentication - Signature Creation - SCD Activation		

	Company	Certification Date	Certification Number	Standard	Validity Range	Contact	Certfication Body
** KPMG AG, ISMS, Zertifizierungsstelle SCESm 0071, Badenerstrasse 172, CH-8036 Zürich 4							
2	QuoVadis Trustlink Schweiz AG Poststrasse 17 CH-9001 St. Gallen SWITZERLAND	31.01.2018	104/2018 (Valid until 31.01.2021)	Trust Service Provider (TSP): - SR 943.03 (ZertES) - SR 943.032 (VZertES) - SR 943.032.1 (TAV) - ETSI EN 319 411-1 (2016-02) - ETSI EN 319 411-2 (2016-02) - ETSI EN 319 412-1 (2016-02) - ETSI EN 319 412-2 (2016-02) - ETSI EN 319 412-3 (2016-02) - ETSI EN 319 412-5 (2016-02) - ETSI EN 319 401 (2016-02)	Operating as a Trust Service Provider (TSP) for the issuance of Qualified Electronic Signatures (QES), Advanced Electronic Signatures (AES) "Qualified" Certificate, Advanced Certificate: - Certification Authority (CA) - Registration Authority (RA) - Key Management - Access Control - LDAP Lightweight Directory Access Protocol (directories) - Card Management	QuoVadis Trustlink Schweiz AG Mr. Thomas Moretti CEO Poststrasse 17 CH-9001 St. Gallen SWITZERLAND +41 71 272 60 60 Internet: www.quovadis.ch support.ch@quovadisglobal.com QuoVadis Limited 7 Reid Street Washington Mall, 3F Hamilton HM 11 BERMUDA	KPMG AG SCESm 071**
		31.01.2018	105/2018 (Valid until 31.01.2021)	Qualified Time Stamping Authority (QTSA): - ETSI EN 319 421 (2016-03) - ETSI EN 319 422 (2016-03)	Operating as a Trust Service Provider (TSP) for the issuance of Qualified Time Stamps (QTSA):		
		27.10.2017	101/2017 (Valid until 27.10.2020)	Security Requirements for Trustworthy Systems Supporting Server Signing (TW4S), Sole Control Level 1 and Sole Control Level 2: - CEN/TS 419 241:2014 In conjunction with Swiss regulation: - SR 943.03 (ZertES) - SR 943.032 (VZertES), - SR 943.032.1 (TAV) and the international standards: - ETSI EN 319 411-1 (2016-02) - ETSI EN 319 411-2 (2016-02) - ETSI EN 319 412-1 (2016-02) - ETSI EN 319 412-2 (2016-02) - ETSI EN 319 412-3 (2016-02) - ETSI EN 319 412-5 (2016-02) - ETSI EN 319 401 (2016-02)	Operating as a Trust Service Provider (TSP) for the issuance of Qualified Electronic Signatures (QES), Advanced Electronic Signatures (AES) "Qualified" Electronic Certificate, Advanced Electronic Certificate: - Management - Systems & Operations - Identification & Authentication - System Access Control - Key Management - Accounting & Auditing - Archiving - Backup & Recovery - SCD Setup - Signer Authentication - Signature Creation - SCD Activation		

Seite 3 von 4

	Company	Certification Date	Certification Number	Standard	Validity Range	Contact	Certfication Body
** KPMG AG, ISMS, Zertifizierungsstelle SCESm 0071, Badenerstrasse 172, CH-8036 Zürich 4							
3	SwissSign AG Sägereistrasse 25, CH-8152 Glattbrugg, SWITZERLAND	23.06.2017	95/2017 (Valid until 30.11.2020)	Trust Service Provider (TSP): - SR 943.03 (ZertES) - SR 943.032 (VZertES) - SR 943.032.1 (TAV) - ETSI EN 319 411-1 (2016-2) - ETSI EN 319 411-2 (2016-2) - ETSI EN 319 401 (2016-02) Qualified Time Stamping Authority (QTSA): - ETSI EN 319 421 (2016-03) - ETSI EN 319 422 (2016-03)	Trust Service Provider (TSP) for issuance of qualified electronic signatures (QES) according to SR 943.03 (ZertES), SR 943.032 (VZertES) and SR 943.032.1 (TAV): - Certification Authority (CA) - Registration Authority (RA) - Key Management - Accounting and Auditing - Access Control - LDAP Service - Internet Server - Perimeter Protection (Firewall) - Card Management System - Time Stamping Authority (TSA) Operating as a Trust Service Provider (TSP) for the issuance of Qualified Time Stamps (QTSA):	SwissSign AG Adrian Müller Sägereistrasse 25 8152 Glattbrugg SWITZERLAND E-Mail: adrian.mueller@swissign.com Internet: www.swissign.com SwissSign AG Markus Naef Sägereistrasse 25 8152 Glattbrugg SWITZERLAND E-Mail: markus.naef@swissign.com Internet: www.swissign.com	KPMG AG SCESm 071**
4	Bundesamt für Informatik und Telekommunikation BIT Monbijoustrasse 74 3003 Bern SWITZERLAND	23.06.2017	94/2017 (Valid until 29.12.2019)	Trust Service Provider (TSP): - SR 943.03 (ZertES) - SR 943.032.1 (TAV) - ETSI TS 101 456 2007 (V1.4.3 - ETSI TS 101 861 2011 (V1.4.1) - ETSI TS 102.023 2008 (V1.2.2) - ETSI TS 101.862 2006 (V1.3.3)	Trust Service Provider (TSP) A-Class PKI: - Management - Systems & Operations - Identification & Authentication - System Access Control - Key-Management - Accounting & Auditing - Archiving - Backup & Re-creation of signatures - Generation of digital signature	Bundesamt für Informatik und Telekommunikation BIT Michael von Niederhäusern Monbijoustrasse 74 3003 Bern SWITZERLAND +41 58 463 92 46 E-mail: Michael.vonNiederhaeusern@bit.admin.ch Internet:www.pki.admin.ch	KPMG AG SCESm 071**
		03.01.2017	90 / 2017 (Valid until 31.01.2020)	Extended Validation (EV): - ETSI TS 102.042 (2013-02) with DVCP, OVCP, EVCP - CA/Browser Forum; Baseline Requirements for the Issuance Management of Publicly Trusted Certificates, v.1.1.8 - CA/Browser Forum; Guidelines For the Issuance And Management Of Extended Validation Certificates, v.1.3	Trust Service Provider (TSP) for issuance of certificates based on the policies DVCP, OVCP, EVCP PT-Class PKI: - Management, Systems & Operations - Identification & Authentication - System Access Control - Key-Management - Accounting & Auditing - Archiving - Backup & Re-creation of signatures - Generation of digital signature		
		29.12.2017	106 / 2017 (Valid until 29.12.2020)	Extended Validation (EV): - ETSI EN 319 401 (2016-2) - ETSI EN 319 411-1 (2016-2) - ETSI EN 319 412-1 (2016-2) - ETSI EN 319 412-2 (2016-2) - ETSI EN 319 412-3 (2016-2) - ETSI EN 319 412-5 (2016-2)	Trust Service Provider (TSP) B-Class PKI: - Management, Systems & Operations - Identification & Authentication - System Access Control - Key-Management - Accounting & Auditing - Archiving - Backup & Re-creation of signatures - Generation of digital signature		

Seite 4 von 4

	Company	Certification Date	Certification Number	Standard	Validity Range	Contact	Certfication Body
** KPMG AG, ISMS, Zertifizierungsstelle SCESm 0071, Badenerstrasse 172, CH-8036 Zürich 4							
				Qualified Time Stamping Authority (QTSA): - ETSI EN 319 421 (2016-03) - ETSI EN 319 422 (2016-03)	Operating as a Trust Service Provider (TSP) for the issuance of Qualified Time Stamps (QTSA):		

Abbildung 16 Anerkannte Anbieter Zertifizierungsdienste ZertES

Quelle: (Schweizerische Akkreditierungsstelle SAS, 2021)

Anhang D: Wahrheitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig, ohne Mithilfe Dritter und nur unter Benützung der angegebenen Quellen verfasst habe und dass ich ohne schriftliche Zustimmung der Studiengangleitung keine Kopien dieser Arbeit an Dritte aushändigen werde.

Gleichzeitig werden sämtliche Rechte am Werk an die Zürcher Hochschule für angewandte Wissenschaften (ZHAW) abgetreten. Das Recht auf Nennung der Urheberschaft bleibt davon unberührt.

Unterschrift

digicert + QuoVadis
Digitally signed by
Michael Sieber
(Qualified Signature)
Date: 2021.06.23
16:46:12 +02'00'

Anhang E: Herausgabeerklärung

Erklärung zur Masterarbeit von Michael Sieber mit dem Titel:

Die digitale Signatur in der Schweiz.
Grundlagen. Kommerzielle Nutzungsanforderungen.
Bedürfnisse und Handlungsempfehlungen zur Förderung der breiten geschäftlichen Anwendung.

Die Unterzeichnenden erklären sich mit einer (allfälligen) Publikation der Arbeit, z. B. auf der Webseite der ZHAW oder eines ihrer Institute, ihrer Zentren oder mit einer anderweitigen Herausgabe

☐ Einverstanden

☒ Nur nach Rücksprache mit dem Studierenden einverstanden

☐ Nicht einverstanden

☐ Nicht einverstanden, da Vertraulichkeitserklärung vorliegend

Ort, Datum, Unterschrift des Studierenden

digicert + QuoVadis
Digitally signed by Michael Sieber (Qualified Signature)
Date: 2021.06.23 16:47:30 +02'00'

☐ Einverstanden

☐ Nur nach Rücksprache mit dem Studierenden einverstanden

☐ Nicht einverstanden

☐ Nicht einverstanden, da Vertraulichkeitserklärung vorliegend

Ort, Datum, Unterschrift der Betreuerin