KANTON JURA

E-GOUVERNEMENT & DIGITALES VERTRAUEN

VIRTUELLER SCHALTER LÖSUNG ZUR SICHERUNG ELEKTRONISCHER DOKUMENTE & VERWALTUNGSDIENSTLEISTUNGEN

„Blockchain für digitales Vertrauen in der Schweiz, basierend auf dem estnischen Modell“

WEISSBUCH

18. Januar 2021

JURA.CH
RÉPUBLIQUE ET CANTON DU JURA

egovernment
schweiz·suisse·svizzera

SOFTCOM

SICPA
Enabling trust

INHALTSVERZEICHNIS

ABKÜRZUNGEN 4
1 KONTEXT - DIE DIGITALE SCHWEIZ 5
1.1 ZIELE 6
2 EINLEITUNG - DIE BLOCKCHAIN FÜR DIGITALES VERTRAUEN IN DER SCHWEIZ, BASIEREND AUF DEM ESTNISCHEN MODELL 7
2.1. ZEITSTEMPELUNG UND DIGITALE QUITTUNG 8
2.1.1 GRUNDSATZ 8
2.1.2 DIE BLOCKCHAIN KSI 10
2.2. SICHERE BESCHEINIGUNGEN UND NACHWEISE 11
2.3. FÄLLE FÜR DIE PILOTSTUDIE 12
3 WELCHER NUTZEN 13
3.1 FÜR BÜRGERINNEN UND BÜRGER 13
3.2 FÜR RECHTSPERSONEN (UNTERNEHMEN, ORGANISATIONEN, VEREINIGUNGEN, ...) 13
3.3 FÜR DIE VERWALTUNG 14
3.4 FÜR DIE ÖFFENTLICHEN INFORMATIKDIENSTSTELLEN 14
3.5 FÜR DIE REGIERUNG 15
3.6 FÜR DIE ÖKOLOGIE 15
3.7 FÜR DIE ZUKUNFT - WANDEL AB EINER ELEKTRONISCHEN UNTERSCHRIFT 16
3.8 ZUSAMMENFASSEND 17
4 TEILEN UND VERBREITEN, ABER WIE? 18
4.1 STRATEGIE UND URSPRÜNGLICHE VISION 18
4.1.1. "PROOF OF CONCEPT" ANSATZ 18
4.1.2 "AGILER" ANSATZ 18
4.1.3 UMFASSENDERE VISION DES PILOTPROJEKTS 19
4.2 GEMEINSAME ERFAHRUNGEN 19
4.2.1 ORGANISATIONELLE DIMENSION 19
4.2.2 METHODISCHE DIMENSION 20
4.2.3 ARCHITEKTONISCHE DIMENSION 20
4.2.4 DIMENSION EINSATZ UND GEMEINSAME NUTZUNG VON RESSOURCEN 20
5. ANLEITUNG 21
5.1 ALLGEMEINER ÜBERBLICK ÜBER DIE ARCHITEKTUR 21
5.2 WAHL EINES ANWENDUNGSFALLS 22

5.2.1 FALL NR. 1 :ZEITSTEMPELUNG EINES ANTRAGS AUF BESCHEINIGUNG DER ZAHLUNGSFÄHIGKEIT 22
5.2.2 FALL NR. 2 :UNTERZEICHNUNG DER BESCHEINIGUNG MIT CERTUS-UNTERSCHRIFT 23
5.3 RISIKOMANAGEMENT UND HÄUFIGE RÜCKMELDUNGEN 25
5.3.1 "BIG DESIGN UP FRONT" 25
5.3.2 CHANCEN DES PILOTPROJEKTS 26
5.3.3 "MINIMUM VIABLE PRODUCT" 28
5.4 NUTZEN UND WEITERE ANWENDUNGEN 28
5.4.1 ERWEITERUNG AUF NICHT DOKUMENTARISCHE FÄLLE 28
5.4.2 BETRIEBLICHE FÄLLE 28
6. FAZIT 29
7. KONTAKTE 30

ABKÜRZUNGEN

Abréviation	Définition
CERTUS	Von SICPA entwickelter Service zur Sicherung des Inhalts beliebiger Dokumente mit einem fälschungssicheren QR-Code (Tamper-proof QR code)
API	Schnittstelle des Anwendungsprogramms
KSI	Name der von Guardtime entwickelten Blockchain, die das Estonian State Connection Gateway absichert
GW	Gateway
SaaS	Software als Service
IAAS	Infrastruktur als Service
PoC	„Proof Of Concept" - Machbarkeitsnachweis
PKI	Public Key Infrastructure

1 KONTEXT - DIE DIGITALE SCHWEIZ[1]

Die Digitalisierung spielt eine immer größere Rolle in unserem Leben. Dank ihres stabilen politischen Systems und ihrer hohen Innovationskraft ist die Schweiz gut aufgestellt, um das Modell einer offenen, modernen und lebenswerten Schweiz in die digitale Zukunft zu tragen. Der digitale Wandel ist der Weg zur nachhaltigen Entwicklung des Landes.

Die Strategie „Digitale Schweiz" gibt in diesem Zusammenhang die Leitlinien für das staatliche Handeln vor und zeigt auf, wie und in welchen Bereichen Behörden, Wirtschaft, Wissenschaft, Zivilgesellschaft und politische Akteure zusammenarbeiten sollen, damit die Schweiz von diesem Wandel voll profitieren kann.

STRATEGIE

Der Bundesrat wünscht sich, dass die Schweiz die Möglichkeiten, die mit der Digitalisierung einhergehen, bestmöglich nutzt. Deswegen hat er am 11. September 2020 die Strategie „Digitale Schweiz“ verabschiedet. Die Digitalpolitik der Bundesregierung muss in Zukunft verstärkt auf Umwelt- und Datenaspekte achten.

Das in diesem Dokument vorgestellte Pilotprojekt wird von E-Government Schweiz unterstützt, da es Teil der Umsetzung der Schweizer Strategie für E-Government 2020-2023 ist [2].

[1] https://www.digitaldialog.swiss/de/

[2] https://www.egovernment.ch/files/7916/0863/6097/Plan-de-mise-en-oeuvre_2021_F.pdf

1.1 ZIELE

Der Bundesrat hat die Gewährleistung von Sicherheit, Vertrauen und Transparenz als Kernziel Nr. 2 definiert und wie folgt formuliert: „*In der Schweiz müssen sich Menschen in der virtuellen Welt genauso sicher bewegen können wie in der realen Welt und vor digitalem Missbrauch und ungerechtfertigter Verfolgung geschützt sein. Transparente und datengesteuerte Dienstleistungen schaffen Vertrauen und respektieren die persönliche Entwicklung und Selbstbestimmung*."

Auch der Bundesrat hat die Reduzierung des ökologischen Fußabdrucks als Kernziel Nummer 5 definiert*: „Die Digitalisierung kann einen entscheidenden Beitrag dazu leisten, dass die Schweiz ihre Klima- und Umweltziele erreicht. Damit dies geschieht, dürfen Energie- und Materialverbrauch der Informations- und Kommunikationstechnologien (IKT) nicht im Gleichschritt mit dem zunehmenden Einsatz dieser Technologien wachsen. Sie sind verstärkt und gezielt zu nutzen, um den Energie- und Materialverbrauch in allen Lebens- und Arbeitsbereichen zu senken und den Klima- und Umweltschutz zu verbessern*."

E-Government Schweiz hat auch mehrere Ziele für die Umsetzung der Strategie E-Government 2020-2023 festgelegt. Das Ziel Nimmer 16 betrifft die Förderung innovativer Projekte. Das vorliegende Projekt wird in diesem Rahmen unterstützt. Innovative Projekte können „wegweisend sein und als Modell für andere Projekte dienen oder von anderen Verwaltungen übernommen und angewendet werden". Mit diesem Weißbuch können sich andere Organisationen mit dem verwirklichten Pilotprojekt vertraut machen.

2 EINLEITUNG - DIE BLOCKCHAIN FÜR DIGITALES VERTRAUEN IN DER SCHWEIZ, BASIEREND AUF DEM ESTNISCHEN MODELL

Der Kanton Jura erforscht und evaluiert in seiner „Vision zu digitalem Vertrauen“ der öffentlichen Hand technologische Innovationen, die diese Vision und die Annahme der Einrichtung eines nachhaltigen Raums für Vertrauen durch alle unterstützen können.

Seit mehreren Jahren entwickeln die Unternehmen SICPA und Guardtime neue Technologien für digitale Integrität, die auf der KSI-Blockchain beruhen. Diese Lösungen, wie z.B. die Zeitstempelung, eine digitale Unterschrift der neuen Generation oder die Sicherung offizieller Dokumente (CERTUS), ermöglichen die Umsetzung einer vertrauenswürdigen E-Government-Strategie. Die vorgeschlagenen Lösungen beruhen auf digitalen Technologien, die in Estland entwickelt wurden und die seit 2008 für die Sicherung der Abläufe der estnischen Regierung genutzt werden, vor allem die Blockchain KSI von Guardtime[3]. Es wird darauf hingewiesen, dass Estland als Vorreiter in Sachen Digitalisierung, das seit 2008 Zeitstempel auf der KSI-Blockchain verwendet, derzeit eine dieser neuesten Technologien (CERTUS) untersucht, sie aber noch nicht implementiert hat.

Das vorliegende Projekt schlägt vor, das estnische Modell der digitalen Integrität auf den kantonalen Virtuellen Schalter anzuwenden und darüber hinauszugehen, indem die neuesten Technologien von SICPA und Guardtime integriert werden, insbesondere bei der Umsetzung der Sicherheit von Bescheinigungen und offiziellen Dokumenten. In diesem Zusammenhang und mit Unterstützung von E-Government Schweiz wurde, basierend auf den Erfahrungen des estnischen Modells, im Kanton Jura ein Pilotprojekt für *eine ökologische private Blockchain für digitales Vertrauen in der Schweiz gestartet (Kanton Jura).*

So verfügt jede Bürgerin und jeder Bürger des Jura über eine „Kundenumgebung“, in der er oder sie Dokumente, die ihn oder sie betreffen, mit der Verwaltung austauschen kann. So können Bürgerinnen und Bürger Dokumente bei der Verwaltung einreichen und in gleicher Weise wird die Verwaltung ihnen Dokumente oder Bescheinigungen ausstellen. Derzeit basiert dieses System auf dem Vertrauen der Bürger in die Sicherheit und Integrität der staatlichen Computersysteme. Wenn es jedoch über eine digitale Transaktion zu einer Streitigkeit zwischen Bürger und öffentlicher Hand kommt, wäre es für den Bürger sehr schwierig, wenn nicht sogar unmöglich, ohne die aktive Mitarbeit der staatlichen Dienste seinen guten Glauben nachzuweisen.

Im Rahmen der „Vision digitales Vertrauen" ist das erste Ziel dieses Projekts, eine Lösung vorzuschlagen, die es dem Bürger ermöglicht, durch die Einführung einer „digitalen Quittung“ die vollständige Souveränität über seine Daten und seine digitalen Interaktionen mit dem Staat zu haben. Außerdem wird der Staat in der Lage sein, die Integrität der Daten, für die er verantwortlich ist oder die sich in seinem Gewahrsam befinden, jederzeit zu beweisen und jedem Bürger zu ermöglichen, diesen Beweis unabhängig vom Staat zu überprüfen.

3 Die folgenden, von der estnischen Regierung verfassten Dokumente beschreiben die Verwendung der KSI-Blockchain durch die estnische Regierung und Verwaltung

- https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf
- https://e-estonia.com/wp-content/uploads/2020mar-nochanges-faq-a4-v03-blockchain-1-1.pdf

Beim zweiten Ziel des Projekts handelt es sich um die Sicherung der Integrität und Herkunft der Bescheinigungen, die vom Staat ausgestellt werden, auch wenn die Bürger die Bescheinigung ausdrucken. Die Daten werden nicht geteilt und auch nicht nach außen hin kommuniziert. Sie bleiben zu jeder Zeit auf den staatlichen Servern und somit ist die Privatsphäre der Bürgerinnen und Bürger bauartbestimmt völlig geschützt.

Eines der Ziele dieses Projekts ist auch und vor allem die Bestätigung, dass diese Innovation problemlos auf alle Behördendienste ausgeweitet werden kann, da die zugrunde liegenden Technologien generisch sind.

Dieses Modell, das im Rahmen dieses Projekts validiert wurde, wird auch für andere Verwaltungen von Nutzen sein, da es Projekt alle Elemente liefert, die die Replizierung dieser Vorteile ermöglichen, wobei die grundlegende Infrastruktur sehr schnell erweiterbar ist.

Bei den beiden Dienstleistungen dieses Pilotprojekts handelt es sich um folgende:

- Zeitstempelung und digitale Quittung;
- Sichere Bescheinigungen und Nachweise;

Beide Dienstleistungen werden nachfolgend erläutert.

2.1. ZEITSTEMPELUNG UND DIGITALE QUITTUNG

Die erste Lösung für digitales Vertrauen, die in diesem Pilotprojekt untersucht wird, ist die Zeitstempelung, d.h. die Gewährleistung der Integrität eines digitalen Ereignisses, wie z.B. eines Downloads oder einer Entscheidung, indem eine digitale Quittung fälschungssicher gemacht wird.

2.1.1 GRUNDSATZ

Typische Probleme, die mit Zeitstempeln zu lösen sind, sind in den folgenden Szenarien beschrieben[4]:

1. *Ein Bürger reicht seine Steuererklärung elektronisch am Virtuellen Schalter (in seinem persönlichen Dokumentenbereich) ein. Er tut dies kurz vor Ablauf der Frist, um 23:55 Uhr. Dieser Bürger möchte sicher sein, dass sein Dokument registriert wurde und einen unwiderlegbaren Beweis dafür haben, dass er es rechtzeitig eingereicht hat (wie der Poststempel, der als Nachweis gilt). Außerdem möchte der Bürger irgendwann später nachweisen können, dass er die Gehaltsbescheinigung als Nachweis beigefügt hat.*
2. *Dieser Bürger erhält eine Aufforderung des Finanzamtes, seine Steuererklärung in digitaler Form in seinem persönlichen Dokumentenbereich abzugeben. Der Staat möchte garantieren (und damit beweisen) können, dass dieses Dokument tatsächlich zu einem bestimmten Datum zugestellt wurde, genauso wie bei einem Einschreiben.*

Die Lösung, die für die oben beschriebenen Probleme vorgeschlagen wird, besteht darin, dass jeder „Upload“ von Daten auf der KSI-Blockchain mit einem Zeitstempel versehen wird.

[4] Diese Szenarien sind fiktiv und sind möglicherweise nicht in allen Organisationen relevant. Sie ermöglichen jedoch, sich möglicherweise typische Anwendungsfällen vor Augen zu führen.

Konkret passiert am Virtuellen Schalter folgendes: Sobald ein Dokument heruntergeladen wird (entweder vom Bürger oder von der Verwaltung), wird der Fingerabdruck (der Hash) dieses Dokuments an den lokalen KSI-Blockchain-Server (der z. B. im Rechenzentrum der kantonalen Verwaltung installiert ist) „gesendet“, um mit einem Zeitstempel versehen zu werden. Eine Sekunde später sendet der KSI-Blockchain-Server die KSI-Unterschrift, die den „Zeitstempel“ auf der KSI-Blockchain darstellt, an den Server des Virtuellen Schalters zurück. Diese KSI-Unterschrift, die als „digitale Quittung“ des Dokuments dient, wird im persönlichen Dokumentenbereich neben dem gerade hochgeladenen Dokument gespeichert. Diese digitale Quittung wird dem Bürger (oder der Verwaltung) zur unabhängigen Überprüfung zur Verfügung stehen, wie in *Abbildung 1* dargestellt.

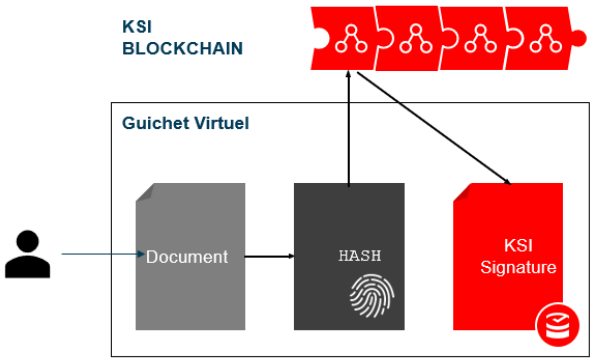

Abbildung 1: Unveränderliche Quittung des digitalen Fingerabdrucks eines Dokuments auf der Blockchain

Diese digitale Quittung (KSI-Unterschrift) ermöglicht folgende Nachweise:

- Integrität des Dokuments: Es kann nachgewiesen werden, dass es sich um das Originaldokument handelt, das mit einem Zeitstempel versehen wurde - wird das Dokument auch nur geringfügig verändert (z. B. ein Buchstabe), entspricht dieses Dokument nicht mehr der KSI-Unterschrift.
- Zeitstempelung: auf die Sekunde genauer Zeitpunkt der Zeitstempelung, die unmöglich im Nachhinein geändert werden kann.
- Aussteller der KSI-Unterschrift: Dies ist der Nachweis, dass diese KSI-Unterschrift tatsächlich von der kantonalen Verwaltung ausgestellt wurde - dies verhindert, dass jemand eine andere KSI-Unterschrift desselben Dokuments zu einem anderen Zeitpunkt von einer anderen Identität auf der KSI-Blockchain (die nicht notwendigerweise die der kantonalen Verwaltung sein wird) erstellt.

Jeder Bürger kann sich in seinen persönlichen Dokumentenbereich einloggen und die verschiedenen Dokumente mit der entsprechenden KSI-Unterschrift herunterladen. So ist der Bürger unabhängig vom Virtuellen Schalter (und damit vom Staat) dazu in der Lage, die Integrität und die Zeitstempelung seiner Dokumente (die er aufgegeben oder von der Verwaltung erhalten hat) nachzuweisen. Die Überprüfung der Integrität von Dokumenten anhand der KSI-Unterschrift erfolgt mit Hilfe einer universellen Anwendung, deren Quellcode öffentlich zugänglich ist. So können alle Bürgerinnen und Bürger oder alle Institutionen ihre eigene Verifizierungsanwendung erstellen, ohne von der öffentlichen Hand abhängig zu sein. Der Staat kann seinerseits seine in den Virtuellen Schalter integrierte Kontrollversion aus Gründen der Einfachheit und des leichten Zugangs zur Verfügung stellen.

2.1.2 DIE BLOCKCHAIN KSI

Die KSI-Blockchain wird ausschließlich als „Vertrauensanker“ verwendet, der es ermöglicht, die Integrität von Daten zu garantieren und nachzuweisen, ohne dass diese Daten die Server der öffentlichen Hand verlassen. Die KSI-Blockchain steht den von ihr gesicherten Anwendungen und Daten neutral gegenüber. Damit ist die KSI-Blockchain, die seit 2008 die digitale Welt in Estland sichert, potenziell für die Sicherung aller Transaktionen weltweit im Sekundentakt verfügbar und ausgelegt. Die Infrastruktur ist so bereits vorhanden und es besteht keine Notwendigkeit, unter gleichzeitiger Sicherung der Privatsphäre eine Ad-hoc-Blockchain für die Bedürfnisse des Kantons Jura neu zu errichten.

Abbildung 2 unten zeigt die verschiedenen Kennzeichen der KSI-Blockchain.

Abbildung 2: Kennzeichen der KSI-Blockchain

Die wichtigsten Punkte:

- Die Daten werden weder geteilt noch Dritten gegenüber offengelegt. Sie bleiben zu jeder Zeit auf den staatlichen Servern und somit ist die Privatsphäre der Bürgerinnen und Bürger bauartbestimmt völlig geschützt;
- Die KSI-Blockchain ist umweltfreundlich, da sie nicht auf Proof of Work-Konsensalgorithmen basiert. Es fällt also kein besonderer Stromverbrauch an (im Gegensatz zum Bitcoin). Zum Vergleich: Die Anzahl der Server der KSI-Blockchain, die die Integrität von Daten weltweit und aus ganz Estland sichern, liegt unter der der IT-Dienste des Kantons Jura;
- Die KSI-Blockchain ist nicht an eine Kryptowährung gebunden und unterliegt daher keiner Volatilität. Daher ist der Preis eines Zeitstempels fest und bekannt und stellt kein Betriebsrisiko dar;

- Alle auf der KSI-Blockchain gesicherten Informationen sind unabhängig von der Infrastruktur, die diese Blockchain betreibt, überprüfbar. Jeder Eigentümer eines Zeitstempels (sei es der Bürger oder der Staat) ist in der Tat im Besitz seiner entsprechenden KSI-Signatur (d.h. seines „digitalen Belegs“). Diese Quittung bleibt universell überprüfbar, auch für den Fall, dass die KSI-Blockchain nicht mehr existiert. Diese Eigenschaft ist sehr wichtig, da sie garantiert, dass jedes Dokument mit einem Zeitstempel versehen und verifizierbar bleibt, auch über einen sehr langen Zeitraum, egal was mit dieser Blockchain, ihrer Infrastruktur oder ihrem Betreiber passiert.

Es muss darauf hingewiesen werden, dass diese KSI-Blockchain bereits im April 2008 für die ersten Piloten der estnischen Regierung in Betrieb war, ein paar Monate vor der Veröffentlichung von Satoshi Nakamotos Bitcoin-Weißbuch.

2.2. SICHERE BESCHEINIGUNGEN UND NACHWEISE

Das Ziel dieser zweiten Komponente des Projekts kann wie folgt dargelegt werden:

> *Ein Bürger beantragt eine Bescheinigung (z. B. eine Bescheinigung des Betreibungsregisters) zur Vorlage bei einer Verwaltungsgesellschaft, um eine Wohnung zu mieten. Derzeit wird diese Bescheinigung in Papierform erstellt und von der Verwaltung unterschrieben und abgestempelt. Für den Fall, dass dieses Zertifikat auch in digitaler Form (z.B. als PDF-Dokument) zur Verfügung gestellt werden kann, muss die Verwaltung die Möglichkeit haben, schlüssig zu prüfen, dass dieses Dokument im Original vorliegt und von der öffentlichen Hand ausgestellt wurde. Wenn der Bürger diese PDF-Datei ausdruckt, muss die Verwaltung außerdem sicher sein können, dass es sich bei dieser auf Papier gedruckten Bescheinigung tatsächlich um eine „echte Kopie“ des amtlichen Dokuments handelt und dass sie nicht gefälscht sein kann.*

SICPA hat einen einzigartigen Online-Service (CERTUSTM) für die Sicherung von Inhalten von Dokumenten, wie Nachweisen, Bescheinigungen, Kennungen, Qualifikationen, entwickelt, wobei ein QR-Code[5] verwendet wird. Dieser QR-Code wird durch eine kryptografische Verbindung mit einem sicheren Validierungssiegel auf der KSI-Blockchain KSI überprüft. Dank dieses auf dem Dokument angebrachten QR-Codes werden die Schlüsselinformationen des Dokuments gesichert, unabhängig davon, ob es sich um ein digitales oder ein Papierdokument handelt. Im Papierformat ist der Begriff des Originaldokuments daher nicht mehr wichtig, da der CERTUS-Dienst die Integrität der Daten und nicht deren Medium garantiert.

Darüber hinaus ist auch die Herkunft des Ausstellers garantiert und universell prüfbar, so dass sichergestellt ist, dass das Dokument von einer legitimen Stelle gesichert wurde. Der "zertifizierte" konforme Inhalt des Dokuments kann von jedem mit einem einfachen Smartphone überprüft werden, entweder über eine Webanwendung (Web App) oder eine Mobiltelefonanwendung (Mobile App), indem der sichere QR-Code gescannt wird. Der Aussteller hat auch die Möglichkeit, den Lebenszyklus dieses Dokuments zu verwalten, mit der Möglichkeit, die Informationen zu beenden, zu widerrufen oder zu reaktivieren.

5 Gegenwärtig handelt es sich bei dem Format um einen QR-Code, da diese Methode in der Welt weit verbreitet ist, aber das schließt andere Formate nicht aus. Je nach Studienfall kann auch ein anderes Format gewählt werden

Es ist zu beachten, dass die Verifizierungsanwendung keinen Zugriff auf eine Datenbank und noch weniger auf den Kundenbereich des Bürgers haben muss. Tatsächlich sind alle Daten in den sicheren QR-Code eingebettet (ohne Verschlüsselung) und es wird nur die Verknüpfung mit dem zeitgestempelten Verifizierungsschlüssel (sicheres digitales Siegel) auf der KSI-Blockchain überprüft. Daher kann dieser QR-Code, wie auch die KSI-Blockchain, unabhängig von jeglicher Infrastruktur verifiziert werden, ohne dass eine Verbindung bestehen muss. Diese Dienstleistung ist konform mit den Datenschutzbestimmungen (DSGVO).

Die folgende *Abbildung 3* zeigt das Prinzip von mit CERTUS gesicherten Dokumenten am Beispiel eines Auszugs aus dem Betreibungsregister. Der Text ist durch den QR-Code gesichert, der wiederum durch eine Verknüpfung mit der KSI-Blockchain gesichert ist. Wird der QR-Code mit einem Smartphone gescannt, werden die Echtheit des Dokuments ebenso wie der Inhalt des Dokuments bestätigt.

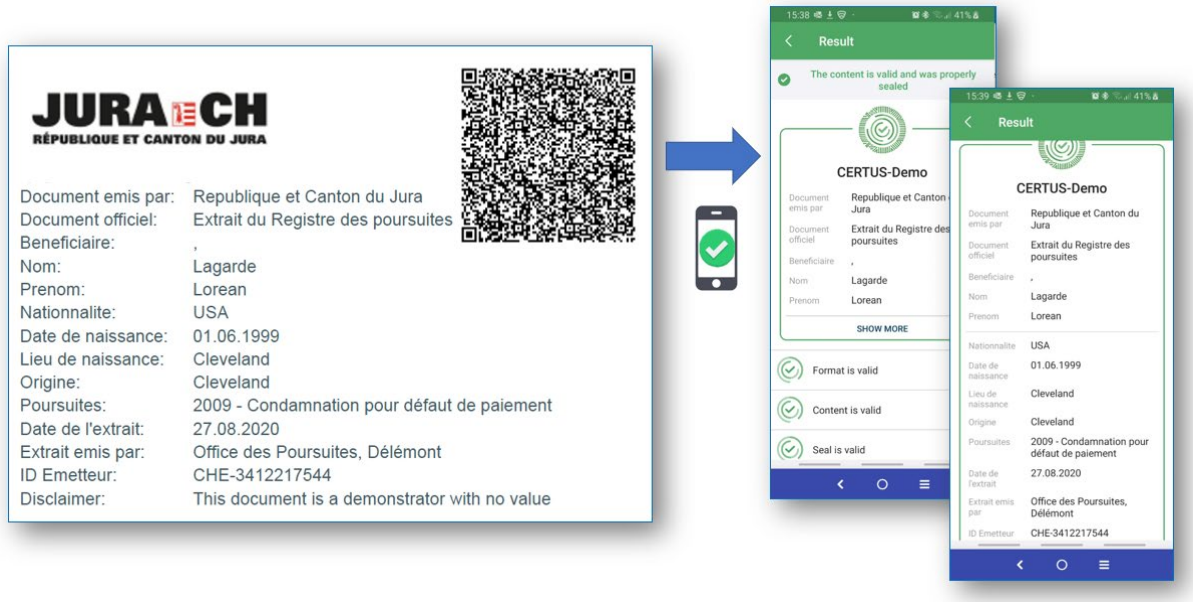

Abbildung 3 - Beispiel eines CERTUS gesicherten Dokuments - Auszug aus dem Betreibungsregister.

Die vorgeschlagene Lösung besteht darin, in den Virtuellen Schalter die Möglichkeit einzubauen, diese sicheren QR-Codes zu generieren (durch Aufruf der entsprechenden APIs) und ihn auf den zu sichernden Dokumenten anzubringen (Bescheinigungen oder Nachweise; z. B. ein Auszug aus dem Betreibungsregister, ein Angelschein, eine Eigentumsurkunde, ein Personenstandsdokument usw.). Der Dienst wird im SaaS-Modus angeboten.

2.3. FÄLLE FÜR DIE PILOTSTUDIE

Die schließlich für das Pilotprojekt ausgewählte Fallstudie besteht in der Absicherung des Antragsprozesses für die Bestätigung der Zahlungsfähigkeit. Konkret wird die Anforderung einer Bestätigung der Zahlungsfähigkeit durch den Bürger mit einem Zeitstempel (*KSI Timestamping*) gesichert, während die vom Betreibungsamt ausgestellte und dem Bürger im PDF-Format zugesandte Bescheinigung mit dem CERTUS-Dienst gesichert wird.

Dieses Pilotprojekt wird daher ein größeres digitales Vertrauen für die Bürger schaffen, indem es unabhängige, widerstandsfähige und ökologische digitale Sicherheitslösungen implementiert und gleichzeitig das Dateneigentum respektiert.

3 WELCHER NUTZEN

Die Entwicklung einer „Vision für digitales Vertrauen“ zielt darauf ab, Dienstleistungen und/oder deren Nutzen für alle oder einige der Beteiligten und Begünstigten zu verbessern.

3.1 FÜR BÜRGERINNEN UND BÜRGER

- Gesteigertes Vertrauen in den Virtuellen Schalter und die Online-Dienste der öffentlichen Hand:
  - „Ich habe die Integrität meiner digitalen Daten unter Kontrolle“;
  - „Ich habe eine ‚digitale Quittung', mit der ich meinen guten Glauben nachweisen kann, unabhängig vom Staat und seinem Computersystem"

- Vereinfachung meiner Kontakte mit der öffentlichen Verwaltung:
  - „Meine Verwaltungsangelegenheiten sind jetzt einfacher zu erledigen, da ich jederzeit und rund um die Uhr meine sicheren Bescheinigungen und Nachweise in digitaler Form abrufen, und sogar ausdrucken, kann“.

- Bereitstellung von Echtzeit-Diensten zur Beschaffung von offiziellen Originaldokumenten „inhärent“.

3.2 FÜR RECHTSPERSONEN (UNTERNEHMEN, ORGANISATIONEN, VEREINIGUNGEN, ...)

- Wesentliche Abläufe sind vereinfacht und können nachgewiesen werden:
  - Die Hinterlegung eines wichtigen Dokuments im Portal kann den Versand eines Einschreibens ersetzen[6] (dank des Zeitstempels und der digitalen Quittung, die das Einschreiben der Post ersetzt).

- Mehr Vertrauen in die vom Bürger eingereichten Dokumente und Beschleunigung der Abläufe:
  - „Als Hausverwalter kann ich einen Auszug aus dem Betreibungsverzeichnis per E-Mail erhalten und dessen Authentizität in wenigen Sekunden überprüfen.

- Weniger Betrug:
  - Ein Betrüger wird nicht in der Lage sein, eine vom Staat über den Virtuellen Schalter ausgestellte Bescheinigung zu fälschen. Dank CERTUS kann das E-Dokument genauso gesichert werden, wie die Version auf Papier. Eine Fälschung der Papierversion ist daher ebenfalls ausgeschlossen.

6 In Fällen, in denen ein Einschreiben nicht gesetzlich vorgeschrieben ist (in der Tat gilt der KSI-Zeitstempel in der Schweiz derzeit noch nicht als erweiterter oder qualifizierter Stempel).

3.3 FÜR DIE VERWALTUNG

- Beschleunigung von Verwaltungsabläufen und Reduzierung von Kosten und Verzögerungen:
  - Rückgang der Ausgabe von Papierdokumenten, durch verstärkte Nutzung des Virtuellen Schalters (angesichts des zunehmenden Vertrauens von Bürgerinnen und Bürgern);
  - Automatisierung der Erstellung von amtlichen Dokumenten für Bürger, die weniger Kontrollschritte erfordern.

- Nachweis, der Rechtsstreitigkeiten vermeiden kann:
  - Der Staat kann sofort beweisen, dass eine Handlung zu einem bestimmten Zeitpunkt stattgefunden hat und dass das Dokument dem Original entspricht.
  - Zeitersparnis bei der Suche nach den Punkten, die eine Anfrage rechtfertigen (die Nachweise sind direkt verfügbar und in wenigen Sekunden überprüfbar).

3.4 FÜR DIE ÖFFENTLICHEN INFORMATIKDIENSTSTELLEN

- **Vertrauen „durch das Design“ für die IT-Stellen**[7]: Da alle auf die Plattform hochgeladenen Dokumente mit einem Zeitstempel versehen sind, kann kein Verdacht aufkommen, dass ein Systemtechniker ein Dokument oder die zugehörigen Metadaten (absichtlich oder aus Versehen) verändert hat.

- **Geringerer Zeitaufwand für die Prüfung von Datensicherheit und -integrität**: Es können Skripts entwickelt werden, die regelmäßig überprüfen, dass jedes E-Dokument der entsprechenden KSI-Unterschrift entspricht. Wenn keine auffälligen Kontrollen vorliegen, kann bestätigt (und damit nachgewiesen) werden, dass kein Dokument geändert oder gefälscht[8] wurde, d.h. Verstärkung der Cybersicherheit mit Verhinderung von böswilligen Eingriffen.

- **Einfache, generische und „anpassbare“ Umsetzung,** (siehe Kapitel „Umsetzung“):
  - Zeitstempelung (KSI-Timestamping):
    - Das KSI-Gateway, das auf den Servern des Kantons installiert werden kann, ermöglicht eine Erweiterung der Zeitstempelung auf alle kantonalen Verwaltungsdokumente (beachten Sie, dass die KSI-Blockchain eine theoretische weltweite Kapazität von 1012 Zeitstempeln pro Sekunde hat);
    - Die Implementierung des Zeitstempels erfolgt über Rest-APIs zu einem auf den Servern des Kantons installierten Webservice, der die genannten Funktionen aufruft;
  - Sichere Bescheinigungen & Nachweise (CERTUS):
    - Diese Lösung ist im SaaS-Modus und über Rest-API zugänglich. Auf den Servern des Kantons ist keine besondere Installierung erforderlich.

7 Diese Art von Szenario ist glücklicherweise sehr unwahrscheinlich, dennoch muss es erwähnt werden

8 Im Stadium dieses Pilotprojekts wird vorgeschlagen, nur die „Datenintegrität“ durch KSI-Zeitstempel durchzuführen. In einem späteren Pilotprojekt wird es möglich sein, eine Schicht „Prozessintegrität“ hinzuzufügen, die sicherstellt (und beweist), dass ein Dokument nach einem definierten Ablauf erstellt wurde und nicht durch ein anderes ersetzt werden konnte (oder dass es nicht gelöscht wurde). Dieser Dienst garantiert, dass die Daten nach einem sicheren, offiziellen Verfahren erstellt, geändert, transportiert und gelöscht wurden. Es handelt sich um eine zusätzliche Dienstleistung.

- **Interoperabilität**: Da die KSI-Blockchain nur als „Vertrauensanker" dient, liegt die Interoperabilität auf der Anwendungsebene, so wie sie heute funktioniert. Das bedeutet, dass bestehende Anwendungen nicht großartig angepasst oder verändert werden müssen. Sie müssen nur die Aufrufe zu den entsprechenden API's hinzufügen.
- **Erweiterung für die digitale Transformation der Verwaltung:** Die Technologien, die im Rahmen dieses Pilotprojektsauf dem virtuellen Schalter implementiert werden (KSI-Zeitstempelung & Dokumente durch sichere Siegel) sind für jeden öffentlichen oder privaten Dienst anwendbar. In der Tat, im Prozess der digitalen Transformation der Verwaltung des Kantons Jura, wurden bereits der Bedarf an interner Validierung und Zertifizierung für Dokumente und Entscheidungsabläufe identifiziert.
- SLA-Backed: Die ausgewählten Technologien wurden von vertrauenswürdigen Schweizer Unternehmen, einem fast hundertjährigen KMU bereitgestellt.

3.5 FÜR DIE REGIERUNG

- **Vertrauen**: Die angewandten Technologien werden das Vertrauen der Bürger in ihre Verwaltung und Regierung erhöhen. Damit wird die Transparenz des Staates erhöht und die Umsetzung der „Vision digitales Vertrauen“ ermöglicht, die der Bund in seiner Strategie „Digitale Schweiz“ formuliert hat.
- **Datenschutz**: Es werden keine Daten vom öffentlichen Server umgeleitet, um auf der Blockchain mit einem Zeitstempel versehen zu werden. Der Datenschutz ist somit inhärent gewährleistet.
  Kostensenkung: Da digitale Integrität ein Mittel zur digitalen Vertrauenssteigerung ist, wird sie dazu beitragen, die Akzeptanz des Virtuellen Schalters zu erhöhen. In ähnlicher Weise wird der Ersatz von Papiernachweisen und Bescheinigungen durch sichere digitale Äquivalente die Kosten für deren Ausstellung durch Automatisierung reduzieren. Estland meldet diesbezüglich Einsparungen in Höhe von 2% des BIP dank der sicheren Digitalisierung ihrer Dienstleistungen.[9]
- **Bessere Dienstleistungen für die Bevölkerung**: Der Ersatz von handsignierten Papierbescheinigungen durch eine digitale oder sichere Papierversion wird zu einem verbesserten Dienst für die Bevölkerung führen. So kann der Bürger eine Bescheinigung sofort, von zu Hause aus, in wenigen Minuten erhalten, und muss nicht zum physischen Schalter der Verwaltung gehen oder einen Tag warten, bis seine Bescheinigung zum Beispiel per Post ankommt.

3.6 FÜR DIE ÖKOLOGIE

- Die vorgeschlagenen Lösungen (wie oben beschrieben), die auf Gegenseitigkeit beruhen und keine Kompromisse bei der Sicherheit und Unabhängigkeit eingehen, erzeugen im Gegensatz zu anderen ähnlichen Blockchain-Technologien, die auf anderen Konsensmodellen basieren und auf Kryptowährungen indiziert sind, keinen übermäßigen Stromverbrauch.
- Es bedarf keiner zusätzlichen Infrastruktur, um diese Lösungen auf alle Schweizer E-Governments (Kantone, Bund und Gemeinden) auszuweiten.

9 https://e-estonia.com/global-digital-society-fund/

3.7 FÜR DIE ZUKUNFT - WANDEL AB EINER ELEKTRONISCHEN UNTERSCHRIFT

Die KSI-Blockchain-Zeitstempel-Lösung stellt zusammen mit der Dokumentenzertifizierung durch CERTUS die nächste Generation der Daten- und Dokumentensicherheit dar. Die oft gestellte Frage lautet, inwieweit sich das von der digitalen Unterschrift eines Dokuments (PKI)[10] unterscheidet.

Die „herkömmliche“ digitale Unterschrift von Dokumenten basiert auf der seit vielen Jahren existierenden PKI-Kryptotechnik. PKI basiert auf einem privaten Schlüssel (der von seinem Besitzer geheim gehalten und geschützt werden muss) und einem öffentlichen Schlüssel, der über ein Zertifikat mit der Identität des Unterzeichners verbunden ist. Jedes Paar aus privatem und öffentlichem Schlüssel muss einer eindeutigen Person (oder einem eindeutigen Server) zugeordnet sein, um mit Sicherheit feststellen zu können, wer der Unterzeichner ist. Für den Einsatz in einer Institution wie z. B. einer öffentlichen Verwaltung kann die Verwaltung (Ausgabe, Erneuerung, Widerruf oder Löschung) dieser Schlüssel und der zugehörigen Zertifikate knifflig sein und zu Problemen oder Sicherheitsverletzungen führen (Kompromittierung oder Verlust eines Schlüssels, Widerruf eines Zertifikats beim Ausscheiden eines Mitarbeiters usw.). Außerdem haben diese Zertifikate eine begrenzte Lebensdauer und daher kann auch die Lebensdauer der entsprechenden Signaturen begrenzt sein, weswegen diese dann erneuert werden müssen.

Darüber hinaus kann die Validierung solcher Unterschriften und die Zuordnung der Signatur zu ihrem Urheber zu Verifizierungen führen, die für eine Durchschnittsperson nicht einfach sind. Um einige dieser Einschränkungen oder Schwächen zu überwinden, haben Signaturanbieter Methoden entwickelt, die erfordern, dass den jeweiligen Betreibern vertraut wird. Dies kann ein Problem für eine Unterschriftenvalidierung in mehreren Jahren oder in einem anderen Land darstellen, das sich der Vertrauenswürdigkeit dieses Betreibers nicht unbedingt sicher sein kann.

Die KSI-Blockchain wurde erfunden und entwickelt, um die Schwachstellen und die komplexe Verwaltung von öffentlichen/privaten Schlüsseln und zugehörigen Zertifikaten zu beheben, die für PKI erforderlich sind. Konstruktionsbedingt trägt eine KSI-Unterschrift (das Ergebnis eines Zeitstempels auf der KSI-Blockchain) automatisch die "Unterschrift" (oder Identität), von der die Signatur erstellt wurde, sowie die Identität (oder Kennung) des Unterzeichners, ohne dass öffentliche und private Schlüssel verwaltet werden müssen. Diese Unterschrift ist unbegrenzt gültig und kann universell von jedem, überall auf der Welt verifiziert werden, ohne dass man dabei einem Dritten, einem Betreiber oder gar KSI sein Vertrauen schenken muss. Außerdem kann ein KSI-Zeitstempel auf jede Art von Dokument angewendet werden, während eine herkömmliche digitale Signatur derzeit nur auf PDF-Dokumenten Einsatz findet. Die Möglichkeit, jede Art von Dokument (und damit auch jede Art von Daten) zu signieren, wird in Zukunft sicherlich sehr wichtig sein, um nicht nur Daten, sondern auch Abläufe zu sichern.

10 A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption – *source en.wikipedia.org › wiki › Public_key_infrastructure*

Ein CERTUS-Siegel (das die Integrität eines Dokuments garantiert) ist ebenfalls durch einen Zeitstempel gesichert und hat damit die gleichen Integritätseigenschaften wie eine KSI-Unterschrift. Es gelten daher die Unterscheidungsmerkmale zwischen einem "CERTUS-signierten" Dokument und einer herkömmlichen digitalen Signatur (PKI-Typ). Ein weiterer Vorteil von CERTUS liegt darin, dass es ausgedruckt werden kann (in Form seines QR-Codes). So ist es möglich, ein Papierdokument mit digital signierten Daten zu haben, was bei einer digitalen Signatur vom Typ PKI unmöglich ist (bei der nur die PDF- und damit digitale Version eine gültige und überprüfbare Unterschrift trägt).

3.8 ZUSAMMENFASSEND

Im Rahmen dieses Projekts wird sich der Großteil des Ökosystems, und damit seine Nutznießer und Akteure positiv entwickeln, um die Vision des digitalen Vertrauens zu stärken. Dieses Projekt zeigt eine Reihe von wichtigen Vorteilen für alle Verwaltungsdienste auf.

Die vorgeschlagenen Lösungen sind dahingehend inklusiv, dass alle Bürgerinnen und Bürger von ihnen profitieren können. Die gesicherten Dokumente sind in der Tat sowohl auf Papier als auch elektronisch überprüfbar.

4 TEILEN UND VERBREITEN, ABER WIE?

4.1 STRATEGIE UND URSPRÜNGLICHE VISION

Jedes wie auch immer geartete Projekt, muss auf eine Vision und Ziele ausgerichtet sein. Über das „Warum“ hinaus müssen die Vision und die Ziele das „Wie“ mit dem Ansatz zur Umsetzung in Einklang bringen.

Bei den für die Umsetzung dieses Pilotprojekts festgehaltenen Zielen handelt es sich um folgende:

- **Innovative Lösungen,** die dem Bürger **vollständige Souveränität über seine Daten und seinen Austausch mit der öffentlichen Hand erteilen**;
- Sicherung **der Integrität und Herkunft** der von öffentlicher Stelle ausgestellten Bescheinigungen, **auch in Papierform.**

4.1.1 „PROOF OF CONCEPT“-ANSATZ

Der Ansatz des Pilotprojekts ist ***Proof of Concept (PoC)*** basiert. Dies ist aufgrund folgender Aspekte erforderlich:

- Disruptive Aspekte der Blockchain-Technologie im Kontext einer öffentlichen Verwaltung;
- Bedeutung der Notwendigkeit von Popularisierung und Vertrauensaufbau bei Stakeholdern;
- Bedeutung des Vertrauensaspekts, der durch den Einsatz der Blockchain-Technologie gelöst werden soll;
- Kontinuierliche Anpassung und Verfeinerung der Lösungsarchitektur;
- Kontinuierliche Anpassung und Verfeinerung der ausgewählten Anwendungsfälle;
- Ermöglichte Steigerung der technischen und funktionalen Kompetenz aller Akteure des Pilotprojekts.

Zusammenfassend lässt sich sagen, dass das Hauptziel des Proof of Concept darin besteht, sowohl die technologischen Aspekte der Lösung als auch das Verständnis für die funktionalen Probleme, die die KSI-Blockchain und die CERTUS-Sicherheit mit sich bringen, zu entschärfen. Das Pilotprojekt sollte den verschiedenen Interessengruppen eine klarere Vorstellung von den möglichen Anwendungsfällen für die eingesetzten Technologien vermitteln.

4.1.2 „AGILER“ ANSATZ

Unter agilem Vorgehen verstehen wir ein iteratives und inkrementelles Vorgehen. Von jeglicher Methodik abgesehen war es das Ziel, eine „learn as we go“-Kultur in die Umsetzung dieses Pilotprojekts zu bringen.

Da es sich bei diesem Projekt um den ersten Schritt einer Sicherung größeren Ausmaßes handelt, war es wichtig, die Akteure auf einen gemeinsamen und pragmatischen Ansatz auszurichten, um nicht in den klassischen „Big Design Up Front“ Ansatz zu verfallen.[11]

11 https://en.wikipedia.org/wiki/Big_Design_Up_Front

4.1.3 UMFASSENDERE VISION DES PILOTPROJEKTS

Von Beginn des Projekts an war eine Umsetzung auf Grundlage des Proof of Concept geplant. Sie wird auf den Ergebnissen der Proof-of-Concept-Phase aufbauen. Ihr geht eine Übergangsphase voraus, in der die Beobachtungen und Erfahrungen aus der Proof-of-Concept-Phase abgeglichen werden.

Abbildung 4 - Die wichtigsten Phasen

Die Umsetzung des Pilotprojekts in einem isolierten und definierten Funktionsbereich (Dokumentenstrom) wird die erste direkte Wertschöpfung für den Bürger darstellen. Sie wird uns die Auswirkungen und Vorteile für den Endbenutzer (den Bürger und die mit ihm interagierenden Stellen) aufzeigen.

Die Umsetzung ist auch als solche eine Wiederholung einer Vision von globaler Sicherheit für die Interaktion zwischen Staat und Bürgern auf einer höheren Ebene. Letztendliches Ziel ist es, Transparenz und Vertrauen für den Bürger, aber auch für Unternehmen bei ihren jeweiligen Beziehungen zum Staat zu schaffen.

4.2 GEMEINSAME ERFAHRUNGEN

4.2.1 ORGANISATIONELLE DIMENSION

Das Pilotprojekt wurde in Zusammenarbeit mit vier Akteuren verwirklicht:

- **E-Government Schweiz**, die Schweizer Agentur, die für die Unterstützung der Schweizer E-Government-Strategie für Bund, Kantone und Gemeinden zuständig ist;
- **Der Integrator,** *Softcom Technologies S.A.*, Integrator der Lösungen *Guardtime* und *SICPA;*
- **Der vertrauenswürdige Dienstleister,** *SICPA S.A.*, Dienstleister für *KSI*- und *CERTUS*-Zeitstempelung;
- **Der Kunde**, Informatikdienst des Kantons Jura (SDI).

Es wurde ein regelmäßiger und fester Iterationsrhythmus zwischen den Akteuren definiert, der es erlaubt, die entstandenen Inkremente zu teilen, schnell Entscheidungen zu treffen, um den Umfang abzustimmen und auf die festgestellten Abweichungen/Fehlausrichtungen zu reagieren, sowohl auf funktionaler als auch auf technologischer Ebene.

4.2.2 METHODISCHE DIMENSION

Wie oben beschrieben, haben die „Proof of Concept“- und „agilen" Ansätze die Akteure natürlich dazu gebracht, einen iterativen und inkrementellen Ansatz zu bevorzugen, der in 4 verschiedene Phasen unterteilt ist:

- **Phase 1: Funktionale und technische Studie**
  Initiale Phase, die es ermöglicht, die erste Vision des Projekts in Bezug auf funktionale Anforderungen (ausgewählte Anwendungsfälle) und nicht-funktionale Anforderungen (Technologie, Lösungsarchitektur) festzulegen.
- **Phase 2: Umsetzung der Infrastruktur**
  Es gibt mehrere Möglichkeiten zur Umsetzung der Infrastruktur. Mehrere Gespräche waren erforderlich, um die letztendlich verwendete Möglichkeit festzulegen.
- **Phase 3: Umsetzung des Dokumentenstroms**
  Die tatsächliche Implementierung der Anwendungs- und Software-Komponenten, die verwendet werden, um den gewünschten Wert für den Proof of Concept zu erzeugen. Der Kunde führt kontinuierlich Funktionstest durch.
- **Phase 4: Kommunikation, Schulung und Wissensübertragung** Abschließende Projektphase. Realisierung von globalen Kommunikationsaspekten.

4.2.3 ARCHITEKTONISCHE DIMENSION

Der Proof-of-Concept-Modus zielt darauf ab, sich auf die neuen Elemente zu konzentrieren, bei denen zusätzliche Fähigkeiten notwendig und wichtig sind, um alle Aspekte erfassen zu können, die eine fundierte Auswahl für eine Produktionseinführung ermöglichen. Als Ergebnis lässt sich die Architekturstrategie durch die folgenden Entscheidungen zusammenfassen:

- Begrenzt die Auswirkungen auf die bestehende Architektur, indem Komponenten hinzugefügt werden, die die derzeit vorhandenen Elemente außer Acht lassen;
- Hinzufügung von unterstützenden Bestandteilen, die für die Durchführung der Anwendungsfälle für das Proof of Concept erforderlich sind;
- Iterative Verfeinerung der Architektur.

4.2.4 DIMENSION EINSATZ UND GEMEINSAME NUTZUNG VON RESSOURCEN

Die anfängliche Projektvision sah in Bezug auf die Ressourcen die Installation der gesamten notwendigen Infrastruktur auf dem Gelände des Kunden vor (On Premise Modus).

Es wurde schnell beschlossen, diesen Aspekt im Proof-of-Concept fallenzulassen, um sich hauptsächlich auf die Anwendungs- und Funktionsaspekte konzentrieren zu können. Daher wurde die Entscheidung getroffen, die Lösungsbestandteile im Saas-Modus (*Software-as-a-Service*) zu nutzen und die folgenden von SICPA zur Verfügung gestellten Komponenten zu verwenden:

- Einsatz der CATENA-Middleware, die eine globale Anwendungskomponente bereitstellt und auch eine Datenbank integriert. Dank der Verwendung der Middleware (anstelle des SDKs) konnten wir uns von der Arbeit an der Infrastrukturimplementierung befreien, die für den Proof-of-Concept nicht entscheidend war;
- Verwendung von SAAS CERTUS für die Verwaltung der CERTUS-Unterschriften.

5. ANLEITUNG

In diesem Kapitel sind die wesentlichen Elemente beschrieben, die zum Erfolg dieses Pilotprojekts geführt haben.

5.1 ALLGEMEINER ÜBERBLICK ÜBER DIE ARCHITEKTUR

Die für das Proof of Concept eingerichtete Architektur wird hiernach beschrieben:

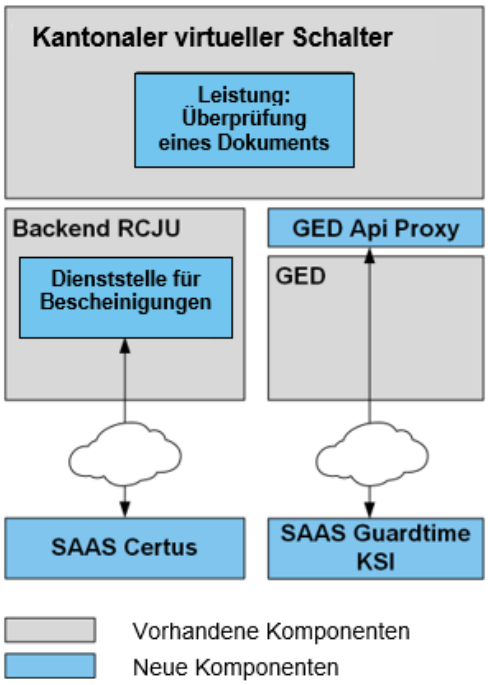

Abbildung 5 – Hochwertige Lösungsarchitektur

Die vom PoC verwendete Architektur besteh aus folgenden Teilen:

- **Dienstleistung „Ein Dokument überprüfen“**: die Dienstleistung des Virtuellen Schalters, die dem Bürger zur Verfügung gestellt wird, um die für ihn bestimmten Dokumente zu überprüfen (Siehe Punkt 6.3.2.2);
- **EDV Api Proxy**, Proxy auf der EDV-Komponente, für die Bearbeitung der KSI-Unterschriften der Dokumente, die dies erfordern;
- **Dienstleistung Nachweise**, zusätzliche Komponente, die die Wiederintegration der Bestätigung der Zahlungsfähigkeit in den digitalen Fluss ermöglicht (EDV);
- **SAAS Certus**, Unterschriftendienst von Sicpa, Verwendung im SAAS-Modus;
- **SAAS Guardtime KSI**, Zeitstempelungsdienst von KSI Guardtime, Verwendung im SAAS-Modus

5.2 WAHL EINES ANWENDUNGSFALLS

Die Wahl eines Anwendungsfalls ist von wesentlicher Bedeutung. Die Herausforderung besteht darin, einen relativ einfachen Anwendungsfall zu verwenden, der gleichzeitig aussagekräftig ist und einen effizienten Dokumentenfluss im Rahmen der Beziehung zwischen dem Bürger und dem Staat darstellt.

Des Weiteren ist es schwierig, sowohl den Zeitstempel als auch die Certus-Signatur verwenden zu können. Die beiden gewählten Anwendungsfälle werden nachstehend erläutert.

5.2.1 FALL NR. 1: ZEITSTEMPELUNG EINES ANTRAGS AUF BESCHEINIGUNG DER ZAHLUNGSFÄHIGKEIT

Der Kanton Jura bietet bereits seit einigen Jahren einen virtuellen Schalter an, der es den Bürgern ermöglicht, über digitale Dienste mit dem Staat zu interagieren. Eine der erbrachten Dienstleistungen betrifft die Bestätigung der Zahlungsfähigkeit. Das nachstehende Schaubild erklärt den **gegenwärtigen** Ablauf des Antrags auf Bestätigung der Zahlungsfähigkeit:

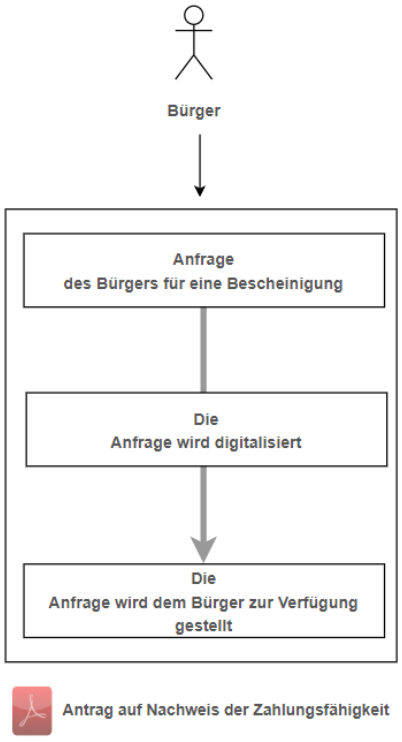

Abbildung 6 - Gegenwärtiger Ablauf

Dieser Anwendungsfall wurde zur Veranschaulichung der von KSI bereitgestellten Zeitstempel-Funktionalität gewählt. In diesem Zusammenhang hat die Zeitstempelfunktionalität nach seinem Antrag auf Bestätigung der Zahlungsfähigkeit **den Wert einer Quittung für den Bürger**.

Der **gewählte** Anwendungsfall wird nachstehend kurz zusammengefasst:

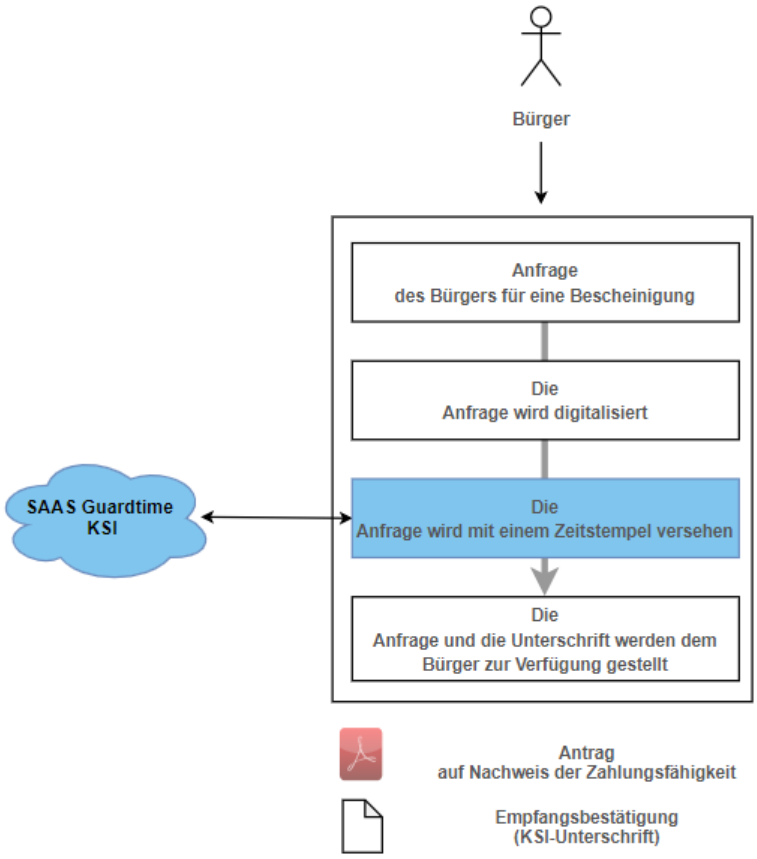

Abbildung 7 - Zielablauf

Der geplante Zielprozess hat ein zusätzliches Element: **den Zeitstempel der gescannten Anfrage**. Diese Zeitstempelung wird mit der SAAS Catena DB Plattform (SAAS Guardtime KSI) durchgeführt, bevor das Dokument zur Verfügung gestellt wird. Die Signatur, die sich aus dem Zeitstempel ergibt, hat die Form einer Quittung der Anfrage.

5.2.2 FALL NR. 2: UNTERZEICHNUNG DER BESCHEINIGUNG MIT CERTUS-UNTERSCHRIFT

Es ist darauf hinzuweisen, dass dieser Anwendungsfall eine Fortsetzung von Anwendungsfall 1 ist. Sie stellt einen kompletten funktionalen Arbeitsablauf dar (Antrag durch den Bürger, Bereitstellung durch den Staat). Das ist wichtig, denn so war die Konzentration auf einen einzigen Bereich der Wertschöpfung möglich und mussten nicht mehrere verschiedene funktionale Themen verwaltet werden, wodurch der Fokus auf den Zielen des Pilotprojekts lag.

Die Ausstellung der Bescheinigung der Zahlungsfähigkeit durch den Staat ist ein Prozess, der aus überwiegend menschlichen Handlungen besteht. Abbildung 5 zeigt die gegenwärtigen Schritte dieser Ausstellung:

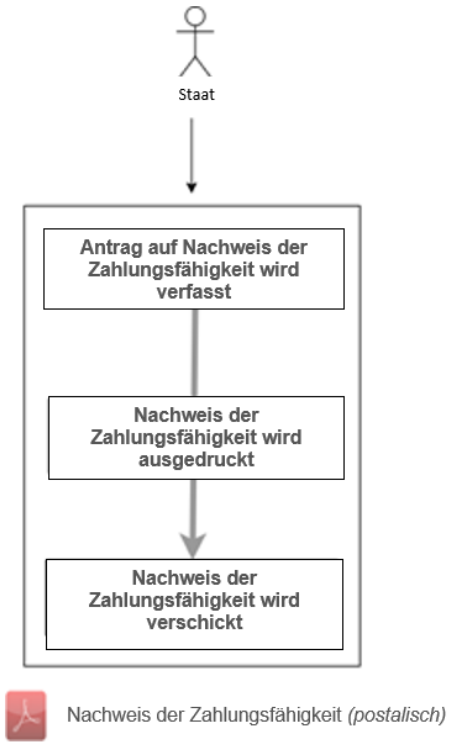

Abbildung 8 - Gegenwärtiger Ablauf für die Ausstellungen einer Bescheinigung der Zahlungsfähigkeit

Die Schritte der Ausstellung sind hiernach beschrieben:

- Die zuständige Dienststelle wird per Mail über den eingegangenen Antrag informiert;
- Der Mitarbeiter der Dienststelle stellt die Bescheinigung anhand eines Word Dokuments aus;
- Das Dokument wird ausgedruckt und mit der Post an den Antragsteller geschickt.

Es ist zu beachten, dass die Bescheinigung der Zahlungsfähigkeit in ihrer jetzigen Form nicht in den EDV-Dokumentenfluss eingeht (im Gegensatz zum Antrag nicht in EDV eingestellt wird). Dies ist wichtig, da im Rahmen des PoC die Bonitätsauskunft in den Standardfluss integriert werden muss. Eine zusätzliche Komponente wird implementiert (Dienst Bescheinigungen), um die Reintegration der Bescheinigung in einen digitalen Workflow zu verwalten.

Die nachstehende Abbildung veranschaulicht den Zielablauf:

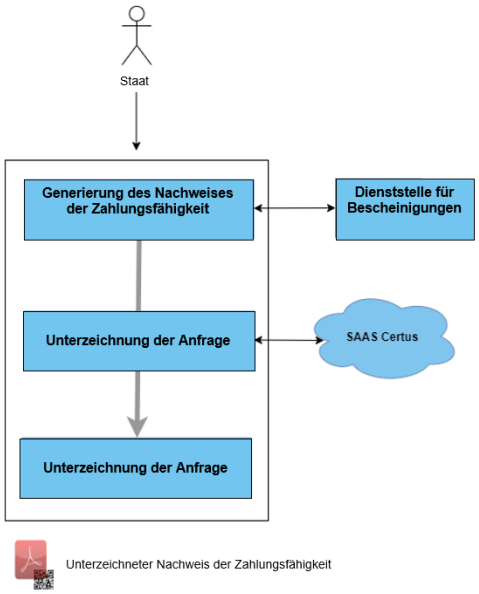

Abbildung 9 - Zielablauf der Ausstellung einer Bescheinigung der Zahlungsfähigkeit

Im Vergleich zum gegenwärtigen Ablauf gibt es folgende Unterschiede:

- Der Mitarbeiter der Dienststelle generiert die Bescheinigung anhand der neuen Komponente „Dienst Bescheinigungen“;
- Sobald das Dokument (digital) validiert ist, wird es über die Certus-Plattform unterzeichnet;
- Die Bescheinigung wird dem Bürger in seinem Dokumentenfach zur Verfügung gestellt.

5.3 RISIKOMANAGEMENT UND HÄUFIGE RÜCKMELDUNGEN

Das Konzept des häufigen und regelmäßigen Feedbacks zu den vom Projekt produzierten Inkrementen, das von agilen Ansätzen gefördert wird, war ein sehr effektives Instrument zur Risikominderung. In der Tat hat sich der Reifegrad der verschiedenen Akteure während des Projekts deutlich weiterentwickelt, was den „Proof-of-Concept“-Ansatz de facto validiert.

Im Rahmen des „Learn-as-you-go“-Ansatzes haben die zwischen den Akteuren ausgetauschten Aspekte einen globalen Kompetenzzuwachs und vor allem eine Verfeinerung und den Austausch der Themen auf höherem Niveau ermöglicht.

5.3.1 „BIG DESIGN UP FRONT“

„Herkömmliche“ architektonische Ansätze haben sich, vor allem aus Bequemlichkeit, oft in einem "Up Front"-Modus befunden. Darunter ist ein Ansatz zu verstehen, bei dem alle Details der Architektur (technisch und funktional) von Anfang an definiert sind. Man sollte jedoch nicht zögern, gegen den Strom zu schwimmen und sich für einen aufstrebenden Ansatz entscheiden, der wiederum von agilen Praktiken favorisiert wird. Die

sukzessiven Iterationen der getroffenen Entscheidungen sowie die Tatsache, dass man auf diese Entscheidungen zurückkommen konnte, ermöglichten eine Umsetzung, die sich sehr eng an die Realität hielt und gleichzeitig den Umfang der dem Pilotprojekt gewidmeten Ressourcen respektierte.

5.3.2 CHANCEN DES PILOTPROJEKTS

Mit dem Fortschreiten des Pilotprojekts wurde das Projektteam immer versierter in den Technologien rund um die KSI-Blockchain. Die Möglichkeit, zwei ursprünglich nicht geplante Funktionen hinzuzufügen, wurde untersucht und genehmigt, da sie im Rahmen der Projektressourcen durchgeführt werden konnte. Das Projekt brachte also zwei zusätzliche Anwendungsfälle auf die Endanwenderebene:

Die Validierung aller Dokumentarten, die von der öffentlichen Hand ausgestellt werden;

Die Hinzufügung eines Links im Dokumentbereich des Bürgers für jedes Dokument, damit der Bürger die KSI-Unterschrift des jeweiligen Dokuments einsehen und bestätigen kann.

Diese beiden Anwendungsfälle wurden durch einen neuen Dienst im kantonalen Virtuellen Schalter umgesetzt.

DIE VALIDIERUNG ALLER DOKUMENTARTEN, DIE VON DER ÖFFENTLICHEN HAND AUSGESTELLT WERDEN

Die Dienstleistung ***Überprüfung eines Dokuments*** wurde eingerichtet, damit der Bürger eine visuelle Kontrollmöglichkeit hat. Die Dienstleistung ist über zwei Einstiegspunkte zugänglich:

Über den Link auf den Dokumenten im Dokumentbereich des Bürgers;

Direkt über die Dienstleistung, durch die Hinterlegung des zu überprüfenden PDF.

Abbildung 10 - Schnittstelle der Ablage der zu überprüfenden PDF-Datei

Abbildung 11 - Schnittstelle des Überprüfungsergebnisses

HINZUFÜGUNG EINES LINKS AUF DEN DOKUMENTEN DES BÜRGERS

Um es den Bürgern einfacher zu machen, wurde im Dokumentbereich des Bürgers für jedes Dokument ein Link eingefügt. Dieser Link bietet direkten Zugriff auf den Validierungsdienst für das gewählte Dokument, der folgende Screenshot veranschaulicht diese Funktionalität:

Abbildung 12 - Schnittstelle Dokumentverwaltung für den Bürger

5.3.3 „MINIMUM VIABLE PRODUCT“

Das gesamte Projekt wurde als Produktentwicklung durchgeführt. Daher wurde der Minimalansatz mit dem Ziel verfolgt, nur die am meisten erwarteten Funktionen im Einklang mit der Vision und den Zielen zu produzieren (MVP-Modus). Die Einzelheiten wurden diskutiert und als ein Punkt aufgenommen, der zu einem späteren Zeitpunkt behandelt und verfeinert werden soll. Auf diese Aspekte wird zu gegebener Zeit und wenn es der Kontext erfordert (Übergangsphase, Produktionsstart) eingegangen.

5.4 NUTZEN UND WEITERE ANWENDUNGEN

Dieses Pilotprojekt wird den Bürgern konkrete Lösungen bieten und so zur Stärkung des digitalen Vertrauens beitragen. Es ermöglicht ihnen, den Mehrwert zu verstehen und Feedback zu geben. Dieses Projekt hat zu den folgenden Überlegungen über mögliche Funktionserweiterungen geführt, wobei auch die Ergebnisse und Beobachtungen der Bürger berücksichtigen werden sollten:

5.4.1 ERWEITERUNG AUF NICHT DOKUMENTARISCHE FÄLLE

Das Zeitstempeln und Signieren von Dokumentenflüssen ist der offensichtlichste Anwendungsfall für die Nachvollziehbarkeit und Integrität digitaler Elemente. Auf der anderen Seite hat es die gewonnene Reife der Projektbeteiligten ihnen ermöglicht, sich eine Vielzahl von Nutzungsmöglichkeiten vorzustellen, darunter:

- Staatliche Transparenz beim Umgang mit Bestandteilen, die dem Bürger gehören (Zugang, durch wen und warum, zu Daten, die dem Bürger gehören);
- Integration des von CERTUS bereitgestellten Workflow-Modus in bestehende Abläufe (Erstellung, Stornierung und Widerruf von Unterschriften);
- Erweiterung auf andere Partner der öffentlichen Hand (Vereinigungen, Rechtspersonen, usw.)

5.4.2 BETRIEBLICHE ANWENDUNGSFÄLLE

- Die Verwendung von Zeitstempeln auf operativen digitalen Bestandteilen (digitale Artefakte, Konfigurationen usw.) würde es außerdem ermöglichen, nicht nur die funktionalen Aspekte, sondern auch alle Operationen des Infrastrukturmanagements im weitesten Sinne zu sichern.
- Auch könnten die dem Kanton von verschiedenen Anbietern zur Verfügung gestellten Leistungen digital signiert werden, wodurch die Integrität dieser Leistungen für den Kanton gewährleistet wäre.

6. FAZIT

Das Pilotprojekt zeigte auf pragmatische und konsequente Weise, wie der Kanton Jura in seiner „Vision für digitales Vertrauen“ des Staates in einem ersten konkreten Szenario innovative Lösungen zum Nutzen von Bürgern, juristischen Personen, der Verwaltung, ihren IT-Diensten und der Regierung umgesetzt hat.

Der in diesem Pilotprojekt verwendete Ansatz und die technologischen Lösungen erreichten auch das Ziel, den Nutzen der Ausweitung der Erfahrungen des Pilotprojekts auf andere Bürgeranfragen, die über den virtuellen Schalter des Kantons gestellt werden, zu zeigen, d.h. die Sicherung der Anfrage mittels Zeitstempelung (KSI Timestamping) und die Sicherung, wenn der Anwendungsfall es erfordert, der offiziellen Dokumente über CERTUS.

Auf der Grundlage eines Modells, das durch das vorliegende Pilotprojekt im Kanton Jura inspiriert wurde, sind die verschiedenen beteiligten Partner in der Lage, den Einsatz von KSI-Zeitstempeln und Dokumentensicherheit über CERTUS zu implementieren und zu verallgemeinern.

Dank der in diesem Projekt vorgeschlagenen zusätzlichen Dienste, wie z.B. CERTUS, werden die Daten UND Dokumente der Bürger und des Staates vor möglichen betrügerischen Manipulationen und unberechtigtem Zugriff geschützt. Während der Umsetzung dieses Projekts und dieser ersten Rückmeldungen sind Kommunikation und die Fähigkeit, neue Technologien und ihre Vorteile für alle Akteure, vom Bürger bis zum Entscheidungsträger, klar und einfach zu erklären, ein wesentlicher Punkt, um digitales Vertrauen zu fördern. Daher wurde mit der Erstellung von Kommunikationsmaterial begonnen, um das Verständnis und die Annahme der Umsetzung eines nachhaltigen Vertrauensraums, insbesondere im Hinblick auf den ökologischen Fußabdruck, durch alle zu unterstützen. In der Tat unterstützen diese neuen Dienste die Digitalisierung von Dienstleistungen, ohne einen zusätzlichen Kohlenstoff-Fußabdruck zu hinterlassen. Die Digitalisierung von Dienstleistungen reduziert die Notwendigkeit, Papierdokumente zu drucken und zu transportieren.

Wie in Estland[12] wird die KSI-Blockchain Technologie genutzt, um die Datenintegrität und die Integrität der öffentlichen Systeme zu stärken. Digitales Regieren erlangt strategische Bedeutung, um die Wettbewerbsfähigkeit eines Landes zu verbessern und das Wohlbefinden der Bevölkerung zu steigern. Es geht dabei darum, einen Staat zu schaffen, der transparent rund um die Uhr funktioniert. Der Schutz persönlicher digitaler Daten ist zweifelsohne der Dreh- und Angelpunkt für den Aufbau von Vertrauen in die virtuelle Verwaltung eines Staates.

Für den Kanton Jura sind die geplanten Anwendungen zwar sehr breit gefächert und müssen noch genau definiert werden, aber sie sollten es ermöglichen, Sicherheit und Transparenz in der Arbeitsweise des Staates und Effizienz in den erbrachten Dienstleistungen zu gewährleisten, indem sie sich auf die Technologie stützen, um noch mehr Vertrauen zu schaffen.

In Zukunft wird es möglich sein, diese Dienste auf alle Entscheidungsprozesse auszuweiten und so die Eindeutigkeit, Nachvollziehbarkeit und Authentizität von Entscheidungen auf transparente Weise zu gewährleisten.

12 99% der estnischen Dienste sind online verfügbar.

7. KONTAKTE

Kanton Jura:

Matthieu Lachat
Dienstleiter
matthieu.lachat@jura.ch
+41 32 420 5900

David De Groote
Verantworlicher E-Government
david.degroote@jura.ch
+41 32 420 5900

SICPA SA:

Marco Aloe
Director Integrity Solutions
Marco.Aloe@sicpa.com
+41 21 627 5555

Softcom Technologies SA:

Philippe Zimmermann
Verantwortlicher für den eGov-Markt
philippe.zimmermann@softcom.pro
+41 26 422 80 90