Einordnung der BDR Zeugnislösung

Autor-. [redacted]

Beantwortung der Fragen

1. *Gibt es aus Ihrer Sicht Hinderungsgründe, das Zeugnissystem der Bundesdruckerei für digitale Zeugnisse einzusetzen, in Bezug auf:*

Datenschutz und IT-Sicherheit

Eine abschließende Begutachtung kann auf Basis der gesichteten Dokumente nicht abgegeben werden. Es wird empfohlen, hier zuerst das entsprechende Anforderungs-Papier des BSI abzuwarten, welches sich momentan in Erstellung befindet. Dann sollte die vorliegende Lösung, bzw. das Konzept für eine hierauf aufbauende Lösung auf Einhaltung durch eine unabhängige Stelle überprüft werden. Auch sollte dann hierbei entsprechende Prüfung des IT-Sicherheitskonzeptes und des Quellcodes durch Unabhängige Dritte erfolgen.

Darüber hinaus sollte die Aussage das in der „Blockchain“ keine personenbeziehbaren Daten liegen durch eine Prüfung von Datenschützern oder Vorlage eines durch die zuständigen Datenschützer (AK Technik bzw. AK Schule?) anerkanntes Gutachten validiert werden.

Einsatz der Blockchain

Grundsätzlich stellen DLTs eine gute Möglichkeit dar, um eine Validierung von Claims durchzuführen, ohne dass die ausstellende Institution in diesen Prozess involviert ist. In der vorliegenden Lösung ist dieser Mehrwert aber ab absurdum geführt da, die Blockchain als Private Blockchain ausgeführt ist und nur über eine als Gatekeeper funktionierende API zugänglich ist. Positiv ist zu bewerten das eine standardisierte Blockchain zum Einsatz kommt, welche die spätere Interoperabilität erleichtert.

Auch ist zumindest kritisch zu hinterfragen, ob die Blockchain der richtige Platz ist um die Trusted Issuer Registry zu führen (siehe Anhang).

Grundsätzlich ist zu bemerken, dass auch Blockchain-freie Lösungen (PKI Infrastruktur) in der Lage wären, die Anforderungen einer Zeugnislösung zu erbringen.

Neben der Frage: „Muss es eine Blockchain sein?“, die mit: „Kann, nicht aber muss“ beantwortet werden, muss noch die Frage beantwortet werden: „Muss es diese Blockchain sein?“. Hier ist die Auswahl der proprietären Blockchain von GovDigital insbesondere mit Hinblick auf Nachhaltigkeit, Vendor-Lockin und Zugänglichkeit zwar mit Blick auf einen Prototyp nachvollziehbar, eine hinreichende Analyse von alternativen Lösungen mit Blick auf einen dauerhaften Betrieb fehlt hier (bspw. Nutzung von EBSI, und zwar als primäre Infrastruktur, nicht als zusätzlicher Layer/Interoperabilität) . Grundsätzlich ist dabei eine offene Lösung zu bevorzugen, wobei mit Blick auf den Ressourcenverbrauch nur solche Lösungen in Betracht gezogen werden sollten die über ein ProofOfAuthority oder vergleichbare Mechanismen verfügen.

Mindestens die Verifikation von Zeugnissen sollte dabei dezentral und ohne Einbeziehung Dritter möglich sein. Hier sollte ein öffentlicher Lesezugriff auf die Chain möglich sein, genauso wie ein dezentraler Betrieb der notwendigen Softwarekomponenten. Dies ist bei der vorliegenden Lösung nicht gegeben.

Erstellung der Zeugnisse

Dass die Zeugnisse maschinenlesbare Informationen enthalten, ist ein zwingendes Kriterium von Digitalen Nachweisen, welches in der vorliegenden Variante erfüllt ist. Mittelfristig werden sich voraussichtlich

Hier ist zwar eine Standardisierung im Sinne des beschreibenden Standards (ELMO) vorgesehen, die genaue Ausgestaltung ist aber momentan nicht definiert. Dies erhöht zwar die Flexibilität und damit ggf. die Adaptionsgeschwindkeit und Rate erschwert aber die Nutzung. Daher ist eine landesübergreifende semantische Vereinheitlichung perspektivisch wünschenswert.

Darüber hinaus ist das kommunizierte Finanzierungsmodell insofern es richtig verstanden wurde (PayPerUse) als problematisch zu bewerten, da es hinderlich für eine breite Adaption der Lösung ist. Somit ist davon auszugehen, dass die Lösung eine Insellösung wird, neben der sich andere Lösungen etablieren werden. Dies ist im Zweifelsfall nachteilig für das Nutzendenerlebnis.

Übergabe der Zeugnisse

Der analoge Prozess der Übergabe der Zeugnisse mit anschließenden Download ist funktionabel. Es sollte aber geprüft werden, ob der Prozess noch vereinfacht werden kann (insbesondere Reduzierung der Prozessschritte).

Da die begutachtete Lösung auch für weitere Leikas verwendet werden soll (bspw. erneute Ausstellung) sollte dieser Prozess noch dargestellt werden.

Validierung der Zeugnisse

Das Zweistufige Verfahren (Signiertes PDF und ELMO Daten) ist funktional. Mittelfristig mit weiterer Verbreiterung von Wallets und SSI wird es eher auf VCs mit daraus abgeleiteten visuellen Repräsentationen hinauslaufen.

Authentifizierung der Schulen

Siehe hierzu → Anhang, Versteckte Register Funktionalitäten

2. *Gibt es aus Ihrer Sicht Gründe, die gegen den langfristigen Betrieb des Zeugnissystems der Bundesdruckerei sprechen?*

Wie unter 1 geschildert gibt es momentan mehrere Gründe:

- Fehlende Validierung durch einen der größten Verwender (SfH)
- Fehlende Prüfung der IT Sicherheit (siehe 1)
- Keine Wirtschaftlichkeitsanalyse, insbesondere im Vergleich zu anderen Lösungen
- Geschlossenheit des Systems

3. Gibt es aus Ihrer Sicht Hinderungsgründe das Zeugnissystem der Bundesdruckerei für weitere Zeugnisarten zu nutzen?

Wie unter 1 geschildert, gibt es momentan mehrere Gründe:

- Finanzierungsmodell
- Geschlossenheit des Modells

Insbesondere fehlt eine Analyse der Akzeptanz durch Hochschulen und die dortigen CaMS Anbieter.

Anhang

Versteckte Register-Funktionalitäten

Die von der BDR vorgestellte Lösung beinhaltet zwei Komponenten, die als Register-Funktionalitäten zu verstehen sind und die dediziert betrachtet werden müssen.

Zum einen beinhaltet die Lösung eine dauerhafte Speicherung der Zeugnisse. Diese findet verschlüsselt statt, die Zeugnisse können dann mit dem Schlüssel der Schule oder der nächsten obergeordneten Instanz entschlüsselt werden. Grundsätzlich ist es zu begrüßen, dass die Zeugnisse nur verschlüsselt vorgehalten werden, da dies den möglichen Missbrauch und auch Sicherheitsrisiken minimiert. Allerdings gibt es keine technologischen und fachlichen Gründe, die hier für eine produktseitige Verschränkung sprechen.

Die enthaltene Zeugnisablage ist als optionaler Service der BDR zu bewerten. Während es der BDR freisteht dieses als Dienst anzubieten, sollte dies unabhängig vom OZG geschehen, und es muss möglichen sein diesen Dienst nicht zu nutzen oder einen eigenen Dienst hierfür zu nutzen.

Grundsätzlich bleibt auch zu fragen, was der gewünschte Mehrwert ist, und ob basierend hierauf nicht gilt einen eigenständigen Dienst zu konzipieren. Hierbei ist auch zu klären ob nicht alternative Ansätze zu evaluieren sind. Reicht es bspw. das erstellte Dokument zu archivieren, oder muss ein neues Ausstellen ggf. auch mit anderen Formaten möglich sein was alleine auf Grundlage des alten Dokumentes nicht mehr möglich ist. Und wenn es nur um das Aufbewahren geht, was ist mit Ansätzen solche Dokumente als Immutables in dem Servicekonto eines Nutzenden zu speichern. Da dies jedoch auch komplexe Vorhaben sind die ggf. Änderungen im juristischen Raum benötigten sollte dies nicht durch die Hintertür eingeführt werden sondern als dediziertes Projekt.

Auch das Anlegen der Schule und ihrer Organisationshierarchie als ‚reversed PKI-Struktur' in der verwendeten DTL ist diskussionswürdig. Zum einen ist davon auszugehen, dass es im Kontext der NBP und des OZG weitere Anwendungsfälle für ein Register von Bildungsinstitutionen gibt, die zusammengedacht werden sollten. Dieses kann dann auch für den genannten Zweck verwendet werden, bzw. muss mit diesem verknüpft sein.

Da es im europäischen Raum bereits für andere Bildungssektoren ein solches Register gibt[1] sollte zudem geprüft werden, ob hier nicht eine Erweiterung von existierenden Ansätzen sinnvoll ist oder zumindest technische Synergien existieren.

Modularität & Dezentralität

Neben einer Modularisierung der Software, von der ausgegangen wird, gilt es zudem Software und Betrieb getrennt zu betrachten. Nach mündlicher Auskunft der BDR ist dabei auch ein dezentraler Betrieb möglich. Sprich, auch wenn es am Ende dazu kommt das alle Länder die Lösung auch durch einen Dienstleister betreiben lassen, so sollte dies aus Effizienz- und Wirtschaftlichkeitsgründen erfolgen und nicht, weil alternative Szenarien nicht hinreichend betrachtet wurden.

Entscheiden ist dies vor allen Dingen, wenn die Lösung (oder Teile davon) auch von Dritten (bspw. anderen Bildungseinrichtungen) verwendet wird. Hierbei muss sowohl die Nachnutzung von Softwarekomponenten möglich sein, als auch der die Erreichung einer Interoperabilität durch eigene Lösungen.

Migrationspfad

Sind Zeugnisse einmal ausgestellt so gilt es aus Nutzendensicht sicherzustellen, dass eine Verifizierbarkeit über einen langen Zeitraum sicherzustellen (oder explizit zu kommunizieren das dies nicht der Fall ist). Damit unterschiedet sich der hier begutachtete Use-Case etwa von einem Use-Case wie „ich hole mir eine Krankenkassenbescheinigung und reiche diese innerhalb von wenigen Tagen

[1] ETER (eter-project.com)

oder Wochen an der Uni ein“. Dies hat Auswirkung auf die Frage nach einem möglichen Vendor Login aber auch auf den Aspekt einer nachhaltigen Bereitstellung.

Migrationsszenarien sollten daher frühzeitig auf ihre Machbarkeit. Risiken und Aufwände hin geklärt werden: Dazu zählen:

- Umstieg auf eine VC-first Lösung
- Umstieg auf ein andere Technologie
- Umstieg auf einen anderen Betreiber (ganz oder von Komponenten)