

Response to the
Legal Services Board Discussion Paper
“Quality indicators in the legal services market”
(the “Discussion Paper”)
(February 2021)

B. Collier

22 April 2021

Introduction

1. I am a solicitor practising in banking and finance at a firm of solicitors in London. I also research blockchain, distributed ledger technology and advanced databases (“Blockchain”). Details of my previous research are set out at Appendix 1.
2. The substance of this Response relates to the application of Blockchain to client and consumer feedback reporting systems and the novel features it offers, in comparison to traditional reporting and feedback mechanisms, including Digital Comparison Tools (“DCT”).

Key points

3. While the Discussion Paper covered a range of areas for consideration by the Legal Services Board (the “**Board**”) as to how to improve transparency and quality in the legal services market (“**Quality Outcomes**”), the Discussion Paper does not consider feedback mechanisms based on Blockchain which use Self-Sovereign Identity frameworks (“**SSID Frameworks**”).
4. In this Response, it will be argued that:
 - (a) Inclusion of SSID Frameworks: SSID Frameworks address a number of the issues identified in the Discussion Paper in a unique way and the Board should consider including SSID Frameworks in the scope of its review;
 - (b) Adoption of SSID Frameworks: The Board should consider adopting a Blockchain architecture incorporating SSID Frameworks to achieve improved Quality Outcomes.
5. A brief discussion about SSID Frameworks follows, then responses to the Questions. The discussion includes a model for a complaints reporting system using SSID Frameworks which is directly applicable for consumers to make complaints about solicitors.

Background

What are SSID Frameworks?

Self-Sovereign Identity frameworks are identification systems, especially as developed for digital transaction environments, which allow participants to operate and transact without centralised issuance and authentication of identity. Rather, secure information protocols and encryption reduce the need for a centralised authority and allow individuals more control of their identity information.

As explained in a 2016 article¹:

Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale.

A self-sovereign identity must also allow ordinary users to make claims, which could include personally identifying information or facts about personal capability or group membership. It can even contain information about the user that was asserted by other persons or groups.

The author explains that the concept of Self-Sovereign Identity has been considered to include mathematical/coding aspects (using cryptography to protect a user's autonomy and control) and legal aspects (including contractual rules and principles that members of a network agree to follow).

SSID Frameworks are structures for digital identity systems which incorporate some extent Self-Sovereign Identity principles. They offer a radical model of identity and transactions which have many applications.

How are SSID Frameworks established and what is the role of Blockchains?

SSID Frameworks rely on decentralised identifiers and public key cryptography to secure recorded data (and establish records without linking directly to people's identities). Blockchain systems are well suited to managing such functionality.

This Response does not consider and compare different Blockchain systems which would need to be considered by appropriate technical committee. In this Response the focus is on the use of SSID Frameworks in principle.

How do SSID Frameworks compare to traditional identification and transaction environments (Traditional Frameworks)?

Traditional Frameworks rely on very fixed relationships and concepts of identity. In Traditional Frameworks:

- (a) Subject: Many such systems will require a participant/subject to assert their full identity, not a defining characteristic relevant to the enquiry;
- (b) Credentials (evidencing certain facts): Such systems will frame the investigation (process and outcomes) in relation to confirming the validity of a document or credential which asserts a fact or claim (rather than the validity of such claim itself);
- (c) Issuing and Authentication Body: Such systems will typically require a single organisation or authority to verify and issue any such Credentials.

¹ *The Path to Self-Sovereign Identity*, Christopher Allen, April 2016, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html#dfref-1818>

An example of a Traditional Framework is a Practising Certificate issued by a professional body or regulatory organisation such as the Solicitors Regulation Authority (SRA). The Practising Certificate (as a Credential) is issued by the SRA (as Issuing and Authentication Body) to certify facts as to an individual solicitor having qualified and currently being qualified.

The Practising Certificate (as a Credential) supplements information held and published by the SRA - the roll of practising solicitors, which in essence a fact or claim which the SRA maintains and validates.

Disadvantages with Traditional Frameworks include:

- (i) **Cost** – the Issuing and Authentication Body has to verify/on-board subjects and maintain records (registers) to determine facts. Such Body has to be available to give confirmation as to Credentials which are issued. For professional bodies this cost is often met by way of contributions/membership levies from professional members;
- (ii) **Limited datasets**: Facts which Credentials can relate to are limited to very narrow categories – including those which the Issuing and Authentication Body can verify/maintain records of;
- (iii) **Limited Subjects**: Likewise the economic model for Traditional Frameworks limits records being made about a limited set of Subjects (e.g. regulated professionals such as solicitors). There is a steep economic cost to operate Traditional Frameworks to record, process and oversee all client complaints for all members of a profession for example².

SSID Frameworks offer more possibilities as:

- (a) Narrower Subject Query: SSID Frameworks can be built around limited identifying characteristics of a person and their circumstances *without identifying that person* (in what is known as a “claim”)– e.g. that a person is a client of a solicitor (but without knowing such person’s identity). **This can allow a greater number of subjects/queries, without full identity checks;**
- (b) Digital Certifications (evidencing certain facts): Certifications are made digitally and cryptographically³ rather than as a documentary certification by an Authentication Body, and the validity can be checked in the digital records without having to contact an Authentication Body separately. **This can allow a greater variety of datasets recorded while maintaining confidence in outputs;**
- (c) Separate Issuing and Authentication Bodies: Software allows different parties to issue and authenticate/oversee authentication of digital credentials as parties use a shared digital protocol, minimising the direct role of a central authority and increasing speed and efficiency. **This also reduces costs.**
- (d) Metadata: Steps in the Issuing and Authentication processes are recorded and visible to participants and this generates valuable metadata and insights as to the functioning of the system.

With such features it is possible to build more targeted and effective complaints reporting systems. This is because SSID Frameworks are based around *claims rather than identity*.

² It is outside the scope of this Response to consider digital models of complaints management.

³ i.e. using cryptographic time stamps or “hashes”. This means evidence authenticating any information is held with such information.

How do the features of SSID Frameworks work in practice? – An example of an online client reviews of solicitors which protects client identity

Renowned English commentator on digital identity David Birch, described SSID frameworks as involving a form of anonymous but assured interactions, which he referred to as “pseudonyms with credentials”⁴. This means that so long as an authoritative body issues some credential which another party can confirm, then that should be sufficient for transacting, *without having to check the subject’s identity*.

In particular, Birch gives an example of an SSID framework being applied to online reviews. He describes a system to make online reviews more credible by issuing a digital credential (cryptographic token) which verifies a claim/fact – that the person used a service which they are commenting on. This would ensure that the quality of reviews would improve as third parties could verify a commenter used a service, *without knowing who the person’s identity*.

Paraphrasing a passage from Birch, referring to a person who had stayed in a hotel (and is able to verify they stayed at the hotel when giving an online review while protecting their identity), the passage indicates *precisely* how a better system of review and transparency of solicitors could be established using a SSID Framework:

...In the case of reviews, though, how do you know the reviewer [*was a client of a law firm*]? One way would be to institute a system of cryptographic tokens [*set up by a legal regulator and issued by subscribing law firms*] so that the [*client*] can only post a review of something if they have a token showing that they [*used it/instructed the law firm*]....

...The service would work something like this: when you [*sign an engagement letter of a law firm*], your electronic wallet generates a token that the [*law firm*] digitally signs and sends back. The [*law firm*] doesn’t know who this token is going to, only that it is going to someone who really [*was a client of the law firm*]. To write a review, you must submit the token. The review site can easily check the digital signature from the [*law firm*] that proves that you [*were a client of the law firm*] but it doesn’t link to your identity. The [*law firm*] can be sure you were a [*client*], but neither they nor the review service know who you are...⁵

Key points to note from this model include:

- (a) This model incorporating SSID Frameworks offers different features from comparable customer feedback models, including DCTs (which don’t typically include confirmation as to the extent of the reviewer being a client of the reviewed firm) and a regulator operated standardised feedback system – which may receive less reviews and be much more expensive to operate;
- (b) To achieve such functionality (verification by the client itself using the cryptographic token under the SSID Framework), such functionality has to be included at the outset, implying a need to consider a SSID Framework for a client review framework/system;
- (c) Also, while such system is ideally implemented and managed by the Board or similar regulator (to coordinate participation by law firms etc.) the reduced functional requirements on such regulator to operate such system means costs will be lower.

How can SSID Frameworks be implemented to improve Quality Outcomes?

This Response does not discuss implementation steps, however likely considerations will include:

⁴ Identity is the New Money, David G W Birch (2014), Chapter 3.

⁵ Ibid, note 2.

- (a) including SSID Frameworks within policy and planning processes;
- (b) liaising with stakeholders (law firms, client body groups) to determine participation and agreed parameters, identifiers and information protocols (for information recorded in the SSID Framework deployment);
- (c) determining amongst relevant committees, technical standards and the appointment of an operator;
- (d) conducting suitable trials.

I can recommend service providers to assist in these steps if applicable.

Responses to the Discussion Paper Questions

Question 4: Should there be a base level of transparency on quality across the market and enhanced transparency in priority service areas? What should a base level of transparency on quality consist of?

In respect of consumer feedback mechanisms, this Response explains how SSID Frameworks can be deployed to obtain additional information of sufficient credibility in a different way from DCTs (currently, SSID could be added on) and a regulator operated standardised feedback system.

Therefore it is submitted that SSID Frameworks should also be considered by the Board in relation to determining the base level of transparency.

Question 5: How useful could consumer feedback, objective data and general information about providers be in informing consumer choice? What are the benefits and drawbacks of these types of information?

One limitation with consumer feedback is uncertainty as to whether a consumer has been a client of a law firm and trust of the review in general (which is why consumers will give weight to a personal recommendation from someone they trust).

This limitation was noted by the Board on the Infographic which was published by the Board in tandem with the Discussion Paper⁶. In a chart showing a mix of Quality Indicators⁷, Customer Reviews, customer experience ratings and overall star ratings are shown as most helpful but also identified as more untrustworthy/subjective. SSID Frameworks can help improve the trustworthiness of customer reviews and feedback mechanisms.

SSID Frameworks help instill trust, because (i) the credentials/claims are controlled by the subject, (ii) the key identifying information is certified digitally and (iii) identifiers/pseudonyms protect the identity of the subject.

Additional benefits of SSID Frameworks include they can offer a more effective consumer feedback system at less cost. The drawbacks are the requirement for the Board and key stakeholders to embrace new ways of operating.

Question 6: What role, if any, should success rates and complaints data have in informing consumer choice? Is there other quantitative data that would be helpful to inform consumer choice?

The improvement of trustworthiness SSID Frameworks provide has been mentioned, which will better inform consumer choice.

Also, SSID Frameworks will reveal significant patterns in the metadata (recorded in the Blockchain in respect of claims), including around how client feedback is given, common themes, timings as regards certain law firms etc. These will be observable by the operators (including the Board) which will inform policy and analysis and provide useful data to share with consumers.

It is argued that SSID Frameworks help address a key type of data currently missing – whether a consumer who gives feedback was in fact a client of the applicable firm and the adoption of SSID Frameworks will likely result in increased confidence and therefore more data from and for consumers.

⁶ Judging and comparing the quality of legal services providers: A view from the LSB's Public Panel, <https://legalservicesboard.org.uk/wp-content/uploads/2021/02/Quality-Indicators-infographic-20210211-1.pdf>

⁷ "Consumers rely on a mix of quality indicators when choosing a provider"

Question 7: Which of these different channels – law firms’ websites, DCTs, a single digital register – do you think could be most effective in providing access to information on quality? Are there other channels we should consider?

This Response argues that SSID Frameworks represent another type of channel, which should be considered.

However SSID Frameworks can in their installation operate in tandem with existing channels – as an addition to (and will enhance) DCTs. It is also submitted that SSID Frameworks will enhance what would be collected by a single digital register, with relatively less marginal cost (technical and staffing) and with greater data insights.

Question 8: Do you have evidence on current usage of DCTs not mentioned in the paper? How could we best encourage engagement by consumers and law firms with DCTs? What are your views on the specific potential solutions, such as requiring law firms to signpost to DCTs, embed ratings, or prompt consumers to leave a review?

This Response has not examined current usage of DCTs but is based on the premise that without SSID Frameworks, they cannot achieve levels of trustworthiness which are necessary or desirable to achieve better Quality Outcomes.

It is submitted that SSID Frameworks get the right balance in establishing trust for the client creating the review and reduce pressure on and emanating from law firms. As mentioned a key foundation of SSID Frameworks is the control of the process and data lies with the subject (in this case the law firm client), while key tasks of the law firm (digitally signing the applicable token or digital credential) are done passively outside of the service provision.

We also consider that discussion of SSID Frameworks with law firms will prompt a useful discussion on questions of trustworthiness and meeting stakeholder goals for improving customer satisfaction.

Question 9: What, if any, steps should regulatory bodies take to help consumers and legal services providers engage with DCTs safely?

As mentioned SSID Frameworks enhance trustworthiness and it is submitted that the Board should promote the introduction of SSID Frameworks to increase consumers and legal service providers engaging with DCTs safely.

SSID Frameworks can be operated with DCTs as the key functionality is a token/credential which confirms the claim (that the reviewer is a law firm client) before they may make a comment (likely on the DCT platform).

Subject to involvement with other stakeholders (law firms etc) we think there would be a useful discussion which could be convened with DCT platforms and other stakeholders. We also note that as the central coordinator of such system, the Board or regulator would have oversight of the process and could require some licence/conduct fee be raised from the DCT platforms to ensure quality and functionality. The DCTs would benefit from having more relevant reviews.

Question 10: What range of quality information, if any, would it be appropriate to hold on a single digital register?

This Response has considered the benefits of introducing a SSID Framework which can operate in tandem with (and cover some data types not recorded within) a single digital register. The nature of the SSID Framework having narrower subject queries may mean greater quantity of certain types of data is collected than is retained or kept on a single digital register.

Under the proposed SSID Framework, it would be for the stakeholders at the outset to determine the information parameters and identifiers which should be recorded, which should ensure the system was built with appropriate data as to Quality Indicators. This may coincide with or enhance information recorded on a single digital register.

The SSID Framework discussed also operates on the basis of digital certification to ensure credibility of information recorded. Such information may be usefully recorded (as cross-reference) on a single digital register.

Question 11: What are your views on the relative merits of a market-led approach compared with standardised regulator-led approach?

One key point of this Response is that the SSID Framework when implemented, is likely to involve elements of both a market approach and a regulator-led approach. It is considered that certain insights and regulatory oversight will be forgone in an approach which is solely led by either market participants or the Board.

It is proposed that the Board or other regulator is well placed to convene the discussion with stakeholders to decide on information protocols, identifiers, procedures and to host the SSID Frameworks (using a Blockchain architecture). Law firms will need to be involved in running software to sign digital credentials and making available to clients/DCTs access to the credentials/digital tokens.

On a full implementation of SSID Frameworks, DCTs or other platforms could include submission of such credentials with reviews by consumers/clients.

Importantly however, once set up this system should run fairly autonomously and the Board or regulator will likely have a bigger role in observing reports, analysing data and liaising directly with firms where reports and use of the SSID Frameworks indicate concern.

This represents a new mode of operating for the Board and other regulators, but it is argued this is a newer, relatively informal manner of regulation which nevertheless uses available data in an intelligent manner.

If this is of interest, the author would be happy to provide further materials setting out the governance arrangements and proposed functional relationships of stakeholders, including the Board, under an SSID Framework arrangement.

Appendix 1

Prior research by the Author

Recent publications and presentations:

- Submission, *UK Parliament, Foreign Affairs Committee, Xinjiang detention camps*, October 2020
- Submission, *UK Parliament, Business, Energy and Industrial Strategy Committee Inquiry into forced labour in UK value chains*, October 2020
- Contributor, *Legal Statement on cryptoassets and smart contracts*, The Lawtech Delivery Panel – UK Jurisdiction Taskforce, November 2019
- Contributor, *Law Commission Report: Electronic execution of documents*, Law Commission, July 2019
- Presentation, International Property Registers, *Lessons from the International Registry of Mobile Assets*, January 2019
- Panelist, Regulatory panel, *British Bankers' Association Forum on Utilising Blockchain in Banking*, London, 21 June 2016
- Co-Speaker, *Regulatory Approaches and Issues in Practice of Blockchain DLT in Financial Markets*, ISITC Blockchain DLT Working Group Meeting, London, December 2016
- Banking Technology, *Testing environment for Bitcoin exchanges*, November 2016
- Tech City News, *Accelerating Blockchain: UK regulators push ahead with regulation*, September 2016