*Marc Stauch*[1]

# The online delivery of public services, digital identity and data protection: lessons from the UK?

## A. Introduction

Over the last twenty years, it has become common for goods and services to be provided via digital transactions that take place online. This also applies to the provision of public services by government departments and other central or local authorities. As such transactions do not take place face-to-face, a crucial element in their execution is that one party can trust that the other party is who they claim to be in terms of the characteristics required in the situation: From the perspective of the public service provider, the recipient should therefore fulfil the eligibility criteria for the use of a particular service. In the private context, they must fulfil relevant legal hurdles (e.g. a minimum age) in order to benefit from the good and have the means to pay for it.

Initially, the approach to identity verification in both the private and public sector was primarily functional and driven by the respective platform or service provider[2]. The citizen/user chooses a username and password when setting up an account and provides further data on their relevant attributes (e.g. delivery address and payment details if purchasing goods). These were then stored by the provider, which enabled the user to log in to their account at a later date by resubmitting the login details they had used during initial registration.

This compartmentalised approach in principle allowed the same person to have different surface identities in the form of pseudonymous credentials with different services (e.g. a Facebook account, a Google account, etc.)[3]. The disadvantage was duplication and inconvenience for users (who had to

---

1 Leibniz Universität Hannover. Dr. jur. (Göttingen), M.A. (Oxon.). This paper is based upon research that was carried out as part of the BMWK-Schaufenster-Projekt, SDIKA: https://www.sdika.de/. The author would like to thank Professor Dr. Margrit Seckelmann and Professor Dr. Christiane Trüe LL.M. for their valuable support and insights.

2 Beduschi, A, 'Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations', Data & Policy (2021), 3: e15 (3).

3 Sedlmeir, J, et al, 'Digital Identities and Verifiable Credentials', Bus Inf Syst Eng (2021) 63(5):603, 604.

provide personal data each time they registered) and the risk of fraudulent impersonation, as users tended to reuse the same credentials (usernames and passwords) on multiple websites and services[4]. More recently, the private sector has developed innovative approaches to provide a high level of assurance that individuals making online transactions are who they claim to be, including in relation to their underlying, real identity (as a specific natural person). This was done by asking customers to provide more and more data at registration (often far beyond what is required for contract fulfilment) and by companies using the technical capabilities of cookies and electronic communications to track customers' online behaviour across different websites and services: The resulting profiles, augmented with further data from smart data analytics, are often very granular and, aside from being able to rely on the identity and creditworthiness of their customers, allow companies to predict their future choices and interests in order to conduct targeted marketing. In the case of some larger platforms, they have now also decided to offer customer identity assurance to other companies[5].

These developments pose the question of how the public sector can best catch up. And to what extent should it try to imitate the resources of the private sector? Prima facie, it could be argued that the state, as a provider of public services that are funded by taxation and are free at the time of provision, has a particular interest in being more certain that each recipient is the natural person they claim to be and that they fulfil the eligibility criteria for the service. Indeed, the main guarantor of a person's identity has traditionally been their national government[6]. Its birth, marriage and death registers, identity cards and passports gave it a privileged role, as part of its record-keeping function, in conferring identities on its citizens and in issuing documents guaranteeing the citizen's identity to third parties (be they private individuals or foreign states).

At the same time, the idea of the state collecting extensive data on its citizens, revealed through their myriad digital transactions, raises significant privacy and data protection concerns, as there are fears that the data could be misused to cement the power of the "surveillance state". In Europe, with its strict data protection regulations, the issue is particularly sensitive. The intention to strengthen the rights of EU citizens in this area (including by

4 Ibid; Bitkom, 'Strengthening trust: Practical guide to digital identities, SSI & DLT', (2023) 6.

5 Schreier, N, Renwick, R, and Ehrke-Rabel, T, 'The Digital Avatar on a Blockchain: E-Identity, Anonymity and Human Dignity', ALJ 2021, 202-218 (http://alj.uni-graz.at/index.php/alj/article/view/152); Bitkom (ibid.) 7.

6 Centre on Regulation in Europe (CERRE), 'eIDAS 2.0: Digital Identity Services in the Platform Economy', 2022 Issue Paper, 9.

displacing the role of large US platforms as insurers of digital identities) was a key motivation for the 'eIDAS 2.0' regulation adopted in spring 2024[7], which aims to provide an EU-wide approach to digital identity. At present, however, this remains a framework construct that requires a lot more implementing legislation, with some critics fearing that it could weaken rather than strengthen privacy[8].

With the above in mind, it may be instructive to look at the recent experience of the UK, a country with a traditional aversion to centralised identity systems and strict data protection rules (as a legacy of its EU membership[9]), as it attempted to set up an online identity registration system for government services. This arguably reveals some of the inevitable compromises required of governments when deciding how best to design registration systems for access to their services.

The next part (B.) of this paper describes the relevant developments in the UK, namely the creation and subsequent failure of the 'GOV.UK Verify' scheme, which aimed to introduce a federated identity assurance approach (prioritising the protection of citizen data), and its replacement now with a more centralised ID database approach, 'GOV.UK One Login', which will act as part of a wider proposed framework for digital identities. The part C. assesses the impact of this change, in particular the move from an approach where data protection was inherent in the architecture to one that relies more heavily on rules of practice to achieve this goal: As will be discussed, one of the main motivations for this shift appears to be the desire to develop new forms of public service delivery. Part D. concludes by considering possible lessons for the eIDAS approach introduced by the EU, which (even more than the old 'UK Verify' approach) seeks to build data protection into the architecture of digital identity verification.

## B. Recent Developments in the United Kingdom in the online Verification of Citizens

In the UK, responsibility for setting up systems that allow citizens to identify themselves online in order to access public services lies with Government

7 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European framework for a digital identity.

8 CERRE, footnote 6, 16-17.

9 The GDPR continues to apply in the United Kingdom in a UK version under the Data Protection Act 2018.

Digital Services (GDS), which is part of the Cabinet Office[10]. The "Verify" system for public services ("UK Verify") introduced in 2016 has its origins in the change of government in 2010 to a Conservative-Liberal coalition: one of the new government's election promises was to abolish the introduction of national identity cards, which would be backed up by a central identity database[11]. This policy had been supported by the previous Labour government, but was unpopular with the public due to concerns about data protection and state surveillance[12].

In developing a new way forward, the coalition drew on the 2008 "Crosby Report"[13], which argued for a user-centred approach that prioritises the privacy interests of citizens over efficiency or other administrative interests of the state/public service providers. In this context, the report distinguishes between "identity management" and "identity assurance"; while the former is motivated by the concerns of the information owner, the latter aims "primarily to deliver a high levels of assurance for consumers [and] will address issues such as the amount and type of data stored and the degree to which this information is shared, differently to [an approach] inspired mainly by the needs of its owners"[14].

Accordingly, UK Verify incorporated privacy/data protection into the design through a federated model where commercial trusted third parties acted as a buffer between the citizen (and their identity data) on the one hand and the government/public sector bodies in the role of service provider on the other. Specifically, under UK Verify, the government accredited several private companies that fulfilled the certification and security requirements to act as identity providers on behalf of citizens to the relevant public service provider: When the citizen registered online with a particular public authority, the system passed their registration details supporting their identity claim to one of the identity providers (chosen by the citizen); the latter then carried out the various data collection and checks to authenticate the citizen's claim[15].

A 'double-blind' system operated here: firstly, public service providers would only receive a simple confirmation from the identity provider that the citizen's identity had been accepted, and would remain unaware of the

10 [https://www.gov.uk/government/organisations/government-digital-service].

11 Whitley, E, 'Trusted digital identity provision: GOV.UK Verify's federated approach', CGD policy paper 2018, 131; Center for Global Development, Washington, USA, 22.

12 Ibid.

13 Sir James Crosby, 'Challenges and opportunities in identity assurance', HM Treasury, 2008.

14 Ibid, para 1.7.

15 Whitley, footnote 11, 29 et seq.

nature of the data used to do so, or whether other public services had been accessed or used by the citizen. Secondly, in relation to the identity provider, they would receive the identity verification request from UK Verify's central 'hub' - in this process they would not know which specific government agency the request was made by, nor what type of public service the citizen was seeking to use[16]. By 2018, seven companies were authorised by the government to act as identity providers, including Experian, Barclays Bank and the Post Office[17]. These companies themselves were bound by a strict governance framework to ensure the necessary data security and to comply with all applicable data protection principles when processing citizen data for the purpose of their identification[18].

Another privacy-friendly feature of UK Verify, derived from the 'risk-based' approach of the Crosby report, was the authorisation of graduated levels of identity assurance, with "each level provid[ing] an increasing level of confidence that the applicant's claimed identity is their real identity": At the fourth and highest level, the user "is required to provide further evidence and is subjected to additional and specific processes, including the use of biometrics, to further protect the identity from impersonation or fabrication"[19]. In contrast, less evidence would be required for the identity provider to return a positive confirmation for the lower levels. In this way, the use of personal data was reduced where this was not justified by the importance of avoiding false positive identification in individual cases[20].

Unfortunately, as it turned out, UK Verify was unable in practice to impress either its citizen users or government agencies as a viable approach. In particular, too many false negatives were consistently returned, i.e. not enough true claims were confirmed with a positive verification. In 2019, the verification success rate was 48% compared to a forecast of 90% in 2015[21]. In this context, the system does not appear to have been sufficiently calibrated to resolve surface discrepancies between the registration data submitted by the citizen and their data from previous transactions (including data from government agencies) against which it was cross-checked. In addition, some

16 Ibid; Glick, B, 'Do we really want a single digital identity system to access government services?', Computer Weekly (17 September 2021).

17 Whitley, footnote 11, 32.

18 Ibid, 53; Among other things, they were obliged to keep citizens' data for audit purposes only and to store it in a separate secure database: Ibid, 36.

19 Ibid, 25.

20 Ibid.

21 UK National Audit Office, 'The challenges in implementing digital change', Report HC 575 (July 2021), 20.

types of identity verification were excluded from the scheme from the outset, e.g. for companies or when, for example, a tax advisor wanted to act as the representative of his client[22].

This was frustrating for users who spent time entering their details into the system only to be refused verification. Furthermore, despite central government's intention for all government departments to use UK Verify, there was no mandatory requirement to do so. In practice, several departments, such as HM Revenue and Customs (in managing the online receipt of tax returns), preferred to stick with their own bespoke systems, further discouraging citizens who were able to use far fewer public services than intended. The result was low uptake, with the system attracting less than a sixth of the predicted 25 million users by 2020[23]. The lack of profitability for the accredited commercial identity providers (who were paid according to the number of successful verifications) in turn led to the majority withdrawing from the system, with only two remaining by 2019[24].

UK Verify's failure to meet its performance targets, coupled with its high cost (in total, the government invested over £200 million in developing the system[25]), drew criticism from the House of Commons Audit Committee in 2019[26], and it was decided to discontinue support for the programme. Due to the Covid pandemic and to give GDS more time to develop a replacement, funding was then continued until April 2023, but it has now been discontinued. The system's successor, known as GOV.UK One Login ("UK One Login"), was introduced and has been in beta form since August 2022[27].

The underlying architecture of UK One Login represents a significant change compared to UK Verify. In particular, it removes the approach of using private organisations to carry out the identity verification process and act as an identity data buffer. Instead, when a citizen uses the UK One Login portal, their registration data will be submitted directly to the relevant government agency to verify their identity claim (based on the data they submit): For example, if they have provided their driving licence number, this will be sent to the Department for Transport to check against their

22 Ibid.

23 Trendall, S, 'What next for GOV.UK Verify?' Public Technology Net (15 May 2020).

24 Ibid.

25 Glick, B, 'Government to impose new digital identity system across all Gov.uk services', Computer Weekly (15 February 2021).

26 House of Commons, Public Accounts Committee, 'Accessing public services through the Government's Verify digital system' (HC 1748, May 2019).

27 [https://gds.blog.gov.uk/2023/06/24/gov-uk-one-login-june-2023-update/].

records[28]. At the same time, the UK One login hub will request further data from other government departments to generate knowledge-based questions to test the citizen's claim: for example, it might ask HM Revenue and Customs to disclose the last amount of tax paid by the citizen in question and then ask the latter to provide the correct figure[29]. Once the citizen has successfully passed these tests, they will be given a UK One login account which they can use to log in to other government services in the future. At this later stage, they will no longer have to go through an identity check, i.e. it is a "once-only" system[30].

According to GDS, UK One Login was already successfully used by over 1.5 million users to verify their identity in 2023[31]. Here, central government has also learnt from the mistake it made with UK Verify by explicitly asking all government departments to switch to the new identity verification system (and shut down their own systems)[32]. The government is currently bringing forward delegated legislation authorising government departments to share data for identity verification purposes as the basis of the system[33]. Moreover, it plans in the future to use the citizen data it holds in various departments to provide identity services to private organisations themselves: This will happen as an aspect of the wider UK Digital Identity Framework (which also applies to the private sector)[34].

## C. Balancing Data Protection and the Provision of Public Services

As we have seen, the main difference in architectural design between UK Verify and UK One Login is that the use of private commercial companies has been removed from the latter system. As mentioned earlier, the reason for this design was very much centred around data protection: Citizens

28 UK Cabinet Office, 'Government response to the consultation on draft legislation to support digital identity verification' (23 May 2023).

29 Ibid.

30 This means that if a citizen has already submitted relevant data (proving their eligibility for a particular service) to a public authority, they will not have to do so again when accessing a similar public service within the UK One Login system.

31 [https://www.gov.uk/government/news/15-million-people-already-benefiting-from-reform-of-government-services-online].

32 Glick, footnote 25.

33 The Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2023, made under the Digital Economy Act 2017.

34 UK Information Commissioner's Office, 'Response to the Government's Digital Identity and Attributes Consultation' (13 February 2021).

could be assured that their identity and other data was not collected in a central database when using government services online, but that aspects of identity data were managed separately, independent of the state. In contrast, UK One Login stores the identity data submitted to it (plus confirmation from the relevant government department the citizen wished to access, that it matches their records). Over time, as more and more citizens use the system, this will enable GDS as an operator to build an increasingly complete database that matches individuals and their characteristics with the public services they access[35].

In response to data protection concerns, GDS has emphasised that the use of UK One Login will remain optional. For those citizens who are unwilling or unable to use it, the government will continue to offer alternative analogue means of identification[36]. This concession seems essential to ensure inclusivity and non-discrimination, which are themselves important public service objectives. Even so, a large-scale access campaign is underway to enable people without a passport or conventional ID to physically register for UK One Login at their nearest post office[37]. In this context, it appears that GDS hopes that a significant majority of UK citizens will use the new system, not only to realise efficiency savings (and justify the cost of setting up the system), but - as further discussed below - to lay the foundations for a new way of delivering public services.

At the same time, proponents of the new system insist that it continues to take privacy and data protection seriously, in particular at the level of norms and standards. Thus, UK One Login (like UK Verify before it) is underpinned by a strict legal framework set out in the Code of Practice for public authorities sharing data for the provision of public services under the Digital Economy Act 2017[38]. Among other things, the Code refers to the need to comply with data protection rules under the UK GDPR as well as the Data Sharing Code published by the Information Commissioner's Office[39]. In addition, UK One Login maintains UK Verify's "Levels of Assurance" approach as reflected in the GDS Good Practice Guides on identity

35 Glick, footnote 16.

36 Ibid.

37 [https://gds.blog.gov.uk/2023/08/30/the-new-in-person-identity-check-for-gov-uk-one-login/].

38 [https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/].

39 Ibid, Para 1.1, 7-9.

verification[40]. In this context, emphasis is placed on the principle of data minimisation, i.e. no more identity data is processed than is necessary to meet the relevant level of assurance. This approach is also enshrined in the proposed broader framework for digital identities (which also applies to identity verification in the private sector) currently being put forward by the UK Department for Digital, Culture and Media[41].

However, the point remains that under the new architecture, all data sharing will be managed by government bodies; here, any limitation on data use will depend on the self-restraint of the government itself. Given the UK's strong legal framework, this is currently something it wishes to exercise. But of course the political climate may change, and then there is a risk of a slide towards greater data profiling, including for surveillance, which would be less likely if private organisations also remained part of the system: Thus, if the government were to put pressure on a commercial provider to disclose its data, the matter could well end up in court, giving a judge the opportunity to consider the competing interests at stake.

Ultimately, it seems that the UK government believes that this reduction in data protection at the level of design is a price worth paying. In particular, as indicated above, a key motivation for government is the potential to develop a more sophisticated, data-driven model of public service delivery. This is recognised at the outset of the Government's response to the 2023 consultation on the Digital Identity Review, in which it commits to "transform the delivery of public services so that they are easier to use, connected, secure and offer better value for money to the taxpayer"[42]. In fact, this approach of greater data collection in the interests of improved public provision has a longer tradition[43], and has previously fuelled debates about the extent to which it risks contributing to a 'surveillance state' as opposed to a 'service state'[44].

Interestingly, the proactive use of citizen data to improve service delivery was recently strongly endorsed by the United Nations in its 2022 eGovern-

40 [https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity].

41 [https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework].

42 Footnote 28, 'Executive Summary', 5.

43 Roy, J, 'Digital government and service delivery: An examination of performance and prospects' (2017) Canadian Public Administration-administration Publique Du Canada.

44 Miriam B. Lips, A et al 'Managing Citizen Identity Information in E-Government Service Relationships in the UK', (2009) Public Management Review, 11:6, 833-856.

ment Survey[45]. There, the UN recommended that states make greater use of 'disaggregated' as well as 'longitudinal' data to identify their most vulnerable citizens and ensure they are not excluded from the benefits of digital services[46]. This suggests that it regards the collection of detailed data that tracks individual use of public services over time as something desirable, enabling states to gain the necessary insights into the characteristics of those who need extra support.

Arguably, these developments also pose questions for the current EU approach to digital identity which, in its endeavour to technically integrate strong data protection into the way citizens interact with public (and private) service providers, could prevent or at least complicate the use of citizens' data for better public service delivery. This issue will be briefly addressed in the concluding part of this article.

## D. Lessons fort he Digitally Mediated Delivery of Public Services in Europe?

If the above argument - namely the need to balance data protection against the benefits of better public services - is correct, there appear to be interesting implications for the European Union's current 'digital wallet' initiative contained in the eIDAS 2.0 Regulation. As noted in part A., this framework is subject to ongoing technical development, as well as the development of detailed normative standards (to be set out in further EU implementing acts)[47]. However, while important details thus remain to be finalised[48], the initiative's avowed aim (more so even than the former UK Verify approach) is to make data protection part of the system design. In particular, through a complex architecture that utilises either a distributed ledger or public key infrastructure[49], the EU-citizen wallet holder should be able to decide for themselves which data they want to pass on for identity or attribute verifi-

45 UN, DESA, 'E-Government Survey 2022: the Future of Digital Government', New York 2022.

46 Ibid, at 138-39.

47 Reutner, J, et al, 'Sichere digitale Identitäten in der 'Brieftasche'?' Verwaltung & Management, 30 (2024), 206-217.

48 Heeger, V, 'Digitale Identitäten: Endspurt für die eIDAS-Verordnung', Tagesspiegel Background: Digitalisierung & KI (7 November 2023).

49 Bitkom, footnote 4; Schwalm, S, Albrecht, D, Alamillo, I, 'eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI', Open Identity Summit 2022, Bonn: Gesellschaft für Informatik.

cation when interacting with a particular service - an example of so-called "Self-Sovereign Identity" (SSI)[50].

According to its proponents, the advantage of the SSI approach is that it replicates for the online environment the dynamics that existed in traditional analogue proof of identity scenarios: in these cases too, in many contexts, the person concerned had the choice of which documents to disclose to the other party, e.g. passport, driving licence or health card. SSI even goes a step further by allowing the wallet holder to disclose the minimum data required for the transaction in question[51]. In order to prove their age (e.g. to buy alcohol), they would therefore not have to present documents that also contain other data - such as their name and date of birth, as noted on their health card, but simply a cryptographically verified certificate in their digital wallet from the competent authority that they are over eighteen years old – known as a "zero-knowledge proof"[52].

However, the question arises as to how this fits in with the endeavour to provide public services in a joined-up and citizen-responsive way. In the context of the eIDAS 2.0 legislative process, this seems to have been little discussed. However, a digital wallet that gives the user self-sovereign technical control over the data they disclose could well have a negative impact in this respect. The user can, of course, agree to allow the exchange of data between the public services they use in return for a more personalised service. On the other hand, they can choose not to. The risk here is that disadvantaged groups who lack the necessary trust in state actors will exclude themselves - the very groups that would potentially benefit most from improved services.

For its part, the German government appears ambivalent about the impact of the eIDAS 2.0 legislation on digital identity verification[53]. It is currently funding a number of projects aimed at developing and testing use cases in which citizens on the one hand and public and private service providers on the other have a clear benefit (and therefore incentives) for

50 ENISA, 'Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust', European Union Agency for Cybersecurity (January 2022).

51 Allen, C: [https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md].

52 Allende Lopez, M, et al, 'Self-Sovereign-Identity, the Future of Identity: Self-sovereignty, Digital Wallets, and Blockchain', LACChain Global Alliance digital identity working group (2020), 30.

53 Answer of the Federal Government to the minor interpellation of the CDU/CSU parliamentary group - printed matter 20/8040 - Status of implementation of the eIDAS 2.0 Regulation (01.09.2023); Bundestag - Wissenschaftliche Dienste, 'Zur Umsetzung der eIDAS-VO 2.0 und der Einführung der europäischen Brieftasche für die Digitale Identität', WD 3 - 3000 – 073/24 (21.08.2024).

using digital wallets[54] . Some, but not all, will use the decentralised digital identity architecture favoured by the EU[55]. In doing so, as the UK experience suggests, it may be helpful to recognise the trade-off between data protection and other policy objectives: A lower, but for most purposes still high, level of data protection (anchored in standards rather than technical design) may be the price to pay for developing plausible and useful public service use cases.

*List of References*

Allende Lopez, M, et al, 'Self-Sovereign-Identity, the Future of Identity: Self-sovereignty, Digital Wallets, and Blockchain', LACChain Global Alliance digital identity working group (2020), 30.

Beduschi, A, 'Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations', Data & Policy (2021), 3: e15.

Bitkom, 'Strengthening trust: Practical guide to digital identities, SSI & DLT', (2023) 6.

Bundestag - Wissenschaftliche Dienste, 'Zur Umsetzung der eIDAS-VO 2.0 und der Einführung der europäischen Brieftasche für die Digitale Identität', WD 3 - 3000 – 073/24 (21 August 2024).

Centre on Regulation in Europe (CERRE), 'eIDAS 2.0: Digital Identity Services in the Platform Economy', 2022 Issue Paper.

Crosby, Sir J, 'Challenges and opportunities in identity assurance', HM Treasury, 2008.

ENISA, 'Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust', European Union Agency for Cybersecurity (January 2022).

Glick, B, 'Do we really want a single digital identity system to access government services?', Computer Weekly (17 September 2021).

Glick, B, 'Government to impose new digital identity system across all Gov.uk services', Computer Weekly (15 February 2021).

Heeger, V, 'Digitale Identitäten: Endspurt für die eIDAS-Verordnung', Tagesspiegel Background: Digitalisierung & KI (7 November 2023).

House of Commons, Public Accounts Committee, 'Accessing public services through the Government's Verify digital system' (HC 1748, May 2019).

Miriam B. Lips, A, et al 'Managing Citizen Identity Information in E-Government Service Relationships in the UK', (2009) Public Management Review, 11:6, 833.

Reutner, J, et al, 'Sichere digitale Identitäten in der 'Brieftasche'?' Verwaltung & Management, 30 (2024), 206.

54 BMWK, 'Schaufensterprogramm, 'sichere digitale Identitäten'; see also ENISA, footnote 50, 24.

55 The project, SDIKA (Secure Digital Identities Karlsruhe), is designed to dispense with the DLT approach by using a separate open source SDI-X adapter solution: [https://digitale-identitaeten.de/portfolio/sdika/].

Roy, J, 'Digital government and service delivery: An examination of performance and prospects' (2017) Canadian Public Administration-administration Publique Du Canada.

Schreier, N, Renwick, R, and Ehrke-Rabel, T, 'The Digital Avatar on a Blockchain: E-Identity, Anonymity and Human Dignity', ALJ 2021, 202.

Schwalm, S, Albrecht, D, Alamillo, I, 'eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI', Open Identity Summit 2022, Bonn: Gesellschaft für Informatik.

Sedlmeir, J, et al, 'Digital Identities and Verifiable Credentials', Bus Inf Syst Eng (2021) 63(5):603.

Trendall, S, 'What next for GOV.UK Verify?' Public Technology Net (15 May 2020).

UK Cabinet Office, 'Government response to the consultation on draft legislation to support digital identity verification' (23 May 2023).

UK Information Commissioner's Office, 'Response to the Government's Digital Identity and Attributes Consultation' (13 February 2021).

UK National Audit Office, 'The challenges in implementing digital change', Report HC 575 (July 2021).

UN, DESA, 'E-Government Survey 2022: the Future of Digital Government', New York 2022.

Whitley, E, 'Trusted digital identity provision: GOV.UK Verify's federated approach', CGD policy paper 2018, 131; Center for Global Development, Washington, USA.