Part 2 of the Data Protection & Digital Information Bill: Digital Verification Services (i.e. Identity)

In the dying days of an administration,[1] the Home Office is imposing ID checks on law-abiding people, and DCMS has handed[2] DeSIT a Bill to which nominally places an existing scheme onto a statutory basis – while that scheme is being broken and is not in compliance with the Bill as written. Will there be clarity before the Bill reaches Commons Report stage?

Context

This Part gives statutory force to the UK Digital Identity & Attributes Trust Framework,[3] but the Framework *as currently operated* and according to the definitions in clause 48(2) does not comply with clauses 48(1) and 48(4) as laid. This has been raised with DCMS, but DCMS was unwilling or unable to have the non-compliant department change their practice. No meeting has taken place since DeSIT took over and we do not know the position of the new department..

It is unclear whether and when DeSIT will weaken the legislation to appease the Home Office.

In the second part of this briefing, we use as a 'worked example' the Home Office Right to Work [4] and Right to Rent [5] online checks that were extended to cover all British and Irish citizens from 6 April 2022, which DCMS used as a "live test case" for its Framework.[6]

What the Bill *doesn't* say, and why that matters

Introducing what are effectively 'digital ID cards', without providing specific protections for those whose digital 'identities' and attributes are being processed for profit, and whose access to basic necessities like a job or a home could be jeopardised, is cavalier at best.

IDentity Service Providers (IDSPs) are already being certified under the beta Trust Framework and – under ID and attribute checks already being done – some UK citizens and residents are already encountering difficulties gaining work or a home.

---

[1] This line originally referred to the Johnson Administration, the Truss administration ignored the Bill, and the Sunack administration is, to use a footballing analogy, running out of normal time.
[2] The Machinery of Government change makes this slightly complicated. For clarity, past actions that were taken by DCMS are referred to as DCMS because it was DCMS who made those choices, whereas current Bill text and future governance decisions are owned by DeSIT.
[3] The Framework states, "In order to participate in the trust framework, providers must get certified against trust framework rules by an approved certification body." https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#how-organisations-participate-in-the-trust-framework
[4] While the Home Office's online Right to Work checks are not (yet) mandatory for everyone, the threat of civil penalties of up to £20,000 and, in serious cases, up to 5 years in prison and an unlimited fine https://www.gov.uk/government/publications/right-to-work-checks-employers-guide/an-employers-guide-to-right-to-work-checks-6-april-2022-accessible-version#what-are-the-sanctions-against-illegal-working will clearly incentivise employers to use this mode of checking, for much the same reason as similar civil penalties have driven checking for purchases of age-restricted products from "over 18?" to "Check 25".
[5] The first civil penalty for renting to a "disqualified person" may be less than that for selling alcohol to a child, but it is backed by the same threat of up to 5 years in prison and an unlimited fine. https://gov.uk/government/publications/landlords-guide-to-right-to-rent-checks/landlords-guide-to-right-to-rent-checks-6-april-2022-accessible-version#what-are-the-sanctions-if-you-are-found-to-be-renting-to-a-disqualified-person
[6] https://www.gov.uk/government/publications/digital-identity-certification-for-right-to-work-right-to-rent-and-criminal-record-checks/digital-identity-certification-for-right-to-work-right-to-rent-and-criminal-record-checks

The Bill says the Trust Framework should "secure the reliability of digital verification services" and mentions a "trust mark", but it does not provide an explicit – and hence legally robust – statutory basis for the new entity DeSIT is calling the "Office for Digital Identity and Attributes".

This new Quango would be responsible for ensuring "scheme owners" have a "complaints, redress and escalation process" in place, but the Bill as drafted provides individuals using these "schemes" and Digital Verification Services with no overarching recourse or redress other than via their general rights under Data Protection law, and – other than removal from a Register, or taking away permission to use a logo – provides no teeth or independent oversight to ensure compliance with the Framework and 'ID market' it defines.

This absence of critical governance functions raises further questions on which the Bill remains silent – such as a 'provider of last resort' when or if suppliers fail, or if the market fails to serve certain groups. **Does DeSIT believe its scheme is so perfect that such a thing will never be needed? Is this another function of the "Office for Digital Identity and Attributes", or will it be outsourced? And, if so, at what cost?**

(While the Bill repeatedly refers to "Digital Verification Services" and "DVS", it is notable that the current 'beta' version of the Framework itself (still[7]) makes *not a single mention of either term*. In itself, this is only a minor point – but it is indicative of the far wider and deeper problems DCMS previously has had in (not) defining important terms and key concepts consistently. Or at all.)

The Problem

The Bill says, at sub-Clause 46(2):

> *"digital verification services" means verification services provided to any extent by means of the internet, and*
>
> *"verification services" means services that are provided at the request of an individual and consist in—*
>
> > *(a) ascertaining or verifying a fact about the individual from information provided otherwise than by the individual, and*
> >
> > *(b) confirming to another person that the fact about the individual has been ascertained or verified from information so provided*

Applying these definitions to the Home Office online Right to Work and Right to Rent checks:

- The checks are online, thus "provided to any extent by means of the internet";
- The checks are "provided at the request" of an individual – though in practice, the individual has little choice if they want a job, or place to live;
- The facts being ascertained and/or verified are from "information provided otherwise than by the individual" – the 'facts' are what the Home Office deems to be true;
- The facts are confirmed to another person.

The confirmation of facts may be done 'indirectly', e.g. via an IDentity Service Provider, or directly. For example, under the Right to Work scheme, the Home Office itself issues verified

[7] We mentioned this to DCMS when the Bill first came out, they've not fixed it.

attributes – a 'Positive Verification Notice' for some job applicants [8] – as part of an online process.

That the Home Office also verifies people's identities for a range of companies' Digital Verification Services, e.g. by doing checks against passport photos, means it is the source of verified attributes for large parts of the ID ecosystem. Why, therefore, is the Home Office not *required* to be accredited and certified under the Framework, as both an attribute and an identity provider?

And why would anyone – individual or supplier – trust a scheme and Register that doesn't even list the body providing verified attributes on which many (if not most) services depend?

DCMS has previously claimed [9] that the Home Office is only a "relying party", i.e. an organisation 'that uses (or 'consumes') products or services from other participants in the trust framework', but this is clearly not the case. Even during the current pilot or testing phase, other participants are "consuming" attributes verified by the Home Office. (As well as the "Verification Notices" that the Home Office itself issues as part of an online process.)

What to do about it

Bring the Home Office into full compliance with the Framework, prior to Commons Report Stage

If DeSIT cannot ensure that all of the participants in its Framework are properly accredited for a limited trial that is nonetheless delivering real decisions, affecting people's ability to get a job or a home, what hope is there that the Framework and wider ID scheme(s) will operate correctly, much less command the necessary public confidence?

If DeSIT cannot show that the Home Office is in full compliance with clauses 48(1) and 48(4) as laid, according to the definitions in clause 48(2) and part 10 of the Framework,[10] then Part 2 should be removed from the Bill – as the Secretary of State will have brought legislation before Parliament to put onto a statutory basis an ID scheme and 'Trust' Framework that the current actions of the Home Office *demonstrably breach* in DeSIT/DCMS's live trial.

Simply put, DeSIT has inherited a mess, the legacy of DCMS's dash to legislate before it could even walk on this topic.

medConfidential

---

[8] "The Home Office will send you a 'Positive Verification Notice' (PVN) to confirm that the applicant has the right to work": https://www.gov.uk/check-job-applicant-right-to-work – that the PVN is (for now) a paper document does not make it any less an **attribute**, and that the Employer Checking Service under which PVNs can be issued is an **online service**: https://www.gov.uk/employee-immigration-employment-status clearly means it meets the Bill's definition of a "verification service provided to any extent by means of the internet".

[9] In engagement sessions with civil society, e.g. on 16 June 2022. There has not yet been a meeting with DeSIT.

[10] "In order to participate in the trust framework, providers must get certified against trust framework rules by an approved certification body." https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#how-organisations-participate-in-the-trust-framework