BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

Establishing a framework for a European digital identity

Impact assessment (SWD(2021) 124, parts 1-3, SWD(2021) 125 (summary)) accompanying a Commission proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity, COM(2021) 281.

This briefing provides an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above-mentioned proposal, submitted on 3 June 2021 and referred to the European Parliament's Committee on Industry, Research and Energy (ITRE). The proposal[1] seeks to amend Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation) in order to better meet the new market and societal demands for trusted government eID linked solutions and for attributes[2] and credentials[3] provided by the public and private sector, which would be recognised across the EU for accessing both public and private services. This proposal would also address users' expectations to have more control over their personal data. This initiative, which European Commission President Ursula von der Leyen announced in her State of the Union speech of 16 September 2020, is included in the Commission's 2021 work programme and is part of the strategy on shaping Europe's digital future. In its conclusions of 1-2 October 2020, the European Council invited the Commission to come forward with a proposal for a European digital identity framework by mid-2021.

Problem definition

The eIDAS Regulation (EU) No 910/2014 (eIDAS) created a cross-border framework for trusted electronic identification of natural and legal persons, and trust services (the certification of a digital identity, e.g. electronic signatures). It enables the cross-border recognition of government electronic identification (eID) for access to public services, provided that the national eID has been notified to the Commission under the eIDAS. To facilitate mutual recognition, an interoperability framework with technical eIDAS nodes (application components) – to which services need to connect – has been established. The eIDAS does not oblige Member States to develop a national eID and to notify it. The evaluation of the eIDAS found that it has contributed to the functioning of the internal market in various sectors, such as the financial services one, but has only partially achieved its objective of enabling cross-border access to public online services. Not all Member States have issued eIDs and notified them, there is no full operability of the technical nodes, and the eIDAS does not address the needs of certain sectors (e.g. education). The scope of the eIDAS is limited as it focuses on secure cross-border access to public services, whilst the vast majority of the needs of eID and remote authentication remains in the private sector. The IA refers to the rapid digitalisation of society in recent years – accelerated by the coronavirus pandemic – which has also affected the provision of both public and private services. This has triggered a paradigm shift towards advanced and user-friendly solutions that can integrate users' certificates and verifiable data and provide an easy and secure access to different public and private services, under users' full control. As a consequence, the demand for means to identify and authenticate online, and digitally

Author: Mari Tuominen with Solène Festor
Ex-Ante Impact Assessment Unit

PE 694.244 – October 2021

exchange information related to users' identity, attributes or qualifications with a high level of data protection, has increased significantly. The IA refers to an estimated annual global growth between 13 % and 20 % for the digital identity market. (IA part 1, pp. 1-10, 21)

The IA has identified **four problems**:

P1) **Increased demand by public and private services for trusted identification and exchange of digital attributes is not met**, as the eIDAS focuses on access to cross-border public sector services and has been able to offer this access only to a limited number of them. According to the IA, only 14 % of key public service providers in the Member States have allowed cross-border authentication with a notified eID. The IA also mentions issues in the interoperability network (the eIDAS node sending and receiving capacity), as 67 % of the Member States have receiving capacity and 37 % have sending capacity in production 'for some Member States'. On the other hand, private online services cannot provide a high level of legal certainty and data protection, and the use of notified eIDs by the private sector in the cross-border context is 'practically inexistent', among others, on account of liability or lack of commercial models. The digital exchange of attributes and credentials (e.g. certificates, qualifications) is not covered by the existing eIDAS, and the public and private offer is scattered and lacks legal effects in the cross-border context. (IA part 1, pp. 2-3, 10-12)

P2) **Current user expectations for seamless and trusted solutions to identify and share attributes across borders are not met**. Under the existing eIDAS, only 14 Member States have notified eIDs and a limited number of citizens (59 %) have access to trusted and secure government eID means in the cross-border situations. Only a few Member States have involved the private sector in the provision of eID means and recognised their services for access to online public and private services. The IA refers to users' expectations to use mobile applications and 'single-sign-on' for online services in the public and private sector. It furthermore notes that, while new identification solutions are being developed, they would be less secure unless they are linked to the national eIDs. (IA part 1, pp. 9, 12-13)

P3) **Data control and security concerns are insufficiently addressed by available digital identity solutions**. The IA refers to security risks and incidents involved in providing personal data online, and mentions some examples, such as the data leaks of 500 million Facebook users in 2021 and the exposure of around 4.1 billion personal data records due to data breaches in 2019. A Eurobarometer survey in 2019 found that 75 % of EU citizens use low-level security identity tools provided by the private sector and that 88 % of consumers would like to have more control over their data. Even though the eIDAS framework provides a high level of security, the IA mentions that users cannot limit the sharing of personal data to what is strictly necessary for a specific transaction, contrary to what the 'privacy by design' concept in the General Data Protection Regulation (GDPR) would require. As for platforms and social media, users are usually required to register for platforms' 'own' services in order to access other products (e.g. social networks), which may create some data protection issues. The European Data Protection Supervisor (EDPS) has highlighted the issues of non-transparency of data management and repurposing of data causes, which means that data may lose its original context and limit users' control over their data. (IA part 1, pp. 13-14)

P4) **Unequal conditions for the provision of trust services and insufficient scope of the regulation**. The IA points out that identity-proofing methods are defined in different ways at national level, which creates market-entry barriers and an uneven playing field (e.g. some Member States allow video identification). The IA also mentions national differences in the conformity assessment of qualified trust service providers in terms of requirements and standards, and in the application of the rules for national supervision. According to the IA, a more harmonised approach would be needed also for auditing (conformity assessment reports), e-archiving services and the management of electronic signatures (requirements, standards). As for the provision of qualified website authentication certificates (QWAC) introduced by the eIDAS – which allow users to know the identity of the entity responsible for a specific website in order to prevent fraud – web browsers (most of them in the United States) have refused to support them. (IA part 1, pp. 14-15)

The IA defines and explains **seven problem drivers**: D1) market, societal and technological developments triggering new user and market needs (linked to P2-4); D2) notification by Member States of eID schemes under eIDAS is voluntary and the process is complex (P1-2); D3) not all Member States have notified national eIDs and opened them to the private sector for domestic reasons or for lack of incentives (P1-2); D4) private providers of digital identity attributes are not subject to a harmonised regulatory framework ensuring trust and security across borders (P1-3); D5) due to diverse and ineffective conditions, private online service providers cannot rely on trusted and secure eIDs across borders (P1-2); D6) the set of identity data provided by eIDAS is too limited and rigid (P1-2); D7) inconsistent interpretation, divergent application and lack of acceptance of the eIDAS Regulation in relation to qualified website authentication certificates (QWACs) (P4). According to the IA, these drivers relate to changes in the context (D1), regulatory shortcomings (D2, D4-D7) and implementation weaknesses (D3, D5, D7). (IA part 1, pp. 10, 15-21)

Overall, the problem definition is well evidenced, drawing on the evaluation of the eIDAS Regulation, stakeholder consultation, Eurobarometer survey, and studies and reports on the digital identity market. The IA underpins the description of the problems and their scale with quantification. The intervention logics graph, presenting the links between the problems and problem drivers, is to some extent confusing, as, based on the description, one might expect a link between P3 and D6, and also between P1 and D1 (IA part 1, p. 10). The IA mentions that digital identification will 'become an important factor of social inclusion', which could have been explained further in greater detail (IA part 1, p. 12). Likewise, the IA could have addressed more the expected consequences if the problems are not addressed at the EU level, e.g. negative effects on a level playing field or growing online payment fraud (IA part 1, pp. 21-22).

Subsidiarity / proportionality

The legal basis of the proposal is Article 114 of the Treaty on the Functioning of the European Union (TFEU). The IA presents sufficient justification for EU action. The initiative aims to provide improved means for digital identity solutions and portability of personal identity attributes and credentials for citizens and businesses across the EU. National measures would not suffice to address cross-border challenges of interoperability and security (trusted eIDs). (IA part 1, pp. 22-24) The IA does not provide a dedicated subsidiarity grid, contrary to what is recommended by the Task Force on subsidiarity, proportionality and 'doing less more efficiently'. Proportionality is one of the key criteria used in the comparison of policy options, as required by the Better Regulation Guidelines (see also Toolbox, Tool#5), and it is also discussed in the context of the preferred option. None of the national parliaments submitted any reasoned opinions by the deadline of 4 October 2021.

Objectives of the initiative

The **general objective** is to 'ensure the proper functioning of the internal market, particularly in relation to the provision and use of cross-border and cross-sector public and private services relying on the availability and use of highly secure and trustworthy electronic identity solutions'. The IA identifies four **specific objectives** derived directly from the four problems identified: SO1) 'provide access to trusted and secure digital identity solutions that can be used cross borders, meeting user expectations and market demand'; SO2) 'ensure that public and private services can rely on trusted and secure digital identity solutions cross border'; SO3) 'provide citizens full control of their personal data and assure their security when using digital identity solutions'; and SO4) 'ensure equal conditions for the provision of qualified trust services in the EU and their acceptance' (IA part 1, pp. 24-26). In accordance with the Better Regulation Guidelines, the IA is due to present operational objectives (defined in terms of the deliverables of specific policy actions) after the selection of the preferred option. However, in the monitoring and evaluation plans, the indicators are linked to objectives that are quite generally formulated. The defined objectives should be specific, measurable, achievable, relevant and time-bound (SMART criteria). It appears that the formulation of the objectives is not time-bound, and could have been more measurable.

Range of options considered

The IA presents three legislative options in addition to the baseline. The options are interdependent and cumulative, i.e. Option 2 builds on Option 1, and Option 3 builds on the measures of Option 1 and Option 2. (IA part 1, pp. 26-44)

Baseline: No action.

Option 1 (Improve the current legal framework for cross-border recognition of national eIDs and trust services) would oblige Member States to provide eIDs and to notify them under the eIDAS, including a streamlined notification procedure, e.g. timeframe (SO1, measure M1.1.). Member States would also be required to allow private online service providers to rely on notified eIDs (M1.2.). This option would establish a harmonised commercial model (cost-model, contractual conditions, security requirements) and liability rules to facilitate private online service providers to use the notified eID schemes (M1.3.). It would also extend the personal identification data set recognised cross-border, which would support identity matching and access to sector-specific services (M1.4.). (SO2) To address SO3, Option 1 would strengthen the security requirements for mutual recognition (M1.5.). It proposes a new trust service for e-archiving (M1.6.); harmonising the certification process for remote electronic signing (M1.7.); and strengthening the recognition of QWACs, by requiring web browsers to ensure support and interoperability with them (M1.8.). (SO4)

Option 2 (Creating a market for the secure exchange of data linked to identity) proposes, in relation to SO1, the same measure M1.1. as in Option 1, and in addition, a new qualified trust service for the secure exchange of data linked to identity (e.g. driving licence, proof of residence) (M2.1.), as well as a requirement for Member States to make available data stored in authentic sources (under the users' control) for the secure exchange of data linked to identity (M2.2.). For SO2, besides the same measure (M1.4.) as in Option 1, Option 2 proposes security requirements and common technical standards for the secure exchange of data linked to identity (M2.3.). It would define the legal effect of digital identity credentials (M2.4.) and oblige the public sector and regulated sectors (e.g. energy, finance) to rely on qualified digital credentials (M2.5.). As regards SO3, in addition to the measure (M1.5.) under Option 1, Option 2 introduces legal requirements to ensure the protection of personal data, especially in relation to the purpose limitation principle (identity data to be kept separate from other personal transactional/behavioural data) (M2.6.). The measures concerning trust services (SO4) are the same as in Option 1.

Option 3 (Personal digital identity wallet (EU eID) available to residents and companies) (preferred option) includes the same measures for SO1 as in Option 2 (M1.1., M2.1., M2.2.), and, in addition, proposes two sub-options for the deployment of the digital wallet (M3.1.), but does not indicate a preference between them. Sub-option 1 creates a new qualified trust service for the provision of a user-controlled secure European digital identity wallet application. Sub-option 2 extends notified eID schemes or provides a user-controlled secure European digital identity wallet application by the Member States. For SO2, Option 3 proposes the same measures as in Option 2 (M1.4., M2.3, M2.4., M2.5), and introduces common standards for a European digital identity wallet application (M3.2.) and security requirements (M3.3.). The digital wallet would make it possible for users to securely exchange data linked to their identity to public and private online service providers with full control over their personal data. As Option 3 presents a common technical architecture, a reference framework and standards, reliance on the eIDAS technical nodes would no longer be necessary. For SO3 and SO4, Option 3 proposes the same measures as Option 2.

As required by the Better Regulation Guidelines, the IA presents a sufficiently broad range of options. It provides a good description of the options, including also concrete examples of how various measures would be implemented. However, the IA does not systematically present stakeholder views on the options and only mentions some views regarding a few individual measures.

Assessment of impacts

The IA assesses – mostly qualitatively – the main economic, social and environmental impacts of the policy options, as well as the impacts on fundamental rights. In addition, it addresses the technological impacts. In the **economic** assessment (partially quantified), the proposed measures under all options would entail costs for the public authorities (e.g. eIDAS obligations, certification, standardisation), online service providers (e.g. infrastructure, QWACs), trust service providers (SMEs not specified) (e.g. introduction of new trust services, increased personal data protection), conformity assessment bodies (e.g. familiarisation with new standards) and digital wallet providers (e.g. development, maintenance). The IA mentions that a quantification of the costs and benefits would be presented also for the baseline, but it appears that the analysis of the baseline is only qualitative (except cost references concerning the notification process). (IA part 1, pp. 45-46; IA part 3, pp. 34-37) The IA also analyses the macroeconomic impacts and finds that the proposed measures would, for example, generate additional jobs, economic growth and investments. As regards **social** impacts, the IA briefly discusses the expected positive effects on employment in all options and finds that measures under Option 3 could facilitate access of elderly people and people with disabilities to services, but notes the low level of web accessibility in the public sector at present. The IA expects positive impacts also on **fundamental rights**, such as protection of personal data, social inclusion and civic participation through increased digital inclusion. However, the IA points out that the expected benefits are 'partially offset by the relatively high requirements as regards necessary (safe but costly) equipment on the side of the user (under Option 3)' and that digital and social inclusion benefits might be affected by 'barriers to access to technology' (IA part 1, p. 62). It would have been useful if these issues had been discussed more (e.g. IT literacy and digital inclusion by elderly people, people with disabilities, disadvantaged groups). When assessing the options' impacts on **data protection**, the IA takes into account the requirements of the GDPR and the issues identified in the problem definition. The IA explains that the preferred Option 3 would ensure full control by users of their personal data and provide data protection safeguards (e.g. purpose limitation) supported by a new trust service. As for **technological** impacts, the IA expects all options to positively impact innovation, e.g. highly secure eID solutions in Option 1, cutting-edge eIDAS-compliant solutions in Option 2, and secure elements in mobile devices and incentives to invest in digitalisation technologies in Option 3. In relation to **environmental** impacts, the IA explains that measures would contribute to environmentally friendly paperless identification processes, but it also refers to 'some caveats'. It mentions that electricity consumption linked to increased online interactions would partly offset the expected benefits. Environmental impacts, addressed in a very limited manner, could perhaps have deserved a more detailed discussion, in particular, on 'caveats'. (IA part 1, pp. 45-65)

The policy options were compared against the defined objectives and the Better Regulation criteria of effectiveness, efficiency, coherence and proportionality. As regards **effectiveness**, the IA considers Option 3 (both sub-options) the best option as it would fully achieve the objectives, i.e. it would 'allow maximum flexibility in accessing and managing both qualified and non-qualified attributes and eID related data, which cannot be achieved under options 1 and 2' (IA part 1, p. 66). In the comparison of options against the criteria of **efficiency**, the IA provides only partial quantification of costs and benefits, and openly explains the difficulties in making quantifications. In terms of the cost-benefit ratio for businesses (compliance and administrative costs), Options 2 and 3 are found equally efficient and better than Option 1. As for the cost-benefit ratio for the public sector (compliance and enforcement), all options have similar scoring as regards efficiency. In the overall comparison of quantifiable costs and benefits, the IA finds that the costs (€58+ million) would exceed the benefits (€54+ million) in Option 1. For Options 2 and 3, the IA gives the same estimate for the expected net benefits (€800 million - €6.5 billion), pointing out that all the costs and benefits cannot be quantified. Therefore, a wide estimate range is provided for the overall benefits (Options 1 and 2 at €3.9 billion – €9.6 billion), and regarding the overall costs, the IA provides only the minimum but not the maximum costs. However – although found similar in terms of net benefits

in the IA – given that the overall costs of Option 3 are higher (€3.2+ billion) than the costs of Option 2 (€3.1+ billion), the net benefit range of Option 2 appears better than that of Option 3. The IA finds all options equally **proportionate**, stressing that costs are proportionate in relation to the objectives and expected benefits. Options 2 and 3 are found equally **coherent** with the evolution of the wider policy objectives and better than Option 1; yet, the IA states that only Option 3 would be fully coherent with the political mandate set by the Council and the Commission, and Option 3 would be 'most coherent' with the EU's overarching priorities. (IA part 1, pp. 65-78)

SMEs / Competitiveness

The IA finds that the present initiative would create new market opportunities and promote competitiveness of European businesses through innovation (technologies) and greater digitalisation of services, although these aspects could have been addressed more. (IA part 1, pp. 4, 58, 61) The IA states that small and medium sized enterprises (SMEs) are eID/trust service providers and end users in the EU's digital identity market. The IA notes that the 'large majority' of trust service providers (not quantified) are SMEs (microbusinesses are not mentioned). According to the IA, addressing complexity and a lack of information – which hinder SMEs' uptake of eID and trust service solutions (currently 17 %) – could support SMEs in digitalising their services. The preferred Option 3 is expected to offer new business opportunities also for SMEs in its sub-option 1, but the IA mentions that 'development and certification costs are likely to act as an entry barrier' and that 'SMEs would need to identify a strong business case to deploy the necessary resources and develop the wallet and conclude agreements with other players in the wallet ecosystem' (IA part 1, p. 64). This would have deserved a more detailed discussion in the IA, given also that its description of impacts of the preferred option on SMEs is overall very brief, and SMEs' views specifically are not mentioned. The IA estimates that for SMEs – as end users – the use of digital wallets will entail costs that could be offset by savings from efficiency and simplification measures. (IA part 1, pp. 63-64) It would have been useful if the IA had provided information on why an SME test was not considered necessary.

Simplification and other regulatory implications

The initiative is part of the Commission's regulatory fitness and performance programme (REFIT). In the REFIT section, the IA provides estimates of the cost savings of the preferred option (partially quantified), such as reduced costs for cybercrime damages in financial services ranging from €0.85 billion to €1.4 billion per year, and savings resulting from a reduced administrative burden for users of around €350 million – 400 million per year. (IA part 1, pp. 78-79) The preferred option would be in line with the existing EU legislation (e.g. GDPR, Cybersecurity Act, Single Digital Gateway Regulation) and political priorities and commitments (e.g. European Green Deal, digital decade communication, shaping Europe's digital future strategy), as well as supporting forthcoming EU instruments concerning a future European digital driving licence and a future European social security passport, for instance. (IA part 1, pp. 3-4, 71-74)

Monitoring and evaluation

In the monitoring and evaluation plan, the IA presents relevant indicators to monitor implementation, application and contextual information, and also mentions the data sources (e.g. national authorities, annual survey, Eurostat). Operational objectives do not appear in the monitoring plan, and the indicators are linked to some of the specific objectives (although formulated differently) and to objectives, which are not defined earlier ('the development of new digital identity services'). The IA does not mention evaluation obligations. (IA part 1, pp. 79-81)

Stakeholder consultation

As required by the Better Regulation Guidelines, the IA provides a separate annex describing the broad stakeholder consultations held (IA part 2, pp. 9-29). Feedback on the inception impact assessment (IIA) garnered 53 responses (number not provided in the IA) from 'public and private stakeholders' (not further specified in the IA) between 23 July 2020 and 3 September 2020. The open

public consultation (OPC) – which requested feedback on, e.g., impacts of the implementing options of an EU digital identity – got 318 replies between 24 July 2020 and 2 October 2020 (partially in parallel with the IIA consultation), not meeting the 12-week requirement of the Better Regulation Guidelines (justification not provided). Most of the responses represented EU citizens (116), companies, business organisations and associations (132), public authorities (28) and academia (11). A stakeholder survey received 106 responses, in particular from trust service providers (36), supervisory and conformity assessment bodies (34), and Member States (19). In addition, the IA mentions that the Commission gathered views from the eIDAS cooperation network, bilateral meetings and interviews of public and private stakeholders. The IA explains that the feedback on Option 3 is 'more limited', because during the consultation process digital wallets were further developed, and the Commission undertook targeted consultations to fill this gap. From the summary it appears, for instance, that 63 % of respondents (another figure, 60 %, also mentioned) in the OPC were in favour of a European digital identity scheme, but on the other hand 57 % (another figure, 52 %, also mentioned) voiced complexity of set-up and governance as its possible disadvantages. The views of stakeholder groups could have been indicated more clearly, as views are at times referred to quite vaguely (e.g. 'various stakeholders', 'multiple interviewees', 'respondents'). Moreover, the IA does not specify whether data protection experts were consulted, nor does it mention the views of the SMEs in the consultation summary. It would have benefited the description if more use had been made of the information on stakeholders' views provided in the IA's 'supporting study', which is referred to several times.

Supporting data and analytical methods used

The IA is based on stakeholder consultations, surveys and studies, such as the study supporting the evaluation of the eIDAS Regulation (Deloitte, VVA, Spark Legal Network, Ecorys), a study supporting the IA for the revision of the eIDAS Regulation (PwC, DLA Piper) and a study supporting the IA for the 'Digital Identity Act' (PwC-led consortium). As these two last studies are not linked, it is not possible to verify if they are actually one and the same study referred to with different names in the IA. The references to the 'supporting study' could have been at times more complete as it was not always clear to which supporting study the IA was referring (IA part 2, pp. 9, 12; IA part 3, pp. 39- 47). Moreover, references and a link to the evaluation study are provided only in the annexes but not in the main text. The assessment is mostly qualitative, but it also presents quantitative estimates. The IA openly refers to limitations in quantification. The IA explains the analytical methods, such as the model used (input-output dynamic stochastic general equilibrium model), the econometric methodology (Bayesian estimators) and the main data sources (OECD, STAN structural analysis database, Eurostat) (IA part 3, pp. 15-22). The IA and the model used are included in the Commission's public modelling inventory and knowledge management system (MIDAS).

Follow-up to the opinion of the Commission Regulatory Scrutiny Board

The Regulatory Scrutiny Board (RSB) adopted a negative opinion on a draft version of the IA report on 17 March 2021, due to significant shortcomings. The second opinion of 5 May 2021 was positive; however the RSB recommended making further improvements, especially regarding the description and comparison of options in terms of efficiency and effectiveness, and the presentation of stakeholders' views. The IA explains in an annex how these points have been addressed (IA part 2, pp. 1-8). It would appear however that the RSB's concerns have not been entirely addressed in regard to the comparison of options and the presentation of stakeholders' views.

Coherence between the Commission's legislative proposal and the IA

The proposal appears to largely follow the IA's preferred Option 3 (with sub-option 2). Article 6a specifies that European digital identity wallets are issued by a Member State, under a mandate from a Member State or independently but recognised by a Member State. The proposal includes electronic ledgers and qualified electronic ledgers providing proof and an audit trail for the sequencing of transactions and data records, which are not mentioned in the IA. The IA does not

include evaluation obligations, but the proposal states that the Commission would review the regulation within 24 months after its entry into force, and then every four years. It also includes reporting requirements for the Member States on the collection of statistics. It can be noted that the EDPS stated in his formal comments of 28 July 2021 on the legislative proposal that 'whether the specific safeguards are sufficient depends mainly on the technology to be used in implementing the proposal'.

The IA provides a well-evidenced problem definition and a sufficiently broad range of policy options. The IA is based on reliable and recent data from various sources, including an evaluation of the eIDAS Regulation, in line with the evaluate-first principle. The Commission has conducted broad stakeholder consultations; however, the consultation period of the OPC did not meet the 12-week requirement. The IA is mostly qualitative, and it openly informs of the difficulties in quantifying the costs and benefits of the policy options. It would have benefited the analysis if the scoring of options had been further clarified and if the identified social and environmental impacts had been discussed in greater detail. Data protection aspects have been duly discussed, and according to the IA, the preferred Option 3 would ensure users' full control over their personal data and provide data protection safeguards. The description of the preferred option's impacts on SMEs is very limited, and specifically SMEs' views are not indicated in the IA. It is not clear from the stakeholder consultation summary whether data protection experts have been consulted. Overall, stakeholders' views could have been presented more clearly, as views on the policy options are not systematically indicated, and stakeholders' views are at times quite vague. Finally, more use of the information from the annexes as well as clear references and links to the supporting studies in the main text would have improved transparency and reader-friendliness.

ENDNOTES

[1] See EU Legislation in Progress Briefing, Updating the European digital identity framework, by Mar Negreiro, EPRS, October 2021

[2] The IA defines 'attributes' as 'pieces of information about one person or organisation', e.g. a legal name, date of birth, social security number, or professional qualifications, licenses (IA part 1, p. iii).

[3] The IA defines 'credential' as a 'set of claims that prove qualification, achievement, quality or aspect of a person's background' (IA part 1, p. iii).

This briefing, prepared for the Committee on Industry, Research and Energy (ITRE), analyses whether the principal criteria laid down in the Commission's own Better Regulation Guidelines, as well as additional factors identified by the Parliament in its Impact Assessment Handbook, appear to be met by the IA. It does not attempt to deal with the substance of the proposal.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)