AGENCY FOR DIGITISATION
MINISTRY OF FINANCE

Memo

24 September 2020

The Danish Government's response to the public consultation on the eIDAS review

The Danish Government welcomes the public consultation on the eIDAS review and agrees with the Commission's assessment that the existing eIDAS framework needs to be revised to achieve the policy objectives of the Regulation.

General remarks

The Danish Government considers the Regulation of Electronic Identities and Trust Services (eIDAS) as a prerequisite for the digital transformation and for the strengthening of the EU's digital single market. The COVID-19 pandemic has underlined the importance of citizens and businesses having the ability to perform their daily tasks digitally. It is paramount that the continued European digitisation serves the interests of society in a safe, trustworthy and predictable way while contributing to the green economy as well.

Thus, the Danish Government believes that quality, safety and predictability should be guiding principles in the forthcoming revision of the eIDAS Regulation. These principles should be adhered to:

- Increased focus on the interdependencies between the eIDAS Regulation and other relevant legislation,
- Clearer rules and assessment parameters, maintaining the Regulation's technology-neutral and framework-setting nature for electronic identities and trust services, and
- A focus on future-proofing the Regulation.

The Danish Government calls on the Commission to adopt a holistic view across relevant EU legislation. Although the eIDAS Regulation is the primary regulation for electronic identities and trust services, other pieces of EU legislation are closely related, e.g. the GDPR, NIS, PSD2 and the EIF. Moreover, Denmark calls on the Commission to take into account the current considerations of a European Social Security Number (ESSN) in this regard. Additionally, the revision must be regarded in the context of the implementation of the Single Digital Gateway. Denmark encourages the Commission to work to reuse language, definitions and align associated guidelines and instructions in these packages of legislation. For instance, the time limit for safety notifications is 24 hours according to the eIDAS regulation but 72 hours according to the GDPR.

The Danish Government believes that the existing eIDAS framework constitutes the best foundation for the above-mentioned objectives. Overall, Denmark supports the aims of the suggested policy option 1 and, to some extent, policy option 2. In regards to policy option 3, it is crucial for the Danish Government that costs for Member States with a high degree of eID legacy are minimised and therefore that any European Digital Identity-solution is based on the existing eIDAS infrastructure.

In the Commission's Inception Impact Assessment (IIA), a number of expected positive impacts of the policy options are described. The Danish Government invites the Commission to provide documentation and argumentation for these expectations. Furthermore, the IIA also touches upon likely economic impacts of the policy options. The Danish Government invites the Commission to elaborate on these impacts including the expected costs for Member States associated with implementing the different policy options.

Policy Option 1: Improving Coherence, Consistency and Interoperability

Option 1 aims to make incremental changes by suggesting the introduction of new implementing acts which would reference specific standards, adoption of targeted guidelines on the application of specific provisions (e.g. remote identification, identity proofing), introducing references to certification schemes in the identity assurance element of levels of assurances (LoA). Furthermore, option 1 aims to raise awareness and create incentives for the uptake of eIDs under eIDAS by the private sector via guidelines on costing, liability and on the opportunities to fulfil various regulatory requirements by the use of eIDs.

The Danish Government's opinion

General Comment

The Danish Government believes that Option 1: Improving Coherence, Consistency and Interoperability is a viable and beneficial approach and looks forward to discussing which concrete implementing acts would be introduced by Option 1.

Although the eIDAS Regulation entered into force on 1 July 2016, the specific articles regarding the obligations on mutual recognition have only been in effect since 28 September 2018. There is still a large effort to be done before all Member States and e-services are fully functioning when accessed with a notified eID. This must be taken into account when cataloguing the achievements of the Regulation—including Member States' uptake and usage in the private sector. Major changes to the general requirements concerning mutual recognition and the eIDAS Regulation as such would not be timely.

Several Member States require a Personal Identification Number (PID/PIN) issued by the Member State in order to provide services to the citizen. This national PID must be linked to the citizen's eID when they wish to authenticate and identify

themselves to an e-service while using an eID from a different Member state. This commonly means that the receiving Member State must match a PID/PIN in that Member State with the claimed identity from the eID from another Member State. Many Member States are in the process of developing and implementing such processes in their national digital infrastructures. However, much effort remains before reaching parity between the digital services offered to national citizens and citizens from other Member States.

The Danish Government supports the idea of creating greater coherence between the developed standards and the implementing act, as originally envisioned in the creation of the eIDAS Regulation. Referencing standards that have already been developed by the European Telecommunications Standards Institute (ETSI) would ensure greater harmonisation, transparency and coherence. This would ease the path for providers of trust services to deliver products, which fulfil the requirements, and help achieve the ambitions of the Regulation with regard to ensuring high-level security of qualified trust services and of the products used or provided.

Remote Identification

Several Member States are increasingly relying on a higher degree of remote identification of their citizens. It is therefore important that a common framework is developed containing requirements and guidance on the characteristics, qualities and functionalities that should be present in a remote identification solution and thereby the underlying identity proofing. These are prerequisites for evaluating the security and qualities of a specific implementation of remote identification. The Danish Government urges the Commission to include these issues in the revision proposal.

The Private Sector

Private sector usage of national eIDs is quite low across the EU. Many Member States impose requirements, conditions and obligations on private service providers. It is important to enforce the regulative obligation of mutual recognition of national eIDs—i.e. there must be no national obstacles for the use of eIDs across international borders. This should be a high priority for the revision, but it does not necessitate rethinking the entire Regulation. The revision should focus on ensuring private service providers easier access to existing eIDs, including the interoperability infrastructure in the form of the eIDAS nodes.

Work to increase eIDAS' uptake among private service providers has begun, yet seemingly, it appears stalled. The Commission should continue the work to identify barriers and opportunities for improving the uptake of private services. This work should result in proposals and improved guidelines within the existing regulative framework. These proposals and guidelines should take into account that use of public eIDs issued by private service providers is already high is a number of European countries, while less in others. New requirements and guidelines must not become an obstacle for the countries that already have a high uptake in the private sector. The Danish Government believes that it is crucial that it remains possible

for the Member States to use existing systems that already adhere to the eIDAS Regulation without additional costs imposed by new EU legislation. As an example, the Danish Government and Danish banks have nurtured a successful collaboration and business model for our national eID (NemID) since 2010. Around 450,000 private companies use NemID for validating and signing, and more than 700 private companies use NemID to validate their customers. By 2021, MitID will replace NemID, aiming to create a flexible, modular and modern solution that can be used for both public and private digital services—e.g. brokers will be inserted to link service providers with internet service providers, a solution also worth considering at the European level, when considering new approaches to the private sector

Qualified Web Authentication Certificates
Uptake of Qualified Web Authentication Certificates (QWAC) has been slow and issues persist with browser vendors. However, there already exists a thriving private marked for web-certificates. The EU and its Member States should support the continued development of international standards and requirements instead of developing and operating its own concept.

Business Identities
The Danish Government calls on the Commission to include considerations of business identities (business representations) in its preparatory work. The current eIDAS Regulation does not adequately regulate this issue. It is necessary to break down the barriers that prevent EU citizens and businesses from accessing digital services across Member States. Efforts should be made to establish a legal framework for the cross-border recognition of powers, rights and mandates.

Policy Option 2: Private Sector Extension
This option consists of a more far-reaching legislative intervention and intends to extend the scope of the eID Regulation under eIDAS to the private sector, notably introducing new trust services for identification, authentication and for the provision of attributes, credentials and attestations and allowing the provision of identification for devices. The introduction of requirements for digital identity providers to help enforce the provisions of the GDPR will be considered. In this context, digital services providers, when acting as providers of digital ID services, could be required to keep data collected for the purpose of user identification and the provision of the digital ID service separate from data generated by the user's subsequent activity on the third-party service providers' website. The digital ID service provider could be precluded from using data generated without consent from the user.

The Danish Government's opinion

General Comment
The Danish Government acknowledges the Commission's ambitious goal of extending the eIDAS Regulation to the private sector, but considers some of the proposed initiatives too far-reaching. These are highlighted below.

Recalling the comment on Option 1, "The Private Sector", the Danish Government believes that it is crucial that it remains possible for all Member States to use existing systems that already adhere to the eIDAS Regulation without additional costs imposed by new EU legislation.

The main challenge at the European level is to highlight the value of usage for the private sector and to identify, document and remove barriers to using eIDAS, such as payment and registration requirements.

Merging Levels of Assurance Standards
Several Member States in the EU have developed their eID infrastructures based on the concept of LoAs, either by integrating the eIDAS model into national frameworks or by referencing the eIDAS Regulation. The requirements related to the different LoAs is part of the requirements for the procurement of new eID schemes and the processes related to issuance, revocation and governance, implemented into national processes. Changing the amount of LoAs to two, or, as it has been proposed, to use the same model as trust services with qualified and unqualified services would potentially require Member States to make considerable changes if they are to stay aligned with the eIDAS Regulation.

Experience from previously completed peer reviews have shown that there are substantial issues regarding differentiating between Assurance Level 'Substantial' and 'High' for an electronic identification scheme. A frequent issue is the requirements to the issuance processes, which do not allow much flexibility in actual terms. Rather it frequently becomes variations of physical presence. Work should be started on clarifying what the purpose and risk profile of an electronic identification scheme at level 'Substantial' should be, and then work must commence on providing requirements that fulfil this. This would benefit all Member States.

In Denmark, for instance, the 'National Standard for Assurance Levels' is aligned with the eIDAS Regulation and Implementing Act EU 2015/1502. This standard is known and followed by all service providers and identity providers in Denmark. Thus, the Danish Government emphasises that it is necessary to avoid extensive changes to the eIDAS Regulation, which would require implementing extensive changes to the national standard to retain alignment. This would incur extensive consequences for stakeholders who presently rely on the national standard. The stability of central legislation, such as eIDAS, is of significant importance.

The next generation of the Danish national eID, MitID, has based many of its requirements on the current eIDAS Regulation, and the contractor is required to initiate the notification process following the current notification procedure and the requirements to the levels of assurance present in the eIDAS Regulation and the implementing acts. Changing the requirements would force the Danish Government to change the requirements and the procurement in order to follow the changed process for notification and the requirements fulfilment, which would be financially unacceptable.

eID as a Trust Service

It has not been demonstrated how or why the private sector might prefer a model where eIDs would be seen as a trust service or how it would make it easier to go through the notification procedure, nor has the desired effect itself of the changed approach been documented. It is unclear how it would be easier for a conformity assessment body to complete a review of an eID when national experts from each Member State already participate in the peer-review process. It would also likely turn into an audit, as opposed to the current situation, where the peer review builds trust and promotes knowledge sharing across the different Member States, which has long been a valued and protected principle.

The Danish Government calls on the Commission to specify any plans for an additional chapter on eIDs as a trust service with a special focus on governance, the handling of eIDs that already function as trust services (e.g. NemID) and the possibility for private providers to use the existing eIDAS interoperability infrastructure in the form of the eIDAS nodes. If eIDs are considered a trust service, it is essential to clarify the relationship between eIDs regulated under the current eID regulation (eIDAS Chapter 2) and eIDs regulated as a trust service (proposed new chapter). A scenario where only privately issued eIDs would be considered as trust services would create two parallel systems with different requirements, obligations and conditions. This would make it more difficult to communicate and understand the eIDAS Regulation and electronic identification scheme notification model to the service providers whom rely on a secure and trustworthy model. Service providers would have to understand and the differentiate between privately issued eIDs and ones issued by Member States in order to adopt appropriate risk profiles for their specific services.

Governance – Cooperation Network / Supervisory Framework

Within the Cooperation Network, the European Commission has proposed three different sub-models for governing and integrating to the existing eIDAS Regulation; (1) the status-quo (eIDs issued by the private sector would be integrated to the current set of the current trust services – the eID chapter would remain untouched), (2) extending the Cooperation Network mandate (to endorse privately issued qualified eID schemes to be deployed and recognised at European level) and (3) by establishing a European supervisory authority for trust services.

It is unclear how sub-model 1 can be achieved as each Member State currently designate a Conformity Assessment Body and Supervisory Body to facilitate the approval of trust services. Consequently, this means that it would be the individual Member States' responsibility to approve privately provided electronic identification schemes while the publicly provided would still be going through the current notification process. This would result in the two types of eIDs being kept separate and be subject to different requirements and governance models, making it more difficult for service providers and other stakeholders to gain knowledge and build trust across systems.

Sub-model 2 and 3 deviate from the trust service model established in the eIDAS Regulation where the Conformity Assessment Body provides an assessment report to the supervisory body appointed by the Member State. Instead, it would either be the Cooperation Network being mandated to endorse the privately issued electronic identification schemes or the creation of a European Supervisory Authority for Trust Services. In order to retain some parity between the publicly and privately provided eIDs the Cooperation Network must continue its current role of formulating opinions on eIDs and endorsing their notification.

Sub-model 3 would remove the obligations of the Member State and thereby the ability to gain the same level of insight into the trust and security related to a privately provided eID, which would fully ensure that the two models of eIDs would be separate, and it would remove the basis for comparison and joint evaluations.

Attributes Services as Trust Services
The introduction of attribute services as a type of trust service with all the requirements and obligations currently contained in the eIDAS Regulation would form the basis for a larger degree of data sharing. It would help pave the way for the recognition of attributes on representation and other valuable information, which would help the fulfilment of the requirements under the Single Digital Gateway Regulation. As such, the Danish Government supports the proposal of incorporating attribute services as a trust service.

Identification for Devices
The Danish Government is interested in the Commission's thoughts on ensuring identification of units and recognises that there is a need to identify units, including non-human actors. However, the Danish Government believes that it is essential to ensure a high level of flexibility in any eID regulation and therefore does not believe that the regulation should be part of the eIDAS Regulation.

Policy Option 3: European Digital Identity
This option would introduce a European Digital Identity scheme (EUid) complementary with eIDAS for citizens to access online public and private services when identification is necessary. The use of EUid would be voluntary. The introduction of requirements for online service providers to accept and recognise EUid will be considered, as well as requirements for Member States to ensure general availability and access to eIDs and to make notification of national eID schemes under eIDAS mandatory.

It is currently undecided whether the Commission will suggest an underlying structure of national eIDs, where EUid is a superstructure or front, or whether EUid would be an independent solution. For example, the IIA contains mixed characterisations, sometimes referring to a common EU scheme, sometimes to a single, universal eID. However, within the Cooperation Network, the Commission has proposed three policy sub-options in regards to establishing the EUid of Option 3: (1)

EUid as an aggregator of existing national eID schemes – an extension of the current eIDAS framework; (2) Introduction of a new European eID scheme managed by an EU Body; (3) Introduction of a new European eID scheme managed by a consortium / association current eIDAS framework.

The Danish Government's opinion

General Comment

The Danish Government recognises and acknowledges the Commission's objective of creating a better framework for personal data protection and the need for a safe, legal counterweight to commercial eIDs, while also supporting Member States without existing strong, viable national eIDs.

However, the Danish Government has a number of reservations to Option 3. Some of these have previously been set out in the Danish Government's non-paper on EUid.

The eIDAS Regulation in its current iteration has the potential to provide the citizens of Europe access to both public and private services as long as these are connected to a national node. Citizens will be able to choose the electronic identity scheme from which they have an electronic identification means in order to authenticate them-selves. This is the baseline of the eIDAS Regulation. It is difficult for The Danish Government to identify assured benefits and changes provided by the adoption of the EUid sub-option 1 as an aggregator of existing national eID schemes, which are not possible to attain by pursuing Policy Option 1 and to some extent Policy Option 2.

Protection of the Data Protection and Privacy Rights of EU Citizens

The Danish Government recognises the Commission's desire to develop an alternative to private service providers who offer their services as an eID solution to ensure better protection of personal data.

The Danish Government assesses that an increased focus on personal data protection can take place within the existing eIDAS framework. The Commission should examine the possibilities for regulating differently for, on the one hand, data obtained in connection with private service providers making their services available as an eID, and, on the other hand, data obtained in connection with citizens' unrelated actions in the private sector service provider services. This work should be closely linked with the work of the ongoing revision of the GDPR Regulation.

Study the Potential EU Citizens' use of EUid

Option 3 is based on the assumption that EU citizens would use an EUid if one was developed. As far as the Danish Government is aware, it is presently undocumented that this is probable. The Danish Government therefore calls on the Commission to fully assess whether it is likely that a sufficient number of EU citizens would use an EUid before developing any proposal.

Additionally, if an EUid was developed in an advanced form, socially inclusive alternative solutions must be ensured for citizens who *cannot* or *do not wish to* use an EUid. The Danish Government is willing to share experiences on social inclusion in regards to our national eID, NemID.

The Relationship of EUid and National eID Solutions

The Danish Government calls on the Commission to elaborate what the relationship between EUid and national eIDs could look like. The Danish Government is particularly interested in understanding whether an EUid could function as a simple broker and thus facilitate the Member State process of recognising one another's eID solutions.

Through the Cooperation Network, the Commission has deliberated three sub-options for the technical design of an EUid solution. If pursued further, it is crucial for the Danish Government that costs for Member States with a high degree of eID legacy are minimised and therefore that any EUid solution is based on the existing eIDAS infrastructure.

Experience and insights from our work on the implementation of the eIDAS Regulation over the past years raise concerns regarding the development of a distinct EUid - especially if separated from the eIDAS Regulation (sub-option 2 and 3). The Member States are very different with respect to their implemented eID schemes and the general approach to electronic identification and electronic service provision. Negotiations about an EUid could expose many technical, political, legal and practical uncertainties and challenges—as well as challenges to eID-issuance, basic subsidiarity concerns on issuance of identities, general governance and division of responsibilities.