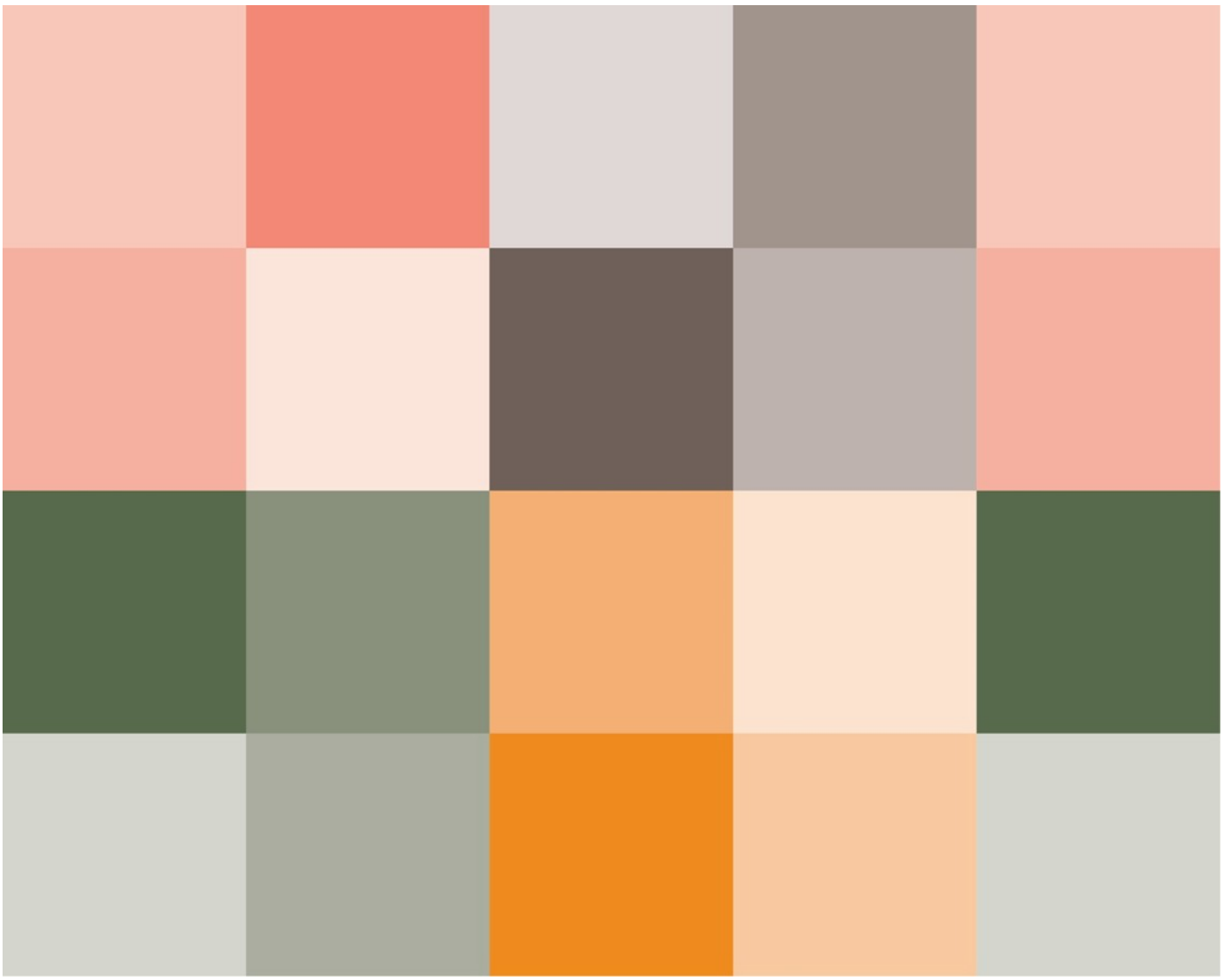

Impact assessment for the Regulations on requirements for provider applications for connection to authorisation systems for electronic identification and digital mail services

17 December 2024

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Reference number 2024-7906

Summary

On the basis of Section 6 of the Ordinance (2023:709) on authorisation systems for electronic identification and digital mail services, the Swedish Agency for Digital Government (Digg) intends to adopt regulations laying down requirements that are to be met in order for a provider's application for connection to authorisation systems for electronic identification and digital mail services to be approved.

Digg is the providing authority of authorisation systems[1] for electronic identification and digital mail services. As the providing authority of authorisation systems, Digg shall, among other things, set requirements that are to be met in order for a provider's application for connection to authorisation systems to be approved. All the requirements that must be met in order for a provider's application for connection to authorisation systems to be approved shall be published by Digg on a website.[2]

Digg has been authorised by the Government to issue regulations on the requirements that must be met in order for a provider's application for connection to an authorisation system to be approved. This impact assessment relates to the requirements that Digg intends to set in regulations.

[1] Section 2 of the Ordinance (2023:709) on authorisation systems for electronic identification and digital mail services.
[2] Section 6 of the Act (2023:704) on authorisation systems for electronic identification and digital mail services.

Table of contents

1 Introduction

1.1 What is an authorisation system?

In January 2024, the Act (2023:704) on authorisation systems for electronic identification and digital mail services (hereinafter the Authorisation Systems Act) entered into force. The Act lays down provisions on authorisation systems for services for the electronic identification of individuals and for digital mail (hereinafter 'authorisation systems').

Authorisation systems are a means for public entities to acquire services for electronic identification[3] and for digital mail[4] without having to procure[5] the services. It is also a way for providers of electronic identification and digital mail services to offer their services to public entities[6].

Digg has been designated as the providing authority of authorisation systems[7] which means, among other things, that Digg must set requirements that must be met in order for a provider's application for connection to an authorisation system to be approved. The regulations that Digg is now developing lay down the draft requirements that must be met in order for a provider's application for connection to authorisation systems to be approved. Requirements are also laid down in the Authorisation Systems Act.

All the requirements that must be met in order for a provider's application for connection to authorisation systems to be approved shall then be published on a website. This means that Digg is also able to impose additional requirements for approval, provided that they are published on a website.

Digg will then screen providers against the requirements imposed. Providers that meet the requirements shall be approved by Digg, which will then enter into an agreement for the implementation of the services. There will be no selection of providers; instead, all providers who meet the imposed requirements may sign agreements to offer their services.

Public entities may, in turn, enter into agreements with Digg to use the services in their operations. Authorisation systems also allow individuals to

---

[3] *Electronic identification* means the same as in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (see Section 3 first paragraph of the Authorisation Systems Act).

[4] *Digital mail* means electronic mail sent from a public entity to an individual through the infrastructure shared by public authorities for digital mail (see Section 3 second paragraph of the Authorisation Systems Act).

[5] For a more detailed description of the relationship between authorisation systems and public procurement, the reader is referred to recital 4 of Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.

[6] For a definition of the entities covered by the term *public entity*, the reader is referred to Section 4 of the Authorisation Systems Act.

[7] Section 2 of the Ordinance (2023:709) on authorisation systems for electronic identification and digital mail services designates Digg as the providing authority of authorisation systems.

choose which provider will perform the services for them in their contact with the public entity.

1.2 Digg will establish two authorisation systems

Digg initially intends to establish two authorisation systems: one authorisation system for electronic identification services and one authorisation system for digital mail services. The present draft regulations lay down those aspects of the requirements that must be met in order for a provider's application for connection to the respective authorisation system to be approved.

In this context, it should be noted that the draft regulations do not preclude Digg from establishing more authorisation systems for electronic identification and digital mail services in the future.

1.3 Digg will provide infrastructure for electronic identification and digital mail

In addition to being the providing authority for authorisation systems, Digg also provides the infrastructure for electronic identification which consists, inter alia, of the *Trust Framework for Swedish e-identification*.[8] The framework is based on international standards and reflects the requirements set out in the eIDAS Regulation,[9] as well as rules that apply to Swedish eIDs. The framework specifies the requirements that are to be met in order to ensure the specified assurance level in issued eIDs.

Digg also provides the infrastructure shared by public authorities for digital mail called Mina meddelanden (EN: My Messages).[10] Connected to the infrastructure shall be public entities, individuals who have requested access to digital mail from public entities, and providers of electronic mail delivery services and electronic mailboxes (mailbox operators). In order for a letterbox operator to connect to the infrastructure, it must be screened and approved by Digg based on the requirements applicable for connection to the infrastructure.

1.4 Scope of the impact assessment

An impact assessment shall be proportionate to the scope and effects of the proposal or decision.

The legislator has already decided that authorisation systems for electronic identification and digital mail services are to be put in place, and how they

[8] The framework is published on the Digg website, www.digg.se.
[9] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 laying down minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation).
[10] Digg's task of providing Mina meddelanden is set out in the Ordinance (2018:357) on the infrastructure shared by public authorities for digital mail. That Ordinance also regulates which entities can connect to the Mina meddelanden infrastructure.

should be put in place. The impact of putting authorisation systems in place has been investigated and described in the Government bill *Authorisation systems for electronic identification and digital mail services*, Bill 2023/24:6. This also describes the impact of the requirements set by the legislator on providers for the approval of their applications for connection to authorisation systems.

Digg's draft regulations thus constitute a subset of the requirements that must be met for the approval of applications from providers of electronic identification and digital mail services. Digg has therefore limited this impact assessment to the impact of the requirements that Digg, in the regulations, proposes shall apply to providers of electronic identification and digital mail.

1.5 Digg's work to develop and formulate the requirements

In developing and formulating the requirements that are to be met by providers, Digg has based its work on the existing rules and regulations for electronic identification and digital mail. Digg has also taken into account the now repealed Act (2013:311) on systems of choice for electronic identification services (the Systems of Choice Act) and the requirements imposed on providers within the systems of choice established pursuant to that Act.

Digg has also involved a selection of public entities (e.g. public authorities, the Swedish Association of Local Authorities and Regions [SKR] and association of local authorities), expert authorities[11] (e.g. the Swedish Companies Registration Office, the Swedish Authority for Privacy Protection, the Swedish Civil Contingencies Agency, the Swedish Police Authority, the Swedish Post and Telecom Authority and the Swedish Tax Agency) and providers of electronic identification and digital mail services in the development of the requirements. The aim of involving these entities has been to bring together the expertise of the public sector in this area and to ensure that the requirements are appropriate to the needs of public entities, and that they are also proportionate.

Digg has held meetings, both in groups and individually, with the entities to gather needs and views on the requirements that Digg now intends to impose on providers. Digg has also circulated draft requirements to a selection of the entities and received their comments. Not all comments have been taken into account within the framework of Digg's current work to formulate the proposed requirements, but Digg intends to continue working and developing authorisation systems and has, through the evidence gathered, a good starting point for future work.

In this context, it should be mentioned that all forms of cooperation that have taken place with providers have been published on the Digg website in order to enable all interested providers and potential providers to participate and have access to the same information.

[11] Expert authorities are authorities which, on the basis of their official duties, have special knowledge in the areas covered by the requirements.

2 The problem at issue and what change is sought

According to the legislator, access to government-wide, secure and controlled services from approved providers is key to the introduction of authorisation systems. Given the current security situation, the digital infrastructure needs to be robust. The services should also be developed based on the needs of citizens. These aspects are central to the formulation of the requirements for providers and their services.

By setting the requirements that must be met by providers of electronic identification and digital mail services, Digg ensures that public entities have access to robust, quality-assured government-wide services through authorisation systems.

3 Explanation of the consequences expected if no action is taken

A key task for Digg as the providing authority of authorisation systems is to ensure that public entities have access to government-wide, secure services for electronic identification and digital mail developed based on citizens' needs. To achieve this, Digg needs to impose requirements on providers.

If Digg does not impose requirements on providers to ensure that public entities have access to government-wide, secure services for electronic identification and digital mail developed based on citizens' needs, there is a risk that public entities will use services that are not secure and do not meet citizens' expectations and needs. There is also a risk that the services will not ensure a robust digital infrastructure.

It is also clear from the Act and Ordinance that Digg, in its role as the providing authority of authorisation systems, must impose requirements on providers and their services. If Digg does not impose requirements, Digg is failing to comply with the legal provisions for the establishment of an authorisation system for electronic identification and digital mail services.

4 The different options available to achieve the change and the advantages and disadvantages associated with each

4.1 Background to the laying down of requirements for providers in regulations

Under Section 6 of the Authorisation Systems Act, Digg shall publish on a website the requirements that are to be met in order for a provider's

application for connection to an authorisation system to be approved. Digg shall then, in accordance with Section 11, examine the provider's application against the requirements published by Digg on the website.

According to Digg's interpretation of the legislation, it would be sufficient for Digg to publish the requirements that must be met for a provider's application for connection to be approved on a website for them to be valid. The purpose of publishing the requirements on a website has not been further described in the preparatory work for the legislation, but Digg understands that the purpose is primarily for providers to have equal access to the requirements.

The advantage of only publishing the requirements on a website is that they would be relatively easy to amend as the need for change arises. However, the requirements set by Digg are formulated in general terms and directed at a broader audience. They shall also form the basis for Digg's decision on whether to approve a provider's application for connection to an authorisation system. Furthermore, should Digg decide to reject a provider's application for connection to an authorisation system, it would be for the administrative court to review Digg's decision against the requirements imposed by Digg on providers. Digg believes that such types of binding rules as the requirements for providers in this case are well suited to be laid down in regulations.

4.2 Requirements for providers

4.2.1 General requirements for providers

The general requirements that Digg intends to impose on providers mean that the provider must provide certain information in its application. The information is needed for Digg to process the provider's application and ultimately make a decision on the approval of the provider's application.

In addition to specific requirements for the application, the requirements aim to enable Digg, in various ways, to check the provider, its operations and its representatives. The checks, in turn, aim to ensure that the provider has both the financial and technical capacity to fulfil the agreements within authorisation systems and thus comply with the requirements that must be met by providers of electronic identification and digital mail services.

In many cases, Digg can collect information about the providers on its own, for example through access to different types of official register. Collecting the data directly from official registers reduces the risk that the information collected is outdated or tampered with in any way. In situations where Digg cannot access the information, Digg is able, according to the proposed regulation, to request the provider to submit the information in various forms of documentation. The reason why Digg requires that documentation should not be older than a certain period is to ensure that the information is up to date.

4.2.2 Requirements for providers of electronic identification services

Electronic identification services include various forms of service. For the first aspect of relevance in the context of an authorisation system for electronic identification, the issuance of eIDs, rules are provided in the Trust Framework for Swedish e-identification. Digg considers that this aspect is so essential in an authorisation system for electronic identification that it should be one of the requirements for approval that is to be specified in the regulations. The regulations thus state that a provider applying for connection to an authorisation system for electronic identification must be approved by Digg in accordance with the Swedish e-identification trust framework for the relevant assurance level.

The trust framework for Swedish e-identification is a risk-based technology-neutral framework imposing requirements on eID issuers regarding organisation, information security and physical security, as well as the design of identity checks. The framework is based on international standards with different levels of security for different ‘assurance levels’; the higher the assurance level, the higher the requirements imposed on the issuer when issuing eIDs. The trust framework for Swedish e-identification covers assurance levels 2, 3 and 4, which correspond to the assurance levels low, substantial and high in the eIDAS Regulation.

eIDs that are issued to individuals who have a personal identity number and that achieve one or more of the assurance levels 2, 3, and 4, as defined in the Trust Framework for Swedish e-identification, shall be included in the authorisation system for electronic identification. The requirement for approval under the Trust Framework for Swedish e-identification in the regulations means that providers approved by Digg at these assurance levels can demonstrate that they meet the requirements through the approval.

By referring to an approval under the Trust Framework for Swedish e-identification published on the Digg website, it becomes clear what requirements apply. Since the requirements in the Trust Framework for Swedish e-identification stem from international standards and corresponding requirements exist within the EU, the requirements can be considered well-established and generally accepted.

An alternative to requiring that a provider applying for connection to an authorisation system for electronic identification must be approved by Digg under the Trust Framework for Swedish e-identification would be to, instead of requiring approval by Digg in the regulations, merely state that the requirements of the Trust Framework for Swedish e-identification must be complied with.

Another option would be to not have this requirement at all or to only require that certain parts of the Trust Framework for Swedish e-identification be complied with. However, Digg considers that the latter is not feasible if Digg is to fulfil its mandate of providing public entities with access to standardised and secure electronic identification services. The Trust Framework for Swedish e-identification is an important cornerstone for issuing eIDs, not only in the context of the authorisation system but for electronic identification as a whole in the public sector. As regards the alternative of simply referring to the requirements of the Trust Framework for Swedish e-identification instead

of requiring approval from Digg, this is similar to the constructions found in the system of choice. However, Digg's understanding is that this type of construction was due to prevailing circumstances and Digg cannot see any benefits of such a solution under today's conditions. Such a formulation of the requirement makes it both more difficult for the provider to demonstrate that it meets the requirement and also more difficult for Digg to verify that the provider meets the requirement. Digg also considers that the terms of the connection agreement will be clearer when they can be linked to approval by Digg in accordance with the Trust Framework for Swedish e-identification. Digg could choose to impose other requirements on providers and their services that differ from existing rules and regulations.

4.2.3 Requirements for providers of digital mail services

In the requirements that are to be met for the approval of digital mail providers within authorisation systems, Digg proposes that the provider should be connected to Mina meddelanden as a mailbox operator. Such a requirement means that the provider needs to comply with the requirements applicable to mailbox operators within Mina meddelanden. It also means that providers must meet the requirements applicable to the infrastructure within which the provider is to operate.

If Digg were to impose other requirements, there is a risk that requirements will be imposed on providers that are not necessary for providing services within Mina meddelanden. Such requirements are deemed superfluous. If Digg were to impose other requirements, there is also a risk that the regulations over time would differ, and thus also the requirements on digital mail providers.

Different requirements also mean that providers would have to submit to different types of checks that are actually aimed at ensuring the same thing. This risks being costly, both for the provider and for Digg as the providing authority of authorisation systems and the infrastructure manager within Mina meddelanden. It is therefore not considered appropriate to impose requirements that deviate from the requirements that apply to mailbox operators within Mina meddelanden.

5 The option(s) deemed most appropriate and reasons for this

5.1 Digg needs to impose requirements on providers

As stated above, it is for Digg, as the providing authority, to impose requirements on providers. If Digg were not to impose requirements, there would be no authorisation systems, and thus, as Digg deems it, there are no alternatives to imposing requirements. The question is rather what requirements are appropriate to set.

5.2 Digg primarily collects information itself

As regards the requirement that the provider must submit certain documentation to demonstrate that it meets the requirements, Digg has chosen to design the requirement in such a way that Digg does not request information to which it itself has access to through official registers. In this way, unnecessary tasks are not imposed on the provider.

5.3 The requirements are based on existing rules and regulations

When designing the requirements, Digg has chosen to base them on already existing rules and regulations that apply to providers of electronic identification and digital mail. By relying on existing and already established rules and regulations, the requirements on providers do not go beyond what already applies in each industry. Existing rules and regulations also ensure that the services are government-wide and secure.

6 The authority on which Digg’s decision-making power is based

Authorisation systems for electronic identification and digital mail services are regulated by:

- the Act (2023:704) on authorisation systems for electronic identification and digital mail services; and
- the Ordinance (2023:709) on authorisation systems for electronic identification and digital mail services.

By virtue of Section 6 of the Ordinance on authorisation systems for electronic identification and digital mail services, Digg is authorised to issue regulations on the requirements that must be met in order for a provider’s application for connection to an authorisation system to be approved.

In the preparatory work (see bill 2023/24:6 *Authorisation systems for electronic identification and digital mail services*, p. 39) it is stated that Digg shall lay down generally formulated requirements for connection to authorisation systems aimed at a broader audience. These requirements will form the basis of Digg’s decision to approve a provider’s application for connection to an authorisation system. Digg is therefore authorised to issue regulations in this regard.

7 The draft regulations

The Regulations on requirements for provider applications for connection to authorisation systems for electronic identification and digital mail are to be formulated as follows.

Content of the regulations

Section 1 These regulations contain provisions on the requirements that must be met in order for a provider's application for connection to authorisation systems to be approved.

All the requirements that apply in order for a provider's application for connection to authorisation systems to be approved shall be published on the Agency for Digital Government's website, www.digg.se.

Terms and concepts

Section 2 The terms and concepts used in these regulations have the same meaning as in the Act (2023:704) on authorisation systems for electronic identification and digital mail services.

For the purposes of these regulations, the following definitions apply:

– *the connection agreement*: the agreement concluded by the Agency for Digital Government with each of the approved providers on the implementation of electronic identification or digital mail services.

– *authorisation system*: the authorisation systems for electronic identification and digital mail services established by the Agency for Digital Government by virtue of the Act (2023:704) on authorisation systems for electronic identification and digital mail services.

– *authorisation system for digital mail*: the authorisation system for digital mail services established by the Agency for Digital Government.

– *authorisation system for electronic identification*: the authorisation system for electronic identification services established by the Agency for Digital Government.

– *mailbox operator*: provider of electronic mail delivery services and electronic mailboxes connected to the digital mail infrastructure.

– *digital mail infrastructure*: the infrastructure shared by public authorities for digital mail from public entities to individuals, provided by the Agency for Digital Government by virtue of the Ordinance (2018:357) on infrastructure shared by public authorities for digital mail.

– *The trust framework for Swedish e-identification*: the framework based on international standards setting out the requirements to be met in order to ensure the reliability of issued eIDs at specified assurance levels. The framework shall be published on the website of the Agency for Digital Government, www.digg.se.

Provider’s application for connection to authorisation systems

Section 3 A provider shall apply to the Agency for Digital Government for connection to authorisation systems.

Section 4 The application must be written in Swedish and signed by an authorised representative of the provider.

At the request of the Agency for Digital Government, the provider must be able to demonstrate the representative’s right to represent the provider concerning the application for connection to the authorisation system.

Section 5 In the application, the provider shall indicate the following:

1. name;
2. corporate identity number or equivalent identification number as shown on the registration certificate;
3. postal address; and
4. details of the authorised representative of the provider.

The provider shall also specify their contact person for matters concerning connection to an authorisation system. The provider shall indicate the name, organisation, e-mail address and telephone number of the contact person.

Requirements for approval of a provider’s application for connection to authorisation systems

Section 6 A provider must be established and registered in a country within the European Economic Area, in accordance with the country’s rules on registration, in the register of public limited liability companies, the commercial register or similar register.

At the request of the Agency for Digital Government, the provider shall submit documentation equivalent to a copy of the registration certificate issued by the competent official authority.

The documentation must not be more than two months old, calculated from the date of application.

Section 7 If several providers join forces and jointly apply for connection to an authorisation system, the provider shall confirm that the collaboration, no later than when the connection agreement is concluded, will have been integrated into a legal person as is required to meet the requirement in Section 6, first paragraph.

The provider shall undertake to submit documentation in accordance with Section 6, second paragraph, at the request of the Agency for Digital Government, no later than when the connection agreement is concluded.

Section 8 A provider shall meet the legal requirements for registration for taxes and duties in the home country.

At the request of the Agency for Digital Government, the provider shall submit documentation equivalent to a copy of the registration certificate issued by the competent official authority.

The documentation must not be more than two months old, calculated from the date of application.

Section 9 A provider shall have the necessary economic and financial capacity to fulfil the obligations arising from the connection agreement for at least one year.

Section 10 A provider meets the requirement in Section 9 by having at least a rating corresponding to low risk from a credit reporting agency.

If the provider cannot be checked by the credit reporting agency commissioned by the Agency for Digital Government, the provider shall, at the request of the Agency for Digital Government, demonstrate that it meets the requirement in Section 9 by submitting, within five working days of the request, documentation equivalent to a certificate from another credit reporting agency or equivalent institution showing that the provider has at least a rating corresponding to low risk.

The documentation must not be more than three months old, calculated from the date of application.

Section 11 A provider that cannot demonstrate at least a rating corresponding to low risk in accordance with Section 10 shall, at the request of the Agency for Digital Government, provide an explanation for the divergent rating.

If the provider can furnish an acceptable explanation in accordance with the first paragraph, it may nevertheless be deemed to meet the requirement in Section 9.

Section 12 A provider shall hold valid business and liability insurance or other similar guarantees adapted to the activities of the provider. The insurance or guarantees shall cover any claims for damages caused by the provider or its staff.

The provider shall, at the request of the Agency for Digital Government, submit documentation equivalent to a copy of the insurance policy or similar certificate to demonstrate that the provider meets the requirement in the first paragraph.

Section 13 A provider shall undertake to conclude a connection agreement without reservation or objection to the content of the connection agreement.

Providers in the process of being formed

Section 14 A provider that is a company in the process of being formed shall be deemed to meet the requirements of Sections 6, 8 and 12 if the provider:

1. confirms that, no later than when the connection agreement is concluded, it will meet the requirements; and

2. undertakes to submit, no later than when the connection agreement is concluded, documentation demonstrating that it meets the requirements when the connection agreement is concluded.

Special requirements for approval of a provider’s application for connection to the Authorisation system for electronic identification

Section 15 A provider applying for connection to the Authorisation system for electronic identification must be approved by the Agency for Digital Government in accordance with the Swedish e-identification trust framework for the relevant assurance level.

Special requirements for approval of a provider's application for connection to the Authorisation system for digital mail

Section 16 A provider applying for connection to the Authorisation system for digital mail shall be connected as a mailbox operator to the digital mail infrastructure.

8 Analysis

8.1 Description and calculation of the costs and revenues arising from the regulations for the State, municipalities, regions, companies and other individuals

Digg considers that the requirements imposed on providers wishing to be connected to authorisation systems do not entail any costs or revenues for the State, municipalities or regions.

For providers wishing to apply for connection to an authorisation system, administrative costs will be incurred in the form of the working time required to complete the information requested in the application and provide the documentation requested.

Depending on what information Digg can access on its own through official registers, the working time required to complete the application and attach supporting documents will vary. Assuming that Digg can obtain most of the information itself (which should be the norm), Digg estimates that it should not take more than two hours for the provider to complete the application. At an estimated labour cost of SEK 1 000 per hour, the cost to the provider would then be SEK 2 000.

In cases where Digg is unable to verify information in official registers, there will be a cost to the provider to collect the information itself and then hand it over to Digg. Digg expects that it should not take more than eight hours (one working day) for the provider to submit all the information. At an estimated labour cost of SEK 1 000 per hour, the cost to the provider would then be SEK 8 000. In addition, there may be costs for the documentation. Costs will vary depending on the country in which the provider's information is registered. Digg estimates that the total cost of producing the information should not exceed SEK 5 000.

8.2 Outline of the measures taken to ensure that the draft regulations do not entail costs or restrictions that go beyond what is deemed necessary to achieve the objective

Under Section 5 of the Authorisation Systems Act, Digg shall comply with the principles of transparency, mutual recognition and proportionality when providing authorisation systems. This means that these principles should also apply when Digg is developing requirements for the approval of providers. Digg has therefore carefully considered the requirements to be imposed on providers and has not exceeded those that are deemed necessary.

When designing the requirements, Digg has chosen to base them on the already existing rules and regulations that apply to providers of electronic identification and digital mail. By relying on already established rules and regulations for providers of electronic identification and digital mail, the requirements on providers do not go beyond what already applies in each industry.

Digg intends, primarily, to collect the required information itself from public registers in order to reduce the administrative burden on providers.

8.3 Assessment as to whether special consideration must be given to the date of entry into force and whether special information initiatives are required

It is important that Digg establish authorisation systems as soon as possible. The requirements that must be met by providers of electronic identification and digital mail services are essential in that regard. It is therefore important for the regulations to enter into force as soon as possible. In light of this, Digg proposes that the regulations enter into force on 5 May 2025.

In Digg’s work to introduce authorisation systems, Digg will in various ways provide information about the authorisation systems and thereby also the requirements imposed on providers. The information will be provided in several ways, including through participation in the Digg Forum webinar, on the Digg website, and through targeted actions tailored to different entities.

The work of informing entities has already commenced, and Digg continuously provides updates about the work on its website.

When the draft regulations are notified to the EU (see section 8.5), Digg will provide notification on its website about this, as well as the requirements that are to be met. Once the rules have been reviewed, Digg will also provide notification of this. It is important to Digg that both potential providers and public entities receive the information.

Once the regulations enter into force, Digg will publish all the requirements on a website in accordance with the requirements for publication laid down in the Authorisation Systems Act.

8.4 Description of how and when the impact of the draft regulations can be evaluated

8.4.1 Evaluation of the form of regulation

Since both the regulation of authorisation systems and the task of Digg to provide authorisation systems are new, Digg will need to evaluate whether the regulation laying down the requirements for providers in regulations is an appropriate form.

A first evaluation will be carried out at the end of 2025, in conjunction with Digg evaluating how the Agency has worked with the introduction of authorisation systems. Thereafter, evaluation will be carried out when the requirements are reviewed, which will take place at least every two years.

If the draft rules are examined by a court, Digg will also carry out an evaluation of how the court has applied and interpreted the regulation in connection with its examination. Digg will therefore carry out an overhaul when an administrative court examines a decision rejecting a provider's application for connection to an authorisation system for the first time.

8.4.2 Evaluation of the requirements on providers

Digg intends to continuously monitor the proposed requirements in order to assess whether they enable public entities to access robust, quality-assured government-wide services through authorisation systems. Digg intends to continue working with authorisation systems as early as 2025 and review the requirements set in order to see if they need to be supplemented in any way. Digg also needs to ensure that the requirements imposed are not unnecessarily administratively burdensome for providers, and whether measures can be taken to reduce the provider's administrative burden associated with the application.

In order to monitor the requirements, Digg intends, among other things, to have follow-up meetings with providers, public entities applying the regulations and expert authorities.

In the agreements that Digg develops and will apply to providers connected to authorisation systems, Digg reserves the right to invite providers twice a year to participate in follow-up meetings with Digg.

Digg will also evaluate, after the authorisation system has been established, whether the benefits that the legislator has envisaged from the introduction of authorisation systems are achieved through Digg's introduction or whether there is reason for Digg to change something in, for example, the requirements on providers.

8.5 Assessment of whether the draft regulation is in line with Sweden’s obligations as a Member State of the European Union.

When authorities develop certain types of regulation, there may be an obligation to notify the drafts to the EU. Examples of notification obligations can be found in Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (the ‘Single Market Transparency Directive’), and in Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (the ‘Services Directive’).

Digg considers that there is an obligation to notify the draft regulations to the EU.[12] Digg therefore intends to submit this impact assessment and the related draft rules to the National Board of Trade of Sweden to be forwarded to the EU in December 2024.

It is Digg’s assessment that the draft requirements are consistent with the obligations arising from Sweden’s membership of the EU.

[12] Section 1 of the Ordinance (1994:2029) on technical regulations.