MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Authorisation system for electronic identification – Connection agreement

Draft 2024-12-12

Table of contents

1. The parties to the Agreement

This Agreement (the 'Connection Agreement') on connection to the Authorisation system for electronic identification has been concluded between:

Providing authority (Digg), reg. no 202100-6883, (providing authority)

and

[Provider company name], reg. no [xxxxxx-xxxx] (provider)

Together referred to as the parties.

2. Term of the Agreement

The Connection Agreement shall enter into force on _____.

The date of entry into force presupposes that both parties have signed the Connection Agreement.

The Connection Agreement will then remain in force until further notice.

Either party has the right to terminate the Connection Agreement in writing by giving twelve (12) months' notice, calculated from the end of the month following the notice of termination.

3. General

3.1 Authorisation system for electronic identification

According to the Act (2023:704) on authorisation systems for electronic identification and digital mail services, an authority shall provide authorisation systems for, inter alia, electronic identification.

An authorisation system within the meaning of the Act means a system in which:

1. the authority providing the system approves that providers of services for electronic identification for individuals or for digital mail may enter into a Connection Agreement within the system and enter into Connection Agreements with each of the approved providers for the provision of such services,
2. an individual has the right to choose the provider that will perform the services on behalf of the individual, and
3. a public entity may use the services in the course of its activities under the Connection Agreement with the providing authority.

According to the Ordinance (2023:709) on authorisation systems for electronic identification and digital mail services, Digg has been designated as the providing authority of authorisation systems for, inter alia, electronic identification.

3.2 Approval and conclusion of the Connection Agreement

According to the Act, the providing authority shall approve a provider's application for connection to an authorisation system for those providers that meet the requirements for approval.

Once the providing authority has made a decision to approve a provider, the providing authority shall, as soon as possible, enter into a Connection Agreement with the provider for the performance of the service.

By entering into a Connection Agreement, the provider connects to the Authorisation system for electronic identification.

4. Definitions

The terms and concepts used in the Connection Agreement have the same meaning as in the Act (2023:704) on authorisation systems for electronic identification and digital mail services and in the providing authority's Regulations on requirements for provider applications for connection to

authorisation systems for electronic identification and digital mail, MDFFS 2025:X.

For the purposes of this Connection Agreement, the following definitions apply:

a) *User*: a natural person who holds an eID issued by a provider and who, when using the eID, is identified by an identification and certification function.

b) *Advanced electronic signature*: a signature that meets the requirements for an advanced electronic signature as defined in Article 26 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.

c) *Calculation data:* is defined in Annex 3 – Technical specification for calculation data.

d) eID: an electronic identification document of document quality containing data that can be unambiguously linked to a specific user.

e) *Electronic identification:* an automated check of who has identified themselves.

f) *Electronic signature function*: technical function in the eID to produce an advanced electronic signature.

g) *Identification and certification function:* a service where the provider carries out automated checks, issues the certificate of identity, and sends the certificate of identity to the public entity that ordered it.

h) *Certificate of identity*: electronically signed certificate in electronic form stating the user's identity and attributes.

i) *ID switching*: a procedure whereby an eID is used to increase trust in another already existing eID or to create a new eID

j) *Authentication*: a user uses their eID.

k) *Authentication function*: technical function where the user authenticates themselves for access, submission of information, or signature.

l) *Provider*: an operator who has fulfilled the requirements laid down for approval to authorisation systems for electronic

identification services and who enters into this Connection Agreement.

m) *Cooperation connection:* a connection where an issuer of eIDs is part of a close cooperation with an issuer of identity certificates. Such cooperation shall be lasting and characterised by long-term planning, and shall involve a close technical and organisational link between the issuer of eIDs and the issuer of identity certificates. Furthermore, there must be an ownership relationship between the issuer of the identity certificate and the issuer of eIDs. Upon such connection, the issuer of the identity certificate shall be deemed to be the provider as defined in the Connection Agreement and the issuer of eIDs shall be its subcontractor.

n) *Technical framework*: framework with technical specifications for the identity federation Sweden Connect. The framework is published on the website of the providing authority, www.digg.se.

o) *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 is published on the website of the providing authority, www.digg.se.

p) *Public entity:* the same meaning as in the Act (2023:704) on authorisation systems for electronic identification and digital mail services.

5. Description of authorisation system for electronic identification services

5.1 A provider *shall* provide, in the authorisation system for electronic identification, eIDs issued to individuals who have a personal identity number. A provider *may* also provide eIDs issued to individuals with coordination numbers.

eIDs shall achieve one or more of the assurance levels 2, 3, and 4 as defined in the trust framework for Swedish e-identification.

The authorisation system for electronic identification services is designed in such a way that the provider connecting to the authorisation system and signing the Connection Agreement undertakes to:

a) issue relevant eIDs in accordance with the trust framework for Swedish e-identification at the assurance level for which providers are approved in accordance with the trust framework for Swedish e-identification,

b) provide functions where:

- users authenticate themselves for access, reporting or electronic signature (authentication function),
- the user is identified and a certificate is issued to confirm the identity (identification and certification function),
- the user is identified and a certificate is issued indicating who has signed (electronic signature function),

c) provide the certificates (identity certificates) with information about the user's identity and attributes as well as the electronic signature of the eID provider, and

d) deliver the identity certificate to the public entity that ordered the certificate, using data registered in the entity catalogue if the provider makes the services available in accordance with the technical framework.

5.2 The provider may offer the possibility of ID switching.

6. Connection agreement documents and order of interpretation

6.1 The Connection Agreement includes this main text (the 'Main Agreement') and the following Annexes:

Annex 1 - Application submitted by the provider for connection to an authorisation system demonstrating compliance with the providing authority's Regulations on requirements for provider applications for connection to an authorisation system for electronic identification (Ref [No])
Annex 2 - Remuneration, calculation and invoicing
Annex 3 - Technical specification for calculation data

If there are conflicting provisions in the documents constituting the Connection Agreement, the Main Agreement shall prevail over the Annexes, unless the circumstances clearly indicate otherwise. The Annexes shall take precedence over each other in the order of their numbering. If the parties have decided on additions or amendments to the Main Agreement, these amendments shall take precedence over the provisions of the Main Agreement.

The versions of Annexes 2 to 3 currently in force are available on the website designated by the providing authority.

7. Commitments and obligations of the providing authority

7.1 The providing authority undertakes to remunerate the provider in accordance with Annex 2 – Remuneration, calculation and invoicing.

7.2 The providing authority shall, if it detects inaccuracies in the transmitted calculation data, immediately and in writing, notify the provider thereof.

8. Responsibilities and obligations of providers

8.1 Professionalism

8.1.1 The provider shall meet the requirements applicable for the approval of a provider's application for connection to the Authorisation system for electronic identification throughout the term of the Agreement.

8.1.2 The provider shall, at the request of the providing authority, be able to provide documentation that substantiates compliance with the requirements for approval.

8.1.3 If there are changes to the information provided by the provider regarding compliance with the requirements for approval, the provider shall immediately provide information to the providing authority in accordance with Point 8.14.

8.1.4 The provider shall comply with the trust framework for Swedish e-identification in force, which is published on the website of the providing authority, www.digg.se, and carry out their duties in a professional manner and in accordance with this Connection Agreement, applicable statutes, administrative decisions and good industry practice in the relevant field.

8.2 Issuance and provision

8.2.1 The provider shall issue eIDs to users and provide the authentication function.

In the case of a cooperation connection, the provider shall provide issued eIDs and the authentication function. The providing authority assesses whether conditions are such that a cooperation connection exists.

8.2.2 The eIDs and the provision of the authentication function shall comply with the requirements of the trust framework for Swedish e-identification.

The provider is responsible for ensuring that:

a) eIDs covered by the Connection Agreement meet the requirements of the trust framework for Swedish e-identification,

b) the user interface is designed in such a way that it is clear which public entity has requested authentication, and

c) the user interface in the authentication function is designed so that it is clear when the eID is used for authentication and signature.

8.3 Identification and certification function, identity certificates and advanced electronic signatures

8.3.1 The provider shall provide an identification and certification function relating to identification when using an eID covered by the provider's undertaking as well as an electronic signature function.

8.3.2 The provider is responsible for ensuring that identity certificates have been duly signed electronically in accordance with the technical framework or other connection method referred to in Point 8.4.

8.3.3 The provider has the right, upon notification to the public entity and the providing authority, to make technical changes that do not change the services the provider provides under the Connection Agreement.

8.4 Technical connection method

8.4.1 Providers shall provide a connection method based on accepted standards and technical principles in the fields of electronic identification and electronic signature.

8.4.2 The connection method shall follow the technical integration patterns specified in the technical framework or another connection method.

8.4.3 Providers are responsible for ensuring that if a connection method other than that specified in the technical framework is used, this connection method achieves functionality and security equivalent to that of the technical framework.

8.5 Availability

8.5.1 The provider shall provide the identification and certification function and the electronic signature function with an availability of at least 99.9 % per month, excluding the Internet connection from the public entity to the provider. The response time for the identification and certification function and the electronic signature function, excluding the Internet connection response time and user time, shall be less than one second for 99.9 % of transactions.

8.5.2 The provider may limit the availability and/or use of the identification and certification function and the electronic signature function due to planned maintenance actions that are necessary for development, maintenance or operational reasons. Planned interruptions shall always be scheduled for periods when the use of the identification and certification function and the electronic signature function is at its lowest (for example, at night). Planned outages shall be reported in accordance with Point 8.13.1.

8.5.3 Unplanned outages may be due to unforeseen and unplanned events that require the provider to quickly implement an unplanned service interruption. The provider shall take measures to reduce the number of unplanned interruptions and to minimise the interruption time in the event of unplanned interruptions. Unplanned interruptions shall be reported immediately in accordance with Point 8.13.2.

8.6 Blocking of eIDs

8.6.1 The provider shall provide a blocking service 24 hours a day, 7 days a week, where the user can block their eID.

8.6.2 The provider shall promptly and safely process and execute the blocking request.

8.7 Support and customer service

8.7.1 The provider shall offer support to the user in Swedish and the other languages covered by the provider's service

8.7.2 The provider shall provide customer service with good availability where the user, the providing authority, and the public entity, by telephone, e-mail, or other appropriate contact route, can ask questions regarding the provider's services. Contact details for such customer service shall be published on the provider's website.

8.8 Technical integration

8.8.1 The provider shall, to the extent that may reasonably be required, at the request of the public entity, provide any additional information that, in connection with a user contesting the accuracy of the performed identification and certification function or electronic signature function, may be needed to verify the delivery of or the data in the performed identification and certification function or electronic signature function.

8.8.2 The provider and the public entity shall verify the identity of the counterparty and protect their communication against tampering and forgery through the technical and administrative measures specified for the chosen technical connection method according to Point 8.4.

8.8.3 To the extent that the public entity makes use of another party for the integration of the identification and certification function or the electronic signature function in the business conducted by the public entity, the provider shall cooperate with such party to the extent necessary for the integration of the identification and certification function or the electronic signature function.

8.9 Activation and participation in testing

8.9.1 The provider shall, to the extent necessary, within such reasonable time prior to the activation of the identification and certification function or the electronic signature function as communicated by the public entity, provide connections and functionalities for testing in accordance with the requirements set out in this Section and otherwise to a reasonable extent in the manner specified by the public entity.

8.9.2 The provider shall provide opportunities for the public entity to perform acceptance tests of the identification and certification function or the electronic signature function. The provider shall, inter alia, provide an environment in which acceptance tests can be carried out.

8.9.3 The provider shall offer the public entity the opportunity for increased participation in tests, such as performance tests or extended opening hours for customer service.

8.9.4 The provider shall offer support and processes for ordering and issuing the identification and certification function or the electronic signature function for testing. The identification and certification function or the electronic signature function for testing shall be available to the test persons designated by the public entity.

8.9.5 The provider shall provide information on how tests are run against the provider's identification and certification function or the electronic signature function. This information shall include how the procurement of the test of e-identification can be carried out, how the public entity can access log information, as well as the fault reporting process and contact details.

8.9.6 In the test version of the identification and certification function or the electronic signature function, the provider shall ensure that error situations are described to the testing party. This can be done through an extended error reporting interface or through other processes such as the distribution of logs to the testing party.

8.10 Subcontractors

8.10.1 Only the provider can be the legal counterparty of the providing authority in the Connection Agreement.

8.10.2 The provider has the right to subcontract. The provider shall ensure that the requirements applicable to the provider are also met by engaged subcontractors who are directly involved in fulfilling the Connection Agreement, regardless of the number of intermediaries.

8.10.3 The provider shall, at the request of the providing authority, provide information on which subcontractors the provider uses to fulfil the Connection Agreement.

8.10.4 The provider is responsible for the work of contracted subcontractors as for his own work. In the case of cooperation connection, the provider is also responsible for the actions of the subcontractor as if the actions had been carried out by the provider itself.

8.10.5 The providing authority has the right to check during the contract period that specified subcontractors have paid taxes and statutory fees, and in respect of the tasks assigned to subcontractors, meet the same requirements as are imposed on the provider under the Connection Agreement.

8.10.6 The provider shall assist the providing authority in carrying out the verification and provide the necessary information to enable the providing authority to carry out the specified verification.

8.10.7 If, upon verification, the providing authority finds that a subcontractor contracted by the provider does not meet the requirements, the providing authority is entitled, unless remedial action is taken in accordance with Point 16, to require the provider to replace the subcontractor in question.

8.11 Abuse of services provided

8.11.1 If a provider detects misuse of the services that the provider shall provide under this Connection Agreement, the provider shall immediately suspend the relevant service or take other appropriate measures to prevent repeated misuse.

8.11.2 The provider shall, to a reasonable extent, participate in the investigation of misuse of the service.

8.12 Reporting of changes in the service and other commitments to the public entity and providing authority

8.12.1 The provider shall report to the public entity and the providing authority planned changes in the service, such as new or changed functions in the service or other changes that may have an impact on the public entity.

8.12.2 The reporting of changes regarding technical integration shall, to the extent that they require a change to the interface between the provider and the public entity, take place at least six (6) months before the change enters into force.

8.12.3 Reporting in accordance with the above shall be carried out in accordance with a procedure developed by the providing authority in consultation with providers and public entities and published on the website of the providing authority.

8.13 Reporting of interruptions and unforeseen events to the public entity and the providing authority

8.13.1 The provider shall report planned interruptions to the public entity and the providing authority with sufficient advance notice to enable the public entities to take the necessary measures due to the interruption, and always at least 48 hours in advance in accordance with Point 8.5.2.

8.13.2 The provider shall immediately report to the public entity and the providing authority any unplanned interruptions in accordance with Point 8.5.3.

8.13.3 The provider shall immediately report to the public entity and the providing authority any misuse of services or any other unwanted and unplanned event affecting the security of the services to be provided by the provider under the Connection Agreement.

8.13.4 Reporting in accordance with the above shall be carried out in accordance with a procedure developed by the providing authority in consultation with providers and public entities and published on the website of the providing authority.

8.14 Reporting of changes to the providing authority

The provider shall immediately, in writing, notify the providing authority of:

- any changes or updates to the information provided in the application for connection to the Authorisation system for electronic identification,
- material changes in the provider's performance of its obligations under this Connection Agreement,
- circumstances affecting the provider's ability to fulfil its obligations under the Connection Agreement,
- other circumstances of the provider that risk damaging or harm confidence in the authorisation system for electronic identification.

Reporting in accordance with the above shall be carried out in accordance with a procedure developed by the providing authority in consultation with providers.

8.15 Reporting of calculation data to the providing authority

8.15.1 The provider shall report calculation data to the providing authority in accordance with Annex 2 – Remuneration, calculation and invoicing and Annex 3 – Technical specification for calculation data.

8.15.2 If the provider discovers inaccuracies in the reported calculation data, the provider shall immediately notify the providing authority in writing of the inaccuracy.

8.16 Internal Audit

Each year, after the completion of each internal audit, the provider shall, in accordance with the provisions of the trust framework for Swedish e-identification, send an audit report to the providing authority. The audit report must be submitted to the providing authority no later than one month after the internal audit is completed in accordance with the established audit plan.

8.17 Social and labour conditions

8.17.1 In the performance of the Connection Agreement, the provider shall provide an acceptable level of working conditions for the employees and contractors involved in the performance of the Connection Agreement. Acceptable conditions means offering conditions on a par with, or higher than, collective agreements in the sector.

8.17.2 The provider shall, at the request of the providing authority, be able to provide documentation demonstrating compliance with these requirements.

8.18 Anti-discrimination

8.18.1 In its operations, the provider shall not discriminate against anyone on the basis of gender, transgender identity or expression, ethnicity, religion or other belief, disability, sexual orientation, age or other. The provider undertakes to comply with applicable anti-discrimination legislation.

8.18.2 The provider shall have in place policies and procedures to prevent discrimination and take action in the event of deviations. Policies and procedures shall be available if requested by the providing authority.

8.19 Prevention of corruption

8.19.1 The provider's operations shall be free from corruption and other irregularities. Corruption and irregularities here refer to both criminal acts, such as giving and taking bribes, and behaviour that can be perceived as damaging to trust by outsiders.

8.19.2 The provider shall work systematically to actively prevent, detect and deal with corruption and irregularities.

8.19.3 If requested by the providing authority, the provider shall be able to demonstrate established procedures for preventing and combating corruption and other irregularities within the business.

9. Prohibition of transfer

A provider shall not be entitled to assign its rights or obligations under
the Connection Agreement to another party.

10. Confidentiality

The provider undertakes not to disclose or in any way use confidential information that the provider obtains through the implementation of services included in this Agreement.

11. Intellectual property rights

This Connection Agreement shall not be deemed to entail the transfer, assignment, or licensing of any intellectual property right from one party to another.

12. Amendments and additions to the Main Agreement and the trust framework

12.1 The provider and the providing authority may call for a change to the Main Agreement. Amendments and additions shall be made only after consultation between the parties and after the parties have consented to the amendment or addition.

12.2 The providing authority may, after informing and consulting with the provider, make amendments or additions to the Connection Agreement if the providing authority deems this necessary due to requirements in law or other statutes, binding legal acts within the European Union, government decisions, or authority decisions.

12.3 The providing authority also reserves the right to make changes and additions to the trust framework for Swedish e-identification in accordance with the authority's internal regulations on change procedures for services and agreements for e-identification published on the providing authority's website, www.digg.se. The procedure states that the providing authority must consult and provide information to a reasonable extent before any additions or amendments are made.

12.4 Any amendments and additions to the Main Agreement shall be made in writing and signed by an authorised representative of each party in order to be effective.

13. Amendments and additions to Annex 2 and Annex 3 of the Connection Agreement

13.1 The providing authority shall review the terms of Annexes 2 to 3 of the Connection Agreement at least annually. The providing authority has the right to unilaterally make amendments and additions to Annexes 2 to 3 of the Connection Agreement. Changes and additions shall be published on the website designated by the providing authority and communicated to the provider.

The provider is responsible for keeping up to date with any changes and additions notified by the providing authority.

Changes and additions that are of a substantial nature shall be notified in writing to the provider at least 90 days before they enter into force.

Amendments and additions to Annex 3 – Technical specification for calculation data shall be notified to the provider at least 180 days before they enter into force.

Changes and additions are effective from the date specified.

If the provider objects to a change or addition that is of a substantial nature and considers that this significantly affects its rights or obligations, this shall be notified in writing to the providing authority no later than thirty (30) days before the change enters into force. If no objection is made within this period, the provider shall be deemed to have accepted the change.

14. Follow-up

14.1 The providing authority has the right, upon request, to review and obtain information demonstrating that the provider complies with the Connection Agreement.

14.2 In connection with the review, the providing authority has the right to obtain information from the provider, carry out site visits and interviews with the provider, and make random checks to verify compliance with the requirements. The provider shall assist throughout the review process and provide the necessary resources and offer access to such documentation and premises as are required for the providing authority to verify compliance. The planning of any site visits, interviews, and sampling shall be carried out in consultation between the provider and the providing authority and shall be arranged in such a way that they have as little impact on the provider's operations as possible.

14.3 The request for information shall also otherwise be reasonable, and account shall be taken of the party's need for confidentiality and the fact that certain information may constitute trade secrets.

14.4 The provider shall ensure that the providing authority has the right to carry out checks as described above also on subcontractors whose performance may affect the provider's compliance with material requirements under the Connection Agreement, unless this can be considered unreasonable in view of the scope and nature of the relevant parts.

14.5 If the verification reveals that the provider has not complied with the Connection Agreement and the deficiencies can be considered serious, the provider shall bear the costs of the verification to the extent that such costs are not unreasonable. Otherwise, each party bears its own costs.

14.6 The providing authority has the right, in addition to what follows from this section, to summon the provider to two follow-up meetings of the Connection Agreement per year. The providing authority convenes these meetings. The parties shall bear their own costs in connection with the relevant meetings.

15. Errors and deficiencies

15.1 The provider shall be deemed to have acted incorrectly if the provider acts or has acted in breach of its obligations under the Connection Agreement. The providing authority has the right to report errors and deficiencies even if payment has been made.

15.2 The providing authority shall be deemed to have acted improperly if the providing authority has acted in breach of its obligations under the Connection Agreement. The providing authority shall promptly rectify errors and deficiencies.

16. Action plan

In the event of errors or deficiencies in the provider's fulfilment of its obligations under the Connection Agreement, the providing authority has the right to demand remedial action at the provider's own expense.

Remedial action shall be taken in accordance with the following steps:

a) *Dialogue between the parties*: An initial dialogue between the parties shall be held with a view to identifying the cause of the error or deficiency and discussing possible solutions.

b) *Action plan for measures*: A written action plan must be drawn up. The action plan shall specify:
- the measures to be taken.
- the division of responsibilities between the parties.
- deadline for measures to be implemented.

c) *Follow-up of implemented measures*: The provider shall report the measures implemented to the providing authority. The providing authority shall evaluate whether the measures taken are adequate and in accordance with the action plan.

17. Sanctions

17.1 Right to impose sanctions

The providing authority shall be entitled to impose one or more sanctions in accordance with Points 17.2 to 17.4.

17.2 Repayment of unduly paid remuneration

17.2.1 The provider undertakes to pay back remuneration paid to the provider on an incorrect basis or in an excessive amount if the provider caused the incorrect payment by providing incorrect information, incorrect calculation data, or failed to fulfil its obligation to provide information.

17.2.2 The repayment obligation also exists if remuneration has otherwise been paid incorrectly or in an excessive amount and the provider realised or reasonably should have realised this.

17.3 Right to reduce or withhold payment in the event of errors or deficiencies regarding calculation data

17.3.1 The providing authority has the right to reduce or withhold payment of remuneration if providers do not comply with their obligations regarding the reporting of calculation data. The right to reduce or withhold payment of remuneration only applies for as long as errors or deficiencies in the reporting of calculation data exist.

17.3.2 If the providing authority intends to reduce or withhold payment pursuant to this point, the providing authority shall notify the provider thereof.

17.4 Damages

17.4.1 If the providing authority or the provider intentionally or negligently violates the Connection Agreement and thereby causes damage to the other party, the injured party is entitled to compensation for this damage. Compensation is not awarded for indirect losses, such as loss of sales or loss of profit.

17.4.2 The providing authority and the provider shall, as the injured parties, take reasonable measures to limit their damages. In the event of negligence, the injured party may bear the corresponding part of the loss.

17.4.3 Claims for damages must have been notified to the other party in writing within three months of the damage being discovered or having been discoverable. If a claim is not made within the time limit, the right to assert the claim shall lapse.

The liability is further limited to a total amount of 20 cost-indexed basic amounts per liability event. Cost-indexed basic amount means the cost-indexed basic amount under the Social Insurance Code in force at the time of the occurrence of the damage. Compensation is limited to direct damage.

The limitations of tort law above do not apply if:
- there is intent or gross negligence on the part of the person who caused the damage,
- the cause of the damage arises from inaccuracies in the submitted calculation data.
- Decisions to reduce or withhold remuneration do not impose any restrictions on the providing authority's right to compensation.

17.4.4 If the provider is a government authority in Sweden, it follows from national law that damages cannot be awarded between the parties.

18. Grounds for exemption

18.1 The parties may be released from their contractual obligations if these cannot be fulfilled due to an unforeseeable event at the time of contract conclusion, which is beyond their control and authority.

Examples of grounds for exemption include, but are not limited to: war, widespread labour conflict, blockade, fire, environmental disaster, or serious spread of infection.

18.2 The parties may be released from their obligations under the Connection Agreement if mandatory law or other regulation, binding legal act within the European Union, government or authority decisions make it impossible to fulfil their obligations under the Connection Agreement.

18.3 If the providing authority or the provider intends to invoke a ground for exemption, it shall immediately inform the other party of the circumstance arising, its expected duration and its impact on the ability to meet its obligations.

The parties undertake to take reasonable steps to minimise any damage or inconvenience they may incur as a result of the ground for exemption.

19. Termination and cessation of the Connection Agreement

19.1 Termination of the Connection Agreement

19.1.1 If the providing authority decides to terminate the Authorisation system for electronic identification, the Connection Agreement will cease to apply at the time of the termination of the Authorisation system for electronic identification.

19.1.2 If the provider's approval by the Agency for Digital Government in accordance with the trust framework for Swedish e-identification for the current assurance level is terminated, the Connection Agreement will also cease to apply at the same time.

19.2 Immediate termination

19.2.1 The providing authority has the right to terminate the Connection Agreement with immediate effect if the provider materially fails to fulfil an obligation under the Connection Agreement.

19.2.2 The providing authority has the right to terminate the Connection Agreement with immediate effect if the provider:
- creates or participates in business arrangements that abuse authorisation systems for the purpose of obtaining undue remuneration,
- otherwise similarly creates or participates in arrangements for the purpose of improperly obtaining remuneration through the Authorisation system for electronic identification.

19.2.3 The providing authority and the provider have the right to terminate the Connection Agreement with immediate effect, or at a later specified date, if a new or amended law or regulation, a new or amended binding legal act within the European Union, or a government or authority decision renders the Connection Agreement incapable of being properly performed. Such termination shall be effected as far in advance as circumstances reasonably permit.

19.2.4 The providing authority has the right to terminate the Connection Agreement with immediate effect if the provider:
- does not meet the requirements for a provider's application for connection to the Authorisation system for electronic identification to be approved,
- materially or repeatedly fails to comply with the requirements of the trust framework for Swedish e-identification and the provider does not take the measures specified in the action plan in accordance with Point 16 within the specified time frame

19.2.5 The providing authority has the right to terminate the Connection Agreement with immediate effect if the provider, at the request of the providing authority, has provided information that is materially incorrect.

19.3 Early termination

19.3.1 If the provider does not take the measures specified in the action plan in accordance with Point 16 within the specified time frame, or if the provider on three or more occasions during a period of twelve (12) months violates the Connection Agreement, the providing authority has the right, subject to at least thirty (30) days' notice, to terminate the Connection Agreement.

If the providing authority breaches the Connection Agreement on three or more occasions during a period of twelve (12) months, the provider has the right, subject to at least thirty (30) days' notice, to terminate the Connection Agreement.

19.3.2 If the providing authority amends or makes additions to the Connection Agreement that are of a substantial nature and significantly affect the provider's rights or obligations, the provider shall have the right to terminate the Connection Agreement at the time of the entry into force of the amendment. This presupposes that the provider has objected to the change.

19.3.3 The providing authority and the provider have the right to terminate the Connection Agreement in writing with twelve (12) months' notice, calculated from the end of the month following the notice of termination.

20. Responsibility for personal data

The provider is the data controller for the personal data processing that the provider carries out in order to provide the services specified in the Connection Agreement.

The provider is responsible for drawing up, where applicable, data processing agreements with subcontractors who, within the framework of this Connection Agreement, process personal data on behalf of the provider.

This Connection Agreement does not mean that providers process personal data as a processor for the providing authority or public entities.

21. Applicable law and dispute

The Connection Agreement shall be interpreted and applied in accordance with Swedish law.

Disputes concerning the interpretation or application of the Connection Agreement shall primarily be settled between the parties and, in the alternative, be decided by the ordinary courts, with Stockholm District Court as the court of first instance.

In the event that disputes concerning the interpretation of the Connection Agreement arise between parties that are only state authorities within Sweden, instead of what is stated above, the authorities shall resolve the dispute by negotiation.

22. Contact person

The provider shall designate at least one contact person or contact function responsible for matters relating to the Connection Agreement, complaints and invoice enquiries.

The provider shall inform the providing authority and keep the providing authority informed of current contact routes and contact details for this reporting.

The parties shall immediately notify each other of any change of contact person.

23. Signature

This Connection Agreement has been drawn up in two identical copies, each party having received one copy.

Providing authority	Provider

_____	_____
Name	*Name*
Title	*Title*