Effective as of 4 April 2018

General terms and conditions of the OP Identity Service Broker

1 Scope of application

These terms and conditions shall apply to the OP Identity Service Broker where OP transmits an electronic authentication of a Customer using eService between the provider of the authentication credential and the eService, in accordance with appended service description.

The service description of the OP Identity Service Broker, valid from time to time and revealing the content and functions of identification data, shall apply to the OP Identity Service Broker.

The agreement on the OP Identity Service Broker constitutes a whole together with these terms and conditions, the identification principles for the OP Identity Service Broker and the service description of the OP Identity Service Broker.

2 Definitions

Authentication credential is OP cooperative bank's online service user identifiers. OP Identity Provider Service forms part of the Authentication credential.

Authentication credential provider is the service provider that has granted an authentication credential to the Customer. The Authentication credential provider also provides Identification service to the Authentication credential it has granted.

Chained identifier is a new credential created using the Authentication Credential that may be a strong electronic credential under the Identification Act or another credential to which the Identification Act is not applied. Adding the Customer's identity to the existing customer relationship or an identification means is also regarded as a chained identifier.

Code of conduct is recommendation no. 216/2017 S by the Finnish Communications Regulatory Authority (FICORA) for the code of conduct of the Finnish Trust Network (FTN) (3 April 2017).

Customer refers to private or corporate customers who authenticate themselves to the eService with an Authentication Credential through the OP Identity Service Broker

eIDAS regulation is a regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Finnish Trust Network refers to a network of the providers of identification service that have made a notification to FICORA (§12a of Identification Act).

Identification Act is the Act on Strong Electronic Identification and Electronic Trust Services (617/2009).

Identification data is personal data on the Customer given during the identification event given by OP that includes the Customer's first name, last name and personal ID code (hereinafter personal ID).

Identification service is the part of the authentication credential that the OP Identity Service Broker utilises when implementing an identification event.

Identification service provider (IdP) is both the provider of the authentication credential and of the identity service broker.

International sanctions refer to a sanction, financial sanction, export or import ban, trade embargo or another restrictive action imposed, administered, approved or executed by the Finnish government, United Nations, European Union, United States of America and United Kingdom or their competent authorities or governing bodies.

OP refers to an OP Financial Group party, also a service provider. OP Financial Group consists of OP Cooperative, its existing and future subsidiaries (such as OP Corporate Bank plc) and its Group companies (such as OP Insurance Ltd), entities and foundations and their subsidiaries, OP Cooperative's member cooperative banks and their subsidiaries, OVY Insurance Ltd, OP Bank Group Pension Foundation, OP Bank Group Pension Fund and other existing and future companies, entities and foundations, over which at least one of the aforementioned organisations alone or together exercises control.

Portal constitutes a single service whole. It is defined in greater detail in paragraph 2 Asiointipalveluiden yhdistäminen (Combining eServices) (through weak identification) of interpretation memorandum Dnro: 658/620/2017 issued by FICORA on 22 September 2017.

PSD2 is a directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

3 Identification

OP identifies the Customer and transmits the identification data to the OP Identity Service Broker in a manner specified in the service description of OP Identity Provider Service. The OP Identity Service Broker shall always transmit Customer identification at least according to the higher security level based on the eIDAS regulation. OP Identity Provider Service is allowed to be used, provided that the Customer has in each case used his/her Authentication credential to make an order with the Identity Service Broker within the Finnish Trust Network for identification and disclosure of personal data using his/her Authentication credential. In the case of confirmation of a payment order, the Identity Service Broker is responsible for ensuring that, in respect of both the Identity Service Broker and the eService, meets the requirements of PSD2, its regulatory technical standards and national payment-related legislation.

Identification is based on an agreement between the Customer and the authentication credential provider, on the basis of which the Customer has received an authentication credential eligible for the OP Identity Service Broker.

When the eService requires Customer authentication, the Customer makes an order with the OP Identity Service Broker for implementing a link presented on the eService. Via the link, the Customer moves to the OP Identity Service Broker which executes the Customer's identification order together with the granter of the authentication credential. The OP Identity Service Broker transmits information on the Customer agreed upon with and/or requested by the eService.

OP has the right to require that the Customer separately confirm the identification event, for example, by contacting OP.

The OP Identity Broker Service provides strong electronic identification service under the Identification Act whenever the Customer authenticates himself/herself using the authentication credential notified to the Finnish Trust Network. If the Customer authenticates himself/herself with another electronic authentication credential, the OP Identity Service Broker will inform the Customer that no authentication based on the Identification Act is involved.

Real-time information on authentication credentials working on the OP Identity Service Broker can be found in the Identification principles for the OP Identity Service Broker that is available on OP's website at www.op.fi.

The eService must check that the Identification data corresponds to that provided by the Customer. The OP Identity Service Broker must check that the identification comes from OP by using credential and checksum data it has received from OP. The OP Identity Service Broker shall exercise due care in storing the credentials and checksum data it has received from the bank plus information on the identification event obtained from OP.

331652e

As part of the identification event, the eService must inform OP through the OP Identity Service Broker, based on the service description of the OP Identification Service what kind of an identification event is involved: identification event, an event to create a chained credential based on the Identification Act or an event created for a chained credential to which the Identification Act is not applied.

Identification is based on an agreement between the Customer and the authentication credential provider, on the basis of which the Customer has received an authentication credential. To complete an identification event, OP has the right to require that the Customer confirm the identification event, for example, by contacting OP.

OP does not ensure the right of an identified person to represent the person, company or another entity and their right to do intended legal acts. The terms and conditions of the agreement between the Customer and the eService or the Customer and the Identity Service Broker shall apply to the legal effects of the use of the identification event on the eService or the Identity Service Broker and to the parties' responsibilities. OP is neither a party to these agreements nor is responsible for the fulfilment of these agreements and their terms and conditions or for the validity of legal acts.

The eService has the right to create a new identifier to identify the customer according to the agreement. A chained identifier may be a strong electronic credential under the Identification Act or another credential to which the Identification Act is not applied. The eService must inform the Identity Service Broker of how many chained identifiers the eService have created and whether they have been in compliance with the Identification Act. The eService authorises the Identity Service Broker to provide OP with the information on these chained identifiers. The parties shall ensure that individual identification events are stored and filed as required by law.

4 Restrictions related to the use of authentication credentials

An identification event may be transmitted to the eService only in the service in the EEA. The eService is shall agree to it that the services are not provided outside of the EEA.

The Identity Service Broker may not transmit an identification event to the service executed with the Authentication credential to identify the Customer that is provided or controlled by a party subject to international sanctions. The eService may not use or transmit the identification event executed with the Authentication credential for purposes contrary to this agreement, the laws of Finland or the country of service provision or to good practice. When assessing whether OP's authentication credential is contrary to good practice or not, OP takes account, for example, of its CSR requirements and the Identification Principles for Authentication Credentials as well as the requirements for the eService appended hereto.

The eService may not transfer a strongly identified Customer, as specified in the Identification Act, to the provider of another eService or, for example, to another service. From the perspective of the Identification Act, a weakly identified Customer may be transferred to another service provider only if it is the question of provision of the service as part of the Portal of the original eService. An eService into which the customer has logged for the first time is responsible for all obligations under this agreement towards the Customer and the Identity Service Broker.

Payments may not be accepted with the authentication credential based on identification in the Finnish Trust Network after entry into force of the RTS issued based on the PSD2.

Other restrictions related to the use of the Authentication credential and valid at any given time have been listed in the Identification Principles for Authentication Credentials. For OP's authentication credential, the identification principles are available on OP's website at www.op.fi and on FICORA's website. The eService undertakes not to enable the use of the Authentication credential contrary to the restrictions related to the Authentication credential.

5 Obligations

The party to the agreement is responsible for fulfilling the requirements specified in the Identification Act and at least according to the higher security level based on the eIDAS regulation. In the case of confirmation of a payment order, each party for its part is responsible for ensuring that the transaction meets the requirements of PSD2, its regulatory technical standards and national payment-related legislation. The party to the agreement is obliged to execute the identification order made by the Customer in compliance with the Identification Act, eIDAS regulation, this agreement and the service description of the OP Identity Provider Service.

The Identity Service Broker must have the ability to identify any threats to the service and its users, prevent occurrence of threats and observe and stop data security deviations suffered by the services and their users. In addition, the Identity Service Broker must have the ability to report any threats and data security deviations and have a designated contact person for handling cases of fraud and data security.

The Identity Service Broker and the eService are alone responsible for their products and services and their marketing. Both the Identity Service Broker and the eService shall agree for their part to provide and market their products and services in compliance with laws, decrees and official regulations as well as good practice. The Identity Service Broker and the eService are responsible for fulfilling their performance obligations towards their Customer in accordance with their contract terms and conditions.

The eService must ensure that its Identity Service Broker and OP's services as well as responsibilities are not mixed up.

6 Responsibilities and liability for loss

As soon as the party to the agreement has detected loss or damage, he/she must take reasonable measures to limit his/her damage. If the party to the agreement fails to do so, he/she will be personally liable for the corresponding part of the damage. The Identity Service Broker and the eService are alone responsible for their products and services and their marketing. The parties shall agree to provide and market their products and services in compliance with laws, decrees and official regulations as well as good practice. The Identity Service Broker and the eService are responsible for fulfilling their performance obligations towards their Customers in accordance with their contract terms and conditions as well as the laws of Finland and the country of provision of another service.

The party is obliged to pay damages to the other party for direct losses caused through negligence by the party and proven by the party suffering loss. The party is not liable to compensate for indirect loss, which include loss of income and earnings, interest loss, loss of profit and a loss which is due to a reduction in or interruption of business, disruption caused in other contractual relationships or another loss that is difficult to foresee. The party's annual total liability for loss is limited to a maximum of twenty per cent (20%) of the service charges for the identification events per year. In respect of an individual identification event, the maximum liability is always the price of the identification event less valued added tax.

The party is not liable for any loss caused by a loss or change of data in the public data network or for loss due to a force majeure event. Neither is the party liable for any loss arising from the fulfilment of any obligation under this agreement if such fulfilment were against any obligations laid down for the party elsewhere in law.

The limitations of liability shall not be applied at all if the loss has been caused by violating confidentiality intentionally or through gross negligence. If the loss has been caused by violating confidentiality, obligations regarding personal data processing, IPRs, is due to national legislation of the country other than Finland, to future obligation or the fact that the Identification event has been normally transmitted to the Identity Service Broker despite the deactivation of the Authentication credential performed indisputably by the customer or that the identity verification has been misperformed, quantitative limitations of liability shall not be applied but the limitations of liability related to indirect losses shall be applied.

Nevertheless, the granter of the chained identified is always liable for any loss that has been caused by the fact that it has relied on the Authentication credential when chaining it, unless it can prove that the identification of the Authentication credential for the first time has been misperformed due to Authentication credential provider's gross negligence or intent.

If the Identity Service Broker justifiably considers by law to be liable to pay damages or the Identity Service Broker is regarded as being liable to pay damages, for example, by the authorities or alternative dispute resolution bodies due to the loss caused to the Party or the Customer based on an identification event contrary to the agreement or that is unauthorised, the Identity Service Broker shall pay compensation for all loss caused to the Identity Service Broker, including interest based on the Interest Act, even if the loss were not caused by the eService if the loss is not due to the Identity Service Broker's breach of contract. The limitation of liability shall not be applied to the above. Such losses may be caused, for example, by unauthorised use of the Authentication credential, legal acts, use of eService's services or products performed using the Authentication credential, their errors or delays or other eService's activities.

Claims due to the party's error must be presented to the other party in writing and in sufficient detail no later than one (1) year of the date when the loss was detected or should have been detected. If the claim is not presented within the abovementioned time, the party will have no right to claim compensation in this case. The right to claim compensation terminates when one year has passed of expiry of the agreement, but in any case after five years when the error event occurred.

Complaints and claims must be addressed directly to the relevant party (such as User complaints to the eService). The Identity Service Broker and the eService must provide the Customer with contact details in their own services for making complaints and claims.

7 Processing of personal data

Both the eService and the Identity Service Broker are independent controllers and are for their part responsible for the legitimacy of personal data processing and storage. If the party transfers or discloses identification event data outside the EEA, it must inform the other party and the Customer thereof. In the transfer, the party transferring such data shall use the European Commission's standard contractual clauses or some other transfer mechanism approved by the European Commission.

During the identification event, the Identity Service Broker always transmits identification data to the eService. The Identity Service Broker is responsible to OP for the fact that, when making an order related to authentication, the User has received information in an extensive and understandable manner that OP hands over the User's name and personal ID code to the Identity Service Broker. If the order related to authentication made by the User does not include OP giving the name and personal ID code to the Identity Service Broker, the Identity Service Broker shall have no right to use the OP Identity Provider Service to execute the order.

The eService may process the information it has received during the identification event as such, in part or combined with other data only to implement and verify such an individual strong electronic identification event for which the Customer has made an order with the Identity Service Broker. The Identity Service Broker may disclose the identification data to the eService if the eService has by law the right and otherwise capabilities to process personal data in accordance with law and this agreement.

The eService may not transmit the Customer's customer data outside of its service received through the Identity Service Broker as such, in part or combined with other data or, for example, by providing a third party with an identity service broker, which is based on these data, unless agreed thereupon separately.

8 Technical performance of the service and service outages

In interface implementations, the parties comply with the technical interface standards of the Finnish Trust Network. Each party is responsible for its hardware, software, services and the use, performance, development, maintenance and telecommunication costs of information systems as well as for data security and for its information systems being protected against unauthorised use.

With respect to the service level, the parties treat each other in an equitable and non-discriminatory manner and offer each other a similar service level on the same terms and with the same features as what they offer to other parties to the Finnish Trust Network.

In the implementation of the identification events in the Finnish Trust Network is that the Identity Service Broker is available on a 24/7 basis, excluding servicing, service update, maintenance, any potential incidents and faults that cause a break in the performance of the Authentication credential provider's identification service or the identity service broker. The Identity Service Broker does not guarantee that the Authentication credential provider's identification service or the Authentication credential are available uninterruptedly, and is not responsible for losses caused by the breaks.

The Identity Service Broker has the right to suspend or restrict the Identity Service Broker's service in cases it deems necessary. These include, for example, suspected security threats and action contrary to the agreement, in addition to servicing and a force majeure event.

The parties together participate in troubleshooting incidents in the Identity Provider Service.

9 Intellectual property rights

The eService has the right to use OP's name and trademark only when informing of the opportunities to authenticate oneself to its service, in accordance with the instructions issued by OP at any given time. Use for any other purpose is prohibited. It is prohibited to use OP's trademark or other emblem in such a way that it seeks to increase the goodwill or credibility of the eService or a third party in such a way that it causes harm to the owner of the trademark, logo or another emblem.

The Identity Service Broker has the right to publish the name of the eService accepting the identification of the Authentication credential in its communication related to the Authentication credential and the OP Finnish Trust Network agreement. If the Identity Service Broker is given instructions on the method of presentation of the trademark or another logo, OP must follow the instructions.

The right of the party specified in this agreement to use another trademark or emblem will terminate upon termination of this agreement or if the party otherwise prohibits its use for a justified reason. In such a case, the party undertakes to remove the trademark and any other possible emblems from its own and any possible third-party services and marketing material.

Under this agreement, the parties do not in any respect assign their trademark rights or other intellectual property rights, and this agreement has no effect on ownership of material or data established outside this agreement. The background documents or material given by the other party may be used only for the purpose of this agreement and the right of use may not be given or otherwise assigned to third parties.

10 Service charges

The Identity Service Broker is entitled to bill charges and fees, based on the list of service charges and fees, in another separately agreed manner or otherwise separately agreed upon.

The Identity Service Broker is liable for any taxes and other similar charges related to this agreement and the use of the OP Identity Service Broker.

The Identity Service Broker has the right to change the charges and fees collected under this agreement by notifying thereof on its own website at www.op.fi or in OP's list of service charges and fees. Said change will take effect in three (3) calendar months' time of the date of publishing the notification, at the earliest.

If the charges and fees become subject to new enactments or regulatory provisions or decisions, the parties shall comply with them as of the date

of the final judgement or decision. The decisions or provisions have no effect on the charges and fees paid before their entry into force.

11 Communication

The parties send notifications and other messages related to this agreement to the contact address specified in the contact information appendix, depending on the matter in question. If so agreed separately, the parties are obliged to build an encrypted email connection to send information to the indicated addresses. Messages that include confidential information or personal data shall be sent by encrypted email between the parties.

Notifications sent by post shall be considered to have been received by the other party on the seventh day from the date on which they were sent and notifications sent by email on the day following their sending.

12 Information undertakings

The parties shall inform of changes in contact persons and contact information specified in the Contact persons appendix by sending an updated Contact persons form to the party's contact address.

As far as possible, the parties shall inform of maintenance downtime and its duration in their own service as well as service changes as soon as possible. If the party discovers any error or problem related to the other party, it must inform thereof to troubleshoot or remedy the error or problem.

The Identity Service Broker is under no obligation to inform the eService if the use of the Authentication credential is temporarily prevented and an individual order made by the Customer is suspended or remains unperformed.

OP shall not on its own initiative give the party or a third party information on closure of the Authentication credential or its grounds. Information on the closure or its grounds shall not be given on request either unless the request is related to determining a specified identity error in the Finnish Trust Network. In the case of any possible identity error, the party shall give the other party information regarding the identification event without a charge and shall by reasonable means contribute to the fact that the identity of the person behind the identification event can be found out. Finding out about information on the identification event does not require handing over information in the identification documents.

The party shall inform the other party to the agreement of any major changes in the content of its service or changes in its contact information or other information relevant to the functions under this agreement.

The eService must inform the Identity Service Broker of the details it has requested, such as name, business ID, postal address, phone number, domicile and, whenever the Identity Service Broker so requires, verify its representatives and give their specimen signature as well as notify, for example, of its ownership structure and beneficial owners. The Identity Service Broker may use this information to fulfil its statutory and contractual obligations and to supervise compliance with this agreement. The information may not be saved or otherwise utilise in such a way that the Identity Service Broker could exploit it in providing its own services unless otherwise agreed thereupon.

The eService is responsible for the information being accurate and up to date. The Identity Service Broker is under no obligation to check or supplement the information but may do so if it wants. Furthermore, the Identity Service Broker may check the eService's credit information. However, should the information provided by the eService be found to be incorrect or incomplete or the information is destroyed, the eService shall provide new information upon request. The Identity Service Broker or the Authentication credential provider is not liable for any loss caused to the eService by the fact that the information provided by the eService contains errors or shortcomings.

13 Alteration of the terms and conditions of the agreement

The parties may agree on any changes needed to the terms and conditions of this agreement.

The Identity Service Broker and the Authentication credential provider have the right to alter all terms and conditions, service descriptions, instructions and activities as well as applicable to the Finnish Trust Network and identification principles by notifying the eService thereof.

Such alteration takes effect during the time informed by the Identity Service Broker, but not until (3) calendar months have passed from the date of the notification.

A change which substantially increases the Identity Service Broker's obligations or diminishes its rights and is not due to a legislative amendment, official instructions or a change in banking practice will take effect within the period notified by the bank, but not until thirty (30) days have passed from the date of the notification.

14 Confidentiality

The parties undertake to keep confidential during and after the contractual relationship all information received from the other party on the basis of this agreement and on account of acting in the Finnish Trust Network, and to use it only for purposes permitted under this agreement. The following information is regarded as confidential: all information given by the party that is subject to bank secrecy, classified as business secret or information given to fulfil information undertakings arising from acting in the Finnish Trust Network or otherwise confidential information or material irrespective of in what form such confidential information has received or given or of whether it is protected by intellectual property rights.

Confidential information may apply to the party's products, services, customers, technology, processes, intellectual property rights, hardware, software, objectives, plans, risk management or technological, commercial, financial or other comparable information.

Given information is not regarded as confidential information insofar as its recipient is able to prove that:

a) the information was public when it was given or which has later become publicly available for a reason other than as a consequence of the recipient's action contrary to this agreement;
b) the information has justifiably been in the possession of the recipient without handover or usage restrictions related to any of the confidentiality obligations already before the recipient has received it from the other party;
c) the recipient has justifiably received the information from a third party which has had the right to give the information without restrictions related to any of the confidentiality obligations; or
d) the information must be handed over to a court or authorities in accordance with mandatory legislation or a court rule or a regulation issued by an authority. Before given confidential information to the court or authority, the recipient is, however, obliged to promptly notify the party who has given the information of the request for information presented to it and to give an opportunity to take the necessary measures to keep confidential information secret.

The party has the right to present information in the personal data file to the Customer at his/her request.

Either party shall ensure that employees in its employ and suppliers it may use shall commit themselves to the abovementioned confidentiality clause.

Upon termination of the agreement, the party shall return data and material received from the other party and destroy or delete documentation and copies in its volumes.

This confidentiality clause is valid after termination of the agreement as well. The confidentiality obligation in respect of the parties and cooperation will continue for five (5) years. For the user's personal data, the confidentiality obligation will continue for an indefinite time.

15 Duration, termination and cancellation

This agreement is effective until further notice.

The party may terminate the agreement at thirty (30) day's notice. OP may terminate this agreement only as specified in the Code of conduct (section 4.2).

The party may cancel the agreement with immediate effect if the other party is in material breach of its contractual obligations and does not correct such breach within thirty (30) days of the date when the party presented its demand.

The party has the right to consider the agreement to have been terminated if the other party discontinues its own service or is declared bankrupt, is placed in debt rescheduling, financial restructuring or in liquidation or is otherwise apparently insolvent or the party is removed from FICORA's data file of service providers.

16 Force majeure

Force majeure refers to an unexpected, exceptional cause relevant to the matter preventing the fulfilment of the agreement and occurring after entry into force of the agreement, which the parties could not have taken into consideration upon conclusion of the agreement and which is beyond the parties' control, whose preventing effect cannot be eliminated or escaped, and due to which the obligation under the agreement cannot be fulfilled. A similar cause arising from the telecommunications network, such as a powerful denial of service attack, is comparable with a force majeure event.

Delay on the subcontractor's part is considered to have been caused by force majeure only if such delay is caused by the aforementioned force majeure and subcontracting cannot be performed by another subcontractor without any unreasonable loss of time or costs.

The party shall, as soon as possible, notify the other party of a force majeure event that it has encountered. As the Authentication credential provider, OP may announce such a force majeure circumstance on its website or in a national daily newspaper.

17 Assignment of the agreement

The parties to the agreement have no right to assign this agreement to a Third Party. OP has the right to assign this agreement to an OP Financial Group company or entity.

18 Applicable law and jurisdiction

This agreement shall be construed and governed by the laws of Finland, with the exception of the connecting factor rules. Any disputes arising out of the agreement shall be settled finally by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce by one (1) arbitrator. Arbitration shall be conducted in Finnish and the place of arbitration is Helsinki.