Qualified Electronic Signature Terms

These Qualified Electronic Signature Terms apply to Customer's access to and use of QES and OTP, in addition to the terms set forth in the Agreement. The terms in this QES Exhibit take precedence over any other conflicting or inconsistent terms in the Agreement. Capitalised terms in this QES Exhibit have the same meaning as in the Agreement, unless expressly defined otherwise.

1. Definitions.

1.1. **eIDAS** means Regulation (EU) No. 910/2014 of the European Parliament and of the Council dated 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and all laws implementing, supplementing, or amending the foregoing.

1.2. **Captured Media** means, as applicable, the images/videos of the User's identity document and the images/videos of the User's face provided to Entrust as part of the Services.

1.3. **Certificate Documents** means the QTSP's terms and conditions for issuance of a qualified certificate to the User.

1.4. **Documents to Sign** means the documents provided by Customer to be electronically signed by the User using their QES.

1.5. **Evidence File** means all relevant information collected and validated by Entrust during a Studio workflow, including the Evidence File Summary, all Captured Media, Certificate Documents, and Signed Documents.

1.6. **Evidence Summary File** means a PDF containing a time-stamped audit trail of all relevant information collected and validated by Entrust during a Studio workflow.

1.7. **OTP Provider** means the third-party provider appointed by Entrust responsible for the provision of OTP.

1.8. **Qualified Trust Service Provider or QTSP** means the third-party qualified trust service provider appointed by Entrust responsible for the issuance of qualified certificates in accordance with eIDAS.

1.9. **Signed Documents** means the documents electronically signed by the User using their QES.

2. Technical Requirements.

2.1. Customer is responsible for implementation of QES and OTP as set forth in Entrust's API documentation and Entrust's reasonable instructions. QES and OTP will be available from such date mutually agreed by the parties.

3. Signed Documents.

3.1. Customer acknowledges that Entrust does not monitor or review the Documents to Sign. To the extent required by Customer, Customer is responsible for ensuring that use of QES in the manner

provided by Entrust results in valid and enforceable Signed Documents in accordance with any applicable laws in which Customer operates.

3.2. Entrust:

3.2.1. provides no conditions, warranties, representations or undertakings in relation to the validity or enforceability of the underlying Signed Documents; and

3.2.2. has no liability in connection with the validity or enforceability of the Signed Documents, reliance on QES under applicable laws, or for any breach by the User of the Certificate Documents.

4. Third Party Data Controllers.

4.1. Customer acknowledges that:

4.1.1. QES and OTP includes the use of External Data Providers, the QTSP and the OTP Provider;

4.1.2. the QTSP and OTP Provider will act as independent data controller of Personal Data shared for the purpose of:

4.1.3. in respect of the QTSP, issuance of a qualified certificate under eIDAS under the terms of the Certificate Documents between the User and the QTSP as set out in section 5 below; and

4.1.4. in respect of the OTP Provider, optimizing, routing, securing and maintaining the OTP services and fraud detection.

4.1.5. The QTSP and OTP Provider will process Personal Data only for the purposes listed above and will comply with all Privacy Laws in relation to their Processing.

5. Certificate Documents.

5.1. Customer will inform Users in advance, in a clear and comprehensive manner, of the precise terms and conditions regarding the use of QES and will ensure that Users accept the Certificate Documents prior to issuance of a qualified certificate. Customer will not amend, remove or replace the text provided by Entrust in connection with the Certificate Documents without the prior written consent of Entrust.

5.2. Use of QES will be subject to the terms and conditions set out in the Certificate Documents.

5.3. Entrust will make available to Clients a copy of the Certificate Documents. Clients will provide each User a copy of the Certificate Documents accepted by the User or the confirmation of the User's acceptance of the Certificate Documents on paper or other durable medium upon completion of the QES process.

6. One-Time Password.

6.1. Customer will ensure that its use of QES is coupled with an additional authentication factor, by sending to the User a single-use code generated specifically and individually for the User to their mobile phone.

7. Retention.

7.1. Customer will download and retain the Evidence Files for the period required by applicable law in which Customer operates.

8. Revocation, Suspension, and Termination.

8.1. Customer must:

8.1.1. inform Entrust without delay of any:

8.1.1.1. situation it becomes aware of (a) illegitimate use of qualified certificates; or (b) where the requirements under which the qualified certificate were issued are no longer met, where revocation and/or suspension of the qualified certificate is required; and

8.1.1.2. request received by Customer for revocation and suspension of any qualified certificate issued to Users; and

8.1.1.3. provide all necessary cooperation and documentation in its possession to Entrust and/or the QTSP as required to verify the above reasons underlying the requests for revocation or suspension of certificates.

8.2. Entrust may suspend or terminate the provision of QES and OTP without liability to Customer immediately on giving Notice to Customer if Customer fails to comply with the terms of this QES Exhibit. Such suspension or termination will not be deemed to be a breach of this Agreement by Entrust.