cssf

Commission de Surveillance
du Secteur Financier

Frequently asked questions on AML/CFT and IT requirements for specific customer on-boarding/KYC methods

Commission de Surveillance du Secteur Financier

Frequently asked questions on AML/CFT and IT requirements for specific customer on-boarding/KYC methods

TABLE DES MATIÈRES / TABLE OF CONTENTS

Commission de Surveillance du Secteur Financier

Question 1: What is meant by "Identification/Verification of identity through video chat"?

8 April 2016

By "Identification/Verification of identity through video chat" (hereafter "video identification"), the CSSF means the performance of the identification/verification of the identity of the customer by a professional of the financial sector under the supervision of the CSSF (hereafter the "professional") through an online video conference.

The professional uses this process in order to support and execute certain tasks for the purpose of fulfilling his customer identification and verification of identity obligations as required i.a. by the Law of 12 November 2004 on the fight against money laundering and terrorist financing ("the Law").

Notwithstanding this possibility, it shall be stressed that all other anti-money laundering and counter-terrorist financing ("AML/CTF") professional obligations (e.g. requirements with respect to AML/CTF outsourcing (if applicable), adequate training, internal controls, suspicions reporting, etc.) will have to be strictly applied by the professional.

Question 2: Who can perform the video identification?

8 March 2018

The professional has the following possibilities:

i) Perform the video identification process himself using a tool developed internally, or

ii) Perform the video identification process himself using an external tool he has acquired from an external provider, or

iii) Delegate the identification process to an external provider using his own tool.

In each of these scenarios, the video identification needs to be performed by a specifically trained employee, either of the professional or, if applicable of the external provider.

The video identification/verification of the identity of a customer which is not actually performed by a specifically trained natural person but where the customer is in contact only with a robot, or where the customer simply uploads (a video with) identity documents online, does not qualify as video identification as addressed in the present FAQs due to the absence of a live video chat or real-time interaction between the aforementioned trained natural person and the customer.

Thus, contrary to the video identification, this kind of online/digital or robo-video-identification, without intervention of a natural person on behalf of the professional, requires the application by the professional of supplementary safeguards in order to mitigate those particular risks linked to the automated character of this kind of identification process.

Question 3: Who is responsible for respecting the professional obligations as required by the Luxembourg AML/CTF regulations?

8 March 2018

The professional making use of this video identification process is fully liable for respecting his customer due diligence obligations in accordance with the Luxembourg AML/CTF framework.

It shall be stressed that the professional remains fully responsible for complying with these professional obligations even in case the video identification is outsourced to an external provider.

This includes continuous monitoring of the effectiveness and reliability of the process and ability to intervene, especially in case of changes made by an external provider that would have consequences on the professional's ability to comply with his AML/CTF obligations.

It shall be highlighted that these rules are valid also where the professional uses means of online/digital or robo-video-identification as mentioned in question 2 above. In this case it is also not possible for a professional to delegate his responsibility to an external provider or other professional.

Question 4: Who are the persons that can be identified/verified through the online video conference?

8 April 2016

The persons that can be identified/verified through the online video conference are natural persons. They can be: the direct customer of the professional, the representative of a legal person customer, a proxy-holder, a co-holder of a joint account or a beneficial owner, in accordance with Article 1 of Grand-ducal Regulation of 1 February 2010. The term "customer" will be used hereafter in order to address the different aforementioned situations.

Question 5: In what circumstances is the video identification not possible?

8 April 2016

The video identification process can only be used in cases where there are no ML/TF suspicions, doubts about the veracity or adequacy of previously obtained data or circumstances which carry a higher ML/TF risk.

Thus, and in accordance with Article 3(3) of the Law, the professional is required to identify and perform an assessment of the ML/TF risks regarding the process, prior to the launch and/or the use of the video identification.

The attention of the professional is also drawn to the requirements of Article 4(2) of CSSF Regulation N° 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing ("CSSF Regulation") specifying that: "This risk assessment also includes the identification and assessment of money laundering or terrorist financing risks which may arise in relation to

a. the development of new products and new business practices, including new delivery mechanisms, and

b. the use of new or developing technologies for both new and pre-existing products. This risk assessment shall take place prior to the launch of new products, business practices or the use of new or developing technologies.".

Question 6: What are other preliminary measures that have to be taken prior to the beginning of the process of the video identification?

8 April 2016

i) Prior to using the whole process of identification/verification of the identity, the professional shall elaborate an interview manual/guide in order to conduct the video conference with the customer (see detail in question 7 below) or, where applicable, assess the interview manual/guide elaborated by the external provider.

ii) In case of the implication of an external provider, the professional shall perform a complete due diligence on the external provider from an AML/CTF, technical and security point of view.

iii) Adequate internal procedures of the professional shall support the use of the video identification.

Question 7: What is the contribution of the customer in the context of the video identification?

8 April 2016

i) The professional shall obtain the specific consent of the customer for the recording of the video conference, including the recording of sound and for taking pictures. In case an external provider is performing the video identification on behalf of the professional, the consent of the customer for the transfer of his data to this external provider shall also be obtained, by mentioning to the customer whether or not the provider is located in Luxembourg.

ii) Still, prior to the video identification as such, the customer must have provided his identification data (e.g. form to be filled in online) in order to enable the professional or the external provider to match this information with the information gathered during the video identification process.

iii) During the video identification process, the customer will be required to provide a code (transaction authentication number - TAN) generated by the identification tool that he received by e-mail or SMS. The code has to be verified by the trained employee, as soon as given by the customer, for matching purposes

Commission de Surveillance du Secteur Financier

Question 8: What are the necessary data quality conditions to be observed during the identification process?

8 April 2016

The following data quality conditions have to be observed during the video identification process: - the data on the identification documents must be clearly readable and the person shall be clearly recognizable (e.g. good light conditions; the customer shall not be disguised or wear headgear covering part of his face, etc.); - only official identification documents of the issuing country that contain optical safety features, e.g. holograms, print elements with tilting effect or equivalent features supporting the authentication of the identification documents, are permitted for this verification process; - the video conference with the customer should be done real-time and by a specifically trained employee of the professional (in-sourcing) or of the external provider (outsourcing) so that he is able, for instance,

i) to verify that the customer is the same person as the person on the identification document (e.g. consistency check: match the age of the customer with the customer's physical appearance, etc.),

ii) to read the data and to verify the hologram (the customer has to flip his identification document vertically and horizontally to the camera),

iii) to take screenshots from the customer's face and the customer's identification document (both sides and relevant pages),

iv) to check that the picture is not glued onto the aforesaid document or that the document has not been altered,

v) to verify that the numbers on the document are matching (e.g. date of birth, ID-document number, etc.) with the preliminary collected data (see question 6 above);

vi) to listen to the customer reading aloud the identification number on the identification document;

vii) to decode the MRZ (Machine Readable Zone) and verify additional elements of the identification document as e.g. 3D picture, watermarks, macro/microscript, etc.

These verification measures can be supported by additional questions and specific behavioural/psychological observations. The professional should elaborate an interview manual/guide for this purpose (see also question 6 above). Where the identification process is outsourced to an external provider, the professional and the external provider should agree on such interview manual/guide.

Question 9: What are the professional's obligations in case a problem occurs during the video identification process?

8 April 2016

In case of any problem encountered when performing the visual and/or oral checks due to insufficient quality of the communication, of the sound, of the online picture or any other circumstances that would not allow satisfying the trained employee for the purpose of verifying that the person shown on the screen is indeed the person s/he pretends to be and that the documents are not forged documents, the video identification has to be renounced. In such case, further measures, including identification measures (other than being based on online video/audio communications), should be undertaken, as provided by the Law, respectively, in case of ML/FT suspicion, a suspicious activity report shall be made to the competent authorities. Where the identification process has been outsourced to an external provider, the latter should keep the professional informed of the problems encountered, allowing him to take the appropriate measures.

Question 10: What are the customer data record/retention obligations of the professional?

8 March 2019

With regard to the customer data record/retention obligations, the professional shall collect and retain at least the screen shots and the audio records of the entire conversations "for a period of five years following the carrying-out of an occasional transaction and/or the end of the business relationship", as provided for in Article 3(6) of the Law.

The attention of the professional is also drawn to Article 25(3) of the CSSF Regulation that specifies that the recordkeeping "may be carried out on any archiving medium, provided that the documents meet the conditions to be used as evidence in a […] analysis of money laundering or terrorist financing by the AML/CFT competent authorities.".

Moreover the professional has to implement security measures in order to ensure that the access to the stored data is protected and that the principle of the "least privilege" is respected.

Question 11: What are the customer data record/retention obligations of the external provider?

8 April 2016

In case of the delegation of the process of the video identification to an external provider, the latter shall confirm to the professional that the data of the customer will only be stored for a short period of time i.e. the time which is necessary to transmit the customer's data from the provider to the professional.

Commission de Surveillance du Secteur Financier

Moreover, during the time of storage, the data has to be encrypted by the external provider according to the CSSF recommendations which are detailed in the CSSF Annual Report of 2013 (Chapter XI, Section 2.1.).

Finally, the external provider has to implement security measures in order to ensure that the access to the stored data is protected and that the principle of the "least privilege" is respected. The provider has to ensure that only the professional can access the data of his customers and also, that the access of the professional is limited to the data of his customers only (segregation of the data).

Question 12: What kind of additional security measures should be taken by both the professional and the external provider?

8 April 2016

The additional measures to be taken by both the professional and the external provider are the following:

i) the professional should ensure, or get the assurance from the external provider, that the premises where the video conference takes place are separated from the other offices and that the access to these premises is adequately restricted and secured;

ii) all kinds of communications between the professional, his customer and/or, if applicable, the external provider, which allow the exchange of identification data, have to be encrypted or protected by taking technical measures which ensure the security of these communications;

iii) if the external provider uses a video conference system which is provided for by another third party, this third party is not allowed access to the content of the (flow of the) information;

iv) if, where applicable, the communication between the customer and the external provider is not initiated via the website of the professional (e.g. redirection from his website to the website of the external provider) and therefore is not under the professional's control, the professional has to perform an evaluation of the measures which have been put in place by the external provider in order to prevent fake website or mobile applications (risk of phishing of the external provider).

Question 13: Are there any special conditions regarding data protection requirements?

8 April 2016

The CSSF recommends to the professional to clear the process of identification/verification through video conference with the Commission Nationale pour la Protection des Données (CNPD) and, if applicable, other relevant data protection authorities of the country of residence of the customers, from a point of view of data protection, for which the CSSF is not competent.

Question 14: May AML/CFT obligations of the professional other than the identification/verification of identity of the customer be performed through an online video conference with the customer?

8 April 2016

Yes, the professional may make use of the video chat for the purpose of fulfilling other customer due diligence/KYC (Know Your Customer) obligations. In case of a delegation by the professional of the performance of customer due diligence measures through video chat, Article 3-3 of the Law will have to be respected.

Question 15: What is the role of the CSSF with respect to external providers of video identification (automated or not) tools?

8 March 2018

The CSSF is the competent authority for supervising compliance with AML/CTF regulations by the professionals falling under the scope of its supervision. Thus, the CSSF will verify compliance of these tools and systems as applied by and integrated into the particular processes and overall AML/CTF and IT frameworks of the Luxembourg professional of the financial sector. However, the role of the CSSF is not to provide certification of tools or systems proposed by firms to Luxembourg financial sector professionals.

Question 16: What type of activities related to customer due diligence for AML/CTF purposes would require a licence as a professional of the financial sector in Luxembourg?

8 March 2018

For the purpose of identifying and verifying the identity of customers, Luxembourg professionals are allowed relying on third-party introducers or on outsourcees, in line with the requirements specified in Article 3-3 of the Law.

The Luxembourg Law of 5 April 1993 on the financial sector does not provide for a specific category addressing professionals whose activity would consist of identifying and verifying the identity of customers on behalf of other professionals of the financial sector. However, certain activities, which may also be linked to customer due diligence for AML/CTF purposes, can only be performed by licenced professionals of the financial sector, e.g. activities related to customer document management or communication services. In that case, the following types of licences may need to be considered by entities wishing to be active in this regard (Articles 29-2 and 29-4 of the Law of 5 April 1993 on the financial sector):

- administrative agent

– secondary IT systems and communication networks operator[1]

Commission de Surveillance du Secteur Financier

Interested entities that would like to carry out in Luxembourg an activity that may thus qualify them as one of the aforementioned professionals, shall define their business purpose and their activity in a sufficiently concrete and precise manner to allow the CSSF first to determine if they need a licence and if yes, for which type of licence they would then need to submit an application.

[1] *1 A primary IT systems operator can act as a secondary IT systems and communication network operator, but this licence is not required as such in relation with document management or communication services.*

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu