Remote Identification Procedures

Public Consultation on draft regulations entitled 'Electronic Trust Services (Remote Identification Procedures), Regulations

Consultation Document

Document reference	**MCA/C/20-4007**
Date of publication	**16th October 2020**

Malta Communications Authority
Valletta Waterfront, Pinto Wharf, Floriana FRN 1913
Tel: (356) 21 336 840. Fax: (356) 21 336 846
Website: www.mca.org.mt
E-mail: info@mca.org.mt

Table of Contents

1. Background

On the 1st July 2016 EU Regulation 910/2014 on electronic identification and trust services for electronic communications in the internal market (the 'eIDAS' Regulation) came into force and was as a result directly applicable to Malta. This EU Regulation provided for the repeal of the Directive 1999/93/EC which dealt with the regulation of electronic signatures. The eIDAS Regulation in substance enhances trust in electronic transactions in the EU by providing a common foundation for secure electronic interaction.

As a result of the enactment of the eIDAS Regulation, Government made various amendments to the then existing legislation dealing with electronic signatures. These amendments were mainly done by amending the Electronic Commerce Act (Cap. 426), whereby the then applicable provisions relating to electronic signatures were deleted, whereas new provisions were introduced to facilitate the enforcement of the eIDAS Regulation in line with the requirements of the aforesaid EU Regulation. As a result of these amendments the MCA as the competent regulator under the Electronic Commerce Act assumed the role of the supervisory body responsible for ensuring compliance with the requirements of the eIDAS Regulation.

This consultation is being issued for public consultation post consultation with the office of the Parliamentary Secretary for Financial Services and Digital Economy within the Ministry for Finance and Financial Services. The consultation period will run from the **16th October 2020** to the **20th November 2020**. Please refer to **Section 5** for further details about the submission of comments.

Next Steps

The MCA will, after taking into consideration the responses received to this consultation, submit to the Parliamentary Secretary for Financial Services and Digital Economy within the Ministry for Finance and Financial Services its proposed amendments to the Regulations.

2. Purpose

Article 24 of the eIDAS Regulation requires that a qualified trust service provider ('QTSP') verifies the identity, and where applicable any special attributes, of the person to whom a qualified certificate is being issued. Article 24 lists amongst the diverse identification methods that may be used, the following methods namely:

'other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence'.

The eIDAS Regulation further requires that such 'equivalent' assurance' is confirmed by a conformity assessment body ('CAB'). One such method which is gradually being used in various EU member states is the use of remote identification procedures by using video-conferencing.

The purpose of the proposed regulations is to regulate the use of remote identification procedures by QTSPs, ensuring that the procedures used are duly certified by a CAB as being in compliance with the safeguards provided for in the said proposed regulations.

3. The salient points of the proposed regulations

Unless stated otherwise the definitions in the eIDAS Regulation and the Electronic Commerce Act apply. This serves to ensure that there is consistency in the interpretation of the terms used in all the applicable laws.

A QTSP before making use of a remote identification procedure, is required to submit to the MCA a conformity assessment report ('CAR') issued by a CAB, which report must confirm that the QTSP provides equivalent assurance in terms of physical presence and meets all the requirements as stated in the draft regulations.

The draft regulations require a QTSP to undertake various measures before adopting a remote identification procedure, including carrying out a risk analysis, tests of the effectiveness and safety and an internal assessment of the adequacy of the method to be used to mitigate any risks identified in the risk analysis.[1] The draft regulations also provide for a number of technical and organisational requirements that the QTSP must abide with, norms to be complied with during the actual remote identification session, and norms requiring the recording and retention of such a session.[2]

The draft regulations provide the necessary enforcement tools to enable the MCA to inspect and require any information about any remote identification procedures carried out in compliance with the draft regulations. The MCA is furthermore empowered to require any person to desist from the continued use of any remote identification procedure if there is non-compliance with the applicable norms.[3] The draft regulations empower the MCA to impose administrative fines if there is a breach with the provisions of the proposed regulations.[4]

[1] See reg. 6 of draft regulations.
[2] Ibid regs. 7 to 12.
[3] Ibid reg.15.
[4] Ibid reg.16.

4. The need to regulate remote identification procedures

Such regulation is required for a number of reasons namely:

- The MCA had received a number of requests from potential foreign QTSPs who were interested in establishing their business operations in Malta. Since Malta does not currently expressly cater for remote identification regulation, these QTSPs did not proceed with their plans.

- Various EU member states have taken measures to facilitate the use of remote identification procedures. Malta, in line with such developments in other countries, needs to actively consider the introduction of the appropriate regulatory measures more so if it is to attract foreign based QTSPs to Malta.

- Such procedures shall contribute to the uptake of eCommerce and the general trust of the public and business in information systems. For instance, the ability to securely sign documents without the need for a wet signature will greatly improve the efficiency of electronic transactions.

- It is important that there is a solid regulatory regime factoring such safeguards facilitating such procedures whilst ensuring that there is no misuse or abuse of such procedures.

5. Invitation to comments

The Authority invites comments on the draft regulations, and proposals on any other aspects that may be deemed relevant for the purposes of this consultation. For the sake of clarity and ease of understanding, the Authority encourages stakeholders to structure their comments in the same order as adopted throughout this document.

In accordance with its obligations under Article 4A of the Malta Communications Authority Act [Cap. 418 of the Laws of Malta], the Authority welcomes written comments and representations from interested parties and stakeholders during the consultation period, which shall run from the 16th October 2020 till the 20th November 2020.

The Authority appreciates that respondents may provide confidential information in their feedback to this Consultation document. Such information is to be included in a separate annex and should be clearly marked as confidential. Respondents are also requested to state their reasons why the information should be treated as confidential. For the sake of transparency, the Authority may publish a list of all respondents to this Consultation on its website, within three (3) working days following the deadline for responses.

The Authority will take the necessary steps to protect the confidentiality of all such material as soon as it is received, in accordance with its confidentiality guidelines and procedures. Respondents are however encouraged to avoid confidential markings wherever possible.

The MCA will, after taking into consideration the responses received to this consultation, submit to the Parliamentary Secretary for Financial Services and Digital Economy within the Ministry for Finance and Financial Services the proposed changes to the Regulation.

The consultation period will run until close of business of 20th November 2020.

All responses are to be submitted to the MCA electronically on eidas@mca.org.mt or in writing to:

The Chief Executive Officer
Malta Communications Authority
Valletta Waterfront,
Pinto Wharf, Floriana, FRN1913 Malta.
Tel: +356 21 336840
Fax: +356 21 336846

Extensions to the consultation deadline will only be permitted in exceptional circumstances and where the Authority deems fit. The MCA reserves the right to grant or refuse any such request at its discretion. Requests for extensions are to be made in writing within the first ten (10) working days of the consultation period.

Appendix I - Proposed Regulations

ELECTRONIC COMMERCE ACT
(CAP. 426)

Electronic Trust Services (Remote Identification Procedures) Regulations, 2020

IN exercise of the powers conferred on him by article 25 of the Electronic Commerce Act, the Minister responsible for communications has made the following regulations:

Citation

1. The title of these regulations is the Electronic Trust Services (Remote Identification Procedures) Regulations, 2020.

Definitions,
Cap. 426,
Regulation (EU) No 910/2014

2. (1) Any reference in these Regulations to "the Act" is a reference to the Electronic Commerce Act, and any reference to "the EU Regulation" is a reference to the 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. Unless stated otherwise in these Regulations the provisions of article 2 of the Act, and of Article 3 of the EU Regulation shall apply in relation to these Regulations.

(2) In these Regulations unless the context otherwise requires:

Cap. 418
"approved alternative means of communication" means an alternative means of communication to videoconferencing, which means is approved in writing beforehand by the Authority in accordance with the regulation 7 of these Regulations;

"Authority" means the Malta Communications Authority established under the Malta Communications Authority Act;

Cap. 586
"Data Protection law" means the Data Protection Act, any regulations made thereunder and any applicable EU legislation regulating data protection including Regulation (EU) 2016/679 (General Data Protection Regulation);

Cap.258
"identity document" means an identity card, a residence document or an identification document issued under the Identity Card and Other Identity Documents Act, or an identity card or passport issued by the pertinent authorities of a Member State of the European Union, Norway, Iceland, Liechtenstein or Switzerland;

"qualified trust service provider" includes any person acting under the authority of or engaged by a qualified trust service provider, to perform any functions on its behalf in accordance with these Regulations; and

"video-conferencing" means such means of communication that consists of any form of interactive communication that allows the transmission and capture of sound, image and data in real time.

Purpose

3. The purpose of these regulations is to regulate the use of remote identification procedures by qualified trust service providers, which procedures provide equivalent assurance in terms of reliability to physical presence as referred to in Article 24(1)(d) of the EU Regulation.

Submission of a conformity assessment report

4. (1) A qualified trust service provider established in Malta that intends to identify individuals through remote identification procedures in accordance with the provisions of Article 24(1)(d) of the EU Regulation, shall prior to the implementation of such procedures, submit to the Authority a conformity assessment report issued by a conformity assessment body. This report shall consist of a separate report that shall confirm or otherwise that the qualified trust service provider concerned and the aforesaid remote identification procedures provide equivalent assurance in terms of reliability to physical presence, and meet the requirements stated in regulations 5 to 14 of these regulations.

(2) A qualified trust service provider shall not make use of a remote identification procedure unless the Authority first approves in writing the conformity assessment report required in accordance with subregulation (1):

Provided that the Authority shall communicate its decision as to whether it approves or not the required conformity assessment report to the qualified trust service provider within three months from the receipt by the Authority of the aforesaid report.

Risk assessment and risk management

5. (1) Prior to the adoption of a remote identification procedure a qualified trust service provider shall:

(a) carry out a risk analysis in accordance with Article 19(1) of the EU Regulation with regards to the implementation of the identification of individuals through remote identification procedures. Such risk analysis shall in particular identify:

(i) the risk of mistaken identification and impersonation,

(ii) the risks related to the presentation of falsified or counterfeited documents, and

(iii) the risks related to the tampering of image capturing systems or of communication channels; and

(b) carry out tests of the effectiveness and of the safety of the implemented remote identification method;

(c) carry out internal assessment of the adequacy of the remote identification method used to mitigate the risks identified in the risk analysis:

Provided that within the context of any such assessment, efficiency of identifying the aforesaid risks shall be at least equivalent to the physical presentation of the identity document;

(2) Any analysis, test or opinion however so described made under this regulation shall be recorded and logged for a minimum period of four years or any such longer period as the Authority may consider appropriate in the circumstances.

Requirements relating to the personnel of a qualified trust service provider

6. (1) Remote identification methods shall only be operated by trained and fully skilled persons who are duly authorised by a qualified trust service provider to act on its behalf and to undertake any work related to such methods.

(2) A qualified trust service provider shall ensure that any persons who operate remote identification methods on its behalf, undertake periodic training with regards to the

verification of national approved identification documents, to the identification of fraud and, or to counterfeit practices of identity evidence and, or of documents.

Technical and organisational requirements

7. (1) A qualified trust service provider shall ensure that:

(a) remote identification is carried out by means of videoconferencing or of an approved alternative means of communication done in real time and without interruption or pause, and in a place with restricted access both physically and from a computer and, or communications network perspective;

(b) the remote identification session relating to the person to be identified is adequately protected with end-to-end encryption ensuring its integrity and confidentiality;

(c) the remote identification session is recorded in such a manner as to adequately ensure sound and colour image recording of sufficient quality to allow verification of the collected identification data:

Provided that such a recording shall include the date and time of the recording and the identification of the person or persons who operated and were responsible for the remote identification session:

Provided further that the data of the remote identification session shall be recorded in such a manner as to ensure its integrity and to prevent any counterfeiting thereof;

(d) the means of remote identification is of adequate quality such as to allow the clear identification with a high degree of definition, of the elements and security features of the identification document of the person to be identified;

(e) the system used for remote identification recognises and interprets the machine-readable zone (MRZ) of the identification document;

(f) it establishes and regularly updates written and documented scripts for conducting remote identification, which scripts shall be used by any person acting on its behalf in the context of any remote identification videoconferencing conducted in accordance with these Regulations:

Provided that such scripts shall enable the verification of identification documents and of the person to be identified in such a manner that ensures that the checks and the order of such checks cannot be predicted:

Provided further that the scripts shall include the use of a single disposable code of limited duration, such as a one-time password, specifically provided for the purpose of the remote identification session, which code shall be generated centrally ensuring the traceability of the identification procedure and the provision of real time and uninterrupted videoconferencing or approved alternative means of communication. Such a code shall be sent to the person to be identified through a secondary channel such as by secure e-mail or by short message service (sms).

(2) A qualified trust service provider may, when submitting a conformity assessment report in accordance with regulation 4 whereby it intends to identify individuals through remote identification procedures, submit to the Authority for its approval an alternative means of communication to videoconferencing. In doing so the qualified trust service provider shall provide the Authority with all the technical information necessary to demonstrate to the Authority that the proposed means of communication is a viable alternative to videoconferencing and that such means provides security and assurance which are equivalent to the requirements stated in these Regulations:

Provided that it shall be at the discretion of the Authority to decide whether or not to approve such alternative means of communication. The Authority shall communicate any such decision in writing giving its reasons therefor:

Provided further that the Authority may require the provision of any relevant information in order to assist it in determining the suitability or otherwise of any such alternative means of communication.

Permitted identification documents

8. (1) The procedure for remote identification shall be applicable only to natural persons who have an identification document which is recognised under Maltese Law and which allows clear identification and verification of the photograph of the holder of the aforesaid identification document, includes the signature of the person concerned on the said document, and a minimum set of at least two security features of different categories.

(2) The qualified trust service provider shall make a list of the identification documents it accepts for the purpose of remote identification, which list the aforesaid service provider shall submit for approval by the Authority.

Requirements to be observed during remote identification

9. (1) A qualified trust service provider when operating a remote identification method shall:

(a) check the status of the identification document used by the person to be identified, ensuring that the document is not damaged or altered in any way;

(b) check the overall layout of the identification document, its size, the position, spacing and size of the characters, and the typographic font:

Provided that in doing so, comparison shall be made against a verification template of the document being checked;

(c) check at least two security features of different categories;

(d) require the person to be identified to tilt the document horizontally and, or vertically in front of the camera;

(e) check the content of the individual characteristics found in the identification document, namely the comparison of primary and secondary photographs (identigram);

(f) capture a front and back image of the identification document;

(g) verify that the photograph and the personal description in the document identify the persons to be identified;

(h) verify the accuracy of the information contained in the identification document;

(i) ascertain the veracity of the information provided by the person to be identified during the remote identification session;

(j) use type and sequence of questions that are not identical in consecutive identification sessions;

(k) verify the consistency of the information collected about the person to be identified and the information resulting from the automatic calculation of machine-readable zone (MRZ) characters; and

(l) ask the person to be identified to do one or more causal acts so as to demonstrate the authenticity of the remote identification process.

(2) The procedure for proving identification shall only be considered to be complete after the insertion by the person identified of the single code such as a one-time password, and of the respective confirmation of that unique code by the remote identification methods used.

(3) An identification document provided for the purposes of these Regulations, must include a recent and recognizable photograph of the person concerned, his signature and must be issued by a competent public authority duly authorised to issue such a document.

Interruption of identification procedure

10. A remote identification session shall be interrupted and considered as null and void and without any effect at law if:

(a) the technical conditions necessary for the proper conduct of the remote identification are not adhered to, especially in the case of, but not limited to, poor picture quality, poor lighting, poor sound or interruptions or delays in the remote identification session or video transmission;

(b) the identification document presented during the remote identification session, gives rise to any doubt as to its content, authenticity, timeliness, accuracy or adequacy ; or

(c) during a remote identification session there is any doubt as to the veracity of any of the identification elements.

Declaration

11. (1) Prior to a remote identification session, the qualified trust service provider shall capture any photograph and any other identification document that shall be recorded throughout the entire remote identification session in relation to the identified individual:

Provided that in accordance with this regulation, the remote identification session shall be logged by the qualified trust service provider.

(2) Prior to the commencement of a remote identification session the qualified trust service provider shall provide the person to be identified with all the necessary information about the processing of his personal data, and then shall require such a person to sign a declaration that he is aware of the use that may be made of his photograph and, or any other identification document that may be required of him in order to facilitate any such session.

Retention and recording

12. The qualified trust service provider shall ensure that the entire remote identification session is recorded and that the recording thereof is kept for a minimum period of seven years after the expiry of the qualified certificate issued as a result of a session in accordance with Article 24(2)(h) of the EU Regulation.

Changes to the remote identification procedures

13. (1) A qualified trust service provider shall notify the Authority of any change in the implementation of the remote identification procedures covered by the conformity assessment report referred to in regulation 4 of these Regulations:

Provided that any such change shall be notified to the Authority at least forty days prior to the proposed implementation of such changes by the qualified trust service provider.

(2) Any changes to the remote identification procedures shall not be implemented unless first approved in writing by the Authority.

(3) The Authority may, on being notified of any change to the remote identification procedures, require the qualified trust service provider to request a conformity assessment body to perform a conformity assessment report of the changes to the remote identification procedures to confirm or otherwise that the changes are in compliance with the provisions of these Regulations:

Provided that if the Authority requires conformity assessment report then the provisions of regulation 4(2) shall apply:

Provided further that any expenses related to any such report shall be borne by the qualified trust service provider.

Compliance with data protection law

14. The qualified trust service provider shall ensure that any personal data is processed in accordance with Data Protection law.

Enforcement powers of the Authority
Cap. 418

15. (1) Without prejudice to its powers under the Malta Communications Authority Act, the Authority shall have the power to inspect and, or require any information from any person about any remote identification procedures carried out under these regulations:

Provided that the Authority may also require that the qualified trust service provider at its expense requests a conformity assessment body to perform a conformity assessment of its remote identification procedures.

(2) The Authority may at any time require any person to desist from the continued use of any remote identification methods in accordance with these regulations, if the Authority considers that there is non-compliance with any of the provisions of these regulations:

Provided that in doing so the Authority shall in writing state its reasons for doing so, which reasons shall be communicated to the person concerned.

Non-compliance with these Regulations

16. The Authority may, in accordance with its powers under Part VII of the Malta Communications Authority Act, impose such sanctions as it may consider appropriate for any breach of these regulations:

Provided that any administrative fines that the Authority may decide to impose shall not exceed the amount of twenty-five thousand euro (€25,000) for each breach and two thousand five hundred euro (€2,500) for each day during which failure to observe the provisions of these regulations persists.

Fees due on submission of a conformity assessment report

17. A qualified trust service provider who, in accordance with regulation 4 of these regulations, wishes to provide remote identification procedures, shall when submitting to the Authority a conformity assessment report issued by a conformity assessment body as required under the aforesaid regulation 4, pay to the Authority an one-off fee of two thousand euro (€2,000) .