PROVISIONS FOR IDENTIFICATION AND VERIFICATION WITHOUT PHYSICAL CONTACT

JULY 2026

Scharlooweg 172-174 • Willemstad, Curaçao • t. +599(9) 737-2299 • e. info@cga.cw • www.cga.cw

Contents

I. SCOPE AND LEGAL BASIS OF THE PROVISIONS 4

Provisions for the implementation of Article 3 paragraph 1 of the NOIS 4

a. Required Identification Documents 4

b. Identification and Verification without physical contact 4

c. Required Provisions for Identification and Verification without physical contact 4

d. Compliance with Provisions for Identification and Verification without physical contact 5

e. Sanctions for violation of the Provisions for Identification and Verification without physical contact 5

II. IDENTIFICATION & VERIFICATION WITHOUT PHYSICAL CONTACT 6

Establish Identity of Natural Person 6

II.1 Identity Validation 6

II.2. Verification of Identity 7

III. POLICIES AND PROCEDURES 11

III.1. Pre-implementation requirement for remote onboarding solutions 11

III.2. Policies and procedures relative to the use of remote onboarding solutions 12

III.3. Ongoing Monitoring of remote onboarding solution used 12

III.4. Definition of method for Ongoing Monitoring of remote onboarding solution 13

III.5. Remedial actions in case of materialized risks relative to the remote customer onboarding solution 14

IV. TECHNOLOGY AND SECURITY REQUIREMENTS 15

V. IMPLEMENTATION 17

Transitional Provision 17

Appendix 1. Glossary & Definitions 18

PREFACE

Article 3 paragraph 1 of the National Ordinance on Identification when rendering Services (NOIS)[1] stipulates that the authorities entrusted with supervision of the national ordinance must establish provisions for the identification and verification of a natural person that is not physically present for identification, taking into account the risks associated with the type of client, business relation, service, product or transaction that is provided and with the geographical risk factors.

Therefore, the Curaçao supervisory authorities entrusted with supervision of the NOIS – the Central Bank of Curaçao and Sint Maarten ("CBCS"), the Financial Intelligence Unit ("FIU") and the Curaçao Gaming Authority ("CGA") - together and in close collaboration with the private sector drafted these provisions of which the primarily objective is to comply with the stipulations in article 3 of the NOIS. These provisions, furthermore, provide for a uniform approach among sectors under supervision when conducting identification and verification without physical contact and ensure compliance with existing AML/CFT/CFP legal requirements. Therefore, the provisions for identification and verification without physical contact form an integral part of the existing AML/CFT/CFP provisions and guidelines for the various sectors under supervision. Existing legislative provisions shall take precedence over these provisions in case of conflict. Finally, these provisions aim to safeguard the responsible use of available and new technologies when conducting identification and verification without physical contact.

[1] Service providers must always ensure that they comply with the most recent stipulations of law and executive decrees.

I. SCOPE AND LEGAL BASIS OF THE PROVISIONS

Provisions for the implementation of Article 3 paragraph 1 of the NOIS

These provisions provide for the implementation of article 3 paragraph 1 of the NOIS and must be complied with by all service providers within scope of the NOIS ("service providers").[2] This specific article in the NOIS provides for the identification of a natural person and further provisions to be observed by service providers as detailed below under a) up to and including e).

a. Required Identification Documents

If the client is a natural person, identity will be established using one of the following documents valid in the country of issuance:

a. a driving license;
b. an identity card;
c. a passport;
d. another document to be designated by the Minister of Finance.

Furthermore, paragraph 2 and 4 of article 3 stipulate that for individuals who are considered controllers, proxy-holders, directors, representatives or ultimate beneficiaries which are legal entities, the identification of these individuals must be done in line with paragraph 1. Therefore, these provisions apply to their identification/verification.

b. Identification and Verification without physical contact

Furthermore, the article stipulates that if the natural person is not physically present for identification, **the identification** and **verification** shall take place taking into account the specific risks associated with business relations or transactions without personal contact.

c. Required Provisions for Identification and Verification without physical contact

Refers to these provisions.

[2] These provisions are not applicable to money transfer companies. These companies cannot have non-face-to-face clients.

d. Compliance with Provisions for Identification and Verification without physical contact

A service provider is obliged to implement the provisions issued by the Supervisor.

e. Sanctions for violation of the Provisions for Identification and Verification without physical contact

The service provider is required to comply with these provisions issued by the supervisory authority. Failure to comply with these provisions will result in violation of article 3 paragraph 1. Articles 9a, 9j and 9v of the NOIS provide for administrative and criminal sanctions including fines, penalties, license revocation and imprisonment for violation of these provisions.

II. IDENTIFICATION & VERIFICATION WITHOUT PHYSICAL CONTACT

Establish Identity of Natural Person

The required identification documents as stipulated in the NOIS are internationally recognized and comply with the principle of being independently sourced documents as required by the Financial Action Task Force ("FATF") Recommendations. The validation of the (copy of) identification documents for clients who are not physically present is to be established through the application of a properly sourced verification and authentication process which may include the following methods.

II.1 Identity Validation

Through this process the authenticity of information or documents provided is confirmed. Methods through which this may be achieved are:

II.1.A. Certification

This method was until the amendment of NOIS in May 2024 the only acceptable method of validation of identification without physical contact. This remains a valid and secure method of identification without physical contact. A photocopy of one of the documents listed in section I a) provided it is accompanied by:

a. certified copy or extract from the Civil Registry of the client's place of residence or admission; or
b. the sending of one of the documents mentioned electronically, provided the service provider receives a certified copy of the sent document within two weeks of electronic receipt.

II.1.B. Use of advanced technology

It is possible to use advanced technology for identity validation purposes.

Examples of this include:

I. To detect fine laser engraving features of an ID, remotely, where this applies. Since these (laser) engraved text or images might only be visible under magnification or specific lighting, special advanced technology might be required.
II. Verification of biometric data such as fingerprints, face recognition, or iris scans through video images, to match the individual to the document, ensuring its authenticity.
III. Scan and verify the authenticity of (various) IDs using specialized software and/or applications. These tools compare documents against known templates and security feature databases.
IV. Detecting microprinting where applicable. Some documents include microprinting, tiny text or patterns that are difficult to reproduce without specialized equipment. Advanced technologies might contain magnifying tools that can help identify these safety features, even remotely.
V. Videoconferencing: Using videoconferencing for identity verification, through a visual ID-check, combined with document verification, likeliness checks and other appropriate measures. Videoconferencing may be conducted using commonly available platforms that allow real-time audio-visual interaction. Identity verification through videoconferencing must not be limited to a visual inspection of an identity document and must be supplemented by additional verification measures where required by the risk-profile of the customer.

II.1.C. Comparing with Official Records and/or reliable public sources

Where available, verification against an official government or institution database and/or reliable public sources can help determine if the ID number, name, and other details match official records. With this the electronic copy can be authenticated.

II.2. Verification of Identity

Through this process the information and documents are matched against the natural person. The following verification methods can be considered when verifying the validated ID of a client.

II.2.A. QR Code Scanning

Many modern IDs contain a QR code that store information about the individual. Scanning these codes can verify the details, such as the date of birth, address, and other key data, against the provided copy of the ID and the issuing authority's database. Note that not all countries make the QR-code data accessible to the wider public.

II.2.B. Other advanced technology options for verification of identity

Remote customer onboarding solutions implemented by a service provider must, at a minimum, enable the confirmation of a match between the visible information of the natural person and the documentation provided, as part of their verification process.

Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, service providers must make sure that the biometric data is sufficiently unique to be unequivocally linked to a single natural person. Service providers must use strong and reliable algorithms to verify the match between the biometric data provided on the submitted identity document and the customer being onboarded. In situations where the solution does not provide the required level of confidence, additional controls must be applied.

In situations where the evidence provided is of insufficient quality resulting in ambiguity or uncertainty so that the performance of remote checks is affected, the individual remote customer onboarding process must be interrupted and restarted or redirected to a face-to-face verification.

Where service providers use unattended remote onboarding solutions, in which the customer does not interact with an employee to perform the verification process, they must:

a. ensure that any photograph(s) or video is taken under adequate lighting conditions and that the required properties are captured with necessary clarity to allow the proper verification of the customer's identity;
b. ensure that any photograph(s) or video is taken at the time the customer is performing the verification process;
c. perform liveness detection verifications, which may include procedures where a specific action from the customer is required to verify that he/she is present in the communication session, or which can be based on the analysis of the received data and does not require a specific action by the customer;

d. use strong and reliable algorithms to verify if the photograph(s) or video taken matches the picture(s) retrieved from the official document(s) belonging to the customer.

For the purposes of these provisions, 'strong and reliable' shall be assessed with reference to internationally recognized standards (such as relevant ISO/IEC/ or NIST frameworks), without mandating a specific standard. Service providers shall document the basis on which the robustness and reliability of the technology is determined.

Where service providers use attended remote customer onboarding solutions in which the customer interacts with an employee to perform the verification process, they must:

a. ensure that the quality of the image and/or audio is sufficient to allow the proper verification of the customer's identity and that reliable technological systems are used;
b. foresee the participation of an employee who has sufficient knowledge of the applicable AML/CFT/CFP regulation and security aspects of remote verification and who is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence;
c. properly document in case unusual/suspicious behavior is detected.
d. have in place an escalation process defining the subsequent steps of the remote verification process as well as the actions required by the employee.

Staff procedures must include guidance on observing and identifying unusual behaviors or other features that might characterize suspicious behavior during remote verification.

Minimum standards for the use of technological solutions for the verification and authentication of customer identity must comply with:

a. the information obtained through the remote customer onboarding solution is up-to-date and adequate to meet the applicable legal and regulatory standards for initial customer due diligence;
b. any images, video, sound and data are captured in a readable format and with sufficient quality so that the customer is unambiguously recognizable;
c. the identification process does not continue if technical shortcomings or unexpected connection interruptions are detected.

Service providers must ensure, through their internal control frameworks, that remote verification tasks are performed only by personnel with adequate knowledge, skills and training, and who have been expressly authorized to perform such tasks.

III. POLICIES AND PROCEDURES

Article 5e of the NOIS requires the service provider to have policies and procedures in place to address the specific risks associated with business relationships or transactions without physical contact. This section of these provisions sets out the standards for these policies and procedures.

III.1. Pre-implementation requirement for remote onboarding solutions

Service providers falling under the scope of the NOIS, must set out the scope, steps and record keeping requirements of the pre-implementation assessment in their policies and procedures, which must include at least:

a. an assessment of the adequacy of the solution regarding the completeness and accuracy of the data and documents to be collected, as well as of the reliability and independence of the sources of information it uses;
b. an assessment of the impact of the use of the remote customer onboarding solution on its business-wide risks, including ML/TF, operational and IT related, reputational and legal risks;
c. the identification of possible mitigating measures and remedial actions for each risk identified in the assessment under letter b);
d. tests to assess fraud risks including impersonation fraud risks and other information and communications technology ("ICT") and security risks (note: here reference can be made to other regulation issued by the supervisory authority on this matter);
e. an end-to-end testing of the functioning of the solution targeting customer(s), product(s) and service(s) identified in the remote customer onboarding policies and procedures.

Service providers must be able to demonstrate to their supervisors which assessments they carried out before implementation of the remote customer onboarding solution, the outcome of their assessment and how its use is appropriate in light of the ML/TF risks identified for the types of customer(s), service(s), geographies and product(s) in its scope.

Service providers must start using a remote customer onboarding solution only once they are satisfied that it can be integrated into the institution's wider internal control system, thereby allowing the service provider to adequately manage the ML/TF risks that may arise from the use of the remote customer onboarding solution.

The pre-implementation requirements apply to the introduction or material modification of remote identification solutions and shall be implemented within the transitioned period provided for these Provisions.

III.2. Policies and procedures relative to the use of remote onboarding solutions

The policies and procedures relative to the remote onboarding of clients must be risk-sensitive and set out at least:

a) a general description of the solution the service provider has put in place to collect, verify, and record information throughout the remote customer onboarding process. This must include an explanation of the features and functioning of the solution;
b) the situations where the remote customer onboarding solution can be used, taking into account the risk factors identified and assessed in accordance with Article 2, paragraph 4 of the NOIS and in the business-wide risk assessment, including a description of the category of customers, products and services that are eligible for remote onboarding;
c) which steps are fully autonomized and which steps require human intervention;
d) a description of the induction and regular training programs to ensure staff awareness and up-to-date knowledge of the functioning of the remote customer onboarding solution, the associated risks, and of the remote customer onboarding policies and procedures aimed at mitigating such risks.

The policies and procedures, when implemented, must enable service providers to ensure compliance with all applicable laws and regulations, especially AML/CFT/CFP obligations, including the requirements applicable under:

- Reliance on third parties and outsourcing;
- ICT and security risk management; and
- data protection and privacy legislation requirements.

III.3. Ongoing Monitoring of remote onboarding solution used

Service providers must monitor the method used for remote identification and verification on an ongoing basis to ensure that it operates in line with the service providers' expectations. They must complement their policies and procedures with a description of at least:

a) the steps they will take to be satisfied with the ongoing quality, completeness, accuracy and adequacy of data collected during the remote customer onboarding process, which must be commensurate to the ML/TF/PF risks to which the service provider is exposed to;
b) the scope and frequency of such reviews; and
c) the circumstances that will trigger ad-hoc reviews, which must include at least:
    I. changes to the ML/TF/PF risk exposure of the service provider;
    II. deficiencies on the functioning of the solution detected in the course of monitoring, audit or supervisory activities;
    III. a perceived increase in fraud attempts;
    IV. changes to the legal or regulatory framework.

Where monitoring identifies deficiencies that affect the effectiveness or reliability of the remote customer onboarding solution, the service provider must document the remedial actions taken. Such actions may include enhancement of the solution, temporary suspension of its use, or discontinuation thereof, in accordance with the service provider's AML/CFT governance framework and risk management policies and procedures.

III.4. Definition of method for Ongoing Monitoring of remote onboarding solution

Service providers must consider the most effective way to monitor the ongoing adequacy and reliability of the remote customer onboarding solutions. They must consider one or more of, but not limited to, the following means:

I. quality assurance testing;
II. automated critical alerts and notifications;
III. regular automated quality reports;
IV. sample testing;
V. manual reviews.

This section also applies where fully automated remote customer onboarding solutions are used which are highly dependent on automated algorithms, without or with little human intervention.

The policies and procedures, when implemented, must enable institutions to ensure compliance with the provisions in articles 2 and 3 of the NOIS when conducting non-face- to-face identification and verification.

III.5. Remedial actions in case of materialized risks relative to the remote customer onboarding solution

Service providers must set out in their procedures and processes remedial measures where a risk has materialized, or where errors have been identified that have an impact on the efficiency and effectiveness of the general remote customer onboarding solution.

These measures must include at least:

- a review of all affected business relationships, to assess whether sufficient initial CDD has been applied by the service providers. Service providers must prioritize those business relationships that carry the highest ML/TF/PF risk;
- taking into account the information obtained in the above-mentioned review, an assessment of whether an affected business relationships must be:
  a. subject to additional due diligence measures;
  b. subject to limitations, such as limits on the volume of transaction, where permitted under national law, until such time as a review has taken place;
  c. terminated;
  d. reported to the FIU;
  e. reclassified into a different risk category.

Service providers must be able to demonstrate to their supervisor which reviews they carried out and the remedial steps[3] they have taken to rectify any shortcomings identified throughout the lifetime of the remote customer onboarding solution.

[3] Remedial actions shall be proportionate to the nature, severity and impact of the identified risk. Service providers must define materiality thresholds to distinguish between minor deficiencies and material or systematic issues.

IV. Technology and Security Requirements

The chosen technological solution must be thoroughly tested for accountability and reliability before it can be used. The following aspects have to be minimally included in the supervised institution's testing policies and procedures:

- Audit trail – detailed registration of the steps in the identification and verification process. Time stamps, IP addresses and other relevant data are important. Logbook, so that one can track what is changed and by whom. - Secure storage of evidence (important for compliance reviews/audits)
- Encryption of data
- Safeguarding customer privacy
- Use technology (watermarks etc.) that can verify the authenticity of identification documents and/or verification technology (facial recognition etc.)
- Security audit and penetration testing
- Measuring the accuracy of biometric verification technology
- Resistant to cyber-attacks and other threats (unauthorized access)
- Periodic and event-driven review and improvement of processes ,, commensurate with the nature, scale and risk of the activities
- Periodic and event-driven quality assurance activities, proportionate to the identified risks (with documentation)

The procedures must ensure that risks related to remote onboarding are identified and assessed as part of the service provider's business- wide risk assessment and the systematic AML/CFT risk assessment (SARA).

Service Providers should ensure that all bespoke technologies be developed using an industry-recognized Secure Software Development Lifecycle (SSDLC), ensuring secure coding practices are integrated throughout development and/or procurement.

- **Institutions must implement secure, tamper-proof technologies to support identity verification. These technologies must:**
  - Support end-to-end encryption (data in transit, at rest, and at processing)
  - Exploit multi-factor authentication (MFA) where applicable
  - Log system access, processing, and modifications for auditability

- **Biometric systems must:**
  - Be tested for bias and false acceptance/rejection rates

- Undergo regular performance and fairness audits
- Store biometric data in tokenized or encrypted form, separate from identity attributes

➢ **Managed service providers for cloud-based or outsourced verification systems must:**
- Demonstrate robust commitment to information security and organizational resilience aligned with internationally recognized standards (preferably through ISO 27001 and 22301 certifications);
- Be able to provide periodic independent assurance of robust and effective controls in place to safeguard data and maintain security, availability, processing integrity, confidentiality, and privacy of information (through e.g. SOC or ISAE3402 Type 2 reports).

➢ **Cloud-based or outsourced verification systems must:**
- Be hosted in jurisdictions with strong data protection laws (e.g., GDPR adequacy), complementing local data protection laws and regulations
- Undergo independent security testing and penetration testing annually

➢ **All customer-facing applications must:**
- Be subject to regular vulnerability scans
- Include clear privacy notices and consent capture mechanisms

V. IMPLEMENTATION

These provisions enter into force on the date of their publication.

Service providers that do not yet make use of a remote customer onboarding solution must comply with all provions set out herin prior to implementing any such solutions.

Transitional Provision

Service providers that, at the date of entry into force of these provisions, already make use of a remote customer onboarding solution must ensure that they fully comply with the requirements set out in these provisions as of May 1, 2027.

During this transitional period, existing solutions may continue to be used, provided that the service provider has initiated the steps necessary to achieve compliance and can demonstrate this to the Supervisor upon request.

Appendix 1. Glossary & Definitions

Authentication:	establishes that the person who attests his or her identity is the same person whose identity was obtained, verified, and credentialed during on-boarding.
Identification data:	refers to reliable, independent source documents, data or information.
Remote Identification and Verification:	Identification and Verification without physical contact
Service Providers:	any person who provides a service professionally or commercially within the context of article 1 paragraph 1 of the NOIS
Supervisors:	the Central Bank of Curaçao and Sint Maarten, The Supervisory Department of the Financial Intelligence Unit, Curacao and the Curacao Gaming Authority in accordance with the provisions of article 11 of the NOIS.
Validation:	is part of identity proofing and involves determining that the documents are genuine (not counterfeit or misappropriated) and the information the evidence is accurate by checking the identity information/evidence against and acceptable (authoritative/reliable) source to establish that the information matches reliable, independent source data/records.
Verification:	Link the individual to the identity evidence provided (e.g., using biometric solutions like facial recognition and liveness detection).