هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY
Kingdom of Bahrain - مملكة البحرين

Facial Recognition Requirements Document

In 2015, the TRA issued an Electronic Solution Requirements Document. That document was issued to enable mobile network operators to comply with their obligations under Article 7 of the SIM-Card Enabled Telecommunications Services Registration Regulation ('the Regulation'). Except as provided for in clause 6 below, this Facial Recognition Requirements Document ('the FRT Requirements Document') supplements the Electronic Solution Requirements Document. It does not replace it. As such it is also aimed at enabling Affected Licensees to satisfy the requirements of Article 7 of the Regulation by the introduction of facial recognition technology ('FRT').

All defined terms used in this document shall have the definition given to them in the Regulation unless otherwise specified.

1. **Facial Recognition Technology**

   1.1 For the proper implementation of FRT licensees must adhere to the requirements set out in this FRT Requirements Document.

2. **Purpose Limitation**

   2.1. The utilization of facial recognition technology within the telecommunications sector is strictly limited to the sole purpose of identity verification of Subscribers in line with the Regulation.

   2.2. Furthermore, Affected Licensees must clearly communicate to Subscribers prior to the collection and processing of facial data[1], the exclusive purpose of using FRT which is for identity verification during the onboarding process. This information should also

[1] Facial Data includes the features of a Person that are mathematically mapped as a faceprint.

include the specific data being collected. In line with the applicable Data Protection rules, explicit consent must be obtained.

2.3. Affected Licensees must put in place explicit policies to prohibit the use of facial data for any purposes beyond identity verification, ensuring that such data is not processed for marketing, surveillance, or any other unrelated purpose.

3. Consent and Privacy

3.1. Affected Licensees shall design facial recognition systems to allow individuals to easily opt-out should they not want to continue the on-boarding process.

3.2. Affected Licensees are expected to adopt practices that adhere to the principle of data minimization, ensuring that only the data that is absolutely necessary for identification verification purposes is collected.

4. Transparency and Accountability

4.1. Affected Licensees must inform Subscribers prior to registration that facial data collected through recognition technology may undergo manual processing, and clearly communicate the purpose behind manual processing, such as enhancing the accuracy of verification or addressing exceptional cases where automated processes may be insufficient.

4.2. In the event of any breach of this document, Affected Licensees are obligated to promptly (and in any case no later than one working day) notify the TRA.

5. Accuracy and Bias Mitigation

5.1. Affected Licensees must ensure that the FRT being utilized contains the following elements:

5.1.1. **ISO 30107-3 Certification**: Facial recognition solutions must be certified with ISO 30107-3, ensuring compliance with international standards for biometric technologies.

5.1.2. **Risk Indicator Integration**: Risk indicators must be integrated into the facial recognition system. This includes:

a. Virtual Private Network and The Onion Router traffic detection and prevention;

b. Rooted device detection and prevention.

5.1.3. **Restriction on Photo Uploads**: The FRT must prohibit the uploading of pre-scanned photos and required ID documents during the verification process, reinforcing the need for real-time capture to enhance security.

5.2. **Detection of Tampered Documents**: The FRT must contain mechanisms to detect and prevent the use of tampered ID documents against standard templates, including checks for alterations, erasures, or modifications.

5.3. **Document Authenticity Checks**: The Licensee must conduct authenticity checks against ID documents, verifying security features such as holograms, font consistency, expiry date validity, and minimum age requirements.

5.4. **Misuse Reporting**: Affected Licensees must establish a reporting mechanism for any misuse of FRT (any attempt by any person to use the FRT to circumvent the obligations set out in this document with the intent of either providing false identification information or impersonating a third party, e.g., through tampered ID documents, fake ID documents, identity theft, etc.). Affected Licensees are obligated to report instances of misuse to the TRA within three working days.

5.5. **False Acceptance Rate**[2]: Affected Licensees must ensure that a False Acceptance Rate of less than or equal to 0.5% is maintained, ensuring a high level of accuracy in facial recognition.

5.6. **Picture/Photo Liveness Assurance**: The FRT must contain measures to ensure liveness, including the detection of screens, masks, still images, and the verification of face movements to confirm the presence of a real person.

5.7. **Demographic Fairness**: The facial recognition system must provide fair and unbiased results across different demographic groups. Licensees are required to regularly assess and address any biases that may emerge during system operation.

6. Security

6.1. For valid Bahraini ID Card (CPR) holders or valid Bahraini passports holders, the identity verification can be done via fingerprint scanning or FRT.

[2] A statistical measure used to determine the probability of a biometric security system allowing unauthorized user access.

6.2. For valid GCC ID card holders and any valid passport issued by internationally recognized states (except those covered under Clause 6.1 above), FRT must be exclusively used when carrying out identification verification. This will come into effect on the 1 August 2024.

6.3. For the avoidance of doubt, driving licenses shall not be accepted as valid ID document for identity verification.

6.4. To ensure an accurate match for identity verification, the verification process must be capable of comparing the facial features captured in the self-portrait with the controlled scan of the official ID document. Should Affected Licensees wish to adopt an alternative facial recognition verification method, the TRA's consent must be obtained.

6.5. The very first mobile network connection, post-SIM/eSIM installation, should be to the carrier's network in Bahrain. Affected Licensees must not activate the SIM/eSIM if the very first connection is not to a Mobile Network in Bahrain.

6.6. Affected Licensees must implement technical and organizational measures to protect data from accidental destruction, loss, alteration, disclosure, access, and unauthorized processing.

6.7. To prevent interception or tampering during data processing, Affected Licensees must establish protocols for the secure processing of facial data between the user's device and the verification system.

6.8. To safeguard against interception or unauthorized access of facial data, Affected Licensees must adopt end-to-end encryption[3] for facial data at rest and in transit.

6.9. Facial data and ID document scans collected during identity verification processes shall neither be stored/retained within the Affected Licensee's database nor within the solution provider's database. Facial data should be transferred to the Subscriber Database Management System ("SDMS").

7. **Legal Compliance**

7.1. The FRT utilized must align with the relevant legal frameworks, including Bahrain's Personal Data Protection Law and the Telecommunications Law.

[3] Industry standard encryption methods that are accepted and adopted internationally.

Electronic Solution Technical Requirements Document

This document is issued by the Telecommunications Regulatory Authority (the "**TRA**" or the "**Authority**") to assist Affected Licensees in the implementation of an electronic solution to comply with Article 7 obligations of the new SIM-Card Enabled Telecommunications Services Registration Regulation (the "**New Regulation**") (the "**Document**").

All defined terms used in this document shall have the meanings given to them in the New Regulation unless otherwise specified.

1 Electronic Solution Specifications

1.1 In order to fulfil Article 7 obligations of the New Regulation, Affected Licensees will be required to have in place an Electronic Solution that meets the following specifications:

1.1.1 The electronic solution will have to read the smartcard, conduct a biometric scan, and be capable of taking a photograph;

1.1.2 Biometric scanner & smart card reader will have to:

(a) be capable of capturing BMP/WSQ/ISO19794-2:2005 compact card images with a Fingerprint scanning window size of, at a minimum,16 x 24mm and Image resolution of 480x320 pixel, 500 DPI;

(b) be capable of performing match-on-card and match-on-server biometrics verification;

(c) have two colours LED indicator for the biometric scan verification status;

(d) be capable of performing live finger detection;

(e) be compliant with ISO 7816 and EMV 2000;

(f) be capable of contact and contactless smart card reading;

(g) MRZ reading capability for passport registration;

(h) support 5V, 3V and 1.8V smart cards;

(i) support C4/C8 and 8 pin handling;

(j) have two colours LED indicator for smart card reader status;

(k) automatically detects smart card type and show Natural Person Identification Credentials on Workstation/Electronic Solution; and

(l) support plug and play feature.

1.1.3 Workstation/Electronic Solution will have to:

(a) support HTTPS;

(b) restrict the execution of parallel subscription applications;

(c) be compatible with and support the devices and functions mentioned within this document; and

(d) be able to connect to the necessary secured services for the purposes of verifying the biometric data.