EUROSMART
The Voice of the Digital Security Industry

Feedback on BSI draft TR-03166

Technical Guideline for Biometric Authentication Components in Devices for Authentication

August 2021

Eurosmart welcomes this opportunity to provide feedback on the BSI draft TR-03166 "Technical Guideline for Biometric Authentication Components in Devices for Authentication". This document is very timely: the European Commission published two months ago its proposal for a revision of eIDAS, which includes the issuance of a European Digital Identity Wallet in every Member State. Biometric technologies increasingly provide authentication means to access essential services (e.g., finance, administration, soon a European Digital Identity Wallet). Therefore, these technologies need to be secure enough and fulfil some necessary security requirements.

However, requirements applicable to biometric technologies need to undergo a reality check to ensure that they can effectively be implemented on the field, specifically in consumer smartphone devices, as we understand the intention. In this respect, Eurosmart would like to provide its insights on the BSI technical guideline.

1. Clarify the scope

A section presenting the scope of this document seems to be missing. It will be beneficial as the field of application is unclear.

In particular, it should be clarified that this document does not cover the case of biometric authentication used in remote identity proofing.

Besides, biometric cards (card fitted with a fingerprint sensor performing the biometric matching internally) can't meet the requirements stated in this document for several reasons (size of their sensors...) As such, it should be explicitly noted that this document does not apply to biometric cards fitted with sensors (i.e. biometric payment cards).

Also, all the usage of biometric authentication pertaining to law enforcement should be out of the scope of this document, i.e. Automated border Control (ABC) used for border crossing or device for controlling the identity of an individual. The main reason is that these usages are ruled by very specific requirements (Frontex, national requirements…), in particular regarding FAR. Also, as they usually take place in a supervised environment, the risk of presentation attacks is lower, particularly for face biometry.

It seems this document also aims at addressing biometric verification used for physical access control (§A3/UC1b, §2.1/Example). However, we think the current document is unsuitable for physical access control using biometric verification in a single factor authentication. In this use case, it is quite common that the reference biometry of authorised users is preregistered so that the user only has to present its biometry to cross the access control. The biometric system checks the candidate biometry to the reference biometry of authorised users. Therefore, the biometric system does not really perform a

biometric verification in 1 to 1, but in 1 to N – where N is usually small (a few hundreds/thousands). When performing biometric verification in 1 to N (with N small), the requirements of FAR are much harder to meet.

II. Biometric Assurance Level High

A very highly demanding level, but for which use cases?

The BSI technical guidelines do not provide any requirement to fit in with the current commercial use cases. The only applicable requirements for consumer biometrics are those defined by FIDO. As defined by the BSI technical guideline, Biometric Assurance Level “High” requirements are more demanding than those used for current commercial use cases.

Lack of biometric modalities

The FAR for single biometry for BAL “High” (1 in 333,333) is 10 times the one required for BAL “Substantial” (1 in 33,333). For facial biometry, this level of requirement is beyond what NIST currently tests through its Facial Recognition Vendor Test (FRVT), which is limited at 1/100 000, even for Technology Testing. When applied to scenario testing (as per ISO 19795) testing this operation point is entirely impractical. This lack will definitely hamper the deployment on the market of products meeting this highly demanding requirement. Besides, for those that will meet this requirement, it is highly likely that the testing procedure may be questionable, and thus may exhibit some bias. Therefore, alternate modes of implementation as provided by the BSI technical guideline, which rely on multimodal or multi-instance biometry may have to be carried out. While these alternates provide for higher FAR (1/100 000), it still remain very hard to meet for facial biometry for many suppliers, limiting the vendors able to meet this requirement. . Therefore, additional biometric modalities should be added in the scope of the document, such as iris, to allow (1) multimodal biometry or (2) choice of biometry when opting for the single biometry authentication at level "high", which is impossible as of today in the current scope of the document. Also, the technical report should be regularly updated to include any biometric modality that may arise on the market.

BAL “High” does not take into consideration devices already on the field

From the point of view of current devices, the FAR required for single biometry for BAL “High” (1 in 333,333) runs the risk of becoming an obstacle for users. Besides, alternate modes of implementation relying on multimodal biometry may not be possible as whether this multimodal mode of implementation is supported by current devices is not guaranteed. In that regard, a supplemental mode of implementation commensurate with the capacity of devices already on the field should be introduced for BAL “High”. Eurosmart suggests introducing a new mode of implementation combining PIN code and biometric verification to allow devices already on the field to meet BAL "high" but also "Substantial". Also Eurosmart underlines that the FAR required for level Normal (1 in 10,000) is the one currently used for finance and required by FIDO.

Requirements of entropy seem excessive

Similarly, the requirement of an entropy higher than 78 bit for BAL “High” seems excessive. As a point of comparison, a 6-digit PIN amounts to 20 bits of entropy and a 4-digit PIN to 13 bits of entropy. Nowadays, payments are typically secured with no more than a 4-digits PIN.

Requirements of FAR also seem excessive compared to other existing referentials

Regarding the FAR, BAL "High" go beyond current requirements for existing use cases such as payments and Automated Border Controls (ABC). As prescribed by the 2015 Frontex guidelines for ABC[1],the configuration of the face verification algorithm shall ensure a false accept rate (FAR) of 0.001 (0.1%) or less. For the fingerprint verification the FAR is 0.001 (0.1%)

Currently, financial transactions are secured to requirements by EMVCo and major payment operations, which largely coincide with FIDO requirements inspired by these. Google and Microsoft requirements on authentication security also fall close to these requirements.

The requirement for PAD is too high

The experience shows that is hardly possible for a biometric authentication system to be resistant to all presentation attacks with attack potential above "enhanced basic". Therefore, it will be hardly possible for vendors to meet (1) the BAL "High"(which require detection of presentation attacks potential "moderate"), (2) the application module [TR-03107-1] on BAL "Substantial" (which require detection of presentation attacks potential "moderate") and (3) the application module [TR-03107-1] on BAL "High" (which require detection of presentation attacks potential "high"). It will create a lack of products and solutions for these BALs.

Therefore, Eurosmart strongly advise to review these requirements to limit the required level of resistance to all presentation attacks to attack potential "enhanced basic".

For which use cases?

What kind of use cases are envisaged by the BSI for this level High?

Could the requirements of this document jeopardise the uptake of European Digital Identity Wallets?

To be used for the European digital identity wallet, biometric verification system should meet the requirements defined by BAL "High" enhanced by the application module [TR 03107-1]. It stems from the proposal for a revision of eIDAS which states that European Digital Identity Wallet shall meet the requirements with regards to assurance level "High" (article 6a)

Smartphones are set up with biometrics as a system-wide authentication which is used firstly to unlock the phone and secondly to access some applications. Device manufacturers want to implement a convenient system for the most frequent use, i.e. unlocking the phone. Therefore, the excessive requirements for BAL "High" – as described in the former section - strongly reduce the chances of uptake by device manufacturers. Device manufacturers will most likely not want to compromise on user convenience to such an extent. They risk disregarding these requirements ultimately.

Moreover, the level of PAD required by the application module [TR 03107-1] is far beyond what can be achieved today, and as such, no device will meet these requirements. Also, the requirement for security certification under Common Criteria is very demanding. We suggest limiting the requirement for PAD to "Enhanced Basic", which is what can be achieved today.

[1] Best Practice Technical Guidelines for Automated Border Control (ABC) Systems – Frontex (2015) - https://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_ABC.pdf

Otherwise, very few devices, if any existing at all, would be able to support the European Digital Identity Wallet.

Eurosmart's recommendations for Level High

Eurosmart believes that the uptake of the technical guideline, including BAL “High”, will depend on the feasibility of the requirements in a competitive consumer-oriented multi-use device. Eurosmart recommends reconsidering the FAR, PAD as well as entropy requirements.

Today, the FIDO requirements are used by the financial industry, and the system suppliers are related to them; FIDO definitively drives the current market. The PAD requirements are not sufficiently defined to comment in detail, but Eurosmart would suggest using FIDO as a baseline, which is well known in mobiles and finance. Then, BSI should undertake work on complementary tests to reach higher levels as expected for the excellence of the European digital security.

In comparison with the SOG-IS MRA, which aims to provide a level of excellence for the smart cards and similar devices domain, Biometric Assurance Level "High", "Substantial" with application module "[TR 03107-1]" will take time to become effective. Technical work should be initiated between different actors of the biometrics ecosystem: laboratories, national agencies, vendors and schemes. The necessary supporting documents should be defined to support these requirement levels (i.e. the attack catalogue, the attack methods, and the quotation of attacks).

Such supporting documents are already contemplated by the BSI document, and a mode of management is proposed ("BSI will provide a pre-defined list of artefact species, which SHALL be tested during the PAD evaluation"). Eurosmart believes this list shall be shared with the whole technical community (laboratories, national agencies, vendors, schemes, developers, research). Also, Eurosmart recommends that its preparation, update and maintenance involve all the technical community so that it really reflects the state of the art of presentation attacks. Therefore Eurosmart suggests replicating the organisation already in place for the attack methods for secure hardware, where the JHAS gathers all the technical community and certification authorities to maintain the list of attack methods and define their ratings. Eurosmart, which already gathers a substantial technical community in the field of biometry, would be delighted to host this new structure.

III. Reality check for withdrawal and suspension of biometric instance

Withdrawal of biometric instance: a contradictory provision by essence

The draft technical guideline lays down requirements for the withdrawal of biometric instance (3.2). It states that "[i]f a biometric instance is withdrawn by the enrolled data subject as an authentication factor, it SHALL NOT be possible to enrol the same biometric instance for a second time".

This provision implies that the device must retain the template of the withdrawn biometric instance. It is illogical and inconceivable in consumer devices; it even goes against the objective of the withdrawal as the objective is to destroy the template so that others cannot use it. What is the purpose of this provision? If it targets selling a smartphone, then the factory reset is indicated, and the biometric templates will be erased.

The same section state states that "[t]he user MAY notice a successful attack by the usage of a biometric characteristic, e.g. on a similar device. Therefore, the user SHOULD withdraw the affected biometric reference and MAY add the biometric characteristic to a blacklist, where biometric instances and corresponding references are listed, and they cannot be re-enrolled again." Eurosmart observes

that there is no such thing as a blacklist refusing enrolment for specific biometric instances in commercial devices.

Suspension of biometric instances: which use case?

The draft technical guideline also foresees the possibility to suspend the use of a biometric reference (3.2). The document gives the example of the device owner who wants to share a device with other users and temporarily restricts their authentication to the device, and re-activates the authentication at a later date. Eurosmart wonders whether this example corresponds to any real situation. If the owner hands over the device for more than single instantaneous use, he/she will also have handed over the code to unlock the device.

This suspension provision does not fit commercially available devices.

Conclusion

Eurosmart much welcomes the work done by the BSI for this technical guideline. It is a very important document to guarantee that users and services can securely rely on biometric authentication technologies. However, requirements need to be well sized to be widely adopted by the industry, including device manufacturers. End-users expect devices that provide them with a smooth user experience while satisfying their own requirements for essential security. End-users are not willing to invest in a device for the sole purpose of accessing government services in Europe.

Eurosmart recommends looking at other means of upgrading the security level of applications. This can be achieved through multifactor authentication , including the use of codes to allow leveraging on existing devices.

Moreover, based on a realistic and applicable approach for the current market, higher security levels should be defined for well-identified use cases. These requirement levels require a long term-approach with the support and the involvement of the biometrics ecosystem. Due to their wide acceptance, the current industry's security requirements are a good basis for further developments.

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High-Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.
Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sarapis**, **SGS**, **STMicroelectronics**, **Synopsys**, **Thales**, **Tiempo Secure, TrustCB, Trusted Objects**, **TrustSEC**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom – IMT, ISEN – Institut Supérieur de l'Électronique et du Numérique Toulon**), and associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's expert groups: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at the EU level, such as CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, Global Platform, TCA, ISO, SIA and TCG.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | email Contact@eurosmart.com