SECURITY FOR BIOMETRIC AUTHENTICATION

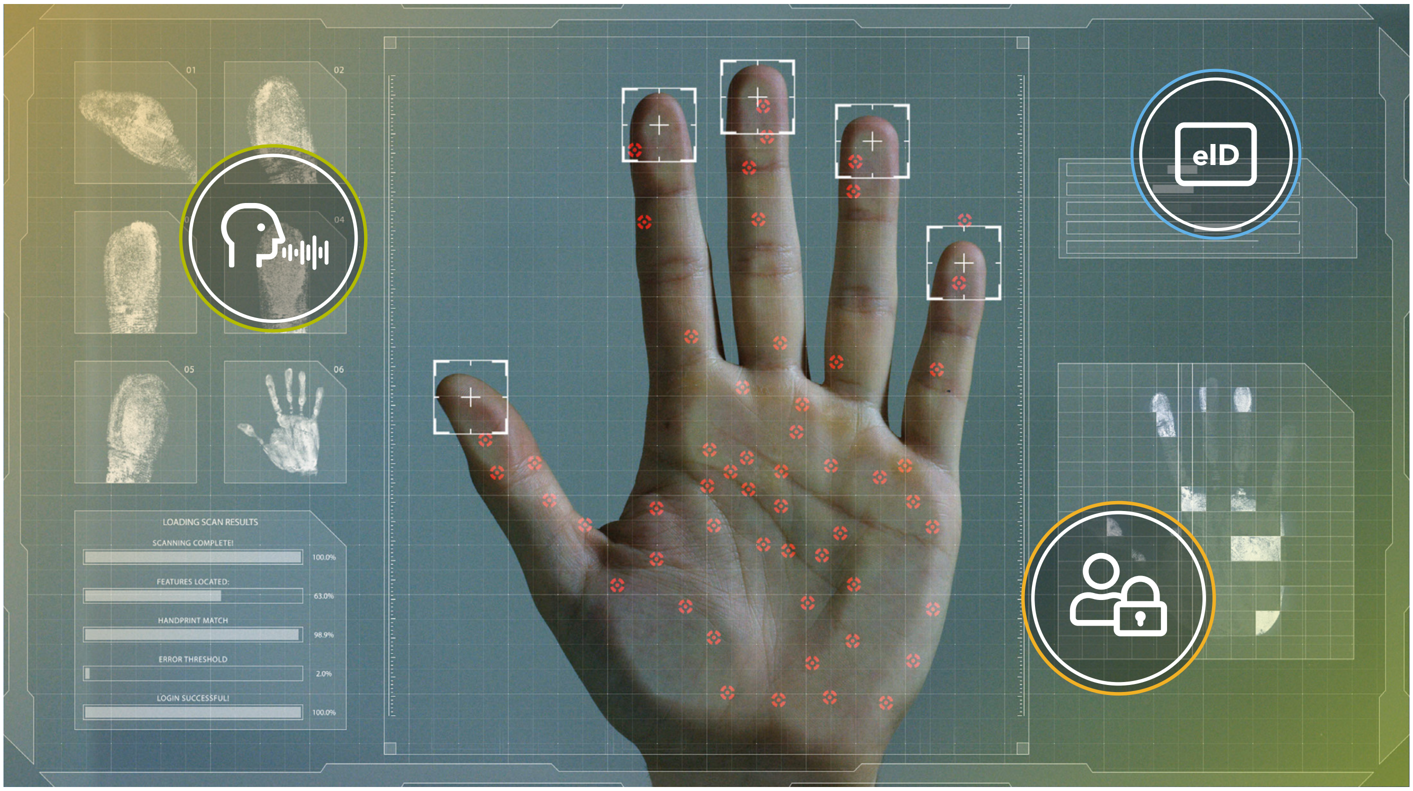
Security issues and solutions related to the use of biometrics for person authentication

www.nxp.com

TABLE OF ACRONYMS/TERMS

Acronym/Term	Explanation
CPU	Central Processing Unit
eNV	Embedded Non-Volatile Memory
FP	Fingerprint
FPoC	Fingerprint On Card
HW	Hardware
I^2C	Inter-Integrated Circuit
IoT	Internet of Things
IP	Intellectual Property
MCU	Microcontroller Unit
MPU	Microprocessing Unit
OS	Operating System
OTP	One-time Programmable
POS	Point-of-Sale
RAM	Random Access Memory
REE	Rich Execution Environment
ROM	Read-only Memory
SE	Secure Element
SoC	System On Chip
SPI	Serial Peripheral Interface
SW	Software
TEE	Trusted Execution Environment
TZ	TrustZone

TABLE OF CONTENTS



1 BIOMETRICS: FROM "WHAT I KNOW" AND "WHAT I HAVE" TO "WHAT I AM"

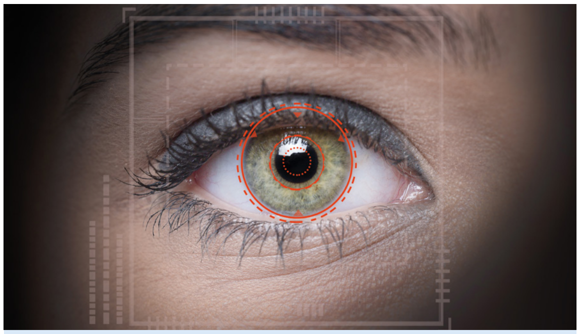
We are surrounded by **interconnected intelligent devices** that assist us with daily tasks, including highly sensitive systems that unlock doors, open bank accounts and access health records. We trust that our personal data will remain secure and private.

Personal access to various devices is often done using one or more authentication factors: "*something you know,*" "*something you have,*" or "*something you are.*" A password or a PIN code are examples of "*something you know.*" A smart card or a hardware key is "*something you have.*" Fingerprints are "*something you are,*" which is commonly known as biometrics.

Biometrics is the use of some unique physical characteristic of a person, including body measurement and body calculations, for identification and access control.

The use of a biometrics to authenticate access and use of digital systems is gaining traction[1]. The key benefits of its adoption is ease of use. Increasingly popular, the convenience of fingerprint- or face recognition-based phone unlocking features are contributing to consumer acceptance of biometric uses.

There are two kinds of biometric authentication: ***biometric identification*** and ***biometric verification***.



Biometric identification

A process where the identity of a person is established among a given, potentially large, population. A good example of this process is the use of biometric identification in a police station where the iris pattern of a suspect is matched against the police database. The key point of biometric identification is that it is a 1 to N match search in a database. The identity is not known a priori and is discovered by matching the biometrics of the person against a set of possible identities.

Biometric verification

A process where the identity of a person is matched against a previous instance of the identity of the same person in a given restricted context. For example, a smart door lock contains enrolled biometrics of the authorized person's face images. When the person prompts the door to unlock, the person's image is matched against enrolled images. The key point of the biometric verification is that it is a 1-to-1 comparison match. The person pretends to have some identity and the system checks on whether it is true.

[1] For example, ABI Research November 2019 report on Biometric Technologies and Applications shows that modalities such as fingerprint recognition, face recognition, iris recognition and vein recognition together with surveillance cameras equipped with face recognition and consumer sensors for fingerprint count for 1.4 billion shipments and it is expected to grow to more than 2 billion shipments by 2024.

Some use cases will combine both biometric verification and biometric identification. For example, e-passports contain the biometric characteristics of the passport owner. The biometric authentication is used to verify the identity of a person locally; it proves that the person presenting the passport is the person that has been enrolled in the secure element of the passport. At the time of entry into a country, a remote biometric identification of the person can be checked against a database of all current criminal investigations or missing people. Another example, important for privacy preserving use cases, is the use of biometric characteristics of a group of people: a person authenticates to a system proving that they are part of the authorized group without revealing which specific person they are out of the registered group members. For example, one can imagine a voting system where the system knows the biometrics characteristics of the persons allowed to vote but not the identity of these voters. When a person votes, the system checks on whether its biometrics is part of the allowed voters but the system cannot correlate the vote to a given individual.

The choice of biometric authentication methods greatly impacts the resource requirements needed to perform the authentication and the privacy-preserving properties of the system.

Many biometric authentication methods are based on a two-step process:

Enrollment phase

The person first registers biometric characteristics into the system. At one of the last steps of the enrollment phase, credentials, called "templates" or "models"[2] are stored.

Authentication phase (or the matching phase)

At a later point in time, a person can authenticate by presenting biometric characteristics to the system again.

During the authentication phase, the credentials are retrieved and used to match against the current biometric readings to determine whether or not the authenticating person matches the enrolled person. Optionally, this includes presenting some indication of the confidence level in the correctness of the matching. Note that choices of where and how the enrollment and the authentication take place is an essential part of the system architecture design. The two steps can occur on different devices and in different geographical locations. For example, with e-passport, the biometrics stored in the template were captured using a biometric reader during the individual's enrollment at a city hall, embassy or other issuing government agency. The biometric authentication occurs at a different biometric reader at another location – in the e-passport, it would be at the border entry gate.

Furthermore, the biometric credentials are provisioned in the e-passport in yet another place: they are inserted in the secure element, which is embedded in the passport in a highly secure environment either during manufacturing at a trusted manufacturer or later in a trusted governmental facility.

Using biometric features to identify a person is not new. Forensic experts rely on biometric data to support police investigations. Their work has shown that some biometric factors are better than others depending on the context of use. In our day to day activities, for example, the ability to distinguish between the members of a family may be good enough for a television remote control but not good enough to unlock a payment transaction or enter another country. Not all biometric features can be used for personal authentication to connected devices – only a handful are good candidates.

[2] The term model is used when machine learning is used for the enrollment and authentication. Sometimes, machine learning is also used to construct the templates. For simplicity and without loss of generality, this paper uses the term template for all types of biometric credentials. Moreover, this choice of terminology does not impact on the architectural choices.

Biometric factors suitable for authentication are chosen based on their qualities, including ease of implementation and handling, hardware and software requirements, speed of authentication, usability and reliability. Furthermore, these following properties of biometric factors should be considered to determine a specific factor that will be used for authentication:

Uniqueness

The factor should uniquely identify a person within the scope of a given set of individuals, members of given population, to identify. A fingerprint is unique to an individual (the chance to find two individuals with the same fingerprint is less than one in millions[3] and as of today no evidence has been found in the already existing records of two different individuals with the same fingerprints), which makes it a good option. A blood-type (A, B, AB, O with positive or negative rhesus factor) would not qualify because it would be applicable to a wider population; for example, 38.67% of the world population has blood group "O+" Moreover, it would be time-consuming and invasive to acquire and process blood quickly.

Ease of acquisition and handling

The biometric authentication should be easy and fast to acquire as well as to compare with previously stored templates. Handwriting- or DNA-based verification would take more time and effort than fingerprint or face recognition.

Robustness

The biometric must withstand environmental conditions. For example, lighting conditions must not impact the image acquisition for facial recognition applications.

Stability

Many biometric factors change during the lifetime of a person. A good biometric factor should be stable and unchanged over a long period of time. However, some systems can regularly update and adjust models for ageing biometric factors.

The ease of use is the most important motivation for the ubiquitous introduction of person authentication by biometrics. People already use it on a daily basis to unlock their smartphones with fingers or faces. The recent improvements in platform performances and security have eased this introduction. For example, NXP has introduced solutions for "Fingerprint on Card,"[4] a system that incorporates biometric authentication directly coupled to the payment authorization on the card itself. In this application, there are no potentially malicious or hacked intermediates between the biometric sensor and the payment chip.

1.1 TYPES OF BIOMETRIC FACTORS

Many different types of biometric factors exist: fingerprint, voice, eye, face, vein patterns, hand geometry and many more (see Figure 1). Each has advantages and disadvantages, as well as desirable or undesirable properties, depending on a specific use-case.

In 2015, we started to see early uses of machine learning algorithms tuned for biometrics, which has also fueled the increased use of some specific biometric factors, including facial recognition. Machine learning can improve the quality of the authentication and reduce the requirements on the platform implementing the biometric authentication.

Today, fingerprint (see [FPoC]), face recognition and iris recognition are the most commonly chosen biometric factors for "***passive biometric***" authentication[5].

[3] Evans, David & Parish, Siobhan. (2015). Predicting the First Recorded Set of Identical Fingerprints. Journal of Interdisciplinary Science Topics.

[4] [FPoC] "What's next for payment cards? An introduction to biometric authentication and Fingerprint on Card technology" (https://nxp.surl.ms/FPOCBlog01 and https://nxp.surl.ms/biometricsinpayment)

Active factors

Some biometric factors require participation, or an action of a person for biometric acquisition. Voice, typing pattern, walking pattern and hand gestures are examples. These are called active factors, because the authenticated person has to do something to enable the measurement of biometric data; a conscious cognitive process is expected from the person. Note that active biometric factors require a person's intent for the authentication: an unconscious or sleeping person can still be identified or authenticated using hand geometry but not using typing patterns.

Passive factors

Contrarily, there are biometric factors that do not require such active participation from the person; the person's body is part of the process. Examples include retina imaging, iris imaging, fingerprints, face and vein patterns. These factors are acquired while the person is passive and the person only has to be there for the acquisition to take place.

Biometric data can be continuously acquired while the person is doing something else e.g., typing a text, browsing the internet (this is a part of some modern CAPTCHAs), walking, using hands to open a door or to press a button. These are behavioral biometrics. When the biometric data is continuously acquired in such way it can present a huge convenience for the person i.e., no need to stop, wait or perform additional actions: the biometrics are available at the point of time the person must be authenticated without additional actions. This convenience, however, comes at the risk of it being equally easy for a malicious person to acquire the same information and use it to perform attacks.

Multi-modal biometrics

Multiple biometric factors can be used together for authentication. For instance, authentication with both voice and fingerprint can be required. Note that the used biometric factors have to be different; two fingerprints from two fingers would not constitute a multi-modal biometrics. Such multimodal systems are usually more secure since it is more difficult to forge two different biometric factors.

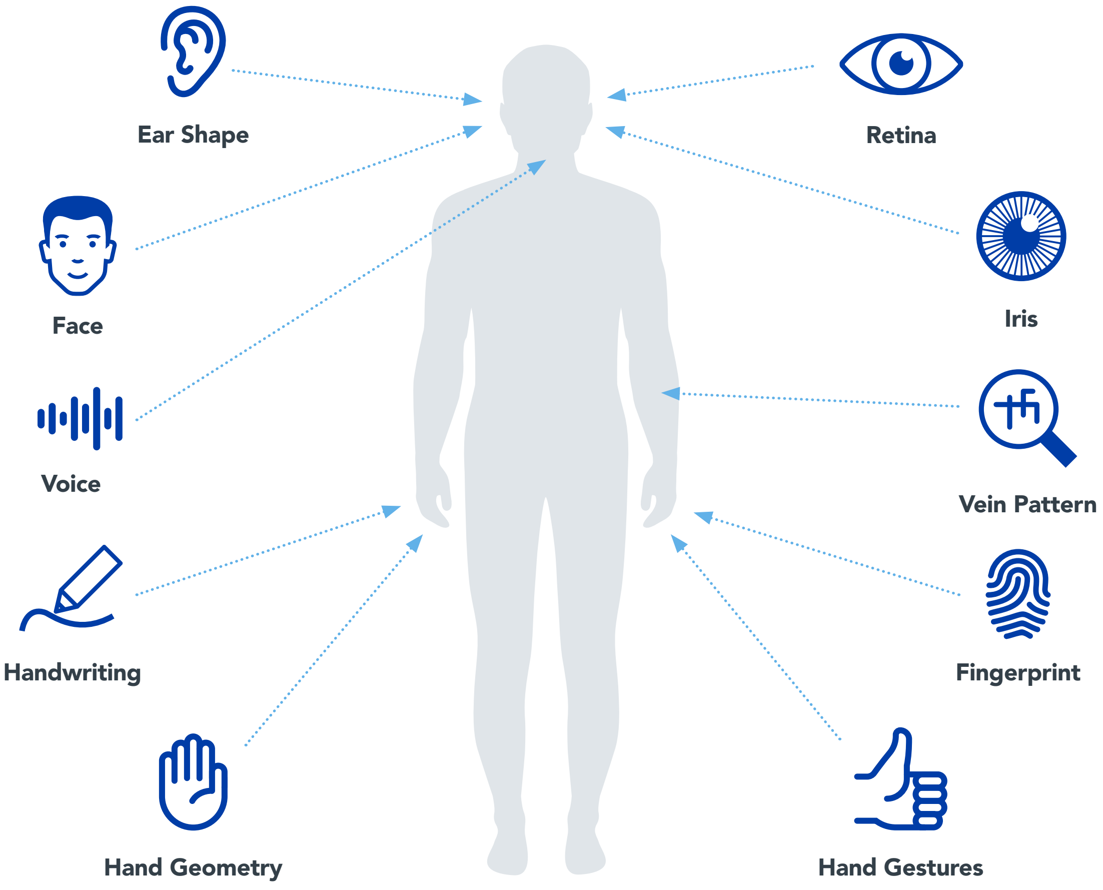
Multi-biometrics

There are several ways of improving the security and robustness of authentication using biometrics:

- **multi-modal** e.g., fingerprint and face,
- **multi-sensor** e.g., capacitive and camera for fingerprint,
- **multi-sample** e.g., both profiles and face picture of person for face recognition,
- **multi-algorithm** e.g., minutiae and texture extraction for fingerprint,
- **multi-instance** e.g., left and right eyes or 2 fingers.

Fingerprint on card is an example of passive biometrics, mono-modal and with one sensor, one finger and several samples of the same finger.

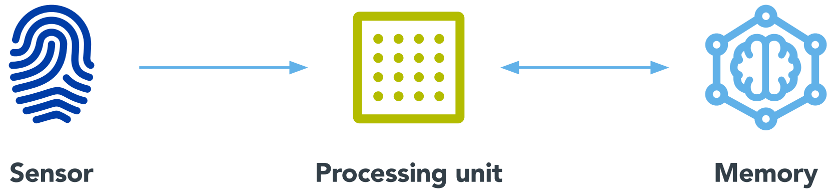
[5] ABI Research Biometrics Quarterly Update of February 2019 shows that in the consumer segment 74% of the shipments are fingerprint sensors, 11% are for face recognition software, 12% are for voice recognition software, 2% are eye/iris modules. The same importance levels are observed in the NIST choices for biometric technologies (https://nxp.surl.ms/NISTbiometrics)



(Figure 1) Examples of biometric factors

1.2 STANDARD ARCHITECTURE

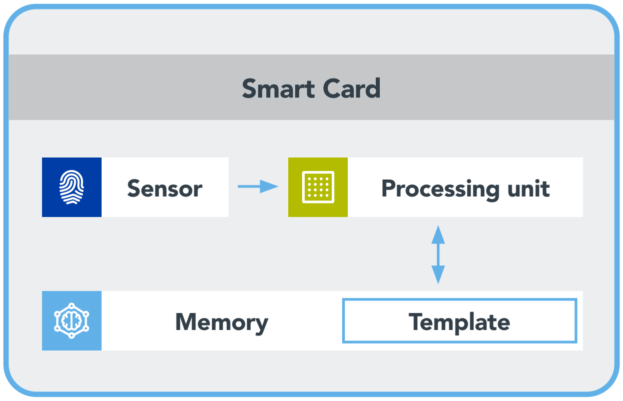
There are many variations of architectures for the hardware design of biometrics-based **authentication systems**. This section presents one of these standard architectures



(Figure 2)
Main components of an authentication system based on biometrics

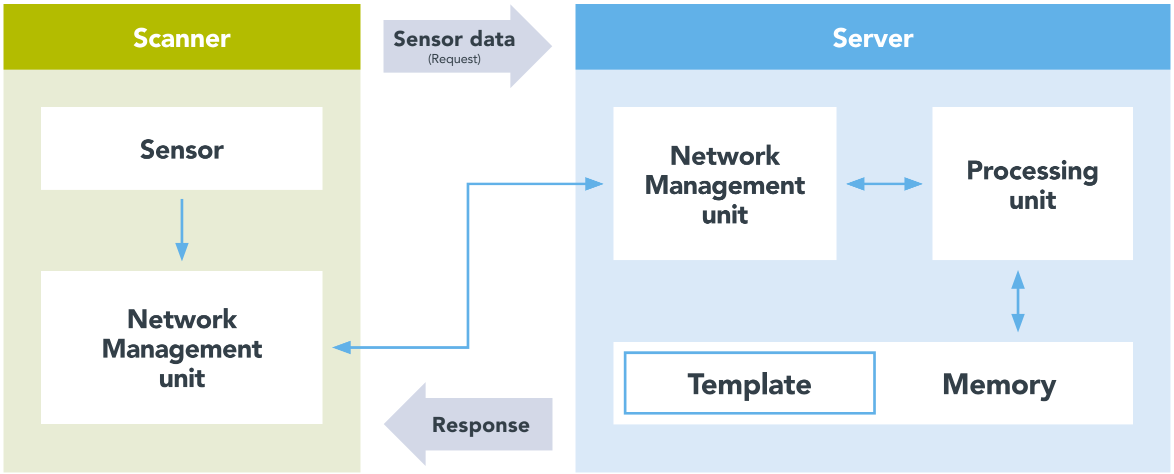
Figure 2 shows the three main parts of a typical biometrics-based authentication system. The system has a sensor which collects the biometric data from the person, a processing unit which extracts specific features from the raw data that was collected by the sensor, and a memory in which the features can be stored. The sensor and the processing unit always execute the same algorithm: the biometric data is collected from the person, its features are extracted and then processed to produce a template.

The third part, however, depends on whether a new person is enrolling in the system or if an existing person is trying to authenticate. During enrollment, a template is built by the processing unit and is stored in memory. During the authentication process, the processing unit builds a template as well, but now compares it against the one which was previously stored in memory.



(Figure 3)
Example of a system where the sensor, the processing unit and the memory with the template are in the same physical device

It is possible that the sensor, the processing unit and the memory are located in the same device, as seen in Figure 3. The system can also be split across several devices or even connected over a network; an example of this is shown in Figure 4. Many different types of applications are possible, and one configuration can be preferred over another one depending on the use case, functional requirements or domain requirements.



(Figure 4)
Example of a configuration where the biometric data is captured on one device and processed and stored on another device

2 FROM SIMPLE BIOMETRICS TO "SECURE & PRIVATE" BIOMETRICS

Similar to core security attributes of connected devices, [6,7] **Confidentiality**, **Integrity** and **Authenticity** are core security features that should be integral part of secure systems. For biometrics, the same principles are to be applied.

2.1 SECURITY

Before going further, keep in mind that there is no such a thing as perfect security; biometrics is not an exception. Real-world devices and their users are part of systems. Making each individual part of a system secure is not sufficient to make the whole system secure.

The security-by-design paradigm must be adhered to while building the complete solution. Among other things, security by design paradigm helps to ensure that the entire system stays secure when several security features are combined. This paradigm must be considered at the initial stage of system design. Credentials, like passwords, keys, etc. are key security assets. Therefore, they should be kept confidential. Thus, credentials should be kept in a secure storage and users should not lose them. These requirements are crucial to avoid severe security incidents.

When biometrics are used for authentication, the approach towards security issues can be completely different from the traditional "something you know" or "something you have" authentication methods such as passwords or hardware security tokens. The reason for that lies in the nature and properties of biometric factors. Biometric authentication factors cannot be lost as easily as for example keys to one's apartment; they are always "with the person" and thus cannot be forgotten like a password. However, at the same time they cannot be kept completely secret; we, most of the time unintentionally, "spread" them all over the place by being on pictures (facial features), touching things (fingerprints)[8] and speaking (voice)[9]. When designing the security architecture of systems based on biometric factors, these new attack avenues must be taken into account.

One of the main steps in an authentication process consists in comparing the credentials presented by the person against the credentials known by the system. The authentication is successful if those credentials "match", e.g., the password entered by the person matches the password of their related credentials or the key matches the lock on the door. In the case of a password or a door key, the presented credential is always the same and the matching procedure always checks for the exact match. The situation is much more complex in case of biometrics mainly due to following three reasons:

(a) Most biometric factors gradually change over the lifetime of a person and some even over a short time span. For example, when looking at facial features, mustaches can be grown or shaved, hair styles can be changed and make up can be applied, —all of these cosmetic changes can result in slightly different appearances.

(b) It is practically impossible to present the biometric factor to the authentication system in the exact same manner on two different occasions; putting a finger on exactly the same spot of a fingerprint scanner, with the same pressure and positioned with the same angle several times is impossible.

(c) Biometric factors may also change temporarily, for example in case of illness or small injuries: voice can change, small cuts or scars on fingers can impact fingerprint features.

For these reasons, the verification procedure for biometric authentication cannot use an exact matching procedure, which would only accept a perfect match when a person presents credentials to the authentication system. In case of biometric authentication, the matching procedure will have to output a probability (sometimes called a confidence level) that the two credentials come from the same person. The system designer will have to put a threshold on the probability which results in a deciding factor on the rejection or acceptance of the person authentication to the system. Another approach is to correlate the result of the biometric matching to some other authentication credentials; another biometric factor, historical data or positioning data. However, none of these approaches can provide pure confidence. This means that there will always be a probability of false rejection (a person cannot authenticate using valid credentials) and a probability of false acceptance (a person will be able to authenticate using invalid credentials). A good biometric authentication system must be designed in such a way that both of these probabilities are as small as possible. The existence of these false acceptance and false rejections rates also introduces a new range of attacks that target the non-exact matching of credentials. These attack avenues against biometric authentication systems should be taken into account when designing an authentication system.

[6] [FITIT] "From the Internet of Things to the Internet of Trust" (https://nxp.surl.ms/FITIT)

[7] [NKIS] "A new kind of IoT Security" (https://nxp.surl.ms/NKIS)

[8] NEVER USE A CHEAP SCREEN-PROTECTOR ON AN EXPENSIVE PHONE – GALAXY S10 USER LEARNS THE HARD WAY (https://nxp.surl.ms/vMl7Bs)

[9] Transfer Learning from Speaker Verification to Multispeaker Text-To-Speech Synthesis (https://nxp.surl.ms/3P3lF2 and https://nxp.surl.ms/hMlYpR)

2.2 PRIVACY

Biometric authentication relies on the **unique personal characteristics** of people. They are part of us; they do not only identify us, but also define who we are. In other words, many of the biometric factors such as DNA, a face or a fingerprint are a part of private, personal information.

Since they are private, people do not necessarily want to unintentionally share them with third parties such as companies and governments. Biometric factors cannot be changed: once they are cloned or copied, there is no way to replace the biometric with a fresh one. The classic urgent request to update a vulnerable password -- “your password has been compromised, change it as soon as possible” -- is not available for biometrics. One exception is the use of cancelable biometrics, which can be used in specific applications.

Cancelable biometrics were derived as a result of undesirable features of biometric authentication. The idea behind cancelable biometrics is simple: once a biometric feature is captured, a special transformation is applied to it. This transformation distorts biometric data in such way that it is still useable for authentication, but the original biometric data cannot be extracted from the distorted version.

This transformation is always the same for the same application (while they should vary for different applications) and it always distorts the input in the same way. All processing is performed on this transformed biometric data as if it was the original biometric information. In this way the back-end handling procedures, such as feature extraction, storage and comparison of the biometric factors, do not have to be modified. As a result, when cancelable biometrics are used, we obtain additional security properties such as:

Better privacy protection

Since the database of biometric features contain only transformed versions, the organization that keeps the database has access to less private information about each person who is enrolled in its system;

Absence of transferability

If the applied transformation is organization-dependent, it offers better security through absence of transferability. Biometric data from one organization cannot be reused to authenticate a person in a different organization. In case the biometric data from one organization is stolen, this same data would not be useable in a different organization even if the same biometric factors are used in both;

Better security through renewability

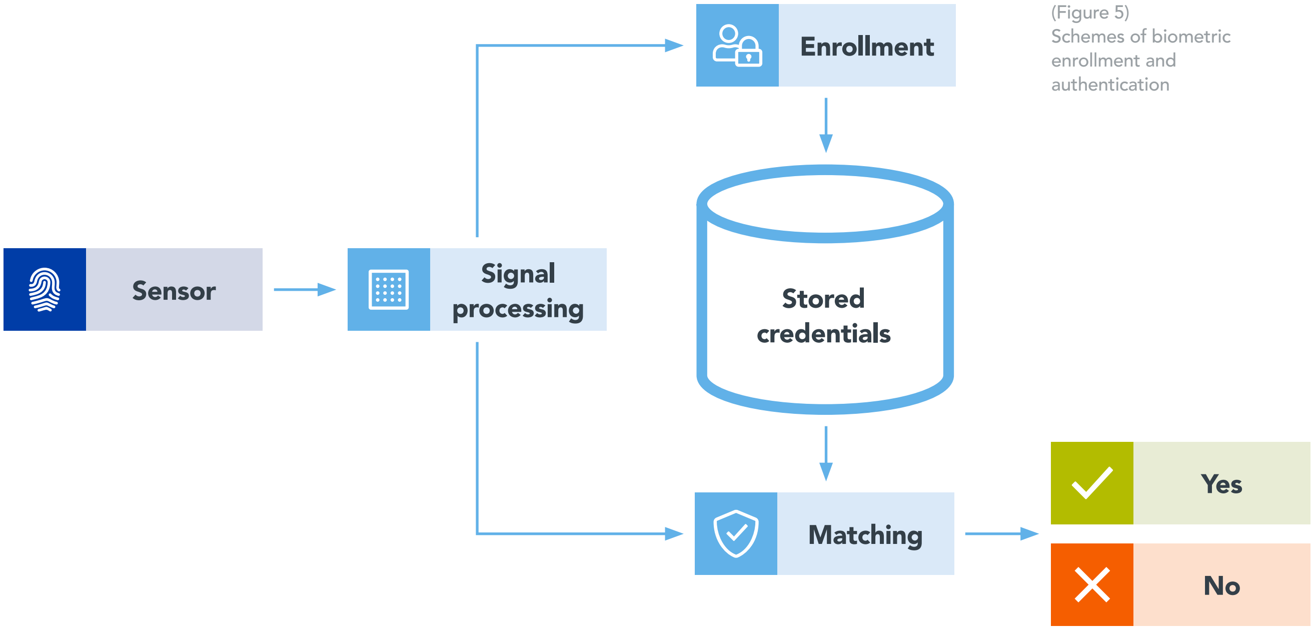
If a database containing biometric information of persons is compromised, it is possible to renew biometric credentials of all people by choosing a different transformation function and replacing the existing one by the new one. In this case, users might have to go through an enrollment procedure again.

Note, that the additional security properties mentioned previously do not make cancelable biometrics a perfectly secure "bulletproof" solution. Stealing the raw data is still possible. For example, a person may be lured in using a compromised device and give away the data before transformation. The system architecture should cover such residual risks.

For private information handling it is important to know *what* kind of private information is stored, but also *where* exactly it is stored. Templates for biometric authentication can be either stored in a database on a cloud or they can be stored locally in smartphones or smartcards. Note, in this second case, private data does not have to be transferred to third parties, which results in better privacy. It has the drawback, however, that personal devices or tokens require higher standards in terms of both secure storage and computational power since the comparison of the template against a new record is usually done on the device. This requirement is met by NXP for applications like payment cards with biometric fingerprint sensors. To help to ensure privacy, the payment card is equipped with a secure element. The storage of the biometric template, as well as the biometric matching process, the related result determination, and the application of the authentication result to unlock a sensitive function are all performed in the tamper-resistant secure element (see [FPoC]).

2.3 SECURITY ANALYSIS

This section describes the **risk and threat** analysis of typical architectures for biometric solutions.

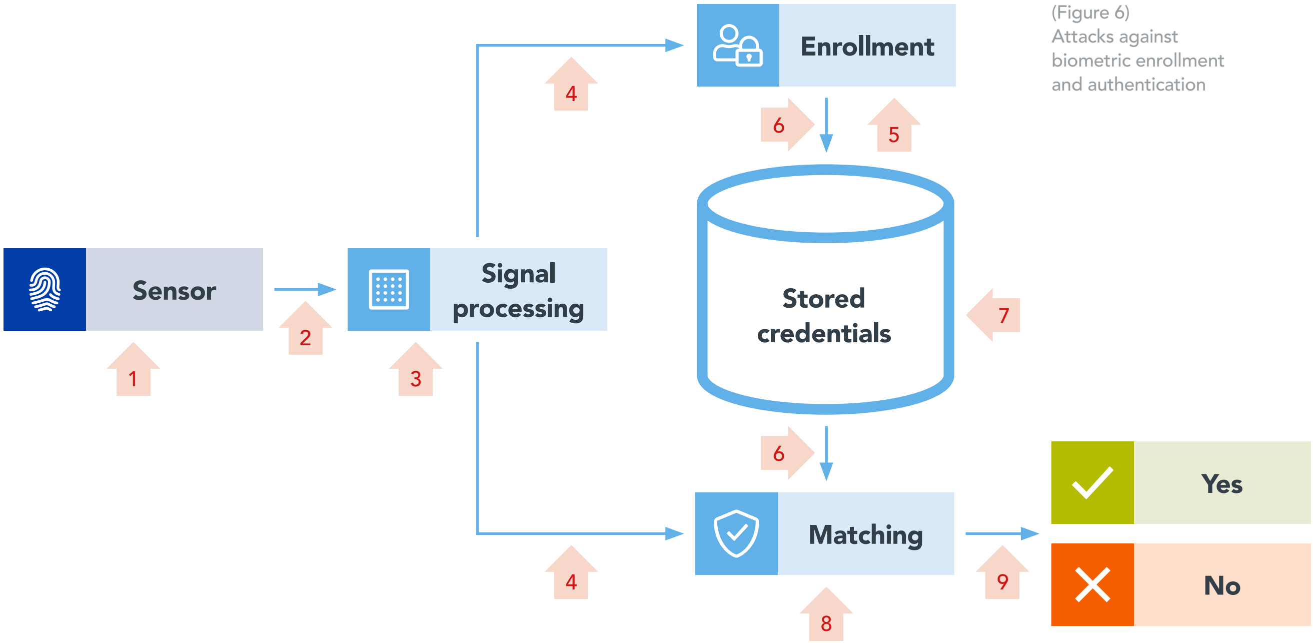


(Figure 5)
Schemes of biometric enrollment and authentication

Figure 5 shows the basic blocks of a biometric enrollment and authentication. During enrollment, the person presents the biometric characteristics to the sensor. The sensor signal is processed. The processed signal is handled by the enrollment algorithm that produces the biometric credentials in the template, which is stored for further use during the biometric authentication. During biometric authentication, the person presents the biometric characteristics to the sensor. The processed signal is now submitted to the biometric matching algorithm that builds a template out of the processed signal to compare with the stored biometric credentials and decides whether or not they match. In most cases, the enrollment algorithm and the matching algorithm share the algorithm to build the template of the processed signal.

The enrollment and the matching algorithms are different because during enrollment, the person is usually but not necessarily required to submit several samples of the biometric characteristics until the system is able to construct a valuable template. The matching authentication algorithm will usually but not necessarily use one sampling of the biometric characteristics. It is also important to note that different components in the system may be manufactured by different companies: some companies specialize in biometric sensors or algorithms and others may specialize in microcontrollers or secure elements.

Since the process is divided into blocks, it opens more attack possibilities.
Figure 6 shows the various points of interest for attackers on the example of the system of Figure 5.



(Figure 6)
Attacks against
biometric enrollment
and authentication

These points of interest make multiple types of attacks possible. An attacker could:

1. Spoof the biometric data of someone else. Examples of this could be the use of special lenses to fake an iris picture or use a picture of a face. The analog biometric data can also be stolen with a second malevolent sensor at the same location (e.g., glued on top of each other) doing the same acquisition but connected to the system of the attacker[10].
2. Spoof the signal between the sensor and the signal processing unit. For example, another analog/digital signal could be replayed. The digital signal could be sniffed from the sensor and replayed later during an attack against biometric matching.
3. Modify the signal processing to alter one or both of the subsequent enrollment and matching. The attacker can also alter the signal processing to leak the information about the biometric data.
4. Fake the digital signal processing outcome with another precomputed signal to enroll another person, or one can sniff the digital signal processing for later reuse during a biometric matching.
5. Alter the enrollment processing to either build another template or to leak the constructed template.
6. Alter the storage of the templates in the database or one can spy on the retrievals from to the database.
7. Alter the content of the templates database or one can steal its content.

[10] See “Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems” by Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin and Kevin Fu (2019; https://lightcommands.com/) for an example of such an attack conducted remotely.

8. Alter the matching processing to arrive at a different outcome or alter the matching to steal a template
9. Alter the result of the matching processing by modifying the decision value yes/no or the confidence weight attached to the outcome of the biometric matching.

The assets to be protected from attacks against confidentiality, authenticity and integrity are:

- **Sensors**
- **Connections between the various processing units**
- **Collected templates**
- **Signal processing unit**
- **Enrollment processing unit**
- **Matching processing unit**

Furthermore, the hardware and software implementations of all these aspects can be subject to intellectual property (IP) protection. Companies making biometric sensors, processing units, algorithms and software consider this IP to be valuable assets and these companies want to protect it against copying, cloning and reverse engineering. For biometrics that use machine learning, the IP considerations are even more extensive as there are attack avenues that only require API access, see more in the NXP whitepaper “Intellectual Property Aspects of Machine Learning”[11].

Mitigating the listed attacks and protecting the sensitive assets requires a system security-by-design approach. This requires the application of many different security features. The choices made for the system architecture must depend on the outcome of a risk assessment derived from a risk and threat analysis.

The two key security features that will block most of the attack vectors listed in Figure 6 are isolation and integrity. The idea behind isolation is to separate the normal applications and simple user programs from the secure applications that handle sensitive data. Isolation can be performed in either hardware or software. In hardware, some approaches that can be taken are the use of:

[11] “Intellectual Property Aspects of Machine Learning” (https://nxp.surl.ms/IPAML)

Multi-processing units

By situating the biometric processing outside of the main application, on separate controllers, for instance, attached to the biometric sensor, with its own private memories, the biometric processing can physically be isolated from the other processing functions of the device.

Multi-core

By dedicating one core of a multi-core processing unit to the biometry is a way to isolate it from malevolent software that would run on the other cores

Connecting the sensors

Connecting the sensors to privileged secure interfaces prevents many sniffing and spoofing attacks: the interfaces are not accessible from the standard processing environment; only the privileged execution environments have access to these interfaces and thus, sensors.

Secure elements

This is the solution that offers a higher degree of security. If the biometric processing can be moved in part or even fully to a secure element, most of the listed attacks can be blocked. A secure element offers secure storage for the credentials and secure processing for the enrollment and authentication. If the sensitive application that requires the authentication is co-located in the secure element (like a payment application for example), the decision of the biometric matching can even be delivered with integrity to the sensitive application. Moreover, modern secure elements have dedicated hardware interfaces where the biometric sensor can be directly connected. However, for some biometrics including facial recognition, pushing the full biometric processing to secure element is challenging: secure elements have limited storage capabilities, limited processing power and limited interface bandwidth to the sensors.

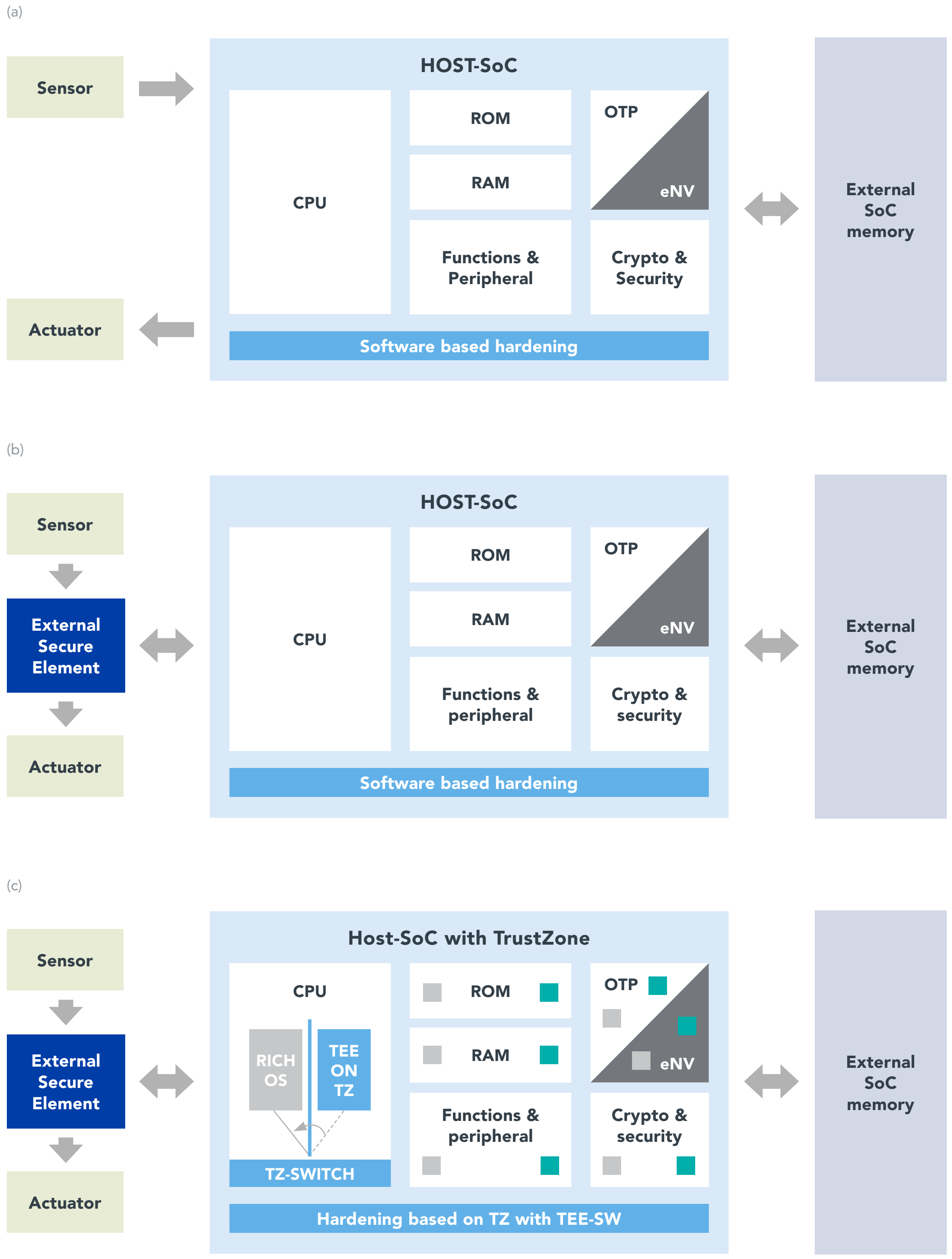
Although weaker than hardware isolation, techniques like virtualization can isolate the software in charge of the biometric from the other software components that are more susceptible to attacks. Sometimes software isolation can be supported by hardware isolation features.

No matter how the isolation is performed, integrity of all the components of the biometric solution is fundamental. Platform security features like secure boot, secure software updates, software integrity, runtime integrity, secure storage and secure interfaces are all desirable.

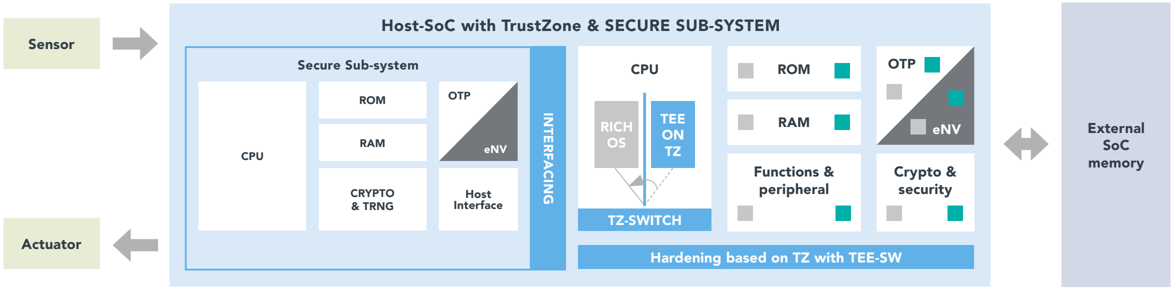
The whitepaper "From the Internet of Things to the Internet of Trust"[12] promotes different IoT architectures (see Figure 7) that can be used as a starting point to fulfill the security requirements described above.

[12] [FITIT] "From the Internet of Things to the Internet of Trust" (https://nxp.surl.ms/FITIT)

(Figure 7) IoT Architectures



(d)



These architectures and security features can help mitigate the attacks 3 to 9 depicted in Figure 6. Analog spoofing (attacks 1 and 2 in Figure 6) of the biometric characteristics is beyond the scope of the solutions described here. It must be addressed by the overall system. For instance, multi-factor authentication makes it unlikely to spoof more than one input of analog biometric characteristics.

2.4 NEW ARCHITECTURES

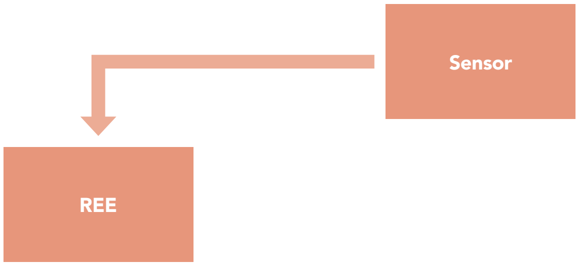
Several hardware architectures can be used to build secure biometric authentication. The purpose of those architectures is to leverage the **security properties** of the secure element to the security properties of the biometrics system solution.

The ultimate goal, as in [FPoC], is to have the critical enrollment and matching processing depending on the secure element, to have the critical biometric assets protected by the secure storage of the secure element and the relationship between the final biometric decision connected to the resulting action being processed in the secure element. When the final decision is related to a physical action on the real world, it is preferable to have the corresponding actuator being directly connected to the secure element and actioned by the secure element without intervention of the Rich Execution Environment (REE).

(Figure 8) New architectures

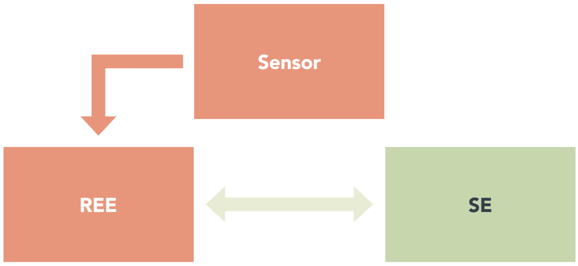
Beware that Figure 8 and Figure 10 label some parts as "Not Secure" but this does not imply that the combination is not secure. It means that the security of the system does not depend on specific security assumptions on the parts labelled "Not Secure".

🟥 **Not secure** 🟩 **Secure** ⬜ **Secure by isolation**



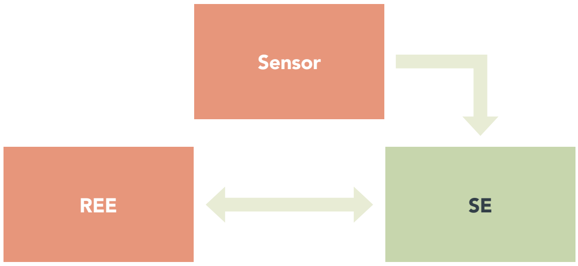
1.

This is the base architecture. The biometrics sensor is connected to the host processor Rich Execution Environment (REE). All the processing (enrollment and authentication) is performed by the REE.
All the data is stored in the REE as well. It can be subject to the attacks of Figure 6.



2.

This architecture adds an embedded secure element (SE). The REE performs all the biometric processing (enrollment and authentication), but it uses the SE as a secure vault to store the templates (protection against attack 7 of Figure 6) and sometimes perform the last step of the biometric processing: the template matching (protection against attacks 8 and 9 of Figure 6). This is useful in architecture {b} and {c} of Figure 7 where the actuators executing the consequence of the matching decision are connected directly to the secure element.

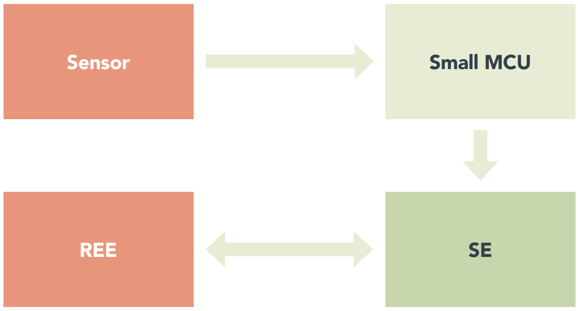


3.

In this architecture, the sensor is connected to the SE instead of the REE. Either the SE must have enough resources to perform the enrollment and/or authentication or the SE must have enough bandwidth to transfer the signal from the sensor to the REE for the enrollment and/or authentication that will be processed by the REE. The SE on the path to the REE improves the system security:

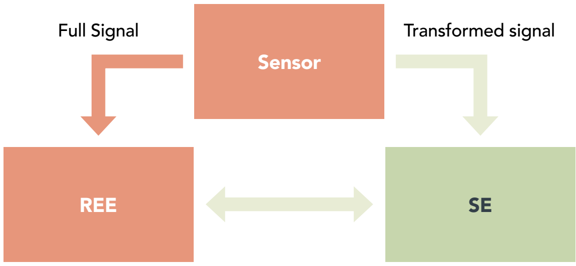
- SE can check whether the REE answer matches its own knowledge of the data sent to the REE originating from the sensor
- SE can alter the data sent to the REE by for example watermarking the data and checking that the signal sent back by the REE to the SE still contains the watermark.

This architecture can help blocking attacks 3 to 9 of Figure 6 if the secure element has enough resources.



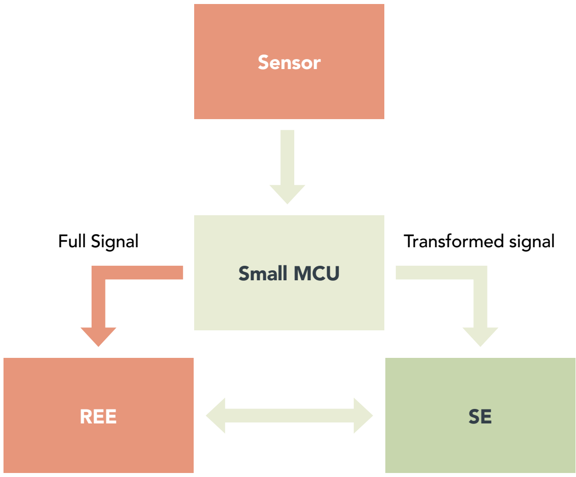
4.

In this architecture, the functionality of adapting a sensor to an SE is performed by a low-end CPU. For example, the small CPU can adapt the hardware interface of a given sensor to the I^{2}C hardware interface of the SE. This architecture requires less resources from the secure element and offers the same level of protection as previous architecture **3**.



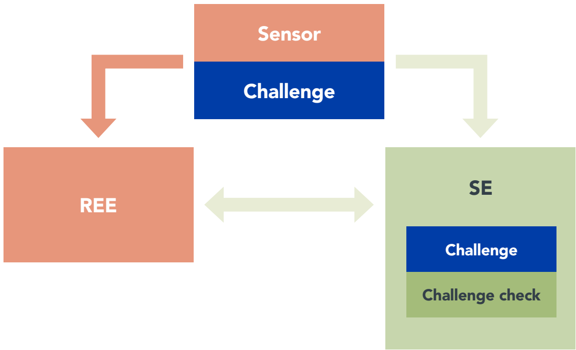
5.

In this architecture, the sensor is connected to both the SE and the REE. This means that the SE has a complete or partial knowledge of the signal sent to the REE and it could determine whether the information it receives from the REE after processing matches its own information. This architecture helps mitigating attacks 3 to 9 of Figure 6.



6.

When the sensor is not capable of performing the dual porting required for the signal splitting for architecture **5**, this architecture can be used. An intermediate low-end MCU performs those tasks. This architecture is an optimization of previous architecture **5**: any sensor can be used and the “Small MCU” performs the adaptation.

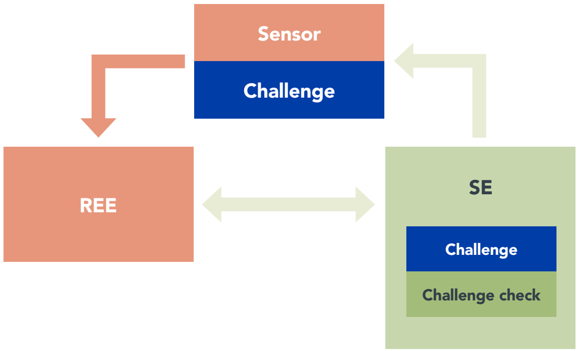


7.

In this architecture, the sensor is capable of adding a challenge to the data sent to the REE and communicates the challenge it has used to the SE.

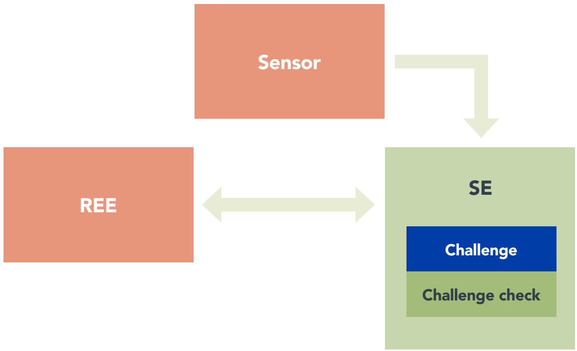
After processing of the data by the REE, the SE can check whether the processed data received from the REE matches the expectations associated with the challenge added by the sensor.

In this architecture, the challenge is generated by the sensor. This architecture brings more protection against replay attacks. It can also be subject to an optimization by the introduction of a “Small MCU” interposed between the sensor and the REE and SE.



8.

In this architecture, the same construction is used, but the challenge is generated by the SE, communicated to the sensor, used by the sensor to alter the signal, which is sent to the REE. The SE then checks whether the processed signal sent by the REE matches the challenge it has sent to the sensor. This improves on previous architecture **7** because the challenge is generated by a truly random number generator present in the secure element.



9.

Lastly, in this architecture, the SE receives the raw signal from the sensor, inserts the challenge in the signal before sending it to the REE, and checks the signal it receives back from the REE for compliance with the challenge the SE had added to the signal.

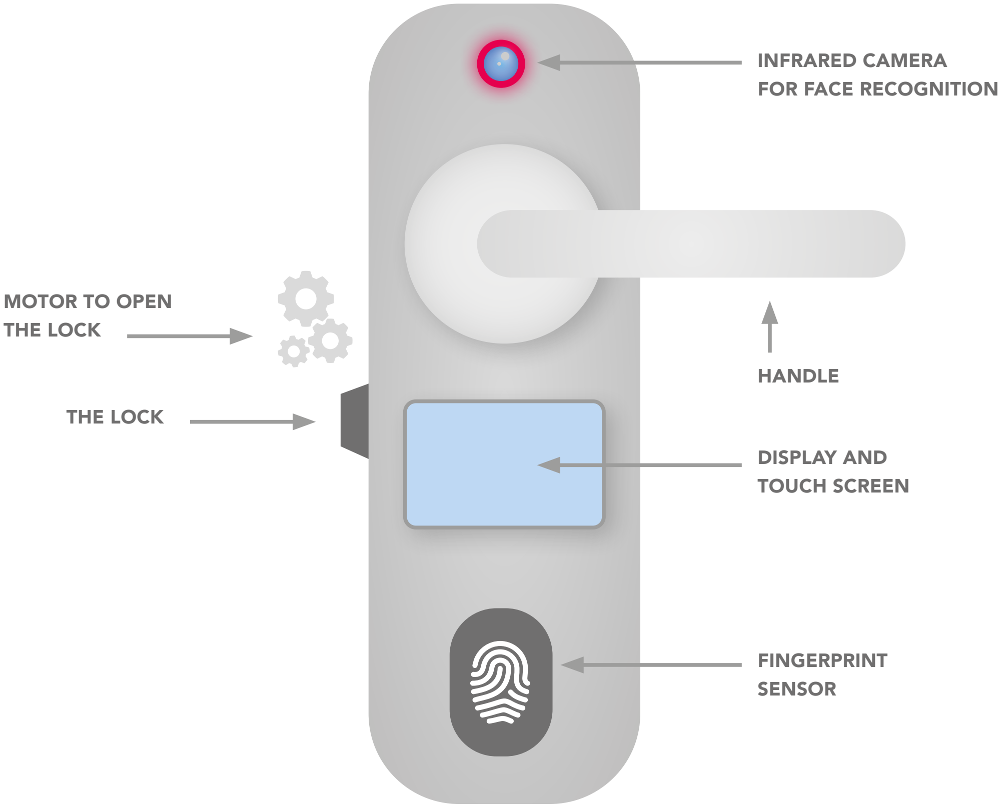
Note that architectures **7**, **8** and **9** of Figure 8 can support the cancellable biometrics referred to in § 2.2.

The use of a secure element improves the security of biometric processing and it enhances the security of the solution by improving the platform integrity. When the sensor is connected directly to the SE, it also protects the other sensors and actuators of the device from malware running on the REE (as show in architecture {b} and {c} of Figure 7). Architectures **3**, **4**, **5**, **6**, **7**, **8** and **9** of Figure 8 may be more demanding on the capabilities of the secure element with respect to signal processing, bandwidth, speed of processing.

Depending on the storage capabilities of the SE, the templates can either be stored in the SE itself or outside of the SE, and encrypted using a key that is stored in the SE and that never leaves the SE (i.e., the SE performs the encryption and decryption of the external storage when required).

Example: Smart Lock

Given the smart lock, artistically depicted in Figure 9, one can design a secure biometric system as depicted in Figure 10. This is an example of a dual biometric factor authentication: fingerprint recognition and face recognition. It is an instance of architecture **6** for the face recognition and of architecture **4** for the fingerprint recognition.



(Figure 9) Smart Lock

Prior to first use, the person entitled to unlock the door will have to enroll for both **face recognition** and **fingerprint recognition**. The credentials constructed based on this enrollment are stored in the secure element SE.

When a person wants to unlock the door, the infrared camera sensor takes the picture of the person in front of the lock in both the visible light and the infrared domains and sends it ① to a small MCU that will send the entire signal to the REE ② and that will compute a "summary" of the picture. The Small MCU sends the "summary" to the secure element ④. The REE retrieves the face recognition credentials from the SE ⑤, performs the face recognition biometric matching and submits the result to the SE .

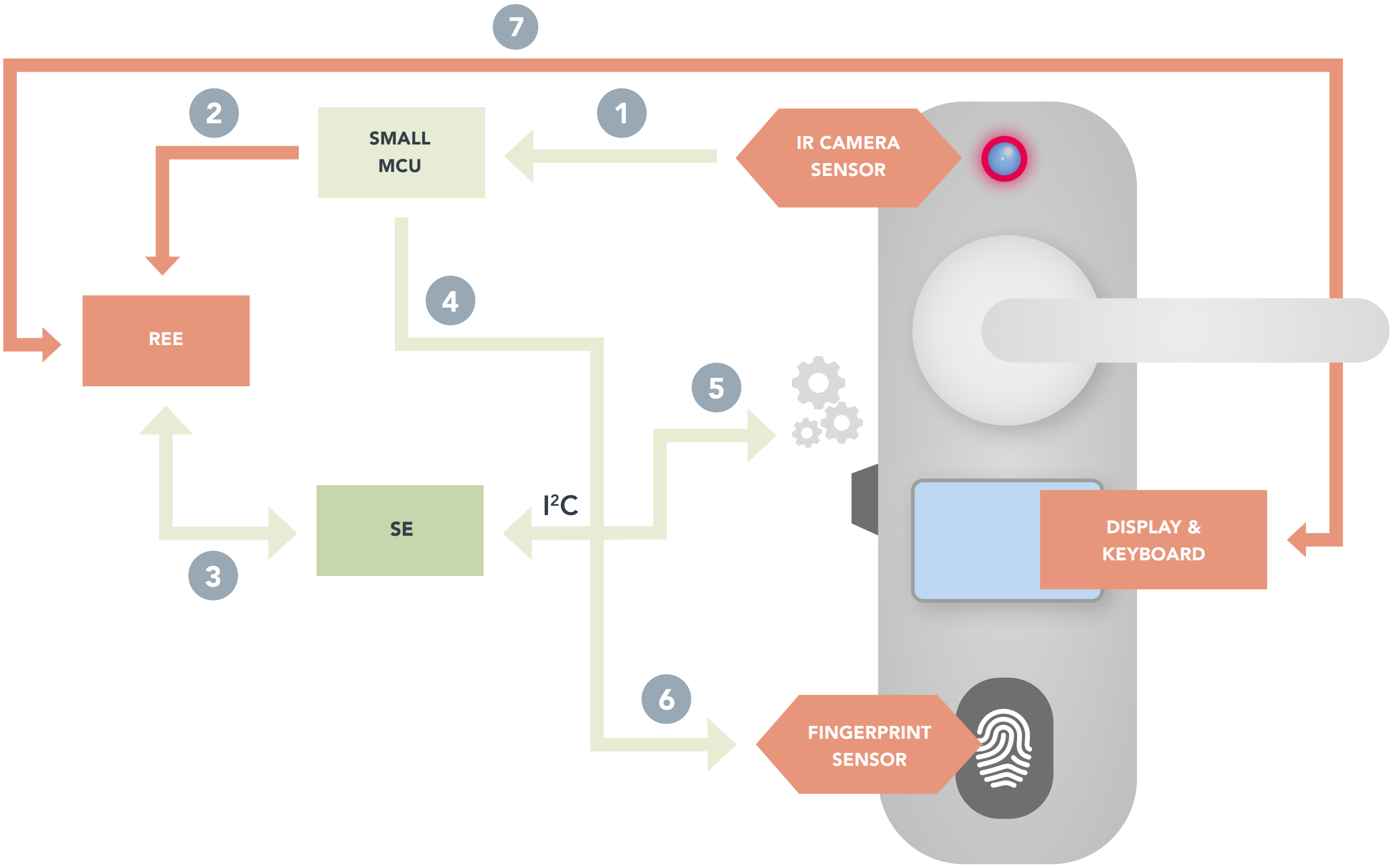
The secure element combines the outcome of the face recognition received from the REE with it knowledge of the "summary" picture to draw a first internal conclusion on the verification of the identity of the person. In parallel, the person puts a finger on the fingerprint sensor, the fingerprint sensor data are sent to the small MCU ⑥, ④, the processed fingerprint data are sent to the SE ④.

The SE performs the fingerprint biometric matching on the fingerprint data and draws a second internal conclusion on the identity of the person. The SE combines the two conclusions to form a final decision on whether or not it authorizes the unlocking of the door. In case of a positive decision, the SE sends the command to the door lock actuator ⑤. During the verification procedure, the LCD display of the Smart Lock, can be used to give instructions to the person ⑦ and the touch keypad can be used to get additional data from the user ⑦.

(Figure 10) Smart Lock secure biometrics architecture

Beware that Figure 8 and Figure 10 label some parts as "Not Secure" but this does not imply that the combination is not secure.
It means that the security of the system does not depend on specific security assumptions on the parts labelled "Not Secure".

🟥 **Not secure** 🟩 **Secure** ⬜ **Secure by isolation**



3 NXP SOLUTIONS

A broad range of NXP products are available to implement both the traditional and the new biometric architectures. They can contribute to the realization of the architectures of § 2.4.

NXP low-end LPC processors can be connected to the secure element, the powerful host processor and to the sensor as shown in architecture **7** of Figure 8. It has the advantage that this solution can be adapted to several kinds of sensors. NXP LPC MCUs have enough processing power to support the implementation of the transformation necessary for various cancellable biometrics methods.

The Rich Execution Environment (REE) host processor can be implemented using any of the NXP LPC, Kinetis®, i.MX RT crossover, or i.MX 8M processors. Many of these processors are equipped with either TrustZone-A, TrustZone-M, multicores or secure subsystems. They provide many ways to partition the biometric processing between the various processing units and the implementation can benefit from the various hardware isolation capabilities.

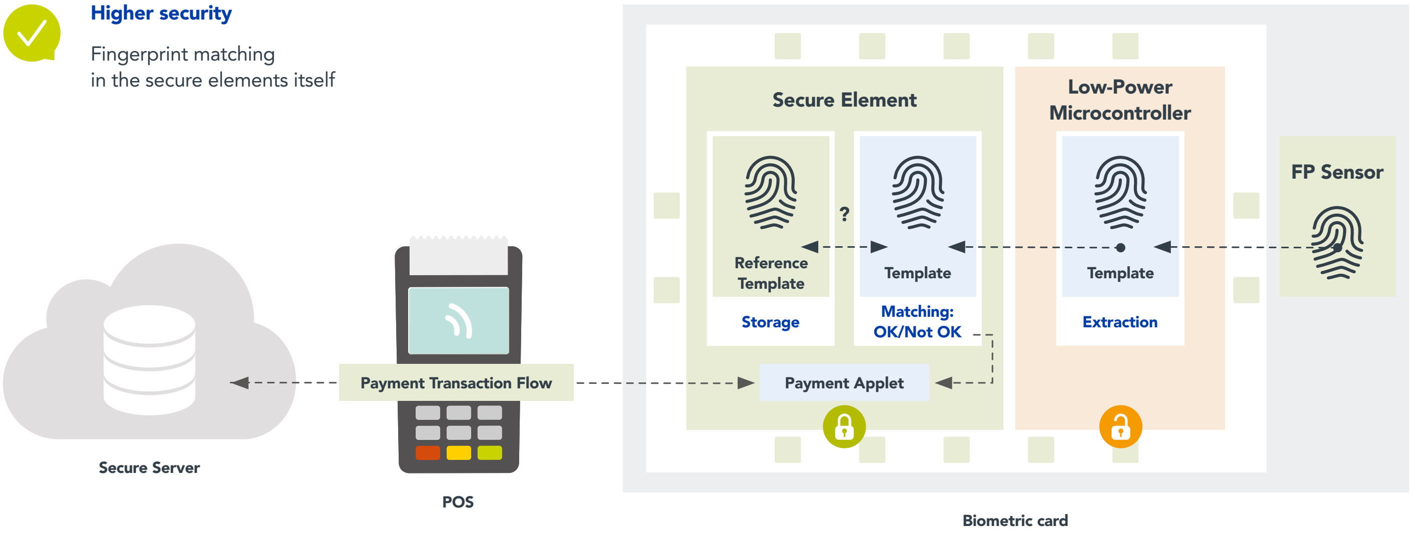
NXP products also support system solutions to address modern privacy issues in two ways: either by offering enough resources to perform the biometric enrollment and biometric authentication locally in a secure and efficient way, or by offering edge computing capabilities to keep some locality for the biometric templates, e.g., by storing the templates for a group of people in an edge node helped by an EdgeLock™ Secure Element for secure storage. With edge computing, the edge node is performing the enrollment and the authentication, as well as acting as the repository of the biometric credentials. Note that placing the enrollment and the authentication in the edge nodes also helps in cases where the IoT devices connected to the edge do not have the resources to perform the enrollment and/or the authentication.

For the Fingerprint on Card use case, NXP has a complete solution (see Figure 11 and [FPoC]). This product combination can be extended to other biometric verification use cases: the signal acquisition, the biometric enrollment, the storage of the biometric credentials, the authentication and the security sensitive application unlocked by biometrics, are all implemented in a secure environment. This applies, for example, to semi-online, semi-offline use cases such as door locks.

Using the secure element to perform fingerprint matching guarantees higher security

Higher security

Fingerprint matching
in the secure elements itself



(Figure 11) FPoC architecture

The rich palette of NXP products gives customers the possibility to extend the emerging IoT and industrial specific smart products (see [FITIT] and [NKIS]) with biometric technology.

4 CONCLUSION

The use of biometrics as an authentication method is becoming ubiquitous. Biometric authentication capabilities can unlock features, grant physical access, authorize payments and give access to data. Moreover, it enhances the user experience. Biometrics come with advantages and features, but also specific security and privacy issues. Therefore its functionality and use must be part of a system design where hardware and software isolation are used judiciously.

However, use of hardware and software isolation is not enough to make the system secure. Data and entities accessed through or protected by the biometric authentication must also to be part of the security and privacy system design. Among other considerations, one of the main ideas that must be kept in mind during the design of a secure biometric authentication is the following: the biometric match decision must reach the protected functionality without being exposed to malicious clones or alterations.

System designs may include solutions with microcontrollers or processors connected to biometric sensors. NXP has a range of EdgeVerse™[13] MCUs and MPUs that are part of the EdgeLock Assurance program, which can be used to implement the biometric functionalities securely, including the biometric authentication. These solutions can be augmented with NXP EdgeLock[14] Secure Element to offer a higher degree of security and confidentiality. NXP EdgeLock Secure Element products offer a hardware tamper resistant vault and secure computation platform for the final biometric matching decision. These products also have mechanisms for the secure association of this decision to the application needing the authentication.

The EdgeLock Secure Element products differentiate from the standard secure elements by their I^{2}C interface that opens the door to new architectures. For example, it allows the biometric sensors to be directly connected to the secure element which can help block many attack avenues. In addition, the very same I^{2}C interface enables architectures where the actuators for IoT or industrial devices are directly connected to the secure element. Ultimately it means that the biometric matching and the action performed by the device can then be taken in a secure tamper resistant execution environment.

Biometric authentication should not be used in complete isolation. An authentication system must foresee multiple alternative authentication mechanisms in case one of the biometric characteristics would not be available or not measurable. Multiple authentication mechanisms that include biometric authentication in the process also improve the confidence associated with the authentication. The system security by design should harmoniously encompass various authentication mechanisms to enhance the user experience, and privacy as well as the security of the entire system.

[13] EdgeVerse™: https://nxp.surl.ms/EdgeVerse

[14] EdgeLock™: https://nxp.surl.ms/EdgeLock