State-of-the-Art in Biometrics for Multi-Factor Authentication in a Federative Context

Martijn Oostdijk[1], Arnout van Velzen[1],
Joost van Dijk[2], Arnout Terpstra[2]

1. InnoValor, P.O. Box 3536, 7500DM, Enschede, The Netherlands
{martijn.oostdijk, arnout.vanvelzen}@innovalor.nl
2. SURFnet, P.O. Box 19035, 3511EP, Utrecht, The Netherlands
{joost.vandijk, arnout.terpstra}@surfnet.nl

Keywords: biometric authentication, multi-factor authentication, identity federation

Abstract: Despite having been a promising technology for authentication for quite a long time, biometric authentication has not seen large scale adoption in federations for higher education and research. Lately, however, in the consumer domain there appears to be increased interest in stronger forms of authentication (e.g., one-time-password apps for smartphones) and biometric applications (e.g., embedded finger print readers in smartphones). It may be the right time for the higher education and research community to evaluate the current state-of-the-art in biometric authentication. This paper investigates the state-of-the-art in biometric technology (anno 2016), establishes a set of evaluation criteria and compares the different biometric modes according to these criteria.

1. Introduction

Biometrics is often mentioned as a promising option to create more secure authentication methods. In practice however, the expectations of biometrics to replace passwords are often inflated: passwords have been declared dead many times. The advantages of biometrics, or “something-you-are”, are clear when compared to traditional “something-you-know” and “something-you-have” authentication factors. For example, users are always in possession of a biometric authentication token. At the same time, the technology also faced some challenges in the past. One of these challenges was the costs associated with introducing the technology to a mass audience. With the advent of smartphones and other mass market mobile devices, equipped with sensors suitable for biometric capturing (camera, microphone, fingerprint sensor, heart monitor), this shortcoming appears to have been almost solved for some of the more popular biometric modes. In addition, multi-factor authentication itself has received increased attention lately as witnessed by the emergence of standards such as FIDO.

These recent trends urged the Dutch NREN SURFnet to assess the current state-of-the-art of biometric authentication with a focus on use-cases within an NREN federative context, as a precursor to a proof-of-concept. In a number of innovation projects SURFnet has already explored possibilities to generically add multi-factor authentication to the existing SURFconext federation (see [11]). In the current paper the primary objective is to study the possibility of *biometric* authentication in the context of strong authentication for a federative system such as SURFconext. A secondary objective is to give an overview of the current state-of-the-art in biometric technology, which may be of interest to the general higher education and research community.

The approach consists of desktop research, complemented by a wisdom-of-the-crowd session in which external biometrics experts were invited.

2. Biometrics background

Biometrics refers to measurements of properties of the human body and behavior. These properties are identifying of individuals and are therefore fit for identification. Biometrics may also be used for medical and forensic purposes, but this report focuses on applications within identity management. A distinction is made between the identification of unknown individuals and verification of known individuals from a database. This report looks at the latter application of biometrics. Compared to other forms of authentication ("something you know", "something you have"), biometrics has important advantages. A biometric characteristic is generally more difficult to spoof or copy, most individuals already have suitable characteristics and they carry it always with them.

Identifying biometric characteristics are also referred to as modes and may be hard (high degree of identification) or soft (to a lesser extent identifying), as well as physiologically (measured on the body) or behavioral (measured on behavior). Multimodal biometrics combine measurements of more than one attribute in biometric applications [14] [15].

Identity Verification differs depending on the selected feature, but roughly requires the following steps:

1. **Registration**: confirm the identity of the subject, for example, by checking a passport or asking to log in with a username and password. Biometric authentication is like any credential for authentication, only as secure as the rest of the verification process.

2. **Enrollment**: create a print or record of the biometric feature with the help of sensors, such as a picture with a camera for face recognition. This process produces a template, either a print or record, which is stored in a database. Before storing the template it may be modesfied, such as cleaning up noise or encrypting the data.

3. **Authentication/verification**: when a person is required to authenticate, then a recording or print is taken again with the aid of a sensor and it is compared to the template in the database. When the recording matches that template in the database, the identity is confirmed. In some use cases identification, rather than authentication/verification is used. Identification means that the recorded feature is compared to all templates in the database, and the closest matches are presented. This paper focuses on authentication only. Sometimes it is necessary to test whether the presented feature is not simulated, for example by liveness detection.

There are important privacy issues to consider when processing biometrics. For example, the storage of a high-resolution eye scan of someone with an eye disease is an example of processing sensitive data that may be subject to privacy legislation.

The performance of a biometric technology can be expressed in quantitative scores. For the enrollment phase one often looks to the Failure to Enroll (FTE) measure, which measures the proportion of a population that could not be successfully enrolled. In the authentication phase, important scoring measures are the False Acceptance Rate (FAR) and False Rejection Rate (FRR): the risks of undue access or unjustified refusal of access. Often, the technology can be configured to balance the FAR and FRR. For example, the FAR can be fixed on the basis of the acceptable risk of incorrect authorization, but may be adjusted so that the corresponding FRR is acceptable from ease of use.

Some biometric technologies are assessed on such quantitative scores experimentally, by running the different technologies (often algorithms) on large preset databases. This is particularly the case for fingerprint recognition and face recognition. However, many suppliers of biometric technologies do not offer the ability to carry out such independent tests, for example because the sensor is embedded in a tamper-resistant manner in a smart phone, and the matching algorithms runs on a secure chip.

Major challenges for biometric authentication are damaging or the absence of the biometric mode at a significant number of people, the change of the biometric property due to aging, the influence of the environment on sensors, and the possibilities for imitating of a biometric characteristic.

Another problem with biometrics is that it is relatively privacy-sensitive. Biometric authentication can expose unforeseen medical conditions, may enable undesirable remote processing of unchanging sensitive information about people (race), create a high degree of traceability, or even be perceived as a breach of human dignity. A possible solution to the privacy problem is the decentralized storage of templates, as close as possible to the user. This may take the form of a tamper-resitant device (a smart card, for example), in which case it is preferred that the matching takes place on this device (so-called "match-on-card"). There are also solutions that make it possible to centralize storage privacy-friendly.

Common examples of biometric authentication are fingerprint authentication to 'unlock' smartphones and the use of face recognition for surveillance purposes. A special application of biometric authentication is continuous authentication: continuously testing a biometric feature to continuously verify identities. Often, this is done by following the behavior of a (genuine) user over extended periods of time. The online learning environment *Coursera*, for example, analyzes typing behavior to determine that the user is always the same as the person who is logged on. An additional advantage of continuous authentication is that differences in the attribute can be noticed over time, and the template can be adjusted automatically, which prevents the necessity for re-enrollment.

Sensors for the reading of biometric characteristics are very diverse, and may be conventional sensors, e.g., a camera on a smartphone, or developed especially for biometrics; for example, an infrared camera on a dedicated device.

There are several standards for biometric authentication. Notable standards are BioAPI, or ISO 19784, and ISO 25709 which describe the communication between various systems that make up a biometric application. Unfortunately, adoption of the BioAPI standard is still quite low. ISO 19794 which describes various formats for storing biometric templates. More recently, the FIDO Alliance, a consortium of organizations, introduced FIDO (Fast Identity Online). FIDO is an authentication standard that describes a communication protocol that requires encrypted communication between users, services and FIDO server where keys are stored safely. In a typical implementation of a biometric authentication method based on FIDO (UAF) the template remains on the device used, for example the smartphone. There are two variants of FIDO: U2F, to use an authenticator as a second factor, and UAF for deploying an authentication credential as a first factor. The Biometric Open Protocol Standard (BOPS), developed at the initiative of biometrics provider Hoyos Labs, was adopted by the IEEE in September 2015 as IEEE 2410-2015. The standard describes a system for online biometric authentication and identification, and is similar in many respects to FIDO.

2.1. Biometrics as authentication or as holder-verification

Biometric technologies can be used as authentication directly (the verification against a template takes place at the identity provider) or as device-holder-verification (the verification takes place in the capture device, for example in a smartphone, and unlocks the authentication device). The former model has security and privacy disadvantages as all templates will need to be stored centrally.

In the latter model the templates are stored locally on the device, which offers a different attack surface than the former model. Typically, in the latter model, the biometrics function as an access credential to unlock private key stored in the device. The actual authentication towards the identity provider is then simply a PKI based authentication, and therefore the latter model is easily integrated in a federated setting. On the other hand, some biometric modes offer so-called continuous authentication, a characteristic which cannot be used if the biometric match merely unlocks a traditional PKI key.

3. Comparing biometric modes

Comparing the different biometric modes is not trivial. There are many biometric modes, of which fingerprint, face, iris, retina, and voice are probably most well-known for authentication. The state-of-the-art scan that was conducted in the current study firstly produced a long list of all known biometric technologies for authentication based on desk research. This list ranged from the above mentioned traditional physiologic and behavioral modes to exotic modes such as butt impression and oto-acoustic emission. A short list of most suitable technologies was then composed and reviewed by various experts in the field. The short list contains the following modes: *fingerprint*, *iris*, *retina*, *finger vein*, *eye vein*, *face*, *heart rate*, *voice*, *handwritten signature*, *user interaction*, and *gesture*. The state-of-the-art scan applied five key criteria on which the different technologies were scored. These criteria are: *performance*, *security*, *universality*, *user friendliness*, and *fit-for-purpose in a federative setting*, which will be explained in more detail below.

It is important that these criteria are measured properly: data needs to be available so that the criteria can be assessed. This applies in particular to the "performance" criterion. Preferably it should be assessed independently, and at the very least vendors should be transparent about it. When the performance of a mode can generally be poorly tested, it scores lower on our performance criterion in the assessment.
These criteria are meant to provide a generic assessment of the biometric modes; much depends on the final application. Nevertheless, it is appropriate to establish a rough estimate, as to be able to make a first selection in suitable solutions. Note, "fitness" in the list below is not the sum of the criteria above, but refers to the suitability for SURFconext Strong Authentication. A biometric mode may score well on the first four criteria, and yet not be suitable, for example, because that solution is too costly or not scalable. Finally, any solution must comply with standards, laws and regulations.

Table 1: Criteria.

Symbol	Criterion		Explanation
	Performance		The quantitative performance of different biometric technologies has been compared in the past, both by the independent research community and by technology vendors in large scale tests (e.g. the so-called “grand challenge” tests as organized by NIST). In such tests biometric technologies are compared on performance metrics such as false acceptance rate, false rejection rate, failure to enroll, etc. Recent developments embed the biometric sensors for the traditional modes in consumer hardware devices (e.g. Apple’s Touch ID) and also introduce new modes like finger vein pattern, eye vein recognition, heart rate, and various behavior based technologies. Commercial vendors nowadays appear to be more protective of their intellectual property. This makes it harder to compare the performance of new biometric technologies.
	Security		The security of biometric technologies, not already covered in the performance criterion above, greatly depends on the ability to keep adversaries from spoofing the sensor. Liveness detection may help to mitigate the risks.
	Universality		The universality of biometric technologies is affected by the availability of the technology in the market. The inclusion of a suitable sensor in a mass market electronic product, especially when that product is mobile and strongly bound to the end-user, makes it very likely that a large audience of students and staff-members will be able to access the particular technology. Contrarily, the need for dedicated (and often costly) additional hardware has a negative impact on the universality criterion. Also, universality is determined by the biometric technology functioning properly under different circumstances and over time.
	Usability		The user friendliness of biometric technologies is influenced by the intrusiveness of the biometric mode and the complexity and effort of use. For instance, for retina scanning the camera needs to be very close to the user’s eye. Also, the time it takes to perform a scan during enrollment and authentication influences the user friendliness of the solution.
SURF NET	Suitability		The suitability, or fit-for-purpose of biometric technologies, depends on how well the technology integrates within the existing authentication infrastructure. Consider, for example, the characteristics of the user base and authentication process, scalability of the solution, or business case. The architecture of the federation also influences this criterion. Within an identity federation the responsibility for authentication is delegated to the identity provider, so that so-called continuous authentication is less obvious. Some biometric technologies require a tighter integration of the authentication process and the service provider. This especially holds true for technologies that rely on user behavior rather than physiological features such as user interaction, gesture recognition, heart rate recognition, etc. Another important factor to fit-for-purpose is the maturity of the technology and market; experimental technology or a few small vendors may adversely affect the decision to adopt biometric authentication solutions.

4. Biometric modes

Based on desktop research a shortlist of biometric modes was compiled. This list was reviewed by external experts in a wisdom-of-the-crowd session hosted by Dutch NREN SURFnet.

4.1. Fingerprint

Fingerprint patterns are uniquely identifying and remain relatively unchanged during aging. Fingerprints can be used for forensic tracking purposes, but also for identification and authentication purposes.

In addition to traditional registration with ink and paper, fingerprints are now mainly obtained through electronic registration via optical, ultrasonic, capacitive (conductivity of the skin) or thermal sensors. The emergence of fingerprint biometrics on smart phones has brought this form of biometrics to the masses, usually via a capacitive sensor (but using a camera also occurs). Motorola was one of the first developers to offer this technology, but now almost all the major smartphone vendors offer this technology. It is predicted that by 2020 at least 34% of all mobile devices will have a fingerprint reader. Qualcomm even has a fingerprint reader in development that remotely creates an ultrasonic print taken in 3D. This also works when a finger is wet or dirty, and even scans through glass or plastic. Hoyos Labs has a solution that will scan four fingers simultaneously with the regular smartphone camera using the flash. According to a study by IHS the market for fingerprint sensors will grow to $ 1.7 billion by 2020. In addition to the market for fingerprint sensors, there is also a wide range of fingerprint software. There are several providers for generic two-factor authentication applications that support fingerprint.

The performance of fingerprint authentication (in terms of FAR and FRR) is pretty good. Fingerprint solutions from major suppliers are regularly compared against standard databases.

A challenge is that the sensor in many cases is sensitive to moisture and dirt. Moreover, fingers may be damaged and are vulnerable to aging. Another problem is that fingerprints can be taken over intentionally. For example, by surreptitiously taking a fingerprint left by a victim and put a plastic cast of the print on your own finger. Liveness detection proves to be difficult with conventional sensors.

4.2. Iris scan

Iris recognition is a form of biometric identification that is applied to video recordings of one or both irises. Iris recognition is often confused with retina scanning; This is another technique of analyzing the unique patterns of blood vessels in the retina.

Use is made of a camera to make recordings of the detailed structure of the iris. Virtually all iris recognition systems capture images of the iris under illumination of near infrared wavelength (Near Infrared Wavelength, NIR, 700-900nm). The reason is that while light-colored eyes reflect the structure under normal lighting (visible wavelength), most people have brown eyes that only within the NIR spectrum reveal patterns sufficiently. Smartphones that support iris scanning, therefore contain an additional infrared LED and an infrared camera.

The iris scan is used among other ways for passport-free border control, such as Privium in the Netherlands. The United Arab Emirates even use this since 2001 for its surveillance. There is often made use of dedicated devices. Providers of such technology on smartphones are unfortunately not much. Fujitsu is the first with an application for smart phones, currently available only in Japan. There are rumors that LG and Samsung will soon offer this technology in their smartphones.

The technology performs well and works fast [4], the performance criterion is therefore green. The iris is also a consistent feature (iris recognition works for up to 30 years after registration!) Because the iris is visible from the outside, but is protected from the environment.

The technology is simple to use, for example, it does not require direct contact with any device. An iris scan can be taken at 4 inches or even a few feet away, and even works with colorless contact lenses, eyeglasses and non-reflective sunglasses.

The main risk, beyond bad photos due to a faulty recording process or technique, is spoofing using high resolution photos or even lenses with a false iris. This ensures that the technology only scores orange on safety. A form of liveness detection is thus advised, for example, by checking whether the iris responds to changes in ambient light.

4.3. Retina scan

The retina is a thin layer of tissue consisting of nerve cells against the back of the eye. Due to the complex structure of blood vessels in the retina the patterns of these blood vessels are unique to everyone. This network of blood vessels is not entirely genetically determined and thus even for identical twins not the same.

Although blood vessel patterns in the retina can change with conditions such as diabetes and cataracts, retinas will normally remain unchanged for everyone's life. Because of the unique and unchanging nature of the retina it is highly reliable biometric characteristic which in terms of performance compares with an iris scan or fingerprint.

A retina scan is done by shining an invisible beam of near-infrared (NIR) light in one eye while the subject looks into the scanner. Because the blood vessels absorb more light they leave a dark reflection and are thus visible in the scan result. The pattern of this variation is then stored digitally in a database.

Retinal scans are used for authentication and identification. There is also a medical use of retina scans, because certain transmissible and genetic disorders are detectable in the eye, such as for example AIDS and leukemia. Sometimes retinal scanning technology is confused with iris scans or eye vein recognition.

There are at the moment of writing no commercial smart phones that contain this technology. However, there is an interesting open source project from New Zealand that uses additional hardware smartphones that enables you to scan the retina. PCMag claims the Chinese phone developer ZTE offers retina scanning technology in a smartphone, but this appears to be eye vein recognition in fact. Therefore retina scanning scores low on universality and suitability for SURFnet.

While retinal scans are fast and reliable, there are certain diseases that affect the retina and retinal scanning requires additional equipment. Because the subject needs to keep the camera relatively close to the eyes the technology also scores low on ease of use.

4.4. Finger vein patterns

Vein Pattern Recognition for biometric authentication makes use of patterns of blood vessels in the finger, but this is also possible with the palm of the hand, wrist, back of the hand, or elsewhere in the body. Vascular patterns are a unique identifier. Thereto Near Infrared (NIR) light is shone on the finger. The blood vessels absorb infrared light, making them leave dark lines on a picture. The picture that is taken, is then used for template matching. Authentication based on these templates can be done within 2 seconds. Usually, there are dedicated devices required for finger vein recognition. This technique can easily be combined with fingerprint recognition by integrating that into the same device.

Hitachi has developed a finger vein authentication system and patented this in 2005, which is used for credit cards, cars, attendance, cash machines, and computer authentication. The device consists of a NIR LED light, a CCD camera and an encrypted SIM card. Barclay's Bank announced in 2015 to use VeinID technology for online banking. Other providers are Mofiria, NEC and M2SYS. Sony even offers a sensor that is suitable for implementation in a smart card so match-on-card is possible.

Blood vessels are almost impossible to copy without the cooperation of the owner and an extremely unique identifier and therefore safer than for example a fingerprint. Therefore this technology scores well on performance and safety . Finger vein scanning is largely unaffected by environmental factors. Unfortunately, there are no non-dedicated devices such as smart phones that support finger vein recognition. Outside the lacking of fingers and some rare diseases, almost everyone has finger veins.

4.5. Eye vein patterns

The veins in the sclera, the white of the eye, may be included for biometric recognition. Patterns of these veins are stored as a template for subsequent comparison. The pattern of these blood vessels form a stable characteristic that changes little from age, alcohol consumption, allergies or overall redness of the eye [3]. The standard camera on most smartphones is suitable for eye vein recognition. Again, this works even with lenses or eyeglasses, but not with sunglasses. Sometimes it uses infrared light to create an image of the sclera so that it can work in dark conditions (which therefore requires an adjustment to the smartphone).

The company EyeVerify has a patent on this technology. This company provides software applications for eye vein recognition and is supported on iOS and Android. EyeVerify also offers an SDK and partners with Chinese smartphone manufacturers ZTE and Vivo.

There are two studies on the EyeVerify technology that indicate that the implementation of eye vein recognition performs well. However, these studies have been commissioned by EyeVerify. The technology did not pass the same independent testing as for example fingerprint recognition and face recognition. This technology therefore scores moderately on performance in our comparison, but this could well be improved if more independent research is done.

The recording unit should be kept close to the face, which possibly is uncomfortable for the user.

4.6. Face recognition

For face recognition photo or video recordings will be made of the face during enrollment and matching. There are several algorithmic approaches are possible, including eigenface analysis, linear discriminant analysis and Hidden Markov models. Relatively new is to model the face in 3D. Ordinary cameras can be used for face recognition, but there are also face recognition applications on the basis of infrared thermographic images.

Facial recognition is used as a biometric identifier for forensic purposes, identification at border controls or face-in-the-crowd recognition. Other applications include identification at ATMs, attendance monitoring in the workplace or photo applications that people recognize and tag (including iPhoto, Picasa, Live Photo Gallery and Facebook). MasterCard test recently "SelfiePay" where you authorize a payment with a picture of the face, and Alibaba even offers "Smile to Pay" to. Android phones feature Face Unlock, that can be enhanced by the user with cumulative template storage and liveness detection.

There is a very mature market for facial recognition applications. A report from Tractica expects the market to grow from 28.5 million units in 2015 to 122.8 million in 2024, with annual industry growth of 22% from $ 150 million to $ 882 million. In particular applications on mobile devices are expected to increase in number. Hence this technology scores well on universality. Examples of providers of smartphone apps for face recognition as a second factor are VeriLook, Facial Network, Bioscrypt, IdChecker and KeyLemon.

Compared to other biometric technologies such as fingerprint and iris scan face recognition is not the most reliable or efficient. In terms of performance this technology scores mediocre.

An advantage of face recognition is that it can also be performed passively. It is sensitive to differences such as facial expression or the angle at which the picture is taken, as well as environmental factors such as exposure. There are ISO standards that prescribe how recordings should be taken for optimal results.

Some applications of facial recognition can be easily circumvented by holding a picture of a face in front of the camera, liveness detection is therefore important for extra security. Face recognition is also more privacy-sensitive than for example a fingerprint, because a picture says a lot about things like ethnicity and age.

4.7. Heart rate recognition

The heart rate also has patterns that may be used for identifying an individual. This can be measured by means of an electrocardiogram (ECG). After the removal of noise can so-called fiducial points are determined, from which patterns can be drawn, also known as a PQRST pattern. The property depends little on where on the body the sensor is placed.

Many smartphones already have a heart rate monitor, and there are plenty of wearables such as smart watches and fitness trackers that measure heart rate. Examples include Samsung and Apple smartphones, AliveCor Mobile ECG and the Fitbit fitness tracker. Measuring one's own heartbeat, among other health reasons, a trend expected to rise to one third of all Americans in 2018 wearing a heart rate monitor. And when someone does not have the heart rate monitor strapped on yet, it takes only seconds (~ 10) before the measurement is done. The heartbeat is suitable for continuous authentication as well. Halifax Bank of Canada,for example, conducted a pilot to use heartbeat authentication via Nymi bracelet for online banking.

Wearables and smartphones with a suitable sensor are not sufficiently available to put the technology to green on universality, this will remain orange.

Unfortunately, the performance of ECG is poor. Singh and Singh [16] deemed the performance "moderate" and advise to combine this mode with other modes such as fingerprint or face recognition.

In addition to ECG another technology is plethysmographywhich uses an ordinary camera to measure the change in color of the skin from expansion of the capillaries in the skin. This method is less accurate for authentication and is not typically used with authentication in mind. An example of this technique is Phillips' Vital Signs app.

4.8. Voice recognition

Voice recognition recognizes who speaks, not to be confused with speech recognition, which recognizes what is being said. Acoustic patterns of speech are unique to everyone and are caused by both the anatomy (shape of the throat) and learned behavior (tone and style). It is therefore often considered to be a behavioral biometric and is usable for identity verification. Just like face recognition, voice recognition can be done unnoticed by eavesdropping.

During the enrollment process, the voice of the speaker is recorded. From this a number of characteristics are converted into a voice print. During authentication, a voice sample ("utterance") is then compared against voice prints in the database. There are two categories of voice recognition: text dependent and text-independent. When the text during authentication must be the same as during enrollment it concerns text-dependent verification. In text-independent verification of the utterance is not the same as during enrollment, therefore the algorithms for comparing voice prints are complex.

Voice recognition is sensitive to ambient sounds, changes in behavior and emotions, health (think of a cold) and the influence of the microphone. In addition, speech can be recorded and played back.

Microphones are available on many devices, including PCs and smartphones. It is also possible to enable continuous authentication from spoken interaction, for example, telephone calls or by the emergence of voice control (think of personal assistants like Siri or Cortana on smartphones). Many banks use speech and voice recognition in voice response systems. The Dutch bank ING are using voice recognition for access to their app.

There is a mature market for first and second factor authentication applications of voice recognition. Providers include DigitalPersona, Daon, BioID, Authentify and KeyLemon. According Tractica the market for speech and voice recognition will grow to $ 5 billion in 2024, with a variety of apps.

In terms of performance, it is not the most reliable form of authentication. Users may consider it also as "invasive" or: it cannot be used "under-the-table"; it may not be socially appropriate for the user in certain situations to start speaking loudly into an authentication device.

4.9. Handwritten signature

Handwriting is relatively unique to each individual and is therefore becoming increasingly popular for authentication applications. Many systems use three-dimensional analysis of a handwriting sample which considers the form and pressure of writing. Handwriting Analysis can be both dynamic (online, in real time) and static (offline afterwards scanned). An important form of handwriting analysis for authentication is signature analysis. A signature is an accepted form of authentication in the non-digital world. Most people have a signature. A signature also allocates an additional factor ("something you know"). Dynamic signature recognition is used as a behavioral authentication method. The signature is analyzed on the basis of rhythm, shape, timing, and pressure fluctuation. For this application, a pressure-sensitive touch screen is often used, for example, a tablet, smartphone, PDA or dedicated device. This is different than an ordinary photograph or other one-dimensional image of a signature, which, for example, is widely used for a signature for approval. The signature then creates a digital template for subsequent matching. It is also possible to observe changes in the signatures over time to consider at regular authentication. Except for authentication, this technology is also widely used for determining the authenticity of signatures, such as documents or memorabilia signed by celebrities.

Although the shape of a person's signature is often relatively simple, imitating someone's signature remains very complex. Dynamic signature authentication is, therefore, a secure authentication method, however, the accurate determination of a person's signature is also very complex, resulting in a high FRR due to slight changes in handwriting, which in turn is at the expense of the user. Moreover, handwriting recognition works best with a pen or stylus and the user does not always have this with him. Signatures written with a finger on a touchscreen compromises on the accuracy of authentication.

There are a limited number of apps in circulation for signature authentication, often as first factor or digital signature, but many are unreliable. Examples are CIC's iSign digital signature, BioWallet's password manager, screen lock apps like Unlock and KinWrite Signature (for Microsoft Kinect interface). The Samsung Galaxy Note 10 tablet comes with signature recognition software. One application of this technology is Sign2Pay.

4.10. User interaction

Various properties of the interaction of the user (Human Computer Interaction, HCI) with a system enable identification and can be used for biometric authentication behavior. In particular keyboard and mouse dynamics (direct interaction), but also the content of the interaction (indirect interaction, based on knowledge, skill and strategy, think of using applications) are suitable. One advantage is that it is suitable for continuous authentication, but this means that it is less suitable as a primary factor because it does not know a single moment of authentication, but requires a certain time interval, and therefore has a relatively intensive enrollment process.

Keyboard Dynamics looks at the way and rhythm of typing on a keyboard. These patterns form a biometric template for later recognition. For example, an algorithm analyzes how long keys are pressed, the keys used for capital letters, or how often backspace is used and logged the resulting text. The accuracy of these techniques vary widely in precision and success, and vary from simple statistical analysis to the artificial intelligence such as neural networks. Obviously, this technique is intended primarily for PC's with keyboards. The online learning environment Coursera used signature track technology based on keyboard dynamics to continuously verify the identity of users. The market for typing behavior recognition is relatively mature with many providers. Examples include Type Watch, Intensity Analytics AdmitOneSecurity, BioTracker, KeyTrac, KeystrokeID, Type Sense, Psylock, Authenware, bioChec, Probayes and BehavioSec. Keyboard Authentication is complex because typing behavior varies depending on the human condition, environmental factors and common applications, this variation can lead to poor performance of biometric authentication. Moreover, keylogging, recording what users type, is very privacy sensitive, or even prohibited by eavesdropping laws.

Dynamics mouse is very similar to keyboard dynamics, in which mouse movements and click behavior are analyzed. However, mouse behavior is less suitable, partly because less use is made of the mouse navigation. Moreover, this technology is less mature than keyboard dynamics. Often mouse behavior is combined with keyboard dynamics, for example, by BehavioSec. Biometrics based on other input devices such as a stylus or touchscreen are possible.

Another component of biometric authentication on the basis of user interaction is to look at the content, or what the user does. Think of things like frequency of use and navigation. This activity can be detected by exploiting registers of the operating system or through monitoring software. Notable examples of characteristics measured include email behavior, programming style, style of play in videogames, character style (Passdoodles, draw-a-secret), and commands in a command line interface.

In terms of performance keyboard dynamics in particular scores reasonably, mouse dynamics performs worse, and indirect interaction does worst [9], but this is also the order of maturity of the technology. Interaction behavior is very difficult to copy as a biometric factor. Obviously keyboard dynamics relevant only for PCs and not for instance smartphones. The privacy sensitivity of the record of the behavior limit the user acceptance.

4.11. Gesture recognition

Gesture based computer interaction intends to recognize human gestures. Gestures can come from all over the body, but typical of the hands or face. This discipline focuses on emotion recognition and hand gestures. A special application is to interpret sign language with computers. Registration of gestures can be done through special gloves, stereo cameras, and accelerometers in a smartphone. Also, gesture-based input devices such as Kinect and Leap and multi-touch screens for example, smartphone and tablet, can be used for this.

Its biometric performance characteristics suggest gestures are suitable for use in authentication applications. A personal gesture can also serve as a password, which is an additional factor of authentication ("something you know").

An example is AirAuth, an application in which users make gestures to a camera to get access. There are various applications for gestures on a multi-touch screen like a tablet or smartphone. Lockheed Martin provides an example with Mandrake, Georgia Tech developed LatentGesture, and there are several "swipe lock" apps for smartphones. Microsoft Photo Touch allows the user to authenticate themselves by drawing a pattern on a photo. Researchers together with Motorola developed uWave [10], an accelerometer-based gesture recognition mobile application.

There are applications in which the user taps a PIN or pattern on the screen in a musical rhythm. There are already a number of apps for tap authentication with changing functionality and reliability, including Tap Tap app, Tap unlock, Knockr and AuthenWare's Tap-a-Tune.

The performance and safety of gesture recognition are less accurate than for example a fingerprint. Developments in this field are still young. Gesture recognition is reasonably user-friendly and privacy-neutral, although less discreet.

5. Results and conclusions

After applying the criteria to the list of biometric technologies, the solutions that appeared to be most promising for second factor authentication within an NREN's identity federation are: firstly, *fingerprint recognition* using either a specialized sensor (as is becoming increasingly common on high-end smartphones), or using the device camera, is a safe choice in terms of performance, universality, and convenience, yet has some issues with security (spoofability). Secondly, *eye vein recognition* is a reliable solution, although it is patented by a single vendor, hence objective assessment of this technology proved difficult. Thirdly, *face recognition* using the generic device camera is a good option, yet performance when compared to the other two is sub-optimal. The other technologies either have poor performance, require dedicated hardware, are not sufficiently mature, or require tight and continuous integration with the service provider and are therefore less suited for application in a federated setting.

Table 3: Results.

	Performance	Security	Universality	User experience	Suitability
Finger print	+	□	□	+	+
Iris scan	+	□	□	+	-
Retina scan	+	+	-	□	-
Finger vein patterns	+	+	-	+	□
Eye vein patterns	□	+	+	□	+
Face recognition	□	□	+	+	+
Heart rate recognition	-	+	□	□	-
Voice recognition	□	□	+	□	+
Handwritten signature	-	□	□	+	-
User interaction	□	+	□	□	□
Gesture recognition	-	+	□	+	□

For specific use cases these technologies are perhaps interesting. In other areas (e.g. the banking sector), user interaction is an important element in relation to so-called risk-based authentication.

On a final note, comparing biometrics is notoriously complicated, in part because much depends on the properties of specific solutions and vendors. Aside from the five key criteria discussed above, important characteristics to assess are the existing user base of the particular solution, compliance to technological standards such as FIDO, template protection and other security features, and agreement with privacy regulation.

6. References

1. Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M., Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, *2*(3), 13—28, 2009

2. Dantcheva, A., Velardo, C., D'angelo, A., & Dugelay, J. L., Bag of soft biometrics for person identification. *Multimedia Tools and Applications*, *51*(2), 739—777, 2011

3. Das, A., Pal, U., Blumenstein, M., & Ferrer Ballester, M. A. (2013, November). Sclera Recognition - A Survey. In (ACPR), 2nd IAPR Asian Conference on Pattern Recognition, 917—921, IEEE, 2013

4. Daugman, J., Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons, in Proc. of the IEEE, vol. 94 (11), 1927—1935, 2006

5. Daugman, John, New Methods in Iris Recognition, IEEE Transactions on Systems, Man, and Cybernetics – Part B: Cybernetics, 37(5), 1167—1175, http://www.cl.cam.ac.uk/~jgd1000/NewMethodsInIrisRecog.pdf, October 2007

6. Delac, K., & Grgic, M., A survey of biometric recognition methods. In *Electronics in Marine, 2004, Proceedings Elmar 2004. 46th International Symposium*, 184—193, IEEE, June 2004

7. Hulsebosch, B. et al., Milestone M3.1: Inventory of strong identity assurance solutions and how they compare to a web of trust approach, https://www.terena.org/mail-archives/refeds/pdfc3Cedh8OFf.pdf, August 2014

8. Jain, A.K., and Kumar, A., Biometric Recognition: An Overview, Second Generation Biometrics: The Ethical, Legal and Social Context, E. Mordini and D. Tzovaras (Eds.), pp. 49—79, Springer, 2012

9. Jorgensen, Z. and Yu, T., On Mouse Dynamics as a Behavioral Biometric for Authentication, In Proc. ASIACCS '11, ACM, 2011

10. Liu, J. et al. uWave: Accelerometer-based Personalized Gesture Recognition and Its Applications, In Proc. Pervasive Computing and Communications 2009, 10.1109/PERCOM.2009.4912759, 2009

11. Oostdijk M., et al., Step-up Authentication-as-a-Service, https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_step-up_authentication-as-a-service_architecture_and_procedures_final.pdf, November 2012

12. Ortega-Garcia, J., Bigun, J., Reynolds, D., & Gonzalez-Rodriguez, J., Authentication gets personal with biometrics. *Signal Processing Magazine, IEEE*, *21*(2), 50-62, 2004

13. Ratha, N.K., Connell, J.H., and Bolle, R.M., Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal 40(3), 2001

14. Ross, Arun, Jain, Anil K., Multimodal Biometrics: An Overview, Proc. EUSIPCO12, 1221—1224, September 2004

15. Sanjekar, P. S., & Patil, J. B., An Overview of Multimodal Biometrics, *Signal & Image Processing: An International Journal (SIPIJ) Vol. 4*, 2013

16. Singh, Yogendra Narain and Singh, S. K., Evalutation of Electrocadriogram for Biometric Authentication, Journal of Information Security, Vol. 3, No. 1, 39—48, http://dx.doi.org/10.4236/jis.2012.31005, January 2012

17. Spreeuwers, Luuk, Breaking the 99% barrier: optimisation of three-dimensional face recognition, IET Biometrics, 4(3) 169—178, http://dx.doi.org/10.1049/iet-bmt.2014.0017, September 2015

18. Tuyls, Pim, Škorić, Boris, Kevenaar, Tom (Eds.), Security with Noisy Data, Springer, ISBN 978-1-84628-984-2, 2007