ABSTRACT
This is a research in what authentication assurance levels can be reached by the FIDO UAF and the BOPS protocol. Assurance levels are defined by the EU, NIST and ISO, but unclear is what levels the authentication protocols can reach. Requirements of the assurance levels are measured against specifications of the authentication protocols. Concluded is that there are no big software or hardware limitations for the protocols. Biometric performances are however still not perfect.

Keywords
Mobile Devices; Authentication Protocols; Authentication Assurance Levels; Biometrics

1. INTRODUCTION
More and more on-line authentication tasks are done by mobile devices nowadays. This demands safe and correct authentication protocols on those mobile devices. Many mobile devices are developed with some piece of biometric identification hardware, which opens up the opportunity to use this hardware in authentication processes. Two emerging protocols that incorporate biometrics have been analysed on their security and privacy features [16]. Concluded was that the biometric authentication on smartphones has some limitations, but this could be improved in the future. One of the discussed protocols is The Universal Authentication Framework (UAF) from the Fast Identity Allience (FIDO). The other protocol is the Biometrics Open Protocol Standard (BOPS) developed by Hoyos Labs and published as a standard by the IEEE [2]. The makers of the protocols both have their own approaches on making a biometric authentication solution, but both specify a protocol that allows on-line services to authenticate with biometrics.

Since governments are very interested in the development of authentication techniques, regulations called eIDAS are made by the EU concerning electronic identification and trust services for electronic transactions [5]. Furthermore the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce made guidelines on digital authentication [7]. The eIDAS standard as well the NIST standard describe authentication assurance levels that roughly follow the authentication assurance levels defined in the ISO/IEC 29115:2013 standard [10]. The three levels of the eIDAS standard cover mainly the last levels of this ISO standard. The assurance levels provided by those organizations are in terms of the consequences of authentication errors and misuse of credentials. The eIDAS regulation specifies 3 assurance levels: low, substantial and high, whereas the FIDO and the ISO standards specify four levels of assurance.

1.1 Problem Statement
Unclear is which assurance levels can be reached with the mentioned UAF and BOPS authentication protocols used on mobile devices. Research has to be done to clarify what hardware or software-based limitations mobile devices have an what specific authentication assurance levels actually mean concerning biometric authentication protocols.

1.2 Research Questions
Based on the problem statement, the research questions are:

RQ1 Based on the eIDAS, NIST and ISO standards, which authentication assurance levels can be reached with the biometric authentication protocols UAF and BOPS?

RQ2 What are the recommendations regarding authentication protocols on mobile devices?

To answer the first research question an analysis has been done on what the hardware-based and software-based limitations on mobile devices are. Furthermore minor differences between the standards and the specifications of the UAF and BOPS have been explored. Implications that come with biometric authentication on mobile devices have to be analysed to give proper recommendations for the use of this technique.

2. AUTHENTICATION PROTOCOLS

- BACKGROUND
On-line authentication protocols in general are basically build upon an authentication model. This model consists of the user, the identity provider and the on-line service provider/relaying party. A user of an on-line service can be authenticated by an identity provider. The identity provider assures the relying party with a certain level of confidence that the identity of the user is the actual claimed identity of the user. The identity provider runs the whole actual authentication procedure with the user. Many on-line web services as a relying party also have the role as an identity provider.
2.1 Authentication factors
An authentication protocol is based on one of the three authentication factors. One of the authentication factors is the knowledge factor that is widely used in authentication protocols. Examples of a knowledge based factor are passwords or a PIN code. A possession factor is something a user has, such as a ID card or a smartphone. The third authentication factor is based on a biometric of a user i.e. a discriminating physiological or behavioural property. Biometric authentication factors include, fingerprints, face or even gait patterns. As mentioned the UAF and the BOPS protocols make use of the biometric authentication factor. The following biometric specific authentication protocols both have their biometric templates stored locally on the mobile device itself. This means that the biometric data itself isn’t send over a network or stored on a centralized database, unlike a currently most used password system. The data stored locally is not vulnerable to large scale theft of all the data what is a huge advantage towards centrally stored data.

2.2 FIDO Universal Authentication Framework
FIDO is an alliance of different vendors with the same common goals and interests in creating a new way of online authentication. With the UAF they created a protocol for biometric authentications without the need for passwords. In FIDO’s UAF architectural overview document is described what components the UAF has [15]. More specific details about the UAF protocol are in the protocol specification [12]. This section will briefly describe the components of the UAF protocol. A FIDO UAF enabled mobile device has to have the FIDO client software implemented and has to have a FIDO authenticator. The software interacts with the FIDO authenticator and a relying party software for example a mobile app or browser. The authenticator uses a biometric sensor for example a fingerprint reader. Authentication requests are handled locally by the FIDO client together with the FIDO authenticator and verifies the requests with a FIDO UAF server. The FIDO UAF server is part of the relying party’s server.

Initial usage of an authenticator, the authenticator has to be registered on the FIDO server. A relying party is able to detect when a user begins interacting with them with a new authenticator on which the server sends his policy to the authenticator. The user has to present his biometric. The authenticator can now create a private/public key pair which is unique to the mobile device and the service of the relying party. The authenticator sends an attestation and the public key back to the server. With the attestation the authenticator gives a cryptographic proof of the authenticator model to the relying party. The authenticator now is registered and the relying party is now able to request the user to authenticate with a registered authenticator.

In case of an authentication request from the FIDO server a cryptographic challenge that the authenticator has to solve is send to the authenticator. The authenticator unlocks a private key depended on the biometrics of the user. The authenticator responds to the challenge signed with the user’s private key.

To summarize the components, the mobile device consists of the application of the relying party, the FIDO client and the FIDO authenticator. On the server-side of the relying party is the FIDO server. The outlined design of the protocol doesn’t need the existence of an identity provider. Figure 1 gives an overview of the UAF components.

2.3 Biometrics Open Protocol Standard
The BOPS protocol provides an end-to-end identity authentication protocol with modular components that are fully open-source. In comparison with the FIDO UAF protocol the BOPS protocol specifies the protocol in a single layer that also handles authenticator specific protocols. Whereas the specific requirements for the biometric recognition system lays outside the scope of the FIDO UAF protocol. The BOPS protocol has three core components: the mobile device, the BOPS server and the intrusion detection system (IDS). All security protocols lay inside the scope of the BOPS protocol whereas the FIDO protocol specifies much less specific protocols as seen in the figures. The connection between the mobile devices, the BOPS server and the server of the relying party relies on two way SSL/TLS communication. The IDS runs on the mobile device as well as on the BOPS server and prevents attacks such as spoofing attacks and presentation attacks. Figure 2 gives an overview of the BOPS components.

3. AUTHENTICATION ASSURANCE LEVELS OF SECURITY STANDARDS & GUIDELINES
3.1 ISO authentication assurance levels
The ISO/IEC 29115:2013 [10] standard specifies 4 levels of assurance abbreviated as LoAs. Citing the ISO document: "Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity
that uses a particular identity is in fact the entity to which that identity was assigned.” LoA 1 is the lowest level and is used when minimum risk is associated with erroneous authentication. No specific authentication mechanisms are specified that have to be used. LoA 2 is used when there is a moderate risk associated with erroneous authentication and LoA 3 is used when the risk is substantial. LoA 3 prescribes a multifactor authentication method and secret information has to be cryptographically protected when transmitted. LoA 4 is similar to LoA 3, but specifies the need of tamper-resistant hardware devices. Additionally, an in-person identity proofing is needed. In other words when a user wants to enrol himself he has to prove that he is the right person towards a real person.

In Table 1 is stated how the different LoAs map to each other as used in this paper.

### Table 1. ISO LoAs mapping to NIST and eIDAS

<table>
<thead>
<tr>
<th>ISO/IEC 29115</th>
<th>NIST</th>
<th>eIDAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoA 1</td>
<td>LoA 1</td>
<td>Low</td>
</tr>
<tr>
<td>LoA 2</td>
<td>LoA 2</td>
<td>Low</td>
</tr>
<tr>
<td>LoA 3</td>
<td>LoA 3</td>
<td>Substantial</td>
</tr>
<tr>
<td>LoA 4</td>
<td>LoA 4</td>
<td>High</td>
</tr>
</tbody>
</table>

#### 3.2 NIST Authentication Assurance Levels

In SP 800-63-3 [7], the NIST made their own authentication level system based on the four defined levels of assurance in OMB M-04-04 [14] and is also inspired by the ISO assurance levels. In the defined system by the NIST differentiations are made in three categories, the M-04-04 are basically split up in the identity assurance level(IAL), the authenticator assurance level (AAL) and the federation assurance level. The LOAs 2 and 3 are taken together in those categories which results in three levels for each category. As SP 800-63-3 document is still a draft version, the requirements related to the assurance level can still change. In this paper is worked with the requirements that are currently defined (30 nov 2016).

#### 3.3 eIDAS Authentication Assurance Levels

For the assurance level specification in the eIDAS document the ISO/IEC 29115 has been taken into account and the level roughly follow the last three NIST LoAs. Many requirements for the levels low, substantial and high come down to an own interpretation of the specific requirement and other requirements are very clear. Furthermore nowhere in the document are biometrics discussed.

### 4. RELATED WORK

The security and privacy issues concerning the FIDO UAF protocol and the BOPS protocol are researched as mentioned in the introduction [16]. This research specifically reviews how threats to biometric systems in general are handled by the regarding protocols.

Different biometric techniques on smartphones are discussed in ‘Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts’ [4]. The challenges and practicalities of fingerprint, iris and palmprint recognition methods are discussed but there is no unambiguous conclusion of what the most promising technique is. Also some considerations are given on identity theft, security and privacy.

In 2011 the article ‘Security analysis of Authentication Protocols for Nest-Generation Mobile and CE Cloud Services was publicised [9]. A novel authentication protocol was presented with the feature of having no password stored at a specific service. Furthermore existing protocols are discussed, but no biometric authentication protocols are reviewed.

### 5. ANALYSIS

#### 5.1 NIST requirements

The NIST document supports only limited use of biometrics for authentication as it is only supported in combination with another authentication factor. One of the reasons for this limitation is that biometric matching is stated as probabilistic, whereas other authentication factors are stated as deterministic. Other reasons given in the document are the risk of presentation attacks and the limited availability of biometric template protection. First the general characteristic of NIST requirements will be discussed and afterwards the characteristics of the LoAs. Table 2 gives an overview of the NIST requirements.

##### 5.1.1 NIST general requirements

To meet the NIST requirement of using a second authentication factor next to biometric authentication, a possession-based factor could be used or a knowledge-based. With using for example a password as a second authentication factor some advantages of using biometrics will be overridden. Ideally the mobile device itself has to function as a possession factor to overcome the two factor requirement. This way there is no need of second factor authentication device or an knowledge based factor. The FIDO UAF protocol focuses primary on a biometric as only main authentication factor, however when using the UAF protocol, an authenticator has to be enrolled that creates a key pair that is unique to the mobile device. Using a biometric as authentication factor in together with the UAF protocol can be seen as a multi-factor authentication. This observation is also stated in the FIDO documentation and also other multi-factor authentication options are given. It is possible to use a knowledge-based factor or another protocol called U2F together with the UAF protocol. Also the BOPS protocol binds a person’s identity to a mobile device and biometric, which can be used for second factor authentication. Again multi factor authentication isn’t the main focus of the BOPS protocol, but adding more authentication factors is a possibility.

Another general requirement in the NIST document is that the biometric authentication system needs to have an equal error rate (EER) of 1 in 1000 or better and also needs a false acceptance rate (FAR) of 1 in 1000 or better. This is in terms of the newest biometric authentication techniques an achievable requirement. Both the UAF and the BOPS protocol are not limited by this requirement. The feasibility of these requirements is discussed in another section.

Furthermore the NIST specifies a presentation attack detection requirements. The biometric system should have a presentation attack resistance of 90%. This requirement is not mandatory yet, but is strongly considered to be in the future. A presentation attack is the act of presenting a biometric measure of someone’s else to get authorised as the other person. E.g a printed photo of someone face can be used to fool the biometric camera sensor of being that person. To ensure that the presented biometric by certain user is actually from that user, liveness detection could be used. The UAF protocol specifies that liveness detection should be implemented, but no further requirements concerning this problem are given [13].
mented the presentation attack detection system will be in the software of the Authenticator. The BOPS protocol gives a mandatory requirement to include some form of liveness detection or another way to prevent a presentation attack. The BOPS protocol specifies this requirement further: False negatives shall be below 1.2% and false positives shall be below 0.05%. Biometric matching has to occur within 5 seconds and if the matching is under 12 seconds, the false positives shall be below 0.03%.

Every NIST LoA needs to be resistant against man-in-the-middle attacks. This is an attack where an intruder intercepts data that is send between two parties in the protocol. This enables the intruder to modify the data or to abuse it. To prevent this both the UAF and the BOPS protocol use TLS channels between the mobile device and the server of the relying party.

5.1.2 NIST LoA 1

Basically all types of authenticators are allowed for LoA 1. When a authenticator is used within a government agency the authenticator has to meet the requirements of FIPS 140-2 level 1 [6]. This level contains no physical security mechanisms, but cryptographic algorithms or function should be approved. Software of the authenticator may be executed on a general purpose computing system. This either for the UAF and the BOPS protocol no problem.

Another LoA 1 requirement is reauthentication in at least once per 30. This can clearly be achieved with the protocols.

The following LoAs have at least the same requirements as LoA 1.

5.1.3 NIST LoA 2 & LoA 3

An authentication process with LoA 2 or LoA 3 has to resist replay attacks. A replay attack is an attack where an intruder successfully authenticates himself by recording an replaying a previous authentication message. When implemented correctly a TLS protocol should protect against those attacks in case of the UAF and the BOPS protocol.

Reauthentication has to take place at least once per 12 hours or in at least 30 minutes of no use activity. This may still be no problem for the protocols.

The following last LoA has at least the same requirements as previous requirements.

5.1.4 NIST LoA 4

With LoA 4 NIST limits the use to one type authenticator if biometrics authentication is desired. The NIST describes the authenticator type as a multi-factor cryptographic device and specifies specific requirements for those authenticators. Embedded software has to be under control of the manufacturer or from the relying party. This is technically reachable with the authentication protocols.

Another requirement is that the biometric samples has to be overwritten in memory immediately after an authentication, which should also be possible. This LoA also requires users to do an enrolment in person, in another words somebody has to check that the right person enrols with his own biometric. Furthermore the authenticator has to meet the requirements of FIPS 140-2 physical level 3. This includes that the hardware has to be tamper resistant. This means that it is not possible to open the hardware and if it certainly can all stored data has to be wiped. This is a little bit outside the scope of the authentication protocols because it concerns the hardware. However the UAF protocol recommends to use a Trusted Execution Environment, Secure Elements or Trusted Plat-

5.2 eIDAS LoA requirements

The eIDAS requirements roughly One of the general requirements is that personal user data that is stored on the device should be secured and protected against loss. In the UAF specifications is specified that data should be protected, but is not further specified. The BOPS protocol requires encryption of the data on a mobile device. From the substantial level and higher multi-factor authentication is required as well as replay attack resistance. The high LoA requirement specifies the tamper resistant requirement. Also identity data needs to be verified by an authoritative source. This can be any organisation that is nationally trusted to provide valid data, which is in practice comparable to the in-person verification requirement of the NIST. Also a tamper resistance comparable to the NIST requirement is specified. A summary is given in table 3.

6. CONCLUSION

Technically the first LoA levels and their requirements of the NIST and eIDAS can all be met with the FIDO UAF and BOPS protocols. The last LoA level by the NIST as well by eIDAS is constraint because of the in-person requirement. The ability of using those protocols on existing mobile device is also not possible because of the tamper resistant hardware requirement. Recommendations regard-
ing authentication protocols on mobile devices cannot evidently be given based on this results. The next section will discuss this.

7. DISCUSSION

Whether mobile devices are ready for biometric authentication can be called into question. The eIDAS documents mentions that there are possibilities to use a ‘inherent authentication’, where also biometrics belong to, but nowhere are requirements or guidelines specified about the subject. This fact in itself may say something about how mature biometric authentication is. NIST documents do however have specific biometric requirements. Public recommendations do even recommend increased support for Biometrics [1].

Hardware and software of mobile devices will eventually be better and better. The trusted executed environment in combination with the FIDO protocol from TrustZone for example are making successes [3]. Expected is that there will be no limitations concerning hardware or software in the future and that the biometric specific techniques will be the bottleneck. Current verification performances on faces obtained from controlled images are a FRR of 0.3% by a FAR of 0.1% [8]. This implies that is cannot meet the requirement of a 1 in 1000 EER that the NIST specifies. The best verification performances on fingerprints from the FVC ongoing are better with an FRR of 0.032% by a FAR of 0.1%. Those figures are a huge improvement compared to where biometric verification one started but are still not perfect in comparison to other verification techniques as passwords. Also liveness detection rates are far from perfect [11].

8. REFERENCES