Avrupa Bilim ve Teknoloji Dergisi
Sayı 23, S. 22-30, Nisan 2021
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 23, pp. 22-30, April 2021
Copyright © 2021 EJOSAT
Research Article

Protecting Mobile Service User Identity by Adding Additional Security Layer

Busra Ozdenizci Kose[1*], Onur Buk[2], Hacı Ali Mantar[3], Vedat Coskun[4], Utku Erdemir[5]

[1*] Gebze Technical University, Faculty of Business Administration, Kocaeli, Turkey (ORCID: 0000-0002-8414-5252), busraozdenizci@gtu.edu.tr
[2] Turkcell Technology, İstanbul, Turkey, onur.buk@turkcell.com.tr
[3] Istanbul Technical University, Faculty of Computer and Informatics Engineering, İstanbul, Turkey (ORCID: 0000-0002-1066-9942), hamantar@itu.edu.tr
[4] Beykent University, Faculty of Engineering and Architecture, İstanbul, Turkey (ORCID: 0000-0003-3052-9821), vedatcoskun@beykent.edu.tr
[5] Beykent University, Faculty of Engineering and Architecture, İstanbul, Turkey (ORCID: 0000-0003-0273-0501), 160313037@student.beykent.edu.tr

(First received 30 November 2020 and in final form 26 February 2021)

(**DOI:** 10.31590/ejosat.833433)

ATIF/REFERENCE: Ozdenizci Kose, B., Buk, O., Mantar, H. A.. Coskun, V. & Erdemir, U. (2021). Protecting Mobile Service User Identity by Adding Additional Security Layer. *European Journal of Science and Technology*, (23), 22-30.

Abstract

Today, various common identity systems (e.g. Facebook Login, Google Connect, Apple ID) are used to improve operational efficiency for service providers and provide an easier authentication method in web or mobile services for users. Almost all common identity systems focus on delivering seamless user experience while proving user identity securely to the service provider. In particular, the use of common identity systems with a high security level is becoming a more important requirement on smartphones. In this context, MNOs (Mobile Network Operators) are considered as an important actor in providing common identity services, as they have strong GSM capabilities. Currently, it is possible to see many identity management solutions -based on OpenID Connect and Mobile Connect standards- from MNOs which are used for authentication in mobile applications of service providers. However, existing solutions generally does not provide very high level of assurance in the asserted digital identity. With advancements in value-added mobile services and increasing security requirements; there is a need for common identity systems that provide higher levels of assurance (i.e., particularly LoA4), strong authentication and non-repudiation services for service providers and users. This study presents the development and implementation of a multi-factor authentication method for mobile services based on Mobile Connect and OpenID Connect standards. The designed model includes the usage of three identity -knowledge, ownership, biometric- factors of user in order to access sensitive mobile services on the smartphone. The system development and testing studies were systematically presented based on the functional requirements. The realization and deployment of the proposed model by MNOs could play an important role in the development of mobile services that require a high level of assurance in the future.

Keywords: OpenID Connect, Mobile Connect, Identity, LoA4, Multi-Factor Authentication.

Yeni Bir Güvenlik Katmanı Ekleyerek Mobil Hizmet Kullanıcısı Kimliğinin Güvenliğini Sağlam

Öz

Günümüzde, servis sağlayıcılar için operasyonel verimliliği artırmak ve kullanıcılar için web veya mobil servislerde daha kolay bir kimlik doğrulama yöntemi sağlamak için çeşitli ortak kimlik sistemleri (örn. Facebook Login, Google Connect, Apple ID) kullanılmaktadır. Tüm ortak kimlik sistemleri, servis sağlayıcıya kullanıcı kimliğini güvenli bir şekilde kanıtlarken kesintisiz ve sorunsuz kullanıcı deneyimi sunmaya odaklanır. Özellikle akıllı telefonlarda, yüksek güvenlik seviyesine sahip ortak kimlik sistemlerinin kullanılması daha önemli bir gereklilik haline gelmektedir. Bu bağlamda, MNO'lar (Mobil Şebeke Operatörleri), güçlü

[*] Corresponding Author: busraozdenizci@gtu.edu.tr

GSM yeteneklerine sahip oldukları için ortak kimlik hizmetleri sağlamada önemli bir aktör olarak kabul edilmektedir. Şu an, servis sağlayıcıların mobil uygulamalarında kimlik doğrulama için kullanılan ve MNO'lar tarafından sağlanan OpenID Connect ve Mobile Connect standartlarına dayalı birçok kimlik yönetimi çözümünü görmek mümkündür. Fakat mevcut çözümler genellikle ileri sürülen dijital kimlik konusunda çok yüksek düzeyde bir güvence sağlamamaktadır. Katma değerli mobil hizmetlerdeki gelişmeler ve artan güvenlik gereksinimleri ile, servis sağlayıcılar ve kullanıcılar için daha yüksek düzeyde güvence (özellikle LoA4), güçlü kimlik doğrulama ve inkar etmeme hizmetleri sağlayacak ortak kimlik sistemlerine ihtiyaç vardır. Bu çalışma, Mobile Connect ve OpenID Connect standartlarına dayanan, mobil hizmetler için birçok faktörlü kimlik doğrulama yönteminin geliştirilmesini ve uygulanmasını sunmaktadır. Tasarlanan model, akıllı telefondaki hassas mobil hizmetlere erişmek için kullanıcının üç kimlik -bilgi, sahiplik, biyometrik- faktörünün kullanımını içerir. Fonksiyonel gereksinimlere göre sistem geliştirme ve test çalışmaları sistematik olarak sunulmuştur. MNO'lar tarafından önerilen modelin gerçekleştirilmesi ve hizmet sunulması, gelecekte yüksek düzeyde güvence gerektiren mobil hizmetlerin geliştirilmesinde önemli bir rol oynayabilir.

Anahtar Kelimeler: OpenID Connect, Mobile Connect, Kimlik, LoA4, Çok Faktörlü Kimlik Doğrulama.

1. Introduction

Today, various common identity systems are used by service users in order to have easier password management on web or mobile services and to prove its identity to the service provider. Facebook Login, Google Connect, Apple ID are widely and commonly used examples. The main goal of common identity systems is to create an identity information at a service provider of common identity that can be used later for authentication of user in other web or mobile services. In order to use this authentication service, user first needs to register for a common identity system, and then user can benefit from the common identity system on any other web or mobile service that is part of the ecosystem. By this way, user does not necessary to register and enter a separate username and password - and even other personal information - for each service, to remember each password separately, and to change the password frequently.

However, today most of common identity systems are not suitable for web services (e.g., e-government services) that need high security in terms of non-repudiation of user or action. The common identity based solutions on web platforms generally use a username, password and sometimes mobile phone number in order to authenticate the user (Wang et al., 2012). According to the ISO/IEC 29115 Entity Authentication Assurance Framework (2013), such implementations generally refers to a low or medium level of assurance (LoA). Furthermore, the use of common identity systems for mobile based services with very high security level is becoming an important requirement. With the widespread adoption of the mobile technologies, many value added services can be provided for users on smartphones with rich content. In this context, MNOs (Mobile Network Operators) all over the world are recognized as an important actor for providing common identity services since they have strong GSM capabilities.

GSMA (GSM Association) has defined the Mobile Connect standard for the authentication service for mobile ecosystem that can be provided by MNOs based on OpenID Connect and OAuth 2.0 protocols (OpenID Connect, 2014; Mobile Connect, 2020). Mobile Connect offers a trusted way for mobile users to share sensitive data and undertake transactions with confidence (GSMA, 2020). The required API mechanisms are introduced by Mobile Connect standard in order to request a common identity service from relevant MNO. However, the methods of user authentication process by MNO have been left to the authority and responsibility of corresponding MNO. This flexibility enabled each MNO to produce various solutions with different LoA and security in a short time. Similarly, existing Mobile Connect based solutions does not provide very high level of assurance; particularly LoA4. It is evident that there is an urgent need for a common identity system that provide higher level of assurance and security for service providers, as well as for users.

For this purpose, a novel multi-factor authentication mechanism for mobile services -named as TrustedID system- is proposed based on Mobile Connect standard and OpenID Connect standard. The proposed system uses biometric data (e.g., fingerprint) to access various services on the smartphone by taking advantage of the superior capabilities of smartphones. Unlike the traditional, SMS or SIM based authentication methods, the proposed model provides higher level of assurance and security; in other words LoA4. The proposed TrustedID system is also supported by Turkcell Technology A.S. and TUBITAK (The Scientific and Technological Research Council of Turkey) under 1505 Program. This multi-factor authentication system for mobile services and mobile users supports new value added services development as well as mobile ecosystem advancement. In our previous study (Kose et al., 2020), the system analysis and design considerations (i.e., preliminary studies, system context, functional requirements with process flows) of proposed system have been presented clearly.

This paper aims to demonstrate and highlight the development and implementation issues of the proposed multi-factor authentication system. The functional requirements of the system are realized and tested depending on developed business scenarios. Accordingly, rest of this paper is organized as follows: Section II highlights a brief information about ISO/IEC 29115 and Mobile Connect standards; system components and system development considerations. Afterwards, Section III presents the implementation results of functional requirements of TrustedID. Finally, the study is concluded and further work is emphasized in Section IV.

2. Material and Method

2.1. Multi-Factor Authentication, ISO/IEC 29115 Standard

Authentication is the provision of assurance in the claimed identity of an entity (ISO/IEC 29115, 2013). Each authentication mechanism benefits from one or more factors of the user; a strong authentication mechanism should use at least two factors of user (Kose et al., 2020). Today, three factor groups are available for authentication of a user (Ometov et al., 2018):

- Knowledge factor as something the user knows, for example PIN data, username/password data, security question;
- Ownership factor as something the user has, for example smartphones, SIM cards with mobile number;

- Biometric factor as something the user is, for example biometric (fingerprint, face recognition etc.) data.

Two-Factor Authentication (2FA) uses knowledge factors and ownership factors; whereas Multi-Factor Authentication (MFA) mainly uses biometric factors. Multi-Factor Authentication (MFA) aims to provide a higher level of safety and facilitate continuous protection of computing devices as well as other critical services from unauthorized access by using more than two categories of credential (Ometov et al., 2018; Petsas et al., 2015; Harini, 2013; Schneie, 2005).

The ISO/IEC 29115 Entity Authentication Assurance Framework (2013) standard presents four levels of assurance (LoA) for entity authentication. Each LoA describes the degree of confidence in the processes leading up to and including an authentication. The defined LoA levels are as follows:

- LoA1 as little or no confidence in the asserted digital identity;
- LoA2 as some confidence in the asserted digital identity, used frequently for self-service applications;
- LoA3 as high confidence in the asserted digital identity, used to access protected data;
- LoA4 as very high confidence in the asserted digital identity, used to access highly protected data.

Selection of the appropriate LoA is performed by service providers and is based on a risk assessment of the transactions or services for which the entities will be authenticated. Risk assessment outcomes are essential factors in selecting the most appropriate assurance level. ISO/IEC 29115 (2013) assesses the impact levels and maps them to LoA levels as shown in Table 1. This mapping helps service providers in determination of what LoA they require. For example, since LoA4 provides very high assurance in the asserted digital identity's accuracy; in case of authentication errors, serious unrecoverable financial loss to any party or severe long-term damage to the standing or reputation of any party may occur; or the negative impacts for personal safety or severe injuries may happen.

2.2. Mobile Connect Standard

GSMA (GSM Association) has provided Mobile Connect standard for the authentication service that can be provided by MNOs (GSMA, 2020). Mobile Connect standard by GSMA is based on OpenID Connect and OAuth 2.0 protocols. OAuth 2.0 Authorization Protocol is the access and sharing of the information (owned by Resource Owner and managed by Resource Provider) by the service provider under control of authentication server (Hardt, 2012); whereas OpenID Connect Protocol includes the authentication process of the user (OpenID Connect, 2014). Today more than 50,000 service providers use OpenID Connect based authentication services of such as Google, Facebook, Twitter, Yahoo, Microsoft. In this regard, Mobile Connect standard based solutions can be used by mobile services of service providers.

Mobile Connect standard presents two main APIs (Application Programming Interface) over HTTPS (Hypertext Transfer Protocol Secure) protocol. Discovery API is implemented by GSMA API Exchange platform. This API checks which MNO is being used by the application and whether Mobile Connect service is available (Mobile Connect, 2020). Mobile Connect API is the authentication API implemented by MNO (i.e., the provider of the Mobile Connect service). It allows users to verify themselves using their Mobile Connect accounts. As shown in Figure 1, a typical Mobile Connect based authentication process of a user is as follows.

Table 1 : Potential impact at each LoA (ISO/IEC 29115, 2013)

Potential impact of authentication errors	**LoA1**	**LoA2**	**LoA3**	**LoA4**
Inconvenience, distress or damage to reputation	Minimum	Moderate	Substantial	High
Financial loss (damage) or agency liability	Minimum	Moderate	Substantial	High
Harm to the entity, its programs, or public interests	-	Minimum	Moderate	High
Unauthorized release of sensitive information	-	Moderate	Substantial	High
Personal safety (injury, death etc.)	-	-	Minimum-Moderate	Substantial-High
Civil or criminal violations	-	Minimum	Substantial	High

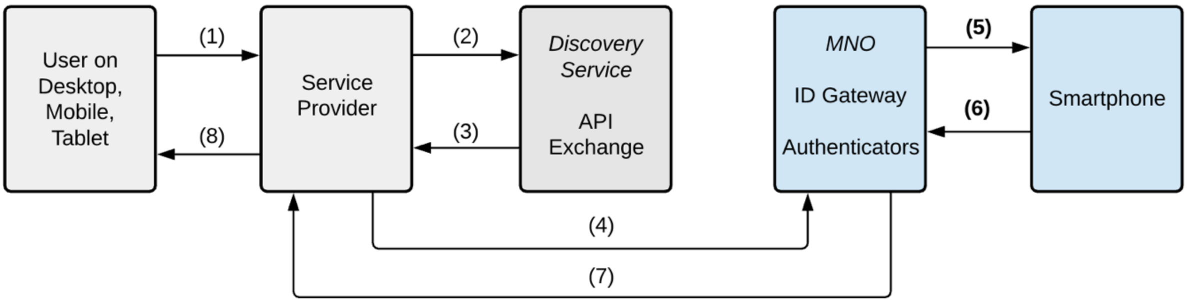


Figure 1: Mobile Connect Standard (Mobile Connect, 2020)

Step (1): When user chooses Mobile Connect connection on the login screen of service provider application, the server of service provider receives the relevant request.

Step (2): The server of service provider requests the mobile operator (i.e., MNO) identification information -that user is connected to- from Mobile Connect system.

Step (3): Mobile Connect server detects the mobile operator information of user with the help of Discovery API and notifies the application (i.e., service provider server).

Step (4): Service Provider requests authentication from the mobile operator of user with the help of the Mobile Connect profile and OpenID Connect protocol.

Step (5): MNO starts the authentication process with the help of the Mobile Connect API.

Step (6): User enters the identity/authentication information that is requested by MNO.

Step (7): The result of user's authentication (approval or rejection) is transferred to the service provider with the level of assurance provided.

Step (8): Service provider application approves or rejects the login request of user.

Articles 1, 2, 3, 4, 7, and 8 of the Mobile Connect protocol are implemented as standard by the relevant actor. However, the authentication method to be used in relation to Articles 5 and 6 is left to the initiatives of MNOs in order to provide flexibility and diversity (Mobile Connect, 2020; Kose et al., 2020). The authentication method used here determines LoA at the authentication stage. Table 2 provides examples of implementations for each LoA.

While the service provider requests authentication, it will notify MNO which LoA it demands. MNO also performs the authentication process -at least- at the requested LoA level, and reports the authentication level it uses (LoA) to the service provider along with the verification result. For example, Orange provides Mobile Connect solutions based LoA2 or LoA3 in France and Spain (Orange Developer, 2016; Orange Developer, 2017). As another example, Turkcell is providing a Mobile Connect service called as Fast Login in Turkey (Turkcell, 2020). The Fast Login authentication service is based on either SMS-OTP (One-Time-Password) or SIM-OTP through the SIM applet software as shown in Figure 2.

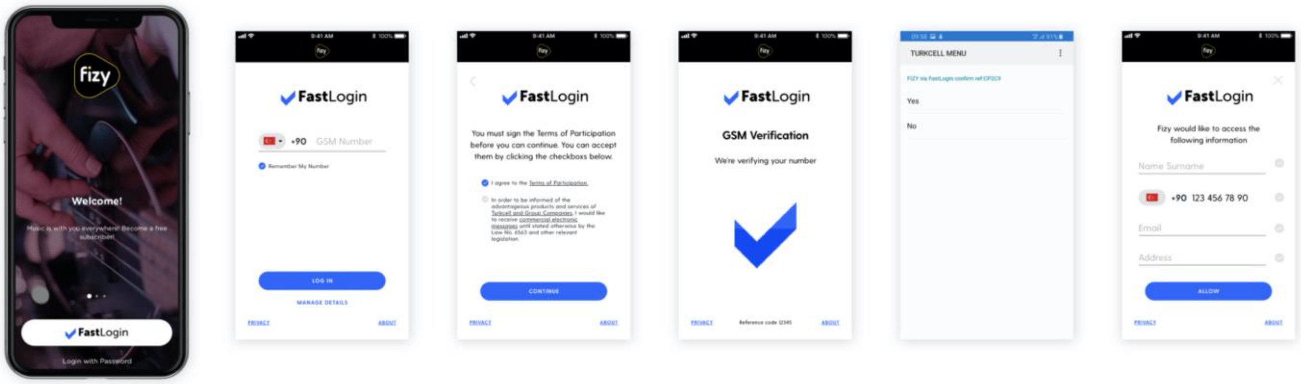
2.3. Proposed System Design and Development

The proposed multi-factor authentication method is based on OpenID Connect and Mobile Connect standards, and supports LoA4 security level in order to access various services -that require very high confidence in the asserted digital identity- on the smartphone. Unlike traditional (i.e., SMS or SIM-based authentication methods), the designed and developed TrustedID system incorporates the biometric as fingerprint data of user by taking advantage of superior capabilities of smartphones.

As shown in Figure 3, the ecosystem includes three main actors: MNO, service provider and user. MNO is the main actor who is the owner and manager of the SIM card, and also is TrustedID service provider. User is the owner of the smartphone, and also uses the TrustedID system. Service Provider is the actor who provides valuable services for the smartphone users. Service Provider Server represents the server application which provides a mobile service(s) to user. Service Provider Application is the mobile service which requires LoA4 and benefits from TrustedID authentication service. User will benefit from mobile services of diverse service providers who are contracted with TrustedID system.

Table 2: Mobile Connect authentication for each LoA

Level	**Application by Mobile Connect**
LoA1	When using Mobile Connect API, this level does not apply.
LoA2	User will be prompted and will need to respond on their mobile device. User gives an authorization from his mobile device to prove that she has control of both the SIM card and the mobile device.
LoA3	User will be required to enter a secret PIN or similar password from the mobile device that they agreed beforehand.
LoA4	LoA4 is similar to LoA3, but it adds the requirements of in-person identity proofing. This level requires usage of personal data especially biometric data to satisfy high risk transactions.



Music is with you everywhere! Become a free subscriber!

You must sign the Terms of Participation before you can continue. You can accept them by clicking the checkboxs below.

I agree to the Terms of Participation.

In order to be informed of the advantageous products and services of Turkcell and Group Companies, I would like to receive commercial electronic messages until stated otherwise by the Law No. 6563 and other relevant legislation.

We're verifying your number

Fizy would like to access the following information

Figure 2: Turkcell's Mobile Connect based Fast Login Service Example

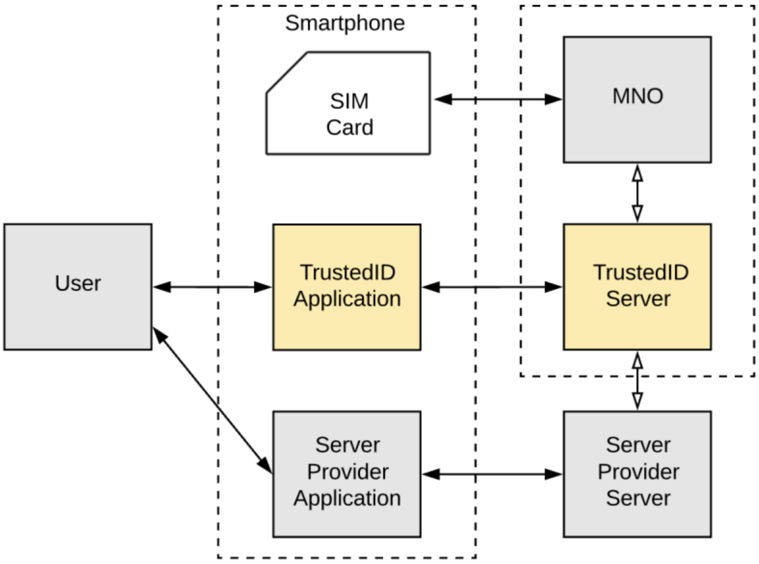


Figure 3: Context Diagram of TrustedID System (Kose et al., 2020)

The designed and developed TrustedID system has two parts: TrustedID (Client) Application and TrustedID Server Application. TrustedID Client Application is the part of the developed TrustedID system that runs on the Android smartphone. During system development, Android APIs using the Java programming language and also other tools were used within Android Studio software development tool. TrustedID Server Application is the part of the developed TrustedID system that runs on the server side. TrustedID Server application was developed by using PHP and MySQL on Eclipse IDE. In order to test TrustedID system, a test Service Provider Application (i.e., Android mobile application) with only TrustedID Login functionality has been developed. The test application was also developed on the Android Studio software development tool using Java programming language.

3. Results

In the previous study (Kose et al., 2020), two main processes of the proposed TrustedID system were designed and explained in detail: System Registration Process and System Usage Process. In accordance with the designed process flows and defined functional requirements, system registration and system usage processes of TrustedID system were developed and tested systematically in this study. This section presents implementation and test results with user interface results of developed mobile applications as well as results on MySQL database.

3.1. System Registration

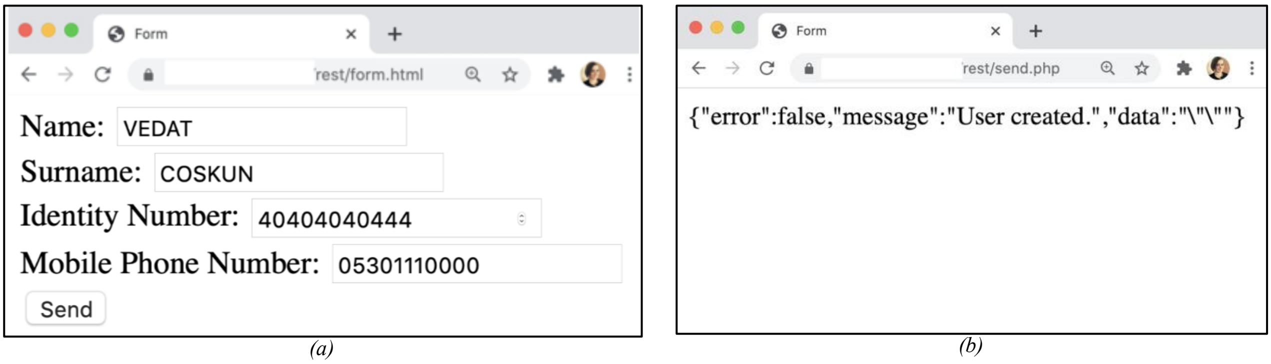
Step (1): User requests registration for TrustedID service. During system implementation, it was assumed that user goes to the store of MNO and makes an application for TrustedID service registration to the MNO officer. The credentials and mobile number of user are entered to the web client interface of TrustedID system for trigerring registration process as shown in Figure 4-a. The registration request is transmitted to TrustedID server and saved on database as shown in Figure 4-b.

Step (2): TrustedID server as MNO side initiates and performs mobile number verification. User opens and launches TrustedID application on the smartphone (Figure 5-a and Figure 5-b). Afterwards, user confirms the received SIM-OTP message on the smartphone as shown in Figure 5-c. TrustedID application sends SIM-OTP result to TrustedID server for confirmation. TrustedID server as MNO side validates the mobile number and registers the mobile number of user as first identification factor -something I have- as seen in database record Figure 8-a. TrustedID server informs TrustedID application about the result as seen in Figure 5-d.

Step (3): After mobile number registration, user registers the biometric data that will be used in TrustedID application. TrustedID application requests the fingerprint data identification from user as shown in Figure 6-a. User enters the fingerprint data (Figure 6-b). Android smartphone generates a key value (i.e., similar to a hash value) of the fingerprint data and TrustedID application transfers the key value to TrustedID server. TrustedID server saves the key data of user as the second identification -something I am- factor. TrustedID server informs TrustedID application about the result as shown in Figure 6-c and Figure 8-b. Accordingly, BiometricPromptHelper class is the main class in which biometric processes are carried out. It checks whether the device has biometric feature, saves new biometric data and performs biometric verification.

Step (4): After fingerprint registration, user registers the PIN data that will be used when launching TrustedID application. TrustedID application requests a four-digit PIN (password) from user (Figure 7-a). User sets a PIN through TrustedID application (Figure 7-b). TrustedID server registers the PIN data as the third identification factor -something I know- and informs TrustedID application about the result as shown in Figure 7-c and Figure 8-c.

Step (5): Finally, TrustedID server notifies TrustedID application that the new user has been successfully registered (Figure 7-d). After registration process, user can benefit from TrustedID service on contracted service provider applications. In this regard, we developed and tested the system usage perspective with a test Service Provider Application.



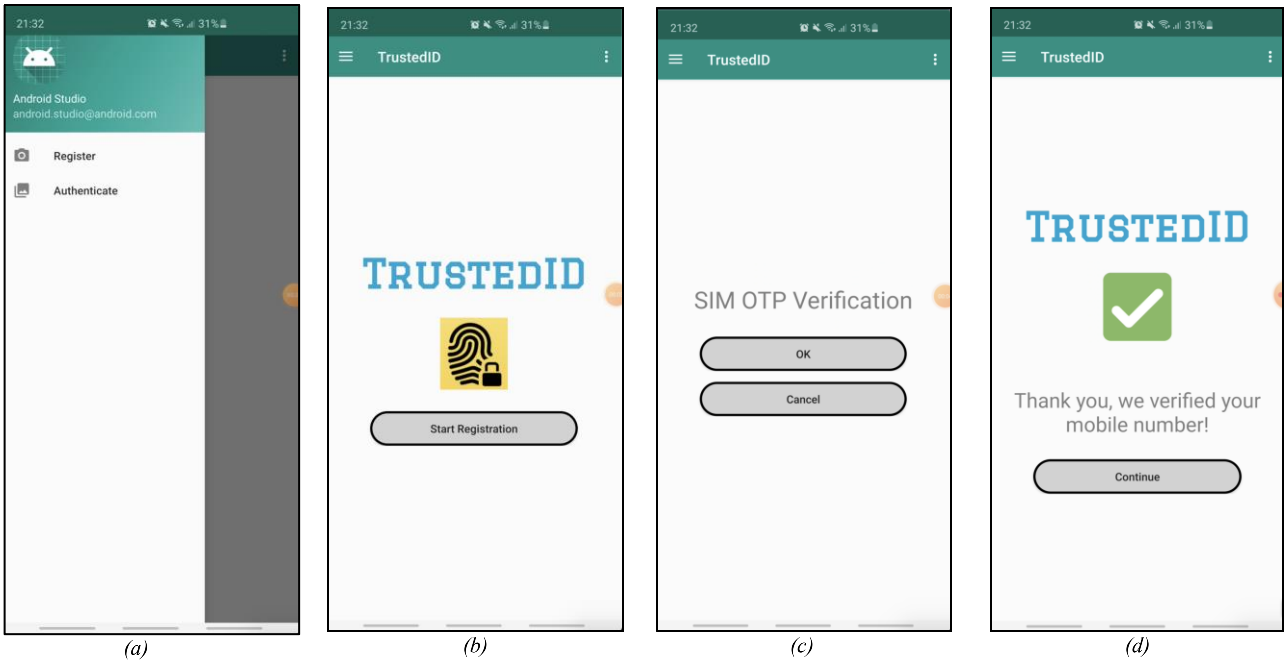
Name: VEDAT
Surname: COSKUN
Identity Number: 40404040444
Mobile Phone Number: 05301110000
Send

(a)

```
{"error":false,"message":"User created.","data":"\"\""}
```

(b)

Figure 4: Creating a TrustedID Service Record via Web Client Interface

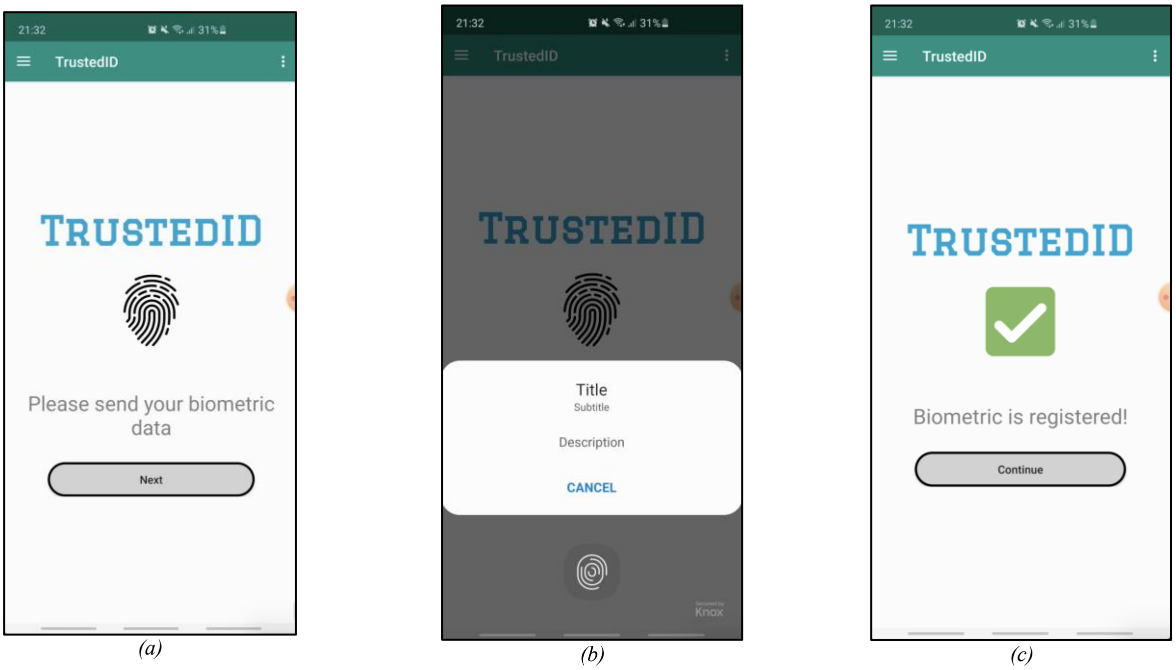


(a) (b) (c) (d)

SIM OTP Verification

Thank you, we verified your mobile number!

Figure 5: Mobile Number as Identity Factor Registration: Something I have

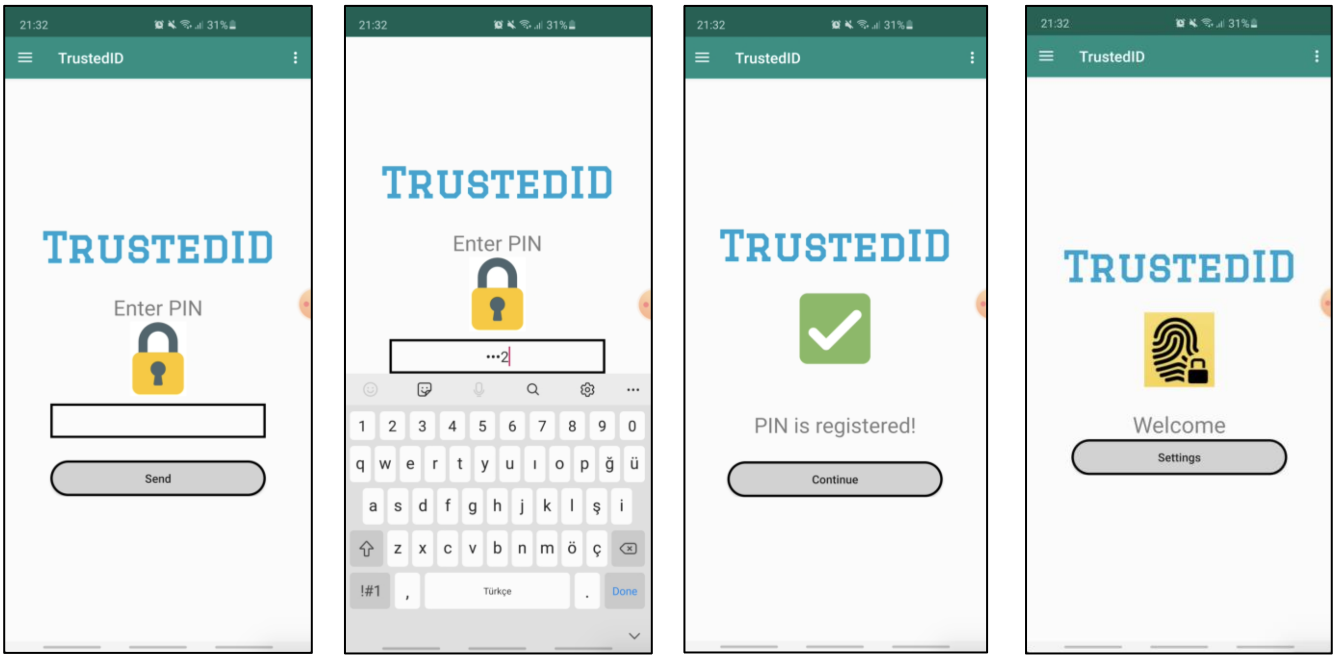


Please send your biometric data

Biometric is registered!

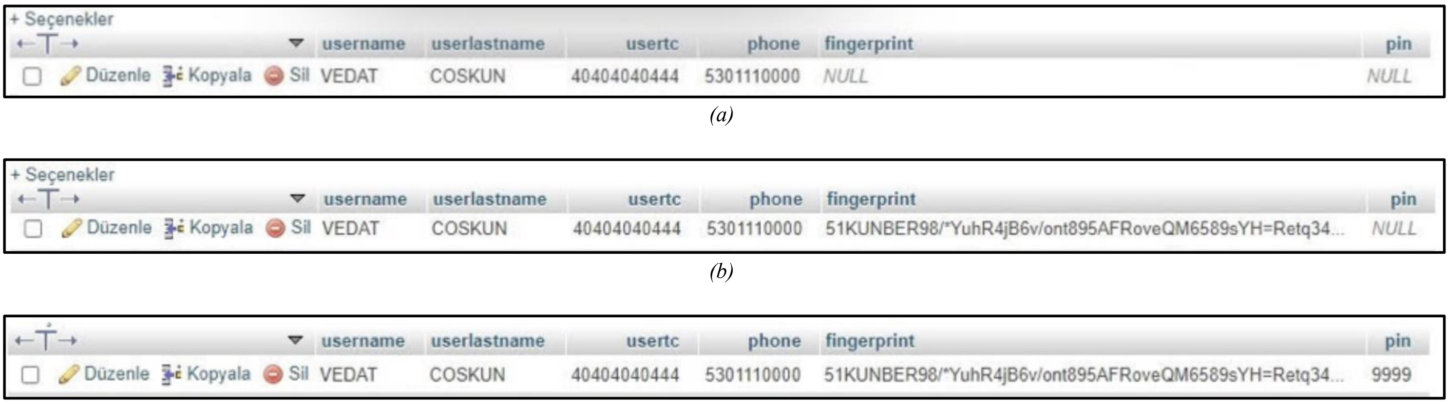
(a) (b) (c)

Figure 6: Biometric Data as Identity Factor Registration: Something I am



(a) (b) (c) (d)

Figure 7: PIN Data as Identity Factor Registration: Something I know



+ Seçenekler

←T→	username	userlastname	usertc	phone	fingerprint	pin
□ Düzenle Kopyala Sil	VEDAT	COSKUN	40404040444	5301110000	*NULL*	*NULL*

(a)

+ Seçenekler

←T→	username	userlastname	usertc	phone	fingerprint	pin
□ Düzenle Kopyala Sil	VEDAT	COSKUN	40404040444	5301110000	51KUNBER98/*YuhR4jB6v/ont895AFRoveQM6589sYH=Retq34...	*NULL*

(b)

←T→	username	userlastname	usertc	phone	fingerprint	pin
□ Düzenle Kopyala Sil	VEDAT	COSKUN	40404040444	5301110000	51KUNBER98/*YuhR4jB6v/ont895AFRoveQM6589sYH=Retq34...	9999

(c)

Figure 8: Registered Identity Factors on TrustedID Server

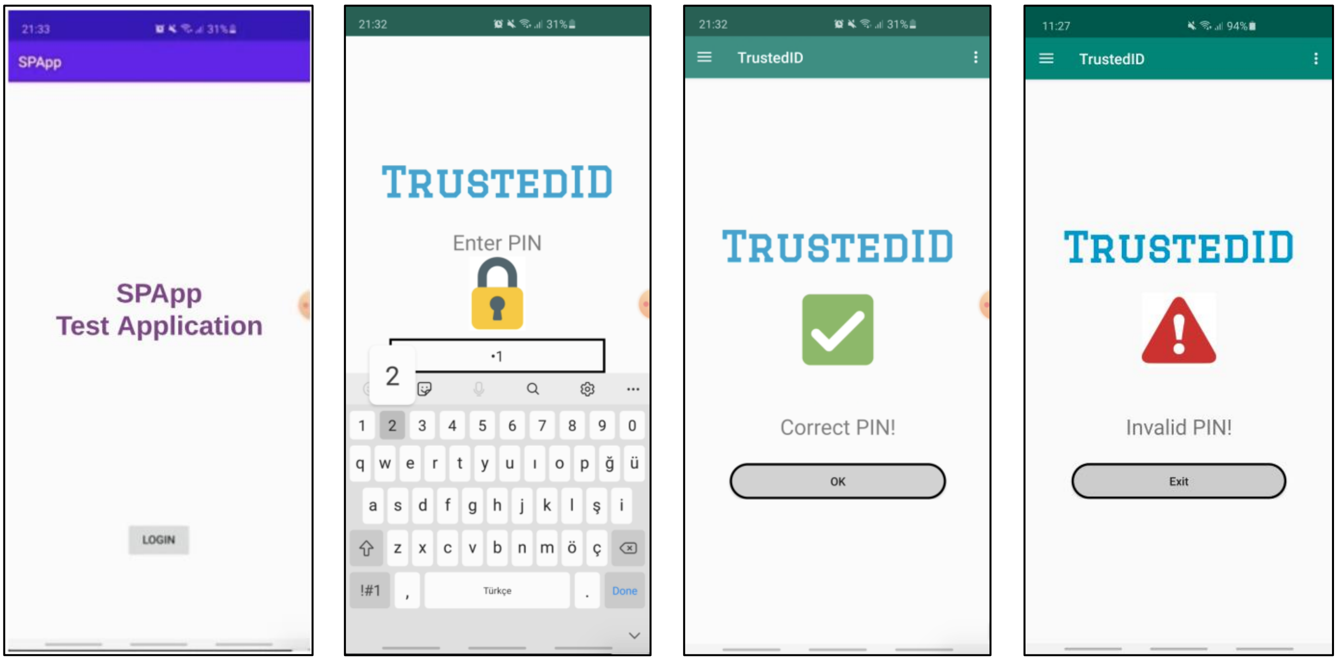
3.2. System Usage Process Flow

Step (1): User requests to use TrustedID login service on Service Provider Application (i.e., SPApp). User selects TrustedID authentication among the login options offered in the service provider application (Figure 9-a). TrustedID application on user’s smartphone launches.

Step (2): Firstly, the control of user’s PIN information is performed. TrustedID application requests the PIN value (Figure 9-b). User enters the PIN data (i.e., previously created for the TrustedID service). TrustedID server checks the sent information with the previously registered information. In case of a valid PIN entry (i.e., 9999 as a test input), the identity factor -something I know- of user is verified, and then user is informed (Figure 9-c). In case of an invalid PIN (i.e., 1122 as a test input), user is informed with an error message as seen in Figure 9-d.

Step (3): Afterwards, the mobile number of user is checked.TrustedID application requests the SIM-OTP service from the TrustedID server to verify the mobile number. TrustedID system initiates SIM-OTP application for the smartphone. User confirms the received message (Figure 10-a). In case of a valid SIM-OTP (e.g., pressing OK button as a test input), the identity factor -something I have- of user is verified, and then user is informed (Figure 10-b). In case of an invalid SIM-OTP (e.g., pressing Cancel button as a test input), user is informed with an error message as shown in Figure 10-c.

Step (4): Finally, the biometric information of user is checked. TrustedID application requests the fingerprint data from user (Figure 11-a). User enters the previously defined fingerprint data for TrustedID service (Figure 11-b). TrustedID application sends the key data generated by Android smartphone to the server. TrustedID server checks the registered data with the received information. In case of a valid biometric data, the identity factor -something I am- of user is verified, and user is informed (Figure 11-c). In case of an invalid fingerprint information, user is informed with an error message (Figure 11-d). After verification of all identity factors by TrustedID system, user accesses the requested Service Provider application successfully.



SPApp Test Application

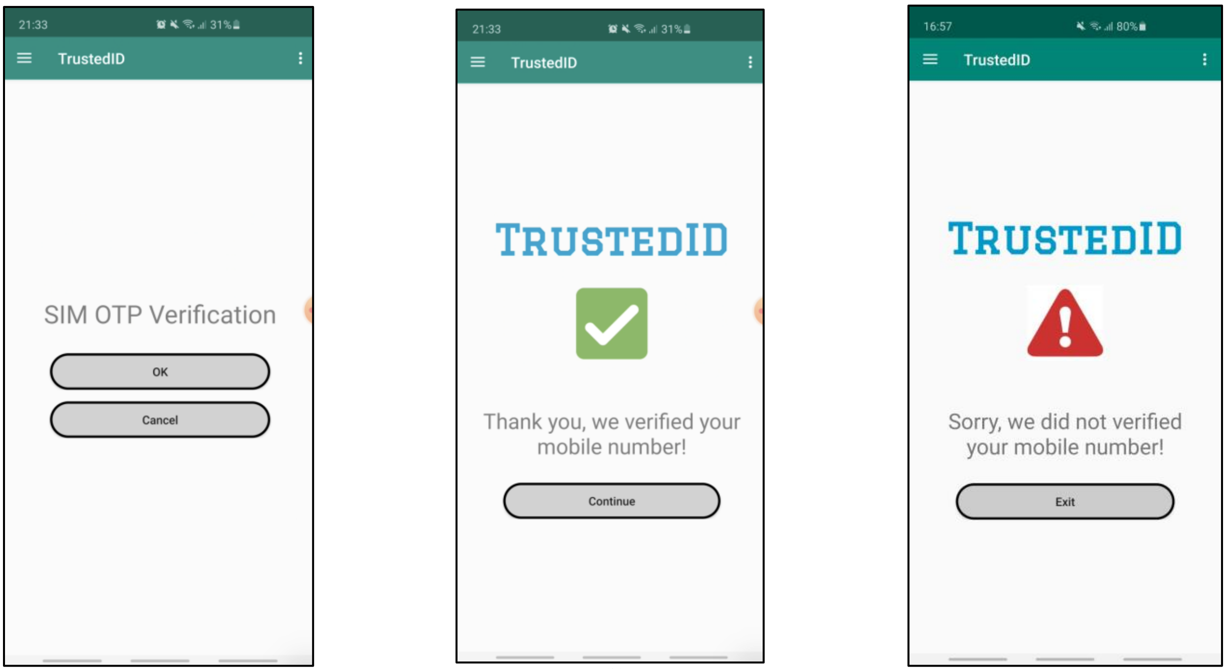
Enter PIN

Correct PIN!

Invalid PIN!

(a) (b) (c) (d)

Figure 9: TrustedID Login Request and PIN Identity Factor Verification



SIM OTP Verification

Thank you, we verified your mobile number!

Sorry, we did not verified your mobile number!

(a) (b) (c)

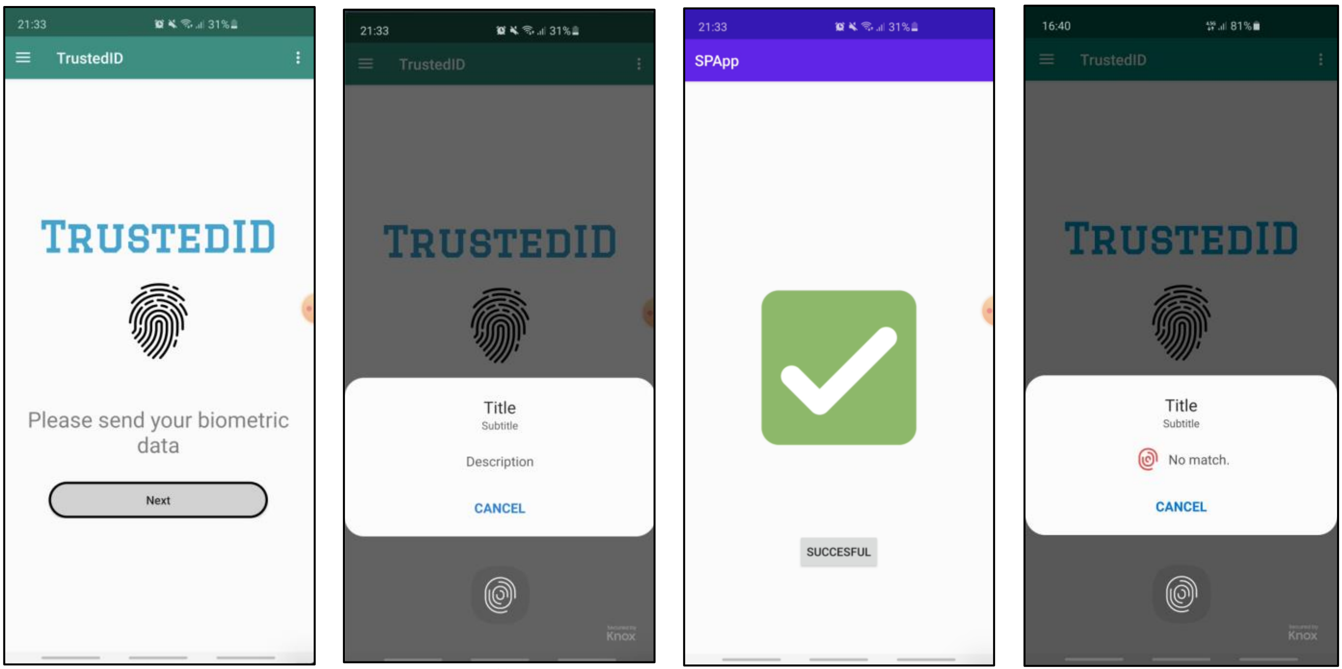
Figure 10: Mobile Number Identity Factor Verification

4. Conclusions

This paper presents the implementation details of a promising authentication system on Android smartphones. The prototype implementation results were explained through user interfaces of developed client mobile application. The designed functional requirements in the previous study (Kose et. al., 2020) regarding system registration and system usage were developed and tested systematically.

The proposed OpenID Connect based (i.e., also Mobile Connect based) authentication system aims to ensure a strong authentication mechanism by using three identity factors (i.e., multi-factor) of the user in order to access secure and sensitive mobile services on the smartphone. The required user identity factors within proposed model are SIM-OTP code for proving something I have, PIN like code for proving something I know and also fingerprint data for proving something I am. The proposed model adds biometric authentication layer as third factor to the existing OpenID Connect and Mobile Connect based solutions with an efficient, new business model design.

The developed mobile application provides a user-friendly and seamless user experience. Morover, the prototype implementation has provided an acceptable time performance and efficiency; it has been observed that the response time between the user's mobile application and the server application is less than five seconds.



(a) *(b)* *(c)* *(d)*

Figue 11: Biometric Identity Factor Verification

The subsequent work will focus on verification and integration of the system with real-world service applications. Also, usability analysis and evaluation of the proposed study can be performed with more comprehensive mobile applications. The security methods and encryption algorithms for data-at-rest and data-in-motion can be also studied depending on MNOs' requirements and capabilities. The realization and deployment of the proposed model by MNOs could play an important role in the development of mobile services that require very high level of assurance in the future.

5. Acknowledge

This work is funded by Turkcell Technology A.S. and TUBITAK (The Scientific and Technological Research Council of Turkey) under 1505 Program, Project no 5190045.

References

Apple Sign-In (2020). https://developer.apple.com/sign-in-with-apple/

Facebook Login (2020). https://developers.facebook.com/docs/facebook-login/

Turkcell (2020). Fast Login. https://hizligiris.turkcell.com.tr/en/fast-login/what-is-fast-login

Google Sign-In (2020). https://developers.google.com/identity

GSMA (2020). Mobile Connect, https://www.gsma.com/identity/mobile-connect.

Harini, N., & Padmanabhan, T. R. (2013). 2CAuth: A new two factor authentication scheme using QR-code. International Journal of Engineering and Technology, 5(2), 1087-1094.

ISO/IEC 29115 (2013). Information technology-Security techniques-Entity authentication assurance framework.

Kose, B. O., Buk, O., Mantar, H. A., & Coskun, V. (2020, October). TrustedID: An Identity Management System based on OpenID Connect Protocol. In 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-6). IEEE.

Mobile Connect (2020). https://mobileconnect.io/

Hardt, D. (2012). The OAuth 2.0 authorization framework (p. 6749). RFC 6749, October.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.

OpenID Connect (2014). http://openid.net/connect/

Orange Developer (2016). Mobile Connect Technical Guide, https://developer.orange.com/tech_guide/mobile-connect/

Orange Developer (2017). OpenID Connect Technical Guide, https://developer.orange.com/tech_guide/openid-connect-1-0/

Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015, April). Two-factor authentication: is the world ready? Quantifying 2FA adoption. In Proceedings of the eighth european workshop on system security (pp. 1-7).

Schneier, B. (2005). Two-factor authentication: too little, too late. Communications of the ACM, 48(4), 136.

Wang, R., Chen, S., & Wang, X. (2012, May). Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services. In 2012 IEEE Symposium on Security and Privacy (pp. 365-379).