UDC 004.056

IMPROVE MOBILE DRIVING LICENSE DATA TRANSFER SECURITY VIA BLE/WI-FI AWARE WITH UWB RANGING

A. LELIAK, A. ASTRAKHANTSEV
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Abstract *– A Mobile Driving License (mDL) solution, according to ISO 18013-5, is a digital representation of the information contained in a physical driver's license, including personal details, driving privileges, and vehicle class. The mDL solution is spreading rapidly worldwide, and countries are adopting this standard. The ISO 18013-5 specification covers most of the security concerns like protection against forgery, protection against cloning, protection against eavesdropping, and protection against unauthorized access. However, some gaps in a security model are present, which are related to device location. Both mDL reader and holder can be sure that an opponent device is placed right near them only while transferring documents via NFC because of the usage range of the NFC technology and the necessity of a physical tap. Data transfer using BLE and Wi-Fi Aware is more convenient for users in most cases as it doesn't require the physical closeness of two devices, and connection stability is much higher as it doesn't depend on a device placement by the user. On the other hand, data transfer using BLE or Wi-Fi Aware cannot guarantee that an opponent's device placement is in sight. This creates a possibility of performing a data transfer to a malicious opponent device located out of sight. Several solutions can address the reader/holder relative location issue for BLE and Wi-Fi Aware data transfer. Still, most don't cover all use cases or have significant drawbacks. Such solutions include biometric verification, visual session identifiers, and NFC authentication. To resolve the relative location issue for other use cases, this paper proposes UWB usage in fusion with BLE or Wi-Fi Aware to ensure that reader and holder devices are located in the expected place for use cases that don't involve NFC communication. The NFC communication can be avoided intentionally to increase data transfer stability or unintentionally as some holder devices can have no NFC technology support. Additionally, this paper proposes integrating the UWB messaging with the mDL session encryption to defend from MITM attacks and provide additional protection even for service messaging.*

Анотація *– Рішення Mobile Driving License (mDL) згідно з ISO 18013-5 — це цифрове представлення інформації, що міститься у фізичному водійському посвідченні, включаючи особисті дані, право водіння та клас транспортного засобу. Використання mDL швидко поширюється по всьому світу, і цей стандарт впроваджується в нових країнах. Специфікація ISO 18013-5 охоплює більшість питань безпеки, таких як захист від підробки, захист від клонування, захист від підслуховування та захист від несанкціонованого доступу. Але деякі прогалини, що пов'язані з розташуванням пристроїв, присутні в моделі безпеки. І зчитувач, і власник mDL можуть бути впевнені, що протилежний пристрій знаходиться безпосередньо біля них лише під час передачі документа за допомогою NFC через діапазон використання технології NFC і необхідність фізичного дотику пристроїв. Передача даних за допомогою BLE та Wi-Fi Aware у більшості випадків зручніша для користувачів, оскільки не вимагає фізичного наближення двох пристроїв, а стабільність підключення набагато вища, оскільки не залежить від розташування пристрою користувачем. З іншого боку, передача даних за допомогою BLE або Wi-Fi Aware не може гарантувати, що протилежний пристрій знаходиться в полі зору. Це створює можливість здійснити передачу даних на зловмисний пристрій, який знаходиться поза полем зору. Існує декілька рішень для вирішення проблеми відносного розташування зчитувача для передачі даних BLE та Wi-Fi Aware, але більшість із них або не охоплюють усіх випадків використання, або мають значні недоліки. Прикладами таких рішень є біометрична перевірка, візуальний ідентифікатор сеансу та NFC-автентифікація. Щоб вирішити проблему відносного розташування для інших варіантів використання, у статті пропонується використовувати UWB у поєднанні з BLE або Wi-Fi Aware, щоб гарантувати, що пристрої зчитування та власника mDL розташовані в очікуваному місці для випадків використання, які не включають NFC спілкування. Використання NFC можна уникати навмисно, щоб підвищити стабільність передачі даних, або ненавмисно, оскільки деякі зчитувачі можуть не підтримувати технологію NFC. Крім того, в роботі пропонується інтеграція обміну повідомленнями UWB із шифруванням сеансу mDL для захисту від атак MITM і забезпечення додаткового захисту навіть для обміну сервісними повідомленнями.*

I. Mobile Driving License overview

A Mobile Driving License (mDL) is a digital version of a traditional driver's license that can be stored and accessed on a mobile device, such as a smartphone or tablet. It is essentially a digital representation of the information contained in a physical driver's li-

cense, including personal details, driving privileges, and vehicle class. The concept of mDL aims to provide convenience and accessibility to drivers by allowing them to carry their driver's license on their mobile device rather than carrying a physical card. It may also offer additional features such as enhanced security measures, easily updating information, and integration with other digital services. mDLs are typically supported by specialized mobile apps or digital wallet platforms provided by government agencies or third-party service providers. Adoption of mDLs may vary by region or country, depending on regulatory approvals, infrastructure, and technological advancements [1].

Nowadays, several countries and regions are exploring or already implementing digital driver's licenses, but widespread adoption may still be in progress in many places. Several states in the U.S., such as Colorado, Delaware, Idaho, Louisiana, Maryland, and Wyoming, have either launched or piloted mobile driver's licenses. The American Association of Motor Vehicle Administrators (AAMVA) has been working on developing standards for digital driver's licenses, which could potentially lead to broader adoption across the country. Australia has been testing digital driver's licenses in select states, including New South Wales, South Australia, and Queensland. These digital licenses are available through dedicated mobile apps. The European Union has been discussing the potential for a European Digital Identity, including digital driver's licenses. Some member states, such as Estonia, already offer digital driver's licenses [2, 3].

While Mobile Driving Licenses offer convenience and accessibility, they also present specific security challenges that must be addressed to ensure the integrity and trustworthiness of the digital credential. Let’s consider the main security issues that can occur when using mDLs instead of physical documents. Initially, hackers may attempt to steal mDL credentials through various means, such as phishing attacks, malware, or hacking into insecure databases. One more issue related to counterfeiting and forgery – attackers may attempt to counterfeit or forge digital licenses. The security of the device used to store the mDL is crucial. Also, if the database or server storing mDL information is breached, sensitive personal data could be exposed to unauthorized parties. In addition, authentication risks, privacy concerns and interoperability issues need to be checked to decrease the security vulnerabilities.

Counterfeiting and forgery pose significant security risks [4, 5] for mobile driver's licenses (mDLs), just as they do for traditional physical licenses. Here's how these issues manifest in the context of mDLs. First of all, it is a digital replication. Malicious actors may attempt to replicate the digital data of an mDL to create counterfeit copies. This could involve extracting and reproducing the digital signature or other authentication features. Secondly, some mDLs may use QR codes or barcodes for quick verification and counterfeiters might try to tamper with these codes to produce fake licenses that appear legitimate when scanned. One more issue related to data manipulation – forgers may attempt to manipulate the data within the mDL to change information such as the name, date of birth, or license expiration date. Also, just like physical cards, mDLs could be subject to cloning attempts where the digital information is copied onto another device or card. In addition,

if the mDL uses digital signatures for authentication, fraudsters may attempt to forge these signatures to make the fake licenses appear authentic.

To address these security issues, robust encryption and authentication mechanisms are essential.

Most of information protection issues from the above analysis can be covered by usage of features like biometric authentication, tamper-proof digital signatures, and secure data transmission protocols to prevent counterfeiting and forgery attempts. But such solutions don't cover location identification of the mDL holder or reader device, therefore, this paper sets the urgent task of developing a solution to solve this threat. To resolve this problem, it's necessary:

- analyze the existing solutions and identify their drawbacks;
- propose a new approach to the solution;
- compare it with existing analogues.

II. Current solutions overview

Mobile driving licenses implementation is defined in the ISO 18013-5 specification. ISO 18013-5 is a specification that pertains specifically to mobile driver's licenses (mDLs). It provides guidelines and requirements for the design, implementation, and security of mDLs to ensure interoperability, security, and privacy. This specification defines the data elements and data structures that should be included in an mDL and includes personal information such as the driver's name, date of birth, address, license number, and any additional relevant information. Regarding the questions of information security in ISO 18013-5 described requirements for cryptographic algorithms, digital signatures, and secure communication protocols to prevent counterfeiting, tampering, and unauthorized access. In besides, it contains guidelines for data minimization, consent mechanisms, and restrictions on using and disclosing mDL data. Also standardized formats and protocols for exchanging mDL data between different stakeholders are recommended. For all protocols and described solutions practical guidelines for implementing mDL systems are included (hardware and software requirements, user interfaces, and user authentication mechanisms among others).

Overall, ISO 18013-5 serves as a comprehensive standard for developing and deploying mDL systems, ensuring that they meet the highest standards of security, interoperability, and privacy protection.

The mDL transaction flow is described in Fig. 1. Only device retrieval is considered for this paper, as server retrieval implies that connection between the mDL reader and mDL holder is performed over the internet, and there is no requirement for the physical presence of both flow participants in the same location. If device retrieval is used, either Bluetooth Low Energy (BLE), Near Field Communication (NFC) or Wi-Fi Aware can be used to retrieve the information [6].

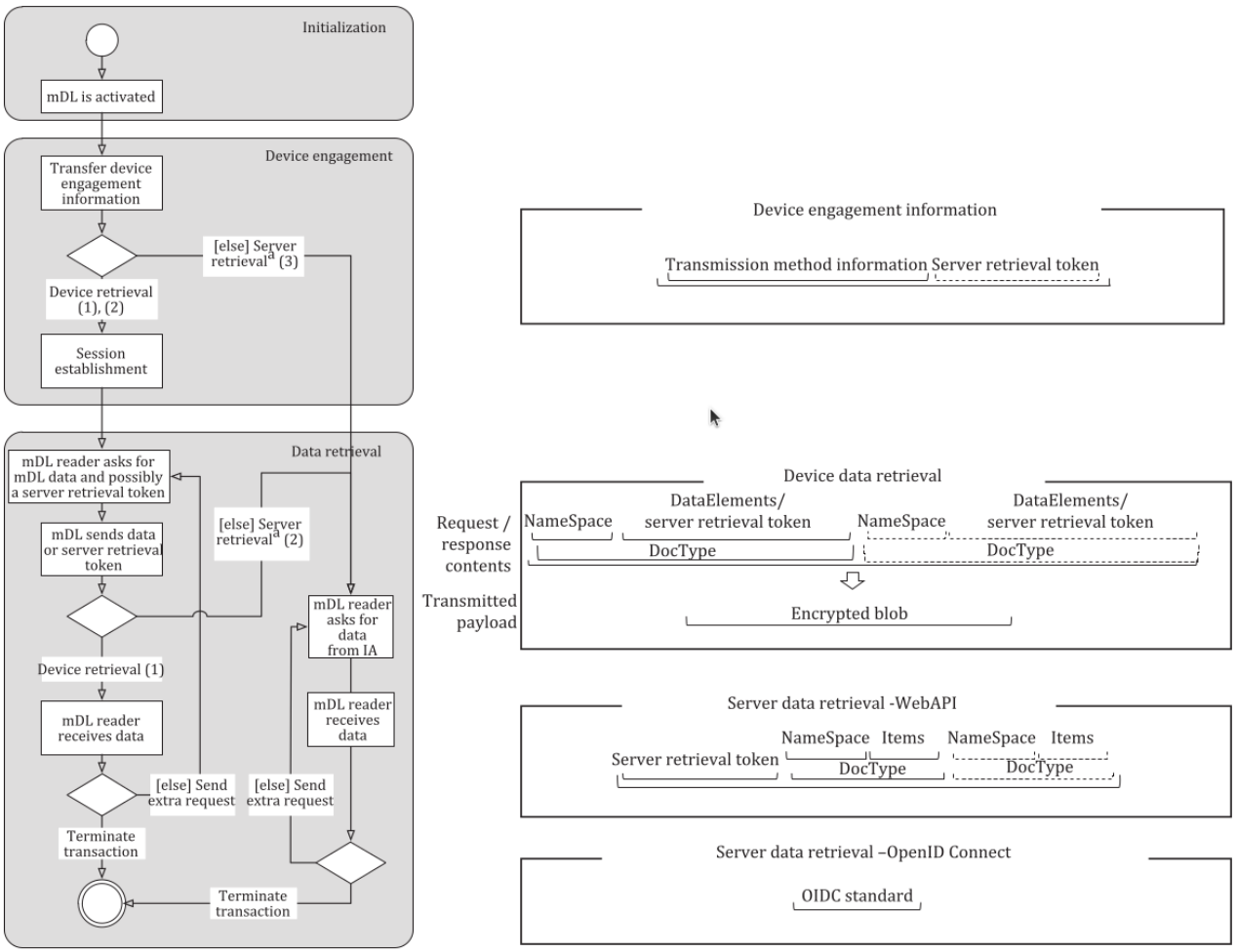

Fig. 1. mDL transaction flow

According to the ISO 18013-5 specification, the authenticity of both the holder and reader is ensured by security design. Communications between mDL and mDL reader are encrypted and authenticated. Device engagement uses a separate communication channel to mitigate the risk of Man-in-the-Middle (MITM) attacks. In addition, the mDL reader can detect MITM attacks by validating the anti-cloning signature or message authentication code, which is created using a key for which the public part is signed by the IA in the mobile security object. If mdoc reader authentication is used, the mDL can detect MITM attacks before returning any data. Server retrieval uses TLS for encryption to further protect against eavesdropping and MITM attacks [7].

But general mDL security design doesn't provide a way to ensure that the mDL reader device is placed right near the mDL holder device, e.g. in the officer's hands, but not in the another room. This creates a possibility for malicious reader to read holder's device engagement data and then transfer it to another reader, which is visually hidden from the holder for the actual mDL data transfer. The same applies to the malicious holder, which can show the device engagement information from another visually hidden holder and present an mDL from another device. If malicious opponent device is located in the BLE or Wi-Fi Aware access range, the mDL can be transferred to/from a device,

which is not expected to participate in this transaction. This issue is applicable for BLE and Wi-Fi Aware only as NFC data transfer requires close proximity of both devices. The solution to this problem is possible in such ways as biometric verification (fingerprint scanning, facial recognition), visually displayed dynamic session identifier or NFC authentication. Biometric verification is difficult to replicate and it is providing a high level of security against forgery [8, 9]. NFC authentication can be used to verify the authenticity of the mDL and prevent unauthorized access [10, 11]. If device engagement is performed via NFC, some unique device ID can be added. Alternatively, the whole data transfer flow can be done via NFC channel, which is allowed by ISO 18013-5. All existing solutions do not resolve the relative location verification problem, do not cover all use cases possible or have accompanying complexities.

In case of using biometric verification, this approach has a set of the issues described below. Biometric data collection and usage requires explicit user consent, which complicates the user enrollment procedure. Also biometric verification doesn't cover the reader verification, as it's not expected that the same reader device will be used by a single officer. Besides this, implementing of biometric verification systems can be costly and complex, requiring specialized hardware, software, and infrastructure. Also need to take into account that the accuracy and reliability of biometric systems are not stable and biometric characteristics may change over time due to injuries or medical procedures and it affecting the accuracy and reliability of system.

However, the use of biometric systems still outweighs the existing disadvantages. To increase the attractiveness of this method, you should explore cloud-based biometric solutions and software-as-a-service (SaaS) models to reduce upfront costs and simplify deployment and perform biometric reader verification also using independent system, which can be trusted by a document holder.

Using of visually displayed dynamic session identifier is not convenient due to problems with low-cost or bare-metal devices (screen can be absent). Also there is a high chance of human error during the visual comparison of some letters and symbols in the session identifier on two devices screens. In addition, the visual representation of anything on the screen is hard to standardize because of multitude of possible implementation. These problems can be partially solved by unifying fonts, but they are not fully resolved at this time, which limits the using of this approach.

The NFC authentication is a viable option and it addresses the main part of the relative location verification problem. Nevertheless, not all devices can support the NFC technology, so alternative method should exist. The typical issues of this approach is fragile of NFC connection (it requires relatively stable device placement in a proximity location during the data transfer phase), the NFC data transfer speed is slower that BLE or Wi-Fi Aware and NFC communication is susceptible to interference from environmental factors.

Using an external NFC reader with more power and better electromagnetic shielding can help solve interference problems.

III. Proposed solution

Ultra-Wideband (UWB) technology is widely recognized for its precision in indoor positioning, boasting accuracy levels down to the centimeter. Its resistance to multipath interference ensures reliable performance in environments where signals may bounce off surfaces. With low power consumption, UWB devices are ideal for battery-operated applications like wearable trackers and IoT sensors. The technology's compliance with regulatory standards simplifies its deployment across different regions. Furthermore, UWB's integration capabilities with other positioning technologies contribute to robust indoor positioning solutions, fostering its adoption across diverse industries.

Integration of Ultra-Wideband and Bluetooth Low Energy technologies for indoor positioning combines the strengths of both to create robust and versatile positioning systems. UWB provides high-precision location data with centimeter-level accuracy, making it ideal for applications where precise positioning is crucial. On the other hand, BLE offers advantages such as low power consumption, cost-effectiveness, and widespread compatibility with mobile devices. The integration of UWB and BLE technologies for indoor positioning offers a balanced approach that combines high accuracy, energy efficiency, and versatility, catering to diverse indoor positioning requirements across various industries.

Indoor localization using UWB and BLE has been an active area of research in last years. Leitch et al. [12] compared such indoor localization technologies as Wi-Fi, BLE, UWB, and IMU. Botler et al. [13] compared specifically BLE and UWB technologies and discussed their possible improvements. Bilge [14] evaluated the approach of enhancing BLE-based location estimation with UWB and have shown its advantages. Dagher et al. [15] provided an open experimental platform for ranging, proximity and contact event tracking using UWB and BLE.

Also, multiple solutions exist for using BLE and UWB fusion to solve a specific task, but none of them cover fully the problem stated in this paper. Kolakowski et al. [16] proposed the UWB/BLE tracking system for elderly people monitoring. System architecture from this paper is not applicable for the reader/holder relative location issue as they used anchor nodes spread through the target location, and mDL flow defines only two actors: reader and holder devices. To provide a standardizable solution, it should be self-sufficient as any helper infrastructure should be standardized as well as the solution itself. Kolakowski [17, 18], Zhang et al. [19] and Brunacci et al. [20] papers were concentrated on a dynamic location map creation using fingerprints and anchor nodes were also used. Also, none of these papers considered UWB messages encryption to avoid MITM attacks.

The proposed solution of the mDL relative location verification problem is to use UWB ranging right after the BLE or Wi-Fi Aware connection establishment to ensure that the opponent device is located near the target device and the target device owner can visually confirm the opponent device owner identity. This approach will cover use cases left for devices that do not support NFC communication and doesn’t have flaws of other approaches mentioned. Also, in the proposed solution the UWB messaging is encrypted by

mDL session encryption which provides the same level of MITM attacks protection as the whole mDL flow does.

The UWB integration to mDL flow is described on the Fig. 2. Current solution takes advantage of mDL session encryption mechanism [21], which specifies a way to derive a symmetric session key from ephemeral asymmetric keys for each transaction.

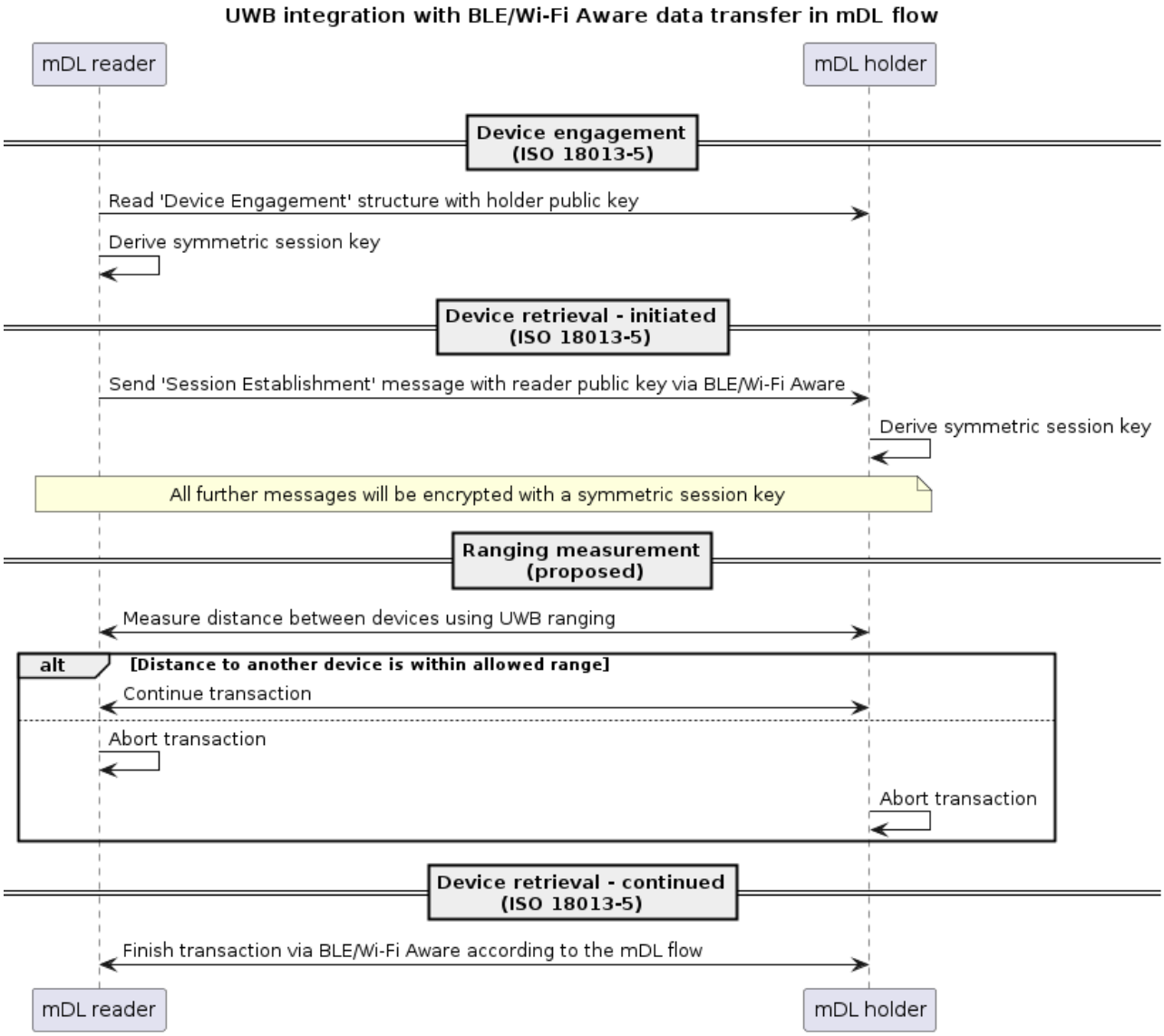

Fig. 2. UWB integration with BLE-Wi-Fi Aware data transfer in mDL flow

The earliest point in the flow where UWB ranging can be performed securely and results can be validated according to the respective policy, is the moment at the device retrieval start when session encryption is established. When device retrieval was initiated by a reader, devices can interchange with additional service messages to perform UWB ranging. After ranging is performed, range validation policy is executed and a corresponding device can make a decision if transaction should be continued.

The range validation policy is recommended to be executed in automated way for a mDL reader device according to a known setting of the room. For example, if an officer sits in a separate room and it's known that any other people cannot be present in the 2-meter circle around the officer, the range validation policy can enforce that a holder device is placed not further than 1 meter from an officer device. Conversely, it's recommended that the range validation policy for a mDL holder device is executed in a manual way as a part of the ISO 18013-5 user consent [22] as each officer room configuration cannot be known beforehand.

IV. Comparison with alternative solutions

As was mentioned in section II, there are several alternative solutions that can address location verification problem, but all of them has their flaws or do not address all use cases. To demonstrate this, solutions were compared by the following criteria:

1. Applicable for holder location check: can reader check the relative location of the holder before requesting the document.
2. Applicable for reader location check: can holder check the relative location of the reader before releasing the document.
3. Hardware/technology required for holder: additional requirements for the holder device.
4. Hardware/technology required for reader: additional requirements for the reader device.
5. Possibility to integrate with mDL session encryption: can authentication/service messages be encrypted by the symmetric session key.
6. Usage range: how close actors (officer and document holder) should be to perform the check.
7. Location precision: how accurate is the location check result
8. Verification time: additional time spent on the verification process beside the main flow.
9. False-negative result probability: how often false-negative check results can occur under normal circumstances.
10. Methods to reach false-positive results: ways to achieve false-positive results under normal circumstances.
11. Software implementation complexity: additional efforts to extend existing solution with this check mechanism.
12. Interference issues probability: change to receive invalid check results because of nearby devices.

The comparison results are provided in the Table 1.

Each of compared solutions is applicable for the holder location check because it's the main use case considered. The biometric verification approach is not applicable for the reader location check as an mDL reader device is usually shared between a set of officers. The NFC authentication and UWB ranging solutions require additional hardware for both

mDL reader and holder devices, meanwhile the biometric verification requires additional hardware only on a reader side and the visual session identifier approach doesn't require anything specific as most of mDL reader and holder devices already have a display.

Table 1. Relative location verification problem solutions comparison

Criterion/Solution	Biometric verification [8, 9]	Visual session identifier	NFC authentication [10, 11]	UWB ranging
Applicable for holder location check	Yes	Yes	Yes	Yes
Applicable for reader location check	No			
Hardware/technology required for holder	Biometric scanner	Display	NFC adapter	UWB adapter
Hardware/technology required for reader	None			
Possibility to integrate with mDL session encryption	No	No	Yes	Yes
Usage range	~ 0.5 m	~ 1 m	~ 0.5 m	Up to 100 m
Location precision	Tends to absolute, visually confirmed	Tends to absolute, visually confirmed	5-10 cm	1-5 cm
Verification time	0.5-3 seconds	5-30 seconds	1-5 seconds	Up to 1 second
False-negative result probability	High	Medium	Low	Low
Methods to reach false-positive results	Biometric input spoofing	Ambiguous font usage	Interference with another device, MITM attack	Interference with another device, MITM attack
Software implementation complexity	Medium	Low	Medium	High
Interference issues probability	Tends to zero	Tends to zero	Low	Medium

The main drawback of the biometric verification and visual session identifier approaches is impossibility of integration with the mDL session encryption, as this data cannot be additionally encrypted during its transfer, meanwhile NFC and UWB message can be. Usage range is within 0.5-1 m for all solutions except of the UWB ranging, which works in up 100 m range, which is the main advantage for this solution. Location precision for each or these approaches satisfies use case requirement as even the upper border of the NFC location precision is around 10 cm, which is comparable with a regular mobile phone size. The verification time of the UWB ranging almost doesn't have an influence on UX as it's up to 1 second in a worst case. The verification time of the biometric verification and NFC authentication is acceptable for most cases, but visual check of a complex unique session identifier can take uncomfortable amount of time and significantly slow up the document checking procedure in a worst case.

The false-negative result probability is a well-known issue for a biometric verification because of variability in biometric data, sensor accuracy, and environmental factors, meanwhile NFC and UWB approaches don't have such drawbacks which influence the false-negative result probability. Each of compared solutions can be attacked in attempt of reaching false-positive results, but attack vectors differ.

The software implementation complexity for UWB is higher comparing to other approaches as this is a relatively new technology with less existing frameworks and less best practices accumulated. The biometric verification and NFC authentication approaches are not technically easier than a UWB solution, but more ready-to-use solutions exist and related knowledge can be found more easily. The visual session identifier approach implementation doesn't require any additional knowledge for a regular developer, so its software implementation complexity is evaluated as low.

The interference issues probability tends to zero for the biometric verification and the visual session identifier approaches as with proper mDL reader arrangement the mDL holder will not cross paths with other people. The same scheme works for NFC authentication, but its interference issues probability was evaluated as low because NFC adapters of mDL reader and mDL holder can potentially interfere with other unrelated devices. The interference issues probability of the UWB ranging solution is medium because of its usage range.

Biometric verification is the most commonly used solution and often included in regular person identity verification policies. Its main disadvantages are (normally) absence of the reader verification check and a multitude of ways to spoof the biometric input material. Also, the biometric scanner with a sufficient scanning quality is regularly an external device, which can be not always convenient for mobile officers like traffic policeman.

The visual session identifier check is the simplest one of these checks, but it requires increased attentiveness to check the identifier by eye. Unique enough identifier should be large enough, e.g. like 16-bytes UUID, which can be hard to check for certain groups of people like elderlies or people with the visual impairment. The main disadvantage of this method is high human error probability.

NFC authentication and UWB ranging are comparable solutions with slightly different pros and cons. Main advantages of these solutions are possibility to provide a verification result with lesser human error factor and possibility to be integrated with mDL session encryption. The main disadvantages are additional hardware requirements for both reader and holder devices and the MITM attack possibility. The MITM attack is addressed by leveraging the mDL session encryption. The additional hardware requirements can be addressed by using both of UWB ranging and NFC authentication methods.

The NFC authentication is a solution with a larger history, thus more frameworks and best practices exist. But the UWB ranging solution has better technical characteristics, as it has a larger range, better precision, and works faster. As modern phones have a built-in UWB adapter, the main use case can include UWB ranging because of its better technical characteristics. The NFC authentication may be used as a secondary option if UWB is not available on a holder device.

Conclusion

The relative location verification problem for reader and holder devices can be addressed using NFC communication already specified in ISO 18013-5. For use cases that don't involve NFC usage because of holder device limitations or specific document validation process policies, it is proposed to use the UWB ranging in fusion with BLE or Wi-Fi Aware data transfer. By checking distance between holder and reader devices before requesting or returning the document, both actors can be sure that the opponent device is located right before them.

The UWB ranging solution has better technical characteristics than the NFC authentication solution such as usage range, location precision, and verification time. The UWB ranging usage range is significantly larger than usage range of other approaches – up to 100 meters comparing to 0.5-1 meter for other approaches. The UWB ranging verification time is smaller than any other approach as it's up to 1 second in a worst case comparing to several seconds for other solutions. Location precision is also better for the UWB technology comparing to NFC roughly in two times – 1-5 centimeters for UWB and 5-10 centimeters for NFC.

Also, the UWB ranging usage provides simpler UX for the mDL data transfer procedure because additional actor movements for an NFC tap is not required. The UWB ranging messaging can be encrypted using the mDL session encryption on symmetric keys as well as the NFC communication to provide MITM attack prevention.

A scientific novelty of this paper is in improving existing mDL data transfer via BLE and Wi-Fi Aware using the UWB ranging. This solution covers the secure mDL data transfer use cases for devices without NFC adapter and provides technical characteristics improvement. Usage range is improved from 0.5-1 meter to up to 100 meters, location precision is improved from 5-10 centimeters to 1-5 centimeters, and verification time is improved from 1-5 seconds to up 1 second.

References

1. A Secure Technology Alliance Identity Council White Paper (2020), "The Mobile Driver's License (mDL) and Ecosystem", **URL**: https://www.securetechalliance.org/wp-content/uploads/Mobile-Drivers-License-WP-FINAL-Update-March-2020-4.pdf.

2. Final Report – EReg Topic Group XIX (2018), "Non-physical driving licences - going mobile", **URL**: https://ereg-association.eu/media/2024/finl-report-tg-xix-on-non-physical-driving-licences.pdf.

3. Transportation Security Administration (2024), "When will the phased digital ID rollout start? Which airports/states will be first in line for this new technology?", **URL**: https://www.tsa.gov/travel/frequently-asked-questions/when-will-phased-digital-id-rollout-start-which-airportsstates.

4. *McConvey, J. R.* (2023), "Banks hit with biometric fraud, fake mobile driver's licenses", **URL**: https://www.biometricupdate.com/202303/banks-hit-with-biometric-fraud-fake-mobile-drivers-licenses.

5. U.S. Department of Homeland Security, Science and Technology (2024), "Misuse of a Mobile Driver's License (mDL) Investigative Aid", **URL**: https://www.dhs.gov/sites/default/files/2024-03/24_0315_st_mdl_investigative_aid_journey.pdf.

6. ISO/IEC 18013-5:2021 (2021), ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application. Section "6.3.2.1 Overview", 8 p.

7. ISO/IEC 18013-5:2021 (2021), ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application. Section "6.3.3 Security mechanisms", 13 p.

8. *Chavan, S., Tupurwadkar, S., Jagtap, P., Pore S.* (2024), "Fingerprint Based Driving License Management System", International journal of Scientific Research in Engineering & Management. P. 1–5. **DOI**: https://doi.org/10.55041/IJSREM29360.

9. *Prasad, N. A., Aishwarya, S., Bindu, M. K., Rakshitha, B. R.* (2024), "A Comprehensive Survey On Authenticated Access Control For Vehicles Through Driver's License And Biometric Verification", International Journal For Technological Research in Engineering, volume 11, issue 5. P. 69–73. **DOI**: https://doi.org/10.5281/zenodo.10468185.

10. *Thammarat, C.* (2020), "Efficient and Secure NFC Authentication for Mobile Payment Ensuring Fair Exchange Protocol", Symmetry, No. 12(10), 1649. **DOI**: https://doi.org/10.3390/SYM12101649.

11. *Lee, W., Baek, S. Y., Kim, S. H.* (2021), "Deep-Learning-Aided RF Fingerprinting for NFC Security", IEEE Communications Magazine, No. 59(5). P. 96–101. **DOI**: https://doi.org/10.1109/MCOM.001.2000912.

12. *Leitch, S. G., Ahmed, Q. Z., Abbas, W. B., Hafeez, M., Laziridis, P. I., Sureephong, P., Alade, T.* (2023), "On Indoor Localization Using WiFi, BLE, UWB, and IMU Technologies", Sensors, No. 23(20), 8598. **DOI**: https://doi.org/10.3390/S23208598.

13. *Botler, L., Spörk, M., Diwold, K., Römer, K.* (2020), "Direction Finding with UWB and BLE: A Comparative Study", Proceedings of the 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Delhi, India, P. 44–52. **DOI**: https://doi.org/10.1109/MASS50613.2020.00016.

14. *Bilge, M. R.* (2022), "Evaluation of Ultra Wide Band Technology as an Enhancement for BLE Based Location Estimation", arXiv, 10 p. **DOI**: https://doi.org/10.48550/ARXIV.2202.00558.

15. *Dagher, R., Molina, F. X., Abadie, A., Mitton, N., Baccelli, E.* (2021), "An Open Experimental Platform for Ranging, Proximity and Contact Event Tracking using Ultra-Wide-Band and Blue-

tooth Low-Energy", Proceedings of the IEEE INFOCOM 2021 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, P. 1–6. **DOI**: https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484579.

16. *Kolakowski, J., Djaja-Josko, V., Kolakowski, M., Broczek, K.* (2020), "UWB/BLE Tracking System for Elderly People Monitoring", Sensors, No. 20(6), 1574. **DOI**: https://doi.org/10.3390/S20061574.

17. *Kolakowski, M.* (2020), "Automatic radio map creation in a fingerprinting-based BLE/UWB localisation system", IET Microwaves, Antennas & Propagation, No. 14(14), p. 1758–1765. **DOI**: https://doi.org/10.1049/IET-MAP.2019.0953.

18. *Kolakowski, M.* (2019) "A Hybrid BLE/UWB Localization Technique with Automatic Radio Map Creation", Proceedings of the 2019 13th European Conference on Antennas and Propagation (EuCAP), Krakow, Poland, P. 1–4. **DOI**: https://doi.org/10.48550/arXiv.2404.03072.

19. *Zhang, Q., D'souza, M., Balogh, U., Smallbon, V.* (2019) "Efficient BLE Fingerprinting through UWB Sensors for Indoor Localization", Proceedings of the 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, P. 140–143. **DOI**: https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00065.

20. *Brunacci, V., De Angelis, A., Costante, G.* (2022) "Development of a Cooperative Localization System using a UWB Network and BLE Technology", Proceedings of the 2022 IEEE International Symposium on Measurements & Networking (M&N), Padua, Italy, P. 1–6. **DOI**: https://doi.org/10.1109/MN55117.2022.9887703.

21. ISO/IEC 18013-5:2021 (2021), ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application. Section "9.1.1.4 Procedure", 46 p.

22. ISO/IEC 18013-5:2021 (2021), ISO-compliant driving licence, Part 5: Mobile driving licence (mDL) application. Section "E.13 mDL holder consent", 144 p.