Trust-Provisioning Infrastructure for a Global and Secured UAV Authentication System

Dominic Pirker*†, Thomas Fischer*†, Harald Witschnig†, Christian Steger*
Email: {dominic.pirker, thomas.fischer3, harald.witschnig}@infineon.com, steger@tugraz.at
*Institute for Technical Informatics, Graz University of Technology, Graz, Austria
†Development Center Graz, Infineon Technologies AG, Graz, Austria

***Abstract*—UAVs are gaining momentum in various areas, whether it is in the commercial or private sector. Novel scenarios are extending the seemingly endless list of use cases for this emerging technology. To avoid ungoverned proliferation and abandoned aerial objects, not only regulations but also technical solutions are indispensable. Authentication of a UAV is required to link to the operator and respective competences. Besides appropriate competences, regulations are depending on regional authorities, which demands a studious concept to avoid insular solutions.**

This paper proposes a thought-through infrastructure for a secured and global operative authentication system. First, upcoming regulations are considered for the concept to make the system regulatory compliant. Then, to avoid a patchwork of proclaimed solutions, the system design is based on the principle of delegated authority, which allows the respective authorities to keep control over their domains. Further, to associate UAVs with their operators, a cryptographic link is created during a provisioning process. This link is represented by a certificate, comparable with a conventional driver's license. The system design allows divestment of respective flight permissions, enabled by certificate revocation. Lastly, we constructed a proof-of-concept for the proposed infrastructure solution and compared it to a decentralized approach.

***Index Terms*—UAV, authentication, TLS, certificates, PKI, mDL, HSM, DNS**

I. Introduction

Registration and subsequent identification of Unmanned Aerial Vehicles (UAVs) is getting essential, since the UAV market is highly dynamic and will heavily increase in the upcoming years. For instance, in Germany the market will grow six-fold in the next decade, from 500 Million Euro to 3 Billion Euro [1]. The number of operational UAVs will increase to almost 1 Million by 2023 [1].

Considering the tremendous growth - infrastructure, services, and procedures have to provide safe Unmanned Aerial System (UAS) operations and support their integration into the aviation systems [2]. A general problem are the region-depended regulations. Therefore, a concept for a global operational system is required to enable automatic position detection as well as intermediate application of region-depended regulations. Fig. 1 depicts a global and secured UAV authentication system, consisting of a flight control and a UAV. On top of the protected communication channel, which is supported by an Hardware Security Module (HSM) on the UAV, the flight information is transmitted. A problem with UAV identification systems is the missing link between the UAV and its operator, even tough it is crucial, since the operator is responsible. Therefore, the system depicted in Fig. 1 needs to be extended.

The main contributions of this work are:

- Proposal of an infrastructure for a global aviation system, based on the global and secured UAV authentication system depicted in Fig. 1 and proposed in [3].
- Designing the certificate deployment process to be globally operational.
- Digital licensing based on a cryptographic link between the UAV and the corresponding operator.
- Evaluation of the proposed infrastructure system and analysis of potential weaknesses.

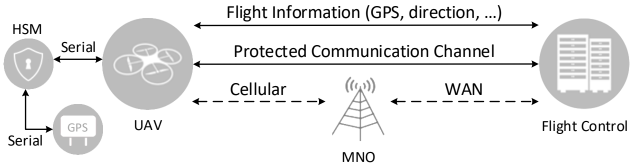
HSM
Serial
Serial
GPS
UAV
Flight Information (GPS, direction, ...)
Protected Communication Channel
Cellular
WAN
MNO
Flight Control

Fig. 1. Connection overview between flight control and UAV including an HSM (adopted from [3])

II. State of the Art

A. Regulatory Framework

The European Union Aviation Safety Agency (EASA) released common rules on UAS to ensure that UAS operations are safe and secure [4]. UAS describes the entire system consisting of the UAV, the ground control station or pilot, and other components such as camera or Global Positioning System (GPS) receiver. Two related documents have been published by the EASA: *Commission Delegated Regulation (EU) 2019/945* [5] and *Commission Implementing Regulation (EU) 2019/947* [2]. The *Delegated Regulation* describes requirements for designing and manufacturing UAS to allow operation based on rules and conditions defined in *Implementing Regulation* [5]. The latter lays down provisions for the operation of UAVs, including personnel and organizational usage [2]. In addition, industry should not diminish in agility, innovation, and continuous growth, while implementing the regulations.

These regulations include requirements for the implementation of three foundations of the *U-space* system [2], that is a set of services and procedures to support safe, efficient,

This is the full version of a paper which appears in 2020 International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom).
The proceedings version is available online at: https://doi.org/10.1109/CoBCom49975.2020.9174131

and secure access to airspace for a large number of UAVs [6]. The operational requirements are geo-awareness, remote identification, and registration of the operator and UAV. Even tough the regulations are defined by the European Union (EU), EASA member states will still remain flexible in the context of defining zones or additional requirements.

B. Digital Driver's License

Digital driver's license is often referred to as mobile driver's license. This kind of driver's license is different from electronic driver's licenses. The latter is basically the traditional driver's license in ID card format, equipped with a security controller to protect personal data such as biometric data [7]. Electronic driver's licenses are, as electronic passports, already available in many countries, whereas digital driver's licenses are for now only in testing and pilot phases [8]. National Institute of Standards and Technology (NIST) is pushing a pilot project in the US together with Gemalto to verify the technical feasibility of digital driver's licenses [9]. Further, the International Organization for Standardization (ISO) has a dedicated working group to tackle the emerging trend towards digital driver's licenses (ISO/IEC JTC 1/SC 17/WG 10). In this regard, the high impact of drones is pointed out by the foundation of a dedicated working group, having drones, their licensing, and further their operator's identity as major subjects (ISO/IEC JTC 1/SC 17/WG 12).

C. Public Key Infrastructure

Public Key Infrastructure (PKI) is a well-established, widely used and centralized mechanism to enable trust, with the key elements: confidentiality, authenticity, integrity, and non-repudiation [10]. In [11], a PKI infrastructure for a large-scale Internet-based healthcare network is proposed to ensure security for connecting a wide-spread spectrum of geographically distributed units. The authors from [11], adopted the traditional hierarchical PKI trust model to enable compartmentalization of different responsibilities. This is also considered in the design of the global aviation infrastructure system, proposed in this work.

Main responsibilities of PKI systems are certificate issuing, certificate deployment, and certificate validation (typically X.509 certificates). Based on public-key cryptography, messages sent via an insecure network can be digitally signed and encrypted. To ensure the affiliation of public keys, digital certificates are used. The primary party of a hierarchical PKI system is the Certificate Authority (CA), also acting as a registration and validation authority simultaneously. Web of trust is a different approach for public authentication, which is based on *OpenPGP* and standardized in RFC 4880 [12].

D. DNS Namespace

The Domain Name System (DNS) is a hierarchical naming system that links IP addresses to domain names. These domains exist in various levels and are connected in a hierarchical tree structure [13]. Example: *maps.google.com*; *"com"* is the top-level domain; *"google"* is a sub-domain and *"maps"* is a lower-level sub-domain. With few exceptions, the domains are associated to regions (e.g. *"at"*, *"de"*, or *"us"*). This regional and hierarchical approach is chosen for the concept of the global lookup service proposed in this paper.

III. The Global Aviation Infrastructure System

The system we proposed in [3], describes a *Global and Secured UAV Authentication System based on Hardware-Security*, that uses the Transport Layer Security (TLS) protocol, supported by an HSM (depicted in Fig. 1). This system requires an established PKI infrastructure. Based on that, the certificate provisioning procedure is performed. This procedure is split into UAV (client) and server authentication. The UAV authentication part is associated with the UAV itself, the UAV manufacturer CA, and the smart remote control (e.g. smartphone), depicted in Fig. 3. The server authentication part is associated with flight control servers, regional CAs, and a global aviation authority lookup service. The server authentication has similarities to the DNS lookup service and is depicted in Fig. 2.

A. Requirements

The main requirements for the infrastructure of the global aviation system including the regulative requirements from the the *Delegated* [5] and *Implemented Regulation* [2] are:

- *Global availability* is a necessity to avoid insular solutions. This includes capability to comply with regulations in respective regions, as well as allowing authorities to keep control over their flight zones.
- *Authentication*, not only identification, which implies the necessity to proof the identity (not just object classification as radar-based systems [14]).
- Regulative requirements:
  - *Geo-awareness* to allow the implementation of no-fly zones.
  - *Remote Identification* to know the operator during flying.
  - *Registration* of *Operator* (Pilot) to allow later identification and verification of possibly necessary proof of knowledge and competences.
  - *Registration* of *UAV* to allow classification and verification of certified hardware.

An additional requirement that was defined during the research process, is the creation of the cryptographic link between the UAV and the operator while authenticating against the flight control server, explained in more detail in Section III-C2.

B. Goal

A UAV that is switched on, must authenticate itself and its operator against a flight control. As regulations may be regional dependent, the UAV must be able to choose the location corresponding flight control server. Therefore, a global lookup service is required. To achieve this high level of scalability, the certificate provisioning process has to be separated into two parts, the preliminary steps and the operational steps.

C. Preliminary Steps

These steps are separated into server and client setup. Each paragraph explains the respective steps for provisioning the certificates before the actual UAV and operator authentication against the flight control server happens.

1) Server Authentication: For this infrastructure, two different types of servers exist, the global lookup server and at least one flight control server. Reasons for multiple flight control servers may include the amount of UAVs, size of the region, and redundancy. Both, the global lookup server and the flight control server must support server authentication. Fig. 2 depicts the steps for the server authentication. In the following figures the preliminary and operational steps are visualized with dashed and solid lines, respectively.

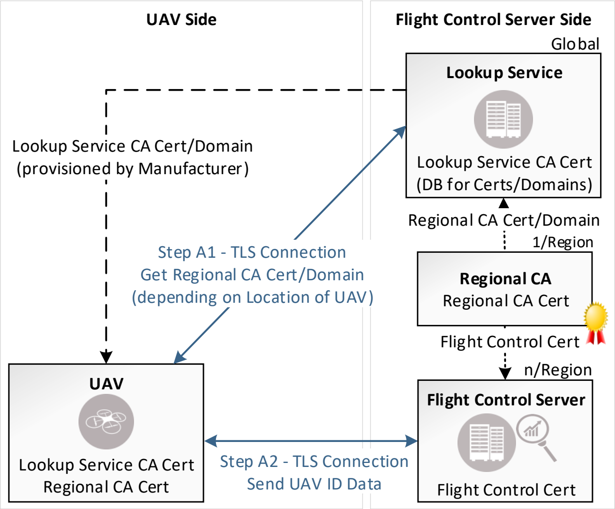

Fig. 2. Infrastructure and certificate provisioning process for server authentication

For authentication of the global lookup service against a UAV, the lookup service certificate must be stored on the UAV, for instance in the protected storage of an HSM. For security reasons, the lookup service certificate should be stored in read-only memory (ROM) to avoid tampering with the certificate. Additionally to the lookup service certificate, the IP address or domain of the global lookup service must be stored in the UAV's memory during the manufacturing process, to be able to request the regional authority certificate and domain later. For the current approach, client authentication against the global lookup service is not required, because it is a public service.

For authentication of the flight control server against a UAV, the regional CA issues and provisions a certificate to each flight control server. The regional CA certificate is stored, together with the respective IP address or domain, at the global lookup service.

2) Client Authentication: Client authentication is required for two reasons, authenticating the UAV against the remote control, and most essentially authenticating the UAV and its operator against the flight control server. To enable this, several steps are necessary as depicted in Fig. 3.

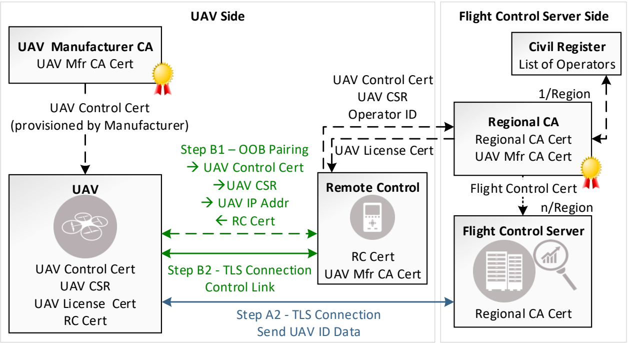

Fig. 3. Infrastructure and certificate provisioning process for client authentication

First, the UAV needs to be paired with the remote control at first use, labeled as *Step B1* in Fig. 3. During pairing, the certificates are exchanged between UAV and remote control, and the IP address of the UAV is stored on the remote control. For this, an Out-of-Band (OOB) pairing method has to be implemented. Specifying the exact method is out of scope, but Near Field Communication (NFC) or a method described in [15] can be used. The RC certificate is a self-signed certificate, and is generated on the remote control.

After the pairing is complete, the secured channel can be used to transmit details for generating the UAV license certificate to securely connect and authenticate to the flight control server. The details include the UAV control certificate and the UAV Certificate Signing Request (CSR).

Preliminary, the UAV manufacturer CA issues a UAV control certificate for each UAV and stores it in the HSM's protected storage. This certificate is used by the UAV to authenticate itself against the remote control, that holds the UAV manufacturer certificate for validation. The deployment of the UAV manufacturer certificate is out of scope, but one solution is to deliver it along with the mobile application for remote control.

The next steps are designed to cryptographically link the UAV and the operator for authentication against the flight control server. This step is necessary, since TLS is designed to utilize exactly one certificate per peer for connection establishment. Alternatively, a second certificate can be sent at the application layer, but this would mix the application with the security layer.

The regional CA is in charge of this linking procedure. Therefore, the UAV control certificate and the UAV CSR, together with a personal identifier of the operator, are required. The CSR is generated by the UAV itself. Specific UAV related information (e.g. model, weight, etc.) are extracted from the UAV control certificate, which is provisioned by the UAV manufacturer. Then, the CSR is generated with this as input and signed with the private key, that is stored in the UAV's HSM. The channel establishment between the remote control and the regional authority is out of scope of this work. Possible solutions include a web API or a separate smartphone application.

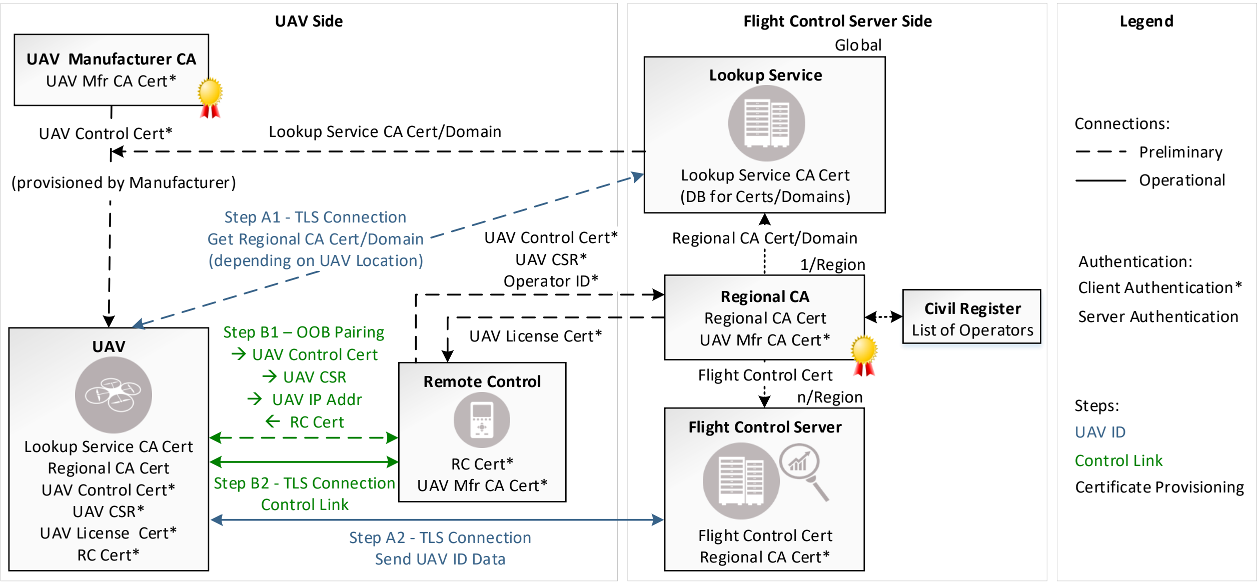

Fig. 4. Infrastructure and provisioning process for the global and secured UAV authentication system

At the regional authority, the UAV control certificate is used to ensure, that the UAV to be registered, is from an accredited UAV manufacturer. The signature of the CSR is validated with the public key of the UAV's control certificate to ensure, the requester possesses the UAV, for which a certificate is requested. Next, the ID of the operator and the UAV details are processed and validated for required competences, based on a civil register. If so, the UAV CSR is extended with operator ID data and signed by the regional CA, which results in the UAV license certificate.

The UAV license certificate is sent to the remote control first, then it is sent via the TLS connection to the UAV, where it is finally used for authentication to the flight control server.

D. *Operational Steps*

After the preliminary steps are complete, the system is ready for operation. First, this includes establishing a protected channel between UAV and remote control labeled as *Step B2*. Second, establishment of a protected channel between UAV and flight control server (*Step A2*). The latter, requires a protected communication channel to the global lookup service beforehand, in order to request the location corresponding flight control server's domain.

The TLS protected control link is established with the UAV control certificate validated with the UAV manufacturer certificate, and the RC certificate validated by the remote control.

Following the boot process of a UAV, a TLS connection to the global lookup service, labeled as *Step A1* in Fig. 2, is established. The global lookup service certificate, stored in the UAV's memory, is used for server authentication.

Using the protected connection, domain, and certificate of the location-dependent regional authority are requested. The required UAV location information can either be provided as GPS coordinates by the UAV, or the lookup service can locate the UAV based on its IP address if the Mobile Network Operator (MNO) provides location specific addresses. Another possibility to get the location information of the UAV, is to extract this information from the connected LTE cell as described in [16].

The TLS connection to the lookup service is closed and based on the recent obtained domain, a TLS protected communication channel from the UAV to the flight control server, labeled as *Step A2* in Fig. 2, is established. The identity of the flight control server is validated by the regional CA certificate retrieved in *Step A1*. The authentication of the UAV and its operator is done with the UAV license certificate. This certificate is validated with the UAV manufacturer certificate stored on the flight control server.

In Fig. 4 both, the preliminary and operational steps, together with all involved parties are depicted.

E. *CA Hierarchy*

The proposed infrastructure requires three different root CAs, the UAV manufacturer CA, the regional CA, and the global lookup service CA. As depicted in Fig. 5, these root CAs are independent. In the described hierarchy, the root CA is at the same time the issuing CA.

The UAV control certificate is issued by the manufacturer CA. The regional CA is issuing the UAV license certificates and the flight control certificates. The lookup service CA certificate is used for server authentication, and does not issue additional certificates.

F. *Permission Revocation*

Divestment of respective flight permissions of specific operators is allowed due to the design of the system. In PKIs, a certificate is expected to be valid for the entire period,

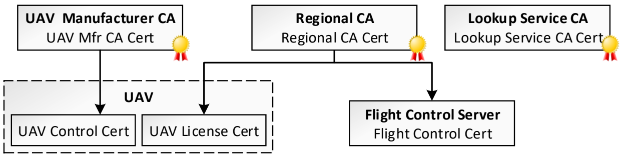

Fig. 5. Certificate authority hierarchy for the global UAV authentication system

set during issuing. Typically, scenarios such as changes in association between subject (e.g. UAV) and CA, or suspected compromise of the corresponding private key, can cause prior invalidation of the certificate [17]. The invalidation is enabled by adding identifier of the corresponding certificate to the Certificate Revocation List (CRL), which is issued periodically to distribution points which are linked within the certificate. One problem with CRL is the delay, caused by the periodic update. Another attack against this revocation mechanism is a Denial-of-Service attack against the distribution points, which would freeze the current status of the CRL, and therefore new permission revocation are affected. A CRL allows two different states of revocation: Revoked (irreversible) and hold (reversible).

The proposed system enables revocation of flight permissions by adding the respective UAV license certificate to the CRL. This is done by the flight control server, based on regional defined regulations. An example could be restricted behavior of the operator, such as flying over highly critical areas (e.g. airports, power plants).

IV. Proof-of-Concept

For the proof-of-concept, a manual step-by-step execution of the certificate provisioning process is performed. For the hardware, we build upon the setup used in [3]. The setup consists of a modular UAV equipped with a Raspberry Pi Zero which was extended with an I2C-connected HSM, and a Raspberry Pi 3, running as a flight control server. Both are operating with Raspbian Stretch. For certificate issuing, the *OpenSSL* toolkit is used, which is publicly available and licensed for commercial and non-commercial usage [18].

A self-signed CA certificate for the UAV manufacturer is generated. With that, a UAV control certificate is issued and stored at the UAV's HSM. Next, a CSR is generated with support of the HSM, which stores the UAV's private key in protected memory. As input for the subject field of the CSR, dummy data is used to simulate UAV related details, such as model or weight. In the proof-of-concept, remote control, flight control, and regional authority are hosted on the same physical system, but distinct TLS channels are established. The certificates used for establishing the control link, are the RC certificate, validated by the remote control, and the UAV control certificate, validated with the UAV manufacturer certificate. The OOB pairing is performed manually by putting the certificates on the corresponding devices.

On the flight control server, a regional CA certificate is generated and a flight control server certificate is issued. To issue the UAV license certificate, which is linking the operator with the UAV, first the UAV CSR is validated with the UAV manufacturer CA. Then, the CSR is extended with dummy attributes (representing operator details) and the certificate is issued with the regional CA certificate and the corresponding key. Then, this certificate is sent to the UAV, where it is used for authentication and protected connection establishment against the flight control server. The certificate's validity is checked with the regional CA certificate.

V. Evaluation

A. Digital Licensing

One key concept of the proposed infrastructure for a global and secured UAV authentication system is the UAV licensing. It is comparable with a digital driver's license, since both licenses are stored on an embedded device and not on chip cards representing a document. The difference is, within the pilot projects, digital driver's licenses are stored on the mobile phone [9], whereas in this concept, the license is stored at the vehicle (UAV in this case). The license is represented by an X.509 certificate (UAV license certificate) and is linked to a specific UAV. Comparing to traditional licensing use cases, for instance car driver's license, the operator is not always in the same location as the UAV, and therefore a link between the vehicle and the operator is mandatory.

B. DNS Similarities

The proposed global lookup service has strong similarities to DNS. Both are a hierarchical mapping of a dynamic database scattered globally [19]. As DNSSEC, the trust relationship has to be built from the root, which is corresponding to the global lookup service within our proposed concept. Trust is established by verifying the lookup server's identity during the TLS handshake, with support of the lookup service CA certificate, stored in the UAV's HSM during manufacturing. The location of the UAV is comparable with the country code within DNS. This concept design was chosen, because the concept as DNS is utilizing, is well established and widely used for providing global available services [19].

C. Concept Evaluation

The global lookup service proposed in this work, brings a major advantage. Due to the fact that in *Step A1* of the provisioning process, the location-dependent domain, respectively the according flight control server certificate, is fetched from the global lookup service, a UAV always connects to the correct, location-corresponding server. Using this measure, regional regulations can be defined by the respective authorities, even tough a global system is used.

One drawback of the proposed infrastructure concept is the potential single point of failure which applies for the global lookup service and the flight control servers. If one of those fails or is attacked, the system might become unavailable. If an attacker manages to retrieve the private key corresponding to the certificate of a server, trust in the entire system is compromised [20].

A countermeasure is to implement redundancy, as briefly described for the flight control servers in Section III-C1. A comparable approach can be implemented for the global lookup service. Therefore, IP or domain to secondary or even tertiary global lookup service can be provisioned during UAV manufacturing. Again, DNS implements a similar approach, where a client can store the IP addresses of multiple DNS servers. Alternatively, a decentralized concept, for instance based on blockchain, is a conceivable solution. Blockchain, a decentralized ledger of transaction, solves the problem of single point of failure, compared to digital certificate systems [20].

VI. Conclusion and Future Work

In this work we proposed an infrastructure and trust provisioning process for a global operative and secured UAV authentication system, that allows authentication of both, the UAV and the corresponding operator. The design allows permission divestment, in cases such violation of no-fly zones is detected. Additionally, region-dependent regulations are respected, which is supported by the implementation of the global lookup service and the corresponding flight control servers.

Future work will further investigate on the weaknesses of the proposed system. Alternative solution for the given problem statement, for instance based on blockchain, as mentioned in the evaluation, will be researched. A promising approach is to design a hybrid solution that combines the advantages of hierarchical and decentralized solutions.

VII. Acknowledgment

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826610. The JU receives support from the European Unions Horizon 2020 research and innovation programme and Spain, Austria, Belgium, Czech Republic, France, Italy, Latvia, Netherlands.

References

[1] V. U. L. (VUL), "Analysis of the German Drone-market," https://www.bdl.aero/, Market Analysis, 2019. [Online]. Available: https://www.bdl.aero/wp-content/uploads/2019/02/VUL-Marksstudie_Deutsch_final.pdf

[2] Council of European Union, "Commission implementing regulation (eu) 2019/947," 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN.

[3] Dominic Pirker, *Design and Implementation of a Global and Secured Drone Identification System with Hardware-Based Security*. TU Graz, 2019.

[4] EASA, "EU wide rules on drones published," https://www.easa.europa.eu/newsroom-and-events/news/eu-wide-rules-drones-published, [Online; accessed 2019-10-21].

[5] Council of European Union, "Commission delegated regulation (eu) 2019/945," 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN.

[6] SESAR Joint Undertaking, "U-space blueprint," 2017, https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF.

[7] A. A. of Motor Vehicle Administrators (AAMVA), "Mobile Driver's License," https://www.aamva.org/, Whitepaper, 2016. [Online]. Available: https://www.aamva.org/FunctionalNeedsWhitepaper-9/

[8] R. T. Raj, S. Sanjay, and S. Sivakumar, "Digital License mv," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 1277–1280.

[9] NIST, "Digital identity for individuals," https://www.nist.gov/itl/tig/digital-identity-individuals, [Online; accessed 2020-04-20].

[10] B. Rajendran, "Evolution of PKI ecosystem," in *2017 International Conference on Public Key Infrastructure and its Applications (PKIA)*, Nov 2017, pp. 9–10.

[11] G. Mantas, D. Lymberopoulos, and N. Komninos, "PKI Security in Large-Scale Healthcare Networks," *Journal of medical systems*, vol. 36, pp. 1107–16, 09 2010.

[12] e. a. J. Callas, "OpenPGP Message Format," Internet Requests for Comments, RFC Editor, RFC 4880, November 2007. [Online]. Available: https://tools.ietf.org/html/rfc4880

[13] P. Satam, H. Alipour, Y. Al-Nashif, and S. Hariri, "DNS-IDS: Securing DNS in the Cloud Era," in *2015 International Conference on Cloud and Autonomic Computing*, Sep. 2015, pp. 296–301.

[14] M. Jian, Z. Lu, and V. C. Chen, "Drone detection and tracking based on phase-interferometric Doppler radar," in *2018 IEEE Radar Conference (RadarConf18)*, April 2018, pp. 1146–1149.

[15] H. Nakajima, S. Suzuki, T. Tokunaga, K. Tanaka, Y. Miyazaki, K. Maruyama, and O. Nakamura, "Out-of-band authentication protocol for digital signage and smartphone interaction," in *2016 IEEE 5th Global Conference on Consumer Electronics*, Oct 2016, pp. 1–2.

[16] Sven Fischer, *Observed Time Difference Of Arrival (OTDOA) Positioning in 3GPP LTE*, 1st ed. Qualcomm, 2014.

[17] e. a. Housley, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Requests for Comments, RFC Editor, RFC 2459, January 1999. [Online]. Available: https://tools.ietf.org/html/rfc2459

[18] OpenSSL Software Foundation, "OpenSSL," https://www.openssl.org/, [Online; accessed 2020-04-20].

[19] M. H. Jalalzai, W. B. Shahid, and M. M. W. Iqbal, "DNS security challenges and best practices to deploy secure DNS with digital signatures," in *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2015, pp. 280–285.

[20] R. Wang, J. He, C. Liu, Q. Li, W. Tsai, and E. Deng, "A Privacy-Aware PKI System Based on Permissioned Blockchains," in *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, Nov 2018, pp. 928–931.