Secure and Flexible Establishment of Temporary WLAN Access

Steffen Fries, Rainer Falk
Corporate Technology
Siemens AG
Munich, Germany
e-mail: {steffen.fries|rainer.falk}@siemens.com

***Abstract*—Several use cases demand for the setup of a separate, dedicated communication channel that provides a specific quality of service, or to separate communications of different criticality. Different properties of communication channels are performance, latency, but may be also security related. In several cases, a reliable association to an already established communication channel is required. Specifically, if a first communication channel has been securely established, a cryptographic binding of a second communication channel to this first communication channel is needed. One example use case is the charging of electric vehicles. Besides the charging control, also value-added services like software updates for the infotainment system shall be provided. To avoid interfering with the charging-related control communications, a second, separate communication channel is established. The two communication channels require different quality of service. However, authorization to access value-added services and maybe also the billing of consumed value-added services shall be to bound to the user that has been authenticated in the setup of the first communication channel. The paper proposes a general solution that allows establishing arbitrary communication channels of different nature on the example of an electric vehicle and a charging station, all bound to the actual charging control session.**

Keywords–communication security; cryptographic channel binding; quality of service; industrial automation and control system; Internet of Things.

I. INTRODUCTION

In network communications, it is typically required to have distinct relations between communicating endpoints, which are defined by several parameters, like the addresses of the communicating endpoints, security credentials connected with the endpoints, but also by certain quality-of-service related features. Quality-of-service (QoS) features may relate to a specific throughput expected by the communication channel or a specific response time or latency of the communication, but also to specific security properties of the communication like integrity protection or combined integrity and confidentiality protection. These properties may be provided by the utilized transport protocol or application protocol, but may already be enforced by the network access. Network access may be achieved as wired access using a classic cable installation, but also using wireless access via wireless LAN (WLAN), 4G, or 5G mobile communications.

Specific QoS features are required for a variety of applications. Examples comprise electric vehicle charging, real-time control of, e.g., industrial control, voice-and-video conferences, or video streaming. Also, specific security applications may leverage a separate communication channel like the provisioning of credentials using a link with weak protection or general access authentication. If the setup of a communication channel with certain QoS features is based on a previously established communication relation, a binding of the two communication sessions can be leveraged in multiple ways.

The aim of this paper is to propose a solution for setting up a new wireless communication channel that utilizes a previously established communication channel. The initial target use case was provided by electric vehicle charging systems that, in addition to the actual charging, provide value-added services. These value-added services may relate to updates of the firmware, software, or map material for the infotainment system of an electric vehicle.

This paper is structured in the following way. Section II provides an overview about a potential target scenario, taking electric vehicle charging as example. Section III investigates existing approaches to provide distinct communication channels with distinct properties. Section IV describes a new approach, and section V analyzes its advantages. Section VI concludes the paper and provides and outlook to future work.

II. ELECTRIC VEHICLE CHARGING WITH VALUE ADDED SERVICES

The number of electric vehicles as bicycles, motorcycles, and cars has increased in the recent years significantly. They are connected to the Digital Smart Grid for charging. Developments are also ongoing for bidirectional charging, which allows to utilize electric vehicles as energy storage system and to feedback energy to the power grid when necessary. Depending on the charging interface between the electric vehicle and the infrastructure, the charging may be accomplished within minutes, or it may need up to several hours. While connected to a charging station, the vehicle exchanges constantly control data with the charging station to provide data like locally measured energy consumption on the vehicle side or charging commands with parameter adaptations from the charging station. This connection time

 ISBN: 978-1-68558-007-0

may also be used to provide value-added services by utilizing the connection already established between the electric vehicle and the charging station.

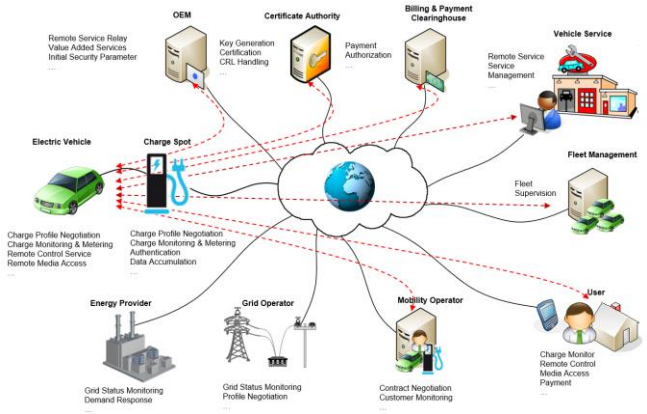

Figure 1. Electric Vehicle Communication Connections

As depicted in Figure 1, there is a multitude of potential communication options with different actors of the system. The communication channel established between the electric vehicle and the charging station may be setup using different standards like ISO/IEC 15118 [1] or CHaDemo [2]. The focus in this paper is placed on ISO/IEC 15118.

The communication may use power line communication when the vehicle is connected via a wired interface, or wireless using WLAN in case of inductive charging. In this case, the charging station provides a WLAN access point to facilitate the communication also in a wireless fashion. According to ISO/IEC 15118, access to the charging station is not protected on the WLAN access layer, but on higher communication layers. This avoids a specific WLAN access configuration of electrical vehicles for a specific charging station. The communication performed in the context of ISO/IEC 15118 allows to provide charging parameter information, billing relevant information, and also to perform mutual authentication of the electric vehicle and the charging station. The security of ISO/IEC 15118-2 has been studied from the early beginning of standardization (cf. for example [3]). Meanwhile, the standard has been completed, and a revision will be published soon as Edition 2.

The communication channel is part of the Digital Grid communication and the control network of an energy utility. Value-added service providers may utilize the communication channel as well, but are independent of the power system operator. The energy distribution network as critical infrastructure relies on the availability of the information infrastructure. Therefore, the information infrastructure must be managed and operated according to the same level of reliability as required for the stability of the power system infrastructure to prevent any type of outage or disturbance. The immediately apparent security needs target the prevention of financial fraud and ensure the reliable operation of the power grid. Especially the interaction between new market participants and value-added services has been investigated and is also addressed in ISO/IEC 15118.

Common to both editions of the standard ISO/IEC 15118 is the security approach and specifically the security setup between the electric vehicle and the charging infrastructure. It relies on the establishment of a secured communication channel based on Transport Layer Security (TLS, version 1.2 specified in IETF RFC 5246 [4], version 1.3 in IETF RFC 8446 [5]). It requires that the charging station authenticates towards the electric vehicle using an X.509 certificate during the TLS handshake. In turn, if the electric vehicle uses plug-and-charge, or if it wants to consume value-added services, it authenticates with an own X.509 certificate that is bound to the charging contract that the vehicle owner has established with his mobility operator. This allows for a seamless charging experience for the vehicle owner, and to access value-added services after connecting to the charging station.

The value-added service communication is performed separately from the control and measurement communication channel. This is to avoid any interference with the charging related control communication. ISO/IEC 15118 facilitates this by establishing a separate communication channel that is bound to the initial authentication of both peers and outlined in section III.C below.

The following section investigates different options of providing an authenticated channel that is bound to a mutual authentication between the electric vehicle and the charging station.

III. Existing Approaches

There exist different approaches for setting up a communication channel bound to another communication channel, which has certain cryptographic properties like the authentication of a single peer or of both peers. This section investigates known approaches.

A. *Socket Secure – SOCKS*

SOCKS [6] is an internet protocol that allows applications (client or server) to connect through proxies in an application layer independent way. This is done by using a SOCKS proxy that creates a TCP connection to the target server on behalf of the client. As SOCKS operates on layer 5, it can handle different application protocols like HTTP, SMTP, or FTP. It allows a client to open a connection from behind a firewall to an external server in an authenticated and authorized way. SOCKS5 allows for different authentication methods, in which the client authenticates towards the SOCKS server. It may also be used in conjunction with TLS. After authentication and authorization check by the SOCKS server, the application protocol is tunneled over the established connection and forwarded to the external target server.

The authentication is done between the requesting client and the SOCKS server, and the tunneling of the application protocol binds to this authentication. However, the server is not aware of this authentication and needs to authenticate the client by other means. As the tunnel is provided on an application base, multiple tunnels for different applications are necessary, all with an own, independent security setup.

 ISBN: 978-1-68558-007-0

B. *Virtual LAN – VLAN*

VLAN or virtual local area networks are defined in IEEE 802.1Q [7]. The standard defines a logical network and allows the separation of different communication channels on layer 2. Different properties may be assigned in addition to this virtual LAN like performance or throughput. To achieve this, infrastructure components like managed switches are used, supporting the differentiation of traffic according to VLANs. A peer sending information in this VLAN (unicast or multicast) will only reach other peers that are part of the same VLAN.

Two basic approaches exist for VLANs. The first approach is a port-based VLAN in which the association to a logical LAN is done by attaching the client to a dedicated physical port of a managed switch. The second approach is a tagged VLAN, in which the Ethernet frames are tagged with a specific VLAN identifier (VLAN ID). Based on this VLAN tag, a switch can forward the Ethernet frame according to its configuration.

With this, VLANs themselves provide a way to separate traffic, which is also a step towards improved security. The definition of this separation is not done on cryptographic means, as stated before. Therefore, it is recommended to provide additional protection of the communication. Examples are IEEE 802.1X [8], providing port-based access control. With this, a client authenticates to the infrastructure (typically a RADIUS or DIAMETER server) via the infrastructure access network switch using different means, e.g., based on the Extensible Authentication Protocol (EAP) [9]. EAP allows for authentication with username and password, but also for a certificate-based authentication employing a client's X.509 certificate. In addition, MAC security (MACSec), specified in IEEE 802.1AE [8], can be used to provide integrity and/or confidentiality protection for the traffic between the device and the network switch in a hop-by-hop fashion.

Security for VLAN can be provided using additional security means like IEEE 802.1X as outlined. If associated to a dedicated VLAN, quality of service parameter may be assigned.

C. *Transport Layer Security Features*

Transport Layer Security (TLS) is a protocol defined in IETF RFC 5246 as version 1.2 [4]. Meanwhile, it evolved to version 1.3 in IETF RFC 8446 [5]. While version 1.3 is being increasingly adopted [14], version 1.2 is still widely used. TLS is probably the most commonly used security protocol to protect TCP-based communications. Prominent applications are protection of web-based communication over http. Also, other TCP-based protocols leverage the bump in the wire properties of TLS, like ISO/IEC 15118. ISO/IEC 15118-20 mandates the support of TLS v1.3, while TLSv1.2 may still be used.

TLSv1.3 features a re-designed handshake, which is not backward compatible to TLSv1.2. The version handling in TLS allows to fall back to TLSv1.2, if TLSv1.3 is not supported yet. The handshake is encrypted, except for the very first message, to better protect the privacy of client certificate information that is thereby already send encrypted. Moreover, the handshake may already transmit application data, which can accelerate the communication setup. This feature is called 0-RTT (zero round-trip time), but the use requires careful review.

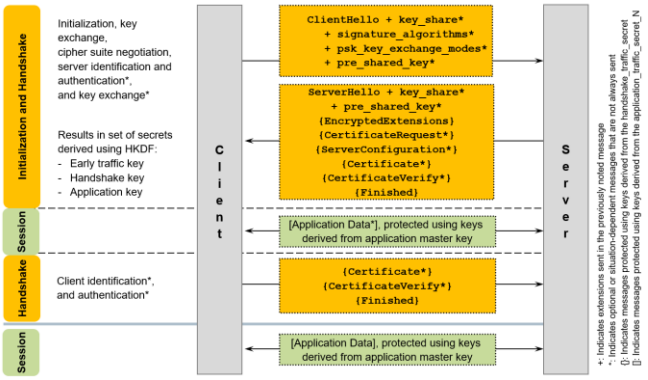

Figure 2. TLS v1.3 Session Establishment with full handshake

The full handshake of TLSv1.3 is depicted in Figure 2. TLS supports different authentication options:

- server-side authentication (mainly used in web traffic) using X.509 certificates;
- mutual authentication involves the client to authenticate using an X.509 certificate in addition to server authentication;
- authentication based on a pre-shared key, which is applied also within TLS as described below;
- authentication based on raw public keys.

Besides the peer authentication, the TLS handshake is used to negotiate further session parameters like the cipher suite for protecting communication integrity and confidentiality.

TLS with mutual authentication is applied in ISO/IEC 15118-20 for plug-and-charge and for access to value-added services. This ensures that billing-relevant charging and service consumption can be associated with a dedicated account.

Besides the establishment of a protected channel, TLS defines further operations for the management of this secured channel, beyond them the update of session parameters during an ongoing session, like the utilized cryptographic key. One important functionality is the so-called session resumption. Session resumption allows a previously established and closed session to be resumed, based on the security parameters negotiated in the initial session. This saves the asymmetric cryptographic operations during the TLS handshake, and it utilizes a pre-shared key included in a ticket from the initial handshake. Note that there is a timely limitation how long a closed session may be resumed, depending on the TLS version. While TLSv1.2 recommends 24 hours, TLSv1.3 limits the validity time in the tickets used for resumption to seven days.

Besides the re-establishment of a closed connection, TLS session resumption may also be used to "clone" an existing session. This can be achieved by opening a TLS connection to a different port on the target host than the original one used and referencing the existing session. Using this, a separate TLS-protected TCP communication channel is established.

 ISBN: 978-1-68558-007-0

As the second communication channel relies on the security parameters of the first one and thus is cryptographically bound to it, it also provides the assurance of mutual authentication to both participants.

ISO/IEC 15118 utilizes this feature to allow the establishment of value-added service communication channels. Note that these are currently restricted to TCP-based communications. There also exists a TLS-like protocol with Datagram Transport Layer Security protocol (DTLS, IETF RFC 9147, [11]) that provides a similar functionality as TLS, but for UDP-based communications. It could be used to protect, e.g., media traffic, which is often transmitted via UDP. Note that interactions between both (TLS and DTLS) are not considered in ISO/IEC 15118, as the protection of the actual value-added service data is left to the value-added service itself.

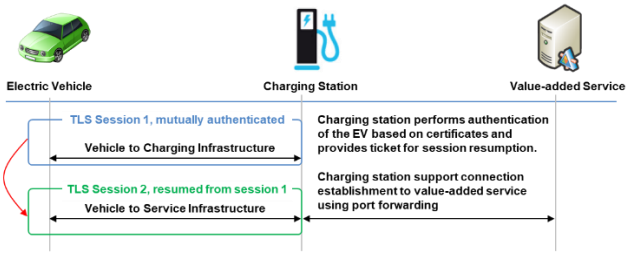

Figure 3. TLS Session Resumption to establish second communication channel

As shown in Figure 3, a second session is opened between the electric vehicle and the charging station using TLS session resumption. This saves communication overhead and provides a binding to the TLS channel protecting the ongoing charging session. Note that while TLSv1.3 has specific optimizations like sending application data already in the resumed handshake (called 0-RTT), this feature is not allowed in ISO/IEC 15118 to avoid replay attacks of application data.

Port forwarding is used at the charging station to forward the traffic to the intended value-added service provider. The security of the communication channel to the value-added service provider is out of scope of ISO/IEC 15118 and needs to be defined and setup by the value-added service separately. For protecting UDP-based traffic between the electric vehicle and the charging station, OpenVPN is mentioned.

D. TLS Channel Binding

IETF RFC 5929 [12] describes a binding of a higher layer communication protocol to a negotiated TLS channel. Different approaches are specified. The most versatile is the definition of the *tls-unique* value. The *tls-unique* value is essentially the first "Finish Message" sent in the latest TLS handshake. The finish message contains a hash over all messages exchanged in the handshake phase.

This definition makes this parameter specific to a session. When a session is resumed or renegotiated (only for TLS 1.2), the *tls-unique* value will change accordingly. This has to be obeyed by the applying application. Using *tls-unique* in an application provides a direct linkage to the properties of the TLS handshake.

An example is the application in the context of Enrollment over Secure Transport (EST, IETF RFC 7030, [13]), a certificate enrollment protocol executed over TLS. In this protocol, the client sends a certification request to enroll a new client certificate. The certification request is signed with the private key of the freshly generated key pair. This provides a proof-of-possession to the receiver, that the sender, i.e., the client, knows the private key corresponding to the contained public key. Part of the certification request can be a *tls-unique* value. As the TLS handshake is performed with mutual authentication, the receiver gets in addition a proof-of-identity of the client, due to the link to the utilized client certificate in the TLS handshake. This is enabled through the inclusion of the *tls-unique* value.

IV. Solution Proposal

As discussed in section I, the aim is to propose a solution for setting up an additional wireless communication channel that utilizes a previously established communication channel. The existing solutions discussed in section III provide elements that are used in the approach.

The following description takes the electric vehicle charging as example as in section II and provides an alternative solution. This described solution specifically allows for multiple connections between a value-added service provider and an electric vehicle, which are all bound to an existing charging session. These multiple channels may be of different nature like TCP/IP or UDP/IP traffic.

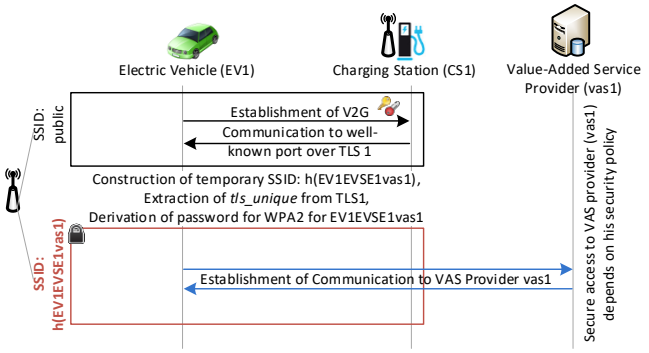

Figure 4. Application of *tls-unique* to protect second WLAN

Figure 4 provides an overview of the solution. According to ISO/IEC 15118-20, a TLS connection is established between the electric vehicle *EV1* and the charging station *CS1* via a well-known service-set identifier (SSID) of the charging station. The well-known SSID may be either preconfigured, or it may be broadcasted using Bluetooth beacons in the vicinity of the charging station. The connection is established based on the authentication of CS1 as server towards EV1. The EV1 authentication can be carried out over the already TLS protected link to protect the identity information of EV1. The client-side authentication may be done based on an X.509 certificate but also using other methods on application layer like HTTP digest authentication or based on a token. Specific for the electric vehicle charging, the owner of the EV may also authenticate directly towards the charging station, avoiding any information to be transmitted over the communication link. In each case, a binding to the originally established TLS connection is required.

 ISBN: 978-1-68558-007-0

To achieve this, the *tls-unique* value is extracted, which is intended as means to provide the binding to the originally established TLS channel for further connections to be opened. This extraction equals to the TLS channel binding described in section III.D.

Over the established TLS channel, an information is provided to the electric vehicle regarding available value-added services via the charging station, which can be consumed during the charging period. These value-added services may be software updates for the infotainment system, normal web access, gaming, or videos to bridge the charging time.

While in section II the additional communication channel for value-added services is opened using TLS session resumption on a different port than the one for the charging communication, the following describes an alternative, which can be used for different types of data exchange.

When the EV selects a value-added service, it will receive the additional configuration information for setting up a second, temporary WLAN access to the charging station for the electric vehicle. The configuration information shall be specific to the charging session between EV1 and CS1 and a specific value-added service provider vas1. This allows for correct billing of consumed services, based on the association.

For setting up a temporary access point, a second network access policy needs to be provided, which may comprise information regarding protection means or quality of service parameter. In case of WLAN, a temporary network name (SSID) and a pre-shared key for access protection to the temporary WLAN are also required to utilize WPA2 and WPA3 for access protection to the temporary WLAN.

Instead of providing this information directly. it can be derived locally on the communication peers based on the already existing charging control communication session as following:

Temporary SSID = Hash (EV ID | CS ID | VAS ID)

In the example in Figure 4, this will result in the hashed value of "*EV1CS1vas1"*. Depending on the utilized hash function the result can be truncated to, e.g., 20 Bytes. With the goal to bind the temporary WLAN to the already existing charging session, the temporary WLAN access credentials in terms of a shared secret are derived incorporating the *tls-unique* value of the initial TLS session as following:

Temp. SSID PW = Hash (tls-unique | EV ID | VAS ID)

The derivation may consist of further parameter besides the EV identifier and the VAS identifier. Depending on the security policy of the charging station operator, the temporary WLAN access for the value-added services may be terminated as soon as the charging session ends. There may be cases for leaving the session open for a grace period, e.g., for ending a specific transaction. This option may also be part of the contract a customer has with a specific charging station operator.

As described, the approach can be generalized to provide the binding also to other network access methods like 4G or 5G. It may also be leveraged to setup further VLANs for separate communication, utilizing derived parameter for VLAN name and access credentials.

V. EVALUATION

The evaluation of the proposed solution is done based on the concept only, as it has not been implemented, yet. In general, the security of an industrial system is evaluated in practice in various approaches and stages of the system's lifecycle:

– A Threat and Risk Analysis (TRA, also abbreviated as TARA) is typically conducted at the beginning of the concept definition, as for ISO/IEC 15118, product design or system development, and updated after major design changes, or to address a changed threat landscape. In a TRA, possible attacks (threats) on the system are identified. The impact that would be caused by a successful attack and the probability that the attack happens are evaluated to determine the risk of the identified threats. The risk evaluation allows to prioritize the threats, focusing on the most relevant risks and to define corresponding security measures. Security measures can target to reduce the probability of an attack by preventing it, or by reducing the impact.

– Security checks can be performed during operation or during maintenance windows to determine key performance indicators (e.g., check compliance of device configurations) and to verified that the defined security measures are in fact in place.

– Security testing (penetration testing, also called pentesting for short) can be performed for a system that has been built, but that is currently not in operation. A pentest can usually not be performed on an operational automation and control system, as the pentest could affect the reliable operation auf the system. Pentesting can be performed during a maintenance window when the physical system is in a safe state or using a separate test system.

As long as the solution proposed in the paper has not been proven in a real-world operational setting, it can be evaluated conceptually by analyzing the impact that the additional security measure would have on the identified residual risks as determined by a TRA. The main objective is to determine the specific benefits that are relevant for the selection of a suitable protection approach. The main aspects relevant for the evaluation of the proposed solution are:

a. The level of isolation of different types of communications (charging control communication; value added services communication);

b. the scope of protection, i.e., what exactly is protected concerning integrity and or confidentiality, and

c. the flexibility to use it for various protocols used by different value-added services.

These aspects can be evaluated qualitatively as follows:

a. The control communication for charging control and the communication of value-added services are taking place on separate layer 1 / layer 2 communication links. While a reliable traffic isolation can be implemented also on a

 ISBN: 978-1-68558-007-0

logical level, the isolation realized by having separate layer 1 / layer 2 communication links ensures by design a strong isolation, avoiding logical interference between these different types of communications. Moreover, this separation offers the option to not only provide different protection options for the communication links, but also to assign different quality of services classes to ensure for instance a dedicated throughput or latency.

b. The proposed solution protects all communications, including, e.g., dynamic host configuration by DHCP or IPv6 auto configuration, or DNS requests. Thereby, also user privacy protection is increased, as meta-data of communication as, e.g., network addresses, cannot be intercepted as all communication is protected on layer 2. Also, active manipulations by 3rd parties, e.g., injected false DNS responses, can be avoided.

c. The solution can be used with any types of communication, including UDP datagram communication. So, it can be flexibly applied also for value-added services using UDP-based communications (e.g., multi-media communications based on RTP).

VI. CONCLUSION

This paper provides a new generic approach for setting up a separate temporary network access channel allowing to assign specific quality of service parameter to the new network access, which is cryptographically bound to an already established communication channel. The approach is discussed in the context of electric vehicle charging combined with value-added services.

The advantage of the proposed approach is the ability to be applied in an application layer protocol independent way by preserving the privacy of user credentials for observers of the network. This is especially important for wireless communication as the exchanged communication can be easily accessed.

The proposed approach is available as concept and needs to be implemented a proof of concept, which would be a future intended step. Such a proof of concept can leverage already specified base mechanisms like *tls-unique* extraction.

REFERENCES

[1] ISO/IEC 15118-20: Road vehicles — Vehicle-to-Grid Communication Interface — Part 20: Network and application protocol requirements, Work in Progress

[2] CHAdeMO, https://www.chademo.com/, [retrieved: July, 2022]

[3] R. Falk and S. Fries, “Electric Vehicle Charging Infrastructure – Security Considerations and Approaches”, Internet 2012, June 2012, ISBN: 978-1-61208-204-2, pp.58-64

[4] T. Dierks and E. Rescorla, IETF RFC 5246, “Transport Layer Security (TLS) Protocol v1.2, 08/2008, https://tools.ietf.org/html/rfc5246, [retrieved: July, 2022]

[5] E. Rescorla, IETF RFC 8446, “Transport Layer Security (TLS) Protocol v1.3”, 08/2018, https://tools.ietf.org/html/rfc8446, [retrieved: July, 2022]

[6] M. Leech et al., IETF RFC 1928, „SOCKS Protocol Version 5, 03/1996, https://tools.ietf.org/html/rfc1928, [retrieved: July, 2022]

[7] IEEE 802.1Q, “IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks”, 2018, https://standards.ieee.org/ieee/802.1Q/6844/, [retrieved: July, 2022]

[8] IEEE 802.1X, “IEEE Standard for Local and Metropolitan Area Networks – Port-Based Access Control”, 2020, https://ieeexplore.ieee.org/document/9018454, [retrieved: July, 2022]

[9] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H.Levkowetz., IETF RFC 3748, “Extensible Authentication protocol (EAP)”, 06/2004, https://tools.ietf.org/html/rfc3748, [retrieved: July, 2022]

[10] IEEE 802.1AE “IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security”, 2018, https://ieeexplore.ieee.org/document/8585421, [retrieved: July, 2022]

[11] E. Rescorla, H. Tschofenig, and N. Modadugu, IETF RFC 9147, “The Datagram Transport Layer Security (DTLS) Protocol Version 1.3”, April 2022 https://datatracker.ietf.org/doc/html/rfc9147, [retrieved: July, 2022]

[12] J. Altman and N. Williams, IETF RFC 5929, TLS channel binding, July 2010, https://tools.ietf.org/html/rfc5929, [retrieved: July, 2022]

[13] M. Pritikin, P. Yee, and D. Harkins, IETF RFC 7030, “Enrollment over Secure Transport “, 10/2013, https://tools.ietf.org/html/rfc7030, [retrieved: July, 2022]

[14] SSL Puls: TLS Dashboard, continuously updated, https://www.ssllabs.com/ssl-pulse/, [retrieved: July, 2022]

 ISBN: 978-1-68558-007-0