

Secure and flexible establishment of temporary WLAN access



Steffen Fries, Rainer Falk, T CST, Siemens

Authors' background: Applied industrial research at Siemens Technology

Cyber Security for Industrial Systems

- Industrial systems need a security design that address the relevant security objectives and respect side conditions for the specific environment (e.g., lifetime, real-time, safety, usability).
- The industrial security standard IEC62443 is applied in different verticals. The responsibilities of the different roles (system operator, integrator, component manufacturer) are distinguished.
- Both authors are engaged in different standardization activities to address IEC 62443 security requirements by specific technical means.
- The security solution as proposed in this presentation addresses certain requirements from IEC 62443 and supports overall system security.

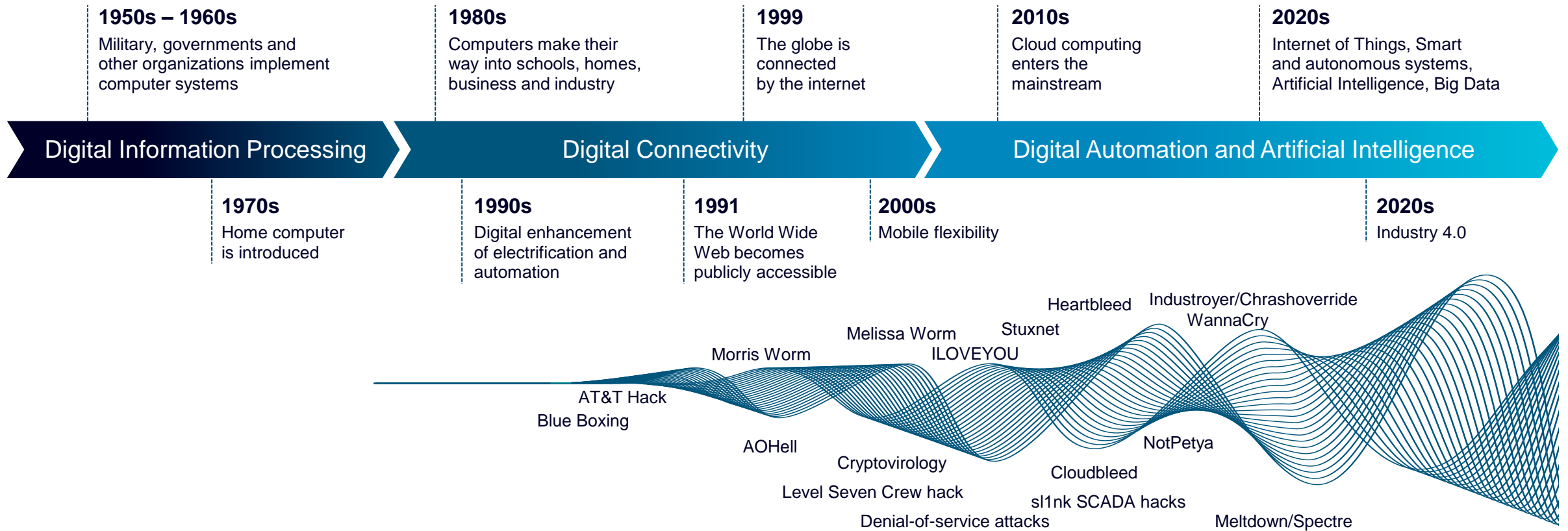


Dr. Rainer Falk
Principal Key Expert
Siemens Technology



Steffen Fries
Principal Key Expert
Siemens Technology

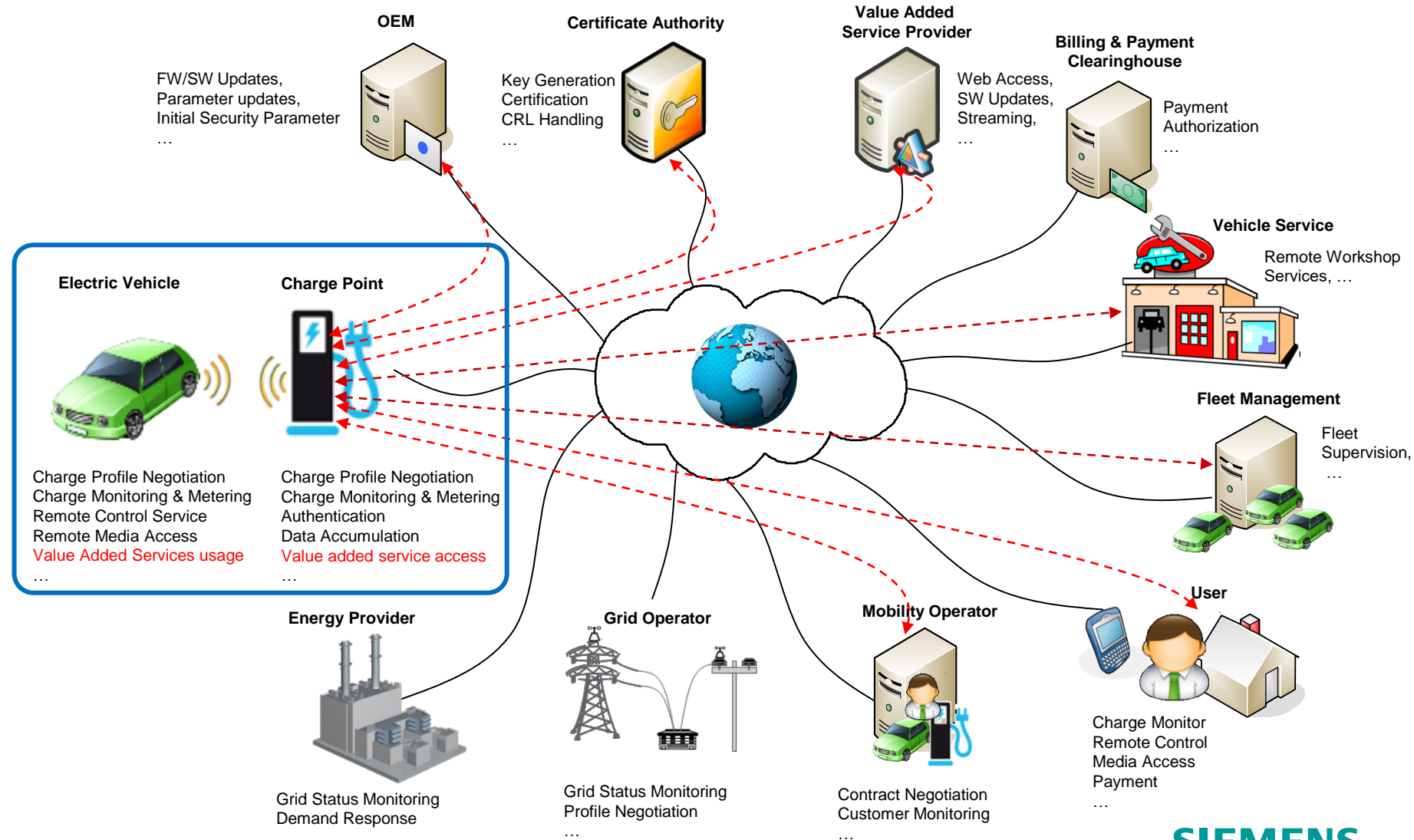
Security must be continuously adopted to the changing threat and vulnerability landscape



Example target use case: Value added service provisioning during electric vehicle charging

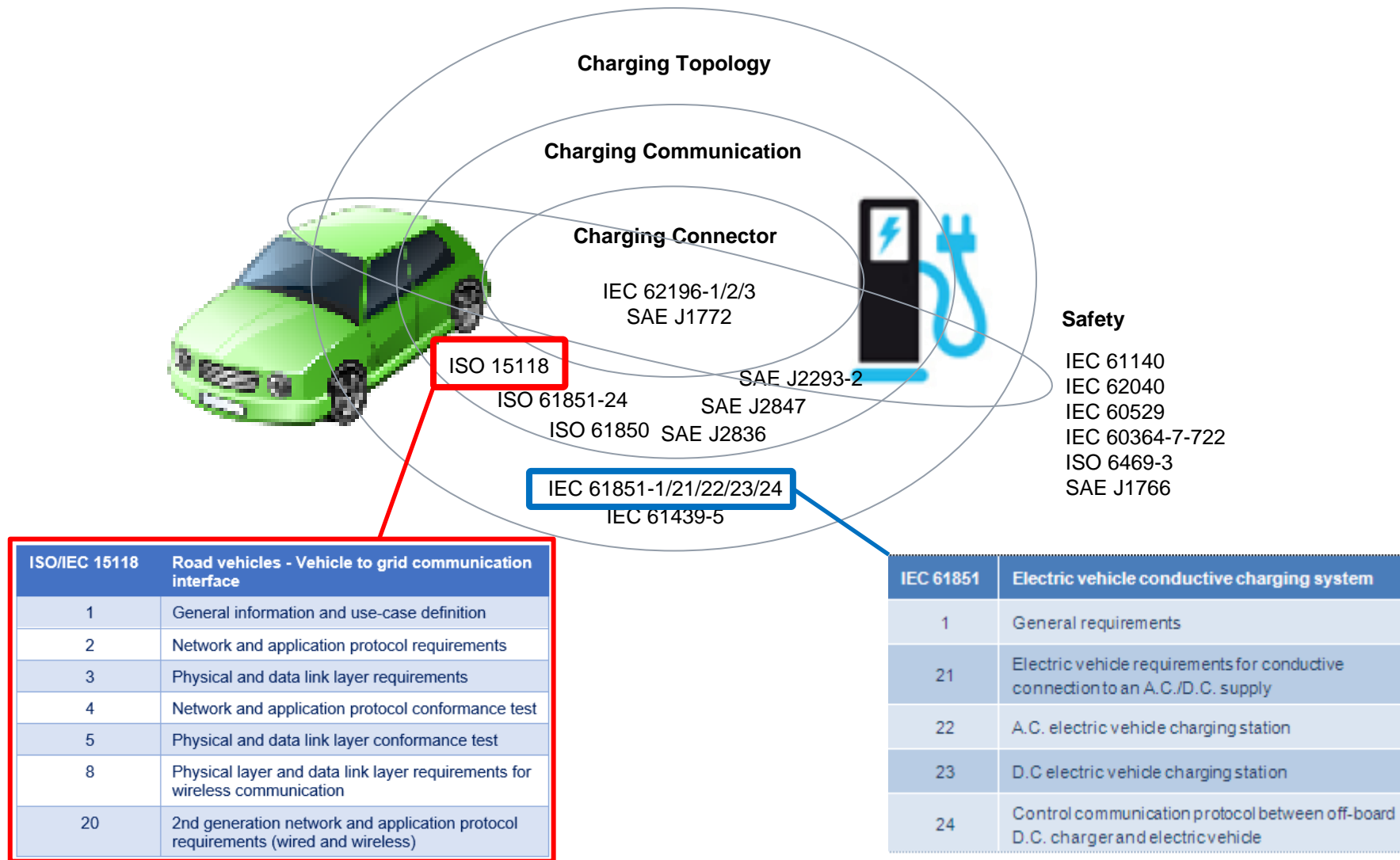
Problem statement

- Various services exist with which electric vehicles may communicate during charging
- Service-related communication during a charging session of an electric vehicle may be an additional offer from charge point operators.
- Binding of service-related communication to a charging session is required for billing and use control of communication facilities.

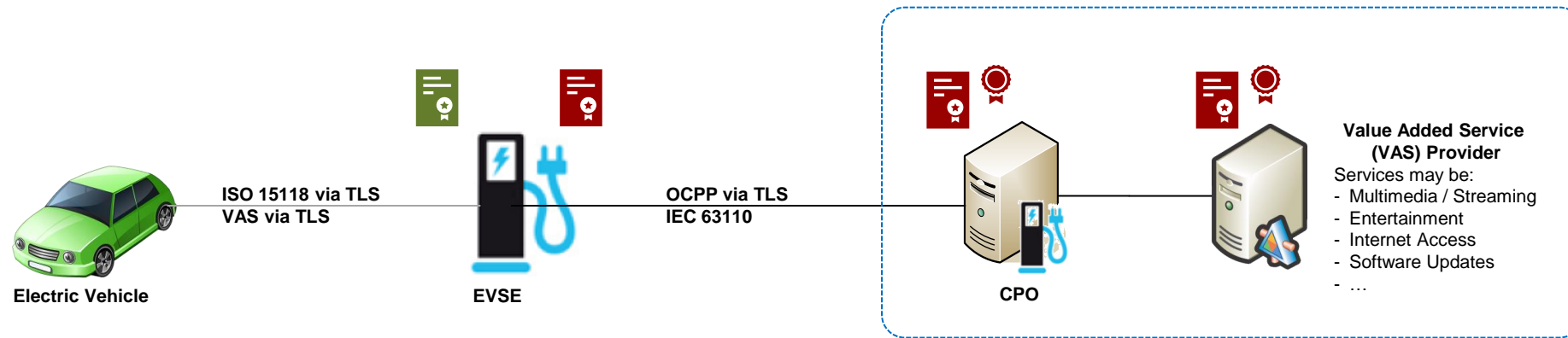


Communication standards around the Vehicle-to-Grid (V2G) charging interface



- ISO/IEC 15118 specifies the communication interface between an electric vehicle and a charging point and is applicable to conductive and wireless vehicle charging.
- Security is an integral part of the standard protecting the charging control communication.
- Security is based on X.509 certificates for authentication, TLS to protect the communication and additional security functionality (firewall) in the charging point.



Architecture for value added service provisioning during electric vehicle charging



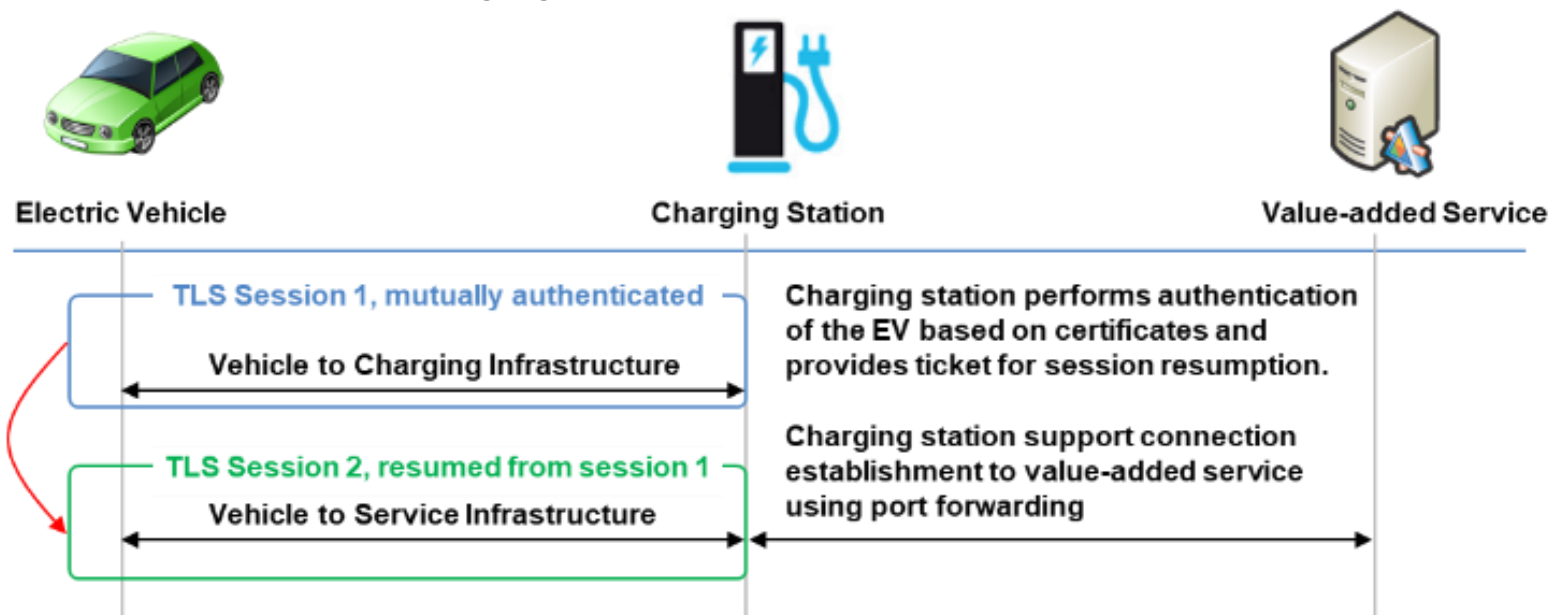
Prerequisite

- Electric vehicle (EV) possesses OEM X.509 certificate and corresponding private key. Distribution of contract related key (X.509 certificate and corresponding private key) specified in ISO 15118.
- Charging Station (EVSE, electric vehicle supply equipment) authenticates towards the EV using a short-term certificate  in the context of a TLS connection establishment. The certificate may be issued by the charge point operator (CPO) certification authority (must have certification path to the V2G Root CA (validated by the EV)).
- EVSE authenticates towards the CPO backend using a long-term certificate . This is issued by the CPO certification authority and may be independent from V2G Root CA.
- The value added service provider may possess a X.509 certificate, to authenticate to the EV (out of scope for ISO/IEC 15118).

Value added service provisioning according to ISO/IEC 15118

- ISO/IEC 15118-20 specifies the control communication for vehicle charging (conductive and wireless)
- Allows value added service (VAS) provisioning during charging.
- Security of communication considered by specifying firewall behavior on the charging station and protection of VAS communication on the interface between the EV and the Charging Station

- Communication may be protected using
 - Separate TLS connection to VAS port on the charging station
 - Resumed TLS session on VAS port, based on the established charging communication. This allows a cryptographic binding of the VAS communication to the charging session.



- Limitations:** Only applicable for TCP-based VAS services

Investigation into existing technologies to enable secure access to value added services using non-TCP/IP communication.

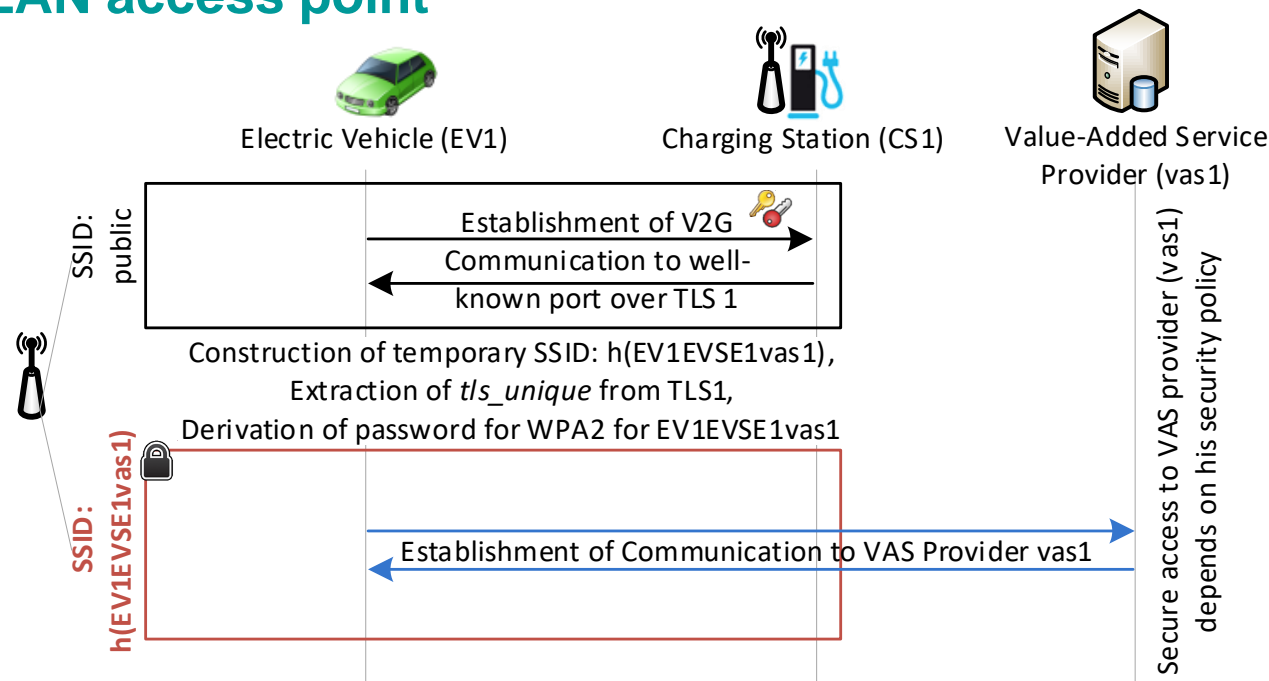
Multimedia services often utilize UDP/IP based communication for real-time transmission of media data or streaming data. Different technologies exist to also enable secure transmission of these data:

- **SOCKS (Secure Sockets):** Internet protocol operating on OSI layer 5 that allows applications to connect through proxies in an application layer independent way. Also relies on TCP for a connection to the target server on behalf of the client. It may also be used in conjunction with TLS. → not applicable as it uses TCP/IP
- **VLAN: (Virtual LAN, IEEE 802.1Q):** Logical network, allows separation of different communication channels on layer 2. Different properties may be assigned to this virtual LAN like performance or throughput. VLANs may be supported either as port-based VLANs (infrastructure switch) or tagged VLANs (requires the client to know the VLAN tag). → Only tagged VLAN applicable but requires the client to know the tag.
- **DTLS (Datagram Transport Layer Security, IETF RFC 9147):** allows similar services like TLS but for UDP/IP communication. Requires DTLS connection from EV to charging point (for the binding to an existing session) and further to VAS provider (for user authentication). Requires UDP/IP support in charging points. Out of scope of ISO/IEC 15118.
- **Distinct WLAN:** Utilize a temporary WLAN to let the EV connect via the access point of the charging point to a VAS. Communication establishment with the VAS can be done in a VAS specific way.

Proposed solution, using a temporary WLAN access point

Information flow and parameter determination

- 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.
 - 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.
 - Access point parameter like temporary network name (SSID) and a pre-shared key for access protection can be derived locally as following:
 - *Temporary SSID = Hash (EV ID | CS ID | VAS ID)*
 - *Temporary SSID PW = Hash (tls-unique | EV ID | VAS ID); tls-unique is derived from the existing TLS connection*
- Depending on the security policy of the charging station operator, the temporary WLAN for accessing the VAS may be terminated when the charging session ends. Alternatively, there a grace period, e.g., for ending a specific transaction.



Conclusion and outlook

- The paper provides an overview based on existing solutions for cryptographic binding of communication channels and specifically proposes a solution to address a limitation of ISO/IEC 15118 to consider only TCP/IP communication for value-added services.
- On the example of electric vehicle charging, the proposed solution utilizes a local derivation of configuration information for setting up a separate temporary access point dedicated to value-added service communication with one specific electric vehicle. Providing an own access point allows to communicate with a variety of communication protocols (TCP/ IP and UDP/IP), which can be restricted by an operator's security policy.
- Moreover, the proposed solution is flexible as it allows to keep this temporary access point only for the duration of the charging period or to exist even after the actual charging session has ended. This can be determined by an operator's security policy.
- As outlined, different access points are used for the communication, which requires support for handling multiple SSIDs simultaneously an both communication peers. This needs to be obeyed for the implementation.
- The proposed solution has not been implemented, yet. This would be the next consequent step to verify the approach and perform comparative tests with the other considered options in terms of security, flexibility, and setup.