







Key Note, June 25<sup>th</sup>, 2014

# The Value of Security Protocols on the Example of Smart Grid

Steffen Fries, [steffen.fries@siemens.com](mailto:steffen.fries@siemens.com)  
Siemens AG, CT RTC ITS

# Siemens is organized in 4 Sectors: Industry, Energy, Healthcare and Infrastructure & Cities

## Siemens: Facts and Figures

Siemens sectors				Key figures FY 2013
<b>Industry</b>	<b>Energy</b>	<b>Healthcare</b>	<b>Infrastructure &amp; Cities</b>	<ul style="list-style-type: none"> <li>• <b>Sales:</b> ~€ 76 bn.</li> <li>• <b>Locations:</b> In 190 countries</li> <li>• <b>Employees:</b> ~362,000</li> <li>• <b>R&amp;D expenses:</b> ~€ 4.3 bn.</li> <li>• <b>R&amp;D engineers:</b> ~29,800</li> <li>• <b>Inventions:</b> ~8,400</li> <li>• <b>Active patents:</b> ~60,000</li> </ul>
<b>Divisions:</b> <ul style="list-style-type: none"> <li>• Industry Automation</li> <li>• Drive Technologies</li> <li>• Customer Services</li> </ul>	<b>Divisions:</b> <ul style="list-style-type: none"> <li>• Power Generation</li> <li>• Wind Power</li> <li>• Energy Service</li> <li>• Power Transmission</li> </ul>	<b>Divisions:</b> <ul style="list-style-type: none"> <li>• Imaging &amp; Therapy Systems</li> <li>• Clinical Products</li> <li>• Diagnostics</li> <li>• Customer Solutions</li> </ul>	<b>Divisions:</b> <ul style="list-style-type: none"> <li>• Rail Systems</li> <li>• Mobility &amp; Logistics</li> <li>• Low and Medium Voltage</li> <li>• Smart Grid</li> <li>• Building Technologies</li> </ul>	
				
<b>~€ 19 bn.<sup>1)</sup></b>	<b>~€ 27 bn.<sup>1)</sup></b>	<b>~€ 14 bn.<sup>1)</sup></b>	<b>~€ 18 bn.<sup>1)</sup></b>	
<b>Corporate functions</b> <ul style="list-style-type: none"> <li>— Corp. Finance</li> <li>— <b>Corp. Technology</b></li> <li>— Corp. Development</li> <li>— ...</li> </ul>				<b>Corporate Technology</b>

1) Sales in FY 2013

# Corporate Technology has 3 missions

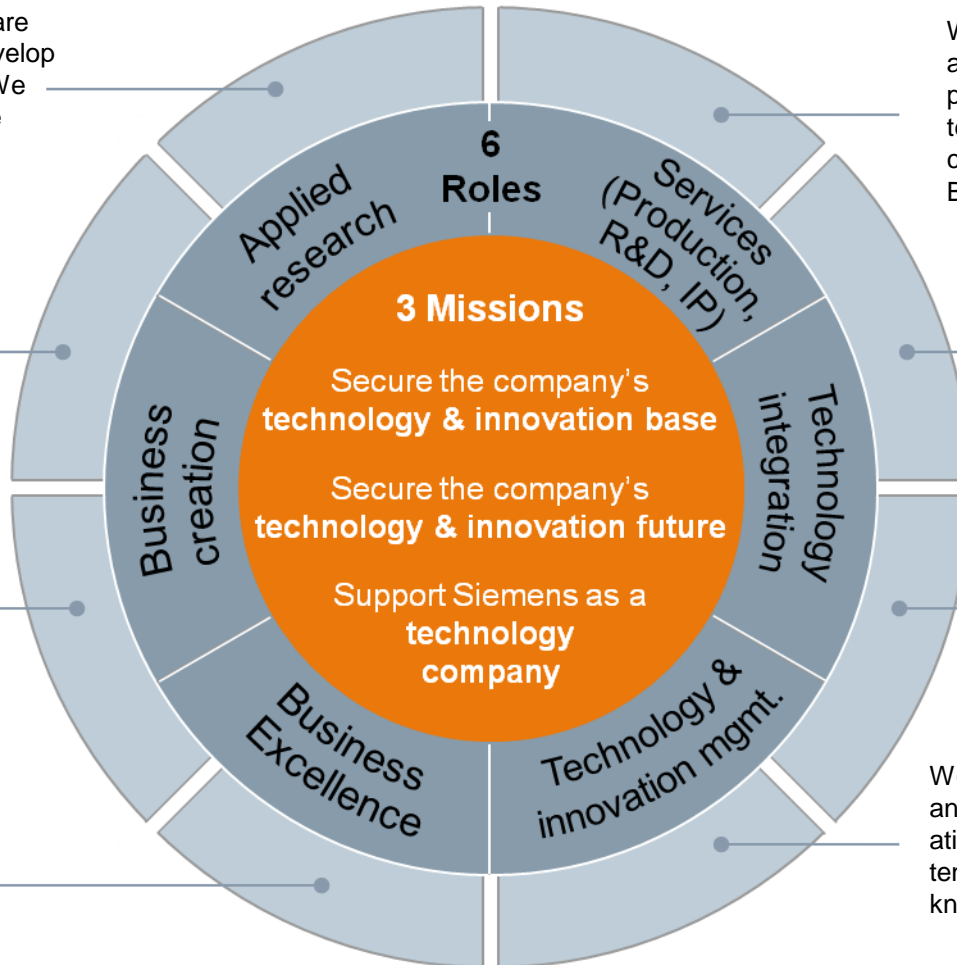
## Corporate Technology: Mission, roles and basic principles

The source of our excellence are our people. We attract and develop creative talents for Siemens. We foster talent exchange with the Business Units.

We foster a culture of innovativeness and high performance and our visibility to all internal and external stakeholders.

We take a focused approach (e.g., in regional setup, technology focus) to achieve high performance.

We primarily serve internal Siemens customers with a global mindset and setup.




We develop Siemens' technology and innovation strategy on corporate level. We ensure seamless technology and innovation processes between Corporate and Business Unit levels.

We deliver services for the businesses as a strategic partner and integral part of their value chain.

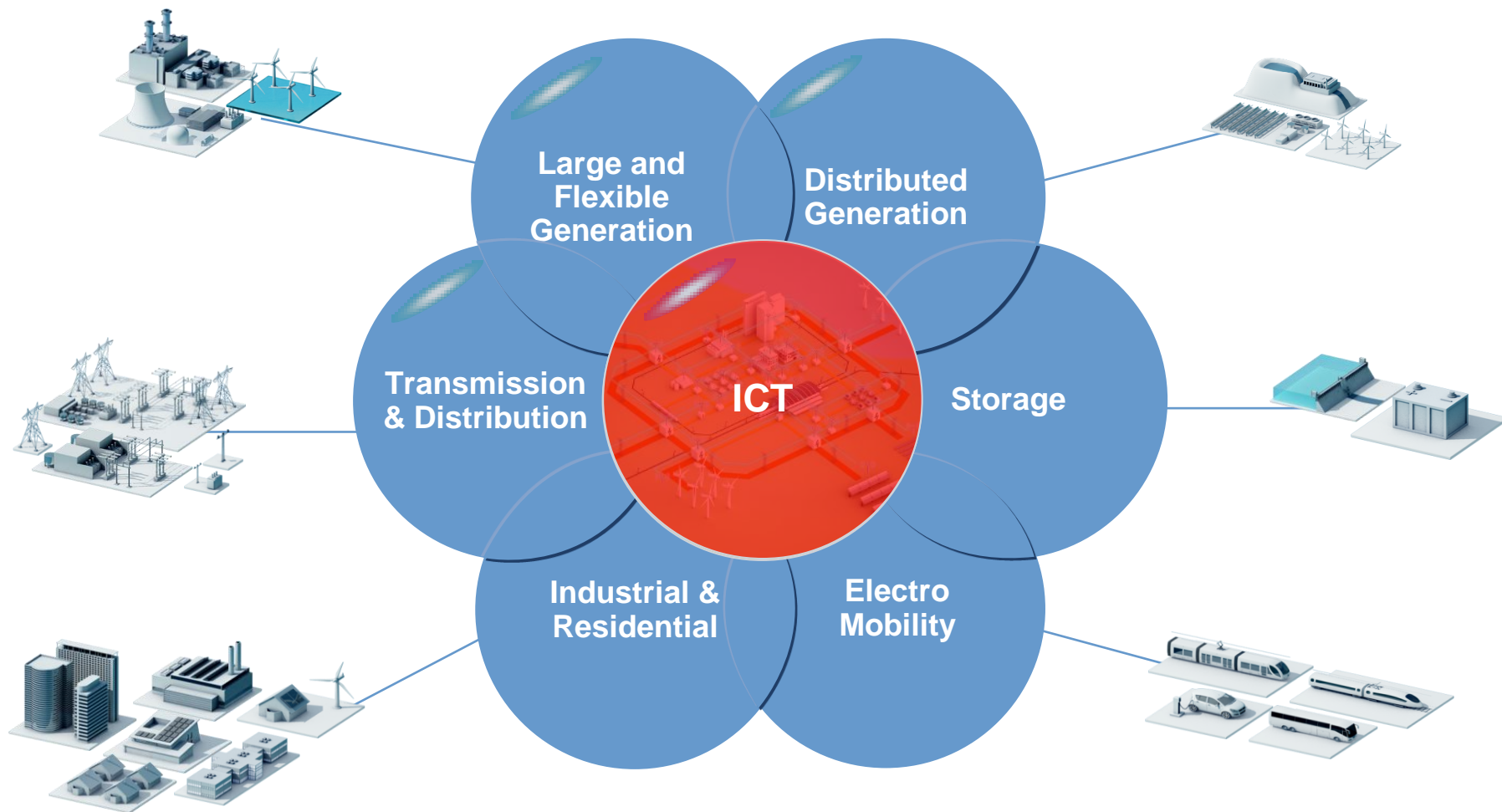
We regularly develop high-impact technologies and innovations for Siemens with a clear focus on results. The business responsibility for implementing innovations lies with the Business Units.

We actively manage our technology and innovation portfolio. We systematically leverage external competence networks to provide the best know-how for Siemens.

# Outline

- 
- ❏ Introduction Smart Grid & Cyber Security
  - ❏ Application of Security Protocols in different Scenarios
    - ❏ Substation Automation
    - ❏ Power Quality Monitoring and Event Collection
    - ❏ DER Integration
    - ❏ Connecting Electric Vehicles to the Charging Infrastructure
  - ❏ Crucial Points for Integrating Security Protocol (Stacks)
  - ❏ Summary & Challenges

# Smart Grid Scope – Incorporation of Decentralized Energy Resources and Flexible Loads requires Security



# What makes Security in Critical Infrastructures like the Smart Grid so important?

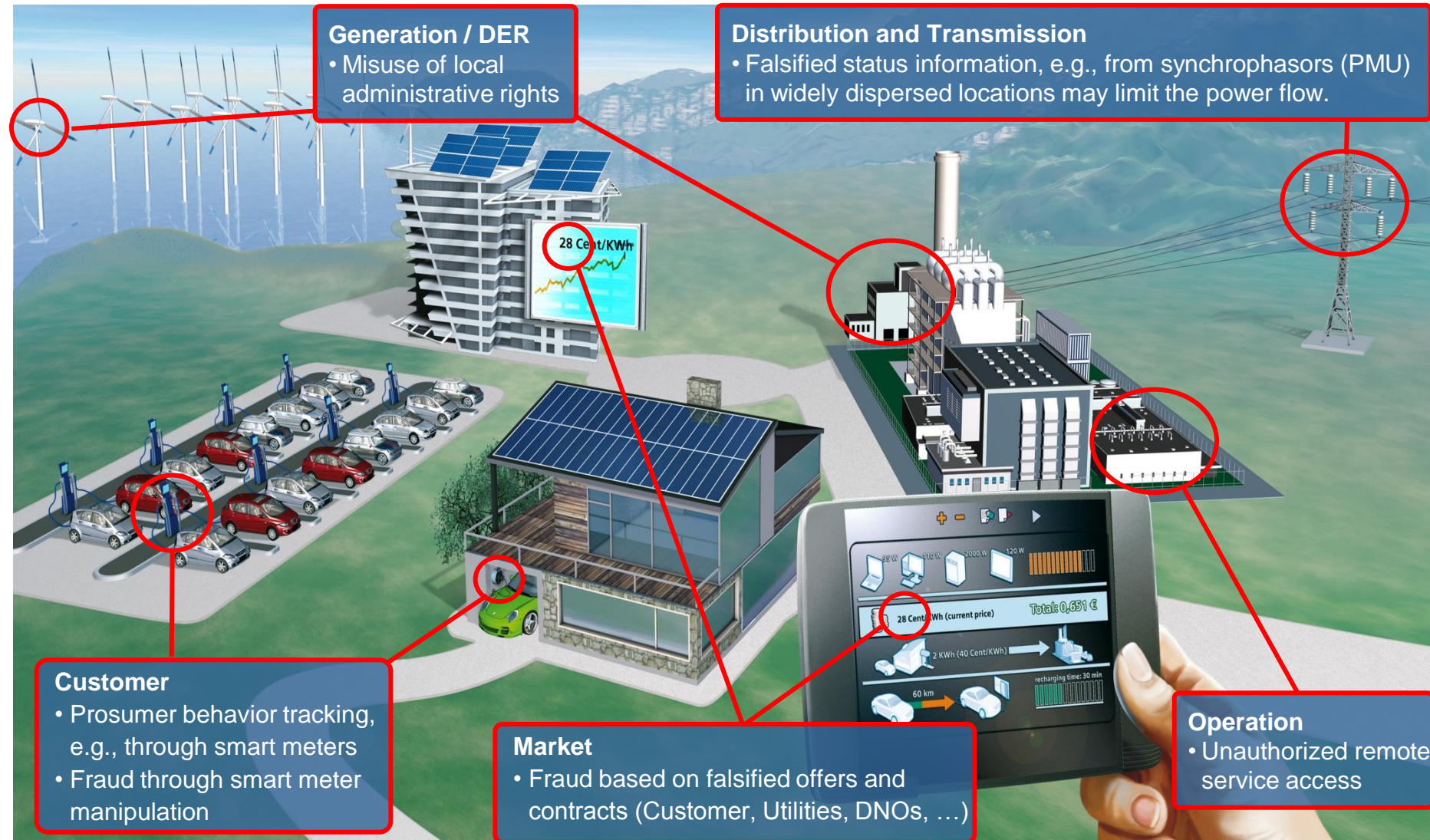
## Security incidents can affect target solution and connected (critical) assets

- Performance degradation
- Loss of system availability & control
- Loss of privacy
- Capturing, modification or loss of data
- Repudiation (Company image)
- Environmental impact
- Financial loss
- Loss of health/life

Secure solutions ensure reliable operation of critical infrastructures

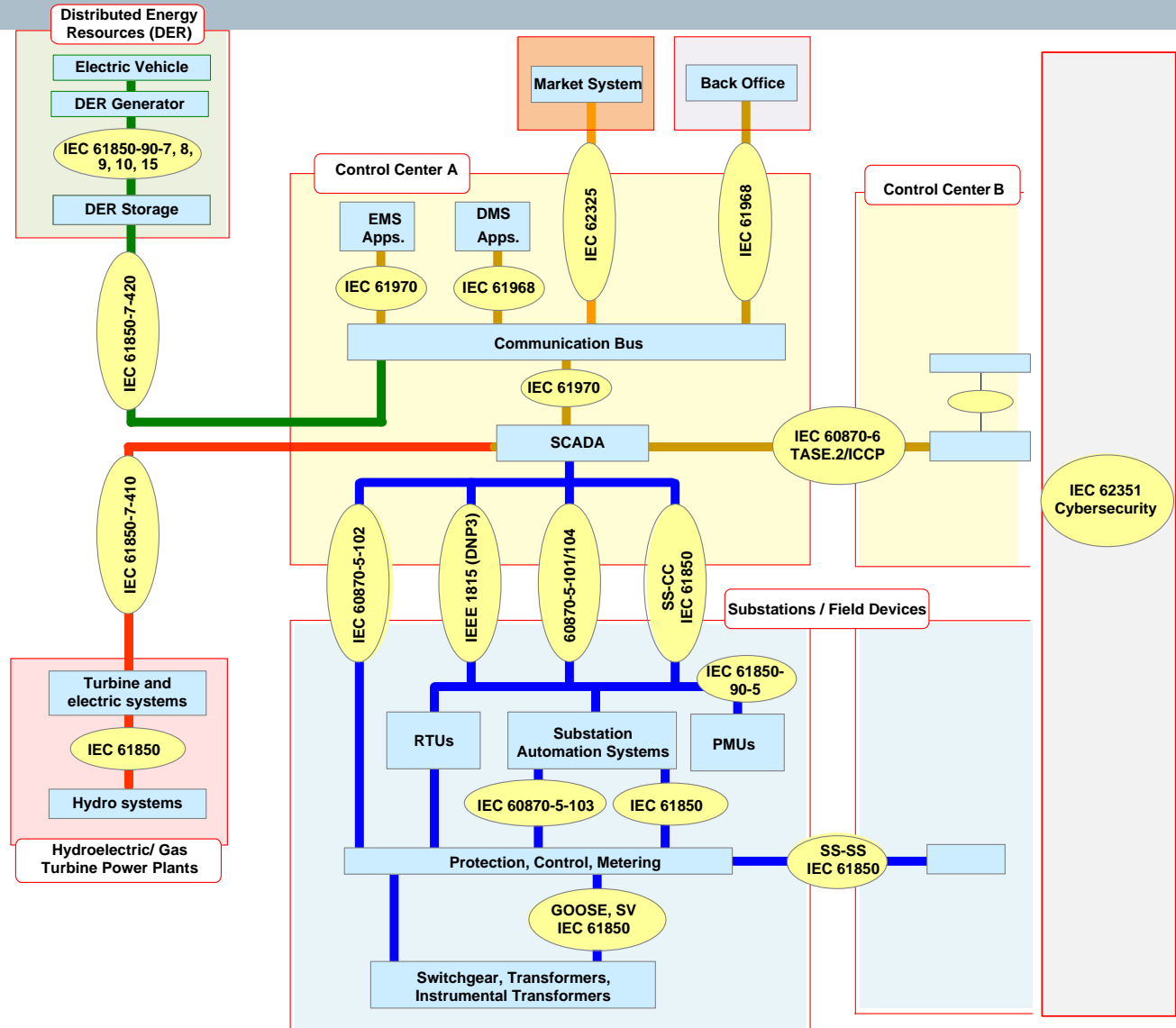


# Security Requirements for Smart Grid Applications stem from a Variety of Potential Attacks (examples)



# Core Communication Standards for Smart Grids – IEC TC57 Reference Architecture

- **IEC 61970 / 61968**  
Common Information Model (CIM)
- **IEC 62325**  
Market Communication using CIM
- **IEC 61850**  
Substation & DER Automation
- **IEC 60870**  
Telecontrol Protocols
- **IEC 62351**  
Security for Smart Grid





# Communication Security provided the naïve way: RFC 3514 “The Security Flag in the IPv4 Header”

Informational RFC ([01.04.2003](#)), Steve Bellovin (AT&T labs)

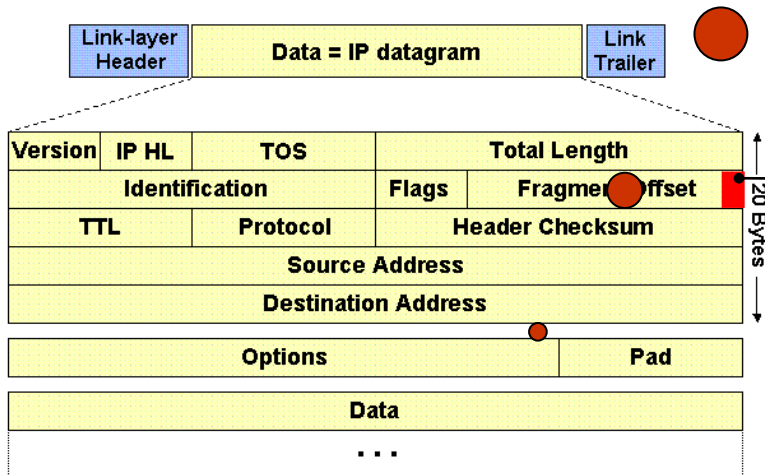
## Basic Idea

- Detection of packets with suspicious addresses
- addresses Filter

Sounds good, but ..., it's a joke 😊

## Concept

- Usage of the unused high-order bits of the offset field to signal malicious content
- For IPv6 options header conveys 128 bit strength indicator



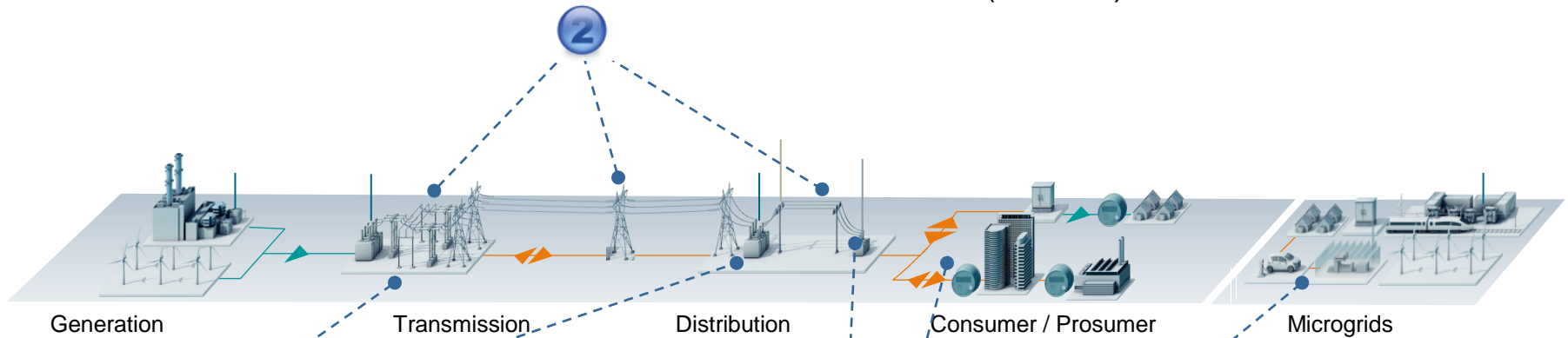
## Evil Flag

- 0x00 – packet has no evil content
- 0x01 – packet has evil content



# Smart Grid Scenario Examples – Secure Communication supports reliable Operation

- Power Quality Monitoring and Event Collection (Transmission/Distribution, Substation)
- Communication Standards used: IEC 61850 (GOOSE)



1

- Substation Automation (Monitoring + Control)
- Remote Service
- Inter Control Center Communication
- Communication Standards used: IEC 60870-5-104, IEC 61850

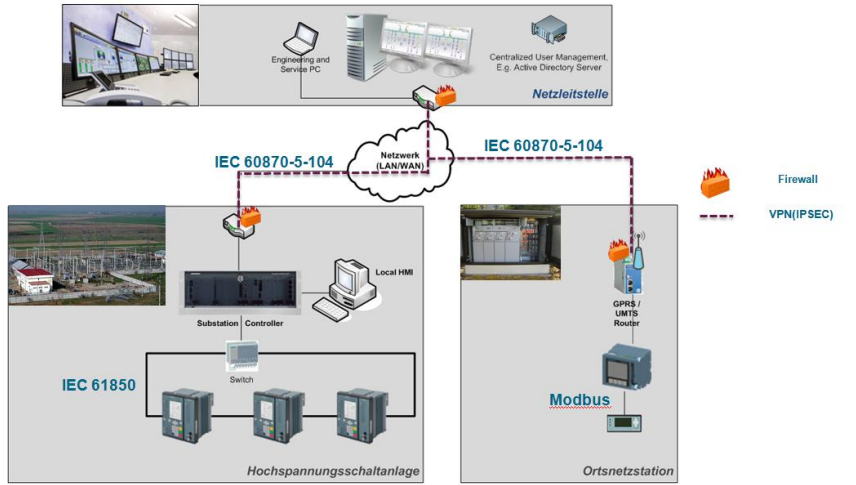
4

- Connecting electric vehicles to the charging infrastructure
- Communication Standards used: ISO/IEC 15118, IEC 61850

3

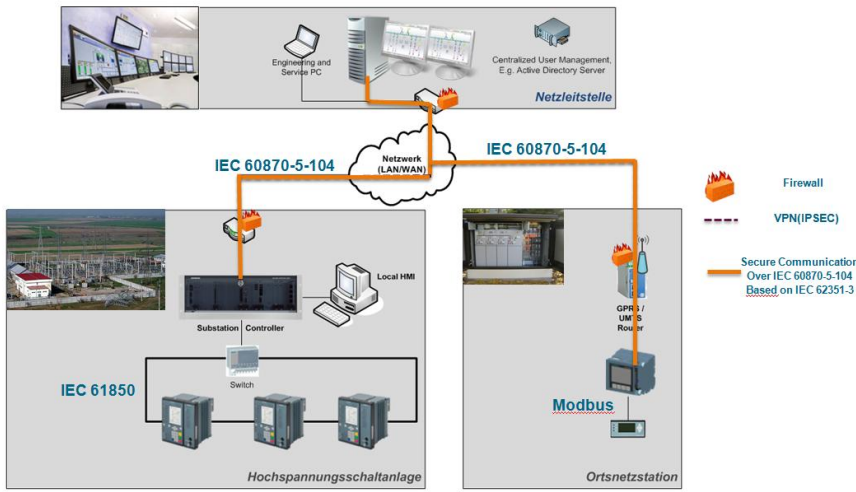
- DER Integration (Metering & Control)
- Communication Standards used: IEC 61850, XMPP (future use)

# Scenario: Substation Automation Applying existing Security Protocols



## Today's Situation

- Communication between substation and control center applies telecontrol protocols like IEC 60870-5-104 and substation automation protocols like IEC 61850. Both base on TCP/IP Communication.
- Additional protocols like VoIP may be used to enable voice/video communication
- Security is often provided by using IPsec based VPNs connecting the two network domains



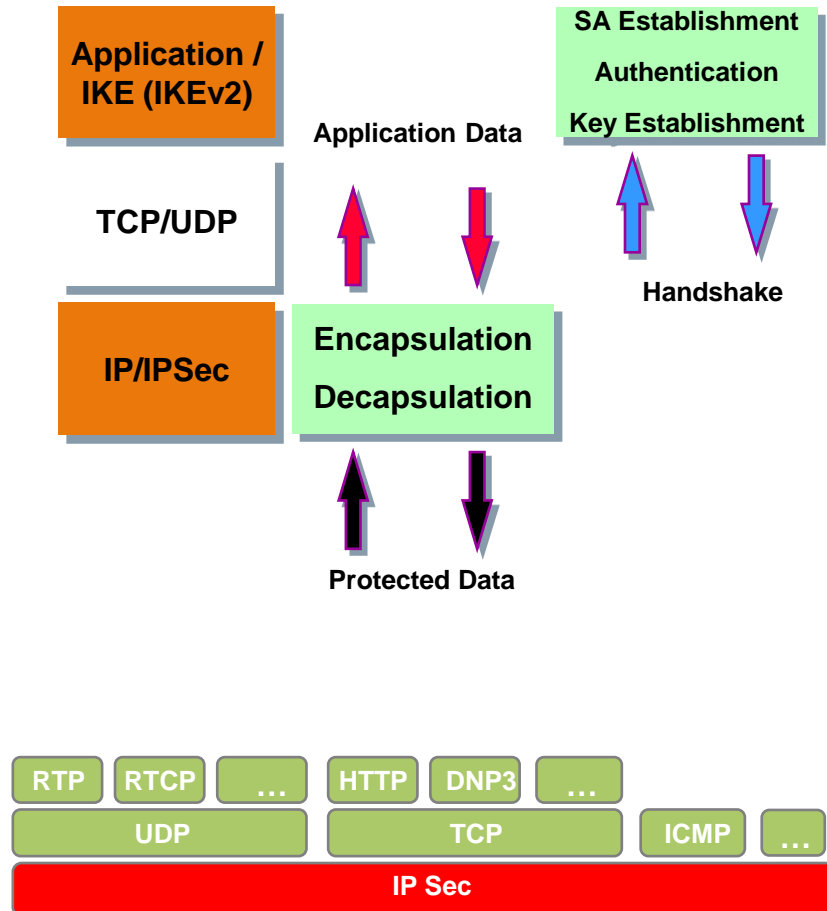
## Way forward targets end-to-end security

- It is desired to ensure that security reaches also “deeper” into the substation to the actual communication end, to support, e.g., RBAC
- IEC 62351 reuses existing security protocols for TCP/IP and profiles TLS (RFC 5246) to ensure end-to-end authentication and integrity and confidentiality.
- Additional means for authentication on application layer are defined, including RBAC based on X.509 certificate enhancements

# Security Protocols used in Scenario 1

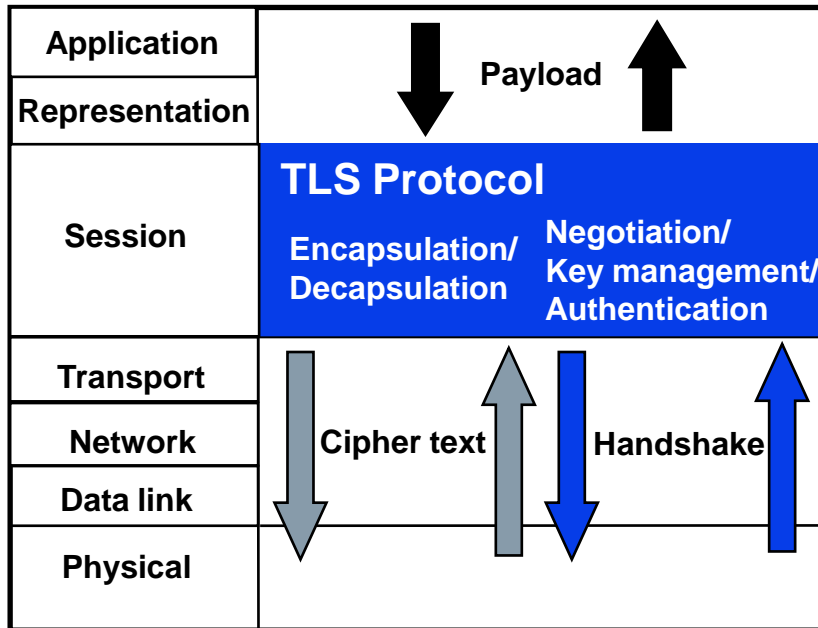
## Internet Protocol Security (IPSec)

- IETF defined protocol: RFCs 4301 (Architecture), RFC 4302 (AH), RFC 4303 (ESP)
- IPSec may be used to secure any protocol transported over IP (IPv4 and IPv6)
- Allows to augment arbitrary client/server applications with classical security services:
  - Mutual entity authentication (via Key Management)
  - Message integrity → RFC 4302 (AH)
  - Confidentiality → RFC 4303 (ESP)
- Security services support host-to-host-, host-to-router-, and router-to-router-communication (VPNs)
- IPSec supports only limited end-to-end security across firewalls
- Key management is handled either manually or automated by using IKE or IKEv2
- Implementation examples: FreeS/WAN, KAME Libipsec, ...



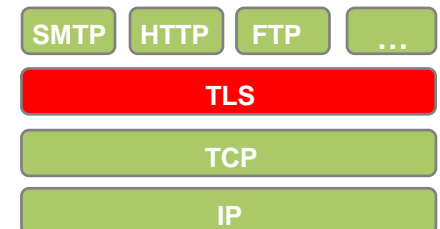
# Security Protocols used in Scenario 1

## Transport Layer Security (TLS)

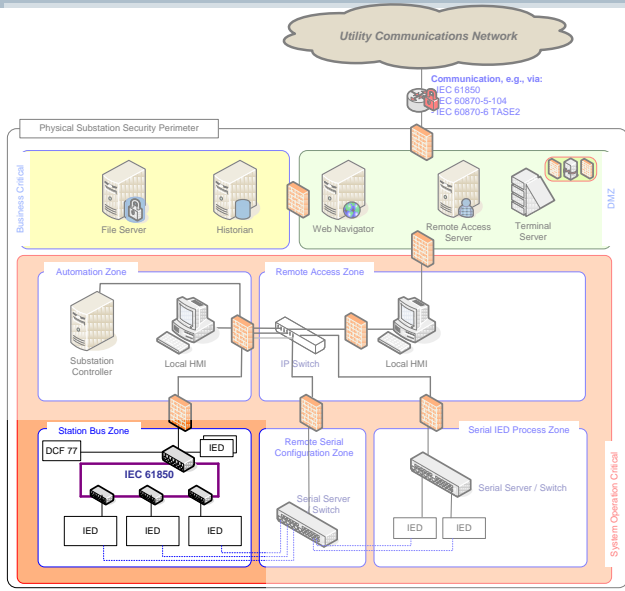


- Independent from application protocols
- Allows to augment arbitrary client/server applications with classical security services:
  - Entity authentication (unilateral, mutual)
  - Message integrity
  - Confidentiality
- Can supply secure end-to-end communications across firewall boundaries.
- Implementation example: openssl, gnuTLS, ...

- TLS specified in RFC 2346 (v1.0) RFC4346 (v1.1), RFC5246 (v1.2)  
→ further extensions to address recently found security flaws
- TLS services are based on
  - X.509-Internet PKI (PKIX) (Certificates and corresponding private key)
  - Reliable transport services (typically TCP)
- Common use cases
  - Secure web connections → https
  - Remote access via SSL/TLS VPNs



# Scenario: Monitoring and Event Collection Applying existing Security Protocols

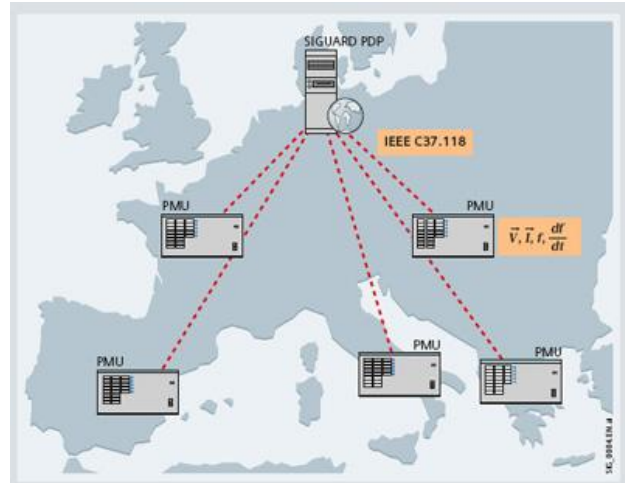


## Substation Internal

- Targets communication of Generic Object Oriented Substation Events (GOOSE), and Sample Values (SV) using, e.g., plain Ethernet as defined in IEC 61850
- Usage of multicast transfer (device local subscription for events)
- Real-time capable security required (message integrity and source authentication)
- Current security target: group based keys used (distributed using existing standards) in conjunction with keyed hashing

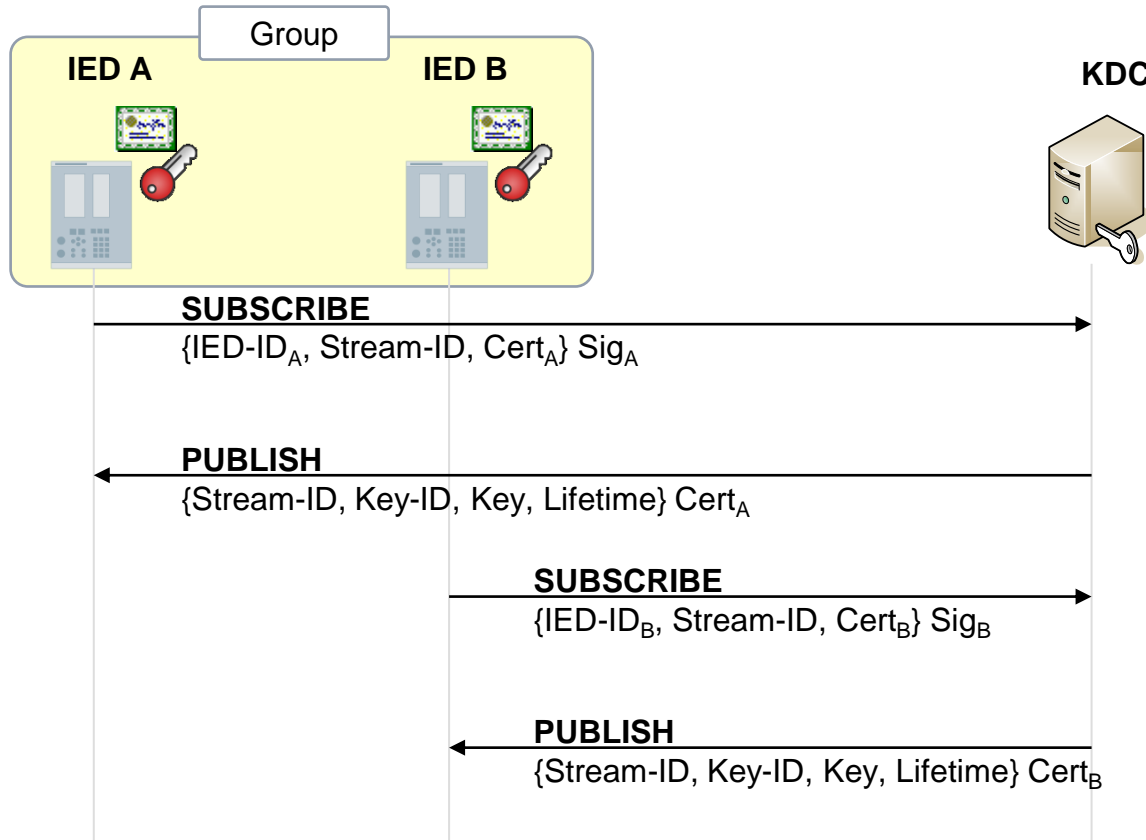
## Wide Area Network Monitoring

- Phasor Measurement Units (PMU) measure current, voltage, phase angle
- Currently communicate via IEEE C37.118 Synchrophasor Protocol
- Future: GOOSE over UDP as further option for communication
- Targets the same security approach as in substation GOOSE



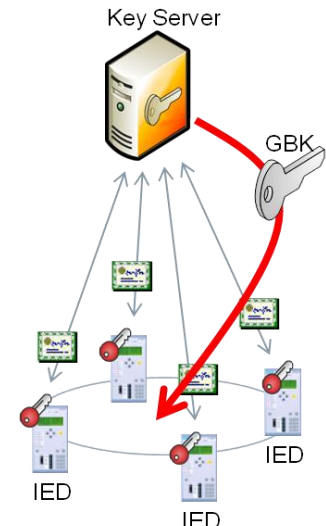
# Group based Key Management provides solution for Substation and Wide Area GOOSE/SV

- Application of a group based key to distribute group key to be used for achieve message integrity.
- IED authenticate towards KDC using IED specific certificates and corresponding private keys
- Key Management based on Group Domain of Interpretation (GDOI, RFC 6407)

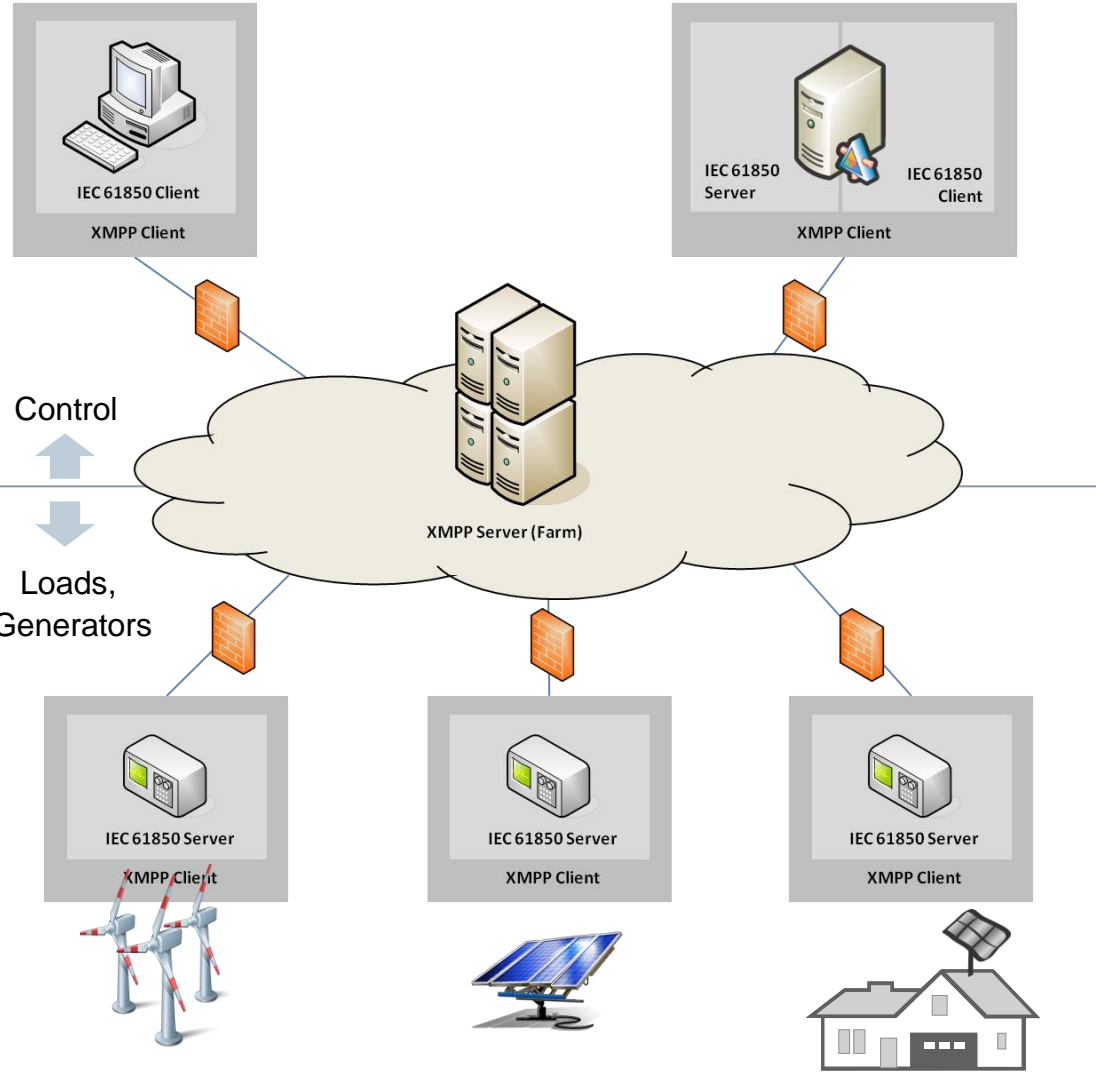


## Key Distribution Center (KDC)

- pre-configured data stream related IED access list
- different data streams
- generates data stream related (group) keys
- May be realized as component within a distinct IED



# Scenario: Integration of Distributed Energy Resources (DER) into Grid Control



## Secure DER integration

- Prosumer or microgrid operator connecting resources and loads to the electrical grid
- Resources and loads need to be known at the control center to ensure grid stability
- Communication controller likely to be operated behind Firewall and NAT
  - Address resolution of target controller may not be always possible
- Inbound connection establishment may not be possible



# Integration of DER into Grid Control

## Application of existing and new security means

### Communication approach

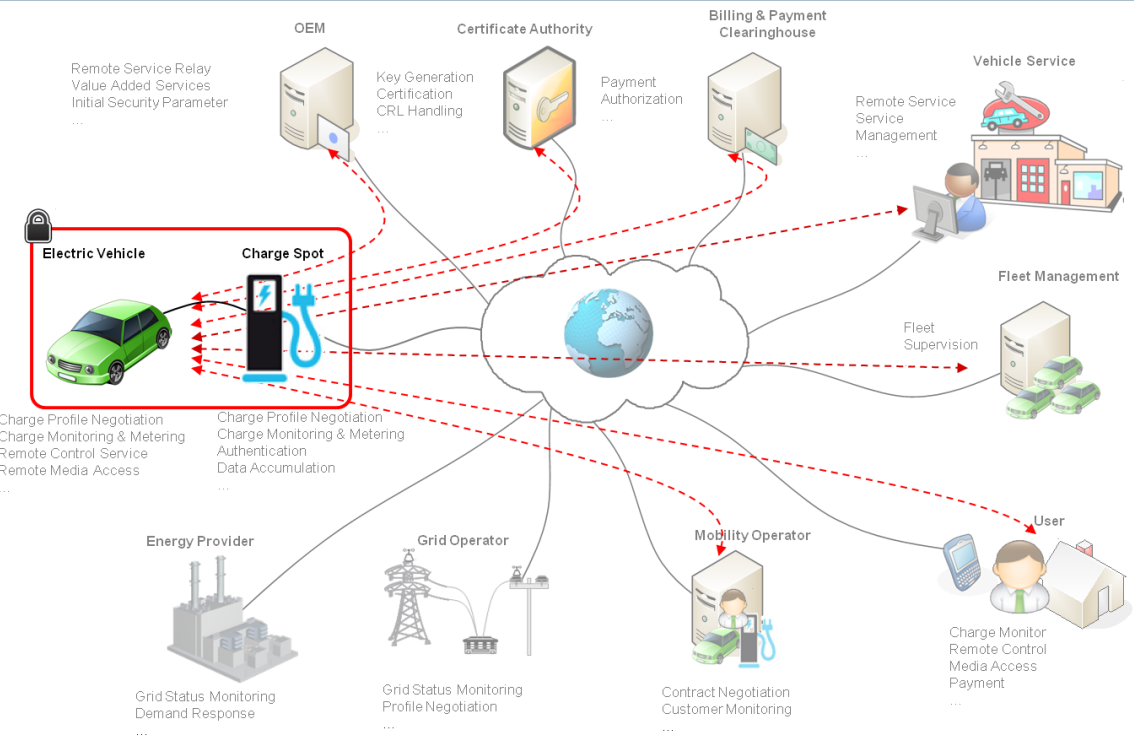
- XMPP (RFC 6120) is a middleware messaging and presence protocol supporting decentralized architectures
- Allows for
  - Registering resources in publicly reachable servers
  - Resolving resources based on names
  - Security (authentication, integrity, confidentiality) for the communication with the XMPP server

### XMPP supported security (current state)

- TLS (Transport Layer Security, RFC 5246) to protect the communication between the different entities and the XMPP server (mutual source authentication, integrity and confidentiality protection)
- SASL (Simple Authentication Security Layer, RFC 4422) is an authentication framework; and allows for authentication on application layer
- Likely to define additional security session for protecting the IEC 61850 client server communication over the XMPP server
  - Server may be operated, e.g., by a telecom service provider, while the IEC 61850 endpoints belong to the distribution network operator (DNO) and the Prosumer/microgrid operator.

# ISO/IEC Standardization of Vehicle to Grid Interface

## IEC 15118 – incorporates Security by Design



### Securely connecting the vehicle to the grid requires support of

- Connection of vehicles to the power grid (control of charging / discharging)
- Billing of consumed energy (charging)
- Roaming of vehicles between different charging spot (operators)
- Value added services (e.g., software updates)

### Security Approach

- Application of standardized security protocol to protect the communication between electric vehicle and charging spot
- Further security means to also protect application layer information beyond the scope of the charging spot (billing, credential provisioning)

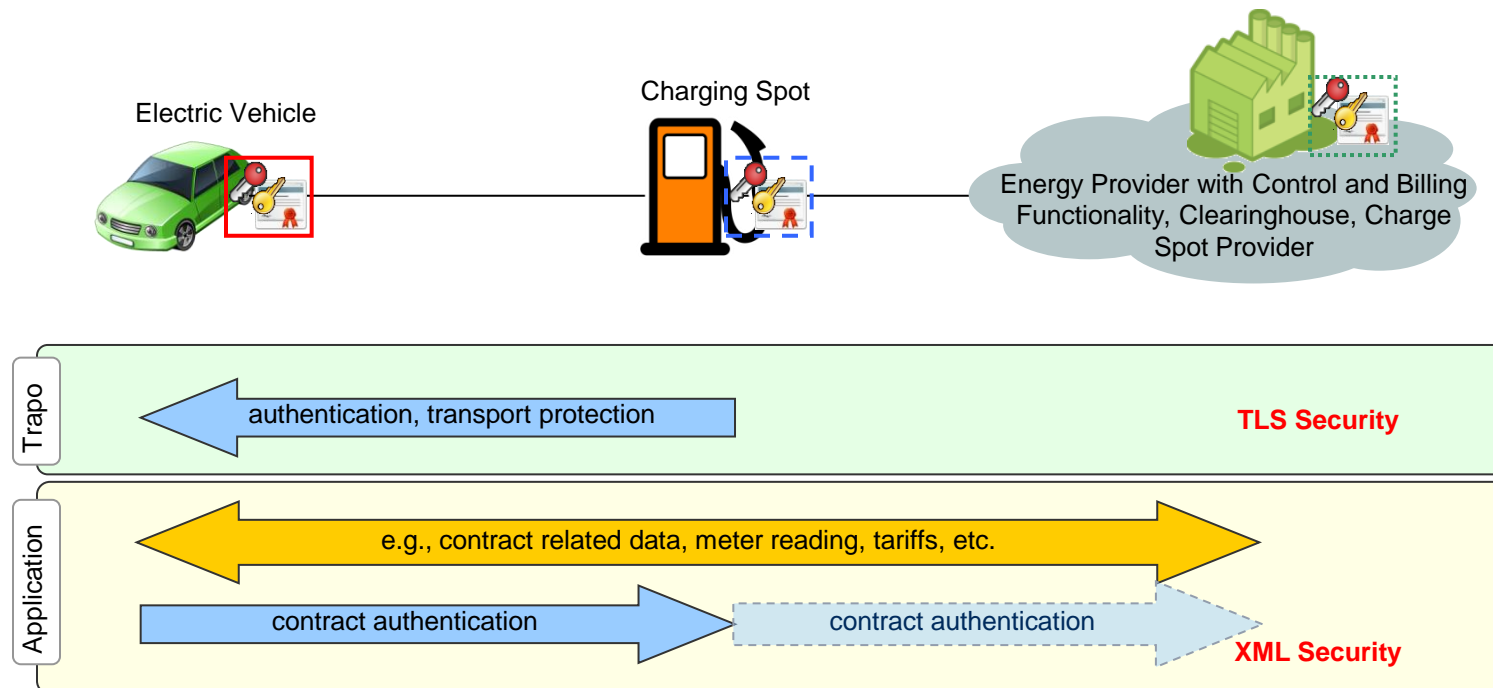
### Attacks in scope (examples)

- Eavesdropping / Interception
- Man-in-the-Middle Attack
- Transaction Falsifying or Repudiation

# Security Protocols used in Scenario 4

## Securely Connecting the Vehicle to the Smart Grid

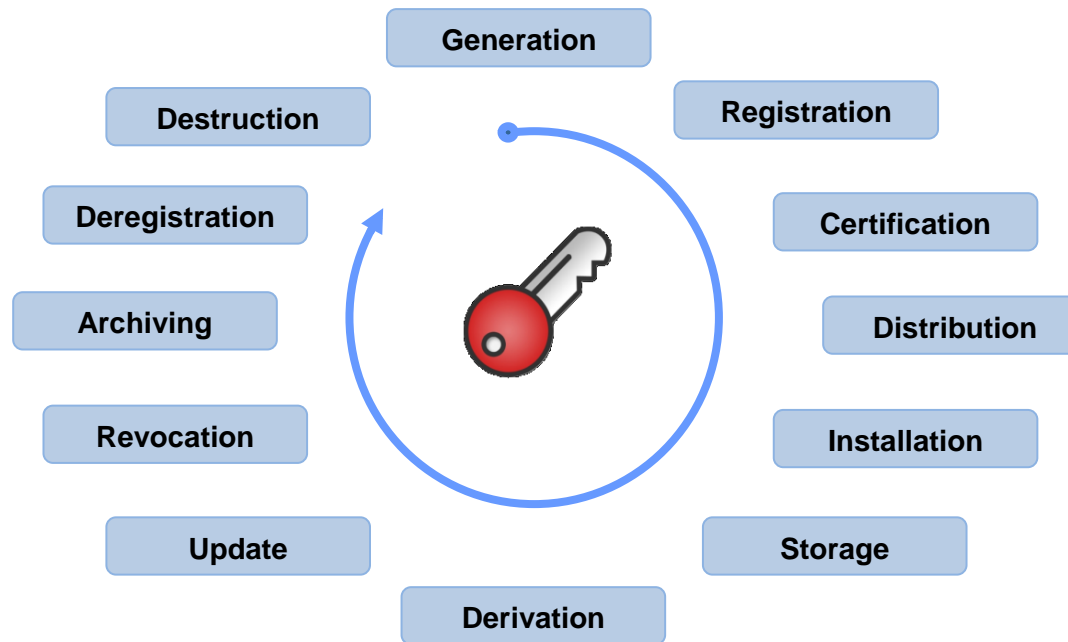
- Application of TLS to provide secure communication channel
  - Source authentication of charging spot as terminating transport peer, integrity and confidentiality protected communication
- Application of XML Digital Signatures and Encryption to communicate with backend
  - To be able to provide signed meter readings from EV to the backend and to provide and encrypted information (e.g. tariff, contract credentials) from the backend to EV



# Crucial Point in all Scenarios

## Security Credential Management

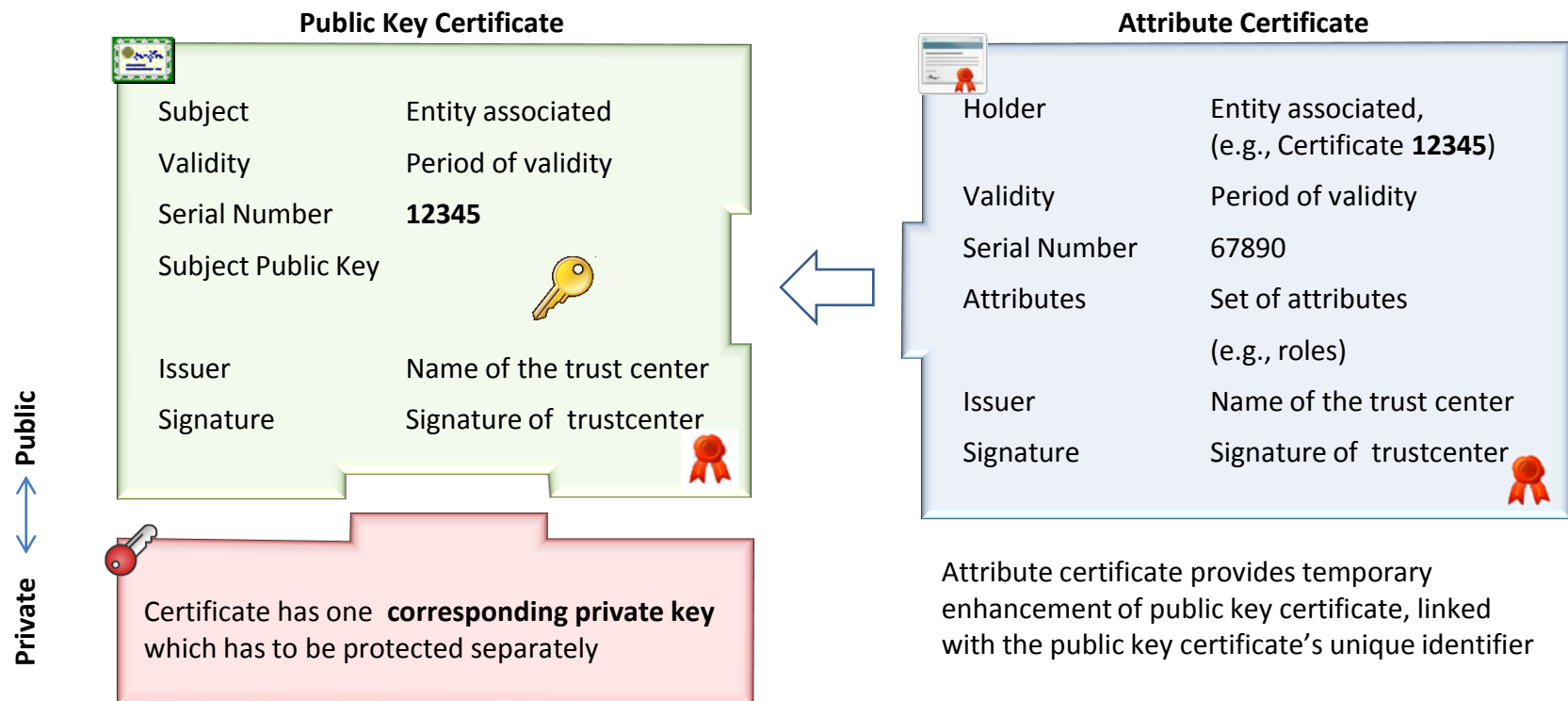
- Credential Management defines the process to assure secure handling of cryptographic key material necessary to protect data and command communication between peers.



- Vast number of security protocols rely on X.509 certificates and corresponding private keys
- The management of these credentials is typically the task of a Public Key Infrastructure (PKI)  
AND: requires additional communication protocols (see following slides)

# What is a Digital Certificate?

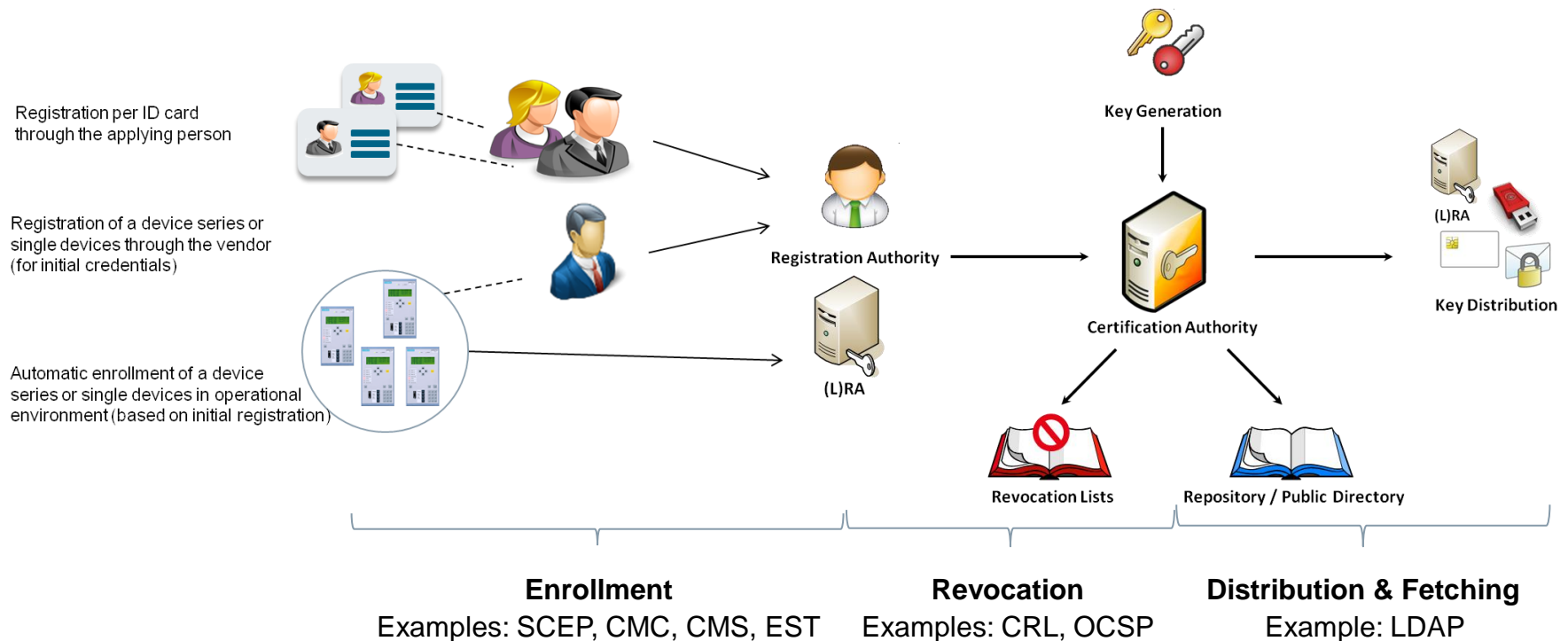
- A data structure that binds a public key value to a subject → Defined in ITU-T X.509 and IETF RFC 5280
- Binding through trusted certification authority (CA) verifying the subject's identity; alternative: self signed
- Limited lifetime, checked by the relying party along with the signature of the issuing CA
- Applied, e.g., in session key management, message protection, services like role-based access control



# Public Key Infrastructure

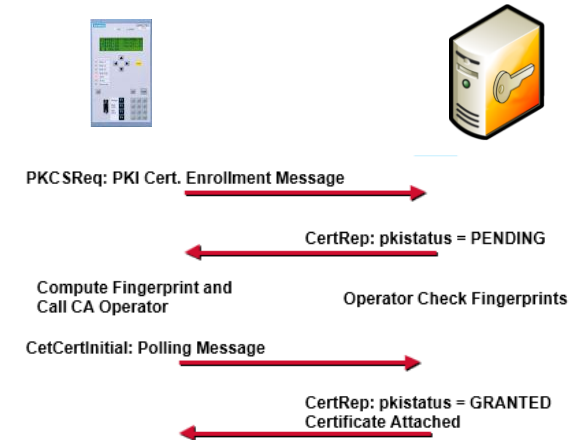
## Which Interactions are necessary?

- Public Key Infrastructure (PKI) provides means to manage X.509 key material for user and IEDs
- IEDs ideally generate key material, only certification is done by the CA
- Human users apply for a certificate; Key generation either through tokens or PKI
- Migration option through self signed certificates in conjunction with certificate white listing

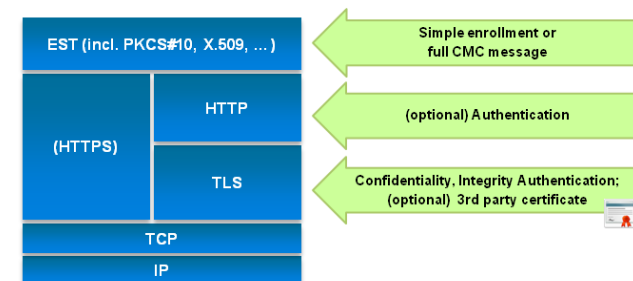


# Enrollment Protocol Examples

- SCEP (Simple Certificate Enrollment Protocol)
  - IETF Historic Draft (draft-nourse-scep-23)
  - PKCS #10 for certificate request, PKCS #7 for signing and enveloping of the certificate
  - HTTP and LDAP for transport
  - Requires manual authentication during enrollment
  - Widely implemented (Cisco, Microsoft, Apple, ...)

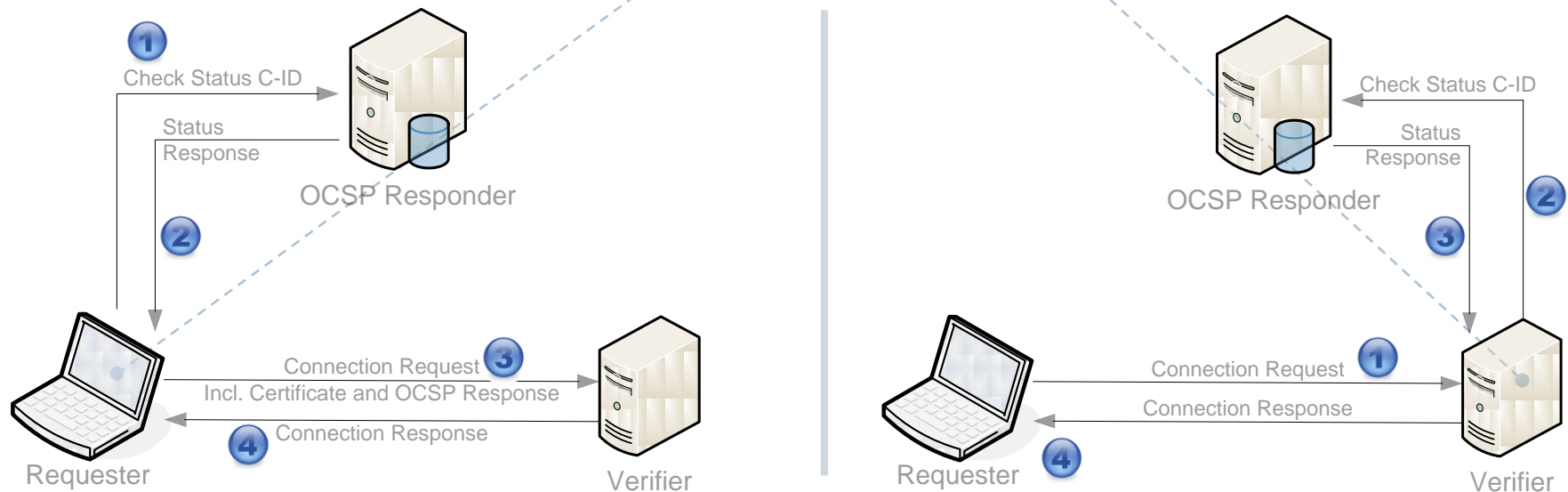


- EST (Enrollment over Secure Transport)
  - IETF RFC 7030
  - Certificate enrollment for clients using Certificate Management over CMS (CMC) messages (PKCS #10) over a secure transport (HTTPS = HTTP over TLS)
  - Expected to be SCEP successor



# Certificate Revocation using OCSP

- Online Certificate Status Protocol (OCSP) is defined in RFC 6960
- OCSP response is digitally signed by the CA and contains (among other information) the certificate status value
- Delegation possible (different certificate than CA)
- OCSP may be done proactive (by the requester) or reactive (by the responder)



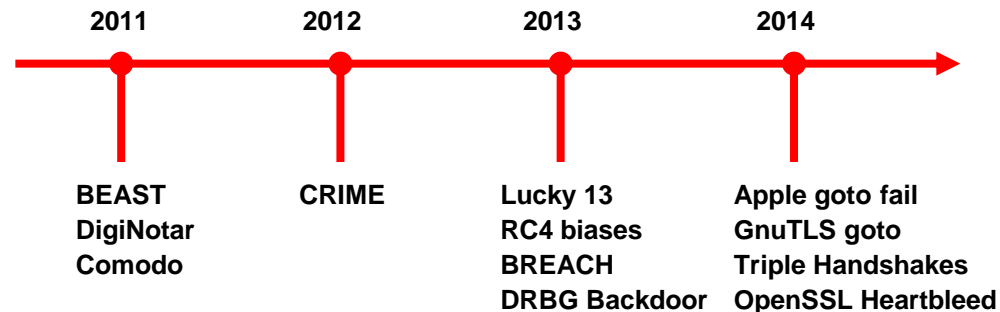
- Applied in IEC 62351 for substation automation in IEC 62351 and in vehicle to grid communication using ISO 15118



# Crucial Point in all Scenarios

## Software Quality

- For most of the security protocols commercial and open source implementations are available.
  - SSL/TLS: OpenSSL, GnuTLS, ...
  - IPSec: FreeS/WAN, KAME Libipsec, ...
- Prominent examples for implementation and integration errors of SSL/TLS libraries



- This argues for (increased )
  - Verification of the protocol state machine → Black/White Box Testing, Fuzzing, etc.
  - Integration of the protocol stack into the application → Fuzzing, etc.
  - Connection to the credential management → Key store access, certificate validation checking, etc.

# Summary and Challenges

## Summary

- Automation environments like the Smart Grid already utilize existing security protocols
- Profiling and potential enhancements of security protocols landscape based on use cases
- Current deployed security means often rely on shared keys.
- Upcoming use cases like DER integration are likely to rely on X.509 key material, which in turn requires the integration of credential management into the current energy automation landscape

## Challenges

- Device-oriented security and identity infrastructure (processes, scalability, limits of authority, ...) supporting efficient creation, distribution and handling of cryptographic credentials (e.g., security modules and their integration into products & production)
- Leverage of domain specific characteristics → engineered networks (e.g., for certificate white listing)
- Extensive software quality improvement for security protocol implementations and their integration environment (applications and also hardware)

# Thank you for the attention! Questions?

