innogy

Cybersecurity for e-mobility system in worldwide standardization

innogy SE · Stephan Voit · 2018-04-10

What is the meaning of “Cybersecurity”?

“Computer security, also known as cybersecurity or IT security, is the protection of computer systems from the theft and damage to their hardware, software or the information, as well as from disruption or misdirection of the services they provide.

Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. Also, due to malpractice by operators, whether intentional or accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods.

Source: https://en.wikipedia.org/wiki/Cybersecurity (as of April 2018)

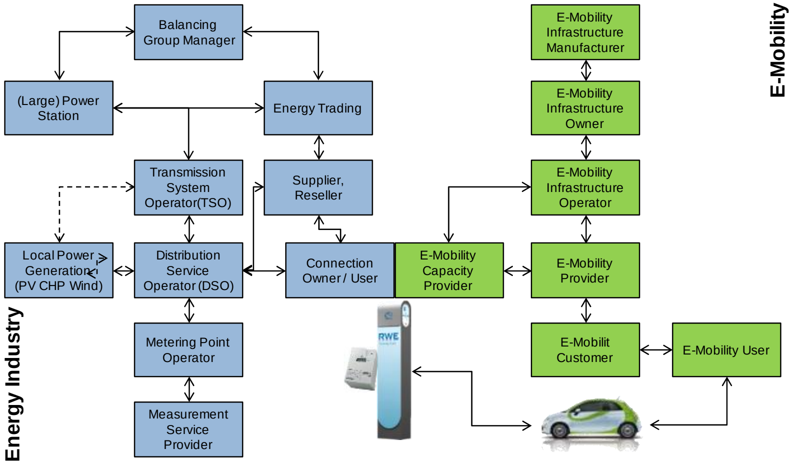
There is no article about Cybersecurity in German Wikipedia. But you can find a lot of information about “IT security” and “Common Criteria for Information Technology Security Evaluation”.

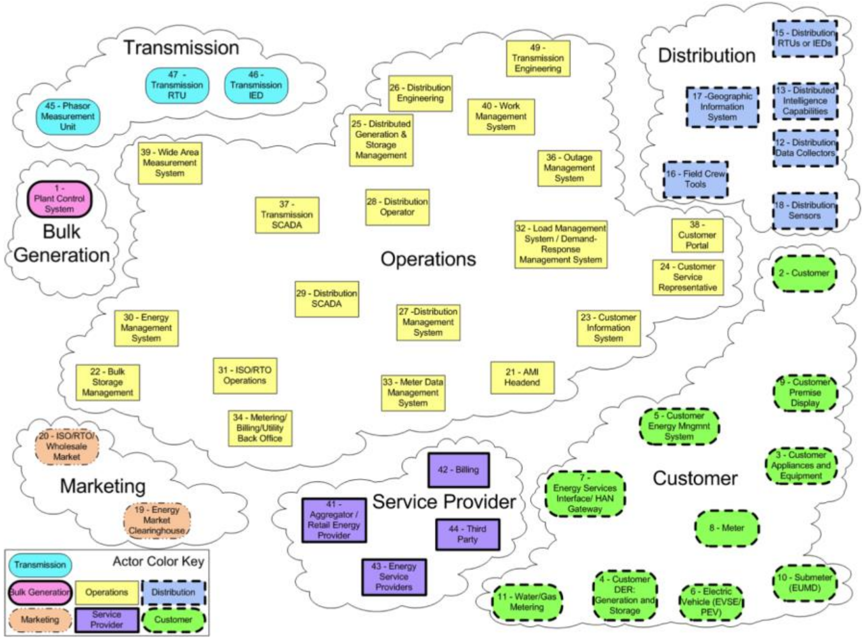
Typical High-Level Use Cases for e-mobility

- Schedule a charging session
- Start a charging session
  - Within a charging sub use cases could be agreed on
    - Get energy for charging the battery and auxiliary services, e.g. heating or cooling the cabin
    - Energy feed-back to EVSE
- Reschedule (re-negotiate) a charging session
- Stop a charging session
- Certificate handling for Plug-n-Charge mode (PnC)
- Invoicing of services

NISTIR 7628: Composite High-Level View of the Actors within Each of the Smart Grid Domains

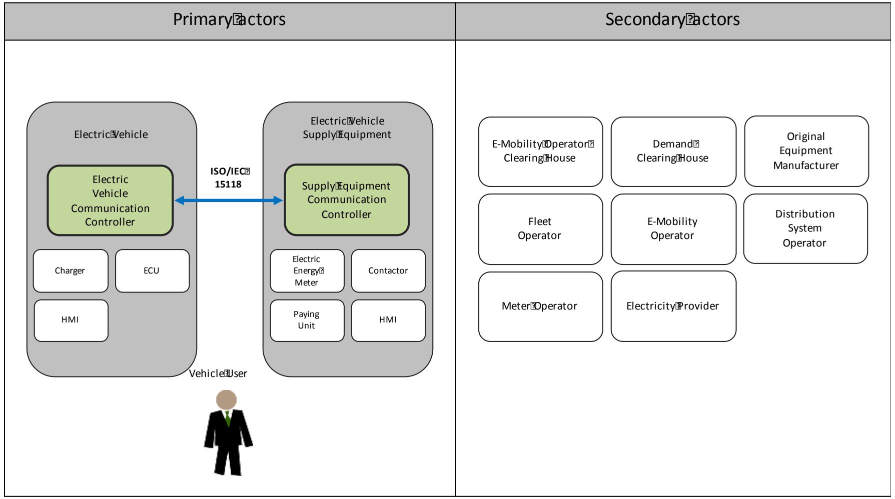
- E-mobility relevant actors / roles of smart grid domains in Europe (left side) and US (right side) are fitting well.


Energy Industry
E-Mobility
Balancing Group Manager
(Large) Power Station
Energy Trading
Transmission System Operator(TSO)
Supplier, Reseller
Local Power Generation (PV CHP Wind)
Distribution Service Operator (DSO)
Connection Owner / User
Metering Point Operator
Measurement Service Provider
E-Mobility Infrastructure Manufacturer
E-Mobility Infrastructure Owner
E-Mobility Infrastructure Operator
E-Mobility Capacity Provider
E-Mobility Provider
E-Mobilit Customer
E-Mobility User
RWE


Transmission
45 - Phasor Measurement Unit
47 - Transmission RTU
46 - Transmission IED
Bulk Generation
1 - Plant Control System
Operations
49 - Transmission Engineering
26 - Distribution Engineering
40 - Work Management System
25 - Distributed Generation & Storage Management
39 - Wide Area Measurement System
36 - Outage Management System
37 - Transmission SCADA
28 - Distribution Operator
32 - Load Management System / Demand-Response Management System
29 - Distribution SCADA
30 - Energy Management System
27 -Distribution Management System
23 - Customer Information System
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
34 - Metering/ Billing/Utility Back Office
38 - Customer Portal
24 - Customer Service Representative
Distribution
15 - Distribution RTUs or IEDs
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
12 - Distribution Data Collectors
16 - Field Crew Tools
18 - Distribution Sensors
Marketing
20 - ISO/RTO/ Wholesale Market
19 - Energy Market Clearinghouse
Service Provider
42 - Billing
41 - Aggregator / Retail Energy Provider
44 - Third Party
43 - Energy Service Providers
Customer
2 - Customer
9 - Customer Premise Display
5 - Customer Energy Mngmnt System
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
8 - Meter
11 - Water/Gas Metering
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)
10 - Submeter (EUMD)
Actor Color Key
Transmission
Bulk Generation
Operations
Distribution
Marketing
Service Provider
Customer

Actors / Roles used by ISO 15118 and NISTIR 7628 are in principal the same (only different names)

Actors in ISO 15118-1



Actors in NIST 7628

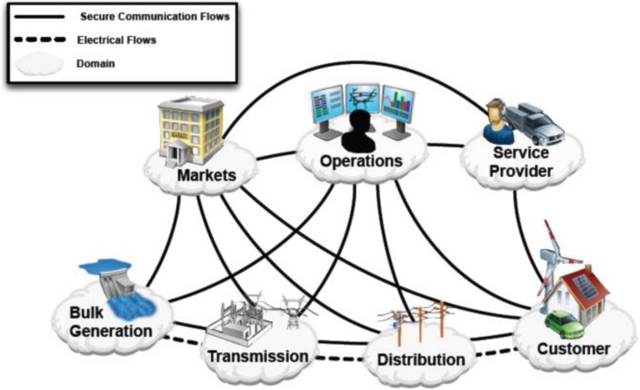


Figure 2. Interaction among actors in Smart Grid domains through secure communication flows and flows of electricity.

Source: *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)*

Stakeholders’ interests in field of charging EV

- EV Driver
  - High quality of services, e.g. charging
  - Ensure (data) privacy by other stakeholders
- Utilities
  - Safe and secure energy supply
  - Integration into energy production management
  - Integration into electric grid capacity management
  - Ensure power quality
  - Billability of services
- Service provider
  - Offers stable services to preferably all drivers at all EVSE
  - Billability of services
- OEM
  - Provide secure driving and charging
  - Protecting the vehicle against "crackers“
- Regulators
  - Support to develop market rules

Ideas of ISO 15118

- Initiated by large European car manufacturers (OEM), utilities, data integrators and (potential) charging station manufacturers in November 2008 with the following goals:
  - Develop a bi-directional communication protocol for charging EV at EV Supply Equipment (EVSE, aka charging point or charging station)
  - Providing (automated) authentication methods, which could also be used for micro-payment
  - Allows consideration of power production (especially of fluctuating renewables), electric grid situation and sales tariffs
  - Respect information (cyber) security, data privacy, data reduction and data economy

Cyber Security and Smart Grid systems

“Effective cyber security is integral to achieving a nationwide Smart Grid, as explicitly recognized in EISA.2

> *It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:*
>
> *(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.*
>
> *(2) Dynamic optimization of grid operations and resources, with full cyber- security.*

This initial version of Guidelines for Smart Grid Cyber Security was developed as a consensus document by the Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP), a public-private partnership launched by NIST in January 2010.”

Source: Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, SGIP CSWG, 09/2010

CSWG’s Methodology for Developing the Guidelines for Cyber Security Strategy

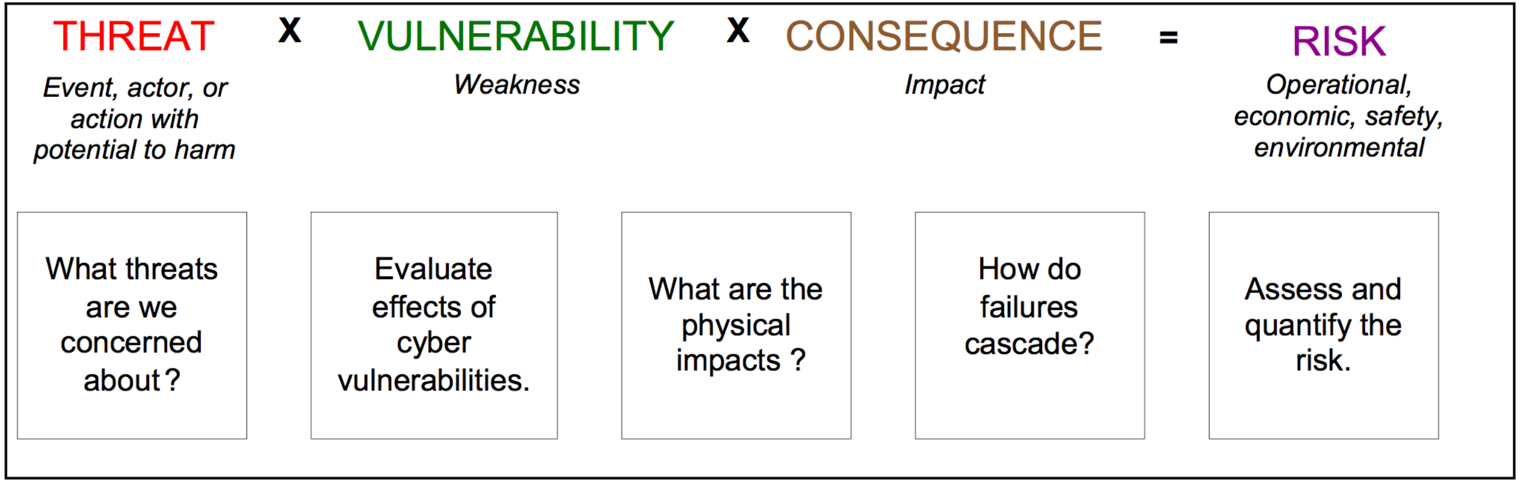
Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) defines 5 steps:

- Step 1: Selection of Use Cases with Cyber Security Considerations
- Step 2: Performance of a Risk Assessment
- Step 3: Setting Boundaries: The Beginnings of a Security Architecture
- Step 4: High-Level Security Requirements
- Step 5: Smart Grid Conformity Testing and Certification

How to manage risks?

- ISO 31000:2009 offers a list on how to deal with risk:
  - Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
  - Accepting or increasing the risk in order to pursue an opportunity
  - Removing the risk source
  - Changing the likelihood
  - Changing the consequences
  - Sharing the risk with another party or parties (including contracts and risk financing)
  - Retaining the risk by informed decision

How to determine the risk?



THREAT x VULNERABILITY x CONSEQUENCE = RISK

Event, actor, or action with potential to harm

Weakness

Impact

Operational, economic, safety, environmental

What threats are we concerned about?

Evaluate effects of cyber vulnerabilities.

What are the physical impacts ?

How do failures cascade?

Assess and quantify the risk.

Source: Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, SGIP CSWG, 09/2010

Risk management within ISO 15118

- Security by design: Make risk management an integrated part of development of ISO 15118, setup a special Project Team (PT5) to make risk analysis and provide solutions
- Data economy, data reduction: Collect and transfer only data which are absolutely necessary
- Analyze all data transfer according to basic principles of Information Security:
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
- Use well known cryptographically methods like cryptographic keys, encryption, digital signatures

Typically risks at ISO 15118's Primary Actors (Examples)

- Services (e.g. charging, certificate handling) are not payed, e.g. usage of invalid contract or credit card
- Private data could be used without permission
- Manipulated or wrong data are used for scheduling a charging session, e.g. electric grid capacity is only available if the price is high

Typically risks at ISO 15118’s Secondary Actors (Examples)

- Meter data are manipulated
  ⇨ wrong statement for utility
- Prices (“Tariff Tables”) and / or grid capacity (“Pmax Table”) are manipulated
  ⇨ EV could not be charged according to drivers need
- EV requests unrealistic amount of energy, e.g. 1 GWh within the next 5 hours
  ⇨ planning of power production and providing grid capacity get disturbed
- A lot of EV get the information to start charging now with high power
  ⇨ Unexpected high demand can cause a black out

Cyber security must be implemented on every layer

- Interactions (and therefor communication) between actors have to be analyzed.
  - CSWG identified more than 130 possible logical interfaces (see next page).
- Each interface has to be analyzed to ensure necessary level of
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation

- „…Security must be applied in layers, … and controls implemented at each layer. The objective is to mitigate the risk so that if one component of the defense is compromised or circumvented, the result will not be a cascading set of failures. Because no single security measure can counter all types of threats, multiple levels of security measures should be implemented.”

Source: Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, SGIP CSWG, 09/2010

Securing the Smart Grid needs individual strategies

- CSWG identified over 180 high-level security requirements applicable to the entire Smart Grid, based on NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems; DHS Catalog of Control Systems Security: Recommendations for Standards Developers, and NERC CIPS (1-9).
- They may be a baseline for individual cyber security strategies by performing
  - Determine the logical interface categories
  - Assess risk
  - Select the initial set of baseline security requirements based on the logical interface categories

Each Smart Grid provider has to assess smart charging according to ISO 15118 based in his cybersecurity strategy.

innogy

ISO 15118 PnC

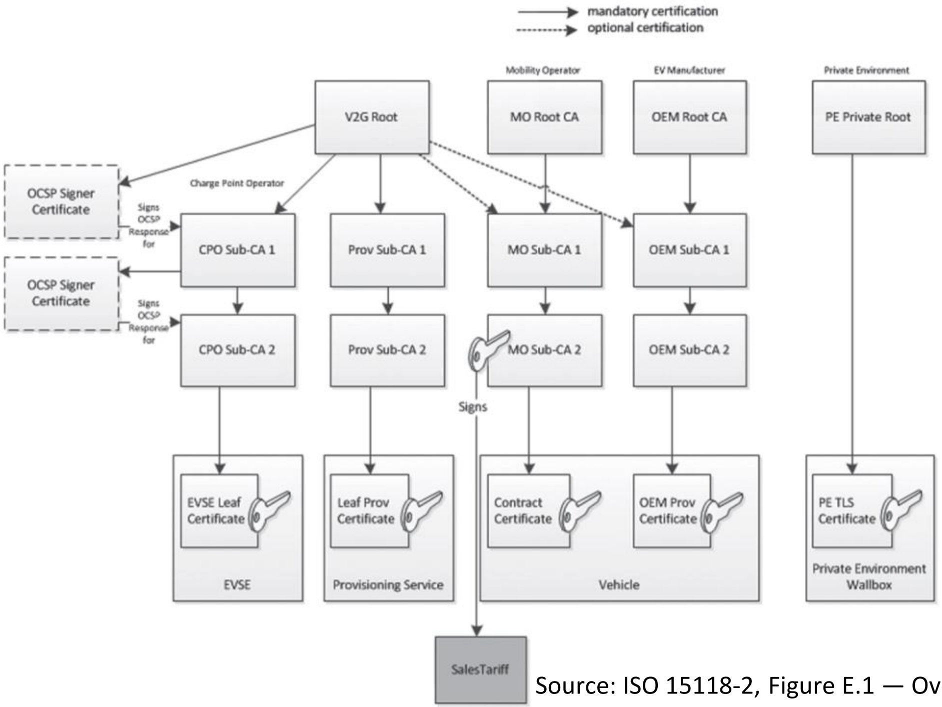
VDE Application Guide

VDE-AR-E 2802-100-1

How ISO 15118's Primary Actors are communicating with Secondary Actors

- ISO 15118 defines a communication protocol between an EV and an EVSE (so called "Primary Actors").
- Data coming from or transferred to so called "Secondary Actors" have to be signed and / or encrypted. Typically a Public Key Infrastructure (PKI) is used to support this.
- The basic requirements for a PKI for Primary and Secondary Actors are part of ISO 15118-2 (see next page).
  - Detailed specification is not part of ISO 15118. In Germany a working group initiated by Porsche started a specification in 2015. Based on this findings the German working group DKE/K 901.0.115 "Information Security for Electric Mobility" will soon published an application guide (in English) for an e-mobility PKI.

Overview of ISO 15118 certificate structure



Source: ISO 15118-2, Figure E.1 — Overview certificate structure

- ISO 15118-2 shows how a PKI structure could be
- Restrictions (e.g. storing as less certificates as possible in an EV) are respected
- Best practice approach was published as VDE-AR-E 2802-100-1:2017-10 “Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118”

How ISO 15118 helps to assess to an individual Cyber Security strategy?

- In ISO 15118-1 and ISO 15118-2 the analysis on information security are described.
- To ensure accordance of an ISO 15118 implementation testing is defined in ISO 15118-4 and ISO 15118-5. International ISO/IEC 15118 Testing Symposia are offered, normally after each working group meeting.
- ISO 15118-2 describes an e-mobility PKI architecture, need data structures and message sets and behavior. A “best practice” is available as VDE-AR-E 2802-100-1:2017-10 “Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118”.
- Data communication with Secondary Actors is also specified. Additionally all transferred data has to be validated by Secondary Actor. E.g. unrealistic data / behavior should be filtered and consequences have to be discussed with the other communication partner.

Individually testing with a Smart Grid provider is necessary

- ISO 15118 based interfaces between EVSE and Secondary Actors have to be tested. This should be done by a well defined set of use cases. E.g.:
  - Transfer of Smart Grid signals for EV respectively EVSE and demand requests from EV to a Smart Grid provider could base on OpenADR.
    - E.g.: Oxygen Initiative's Demand Clearing House (an e-mobility demand response management system) enables already the conversion between OpenADR and ISO 15118 and vice versa.

Thank you!

innogy

Contact partners

Stephan Voit
EMobility
T +49 (173) 326 77 05 or +1 (949)532-9254
stephan.voit < at > innogy.com

innogy

APPENDIX

Glossary

- CI: Communication Interface
- CSWG: Cyber Security Working Group
- DIN: German Institute for Standardization
- DKE: German Commission for Electrical, Electronic & Information Technologies of DIN and VDE
- EURELECTRIC: The Union of the (European) Electricity Industry
- EV: Electric Vehicle (here: plug-in EV)
- EVSE: EV Supply Equipment, a charging point
- FSI: German Federal Office for Information Security (FSI) (German: Bundesamt für Sicherheit in der Informationstechnik (BSI))
- GWh: Giga Watt hour (109 Wh)
- IEA: International Energy Agency
- IEC: International Electrotechnical Commission
- IS: International Standard: Final stage of an ISO or IEC standard
- ISO: International Organization for Standardization
- JWG: Joint Working Group
- NIST: National Institute of Standards and Technology
- OEM: Original equipment manufacturer; here used for „car manufacturer“
- OpenADR: Open Automated Demand Response
- PKI: Public Key Infrastructure
- PT: Project Team, working group within ISO/IEC 15118 JWG V2G CI
- SGIP: Smart Grid Interoperability Panel
- V2G: Vehicle-to-Grid
- VDE: German Association for Electrical, Electronic & Information Technologies

Structure of norm ISO 15118 „Road vehicles — Vehicle to grid communication interface“ Edition 2

Under revision for integration of requirements for wireless charging, feed energy back into grid and specify a few phrases more precisely:

- Part 1, Edition 2: General information and use-case definition (Draft International Standard (DIS) available since 11/2017)
- Part 2, Edition 2: Network and application protocol requirements (CD2 available since 03/2017, DIS planned for 2018)

Availability: Paper / PDF versions of DIS, FDIS, CDV and IS could be bought at ISO (www.iso.org) and IEC (www.iec.ch). CD versions are distributed only within JWG.

References, further readings (1/2)

- Working documents of ISO/IEC 15118 Joint Working Group Vehicle-2-Grid Communication Interface (JWG V2G CI)
  - Published standards ISO 15118-1, ISO 15118-2, ISO 15118-3; Published drafts ISO 15118-2, ISO 15118-2, ISO 15118-4, ISO 15118-5
- German Federal Office for Information Security (FSI) “IT baseline protection” (German: Bundesamt für Sicherheit in der Informationstechnik (BSI) “IT Grundschutz”)
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- NIST Roadmap for Improving Critical Infrastructure Cybersecurity
- NISTIR 7628 Guidelines for Cyber Security
  - Introduction to NISTIR 7628, September 2010
  - Volume 1/2/3, September 2014
- Presentations from EURELECTRIC/IEA Talking Smart Grids - Workshop n°8 “Cybersecurity in Electricity Distribution Grids” 15 October 2015, Brussels

References, further readings (2/2)

- ISO/IEC 27001 “Information technology – Security techniques – Information security management systems – Requirements”
- ISO/IEC 27002 “Information technology – Security techniques – Code of practice for information security controls”
- ISO/IEC 20000: first international standard for IT service management
- ISO/IEC 15408 “Common Criteria for Information Technology Security Evaluation”
- ISO 15443 “Information technology – Security techniques – A framework for IT security assurance”
- BSI (German Federal Office for Information Security)
  - BSI-Standards 100-1 to 100-4: a set of recommendations including “methods, processes, procedures, approaches and measures relating to information security”, aligned with to the ISO/IEC 2700x family
- ETSI: “Information security indicators” (ISI)
- ISO/IEC 14443 “Identification cards – Contactless integrated circuit cards”
- ISO/IEC 7816-1:2011 “Identification cards -- Integrated circuit cards”
- IEEE P1363 “Standard Specifications for Public-Key Cryptography”