1

Introduction

1.1 Introduction

Wireless Communications Security: Solutions for the Internet of Things presents key aspects of the mobile telecommunications field. The book includes essential background information of technologies that work as building blocks for the security of the current wireless systems and solutions. It also describes many novelty and expected future development options and discusses respective security aspects and protection methods.

This first chapter gives an overview to wireless security aspects by describing current and most probable future wireless security solutions, and discusses technological background, challenges and needs. The focus is on technical descriptions of existing systems and new trends like the evolved phase of Internet of Things (IoT). The book also gives an overview of existing and potential security threats, presents methods for protecting systems, operators and end-users, describes security systems attack types and the new dangers in the ever-evolving mobile communications networks and Internet which will include new ways of data transfer during the forthcoming years.

Chapter 1 presents overall advances in securing mobile and wireless communications, and sets the stage by summarizing the key standardization and statistics of the wireless communications environment. This chapter builds the base for understanding wireless network security principles, architectural design, deployment, installation, configuration, testing, certification and other security processes at high level while they are detailed later in the book. This chapter also discusses the special characteristics of the mobile device security, presents security architectures and gives advice to fulfil the regulatory policies and rules imposed. The reader also gets an overview about the pros and cons of different approaches for the level of security.

In general, this book gives the reader tools for understanding the possibilities and challenges of wireless communications, the main weight being on typical security vulnerabilities and practical examples of the problems and their solutions. The book thus functions as a practical guide to describe the evolvement of the wireless environment, and how to ensure the fluent continuum of the new functionalities yet minimize potential risks in the network security.

Wireless Communications Security: Solutions for the Internet of Things, First Edition. Jyrki T. J. Penttinen.

1.2 Wireless Security

1.2.1 Background and Advances

The development of wireless communications, especially the security aspects of it, has been relatively stable compared to the overall issues in the public Internet via fixed access until early 2000. Nevertheless, along with the enhanced functionalities of smart devices, networks and applications, the number of malicious attacks has increased considerably. It can be estimated that security attacks, distribution of viruses and other illegal activities increase exponentially in a wireless environment along with the higher number of devices and users of novelty solutions. Not only are payment activities, person-to-person communications and social media types of utilization under constant threat, but furthermore one of the strongly increasing security risks is related to the Machine-to-Machine (M2M) communications which belong in the IoT realm. An example of a modern threat is malicious code in an Internet-connected self-driving car. In the worst case, this may lead to physically damaging the car's passengers.

There is a multitude of ideas to potentially change the role of the current Subscriber Identity Module (SIM), or Universal Integrated Circuit Card (UICC) which has traditionally been a solid base for the 3rd Generation Partnership Program (3GPP) mobile communications as it provides a highly protected hardware-based Secure Element (SE). Alternatives have been presented for modifying or for replacing the SIM/UICC concept with, e.g., cloud-based authentication, authorization and payment solutions. This evolution provides vast possibilities for easing the everyday life of end-users, operators, service providers and other stakeholders in the field, but it also opens unknown doors for security threats. The near future will show the preferred development paths, one of the logical possibilities being a hybrid solution that keeps essential data like keys within hardware-protected SEs such as SIM/UICC cards while, e.g., mobile payment would benefit from the flexibility of the cloud concept via dynamically changing tokens that have a limited lifetime.

In the near future, the penetration of autonomously operated devices without the need for human interactions will increase considerably, which results in much more active automatic communication, e.g., the delivery of telemetric information, diagnostics and healthcare data. The devices act as a base for value-added services for vast amounts of new solutions that are still largely under development or yet to be explored. Nevertheless, the increased share of such machines attached to networks may also open new security threats if the respective scenarios are not taken into account in early phases of the system, hardware (HW) and software (SW) development.

The field of new subscription management, along with the IoT concept, automatised communications and other new ways of transferring wireless data, will evolve very quickly. The updated information and respective security mechanisms are highly needed by the industry in order to understand better the possibilities and threats, and to develop ways to protect end-users and operators against novelty malicious attempts. Many of the solutions are still open and under standardization. This book thus clarifies the current environment and most probable development paths interpreted from the fresh messages of industry and standardization fields.

1.2.2 Statistics

In the mobile communications, wireless Local Area Networks (LANs) are perhaps the most vulnerable to security breaches. Wi-Fi security is often overlooked by both private individuals and companies. Major parts of wireless routers have been equipped in advance with default

settings in order to offer fluent user experience for installation especially for non-technical people. Nevertheless, this good aim of the vendors leads to potential security holes for some wireless routers and access points in businesses and home offices due to poor or non-existing security. According to Ref. [21], around 25% of wireless router installations may be suffering from such security holes. From tests executed, Ref. [21] noted in 2011 that 61% of the studied cases (combined 2133 consumer and business networks) had a proper security set up either via Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access, enhanced (WPA2). For the rest of the cases, 6% did not have security set up at all while 19% used low protection of Wired Equivalent Privacy (WEP), 11% used default credentials, and 3% used hidden Service Set Identifier (SSID) without encryption.

Ref. [26] presents recent statistics of Internet security breaches, and has concluded that the three most affected industries are public, information and financial services. Typical ways for illegal actions include the following:

- **Phishing**. Typically in the form of email, the aim is to convince users to change their passwords for banking services via legitimate-looking web pages. The investigations of Ref. [26] shows that phishing is nowadays more focused and continues being successful for criminals as 23% of users opened the phishing email, and 11% clicked the accompanying attachments.
- **Exploitation of vulnerabilities**. As an example, half of the common vulnerabilities and exposures during 2014 fell within the first two weeks which indicates the high need for addressing urgent breaches.
- **Mobile**. Ref. [26] has noted that Android is clearly the most exploited mobile platform. Not necessarily due to weak protection as such, but 96% of malware was focused on Android during 2014. As a result, more than 5 billion downloaded Android apps are vulnerable to remote attacks, e.g., via JavaScript-Binding-Over-HTTP (JBOH) which provides remote access to Android devices. Nevertheless, even if the mobile devices are vulnerable to breaches, after filtering the low-grade malware, the amount of compromised devices has been practically negligible. An average of only 0.03% of smartphones per week in the Verizon network during 2014 were infected with higher grade malicious code.
- **Malware**. Half of the participating companies discovered malware events during 35 or fewer days during the period of 2014. Malware is related to other categories like phishing which is the door for embedding malicious code to user's devices. Depending on the industry type, the amount of malware varies, so, e.g., financial institutes protect themselves more carefully against phishing emails which indicates a low malware proportion.
- **Payment card skimmers and Point-of-Sale (POS) intrusions**. This breach type has gained big headlines in recent years as there have been tens of millions of affected users per compromised retailer.
- **Crimeware**. The recent development indicates the increase of Denial-of-Service (DoS) attacks, with Command and Control (C2) continuing to defend its position in 2014.
- **Web app attacks**. Virtually all the attacks in this set, with 98% share, have been opportunistic in nature. Financial services and public entities are the most affected victims. Some methods related to this area are the use of stolen credentials, use of backdoor or C2, abuse of functionality, brute force and forced browsing.
- **Distributed Denial-of-Service (DDoS) attacks**. This breach type is heavily increasing. Furthermore, DDoS attacks are being prepared increasingly via malware. The attacks rely on improperly secured services like Network Time Protocol (NTP), Domain Name System

(DNS) and Simple Service Discovery Protocol (SSDP) which provide the possibility to spoof IP addresses.
- **Physical theft and insider misuse**. These are related to human factors; in general, this category belongs to the 'opportunity makes theft', which is very challenging to remove completely as long as the chain of trust relies on key personnel who might have the possibility and motivation to compromise or bypass security. Detecting potential misuse by insiders is thus an important role to prevent and reveal fraudulent attempts early enough. This detection can be related to deviation of the data transfer patterns, login attempts, time-based utilization and, in general, time spent in activities that may indicate dissatisfaction at the working place.
- **Cyber espionage**. According to Ref. [26], especially manufacturing, government and information services are noted to be typical targets of espionage. Furthermore, the most common way to open the door for espionage seems to be the opening of an email attachment or link.
- Any other errors that may open doors for external or internal misuse.

More detailed information about data breach statistics and impacts in overall IT and wireless environments can be found in Ref. [26].

1.2.3 Wireless Threats

1.2.3.1 General

Wireless communications systems provide a functional base for vast opportunities in the area of IoT including advanced multimedia and increasingly real-time virtual reality applications. Along with the creation and offering of novelty commercial solutions, there also exist completely new security threats that are the result of such a fast developing environment such that users and operators have not yet fully experienced the real impacts. Thus, there is a real need for constant efforts to identify the vulnerabilities and better protect any potential security holes. The following sections present some real-world examples of the possibilities and challenges of wireless communications, the weight being in the discussion of security vulnerabilities and their solutions.

Protection in the wireless environment largely follows the principles familiar from fixed networks. Nevertheless, the radio interface especially, which is the most important difference from the fixed systems, opens new challenges as the communications are possible to capture without physical 'wire-tapping' to the infrastructure. Knowledgeable hackers may thus try to unscramble the contents either in real time or by recording the traffic and attacking the contents offline without the victims' awareness. The respective protection level falls to the value of the contents – the basic question is how much end-users, network operators and service providers should invest in order to guarantee the minimum, typical or maximum security. As an example, the cloud storage for smart device photos would not need to be protected too strongly if a user uploads them to social media for public distribution. The scenery changes, though, if a user stores highly confidential contents that may seriously jeopardize privacy if publicly exposed. There are endless amounts of examples about such incidences and their consequences, including the stealing and distribution of personal photos of celebrities. Regardless of the highly unfortunate circumstances of these security breaches, they can also

work as very useful lessons. Some of the easiest means to minimize the damage is to apply additional application-layer security by encrypting the contents via a separate password, and simply to reconsider the uploading of the most sensitive data to external data storages.

The selection of the security level, whether it is done by the end-user, network operator or service provider, can be optimized by balancing the cost of the protection and the fluency of the utilization. This easy user experience may be an important aspect because a highly secured service may require such complicated procedures to authenticate and protect the contents that it is not practical for the average user. One of the most reliable yet fluent ways is to utilize two-fold authentication, e.g., based on permanent user ID and password as well as a one-time code that is sent to the user via an alternative route such as mobile communications messaging. Along with increasing mobile device penetration, the majority of users already have some kind of mobile device, so one of the most logical bearers for such messaging authentication is based on the robust, widespread Short Message Service (SMS).

1.2.3.2 Wireless Environment

First-generation mobile communications systems, such as the Nordic Mobile Telephone (NMT), British Total Access Communications System (TACS) and American Advanced Mobile Phone System (AMPS), were analogue and based on Frequency Modulated (FM) radio channels for solely voice communications. The conversations of users could be intercepted by tuning a simple commercial-grade radio scanner to the utilized frequencies of the base station and mobile device as there was no contents protection mechanism applied against potential eavesdropping. Also, copying and reutilization of the device credentials such as the telephone number was possible via the non-protected radio interface and Common Signaling System (CSS7) messages. The analogue mobile communications networks have been obsolete for many years, but these early experiences about security breaches have been educational for developing more advanced systems.

Still widely in commercial use, the Global System for Mobile Communications (GSM) is the most popular second-generation mobile communications system that was standardized by applying proper shielding against the obvious security holes noted during the operations of analogue systems. Thanks also to digital transport technologies, protection of the system was easier than in preceding systems. Not only has the radio interface been protected by encrypting the signalling and communications but also procedures for authenticating and authorizing subscribers have provided additional mechanisms for preventing misuse of the systems. However, along with the ageing of the original technology, vulnerabilities of the protection mechanisms have been found. One of the concrete threats of the basic GSM system is that it is possible to set up a spoof Base Transceiver Station (BTS) to capture the call attempts in such a way that the non-Mobile Network Operator (MNO) base station does not need to utilize scrambled channels, since it acts as a mere relay station without the legitimate user's awareness. As the principle for making this happen is based on the replication of the GSM BTS protocol layers which are publicly available, the actual equipment may be constructed by emulating the minimum set of BTS functionalities used in a laptop and by utilizing a commercial Gaussian Minimum Shift Keying (GMSK) modulated transceiver and antenna system [1]. According to the European Telecommunications Standards Institute/3rd Generation Partnership Program (ETSI/3GPP) GSM specifications, the unsecure radio channel, which is not protected by any of the A5 algorithm variants, meaning that the A5/0 is in use, must be

indicated to the user. In practice, this unsecure channel indicator may be displayed as a small symbol such as an open lock, which the end-user might not be able to relate to unprotected communications. In some cases, the symbol might be missing completely regardless of the standards requirements. The basic reason for including the support of unsecured communications into GSM handsets is due to the fact that some network operators do not activate the secure communications, and the handset devices need to be able to function in all of the networks while roaming.

This vulnerability was identified in the early stage of third-generation (3G) standardization, and thus the ETSI/3GPP Universal Mobile Telecommunications System (UMTS) included mutual authentication as one of the enhanced security items since its first release in 1999. The 3G mobile communications are relatively secure against such threats as spoof base stations, although there are other threats that apply to any mobile communications network. One of these is the end-to-end path from user equipment up to the MNO infrastructure which is secured up to the unscrambling equipment, but the rest of the path up to the answering subscriber in a fixed telephony network or up to the receiver's mobile network's scrambling equipment is typically unsecure. Furthermore, even if the MNO's internal network is assumed to be isolated, and focused wire-tapping is challenging due to the increased utilization of fibre optics, the internal transmission of the 2G and 3G communications may be based on unsecured radio links which may expose the possibility to intercept the communications by applying the respective protocol layer stacks for capturing the contents from the bit stream.

The security level is again further increased for the 3GPP Release 8 Long Term Evolution (LTE) and its enhanced phase as of Release 10, which is referred to as LTE-Advanced (LTE-A). The enhanced items include, e.g., new communications algorithms.

Unlike the mobile communications networks that have been traditionally well protected, wireless solutions like Wi-Fi and WiMAX do not contain such a large-scale infrastructure and are thus more vulnerable to security breaches. Despite the deployment of authorization passwords in Wi-Fi hotspots in home use, as well as hiding the ID of the access point and applying new encryption algorithms, wireless LANs tend to be vulnerable to malicious attacks. The consequence may be exposure of the user's communications and stored files, and the attacker might set up an illicit server for spam mailing or illegal contents storage without the user's knowledge.

1.2.3.3 Examples from the Real World

With the improving security of wireless networks, malicious attempts have been increasingly focusing on devices and applications. Not only smart devices but also IoT devices are fruitful targets due to their often under-developed security. The following list summarizes a small snapshot of some of the real-world cases published in 2014–15.

Wired reported that hackers can silently control Google Now and Siri from 16 feet away by using local connectivity of Radio Frequency (RF) to trigger voice commands on commercial phones that have such applications enabled and external headphones/microphone attached to the device. The threat is related to the headphones' cord which functions as an antenna, transporting the captured RF signal and confusing the phone's operating system, which assumes the signal to be the user's own audio commands via the microphone. This attack would serve to command Siri or Google Now to send texts and to force the phone to dial other mobile

devices thus forming a simple eavesdropping device. According to Ref. [74], the commands can also be used to force the phone's browsers to enter malicious sites, to generate spam and phishing messages via email.

Interference Technology has reported on the low-cost Portable Instrument for Trace Acquisition (PITA) developed by Tel Aviv University and the Israeli research centre. It is a hacking device that can steal encryption keys over the air. It is based on the interpretation of the RF emission of computer processors to reveal encryption keys, and the method does not thus depend on standard communication methods like Wi-Fi or Bluetooth. The device is able to work up to 19 inches away from the processors, and may store data encrypted with RSA and ElGamal and decrypt it. Furthermore, the device can transmit the decrypted data over Wi-Fi to the attacker's computer [75].

Ref. [76] reports about remote baby-sitter devices which are possible to hack and then use to spy on people. Rapid7, a US-based company, revealed the magnitude of the risk in a number of commercial devices. Some of the compromised models include iBaby M3S. Upon connecting them to the Internet, the attacker may take over control and use them as hidden cameras and eavesdropping devices. Furthermore, via these devices, it is possible to utilize them as vectors to break through further to the users' home and business networks, which generates a risk for the private and business utilization of the connectivity. The issues related to these security holes include the possibility of externals being able to monitor the home via video and audio. If these devices are close to users, potentially confidential calls can thus be eavesdropped upon.

Ref. [77], together with reports from CNN and Ars Technica, informs about the danger of innocent-looking home and office devices like printers, which may expose security holes even without an Internet connection. Red Balloon Security demonstrated sending text wirelessly by modifying the functions of a printer at the Red Hat event in 2015. Typically, IoT security breaches are based on Internet holes, but less focus has been put on the RF leaking from the devices' components, which can be captured within short distances of the devices. Furthermore, this methodology may expose security holes in computers that are completely isolated from the public Internet, including the highest security environments such as nuclear power plants and banks. The commonly used term for such devices leaking information locally is 'zombie'. More details can be found via the demo presentation of Ref. [77] about data exfiltration using malware.

These examples indicate that not only are networks and devices under threat via typical connectivity technologies but also that many 'out-of-the-box' methods are being constantly invented. The challenging yet highly needed counter-measure is to assess the existing and potential security threats. One solution is that the service or device provider may try to deliberately hack its own systems. This approach is called 'white hat' hacking, as the intentions for finding security holes is done in cooperation with the hacking experts to find and protect the security holes. As an example, Ref. [78] discusses MasterCard's digital security lab for proving the security level of its payment environment. In this case, manual and automatized methods are applied in pre- and post-crime forensics. The aim of the lab is to figure out the ways of thieves trying to attack digital payment systems, such as old-style magnetic stripe credit cards, contactless chip bank cards, smartphone-based biometric systems and new device-based payment methods like those planned for wearables using biometrics, e.g., heartbeat pattern for authentication. Some methods for exploring the exposure and to break the payment technology encryption, passwords and Personal Identification Numbers (PINs) and their potential

issues are based on electron beams, lasers and ionizing radiation. Furthermore, the lab also has the means to investigate physical traces of the DNA of the criminals on ATMs, cards and hacked PIN-entry machines. One example of such illegal intentions is the tampering of payment cards by providing a malicious Radio Frequency Identity (RFID) chip which could broadcast account and PIN details via an RF signal which could be received, e.g., near a Point-of-Sales (POS) terminal or within close proximity of an ATM. The magnetic stripe cards are still widely used, and expose an important risk for the easiness of copying the card (e.g., simply spraying iron fillings on the magnetic stripe which indicates visually the respective binary code that the stripe contains, including account number and other key data). According to Ref. [78], the lab has not yet seen cloned chip cards. As for more sophisticated physical hacking methods, the electrical charge across the Europay, MasterCard, Visa chip connections can be monitored via an electron microscope by observing respective visual flashes to reveal the binary messages that in turn may help hackers reverse engineer the cryptographic keys. To protect against this type of possibility, the EMV chip's connecting tracks can be buried or rerouted, or logic gate positions shuffled, to head off such attacks, as concluded in Ref. [78]. Yet another threat is power analysis, which refers to the monitoring of the power profile of the chip during a cryptographic operation which may give hints about the encryption methods of the chip, thus proper counter-measures have been developed for this case.

Not only the chip cards as such but also a PIN-Entry Device (PED) located at the POS may be vulnerable to tampering efforts such as adding a Secure Digital (SD) card and connectors inside the device so that an attacker may have access to the information the PED executed, including card numbers and associated PINs. Protection mechanisms against such efforts include perfecting the tamper resistance functions in the PED such as device lock and memory cleaning upon tampering efforts.

As Ref. [79] indicates, criminals can try to attack any remote location, including even jail doors by hacking the respective office automatic central control points which manage the heating, lights, air conditioning, water, alarms, web cameras, etc. According to the report, the National Cyber Security Centre of Finland (NCSC-FI) at the Finnish Communications Regulatory Authority (FICORA) has noted the presence of a surprisingly large amount of unprotected devices related to such automatic control systems. If an unauthorized hacker gets access to such a system, costly damages may result. Also, home control systems are equally vulnerable due to default passwords that users do not always change, even if this is one of the simplest ways to increase the protection level. A potential threat of entering such systems is that the criminals may get hold of important information about the hours when the inhabitants are not present, in order to plan the timing for a subsequent burglary.

The unprotected device refers especially to the environment with Internet connectivity for entering the respective system. Password protection does not necessarily guarantee proper safety because the devices may have known vulnerabilities – which may often be very easy to detail from Internet sources for attack intentions. Aalto University has investigated automatized control system vulnerabilities in Finland and found that in the majority of cases there are known vulnerabilities per device with easily tracked instructions on the Internet. Such devices are used in energy production, electricity companies and water services.

One lifestyle-changing innovation is the connected, self-driving car. It is easy to guess that this environment attracts hackers to try to access the car control systems. There is publicly available information about the surprisingly easy ways of hacking some of the current Internet-connected cars as Ref. [80] informs, including more advanced wireless hijacking of the control system even during driving.

These examples merely scratch the surface, but they prove the importance of enhanced protection techniques to ensure safety of home and business environments. One of the challenges, though, is that there are increasingly activities concerned with hacking the IP network infrastructure and consumer gear, including very old components like routers, bridges and consumer accessories like Wi-Fi routers which do not have such systematic SW upgrading procedures as is the case with up-to-date computers, laptops and smart devices.

The importance of protection mechanisms is understandably considerably higher in environments like control systems that are meant for public transportation or other functions involving human well-being. As an example, Ref. [81] discusses the British signalling system for train control which could potentially be hacked to cause a crash. The conclusion of this specific case is that ensuring adequate protection is of utmost importance, in particular in replacing the old signal lights with new computers – if done without proper assessment and a prevention plan – could leave the rail network exposed to cyber-attacks which in turn may lead to a major accident. The system in question, the European Rail Traffic Management System (ERTMS), dictates critical safety information including how fast the trains should go and how long they will take to stop, so potential hackers could theoretically cause trains to travel too quickly with dramatic consequences.

With all the new and existing potential security holes resulting from the growing numbers of Internet-connected devices, it is clear that M2M security requires very special attention. As Ref. [34] summarizes, there is an increasing amount of known (and unimaginable) opportunities in the IoT, some examples being remote home thermostat control, self-driving cars, factories communicating with the container terminal and digitized city infrastructure. At the same time, new business and service models are emerging as our lifestyle becomes more convenient and mobile as a result of the ongoing digital revolution. We are now part of the connected world, which is in general beneficial for all, but as the amount of shared data and information grows, the risks also increase – not only for stored and transferred information but also for networked environments which include the means for controlling safety-critical systems like physical access rights and chemical processes.

The difference between fixed and mobile device security is on the whole not so huge, the openly radiating air interface being the most important differentiator in the wireless environment. The trend seems to indicate that as protection mechanisms of the networks are improving, the interest of the hacking efforts against the infrastructure is lowering. At the same time, with the popularity of the smart devices with vast amounts of applications, security breaches are focusing increasingly on the application level, e.g., via embedded malicious code hidden in the apps or via viruses that alter the functionality of the device or open doors for further attacks. The smart devices, including advanced SW executable mobile phones and tablets with radio connectivity, are assumingly thus becoming the primary targets for hackers, which requires active protection from the end-users as well as the operators providing the connectivity, and the service providers offering the backend for the app communications.

1.2.4 M2M Environment

One of the basic benefits of IoT is to facilitate always-connected devices to automatically control and report without human interaction. A simple example of this M2M communications is a refrigerator alerting about food items that require replenishing. The IoT environment also includes human interactions with machines and systems, e.g., making it possible to turn

lights on and off remotely. The environment may include awareness of various environmental and user-related items. For instance, when a user visits a supermarket, stored information about recently purchased items may trigger reminders on the mobile device as the user walks nearby, to suggest repurchasing the same products. The IoT environment also helps to optimize the logistics chain, presenting items that purchasers are able to carry home and highlighting heavier and less frequently purchased items which may be transported via alternative ways. This environment with everything connected (connected society) in an intelligent way (intelligent homes, offices and transportation) is actually a groundbreaking step in human history. It leverages the automatized Information and Communications Technology (ICT) society to the next level, optimizes the techno-economics and influences positively on the green values as energy consumption and transportation of goods and people is minimized via high level of awareness. This awareness is possible in real time due to collected data and post-processed information of IoT devices as they communicate with each other and systems. IoT is the next big thing to change our living and working environments.

IoT comprises this advanced environment, with a huge amount of networked devices, and objects and users enabling and benefiting from data. Nevertheless, IoT is still in a relatively early stage. The first concrete solutions that are starting to form IoT include smart devices, the cloud and sensors. The combination of various access technologies like RFID, wireless and cellular connectivity, as well as the evolved, miniature components and devices are essential enablers for advancing the connected IoT world. The sub-categories of IoT include industrial Internet and M2M communications, and smart consumer environments with devices and services like health devices and smart wristwatches which are easing mobile banking and many other daily functions.

The M2M environment is currently developing strongly with new, evolved technologies and services coming into commercial markets. It creates a great deal of challenges especially for the management of such a huge amount of always-connected device subscriptions and traffic, and for the security of the communications.

1.3 Standardization

The following sections summarize the standardization bodies relevant to wireless security, and lists the respective key standards.

1.3.1 The Open Mobile Alliance (OMA)

The OMA is a non-profit organization producing open specifications. The aim of the OMA is to create interoperable, end-to-end global services on any bearer network. The OMA was formed in 2002 by the key mobile operators, device and network suppliers, information technology companies and content and service providers. The OMA's specifications support fixed and mobile terminals, such as established cellular operator networks as well as emerging networks with M2M device communications. The OMA drives service enabler architectures and open enabler interfaces independently from the underlying wireless platforms, and has developed programs for testing the interoperability of new products [28].

In addition, the OMA has integrated the WAP Forum, Location Interoperability Forum (LIF), SyncML Initiative, Multimedia Messaging Interoperability Process (MMS-IOP),

Wireless Village, Mobile Gaming Interoperability Forum (MGIF), and the Mobile Wireless Internet Forum (MWIF) into the OMA for promoting end-to-end interoperability across different devices, geographies, service providers, operators and networks. The OMA drives the development of mobile service enablers such as Device Management (DM), M2M communications, Application Programming Interfaces (APIs) and Augmented Reality.

The Device Management Working Group of the OMA (DM WG) specifies protocols and mechanisms to achieve the management of mobile devices, services access and software on connected devices [29]. The OMA's suite of DM specifications includes 21 mobile service enablers and more than 60 management objects that provide ways to deploy new applications and services with low risk. There are an additional 21 management objects defined by other standards organizations and forums in cooperation with the OMA to minimize fragmentation. As an example, the OMA Diagnostics and Monitoring Management Object is used by 3GPP and WiMAX Forum, and other industry bodies have extended the OMA DM to the IP environment for use with remote sensors and in automotive scenarios. The aim of the OMA DM is to manage converged and multi-mode devices in technology-agnostic networks, including devices that do not have a SIM card which makes the OMA DM also suitable for M2M communications [30].

1.3.1.1 OMA Lightweight M2M 1.0

Network operators and enterprises are actively using device management in mobile communications consumer space. The current M2M DM environment relies partially on mobile devices, being typically proprietary as has been the consumers' DM technologies. Today, the OMA DM provides a more standardized way, although even in this case the handset providers normally implement proprietary mechanisms. The OMA's M2M Lightweight Device Management (LWM2M) standard is designed for this M2M market to reduce fragmentation.

The LWM2M stabilized in 2013. It is designed for mobile communications and M2M device environments for enhancing interoperability based on the Internet Engineering Task Force (IETF) standards. It is simple yet provides an efficient set of protocols, interfaces and payload formats. It includes pre-shared and public key methodologies, provisioning and bootstrapping. It is applicable to mobile systems, Wi-Fi and other IP-based devices and networks, and it is possible to be combined with other DM solutions.

The LWM2M defines a strong, holistic security solution via the Datagram Transport Layer Security (DTLS) v1.2 for Constrained Application Protocol (CoAP) communications. CoAP is a SW protocol designed for highly simplified electronic devices that communicate interactively over the Internet, and is especially useful for low-power sensors, switches and other remotely located components requiring supervision and controlling – in other words, it is suitable for IoT and M2M environments. More detailed information about CoAP can be found in Ref. [32].

The DTLS is similar to the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols providing the same integrity, authentication and confidentiality services, but instead of relying on the Transmission Control Protocol (TCP), the DTLS is transported via the User Data Protocol (UDP) which works for securing unreliable datagram traffic. It thus provides communications security for datagram protocols. The defined DTLS security modes of LWM2M are pre-shared key, raw public key and certificate mode. More information about the DTLS can be found in Ref. [33].

Table 1.1 OMA DM specifications as of December 2015

Enabler (document theme, category)	Release type, version
Device management, protocol	Enabler, 1.1.2, 1.2.1, 1.3*, 2.0*
Client side enabler API, protocol	Reference, 1.0
Device management smartcard, protocol	Enabler, 1.0
Client provisioning, protocol	Enabler, 1.1
M2M device classification, white paper	Reference, 1.0
Management object design guidelines, white paper	Reference, 1.0
Provisioning objects, device management application characteristics management object, white paper	Reference, 1.0.1
Browser, management object	Reference, 1.0
Connectivity, management object	Reference, 1.0
Device capability, management object	Enabler, 1.0
Delta record, management object	Enabler, 1.0
Diagnostics and monitoring, management object	Enabler, 1.0, 1.1, 1.2
Firmware update, management object	Enabler, 1.0.4
Gateway, management object	Enabler, 1.0, 1.1*
Lock and wipe, management object	Enabler, 1.0
Management policy, management object	Enabler, 1.0*
Scheduling, management object	Enabler, 1.0
SW component, management object	Enabler, 1.0, 1.1
SW and application control, management object	Enabler, 1.0*
Virtualization, management object	Enabler, 1.0*
OMA LWM2M, protocol	Enabler, 1.0*

* indicates draft or candidate

The LWM2M also includes bootstrapping methodologies that are designed for provisioning and key management via pre-configured bootstrapping (flash-based), and smartcard bootstrapping (SIM-based). The OMA LWM2M Version 1.0 was released in 2013.

1.3.1.2 OMA Standards

Table 1.1 summarizes the current and planned OMA DM specifications as indicated in Ref. [29,31,35].

1.3.2 The International Organization for Standardization (ISO)

The ISO together with the International Electrotechnical Commission (IEC) are worldwide standard-setting bodies for smartcards, among various other technologies related to electronics. They jointly have an important role in the standardization of the SIM card, which is the variant if smartcards are adapted into mobile communications systems. The SIM was introduced along with the 2G systems, firstly via the GSM, and it has been further developed in 3G systems which apply the 2G SIM and 3G Universal SIM (USIM) functionalities representing applications within the UICC.

The ISO provides an open process for participating stakeholders with the aim to facilitate the creation of voluntary standards. ISO 7816 defines Integrated Circuit Cards (ICCs),

commonly called smartcards as defined in Refs. [37] through [53]. This standard defines contact cards, which means that the communication between the card and external devices like card readers happens via the electrical circuit contacts of the card. It also functions as a base for the contactless cards extended via the ISO 14443 standard, which defines the communications via the RF channel. The contactless card is based on Near Field Communications (NFC). Both ISO 7816 and ISO 14443 are provided by the American National Standards Institute (ANSI).

The key standards for smartcards are ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 7501. The ISO/IEC 27000 series is also relevant to smartcards, describing information security management [90]. A complete list of the ISO/IEC JTC1/SC17 working groups and respective ISO standards can be found in Ref. [91].

ISO/IEC 7816 includes multiple parts from which Parts 1, 2 and 3 are related to contact cards and their essential aspects for interfaces, dimensions and protocols whereas Parts 4–6, 8, 9, 11, 13 and 15 include definitions for both contact and contactless card, e.g., for file and data element structures of the cards, API commands for the card use, application management, biometric verification, cryptographic functions and application naming. Part 7 defines a secure relational database for smartcards via Structured Card Query Language (SCQL) interfaces. Part 10 is related to applications of memory cards, including pre-paid telephone and vending machine cards.

The most important reference for the SIM/UICC card used in mobile communications systems is ISO 7816. Parts 1, 2 and 3 define the physical and communications characteristics as well as the application identifiers for embedded chips and data. This standard creates the base for mobile communications smartcards and is referenced in major part of the other standards. Moreover, ISO/IEC 7816 describes, among other definitions, the fundamental physical and logical aspects of the smartcard, voltage levels and file systems. Table 1.2 details the definitions of ISO/IEC 7816. ISO/IEC 7816 is jointly defined by the ISO and IEC, and edited by the Joint Technical Committee (JTC) 1 and Sub-Committee (SC) 17, Cards and Personal Identification [1] and adapted by ETSI, 3GPP and 3GPP2. More details about ISO/IEC 7816 sub-standards can be found in Chapter 4.

Table 1.2 ISO/IEC 7816 standard definitions

Standard	Description
7816-1	Physical characteristics
7816-2	Cards with contacts; dimensions and location of the contacts
7816-3	Cards with contacts; electrical interface and transmission protocols
7816-4	Organization, security and commands for interchange
7816-5	Registration of application providers
7816-6	Inter-industry data elements for interchange
7816-7	Inter-industry commands for SCQL
7816-8	Commands for security operations
7816-9	Commands for card management
7816-10	Electronic signals and answer to reset for synchronous cards
7816-11	Personal verification through biometric methods
7816-12	Cards with contacts; USB electrical interface and operating procedures
7816-13	Commands for application management in multi-application environment
7816-15	Cryptographic information application

ISO/IEC 14443 defines the interfaces of contactless smartcards that are used in NFC within about 10 cm from the respective reader. It includes the electrical and RF interfaces as well as the communications protocols. The cards operate on a 13.56 MHz frequency. This standard is the base for the contactless environment in access control, transit and financial applications as well as in electronic passports and in Federal Information Processing Standards (FIPS) 201 PIV cards.

ISO/IEC 15693 defines the so-called vicinity cards, including the base for the physical aspects, RF power, interface levels, collision management and protocols. The idea of vicinity cards is to operate from a maximum distance of 1 m from the reader. ISO/IEC 7501, in turn, has descriptions for machine-readable travel documents.

1.3.2.1 Other Relevant ISO/IEC Standards

The ISO/IEC has produced various other standards related to ICCs and payment cards. More information of the overall ISO/IEC standards can be found in Ref. [54].

1.3.3 The International Telecommunications Union (ITU)

The ITU is a worldwide organization that takes care of the global requirements of telecommunications. The ITU belongs to the United Nations (UN) and is specialized for Information and Communication Technologies (ICT). The tasks of the ITU include the allocation of global radio spectrum and satellite orbits, and development of technical standards. In addition, the ITU paves the way to enhance globally the access to ICTs to underserved communities. The ITU facilitates people's right to communicate via the developed communications [3]. The ITU is divided into three sectors from which the ITU-T concentrates on the standardization of the telecommunications area whilewhile the ITU-R standardizes the radio area, and the ITU-D focuses on the development of the telecommunications area. The recommendations of the ITU-T can be found in Ref. [4] and the set of recommendations of the ITU-R is located in Ref. [5]. The most relevant documentation of the ITU for the security aspects of telecommunications is found in the ITU-T series X, which describes data networks, open system communications and security.

1.3.4 The European Telecommunications Standards Institute (ETSI)

ETSI produces globally applicable standards for ICT including fixed, mobile, radio, broadcast, internet, aeronautical and other areas. ETSI created the first GSM and UMTS standards. The GSM standardization work was executed in various groups under the Special Mobile Group (SMG) until the 3GPP took over the major part of GSM and UMTS development in 1999. Nevertheless, an important part of the security aspects of mobile communications remains under ETSI [62]. This can be clearly seen from the continuum of the 13-series standards in ETSI. In practice, the security definitions of, e.g., UICC for GSM, 3G and advanced LTE systems are in fact found as a combined set of ETSI and 3GPP specifications.

As for the SIM/UICC, some of the most important ETSI standards are ETSI 102 221 (UICC definition) and ETSI 102 241 (UICC), which are based on the original GSM standards for the SIM as defined in TS 11.11 and TS 11.14.

The European Union recognizes ETSI as an official European standards organization, and one of the aims of ETSI is to provide access to European markets. ETSI clusters represent ICT standardization activities which are divided into Security, Home and Office, Better Living with ICT, Content Delivery, Fixed Networks, Wireless Systems, Transportation, Connecting Things, Interoperability, and Public Safety. ETSI executes standardization work under all of these clusters in various Technical Committees (TCs) and Working Groups (WGs).

As an example of SIM development, ETSI TS 103 384 defines the embedded UICC. It is aligned with the SIMalliance interoperable profile specification v1.0 and GSMA eSIM Technical Specification for M2M v2.0. There is also new development in the field such as the AppleSIM, and open items for handling the SIM-related data beyond SMS as in the case of IP-only remote management via the Bearer-Independent Protocol (BIP), which has been an active discussion topic at 3GPP SA2. The development of the embedded SIM solutions by ETSI and other parties is highly relevant for both consumer and M2M environments along with IoT and new types of end-user devices like wearables. This topic thus falls into the area of interoperable subscription management which is discussed in more detail later in this book.

1.3.5 The Institute of Electrical and Electronics Engineers (IEEE)

The IEEE provides a range of publications and standards that make the exchange of technical knowledge and information possible among technology professionals. One of the most important areas of IEEE standards is the IEEE 802 series, which defines a set of wired and wireless networks, including the Wireless Local Area Network (WLAN). IEEE publications and standards can be accessed via Refs. [6,7].

The IEEE is involved in standardization activities related to network and information security as well as in anti-malware technologies. Areas include encryption, fixed and removable storage, hard copy devices, and applications of these technologies in smart grids [8]. The IEEE Computer Society has a technical committee focused on computer security and privacy, with respective publications. IEEE also has an Industry Connections Security Group for tackling the malware environment. Some of the relevant IEEE standards in encryption domain are presented in Table 1.3.

Furthermore, the IEEE produces a multitude of standards for fixed and removable storage, security for hardcopy devices and Network and Information Security (NIS) for smart grids.

Table 1.3 Some of the most important IEEE standards related to encryption

Standard	Description
IEEE 1363-2000/ 1363a-2004	IEEE Standard Specifications for Public Key Cryptography
IEEE 1363.1-2008	IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices
IEEE 1363.2-2008	IEEE Standard Specification for Password Based Public Key Cryptographic Techniques
IEEE P1363.3	Draft Standard for Identity Based Cryptographic Techniques using Pairings

1.3.6 The Internet Engineering Task Force (IETF)

The IETF is an international and open community of network operators, vendors, designers and researchers. The task of the IETF is to be actively involved in the evolution of Internet architecture. The outcome of the work of the IETF is documented as recommendations, which are numbered as RFC *n*, where *n* is an integer number referring to a specific area of the definition. The list of documents can be found in [10], and the specific documents can be searched in [9,12].

The way of work of the IETF is based on email lists and exchanging comments online. This method greatly differs from the more formal approach of other international standardization organizations. The IETF also organizes meetings, though only three times per year. In addition to the actual standardization, the IETF performs tasks like assignment of parameter values for Internet protocols, which is taken care of in a centralized way by the Internet Assigned Numbers Authority (IANA), chartered by the Internet Society (ISOC). For more detailed information of the work and structure of IETF, Ref. [11] presents useful guidelines.

Specifically related to working group information sharing of Internet security, the IETF has a dedicated web page named the IETF Security Area [13].

1.3.7 The 3rd Generation Partnership Project (3GPP)

The 3GPP was established by several standardization bodies in 1998. Its original aim was to develop and enhance the 3G mobile communications systems. The current cooperating parties within 3GPP are the Association of Radio Industries and Businesses (ARIB), ATIS (Alliance for Telecommunications Industry Solutions), CCSA (China Communications Standards Association), ETSI, TSDSI (Telecommunications Standards Development Society of India), Telecommunications Technology Association (TTA) and Telecommunications Technology Committee (TTC). In addition to the set up of the 3GPP, there is also a group that takes care of the American variant – the 3GPP2.

Since the first introduction of the GSM-based SIM card, the concept has been further developed. Along with the handover of the mobile communications standardization work from the ETSI SMG group to the 3GPP, with the exception of few security-related items that still are taken care of by ETSI, the mobile communications part of the SIM card is included to an extended version of the original, UICC, which contains mobile communications functionalities per radio network type treated as separate applications. Not only the technical aspects have been enhanced, but also the SIM card's frame materials have been evolved, and there are e.g. eco-friendlier cards in the market nowadays [36].

Currently, the 3GPP is formed by a Project Coordination Group (PGC) and a total of five sub-groups which are: Services and System Aspects (SA), Radio Access Network (RAN), Core Network (CN), Terminals (T) and GSM EDGE Radio Access Network (GERAN). The original GSM standardization work of ETSI was taken over by the 3GPP GERAN almost completely in July 2000, excluding some of the security-related topics. The security algorithm specification work is not public. The User Equipment (UE), SIM and USIM specifications are listed in the original 11-series, and in the 34-series in later phases. Some relevant 3GPP specifications for the mobile communications security aspects can be found in 3GPP TS 42.009, V4.1.0, 23 June 2009 (security aspects). The security aspects of 3GPP are taken care of by SA working group 3.

The complete set of 3GPP technical specifications and recommendations as well as study reports can be found in Ref. [18]. For the LTE phase, Refs. [19,20,22] present overall security aspects. Furthermore, some of the most relevant 3GPP LTE security specifications are listed in Tables 1.4 and 1.5.

To summarize, a few of the highest level requirements of the 3GPP specifications, most importantly, the continued usage of current USIM needs to be ensured. The earlier USIM still needs to be able to access the EPS network of the LTE/LTE-A to ensure that previous USIM variants are also functional in future 3GPP networks. Furthermore, the level of the security should be at least equal or better compared to the UMTS.

In principle, the 3GPP specifications are the root information sources for the GSM, UMTS and LTE security aspects. Ref. [20] presents general aspects of the 3GPP security, and more detailed security aspects of the 3GPP systems are discussed in Chapter 2 in this book. The following sections detail further some of the key aspects of the SIM/UICC specifications defined by 3GPP.

The GSM triggered the introduction of the SIM for storing subscription related data. In the beginning, as defined in the first phase ETSI standard TS 11.11, the SIM was merely a physical

Table 1.4 Some of the key 3GPP security specifications

Topic	Specification
LTE security principles	TS 21.133, Security Threats and Requirements TS 33.120, Security Principles and Objectives TS 33.401, System Architecture Evolution (SAE); Security Architecture TS 33.402, System Architecture Evolution (SAE); Security Aspects of Non-3GPP
Security architecture	TS 22.022, Personalization of Mobile Equipment TS 33.102, Security Architecture TS 33.103, Integration Guidelines
Algorithms	TS 33.105, Cryptographic Algorithm Requirements Specifications for 3GPP Confidentiality and Integrity Algorithms: 1) f8 and f9; 2) KASUMI; 3) Implementers' Test Data; 4) Design Conformance Test Data
Lawful interception	TS 33.106, Lawful Interception Requirements TS 33.107, Lawful Interception Architecture and Functions TS 33.108, Handover Interface for Lawful Interception
Key derivation	TS 33.220, GAA: Generic Bootstrapping Architecture (GBA)
Backhaul security	TS 33.310, Network Domain Security (NDS); Authentication Framework (AF)
Relay Node security	TS 33.816, Feasibility Study on LTE Relay Node Security (also 33.401)
Home (e) Node B security	TS 33.320, Home (evolved) Node B Security
Technical reports of 3GPP	TR 33.901, Criteria for Cryptographic Algorithm Design Process TR 33.902, Analysis, 3G Authentication Protocol TR 33.908, Report, Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms

Table 1.5 The complete list of 3GPP security-related 33-series documents

Document	Description
TS 33.102	3G Security; Security Architecture
TS 33.103	3G Security; Integration Guidelines
TS 33.105	3G Security; Cryptographic Algorithm Requirements
TS 33.106	3G security; Lawful Interception Requirements
TS 33.107	3G security; Lawful Interception Architecture and Functions
TS 33.108	3G security; Handover Interface for Lawful Interception
TS 33.110	Key Establishment between a Universal Integrated Circuit Card (UICC) and a Terminal
TS 33.116	Security Assurance Specification for the MME Network Product Class
TS 33.117	Catalogue of General Security Assurance Requirements
TS 33.120	Security Objectives and Principles
TS 33.141	Presence Service; Security
TS 33.187	Security Aspects of Machine-Type Communications (MTC) and Other Mobile Data Applications Communications Enhancements
TS 33.200	3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) Application Layer Security
TS 33.203	3G Security; Access Security for IP-Based Services
TS 33.204	3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) User Security
TS 33.210	3G security; Network Domain Security (NDS); IP Network Layer Security
TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)
TS 33.221	Generic Authentication Architecture (GAA); Support for Subscriber Certificates
TS 33.222	Generic Authentication Architecture (GAA); Access to Network Application Functions Using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)
TS 33.223	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Function
TS 33.224	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Layer
TS 33.234	3G Security; Wireless Local Area Network (WLAN) Interworking Security
TS 33.246	3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)
TS 33.259	Key Establishment between a UICC Hosting Device and a Remote Device
TS 33.269	Public Warning System (PWS) Security Architecture
TS 33.303	Proximity-Based Services (ProSe); Security Aspects
TS 33.310	Network Domain Security (NDS); Authentication Framework (AF)
TS 33.320	Security of Home Node B (HNB) / Home evolved Node B (HeNB)
TS 33.328	IP Multimedia Subsystem (IMS) Media Plane Security
TS 33.401	3GPP System Architecture Evolution (SAE); Security Architecture
TS 33.402	3GPP System Architecture Evolution (SAE); Security Aspects of Non-3GPP Accesses
TR 33.769	Feasibility Study on Security Aspects of Machine-Type Communications Enhancements to Facilitate Communications with Packet Data Networks and Applications
TR 33.803	Coexistence between TISPAN and 3GPP Authentication Schemes
TR 33.804	Single Sign On (SSO) Application Security for Common IP Multimedia Subsystem (IMS) based on Session Initiation Protocol (SIP) Digest
TR 33.805	Study on Security Assurance Methodology for 3GPP Network Products

Table 1.5 (Continued)

Document	Description
TR 33.806	Pilot Development of Security Assurance Specification for MME Network Product Class for 3GPP Network Product Classes
TR 33.810	3G Security; Network Domain Security/Authentication Framework (NDS/AF); Feasibility Study to Support NDS/IP Evolution
TR 33.812	Feasibility Study on the Security Aspects of Remote Provisioning and Change of Subscription for Machine to Machine (M2M) Equipment
TR 33.816	Feasibility Study on LTE Relay Node Security
TR 33.817	Feasibility Study on (Universal) Subscriber Interface Module (U)SIM Security Reuse by Peripheral Devices on Local Interfaces
TR 33.820	Security of Home Node B (HNB)/Home evolved Node B (HeNB)
TR 33.821	Rationale and Track of Security Decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)
TR 33.822	Security Aspects for Inter-Access Mobility between Non-3GPP and 3GPP Access Network
TR 33.823	Security for Usage of Generic Bootstrapping Architecture (GBA) with a User Equipment (UE) Browser
TR 33.826	Study on Lawful Interception Service Evolution
TR 33.828	IP Multimedia Subsystem (IMS) Media Plane Security
TR 33.829	Extended IP Multimedia Subsystem (IMS) Media Plane Security Features
TR 33.830	Feasibility Study on IMS Firewall Traversal
TR 33.831	Study on Security on Spoofed Call Detection and Prevention (Stage 2)
TR 33.832	Study on IMS Enhanced Spoofed Call Prevention and Detection
TR 33.833	Study on Security Issues to Support Proximity Services
TR 33.838	Study on Protection against Unsolicited Communication for IMS (PUCI)
TR 33.844	Security Study on IP Multimedia Subsystem (IMS) based Peer-To-Peer Content Distribution Services (Stage 2)
TR 33.849	Study on Subscriber Privacy Impact in 3GPP
TR 33.859	Study on the Introduction of Key Hierarchy in Universal Terrestrial Radio Access Network (UTRAN)
TR 33.860	Study on Security Aspects of Cellular Systems with Support for Ultra-Low Complexity and Low Throughput Internet of Things
TS 33.863	Study on Battery Efficient Security for Very Low Throughput Machine Type Communication Devices
TR 33.865	Security Aspects of WLAN Network Selection for 3GPP Terminals
TR 33.868	Study on Security Aspects of Machine-Type Communications (MTC) and Other Mobile Data Applications Communications Enhancements
TR 33.871	Study on Security for Web Real Time Communications (WebRTC) IP Multimedia Subsystem (IMS) Client Access to IMS
TR 33.872	Security Enhancements To Support WebRTC Interworking
TR 33.879	Study on Security Enhancements for Mission Critical Push To Talk (MCPTT) over LTE
TR 33.888	Study on Security Issues to Support Group Communication System Enablers (GCSE) for LTE
TR 33.889	Feasibility Study on Security Aspects of Machine-Type Communications Enhancements to Facilitate Communications with Packet Data Networks and Applications

(*Continued*)

Table 1.5 (Continued)

Document	Description
TR 33.895	Study on Security Aspects of Integration of Single Sign-On (SSO) Frameworks with 3GPP Operator-Controlled Resources and Mechanisms
TS 33.897	Study on Isolated E-UTRAN Operation for Public Safety; Security Aspects
TR 33.901	Criteria for Cryptographic Algorithm Design Process
TR 33.902	Formal Analysis of the 3G Authentication Protocol
TR 33.905	Recommendations for Trusted Open Platforms
TR 33.908	3G Security; General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms
TR 33.909	3G Security; Report on the Design and Evaluation of the MILENAGE Algorithm Set; Deliverable 5: An Example Algorithm for the 3GPP Authentication and Key Generation Functions
TR 33.916	Security Assurance Scheme for 3GPP Network Products for 3GPP Network Product Classes
TR 33.918	Generic Authentication Architecture (GAA); Early Implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) Connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF)
TR 33.919	3G Security; Generic Authentication Architecture (GAA); System Description
TR 33.920	SIM Card Based Generic Bootstrapping Architecture (GBA); Early Implementation Feature
TR 33.924	Identity Management and 3GPP Security Interworking; Identity Management and Generic Authentication Architecture (GAA) Interworking
TR 33.937	Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)
TR 33.969	Study on Security Aspects of Public Warning System (PWS)
TR 33.978	Security Aspects of Early IP Multimedia Subsystem (IMS)
TR 33.980	Liberty Alliance and 3GPP Security Interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA)
TR 33.995	Study on Security Aspects of Integration of Single Sign-On (SSO) Frameworks with 3GPP Operator-Controlled Resources and Mechanisms

card that represented the GSM application. Along with the 3G system development, the SIM was enhanced and took the term of UICC. It refers to a physical card that contains logical functionality as described in 3GPP TS 31.101. Furthermore, the USIM refers to the 3G application residing on the UICC as defined in 3GPP TS 31.102. In addition to the 3G-USIM application, the UICC is capable of storing various other applications, among which the SIM, or 2G-SIM, is used for GSM, and the IMS SIM (ISIM) is used for the IP Multimedia Subsystem (IMS) of the LTE/LTE-A. With the further development of the 3GPP system, the UICC still continues to be the trusted element for the LTE/SAE user domain, including newly evolved applications and security. In fact, the importance of the role of the UICC is increasing as of the Release 8 features.

The following sections summarize some of the key aspects in the development path of the SIM/UICC up to the 3GPP Release 12.

1.3.7.1 Release 8

The USIM in the LTE phase is defined in 3GPP TS 31.102 as is the case for the 3GPP 3G. Along with Release 8, the earlier USIM features continue to support LTE. Furthermore, there are now new features that better take into consideration the non-3GPP radio access, Mobility Management (MM) and emergency cases. Unlike previous releases, Release 8 dictates that the USIM authenticates and secures access to the Evolved Packet Core (EPC) for non-3GPP access systems as a result of the USIM support for advanced network selection mechanisms. The additional radio access networks are Code Division Multiple Access (CDMA) 2000 and High Rate Packet Data (HRPD) by enabling USIM Public Land Mobile Network (PLMN) lists for the selection of roaming between CDMA, UMTS and LTE.

As the secure element based on the USIM is highly protected, it is further enhanced for storing the LTE/ System Architecture Evolution (SAE) MM parameters. It also stores important data, such as location and EPS security context instead of the user equipment. Furthermore, Release 8 enhances personal safety aspects by allowing the USIM to store a user's In Case of Emergency (ICE) information, like allergies, blood type and emergency contact information that the emergency personnel can retrieve even if the user is not able to answer or establish a call. The 3GPP has also included a USIM storage for eCall parameters. As soon as it is activated, the eCall is able to establish a voice call (either manually or by relying on the vehicle's sensors) with emergency personnel services and sends key information like the user's location and vehicle identification data in order to speed up the emergency service's action time.

1.3.7.1.1 Release 8 Toolkit features

The 3GPP specification TS 31.111 defines improvements for the Toolkit features of Release 8. The Release 8 Toolkit supports NFC as the contactless interface is integrated with the UICC which allows the UICC applications to proactively trigger contactless interfaces. The Toolkit also supports the triggering of OMA-DS (Data Synchronization) and OMA-DM (Device Management) sessions for easier device support and data synchronization. The OMA-DS protocol (SyncML DS) is a data-type and transport-agnostic protocol for any transport, such as Bluetooth and any mobile radio access, and can synchronize any data type such as contacts, calendar, files and Java credit card records [92].

Furthermore, the Toolkit takes into account devices with limited capabilities like M2M devices and data cards which might not contain a normal user interface such as a screen and keypad. The Toolkit event informs the UICC application about network rejection, e.g., in the case of failure in a registration attempt. Operators may use this functionality for issue solving, e.g., radio outage areas. Finally, the Toolkit supports UICC proactive commands for transferring radio signal strength measurement reports from eNodeB.

1.3.7.1.2 Contact manager

Release 8 defines a multimedia phone book for USIM as stated in 3GPP TS 31.220, based on OMA-DS and its corresponding JavaCard API (3GPP TS 31.221).

1.3.7.1.3 Remote management

Along with the enhanced ability to create IP sessions, Release 8 defines evolved remote management as described in 3GPP TS 31.115 and TS 31.116. It provides capability to utilize remote application and file management over a Card Application Toolkit Transport Protocol

(CAT_TP) link based on a BIP session between the UE and USIM. Also, the related algorithms have been renewed for updating UICC from the Data Encryption Standard (DES) to the Advanced Encryption Standard (AES) algorithm which provides additional flexibility and security.

1.3.7.1.4 Application management with third parties

Release 8 provides means for confidential application management of UICC for third parties, thus providing possibility for hosting confidential third-party applications. This is beneficial for managing and ensuring feasible business models in Mobile Virtual Network Operator (MVNO) and mobile payment environments, e.g., via memory rental of UICC in such a way that this memory and respective contents can be managed remotely and securely by the third party.

1.3.7.1.5 Secure channel

Release 8 provides a trusted and secure communications channel for Universal Serial Bus (USB) and ISO interfaces between UE and UICC, or between applications that are located on UICC and UE. For the overall Secure Channel Protocols (SCPs), please refer to section 4.11.1.

1.3.7.1.6 Other aspects

Among other topics, the 3GPP CS6 group has worked on the following key items that have an impact on UICC.

The home operator and the user are allowed to prioritize certain Radio Access Technologies (RATs) in the PLMN selection via the *support of multi-system PLMN selection*. The added networks are E-UTRAN, CDMA2000-1xRTT and CDMA2000 HRPD. The user may thus select certain operators in the list that are favoured over others. This RAT prioritization functionality can apply to the RATs supported and available in the Home PLMN (HPLMN) as well in the Visited PLMN (VPLMN). The *storage of Electric Power System (EPS) MM parameters on the USIM* provides the possibility to optimize the initial network selection when on an LTE network by provisioning of the EPS MM (EMM) parameters on the USIM. *The provisioning for Home (e)NodeB* refers to the possibility for the UE to maintain a list of allowed Closed Subscriber Group (CSG) identities, and it will be possible to store them in the USIM in the future. The *support of LTE in the EF (Elementary File) Operator PLMN List* is an item that adds the possibility to assign an operator name tag for LTE-based networks to the operator's PLMN list. The *support of EPS in the USIM Application Toolkit (USAT); extension of Call Control* is an item that provides extension of the procedures and commands for the call control when an EPS Packet Data Network (PDN) connection is requested.

1.3.7.2 Release 9

3GPP Release 9 introduces enhancements for M2M and Home eNodeB (femtocell) environments of LTE which have also been taken into account in the UICC development. As the femtocell deployment scenario is highly relevant in paving the way for LTE-Advanced (ITU-compliant 4G), the importance of the respective USIM is increasing for managing provisioning information to the femtocell. Being a highly reliable security element, access to femtocells is an ideal option when relying on the USIM that is based on the CSG list controlled by the operator or user.

The femtocell is in practice a consumer's plug-in element, meaning that it can be deployed by users without any operator control. The challenge of the femtocell is that its location cannot be predicted beforehand by the respective MNO and thus the respective radio network optimization is challenging. The location discovery of femtocells could be provided via enhanced toolkit commands, which are under consideration at 3GPP. Operators could thus use this information for possibly adjusting network services within that area.

The upcoming releases will develop and capitalize on the IP layer for UICC Remote Application Management (RAM) over HTTP or HTTPS. The network can also send a push message to the UICC to initiate a communication using the TCP protocol. Also the M2M dedicated form factor for the UICC is one of the development topics for extending the requirements beyond the currently defined temperatures and mechanics. Yet another discussion topic is the full IP UICC integration to the IP-based UE along with services over Ethernet Emulation Mode (EEM) and USB, as well as the UICC capability to register on multicast-based services.

The main changes of 3GPP CS6 work in Release 9 are related to CSG management. The following lists key changes. The UE shall contain both independent lists: (a) a list of allowed CSG identities controlled by both the operator and the user; and (b) an operator-controlled list of allowed CSG identities. It shall be possible to store both lists on the USIM, and the allowed CSG list on the USIM may be inhibited. It shall be possible to store the CSG type in textual and/or graphical format which has been a Release 8 unfulfilled requirement. It shall also be possible to provide UICC applications with a list of CSG identities available for selection, and to inform UICC applications when selecting and leaving a CSG cell.

Other CS6 key items that impact the UICC in Release 9 are the following. *Introduction of operator controlled CSG list for H(e)NodeB* is a new operator-controlled CSG list. *Correction of controlled CSG list for H(e)NodeB* presents correction of access conditions, names and indicators. *Introduction of an indicator for inhibition of the allowed CSG list* refers to the item based on home operator preferences, and the use of the allowed CSG list on the USIM that may be inhibited.

Furthermore, the following Card Application Toolkit (CAT) commands have been extended. *Terminal Profile* refers to the support of CSG cell discovery and cell selection event. *Provide Local Information* refers to the support of the CSG list and corresponding H(e)NB names of surrounding CSG cells. *Terminal Response* refers to the inclusion of the CSG ID list identifier. There is also a definition produced for the *CSG cell selection* event, and new 'q' class is added to state the support of *Physical Layer Identifier (PLI)* in CSG cell discovery and *event download* in CSG cell selection.

1.3.7.3 Release 10

1.3.7.3.1 Key enhancements

The following summarizes the key highlights of Release 10 enhancements for the UICC. (a) CAT over AT commands and encapsulated CAT (eCAT); (b) UICC access to IMS: IMS Application Reference ID (IARI) of UICC-based applications; Session Initiation Protocol (SIP) session management on the handset; BIP for IMS; (c) USIM for Home(e)NBs (femtocells) is optional for authentication of the hosting party; (d) USIM on Relay Nodes (RNs) has two new applications, i.e., USIM-INI and USIM-RN, and Binding of RN to USIM via Secure Channel (TS 102 484).

Furthermore, the most important 3GPP specifications that impact UICC in Release 10 are TS 31.101 (Physical and Logical Characteristics of the UICC-Terminal Interface), TS 31.102 (Characteristics of the USIM Application), TS 31.103 (Characteristics of the ISIM Application), TS 31.111 (USAT), and TS 31.130 (USIM API for Java Card).

1.3.7.3.2 Main features in Release 10

The RN will have two flavours of USIM, which are USIM-INI and USIM-RN. The USIM-INI is used for the link establishment (initialization) whereas the USIM-RN is used for authenticating with the Core Network (CN) and offering RN services. These have an impact on the 3GPP TS 31.101 and TS 31.102. The *Smartcard Web Server* (*SCWS)* will have an introduction of an SCWS launch functionality. A dedicated EF for the Mobile Equipment (ME) is defined to check which icon and text should be indicated in the phone's main menu in order to access the SCWS on the UICC. The item called *Communication Control by USIM for IMS* is similar to the Call Control but it is meant for the IMS Services. There is also an addition of *USAT facility control* which refers to the USAT commands over the AT modem commands support. The *CSG lists display Control Management by USIM* refers to the possibility to store and manage the CSG lists by USIM with user interaction. The *UICC access to IMS* means an IARI list and SIP Push to UICC Apps [93]. Finally, the *NAS Parameters storage update and corrections* refers to the storage rate of security context and non-access stratum configuration storage.

1.3.7.3.3 Other Release 10 features

The following lists other relevant Release 10 features impacting SIM/UICC. *The SIP Push*, i.e., the UICC access to IMS refers to the item that only applies if class 'e' (BIP) and 't' (UICC Access to IMS) are supported by the ME. In this solution, the IMS access is managed by the ME in the following cases: (a) PDN context establishment; (b) registration and data flow; (c) USIM and ISIM use is possible. Furthermore, the USIM or ISIM include a parameter called EF_UICCIARI, which refers to an EF that contains a list of IMS Application Reference Identifiers associated with active applications installed on the UICC that are included in the SIP Register.

Other items resulting in a modified flow chart are the *discovery of the UICC's IARI and IMS registration*, and *notification of incoming IMS data*. Furthermore, the OTA HTTPS and SIP Push are defined. In this solution, the SIP Push can be used to trigger the HTTPS client in the UICC, and IMS SIP dialogue can be used for indicating the AdminAgent in the UICC the information for the HTTPS access to the OTA server.

1.3.7.4 Release 11

Release 11 includes the following enhancements. The *4FF* (Fourth Form Factor, i.e., nano-SIM) which has been driven by Apple and first used in the iPhone 5. The *secure channel for CAT* has been defined to protect all CAT communication; this item has been inspired by a special-use case for the MVNO environment. The *secure channel for eCAT* has been defined to protect encapsulated CAT exchanged with an eCAT client which could be the Trusted Execution Environment (TEE) in the ME or an endpoint outside the ME; the goal is to enable a trusted user nterface based on CAT. The *adoption of key establishment scenario 3* by GlobalPlatform is an item to establish initial keysets in a service provider's SD; this provides AES-level security based on elliptic curve cryptography. The *Forced Refresh* is an item meant

for cases where the terminal keeps a data connection always on; it is also required for the profile management of the embedded UICC (eUICC). Finally, the *API for HTTPS* has been defined to allow an applet to use HTTPS communication.

1.3.7.5 Release 12

As for the 3GPP Release 12 highlights, the Temporary User Authentication Key (TUAK) is a second standardized authentication algorithm next to Milenage. It is based on the Keccak Hash algorithm, and is the winner of the SHA-3 contest. It is specified as of Release 12 in the 3GPP TS 35.231, with the aim of using it in the eUICC.

Another key topic of Release 12 standardization is the retrieval of the DNS server addresses from the network. This item is similar to the Dynamic Host Configuration Protocol (DHCP) on a personal computer which allows applications based on domain names only. All resolutions are thus provided by the network which means that the reconfiguration has no impact on applets.

1.3.8 The 3rd Generation Partnership Project 2 (3GPP2)

The 3GPP2 is a 3G telecommunications specifications project meant for the North American and Asian markets. It works in cooperation with 3GPP, and its aim is to develop global specifications for ANSI/TIA/EIA-41 -based 3G cellular radio telecommunications evolution and global specifications for the Radio Transmission Technologies (RTTs) supported by ANSI/TIA/EIA-41.

In addition to the communications with the 3GPP, the 3GPP2 is a collaborative effort between five officially recognized standardization development organizations, or Organizational Partners (OPs): Japanese Association of Radio Industries and Businesses (ARIB), TTC, Chinese China Communications Standards Association (CCSA), North American Telecommunications Industry Association (TIA) and Korean Telecommunications Technology Association (TTA). The Technical Specification Groups (TSGs) of 3GPP2 are TSG-A (Access Network Interfaces), TSG-C (CDMA2000), TSG-S (Services and Systems Aspects), and TSG-X (Core Networks). As is the case for freely downloadable specifications and reports of 3GPP, each 3GPP2 TSG has a dedicated section on the website which can be accessed for the downloading of specifications and reports. More information about the 3GPP2 can be found in Ref. [89].

1.3.9 The GlobalPlatform

The GlobalPlatform is an industry organization which consists of several committees for the standardization of subscriber cards and systems [55]. The GlobalPlatform is an internationally recognized non-profit association with the aim to establish, maintain and promote adoption of interoperable infrastructure standards for smartcards, devices and systems. The focus of the GlobalPlatform is to simplify and speed up the development, deployment and management of interoperable security applications and solutions. The GlobalPlatform standards establish mechanisms and policies for enabling secure communications, and many banks have adopted them at a global level for cryptographic data loading based on JavaCard.

One of the focus areas of the GlobalPlatform is secure deployment and management of multiple applications on secure chip technology by using standardized infrastructure, providing service providers means to develop digital services and deploy them uniformly across different devices and channels. This interoperable approach in security and privacy parameters enables dynamic combinations of secure and non-secure services from multiple providers on the same device. The GlobalPlatform is thus an international industry standard for trusted end-to-end secure deployment and management solutions, aiming for global adoption across finance, mobile and telecommunications, government, premium content, automotive, healthcare, retail and transit sectors via interoperability and scalability of application deployment and management through its secure chip technology open compliance program. the GlobalPlatform has over 120 members working on the alignment with existing and emerging market requirements. The GlobalPlatform's interoperability solves service provider issues in ensuring compatibility with different security architectures and APIs which are meant for secure access services offered by devices. The aim of the GlobalPlatform is thus to eliminate compatibility and scalability issues via standardized infrastructure and APIs for the management of applications on secure chips compatible with connected devices.

A concrete example of the recent work by the GlobalPlatform is the development of the interoperable Subscription Management (SubMan) standard. Some other key areas of GlobalPlatform's work are the following.

First, service providers' services rely on a backend server which is under their control. This solution ensures the respective end-point's security level. The GlobalPlatform further gives possibility for service providers to establish a second trusted and secure endpoint, which is a secure chip of the end user's device. This second trusted endpoint provides the service provider and the end-user with end-to-end security.

Secondly, the GlobalPlatform defines two secure components based on the SE and TEE. In addition to protecting service providers and consumers from external hackers, these secure components prevent competing service providers or the consumer from accessing sensitive application information. Each service provider may load secret keys into the SE to protect its own applications.

Thirdly, the GlobalPlatform messaging technology standardizes messaging to ensure the correct utilization of data and formats to load and provision a service into a secure component.

1.3.10 The SIMalliance

The SIMalliance is a global, non-profit industry association with the aim to simplify SE implementation and thus to drive the creation, deployment and management of secure mobile services. The SIMalliance also promotes the useful role of the SE in delivering secure mobile applications and services across all devices with an access to wireless networks. It also identifies and addresses SE-related technical issues, clarifies and recommends existing technical standards relevant to SE implementation, and promotes an open SE ecosystem to facilitate and accelerate delivery of secure mobile applications globally [56]. As is the case with the GlobalPlatform and GSMA, the SIMalliance is also involved in the development of interoperable subscription management solutions.

1.3.11 The Smartcard Alliance

The Smartcard Alliance is a multi-industry association focusing on the information sharing, adoption, use and application of smartcard technology. The Smartcard Alliance coordinates projects such as education programmes, market research, advocacy, industry relations and open forums and eases the networking and innovation of its members and cooperating parties. The Smartcard Alliance acts thus as a centralized industry interface for smartcard technology, and follows the impact and value of smartcards in the United States and Latin America. The worldwide coverage of members include representatives from financial, government, enterprise, transportation, mobile telecommunications, healthcare and retail industries, and therefore has views from issuers and adopters of smartcard technology to understand the implementation of smartcard based systems for secure payments, identification, access and mobile communications [73].

1.3.12 The GSM Association (GSMA)

The GSMA has a long history, going back to the early days of GSM development. Its roots originate from the GSM Memorandum of Understanding (MoU), which was the basis for the agreement of the GSM standards in a form of an association representing the participating operators [58].

Currently, the GSMA represents the interests of mobile operators worldwide. There are about 800 operators and 250 companies involved, including handset and device manufacturers, software companies, equipment providers, Internet companies and other related industry sectors [57]. Some of the concrete key areas of the GSMA are the following.

The first item is the spectrum for mobile broadband. The GSMA is involved in spectrum initiatives to ease the mobile broadband deployments. The GSMA investigates the importance of future availability of affordable, ubiquitous, high-speed mobile broadband services. It can be estimated that the industry is likely to require around 1600–1800 MHz of spectrum to ensure widespread access to mobile broadband services. Also, the data traffic may increase by nearly 10 times by 2019 according to Ref. [70], which is a report authored by GSMA Intelligence, a source of global mobile operator data, analysis and forecasts.

Secondly, the GSMA is involved with public policy. The GSMA contributes, e.g., to the *Mobile Policy Handbook* and policy case studies and is active in areas of capacity building in mobile sector regulation, privacy in the mobile environment, mYouth, energy efficiency, roaming, health, connected society, mobile commerce and economy such as payment, retail and transport, as well as utilities and disaster response.

Thirdly, the GSMA is involved with Network 2020 which is paving the way for the forthcoming 5G, including evolved items such as Voice over LTE (VoLTE), Rich Communications, HD Voice and IP Interconnect.

The fourth key item is Connected Living, which covers a variety of topics such as automotive, health, transport, utilities and trackers. In addition, there are also numerous other activities such as globally recognized events.

Apart from the above-mentioned items, the GSMA actively contributes to subscription management development, and is also involved with the embedded SIM development for the M2M environment. As an example, GSMA eSIM (M2M) Technical Specification v2.0,

together with the contribution of the SIMalliance interoperable profile specification v1.0, resulted in the GSMA eSIM (M2M) TS v3.0 in 2015, combined with the ideas of SCP03t-version for the secure channel.

1.3.13 The National Institute of Standards and Technology (NIST)

The US National Institute of Standards and Technology (NIST), together with various industries, develops a voluntary, non-regulatory cyber-security framework to address critical infrastructure and new challenges especially as a result of the IoT and M2M. The NIST Framework was initiated officially in 2014. The NIST Framework development has involved a Presidential Executive Order, the mobile industry and the telecommunications sector. The focus of the framework is thus on the security and privacy for the evolution of M2M and IoT [23,24].

1.3.14 The National Highway Transportation and Safety Administration (NHTSA)

The focus of the NHTSA is on improving safety and mobility on US roadways. One of its topics is wirelessly connected vehicle technology which involves vehicles such as cars and trains, and facilitates the communication of safety and mobility information to each other. The ultimate aim of the initiative is to help save human lives, prevent injuries, ease traffic congestion and improve the environment. The NHTSA is thus remarkably engaged with vehicle cyber security [25].

1.3.15 Other Standardization and Industry Forums

1.3.15.1 The European Conference of Postal and Telecommunications Administrations (CEPT)

CEPT was initiated in 1959. It soon expanded as new members joined, and currently has 48 members, covering nearly all of Europe. Having first represented monopoly-holding postal and telecommunications administrations, CEPT continues to cooperate on commercial, operational, regulatory and technical standardization issues [14]. CEPT activities are coordinated by the permanent European Communications Office (ECO).

CEPT publishes documents related to requirements for approval, approval authorities, certification bodies and testing laboratories for telecommunications terminal services for attachment to public telecommunications networks or access to public telecommunications services.

1.3.15.2 The Accredited Standards Committee on Telecommunications (T1)

T1 develops telecommunications standards, definitions and technical reports for the needs of the United States. T1 has six Technical Sub-Committees (TSCs), which are administered by the T1 Advisory Group (T1AG). As an example, GSM development is handled by T1P1 (Wireless/Mobile Services and Systems), which is further divided into five sub-groups: T1P1.1 for International Wireless/Mobile Standards Coordination, T1P1.2 for Personal Communications Service Descriptions and Network Architectures, T1P1.3 for Personal Advanced Communications Systems (PACS), T1P1.5 for PCS 1,900, and T1P1.6 for CDMA/TDMA.

1.3.15.3 The American National Standards Institute (ANSI)

The aim of ANSI is to strengthen the position of the United States in the global economy. It also takes care of the important safety and health issues of consumers, as well as the protection of the environment [15]. One of its tasks is to promote the use of the US standards. It also facilitates the adoption of international standards for the US environment if these are seen to be suitable for the needs of the user community. ANSI is the sole representative of the United States at the ISO and the IEC.

ANSI offers an online library with open documents, as well as restricted documents for members only [16].

1.3.15.4 The Association of Radio Industries and Businesses (ARIB)

ARIB is the Japanese standardization body, which has strongly developed 3G definitions of mobile communications, and interacts in cooperation with other bodies developing further stages of mobile communications.

1.3.15.5 The Telecommunications Technology Committee (TTC)

The TTC is another Japanese standardization body, which has been actively developing mobile communications systems. The TTC Standard Summary can be found in Ref. [17].

1.3.16 The EMV Company (EMVCo)

Europay, MasterCard and Visa have formed the EMV Company (EMVCo) and produced the *Integrated Circuit Card Specifications for Payment Systems*, based on the ISO/IEC 7816 standard. The aim of this initiation is to ease the card and system implementation of a stored value system [63].

1.3.17 The Personal Computer/Smartcard (PC/SC)

The PC/SC is an international specification for cards and readers, and is applicable to contact cards. The further evolution of v2.0 also introduces a PIN pad for the card communications. Various Operations System (OS) companies support the PC/SC, and it is currently a common middleware interface for PC logon applications.

1.3.18 The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is an umbrella for national US standards for the implementation of electronic health transaction systems in a secure way. Some examples of the respective transaction functions include patient claims, enrolment, eligibility, payment and benefit coordination. HIPAA sets requirements for smartcards in this environment to ensure data security and patient privacy.

1.3.19 The Common Criteria (CC)

The CC refers to an international security evaluation framework. The basic idea of the CC is to provide reliable IT product evaluation for the security capabilities. These products include the hardware of the secure integrated cards as well as the software of smartcard operating

systems and applications. The CC is thus used for an independent assessment with the result indicating the ability of the product to comply with security standards. As the CC is globally recognized and established, it is especially useful for customers requiring very high security, such as governments that increasingly want the CC certification as a part of their security solution investments. Furthermore, the CC allows the vendors to tackle security solutions based on concrete needs more efficiently while offering a broad set of products. The CC is thus an international standard for computer security certification, including evaluation of information technology products and protection profiles [59].

1.3.20 The Evaluation Assurance Level (EAL)

An important security-related topic for UICC security is compliance with the CC. It refers to standards denoting the EAL from 1 through 7 as summarized in Table 1.6. The SIM/UICC complies with the level 4 EAL which makes it one of the most protected solutions in mobile communications.

The EAL indicates a numeric value that is based on the completion of a CC evaluation, the higher values meaning more enhanced assurance levels. It should be noted that the value of EAL does not explicitly indicate the absolute security level as such but it states at which level the system has been tested to meet specific assurance requirements.

Table 1.6 The EAL classes of CC

Level	Item	Description
EAL 1	Functionality tested	Indicates some confidence in correct operation although the threats are not considered as serious. Evidence that the Target of Evaluation (TOE) functions consistently with the respective documentation, providing useful protection
EAL 2	Structure tested	Applicable in environments where developers users require low or moderate level of independently assured security, e.g., legacy systems
EAL 3	Methodically tested and checked	Applicable in environments where developers/users require a moderate level of independently assured security, with thorough investigation of TOE
EAL 4	Methodically designed, tested and reviewed	Highest level at which it is assumed to be economically feasible to retrofit to an existing product line. Applicable in environments where developers/users require a moderate or high level of independently assured security. Many operating systems belong to this category
EAL 5	Semi-formally designed and tested	Provides developers with maximum assurance from security engineering. Numerous smartcard devices have been evaluated at this level
EAL 6	Semi-formally verified design and tested	Applicable to the development of security TOEs for application in high-risk situations, with additional costs involved but justified by the value of the protected assets
EAL 7	Formally verified design and tested	Applicable to the development of security TOEs for application in extremely high risk situations, with additional costs justified by the value of the protected assets

1.3.21 The Federal Information Processing Standards (FIPS)

FIPS are a set of standards developed by the Computer Security Division within the National Institute of Standards and Technology (NIST). FIPS are designed to protect federal assets, including computer and telecommunications systems. FIPS 140 (1–3) and FIPS 201 apply to smartcard technology and pertain to digital signature standards, advanced encryption standards and security requirements for cryptographic modules.

FIPS 140 (1–3) contains security requirements related to the secure design and implementation of a cryptographic module. The items include cryptographic module specification, cryptographic module ports and interfaces, roles, services and authentication, finite state model, physical security, operational environment, cryptographic key management, Electromagnetic Interference (EMI), Electromagnetic Compatibility (EMC), self-tests, design assurance and mitigation of other attacks.

FIPS 201 specification includes aspects for the multifunction card utilization in US government identity management systems [61].

1.3.22 Biometric Standards

The importance of biometrics as a part of the secure ID environment is increasing steadily. Some examples of the development include the wider utilization of fingerprint and eye iris scanning for identifying legitimate users. Thus, various current secure ID system implementations rely on biometrics as well as smartcards in order to provide increased levels of security and privacy. The following sections summarize some of the respective standards.

1.3.22.1 ANSI-INCITS 358-2002

ANSI-INCITS 358-2002 contains the BioAPI Specification, equivalent to ISO/IEC 19784-1. The BioAPI defines a generic biometric authentication model that fits to all biometric technologies. Among other definitions, it includes the enrolment, verification and identification, and database interface. The latter offers means for Biometric Service Providers (BSPs) to manage the involved device. The BioAPI framework has been ported to various operating systems.

1.3.22.2 ANSI-INCITS 398

ANSI-INCITS 398 defines the Common Biometric Exchange Formats Framework (CBEFF), which is equivalent to ISO/IEC 19785-1. The CBEFF defines data elements that support biometric technologies and exchange data. It provides interoperability for applications based on biometrics and vendor-independent systems.

1.3.22.3 Other ANSI-INCITS and ISO Standards

The following list summarizes other ANSI-INCITS biometric data format interchange standards that specify the data record interchange format for storing, recording and transmitting biometric sample information within a CBEFF-defined environment [60].

- ANSI-INCITS 377-2004: Finger pattern data interchange format.
- ANSI-INCITS 378-2004: Finger minutiae format for data interchange.
- ANSI-INCITS 379-2004: Iris interchange format.
- ANSI-INCITS 381-2004: Finger image-based data interchange format.
- ANSI-INCITS 385-2004: Face recognition format for data interchange.
- ANSI-INCITS 395-2005: Signature/sign image-based interchange format.
- ANSI-INCITS 396-2004: Hand geometry interchange format.

1.3.22.4 ISO/IEC 19794

ISO/IEC 19794 contains biometric data interchange formats including various parts for, e.g., framework, finger minutiae data, finger pattern spectral data, finger image data, face image data, iris image data, signature/sign time series data, finger pattern skeletal data and vascular image data.

1.3.23 Other Related Entities

The International Civil Aviation Organization (ICAO) provides guidance on the standardization and specifications for Machine Readable Travel Documents (MRTDs) such as passports and visas. ICAO has also published specifications for electronic passports based on contactless smartcards.

MiFare is a technology involving ticketing applications, which has a major part of the total contactless transit ticketing card market. Other variants in this domain include, e.g., Cipurse [69].

The Payment Card Industry (PCI) Security Standards include the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS) and PIN Transaction Security (PTS) [65].

The NFC Forum is an NFC industry association. It promotes specification and use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs [64].

The other documents that are related in one or another way with wireless security include Information Technology Security Evaluation Criteria (ITSEC) security standards [67] which have been largely replaced by the CC, as well as industry initiatives such as MULTOS [66] and the Open Card Framework (OCF) [68].

For the IoT environment, one of the relevant parties is the IoT Security Foundation [82].

1.4 Wireless Security Principles

1.4.1 General

The security and safety in wireless environment do not differ too much from wired set ups. The current smart devices are actually kinds of powerful miniature computers, so basically the executable software may have the very same vulnerabilities that we have seen in the personal computer environment. The official app store concept of testing and preauthorization aims to minimize the potential threats with malicious code hidden in the applications, but as indicated in various instances with all the operating systems, this is not bullet-proof.

As indicated in Ref. [27], typical attacks from outside the networks are not the only issue, there also exist concrete new forms of threats related to consumer devices via embedded

malware. According to this reference, there have been incidents of malware-infected consumer hardware and software products, and even tainted peripheral devices. Some examples of pre-loaded malware environments include products like USB sticks, microchips, cameras, battery chargers, digital photo frames, webcams, printers, cell phones, motherboards, system boards and hard drives.

1.4.2 Regulation

The security assurance for wireless networks as well as for the fixed environment is largely related to the protection of user devices and network elements. Some of the integral tasks of the assurance include the protection of the networks, devices and applications. A systematic and controlled way to execute the protection via security architecture design already in an early phase (standardization, research and prototyping) is highly recommended, as well as in all further phases like network planning, deployment, installation, and configuration. As a useful tool for all this is the security process which applies to the testing, certification and other security phases.

These tasks are done by the involving parties such as device manufacturers and mobile network operators based on the available tools and processes. The operators may and typically will create specific requirements that the equipment manufacturers must comply with. Additional help in this can be provided by the regulation with the respective policies.

One example of the fulfilment of regulatory policies and rules imposed is NERC CIP 5 which refers to CIP V5 Transition Program in the United States. It is designed to protect the bulk power system against cyber-security compromises that without proper protection could lead to misbehaviour or instability. This critical infrastructure protection cyber-security standard set represents the progress in mitigating cyber risks to the bulk power system which, in fact, can be an Achilles' heel for the wireless communication networks as for the remote base station powering.

1.4.3 Security Architectures

There are various wireless systems' security architectures outlined throughout this book. The security can be related to the internal protection mechanisms of the networks such as authentication, authorization and encryption of the communication, as well as the supporting functions such as subscription management which requires secure data transfer in a subscription's profile activation and – as supported by the very latest technologies – more advanced data transfer such as the complete SIM/UICC card OS download in a protected way.

1.4.4 Algorithms and Security Principles

Crypto techniques have improved considerably over time, originating from such ancient methods for hidden writing (steganography) documented by Johannes Trithemius in 1499 (and published in 1606), leading gradually to the most modern methods for actually encrypting the contents. In modern mobile communications, it is logically challenging to apply steganography

even if the basic principle is that the encrypted text is typically easy to spot and hard to make plain, whereas the text hidden by steganography is hard to find but relatively easy to interpret once spotted. If not exactly in the mobile communications, modern steganographic techniques are used, e.g., for manipulating pixels of visual contents such as images by applying very small changes to the values that define the colour of the pixel. As an example, a 24-bit image pixel is based on information on the grade of red, green and blue colours. A small deviation to each pixel value modifies the colour but human eye cannot distinguish the difference from the original. The unscrambling of the contents from such an image requires the original reference image to reveal the additional information hidden in the pixel value altering. These techniques are typically called least significant bit insertions for transporting secret messages.

As for standardized mobile communications systems, the steganographic methods are not practical for the encryption of the communications, but they may be used by end-users on the application level. Instead, the algorithms that are applied to the modern mobile communications environment consist of both non-public and public variants of encryption. In general, it is thought that the publicly exposed algorithms provide the most efficient protection as they have been under the hardest and widest testing, and any possible remaining flaws have been encountered more efficiently simply due to the large size of the test community compared to the very limited resources of non-public variants. As an example, the original GSM A5/1 algorithm for encrypting the radio interface communications was kept confidential, which was thought to protect against attacks, but, at the same time, it limited the number of experts for proofing the adequate security level. This non-public approach may be the reason for the eventual exposure of the weaknesses of the algorithm to attacks, including the easier resolution of the contents by knowing the bit-by-bit form of the encrypted initialization message. Nevertheless, regardless of the public or non-public approach, the security of the algorithms needs to be revised every now and then as code-breaking techniques evolve and computer processing power increases.

The basic categorization of the current algorithms can be divided into symmetric and asymmetric variants. The symmetric approach has been applied in the securing of messages for the last two thousand years or so, including modern mobile communications systems like GSM and UMTS. One example of symmetric encryption is the AES algorithm. The drawback of symmetric encryption is that the same key is used for encrypting and decrypting the message, and thus the key delivery in a secure manner may cause vulnerabilities in this method. Code makers or code breakers have been, one at the time, leading the advances in this era.

The asymmetric approach refers to the security system that uses different keys for encrypting and decrypting the messages. One example of asymmetric ciphering techniques is RSA. In practice, the current asymmetric encoding solutions rely on the modular functions that are based on prime numbers and a pair of public and private keys [2]. The mathematical principles of prime numbers provide the possibility to make the encryption in such a way that the reverse analysis for finding the used prime numbers and for eavesdropping is not feasible in practice for sufficiently big numbers, whereas the legitimate receiving party can decrypt the message by knowing the pair of his/her own public key (which the sending party utilized as a part of the encryption) and own private key (which others are not aware of). Thus, once the sending party encrypts the message, they cannot decrypt it any more as it only opens in a feasible manner with the private key paired with the public key.

Table 1.7 lists and compares some of the most relevant ciphering techniques used in mobile and wireless communications today.

Table 1.7 Comparison of ciphering techniques relevant for mobile communications

Algorithm	Principle	Examples
AES	Block cipher, with block size of 128 bits and key length of 128, 192 and 256 bits. Symmetric algorithm. Includes key addition, byte substitution and diffusion layers	Provides efficient SW implementation. Well suited for 8-bit processors such as smartcards, but not efficient on 32- or 64-bit machines. Optimized via look-up tables (T-Box). AES forms part of numerous open standards like IPSec and TLS, and is a mandatory encryption algorithm for US government applications. More information: [83,84]
DES	Block cipher encrypting blocks of 64 bits with a key of 56 bits. Symmetric cipher (same key for encryption and decryption). Iterative algorithm with 16 rounds and respective sub-keys derived from main key	Very efficient in HW such as Field Programmable Gate Array (FPGA) and Application-Specific Integrated Circuit (ASIC). Suitable in very small devices with reduced space, such as RFID tags and low-cost smartcards (high-volume public transportation payment tickets). Vulnerable to differential and linear crypto-analysis attacks excluding the S-box. More information: Ref. [88]
Triple-DES (3DES)	Symmetric cipher and alternative to DES, consisting of three subsequent DES encryptions with three different keys, respectively	Resistant to brute-force attacks and analytical attacks. The advantage of 3DES is the single DES encryption if the keys are the same which benefits the support of legacy systems
RSA	Asymmetric cipher. Encryption and decryption based on integer ring and modular computations of bit strings via public and private keys	Most widely used asymmetric cryptographic scheme. Typically used for small pieces of data such as key transport, and digital signatures, e.g., for digital certificates on the Internet. Much slower than AES so RSA does not replace symmetric ciphers such as AES
Elliptic curve/ discrete logarithm schemes	Elliptic curves are used, e.g., for encryption, digital signatures and pseudo-random generators	Elliptic curve is one of the latest additions for mobile communications security solutions. More information can be found in Ref. [85], and information about related Brainpool can be found in Ref. [86]
Hash functions	Hash functions compute a digest of a message which is a short, fixed-length bit string. Does not have a key.	Hash function can be used as a fingerprint of the message and is thus suitable for digital signature schemes and message authentication. Can be used for storing password hashes or key derivation [87]
MILENAGE	A new algorithm taken into use in mobile communications, as defined in 3GPP TS 35.205, TS 35.206, TS 35.207, TS 35.208 3G security specifications	3GPP TR 35.909, Release 11 presents an example algorithm set for 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*, including algorithm specification, implementers' test data, design conformance test data as well as results of the design and evaluation
TUAK	A new algorithm as described in 3GPP TS 35.231, TS 35.232 and TS 35.233 (Release 12).	The specifications include the algorithm description, implementers' test data and design conformance test data

More background information about crypto techniques in general and in the mobile communications environment can be found, e.g., in references [2,20–23,27,71,72].

1.5 Focus and Contents of the Book

This book summarizes key aspects of the wireless security field, and is aimed to be especially useful for network operators and mobile/IoT device manufacturers, as well as for companies and organizations that are involved in mobile communications security like smartcard providers, embedded security element and 'traditional' SIM card manufacturers, and service providers. This book also clarifies the most important current and future solutions in a practical way for telecommunications students in order to map the theories with industry trends. The primary audience of the book is the wireless security industry, but the book has been aimed at all other interested parties, including personnel of regulators, the gaming industry, defence forces and the academic environment, to explain the overall picture of recent and expected future security solutions.

This book also aims to work as a useful guideline for personnel involved with standardization groups and alliances like the GlobalPlatform, GSMA, SIMalliance, MiFare, Cipurse, 3GPP, 3GPP2 and ETSI.

The first two chapters of the book form the **introductory module** containing a description of the wireless security environment and IoT. They describe the essential basics of the mobile and wireless systems relevant for understanding security aspects such as user authentication, authorization and securing the radio interface, as well as the focus and role of standardization bodies, the development of systems for consumers as well as M2M communications. The most important security algorithms are presented, with further references to the specialized literature for those wanting to study the principles in more detail.

The **second module** presents detailed secure solutions in the wireless environment, including contact and contactless smartcards, secure elements and evolved systems that are useful for securing communications apart from the hardware-based solutions such as cloud payment. Also the current and expected development of subscription management is described based on the most updated information from the involving standardization bodies and industry forums. The second module outlines the overall development of IoT with respective waves of the M2M solutions and mobile connectivity, and discusses the connected society concept as well as other industry forums, alliance and international standard body initiations. Novelty and expected future solutions are discussed, including wearable devices, household appliances, industry solutions and self-driving cars. One of the vast IoT device bases is related to utilities, so the contributing role and technologies of them are discussed with the ways utilities are relying on wireless technologies, including their role in the electric domain, mobility and smart grid applications.

An important part of module 2 is dedicated to smartcards, so reasons are presented on why smartcards are still a useful anchor for security in the era of the IoT. Along with the development of smartcard technologies and parallel solutions, this module also discusses the modifications needed for smartcards to support the IoT, and presents available

or future alternatives. Technical descriptions of contact cards and contactless cards are given, including standards, current solutions, form factors, electrical and mechanical characteristics, use cases for, e.g., wireless payment and access systems, NFC and other wireless techniques. The payment and access environment is described by giving examples such as the EMVCo concept and other banking systems, e-commerce, transport and access systems.

The second module also describes wireless security platforms and functionality by presenting justifications of why each specific security mechanism is relevant. The secure element of both HW and SW-based solutions is described, and secure protocols are also discussed. Based on smartcard principles, this module also details the telecoms environment's SIM/UICC card and embedded SIM/UICC. The SIM-based Over-the-Air (OTA) techniques are presented for initiation of the subscription, subscription life-time management, as well as remote file management and application management. This leads to a more complete environment of subscription management for consumer subscriptions and M2M devices, which is detailed based on the latest knowledge from the industry and standardization fields.

Furthermore, alternative secure solutions for SIM are described, like TEE, cloud and Host Card Emulation (HCE), including the functionality of tokenization. Life-cycle management is also outlined, and the benefits and challenges of subscription management are discussed. The evolution of device types and costs for selection of techno-economically optimal subscription management are also considered, along with potential issues and their solutions for subscription management.

The **third module** details typical security threats in the wireless environment, and explains how to monitor and enhance protection against malicious attacks. This module also outlines future aspects of mobile security. More specifically, this module presents concerns of wireless security mechanisms, potential security holes including the role of human errors and flaws in the network, user equipment, applications, communications, signalling and production. Some attack types are discussed such as eavesdropping, overloading and RF-attacks. Along with the increasing importance of the IoT environment, module 3 outlines impacts of wireless security on the utilities domains and applications. Feasible protection techniques are thus discussed as well as monitoring techniques such as deep packet inspection, virus protection and legal interception.

The future section of the third module discusses the forthcoming wireless environment by summarizing trends, threats and solutions for the security mechanisms in order to avoid performance degradation of wireless technologies along with extensive data transmission. There is also a description of the evolution of sensors networks and their security. Finally, the third module introduces mobile communications systems of 5G and beyond, which is still a set of items under preparation for standardization, as well as the security challenges of future wireless technologies.

Figure 1.1 presents the main level contents of this book to ease the navigation between the modules. The modules and chapters are independent from each other so they can be read through in any preferred order. Nevertheless, for studying the area from scratch, it is recommended to get familiar with the topic gradually in the presented order as this makes it easier to understand the later contents.

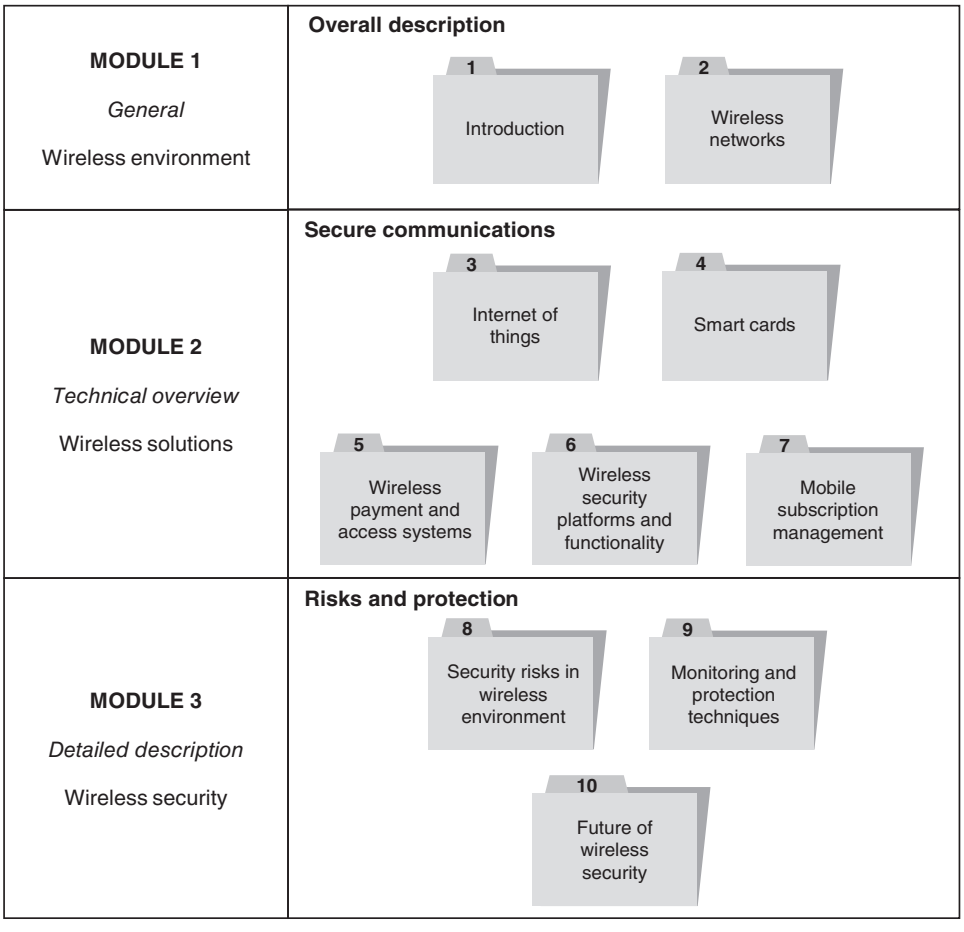

Figure 1.1 The contents of this handbook

References

[1] *Wired*. Hacker spoofs cell phone tower to intercept calls, October 2010. http://www.wired.com/2010/07/intercepting-cell-phone-calls/ (accessed 13 December 2014).
[2] Simon Singh. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. Anchor Books, New York, 1999.
[3] ITU, 2015. http://www.itu.int/en/about/Pages/overview.aspx (accessed 4 July 2015).
[4] ITU-T Recommendations, 2015. http://www.itu.int/rec/T-REC/e (accessed 4 July 2014).
[5] ITU-R Recommendations, 2015. http://www.itu.int/pub/R-REC (accessed 4 July 2014).
[6] IEEE Publications, 2015. http://www.ieee.org/publications_standards/index.html (accessed 4 July 2015).
[7] IEEE Standards, 2015. http://standards.ieee.org/about/get/index.html (accessed 4 July 2015).
[8] IEEE Standards Association. IEEE standards activities in the network and information security (NIS) space. 19 June 2013. 4 p.
[9] IETF RFC search page, 2015. http://www.rfc-editor.org/rfcsearch.html (accessed 4 July 2015).
[10] IETDF, Official Internet Protocol Standards, 2015. http://www.rfc-editor.org/rfcxx00.html (accessed 4 July 2015).
[11] IETF RFC 1677. *The Tao of IETF – A Novice's Guide to the Internet Engineering Task Force*, 2015.

[12] IETF RFC List, 2015. http://www.ietf.org/rfc.html (accessed 4 July 2015).
[13] IETF Security Area, 2015. https://tools.ietf.org/area/sec/trac/wiki (accessed 4 July 2015).
[14] CEPT, 2015. http://www.cept.org (accessed 4 July 2014).
[15] ANSI, 2015. http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1 (accessed 4 July 2014).
[16] ANSI Standards (Restricted Area), 2015. http://www.ansi.org/library/overview.aspx?menuid=11 (accessed 4 July 2014).
[17] TTC, 2015. http://www.ttc.org.jp/cgi/summarydb/index.html (accessed 4 July 2015).
[18] 3GPP, 2015. www.3gpp.org (accessed 4 July 2015).
[19] 3GPP, Security Aspect, 30 May 2011. ftp://www.3gpp.org/Information/presentations/presentations_2011/2011_05_Bangalore/DZBangalore290511.pdf (accessed 4 July 2015).
[20] Anand R. Prasad. 3GPP SAE/LTE Security. NIKSUN WWSMC, 26 July 2011.
[21] Bogdan Botezatu. 25 percent of wireless networks are highly vulnerable to hacking attacks, Wi-Fi security survey reveals, 11 October 2011. http://www.hotforsecurity.com/blog/25-percent-of-wireless-networks-are-highly-vulnerable-to-hacking-attacks-wi-fi-security-survey-reveals-1174.html (accessed 4 July 2015).
[22] Michael Walker, chairman of 3GPP SA3 WG (Security). On the security of 3GPP networks. Eurocrypt 2000.
[23] CTIA, Mobile Cybersecurity and the Internet of Things; Empowering M2M Communication.
[24] Executive Order 13636 Improving Critical Infrastructure Cybersecurity, 12 February 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructurecybersecurity (accessed 6 July 2015).
[25] National Highway Traffic Safety Administration, Preliminary Statement of Policy Concerning Automated Vehicles, 30 May 2013. http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (accessed 6 July 2015).
[26] 2015 Data Breach Investigations Report. Verizon, 2015.
[27] S. Bosworth, M.E. Kabay and E. Whyne. *Computer Security Handbook*. Sixth edition, Volume 1. John Wiley & Sons, Inc., Hoboken, NJ, 2014.
[28] Open Mobile Alliance, 12 October 2015. http://openmobilealliance.org/ (accessed 12 October 2015).
[29] OMA Work Programs, 12 October 2015. http://openmobilealliance.org/about-oma/work-program/device-management/ (accessed 12 October 2015).
[30] OMA DM Development, 29 February 2012. http://technical.openmobilealliance.org/comms/documents/OMA_DM_1.4Billion_PR_Final.pdf (accessed 12 October 2015).
[31] OMA Releases, 12 October 2015. http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/gssm-v1-0 (accessed 12 October 2015).
[32] CoAP. IETF RFC 7252, June 2014. https://tools.ietf.org/html/rfc7252 (accessed 13 October 2015).
[33] DTLS version 1.2. IETF RFC 6347, January 2012. https://tools.ietf.org/html/rfc6347 (accessed 13 October 2015).
[34] Infineon, IoT overview, 1 November 2015. http://www.infineon.com/iot-security-ebrochure/en/index.html (accessed 1 November 2015).
[35] Open Mobile Alliance Release Program document package, 1 November 2015. http://technical.openmobilealliance.org/Technical/Release_Program/docs/GSSM/V1_0-20111220-A/OMA-ERP-GSSM-V1_0-20111220-A.zip (accessed 1 November 2015).
[36] The green life of a SIM card. Giesecke & Devrient, Smart! Telecommunications, 2/2009.
[37] ISO/IEC 7816-1:2011. Identification cards; Integrated circuit cards, Part 1: Cards with contacts; Physical characteristics. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54089 (accessed 1 November 2015).
[38] ISO/IEC 7816-2:2007. Identification cards; Integrated circuit cards, Part 2: Cards with contacts; Dimensions and location of the contacts. www.iso.org (accessed 30 December 2015).
[39] ISO/IEC 7816-3:2006. Identification cards; Integrated circuit cards, Part 3: Cards with contacts; Electrical interface and transmission protocols. www.iso.org (accessed 30 December 2015).
[40] ISO/IEC 7816-4:2013. Identification cards; Integrated circuit cards, Part 4: Organization, security and commands for interchange. www.iso.org (accessed 30 December 2015).
[41] ISO/IEC 7816-5:2004. Identification cards; Integrated circuit cards, Part 5: Registration of application providers. www.iso.org (accessed 30 December 2015).
[42] ISO/IEC 7816-6:2004. Identification cards; Integrated circuit cards, Part 6: Interindustry data elements for interchange. www.iso.org (accessed 30 December 2015).
[43] ISO/IEC 7816-7:1999. Identification cards; Integrated circuit(s) cards with contacts, Part 7: Interindustry commands for Structured Card Query Language (SCQL). www.iso.org (accessed 30 December 2015).

[44] ISO/IEC 7816-8:2004. Identification cards; Integrated circuit cards, Part 8: Commands for security operations. www.iso.org (accessed 30 December 2015).
[45] ISO/IEC 7816-9:2004. Identification cards; Integrated circuit cards, Part 9: Commands for card management. www.iso.org (accessed 30 December 2015).
[46] ISO/IEC 7816-10:1999. Identification cards; Integrated circuit(s) cards with contacts, Part 10: Electronic signals and answer to reset for synchronous cards. www.iso.org (accessed 30 December 2015).
[47] ISO/IEC 7816-11:2004. Identification cards; Integrated circuit cards, Part 11: Personal verification through biometric methods. www.iso.org (accessed 30 December 2015).
[48] ISO/IEC 7816-12:2005. Identification cards; Integrated circuit cards, Part 12: Cards with contacts; USB electrical interface and operating procedures. www.iso.org (accessed 30 December 2015).
[49] ISO/IEC 7816-13:2007. Identification cards; Integrated circuit cards, Part 13: Commands for application management in a multi-application environment. www.iso.org (accessed 30 December 2015).
[50] ISO/IEC 7816-15:2004. Identification cards; Integrated circuit cards, Part 15: Cryptographic information application. www.iso.org (accessed 30 December 2015).
[51] ISO/IEC 7816-15:2004/Cor 1:2004. www.iso.org (accessed 30 December 2015).
[52] ISO/IEC 7816-15:2004/Amd 1:2007. Examples of the use of the cryptographic information application. www.iso.org (accessed 30 December 2015).
[53] ISO/IEC 7816-15:2004/Amd 2:2008. Error corrections and extensions for multi-application environments. www.iso.org (accessed 30 December 2015).
[54] ISO/IEC Standards Summary, 1 November 2015. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_ics_browse.htm?ICS1=35&ICS2=240&ICS3=15& (accessed 1 November 2015).
[55] GlobalPlatform, 1 November 2015. https://www.globalplatform.org/ (accessed 1 November 2015).
[56] SIMalliance, 1 November 2015. http://simalliance.org/ (accessed 1 November 2015).
[57] GSMA, 1 November 2015. http://www.gsma.com/aboutus/ (accessed 1 November 2015).
[58] GSMA history, 9 November 2015. http://www.gsma.com/aboutus/history (accessed 9 November 2015).
[59] Common Criteria, 9 November 2015. http://www.commoncriteriaportal.org/ (accessed 9 November 2015).
[60] Robert Yen. Overview of ANSI-INCITS biometric standards on data interchange format. Biometrics, U.S. Department of Defense, 19 January, 2005.
[61] Federal Information Processing Standards (FIPS), 11 November 2015. https://csrc.nist.gov (accessed 11 November 2015).
[62] European Telecommunications Standards Institute, 11 November 2015. http://www.etsi.org/ (accessed 11 November 2015).
[63] EMVCo, 11 November 2015. http://www.emvco.com/ (accessed 11 November 2015).
[64] NFC Forum, 11 November 2015. http://www.nfc-forum.org (accessed 11 November 2015).
[65] PCI Security Standards, 11 November 2015. https://www.pcisecuritystandards.org (accessed 11 November 2015).
[66] MULTOS, 11 November 2015. https://www.multos.com/ (accessed 11 November 2015).
[67] Information Technology Security Evaluation Criteria (ITSEC). Department of Trade and Industry, London, June 1991.
[68] The Open Card Framework, 11 November 2015. http://www.openscdp.org/ocf/ (accessed 11 November 2015).
[69] CIPURSE V2. Integrating CIPURSE V2 into an existing Automated Fare Collection system. OSPT Alliance, 2014.
[70] GSMA, The Mobile Economy Report 2015.
[71] Crypto tutorial. https://www.cs.auckland.ac.nz/~pgut001/tutorial/ (accessed 11 November 2015).
[72] SSL encryption evaluation. http://www.peerlyst.com/blog-post/a-technical-rant-about-the-different-e-s-in-ssl-tls (accessed 11 November 2015).
[73] Smartcard Alliance, 22 November 2015. http://www.smartcardalliance.org/alliance/ (accessed 22 November 2015).
[74] *Wired*. Siri hack, October 2015. http://www.wired.com/2015/10/this-radio-trick-silently-hacks-siri-from-16-feet-away/?mbid=social_twitter (accessed 22 November 2015).
[75] *Interference Technology*. OTA hacking device. http://www.interferencetechnology.com/unstoppable-new-hacking-device-steals-encryption-keys-out-of-the-air/ (accessed 22 November 2015).
[76] *Helsingin sanomat*. Baby monitoring device security threats, 7 September 2015. www.hs.fi/m/kotimaa/a1441508730024?ref=hs-mob-prio45-1 (accessed 22 November 2015).
[77] *Helsingin sanomat*. Home device security holes, 7 August 2015. http://www.hs.fi/m/ulkomaat/a1438918533873 (accessed 22 November 2015).
[78] BBC. Security breach lab, 20 July 2015. http://www.bbc.com/future/story/20150720-the-hidden-lab-where-bankcards-are-hacked (accessed 22 November 2015).

[79] *Helsingin sanomat*. Remote access breaches. http://www.hs.fi/m/kotimaa/a1435630410758 (accessed 22 November 2015).
[80] *Helsingin sanomat*. Security breach revealed by under aged. http://www.hs.fi/m/autot/a1425284972822 (accessed 22 November 2015).
[81] BBC. Rail signal upgrade could be hacked to cause crashes. http://m.bbc.com/news/technology-32402481 (accessed 22 November 2015).
[82] IoT Security Foundation. https://iotsecurityfoundation.org/ (accessed 22 November 2015).
[83] J. Daemen and V. Rijmen. *The design of Rijndael*. Springer, 2002.
[84] J. Daemen and V. Rijmen. AES proposal: Rijndael. First Advanced Encryption Standard (AES) Conference, Ventura, CA, USA, 1998.
[85] I. F. Blake, G. Seroussi and N. P. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press, New York, 1999.
[86] ECC Brainpool. ECC Brainpool Standard Curves and Curve Generation. 2005. http://www.ecc-brainpool.org/ecc-standard.htm (accessed 12 December 2015).
[87] J. L. Carter and M. N. Wegman. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–277, 1981.
[88] W. Diffie and M. E. Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard. *COMPUTER*, 10(6):74–84, 1977.
[89] 3GPP2 introduction, 2 January 2016. http://www.3gpp2.org/Public_html/Misc/AboutHome.cfm (accessed 2 January 2015).
[90] ISO 27000 Information Security Management. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (accessed 9 January 2016).
[91] ISO/IEC JTC1/SC17 Standing Document 3 – SC17 Work Programme including all published standards and target date summary for all work items under development, 23 August 2006. http://wg8.de/wg8n1255_17n3074_SC17_SD3_Work_Programme.pdf (accessed 10 January 2016).
[92] OMA. A Primer to SyncML/OMA DS. Approved 31 Mar 2008. 27 p. http://technical.openmobilealliance.org/Technical/release_program/docs/SyncML_Primer/V1_0-20080331-A/OMA-WP-SyncML_Primer-20080331-A.pdf (accessed 10 January 2016).
[93] 3GPP TR 31.828 V10.0.0 (2011-04). UICC access to IMS (Release 10). 25 p.