International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4807

(01/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Identification and security

Agility by design for telecommunication/ICT systems security used in the Internet of things

Recommendation ITU-T Y.4807

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	**Y.4800–Y.4899**
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4807

Agility by design for telecommunication/ICT systems security used in the Internet of things

Summary

Recommendation ITU-T Y.4807 addresses possible improvement of security and stability of the Internet of things by ensuring the supporting telecommunication/information and communication technology (ICT) systems and related infrastructure – protocols, standards, etc. – have the flexibility to keep up with advances in telecommunication/ICT security and cryptography. This Recommendation intentionally does not provide guidance on specific cryptosystems, standards or algorithms.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4807	2020-01-13	20	11.1002/1000/14172

Keywords

Cryptosystems, Internet of things, IoT, security.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.4807

Agility by design for telecommunication/ICT Systems Security used in the Internet of Things

1 Scope

This Recommendation is targeted at the telecommunication/ICT systems and supporting infrastructure which support Internet of things (IoT) devices. Both must have the flexibility to keep up with changes in the rapidly moving field of cybersecurity so that they can cope with new security threats and challenges as they emerge. The guidelines described in this Recommendation include, but are not necessarily limited to:

– quantifying risk for an IoT system;

– deployment of updated security protocols and standards;

– adoption of appropriate cryptographic algorithms;

– adoption of relevant authentication systems.

This also applies to the removal of these components when they have been deprecated or their use is no longer advised. The Recommendation intentionally does not provide guidance on specific risk analysis methodologies, cryptosystems, standards or algorithms.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

3.1.1 botnet [b-ITU-T X.1213]: Remotely controlled malicious software robots (bots) that are run autonomously or automatically on compromised computers.

3.1.2 cryptosystem [b-ISO 11568-1]: Set of cryptographic primitives used to provide information security services.

3.1.3 DDoS [b-ISO/IEC 27039]: Distributed denial of service attack - unauthorized access to a system resource or the delaying of system operations and functions in the way of compromising multiple systems to flood the bandwidth or resources of the targeted system, with resultant loss of availability to authorized users.

3.1.4 device [b-ITU-T Y.4000]: A piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.5 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

3.1.6 trust anchor [b-ITU-T X.509]: An entity that is trusted by a relying party and used for validating public-key certificates.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
ICT	Information and Communication Technologies
IoT	Internet of Things
PKI	Public Key Infrastructure
RSP	Remote SIM Provisioning
SDLC	System Development Lifecycle
SHA	Secure Hash Algorithm
TLS	Transport Layer Security

5 Conventions

In this Recommendation:

The keyword "should" indicates a requirement that is recommended but which is not absolutely necessary. Thus, this requirement needs not to be present to claim conformance.

6 ICT security challenges and impact on IoT

Security for telecommunication/ICT systems in general is a challenge and a continually moving target. New threats and vulnerabilities emerge often. New forms of attack emerge too, notably distributed denial of service (DDoS) attacks. In recent years, DDoS attacks have exploited weaknesses in IoT devices. For instance, one element used in the 2016 Mirai attack was a botnet containing hundreds of thousands of webcams and digital video recorders. It is therefore important that IoT devices and the telecommunication/ICT systems should be robust and secure to both minimize exposure to these sorts of attacks and reduce their impact.

There are many telecommunication/ICT systems and technologies which have a role to play to defend against these problems. Those Telecommunication/ICT systems will need to be continually assessed and updated to adapt to both the new security threats when they emerge and also to accommodate technical advances such as updated standards or new protocols. Many of those security defences rely on cryptography which is itself a rapidly moving field. Put simply, deployed cryptosystems and algorithms that are considered "safe" today might be considered less "safe" tomorrow or could even become obsolete. However, protocols and standards are continuously being updated. Examples are provided in Appendix I, noting that these examples do not represent a definitive or exhaustive list of telecommunication/ICT systems that have algorithm agility capabilities.

The telecommunication/ICT systems supporting the IoT need to take account of these sorts of developments and have the flexibility to handle them properly. They should be able to cope with changes in technology, updated protocol standards and advances in cryptography.

In addition, these systems will typically have a much longer lifetime than the IoT devices they are expected to support. For instance, a building's intelligent lighting system will generally outlast the smart lightbulbs it uses. When these lightbulbs fail, they could be replaced by newer devices that make use of more recent cryptosystems and protocol standards that offer better security properties and/or improved performance. If properly designed, the building's lighting system should have the flexibility to be able to accommodate these sorts of changes.

7 Secure design considerations

With many IoT solution providers in a race to market, many design and operational decisions are made that have a direct impact to the overall security and risk posture of the solution. As a result, the products are prone to attack and compromise in-field as indicated in the previous clause.

Developers and solution and service providers should have a system development lifecycle (SDLC) that considers the overall risk of a solution prior to initial deployment. This SDLC should contain:

a. Threat Modelling – This includes profiling the attack surface of the solution to determine the possible components that will have either network visibility or can be exploited for unauthorized usage. This may include: authentication, encryption, third-party libraries, chipsets, cloud hosting and related components, and logging.

b. Threat and risk assessment – While there are several approaches to this, those designing and deploying IoT solutions should use a methodology that best aligns to the organizational goals and objectives. Each party should perform this exercise of formally evaluating security and privacy risks of the solution. This will consider the data, components, services, application programming interfaces (APIs), thirs-party libraries, etc. The scope cannot be restricted, but should include all components of the solution.

c. Testing and validation – Organizations developing and deploying IoT solutions should have a formal testing and validation process to ensure that security and privacy risks that were identified in either a threat modelling or a threat and risk assessment are being mitigated in current software and deployment systems. These test cases and outputs should be retained because they are likely to be needed for regression testing, audits and documentation.

d. Operational awareness – Organizations developing and deploying IoT solutions should have effective processes to allow for the real-time monitoring of systems and devices that are deployed and determine aspects of the solution that might be under active attack. This will include procedures for incident handling for identification, containment and mitigation of these attacks. This may also include in-field updating of software to mitigate these attacks.

Figure 1 indicates that this is an ongoing process to support product risk identification and mitigation. Organization maturity, prevailing local circumstances and regulations will drive how each of these aspects will be implemented.

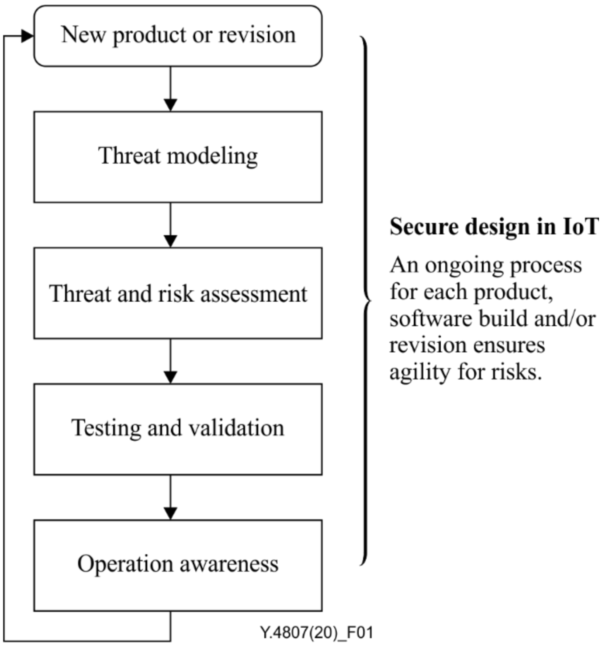
New product or revision
Threat modeling
Threat and risk assessment
Testing and validation
Operation awareness
Secure design in IoT
An ongoing process for each product, software build and/or revision ensures agility for risks.
Y.4807(20)_F01

Figure 1 – System development lifecycle

8 Agility by design

Designers and developers of telecommunication/ICT systems for IoT should ensure that these are designed from the outset to support the concept of agility such as the capacity to introduce new cryptographic algorithms and protocols when these emerge and to withdraw those that are no longer to be used. These systems should not be designed in a way that limits them to use a specific technology because that presents a potentially catastrophic single point of failure.

The examples in Appendix I illustrate how some widely used protocol standards and specifications have taken account of these design decisions and exploited their capabilities in algorithm agility when they have been used. These examples have generally followed the system development life cycle outlined in clause 7. Threat modelling was followed by threat and risk assessments that resulted in the addition or removal of cryptographic algorithms. Testing and validation lead to deployment. Monitoring then provided operational awareness that could be incorporated into further refinement of the protocols used by telecommunication/ICT systems, taking account of operational experience.

Protocol and standards development and deployment is not static. They should be treated as continuous and on-going processes that adapt to changes in technology and new security threats/risks.

9 Conclusion

To provide stability and security, the telecommunication/ICT systems used for the IoT should therefore provide algorithm agility, that is, the ability to add support for new cryptographic algorithms and protocols and also be able to remove support for those that have been obsoleted or are considered no longer satisfactory.

For some IoT environments, the frameworks offered by the most recent versions of the relevant protocols should offer a satisfactory capability for algorithm agility provided they are used appropriately. However, they might be impractical in other settings for reasons such as cost or hardware limitations. For these settings, the guidance provided in this Recommendation can be applied by those designing and deploying software for IoT devices so that the resulting telecommunication/ICT systems are able to support algorithm agility.

It should be noted that this Recommendation intentionally does not provide any advice about which crypto systems, protocols and algorithms should or should not be used. That is primarily a matter for those deploying and operating the telecommunication/ICT systems for the IoT. They are better placed to decide which security solutions are best suited to the prevailing local requirements.

Appendix I

Example telecommunication/ICT systems that utilize algorithm agility

(This appendix does not form an integral part of this Recommendation.)

The following examples are provided solely for illustrative purposes. They do not represent a definitive or exhaustive list of telecommunication/ICT systems that have algorithm agility capabilities. There are other cryptosystems and infrastructure for the IoT that have these attributes. In addition, other systems that have these attributes for the IoT applications could be based on unique persistent identifiers.

1) ITU-T X.509 certificates

Recommendation [b-ITU-T X.509] makes extensive use of cryptographic algorithms, such as hashing algorithms, public-key algorithms and digital signature algorithms. The format for ITU-T X.509 certificates contains an AlgorithmIdentifier element that indicates the cryptographic algorithm or algorithms that were used to generate a certificate. When a certificate gets presented to a third party (for instance a web browser), its AlgorithmIdentifier element tells that third party which cryptographic algorithms to apply in order to validate or authenticate that certificate. Incorporating this AlgorithmIdentifier element in [ITU-T X.509] means that ITU-T X.509 certificates have the inherent flexibility to support arbitrary cryptographic algorithms. This agility capability is exploited in the following two environments which are underpinned by ITU-T X.509 certificates.

SET, the Secure Electronic Transaction Specification [b-SET], is a protocol that was developed by a consortium of credit card companies to secure payment card transactions over the Internet. The specification includes guidance on operational matters such as maximum lifetimes for certificates and keys, key lengths, etc. Although SET defines a default set of cryptographic algorithms that are mandatory for payment gateway systems to implement, the specification allows for algorithms to be added or deprecated when necessary. SET was designed to be algorithm independent. It is possible to introduce additional algorithms while remaining backward compatibility with the installed base of SET-compliant infrastructure. The design of [ITU-T X.509] made that possible.

The Certification Authority Browser Forum (CABF), also known as CA/Browser Forum, is a consortium of Certificate Authorities, operating system vendors, organizations producing Internet browser software and other PKI-enabled applications. It provides Internet security industry standards for web browsers and Certificate Authorities, publishing baseline requirements for the issuance and management of publicly trusted ITU-T X.509 certificates [b-CABF]. Like the SET specification, these CABF requirements includes guidance on operational matters such as maximum lifetimes for certificates and keys, key lengths and so on. Those requirements also define the cryptographic algorithms that are used in CABF-approved signatures and these in turn depend on the AlgorithmIdentifier element defined in [ITU-T X.509]. From time to time the CABF updates these requirements whenever it becomes necessary to add or deprecate cryptographic algorithms. For instance, the CABF announced in 2014 that signatures based on SHA-1 were to be phased out because the algorithm was considered vulnerable, and Certificate Authorities could not issue SHA-1 based certificates after 1 January 2016. This widely adopted example of algorithm agility has been enabled by the ITU-T X.509 design.

2) Transport layer security (TLS)

TLS, the Transaction Layer Security protocol, provides a secure channel between two communicating peers that can be used for authentication, confidentiality and message integrity. It has two main components, a handshake protocol and a record protocol [b-IETF RFC 8446]. The handshake protocol authenticates the communicating parties, negotiates cryptographic modes and parameters, and establishes shared keying material. The record protocol handles traffic encryption once the TLS session has been established. TLS is most commonly used to secure communications between web browsers and servers.

The TLS protocol is designed to be technology neutral and to be capable of supporting whatever cryptosystems and algorithms that communicating peers might choose to use. It offers a variety of different methods for exchanging keys, encrypting traffic and authenticating message integrity.

TLS makes use of a registry that issues code points for secure hash function and cryptographic algorithms. When a TLS session is initiated, these code points are exchanged between the two peers, so that they are aware of each other's cryptographic capabilities. In simple terms, the handshake protocol then signals which cryptographic algorithm or algorithms will be most mutually convenient for the TLS session that is about to be established.

This registry contains code points for a large number of commonly used public key and block/stream cryptosystems and secure hash algorithms. Some entries in the TLS registry are listed as not recommended, largely because they are considered vulnerable or insecure. New code points get added to this registry whenever new cryptosystems become available. Code points have also been set aside for private use or experiments so that these do not cause interoperability problems by conflicting with the installed base.

TLS demonstrates algorithm agility by providing a framework where arbitrary cryptosystems can be added or removed from this registry. Local policy or software configuration determines which of these cryptosystems actually gets used for a TLS session.

3) GSMA remote SIM provisioning architecture

Algorithm agility is inherent to the GSMA remote SIM provisioning (RSP) architecture [b-GSMA]. This architecture specification is based on a public key infrastructure using ITU-T X.509 certificates. It also makes use of the TLS protocol. The specification defines the encryption and secure hash algorithms for authenticating SIM cards used by mobile phones and similar hand-held devices used on mobile telephone networks. Devices are required to support specific signature algorithms offered by TLS. At present, this includes three distinct elliptic curve algorithms. Leveraging ITU-T X.509 certificates and TLS allows RSP to accommodate the introduction of new algorithms and trust anchors and deprecate old ones as and when the need arises.

4) Secure domain name system (DNS)

The DNS Security Extensions (DNSSEC) protocol primarily documented in [b-IETF RFC 4033] and [b-IETF RFC 5155] uses a combination of secure hash algorithms and public-key cryptography so DNS data can be validated. When work began on the DNSSEC protocol, the designers recognized that the algorithms available at that time would eventually get replaced or superseded and made sure the specifications took account of that concern. The DNSSEC protocol uses a registry that issues code points for secure hash function and cryptographic algorithms. These code points are included in the signed DNS data so that validators can tell which algorithms were used to generate the signature and therefore select the appropriate algorithms to validate that signature. The DNSSEC protocol was therefore developed in a way that allowed for the introduction of new algorithms and the withdrawal of old (unwanted) algorithms. The protocol also makes provision for private use algorithms, offering the potential for experiments and testing that would not interfere with the installed base of systems that perform DNSSEC validation.

5) RIPE Atlas

RIPE Atlas [b-ATLAS] is essentially a large IoT system for measuring Internet connectivity and reachability. It includes a global network of thousands of probes: small devices running custom firmware that check the availability and round-trip times to key Internet resources such as important DNS and web servers. Supporting infrastructure for RIPE Atlas includes systems for logging and analysing data returned from the probes, distributing firmware and managing the probe network.

The firmware in these probes gets updated from time to time and for the obvious security reasons these updates have to be cryptographically signed. Firmware updates include details of the algorithms and keys that were used to create their signatures so the probes can select the relevant keys and algorithms to use for verification and authentication.

Algorithm agility is inherent to the design of this firmware. Sometimes new algorithms and keys have to be introduced and old ones get discontinued or removed. This means the management systems need to track which algorithms are currently supported by specific probes and arrange for their firmware to be updated when necessary. In addition, good cryptographic practice requires that the keys (trust anchors) used for verifying signatures on firmware updates have to be changed from time to time. That might also entail replacing one form of public-key encryption or secure hash algorithm with another.

The RIPE Atlas firmware and its supporting infrastructure was designed from the outset to have that flexibility. The entire probe network can cope with multiple encryption and secure hash algorithms and adapt to changes whenever new cryptosystems need to be introduced or old ones get retired.

6) [ITU-T Y.4805] requirements

Many IoT applications require an identifier service that can provide access control over attributes associated with the identifier for IoT device, as well as administrative capabilities to update and manage identifier attributes securely and dynamically to reflect changes of the state information of IoT device. Implementations of identifier service that satisfies requirements stated in [b-ITU-T Y.4805] typically provides all these operational features, as well as the agility that allows new and future security algorithms and/or implementations being deployed. Security algorithms and authentication methods used in protocol exchange are typically registered and identified as a global unique identifier. Associated with the identifier are detailed information about the security mechanism and its implementation. New and future security mechanisms can thus be integrated with the identifier service by registering new identifiers that designate their deployment.

Bibliography

[b-ITU-T X.1213] Recommendation ITU-T X.1213 (2017), *Security capability requirements for countering smartphone-based botnets*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[b-ITU-T Y.2253] Recommendation ITU-T Y.2253 (2014), *Capabilities of multi-connection to support streaming services*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4805] Recommendation ITU-T Y.4805 (2017). *Identifier Service Requirements for the Interoperability of Smart City Applications.*

[b-ISO 11568-1] ISO 11568-1:2005, *Banking – Key management (retail) – Part 1: Principles*.

[b-ISO/IEC 27039] *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS).*

[b-IETF RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.

[b-IETF RFC 5155] IETF RFC 5155 (2008), *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*.

[b-IETF RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3*.

[b-ATLAS] RIPE Atlas
https://atlas.ripe.net

[b-CABF] CAB (2019), *Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, v1.6.4.*
https://cabforum.org/baseline-requirements-documents/

[b-GSMA] GSMA (2018), *RSP Technical Specification Version 2.2.1*.
https://www.gsma.com/newsroom/wp-content/uploads//SGP.22-v2.2.1-2.pdf

[b-SET] Secure Electronic Transaction Specification Book 2: Programmer's Guide
http://www.maithean.com/docs/set_bk2.pdf

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020