NICC ND 1446 V1.1.1 (2022-12)

NICC Document

General Security for Public Electronic Communication Network and Service Providers

NICC Standards Limited

c/o TWP ACCOUNTING LLP,
The Old Rectory,
Church Street,
Weybridge,
Surrey KT13 8DE

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC Security Task Group

1 Scope

The present document highlights the sources of security standards and guidance available within the NICC [5] portfolio, UK Government and other external sources.

The information in this document applies to the providers of public electronic communications networks and providers of public electronic communications services.

These standards and guidance are set in the frameworks that are provided by the UK regulatory environment of OFCOM and the other UK government agencies of the NCSC [6] and CPNI [2].

These frameworks consist currently of the Communications Act and the Telecoms Security Act. These form the basis of basic good security processes and procedures.

The aim of these standards and guidance is to provide a basis for Providers to enact practises and procedures that assist in the detection, mitigation or prevention of security risks such as:

- The ability for an outside agency for unauthorised disruption or removal of service
- The ability for an outside agency to defraud the customer
- The ability for an outside agency to defraud the Provider
- The ability for a customer to defraud the Provider
- The ability for an outside agency to obtain information about or transmitted by a customer
- The ability for an outside agency to obtain information about or transmitted by a Provider

In conjunction with the NICC standards and guidance referenced in this document, Providers should follow practises that promote good general security hygiene by following the relevant Guidelines, Standards and UK legislation.

This document contains:

- References to frameworks in which this industry resides and makes use of
- Industry focused specific guidance on certain situations

2 References

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] CAF Cyber Assessment Framework
[2] CPNI Centre for the Protection of National Infrastructure
[3] ISF Internet Security Forum Standard
[4] ISO International Organization for Standardization
[5] NICC NICC Standards Limited
[6] NCSC National Cyber Security Centre
[7] NIST National Institute of Standards and Technology

2.2 Informative references

3 Definitions, symbols and abbreviations

3.1 Definitions

Botnets	Botnets are networks of hijacked computer devices used to carry out various scams and cyberattacks. The term “botnet” is formed from the word’s “robot” and “network.” Assembly of a botnet is usually the infiltration stage of a multi-layer scheme. The bots serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution.
Jailbreaking	Jailbreaking is the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features. It is called jailbreaking because it involves freeing users from the ‘jail’ of limitations that are perceived to exist.
Provider	An organisation that provides public electronic communications networks or public electronic communications services. These will include Communication and Network Providers, Network Operators, Telecommunications Operators, Internet Service Providers

3.2 Abbreviations

2FA	Two Factor Authentication
3FA	Three Factor Authentication
ADSL	Asynchronous Digital Subscriber Line
AES	Advanced Encryption Standard
All IP (All IP-T)	All IP Telephony
BPI	Baseline Privacy Interface (DOCSIS)
CAF	Cyber Assessment Framework
CIS	Centre for Internet Security (Framework)
CMTS	Cable Modem Transport System
CoP	Code of Practice
CPNI	Centre for the Protection of National Infrastructure
DCMS	Department for Digital, Culture, Media and Sport
DES	Data Encryption Standard
DNS	Domain Name Service
DOCSIS	Data Over Cable Service Interface Specification
DSL	Digital Subscriber Line
ENISA	European Union Agency for Cyber Security
ETSI	European Telecommunications Standards Institute
FTTC	Fibre to the Cabinet

FTTP	Fibre to the Premises
GSMA	Global System for Mobile Association
HFC	Hybrid Fibre Coax
IoT	Internet of Things
IP	Internet Protocol
IPSec	IP Security protocol
IPT	IP Telephony
ISO	International Standards Organisation
ISP	Internet Service Provider
MAC	Media Access Control
NCSC	National Cyber Security Centre
NIST	National Institute for Standards and Technology (USA)
ND	NICC Document
NGN	Next Generation Network(s)
NICC	NICC Standards Limited
NTP	Network Time Protocol
Ofcom	Office of Communications (UK Regulatory)
Radius	Remote Access Dial In User Service
RCS	Rich Communications Services
SIEM	Security Incident Event Management
SIP	Session Initiation Protocol (used in IPT)
SMS	Short Messaging Service
SS7	Signalling System 7 (C7)
TSB	Telecommunications Security Bill
TSR	Telecommunications Security Requirements
VoIP	Voice over IP

4 Generic security frameworks/guidance and best practice

4.1 Overview on security requirements for Providers

The threats that Providers face are increasing both in magnitude and sophistication. There is a range of capable threat actors (that can be state sponsored) or criminal organisations that will target services provided in the UK for their own malicious motives.

A significant breach of UK communications networks would have a catastrophic impact on business and society. The UK Government is responding with a new regime of security requirements aimed to mitigate these risks to an acceptable level. The new regime will see DCMS and Ofcom, with support from the National Cyber Security Centre (NCSC) [6] becoming more engaged with the design, engineering, architecture and operations of Providers operating in the UK. The initial focus will inevitably be on the major Providers but all Providers will ultimately be impacted.

All providers of telecommunications services will need to consider, as a minimum, the following: -

- Providers should take a mitigated risk-based approach to managing the security of their networks and services. This will involve use of Security Frameworks/Policies
- Providers will need to keep abreast of the range of security related guidance, best practice and standards that are relevant to their networks and services
- Providers will need to ensure technical compliance to the chosen security framework and best practices

General security guidance for service providers is provided in the sections that follow.

4.2 Regulation, guidance, standards on security requirements for Providers in the UK.

This section contains information and links to primary external sites for security information.

4.2.1 UK legislation

UK Legislation 2021

The UK is undergoing a significant legislative change in the Regulatory Requirements applicable to the providers of Public Electronic Communications Services and Public Electronic Communication Networks.

The Telecommunications (Security) Act introduces extensive new requirements for Providers and make changes to the Communications Act: 2003. The Act references a Statutory Instrument that defines security duties of Providers as well as defining additional powers given to the Secretary of State and Ofcom. The DCMS Code of Practice, based upon an NCSC [6] drafted set of Telecommunications Security Requirements, will provide guidance on the security controls that are required to be implemented. With such a radical change in the regulations it is understood that no Providers will be fully compliant with the new security measures from the moment they become

law, so the new security measures are expected to become mandatory requirements during 2024 to 2028.

During the same period, Ofcom's role will change, as they become more engaged with Providers' day-to-day activities associated with the provision of public electronic communications services and networks. An Ofcom Procedural Guidance document defines the new approach that Providers will follow. It is expected that Ofcom will engage with Providers once the new regulations become law to establish a starting position regarding compliance and will work with Providers individually to define and agree plans to move towards full compliance.

The legal hierarchy of the various documents is as follows: -

- Telecommunications Security Act:2021 - makes provisions about the security of public electronic communications networks and public electronic communications services
- Communications Act: 2003 – amended in 2021 to align specific requirements for Security with the TSA
- Electronic Communications (Security Measures Regulations) 2022 No. 933 The Electronic Communications (Security Measures) Regulations 2022 – secondary Legislation setting out security measures to be taken by providers of public electronic communications networks and services

4.2.2 Standards

UK Standards
Refer to section 4.3 of this document for information on NICC Standards [5].

International standards
Below are listed a number of international standards that may be used for reference;

- Guidelines on Security Measures under the EECC – https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

- ISO 27001/2 Information Security [4] – https://www.iso.org/

- ISO 22301 Business Continuity Management [4] – https://www.iso.org/

- ITU X.1051 https://www.itu.int/rec/T-REC-X/recommendation.asp?lang=en&parent=T-REC-X.1055

- ITU X.1055 https://www.itu.int/rec/T-REC-X/recommendation.asp?lang=en&parent=T-REC-X.1051

4.2.3 Guidance

Ofcom
Ofcom guidance on security - Ofcom guidance on security requirements in section 105A to D of the Communications Act 2003, 2017 Version (PDF, 377.4 KB)

The Communications Act 2003 and the Digital Economy Act 2017 (Consequential Amendments to Primary Legislation) Regulations 2017
https://www.legislation.gov.uk/ukdsi/2017/9780111160787

The Telecommunications Security Code of Practice has been issued and published, under sections 105E and 105F of the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021).

NCSC
The NCSC [6] is mandated to provide advice, best practise and guidance to Providers. It publishes and updates relevant documentation, as below.

NCSC CAF [1] guidance - NCSC.GOV.UK
https://www.ncsc.gov.uk/collection/caf

Good examples of advice and best Practice as follows –
NCSC guidance - https://www.ncsc.gov.uk/guidance
NCSC guidance - https://www.ncsc.gov.uk/section/information-for/large-organisations

CPNI
The CPNI [2] is mandated to provide advice, Best Practise, and guidance that may be of use to providers.
CPNI [2] guidance - https://www.cpni.gov.uk/advice

4.3 NICC security documents

NICC Standards Limited [5] is a technical forum for the UK communications sector that develops interoperability standards for public communications networks and services in the UK.

NICC Standards Limited [5] develops standards for use in the UK network. These standards are listed on the publication page of the public site.

Below are examples of NICC Specifications [5] that contain variations of the term ‘security’ in their title.

There are more specifications and NDs that contain information on security which is embedded in sections within the document. By searching on the NICC Public site, it is possible to locate other Specifications and NDs covering security on specific technical topics.

4.3.1 NICC Guidelines

NICC [5] has developed and published the following Security Guidelines documents -

- ND1407 – Voluntary Code of Practice for Security of Access to Dial-through Functions in Communications Systems
- ND1438 - Voluntary Code of Practice Mitigating Theft of Service from End User Voice over IP Communications Systems
- ND1440 – Guidance for the use and secure implementation of SIP Application Layer Gateways (ALG)

- ND1443 - Guidelines for the Security of All IP Telephony (All IPT) Service in the UK Telecommunications Network

4.3.2 NICC specifications

NICC [5] had developed and published the following Security Specifications -

- ND1628 – Securing Data Flows with IPSec for NGN Interconnects

- ND 1643 - Guidelines on the Minimum Security Controls for Interconnecting Communication Providers

4.4 Other potential frameworks/guidance

Accessing some of the following documentation and information sources may require membership or payment.

Note that some of the following are based on alternative national standards that may not be applicable to the UK.

Below are listed other frameworks and guidance that may be useful as background reading or reference -

- CAF [1] (Cyber Assessment Framework) at the NCSC [6] Website
- Cyber Essentials
- CIS Top 18 Controls
- CIS Benchmarks
- Gartner Adaptive Security Architecture
- NIST Cyber Security Framework [7]
- NIST Special Publication 800-53 [7]
- Internet Security Forum Standard (ISF [3])

Suitable Security frameworks are:

- ISO 27001/2 Information Security https://www.iso.org/
- ISO 22301 Business Continuity Management https://www.iso.org/

- Telecommunications (Security) Act Resources: https://www.gov.uk/government/publications/electronic-communications-security-measures-regulations-and-draft-telecommunications-security-code-of-practice

4.5 Voice

In the move from circuit-based switching for voice to IP based packet switched voice, Providers will need to evolve their processes and procedures to meet the needs of standard computer security hygiene.
IP Voice based services may now run on standard computer resources. This means that services are running on the same hardware and operating systems that the rest of the internet uses, making voice services much more susceptible to the same risks, attacks and threat actors. Therefore getting the basics of computer security right are more important than ever.

To mitigate the risk of security incidents, processes and procedures need to be put in place to cover such things as:

- Physical Security
- Continuity planning
- Secure Design
- System hardening
- Patch management
- Penetration testing
- Change management
- Logical Access Control
- Security Incident Event Management (SIEM)
- Resilience
- Personnel security

Section 4.4 details further reference material such as the CIS benchmarks which cover the above points.

4.5.1 All-IPT VoIP (Packet switched voice)

For security guidance on All IP Voice, refer to the NICC Guideline ND1443 [5].

4.5.2 App based VoIP (Over the Top)

This section provides references and links relating to security for the development of new Apps and for App based services.

It is recommended that -

- App developers must take ownership of the security for the entire life cycle of an App
- An App should not require the phone to be 'jail broken' for the App to work
- If using SMS for user identification or registration, please see section 4.8

https://support.apple.com/en-gb/guide/security/secf49cad4db/web

https://developer.android.com/topic/security/best-practices

https://www.ncsc.gov.uk/guidance/application-development-guidance-introduction

https://www.ncsc.gov.uk/collection/developers-collection

OWASP Application Security Verification Standard | OWASP Foundation
https://owasp.org/www-project-application-security-verification-standard/

https://www.ofcom.org.uk/consultations-and-statements/category-1/ensuring-compliance-with-security-duties

4.5.3 Circuit switched voice

Circuit switched voice services have always been regarded as inherently secure. There are, however, published NICC Documents that include security aspects that need to be considered when providing or carrying voice services.

In addition to the NDs listed in section 4.3 NICC Security Documents, the following ND documents are available and many contain security sections and sub sections.

ND1034 - UK SIPconnect Endorsement
ND1406 - Voluntary Code of Practice for Design of Private Telecommunication Networks
ND1431 - Guidance on CPE Compatibility on NGNs and NGAs
ND1445 - All-IP Telephony Industry Guidance and Lessons Learnt
ND1611 - Multi-Service NGN Interconnect Common Transport
ND1612 - Generic IP Connectivity for PSTN / ISDN Services between Next Generation Networks
ND1613 - NGN Interconnect: Transport Service Layer Management
ND1644 - Architecture for Ethernet Active Line Access (ALA)
ND1645 - NGA Telephony; Architecture and Requirements
ND1647 - SIP-NNI Basic Voice Architecture

By using the ‘search function’ in the NICC Publication page [5] and typing ‘security’ into the ‘search’ field, more NDs will be listed with security information contained in the text of the document.

4.6 Internet of Things (IoT)

The ever-expanding number of IoT devices, estimated to be more than 70 billion by 2025, that have connectivity to the internet will inevitably give rise to additional risks for consumers and Providers.

Most IoT devices use consumer grade technologies that:

- Are largely unmanaged
- Typically use sub-standard operating systems
- Are supplied by a vast number of suppliers
- Utilise insecure protocols and basic credentials
- Have the ability to connect to other devices inside or outside their physical location

The risks identified in the Scope section that are impacted by IoT include the risk of an outside agency being able to defraud the customer and the ability of an outside agency to obtain information about or transmitted by the customer.

From a business perspective IoT systems may include:

- Access Control Systems e.g. card readers that allow physical access to facilities such as hotel rooms or business locations
- Heating, Ventilation and Air Conditioning systems HVAC
- Remote cameras that operate via internet protocol
- Automatic or smart lighting systems that save energy when people are not present

From a consumer perspective there are a vast number of devices of a variety of types being produced and installed.

Providers, (including ISPs) need to consider IoT in two different scenarios:

1. The use of IoT Systems and solutions within their own business operations
2. The use of IoT devices in their customers

For the scenario 1, the Provider that has deployed IoT solutions within their own infrastructure should:

- Identify, assess and classify all IoT devices connected to their network
- Review the architecture and attempt to separate all IoT solutions as much as practical from the rest of their network
- Ensure that all IoT devices are monitored and any compromised devices are isolated and mitigation measures

With regards to scenario 2, the following considerations are appropriate:

- Provide advice to consumer customers as to the potential dangers associated with IoT devices in their homes
- If a customer IoT device becomes part of a Botnet and this is detected by the Provider, then ask and help the customer to take the steps necessary to remove or clean the compromised device.

The GSM Association has published a set of security guidelines documents to establish a common understanding of IoT (Internet of Things) security issues. The documents provide a methodology for developing secure IoT services and recommendations on how to mitigate common security threats and weaknesses within IoT services.
To find the documents online, search "GSMA IoT Security Guidelines"

4.7 Data service

Data Service

Data services to residential and business consumers have grown to become a fundamental building block of the UK economy. At the end of May 2020 there were just under 32 million fixed broadband connections to customers using DSL and cable technologies and a further 5 million with full fibre.

The infrastructure that provides these data service technologies requires a security environment that protects the provided services from both malicious and accidental misuse.

A security incident affecting local broadband infrastructure will impact thousands of customers who share the access segment. An incident that impacts the wider infrastructure management networks of the Provider or ISP that runs national networks could impact millions of customers.

The main area of concern for a service provider should be the management networks and systems that control and provision the infrastructure that provides services to a customer. If an unauthorised malicious actor was able to penetrate these networks, then service disruption could occur. The Telecoms Security Act [include reference]and associated documentation from Ofcom, NCSC [6] and the DCMS defines the minimum standards that is required, by law, to be implemented to protect these networks.

It is up to the specific Provider to assess their compliance requirements with the Telecoms Security Act. The guidance that accompanies the bill defines the individual control requirements that a Provider will need to fulfil. In summary the main areas that should be assessed and secured are:-

Administrative access. Proving administrators are who they say they are and are entitled to administer the infrastructure to which they are connecting. This control needs to be to all administrators, whether full time employees of the Provider, 3rd party contractors or vendors who provide support.

Infrastructure management. Validating all deployed equipment is security hardened, supported, tested and patched.

Monitoring. Ensuring that the provider has robust logging and monitoring strategies in place to detect anonymous traffic in both the management and data planes.

Customer accounting and authorisation. The systems that authorise customers onto the network must be hardened and implemented with controls similar to the administrative accounts. This will protect the Provider and the customer against fraud as all services will be tied back to active accounts.

Service availability. For the specific operating environment, the service design must consider how the resilience objectives for the service and supporting network will be met, to ensure service availability targets are met.

Supporting service availability. Data services rely on multiple other platforms to give a useable product to the customer. Some examples of critical supporting platforms are DNS, RADIUS (auth), and NTP. The provider must risk assess the full service stack that makes up the product offering to the customer and implement controls that secure these platforms.

Denial of Service mitigation. As data services also connect out to the wider internet appropriate safeguards should be implemented in the Provider network.

For all data services that fall outside of the specific regulatory space, the Provider should take a risk-based approach to the controls that will be implemented to protect their data services.

The good practice guides from Ofcom and the NCSC [6], as linked earlier in this document, are an excellent resource for starting the journey towards good security posture.

https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/connected-nations-update-summer-2020/interactive-report

4.7.1 Broadband technologies

Broadband technologies are used as an enabler for many telecommunication voices services and are likely to come into scope for alignment with the Telecommunications Security Act (TSA) as part of any Provider assessment. This will be within the definitions of Public Electronic Communication Networks and Telecommunications Electronic Services.

As such this document assumes that Broadband Networks and Services that fall in scope will align with areas of TSA, from operating control requirements proportional to the Tier of the provider (Tier 1>3). This will include associated network oversite functions that are deemed in scope, aligning with the TSA Control requirements including supplier management and incident reporting capabilities.

The following list of Broadband technologies is included for information -

ADSL - (VDSL)
Standards can be found here (various ones for the different versions of DSL)
https://www.itu.int/itudoc/gs/promo/tsb/85871.pdf
ADSL and ADSL2 G.992

FTTC – Fibre and VDSL
VDSL and VDSL2 G.993

FTTP – fibre all the way, one technology
https://www.itu.int/ITU-T/worksem/fttp/index.html

HFC/DOCSIS - (Hybrid Fibre Coax / Data Over Cable Service Interface Specification) security is defined in the CableLabs® DOCSIS 3.0 Security Specification (SEC3.0, SECv3.1, SECv4.0), based upon Baseline Privacy Interface Plus Specification (BPI/BPI+).
The link to the cable labs is - https://www.cablelabs.com/

DOCSIS Security Specification describes the MAC layer security functions between a CMTS (Cable Modem Transport System) located in the Providers network and customer premise Cable Modems.

BPI/BPI+ define the use of 40/56-bit DES (Data Encryption Standard). In addition SEC defines the use of 128-bit AES (Advanced Encryption Standard).

4.7.2 Mobile services (2G to 5G)

Mobile bearers are inherently designed to be secure. From the implementation of 2G, ciphering of the air interface has provided confidentiality, and authentication of the user to the network (and the network to the user from 3G onwards) has provided integrity.

Mobile security has evolved over the generations, each building more and more on top of the proceeding generation. 5G can be consider more secure than 4G, 4G more secure than 3G etc. Different Providers may choose to cease support of different generations of mobile at different times allowing effective and efficient use of spectrum or to support longer term requirements. As an example, the current rollout of so-called SMET2 Smart Meters on the O2 network will utilise 2.5G and 3G for years.

Threats against mobile have also increased as the generations have been released. There are a range of actors in this space, from excellent security researchers through to hostile nation state actors, who seek to abuse mobile for nefarious means. Vulnerabilities have been published relating to the air interface, to SIM cards and to the SS7 protocol stack as examples.

In general terms, anyone considering the use of mobile data services as a bearer should conduct a security risk assessment. This should examine the confidentiality, integrity and availability of the

data being transmitted. Also, consider, based on the output of that assessment, layering appropriate additional security over the top of that mobile bearer.

Specific guidance has been issued by both NIST [7] and by the UK NCSC [6] on the use of mobile SMS within multi factor authentication. Whilst it is true to say that MFA using SMS is better than not using MFA at all, consideration should be given to how to best secure the second factor by alternative means, e.g. authenticator apps. Organisations should conduct a security risk assessment to decide on the best solution for them.

General mobile security advice, standards and information can be obtained from the Provider concerned and also from the GSM Association, and specifically their Fraud and Security Group. ETSI is also a good source of standards and information.

4.8 Messaging services security

In general terms and for the vast majority of applications, mobile messaging can broadly be considered as secure. The UK National Cyber Security Centre provides some excellent advice on the use of SMS in critical business processes in their article here:
Protecting SMS messages used in critical business processes - NCSC.GOV.UK

A number of global security authorities and standards bodies have recommended against the use of SMS as a second vector in two-factor authentication. For example, NIST [7] recommended deprecating the use of SMS within 2FA in their Digital Identity Guidelines:
NIST SP 800-63 Digital Identity Guidelines
Despite the above, it is accepted that 2FA using SMS is better than not using 2FA at all so if there is no alternative, use SMS for 2FA rather than not doing 2FA at all.

Services like iMessage (on iPhones) and Google Messages (on Android handsets) use an underlying protocol called RCS. Organisations should consider conducting a risk assessment within their organisations on the use of such services.

Finally, there are a plethora of "over the top" messaging services such as Facebook Messaging, WhatsApp, Signal etc. There is a rich commentary on the various security and privacy concerns associated with these services on the internet and organisations are advised to conduct their own risk assessments within their organisations before using any such service. Again, as with SMS, for general day-to-day communications, such services provide rich and useful functionality but users should beware of security and privacy concerns such as how much data is visible to service owners such as Google, WhatsApp and Facebook.

Due to identity theft and fraud risks due to organisations using SMS as the 2nd Factor, Providers are recommended to have robust identity checking in place prior to any changes in personal details on accounts (i.e. address, home phone numbers) or ordering of replacement SIMs.

History

Document history		
Version	Date	Milestone
1.1.1	14th December 2022	Initial publication