Signalling System No. 7

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Signalling_System_No._7#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Signalling_System_No._7#searchInput)

|  |  |
| --- | --- |
| **Q.700 series** | |
| Signaling System No. 7 | |
| **Status** | In force |
| **Year started** | 1984 |
| **Latest version** | (03/93) March 1993 |
| **Organization** | [ITU-T](https://en.wikipedia.org/wiki/ITU-T) |
| **Committee** | Study Group XI, WTSC |
| **Related standards** | Q.701, Q.711 |
| **Domain** | [telephony](https://en.wikipedia.org/wiki/Telephony) |
| **Website** | <https://www.itu.int/rec/T-REC-Q.700> |

**Signaling System No. 7** (**SS7**) is a set of [telephony](https://en.wikipedia.org/wiki/Telephony) [signaling](https://en.wikipedia.org/wiki/Signaling_(telecommunications)) protocols developed in 1975, which is used to set up and [tear down](https://en.wikipedia.org/wiki/Clearing_(telecommunications)) telephone calls in most parts of the world-wide [public switched telephone network](https://en.wikipedia.org/wiki/Public_switched_telephone_network) (PSTN). The protocol also performs number translation, [local number portability](https://en.wikipedia.org/wiki/Local_number_portability), prepaid billing, [Short Message Service](https://en.wikipedia.org/wiki/Short_Message_Service) (SMS), and other services.

In North America SS7 is often referred to as *Common Channel Signaling System 7* (CCSS7). In the [United Kingdom](https://en.wikipedia.org/wiki/United_Kingdom), it is called *C7* (CCITT number 7), *number 7* and *Common Channel Interoffice Signaling 7* (CCIS7). In Germany, it is often called *Zentraler Zeichengabekanal Nummer 7* (ZZK-7).

The SS7 protocol is defined for international use by the Q.700-series recommendations of 1988 by the [ITU-T](https://en.wikipedia.org/wiki/ITU-T).[[1]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-q700-1) Of the many national variants of the SS7 protocols, most are based on variants standardized by the [American National Standards Institute](https://en.wikipedia.org/wiki/American_National_Standards_Institute) (ANSI) and the [European Telecommunications Standards Institute](https://en.wikipedia.org/wiki/European_Telecommunications_Standards_Institute) (ETSI). National variants with striking characteristics are the Chinese and Japanese [Telecommunication Technology Committee](https://en.wikipedia.org/wiki/Telecommunication_Technology_Committee) (TTC) national variants.

The [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF) has defined the [SIGTRAN](https://en.wikipedia.org/wiki/SIGTRAN) protocol suite that implements levels 2, 3, and 4 protocols compatible with SS7. Sometimes also called *Pseudo SS7*, it is layered on the [Stream Control Transmission Protocol](https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) (SCTP) transport mechanism for use on [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) networks, such as the [Internet](https://en.wikipedia.org/wiki/Internet).



**Contents**

* [1History](https://en.wikipedia.org/wiki/Signalling_System_No._7#History)
* [2Functionality](https://en.wikipedia.org/wiki/Signalling_System_No._7#Functionality)
  + [2.1Signaling modes](https://en.wikipedia.org/wiki/Signalling_System_No._7#Signaling_modes)
* [3Physical network](https://en.wikipedia.org/wiki/Signalling_System_No._7#Physical_network)
* [4SS7 protocol suite](https://en.wikipedia.org/wiki/Signalling_System_No._7#SS7_protocol_suite)
  + [4.1BSSAP](https://en.wikipedia.org/wiki/Signalling_System_No._7#BSSAP)
* [5Protocol security vulnerabilities](https://en.wikipedia.org/wiki/Signalling_System_No._7#Protocol_security_vulnerabilities)
* [6See also](https://en.wikipedia.org/wiki/Signalling_System_No._7#See_also)
* [7References](https://en.wikipedia.org/wiki/Signalling_System_No._7#References)
* [8Further reading](https://en.wikipedia.org/wiki/Signalling_System_No._7#Further_reading)

History[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=1)]

[Signaling System No. 5](https://en.wikipedia.org/wiki/Signaling_System_No._5) and earlier systems use [in-band signaling](https://en.wikipedia.org/wiki/In-band_signaling), in which the call-setup information is sent by generating special [multi-frequency](https://en.wikipedia.org/wiki/Multi-frequency_signaling) tones transmitted on the telephone line audio channels, also known as *bearer channels*. As the bearer channel are directly accessible by users, it can be exploited with devices such as the [blue box](https://en.wikipedia.org/wiki/Blue_box), which plays the tones required for call control and routing. As a remedy, SS6 and SS7 implements out-of-band signaling, carried in a separate signaling channel,[[2]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Ronayne-2):141 thus keeping the speech path separate. SS6 and SS7 are referred to as [common-channel signaling](https://en.wikipedia.org/wiki/Common-channel_signaling) (CCS) protocols, or *Common Channel Interoffice Signaling* (CCIS) systems.

Since 1975, CCS protocols have been developed by major telephone companies and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T); in 1977 the ITU-T defined the first international CCS protocol as [Signaling System No. 6](https://en.wikipedia.org/wiki/Signaling_System_No._6) (SS6).[[2]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Ronayne-2):145 In its 1980 Yellow Book Q.7XX-series recommendations ITU-T defined the Signaling System No. 7 as an international standard.[[1]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-q700-1) SS7 replaced SS6 with its restricted 28-bit signal unit that was both limited in function and not amendable to digital systems.[[2]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Ronayne-2):145 SS7 also replaced [Signaling System No. 5](https://en.wikipedia.org/wiki/Signaling_System_No._5) (SS5), while [R1](https://en.wikipedia.org/wiki/Multi-frequency_signaling) and [R2](https://en.wikipedia.org/wiki/R2_signaling) variants are still used in numerous countries.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

The [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF) defined [SIGTRAN](https://en.wikipedia.org/wiki/SIGTRAN) protocols which translate the common channel signaling paradigm to the IP Message Transfer Part (MTP) level 2 (M2UA and M2PA), Message Transfer Part (MTP) level 3 ([M3UA](https://en.wikipedia.org/wiki/M3UA)) and Signaling Connection Control Part (SCCP) (SUA).[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] While running on a transport based upon IP, the SIGTRAN protocols are not an SS7 variant, but simply transport existing national and international variants of SS7.[[3]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-rfc2716-3)[[*clarification needed*](https://en.wikipedia.org/wiki/Wikipedia:Please_clarify)]

Functionality[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=2)]

[Signaling](https://en.wikipedia.org/wiki/Signaling_(telecommunications)) in telephony is the exchange of [control information](https://en.wikipedia.org/wiki/Protocol-control_information) associated with the setup and release of a telephone call on a telecommunications circuit.[[4]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Russell-4):318 Examples of control information are the digits dialed by the caller and the caller's billing number.

When signaling is performed on the same circuit as the conversation of the call, it is termed [channel-associated signaling](https://en.wikipedia.org/wiki/Channel-associated_signaling) (CAS). This is the case for analogue trunks, [multi-frequency](https://en.wikipedia.org/wiki/Multi-frequency) (MF) and R2 digital trunks, and [DSS1/DASS](https://en.wikipedia.org/wiki/DASS1) [PBX](https://en.wikipedia.org/wiki/Business_telephone_system#Private_branch_exchange) trunks.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

In contrast, SS7 uses [common channel signaling](https://en.wikipedia.org/wiki/Common_channel_signaling), in which the path and facility used by the signaling is separate and distinct from the signaling without first seizing a voice channel, leading to significant savings and performance increases in both signaling and channel usage.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Because of the mechanisms in use by signaling methods prior to SS7 (battery reversal, [multi-frequency digit outpulsing](https://en.wikipedia.org/wiki/Multi-frequency), [A- and B-bit signaling](https://en.wikipedia.org/wiki/Robbed-bit_signaling)), these earlier methods can not communicate much signaling information. Usually only the dialed digits are signaled during call setup. For charged calls, dialed digits and charge number digits are outpulsed. SS7, being a high-speed and high-performance packet-based communications protocol, can communicate significant amounts of information when setting up a call, during the call, and at the end of the call. This permits rich call-related services to be developed. Some of the first such services were call management related, [call forwarding (busy and no answer)](https://en.wikipedia.org/wiki/Call_forwarding), [voice mail](https://en.wikipedia.org/wiki/Voice_mail), [call waiting](https://en.wikipedia.org/wiki/Call_waiting), [conference calling](https://en.wikipedia.org/wiki/Conference_call), [calling name and number display](https://en.wikipedia.org/wiki/Caller_ID), [call screening](https://en.wikipedia.org/wiki/Call_screening), [malicious caller identification](https://en.wikipedia.org/wiki/Malicious_caller_identification), [busy callback](https://en.wikipedia.org/wiki/Automatic_callback).[[4]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Russell-4):Introduction xx

The earliest deployed upper layer protocols in the SS7 suite were dedicated to the setup, maintenance, and release of telephone calls.[[5]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-5) The [Telephone User Part](https://en.wikipedia.org/wiki/Telephone_User_Part) (TUP) was adopted in Europe and the [Integrated Services Digital Network](https://en.wikipedia.org/wiki/Integrated_Services_Digital_Network) (ISDN) User Part ([ISUP](https://en.wikipedia.org/wiki/ISDN_User_Part)) adapted for [public switched telephone network](https://en.wikipedia.org/wiki/Public_switched_telephone_network) (PSTN) calls was adopted in North America. ISUP was later used in Europe when the European networks upgraded to the ISDN. As of 2020 North America has not accomplished full upgrade to the ISDN, and the predominant telephone service is still [Plain Old Telephone Service](https://en.wikipedia.org/wiki/Plain_old_telephone_service). Due to its richness and the need for an out-of-band channel for its operation, SS7 is mostly used for signaling between [telephone switches](https://en.wikipedia.org/wiki/Telephone_exchange) and not for signaling between local exchanges and [customer-premises equipment](https://en.wikipedia.org/wiki/Customer-premises_equipment).[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Because SS7 signaling does not require seizure of a channel for a conversation prior to the exchange of control information, [non-facility associated signaling](https://en.wikipedia.org/w/index.php?title=Non-Facility_Associated_Signaling&action=edit&redlink=1) (NFAS) became possible. NFAS is signaling that is not directly associated with the path that a conversation will traverse and may concern other information located at a centralized database such as service subscription, feature activation, and service logic. This makes possible a set of network-based services that do not rely upon the call being routed to a particular subscription switch at which service logic would be executed, but permits service logic to be distributed throughout the telephone network and executed more expediently at originating switches far in advance of call routing. It also permits the subscriber increased mobility due to the decoupling of service logic from the subscription switch. Another ISUP characteristic SS7 with NFAS enables is the exchange of signaling information during the middle of a call.[[4]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Russell-4):318

SS7 also enables Non-Call-Associated Signaling, which is signaling not directly related to establishing a telephone call.[[4]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Russell-4):319 This includes the exchange of registration information used between a mobile telephone and a [home location register](https://en.wikipedia.org/wiki/Network_switching_subsystem#Home_location_register_.28HLR.29) database, which tracks the location of the mobile. Other examples include [Intelligent Network](https://en.wikipedia.org/wiki/Intelligent_Network) and [local number portability](https://en.wikipedia.org/wiki/Local_number_portability) databases.[[4]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Russell-4):433

**Signaling modes**[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=3)]

Apart from signaling with these various degrees of association with call set-up and the facilities used to carry calls, SS7 is designed to operate in two modes: *associated mode* and *quasi-associated mode*.[[6]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-6)

When operating in the *associated mode*, SS7 signaling progresses from [switch to switch](https://en.wikipedia.org/wiki/Telephone_exchange) through the Public Switched Telephone Network following the same path as the associated facilities that carry the telephone call. This mode is more economical for small networks. The associated mode of signaling is not the predominant choice of modes in North America.[[7]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-7)

When operating in the *quasi-associated mode*, SS7 signaling progresses from the originating [switch](https://en.wikipedia.org/wiki/Telephone_exchange) to the terminating switch, following a path through a separate SS7 signaling network composed of [signal transfer points](https://en.wikipedia.org/wiki/Signal_Transfer_Point). This mode is more economical for large networks with lightly loaded signaling links. The quasi-associated mode of signaling is the predominant choice of modes in North America.[[8]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-8)

Physical network[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=4)]

SS7 separates signaling from the voice circuits. An SS7 network must be made up of SS7-capable equipment from end to end in order to provide its full functionality. The network can be made up of several link types (A, B, C, D, E, and F) and three signaling nodes – [Service Switching Points](https://en.wikipedia.org/wiki/Service_switching_point) (SSPs), [Signal Transfer Points](https://en.wikipedia.org/wiki/Signal_Transfer_Point) (STPs), and [Service Control Points](https://en.wikipedia.org/wiki/Service_Control_Point) (SCPs). Each node is identified on the network by a number, a signaling point code. Extended services are provided by a database interface at the SCP level using the SS7 network.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

The links between nodes are full-duplex 56, 64, 1,536, or 1,984 kbit/s graded communications channels. In Europe they are usually one (64 kbit/s) or all (1,984 kbit/s) [timeslots](https://en.wikipedia.org/wiki/Timeslot) ([DS0s](https://en.wikipedia.org/wiki/DS0)) within an [E1](https://en.wikipedia.org/wiki/E-carrier) facility; in North America one (56 or 64 kbit/s) or all (1,536 kbit/s) timeslots ([DS0As](https://en.wikipedia.org/wiki/DS0A) or DS0s) within a [T1](https://en.wikipedia.org/wiki/T-carrier) facility. One or more signaling links can be connected to the same two endpoints that together form a signaling link set. Signaling links are added to link sets to increase the signaling capacity of the link set.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

In Europe, SS7 links normally are directly connected between switching exchanges using F-links. This direct connection is called *associated signaling*. In North America, SS7 links are normally indirectly connected between switching exchanges using an intervening network of STPs. This indirect connection is called *quasi-associated signaling*, which reduces the number of SS7 links necessary to interconnect all switching exchanges and SCPs in an SS7 signaling network.[[9]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-9)

SS7 links at higher signaling capacity (1.536 and 1.984 Mbit/s, simply referred to as the 1.5 Mbit/s and 2.0 Mbit/s rates) are called [high speed links (HSL)](https://en.wikipedia.org/wiki/High_Speed_Link) in contrast to the low speed (56 and 64 kbit/s) links. High speed links are specified in ITU-T Recommendation Q.703 for the 1.5 Mbit/s and 2.0 Mbit/s rates, and ANSI Standard T1.111.3 for the 1.536 Mbit/s rate.[[10]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Q.703-10) There are differences between the specifications for the 1.5 Mbit/s rate. High speed links utilize the entire bandwidth of a T1 (1.536 Mbit/s) or E1 (1.984 Mbit/s) transmission facility for the transport of SS7 signaling messages.[[10]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Q.703-10)

[SIGTRAN](https://en.wikipedia.org/wiki/SIGTRAN) provides signaling using [SCTP](https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) associations over the [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol).[[4]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-Russell-4):456 The protocols for [SIGTRAN](https://en.wikipedia.org/wiki/SIGTRAN) are [M2PA](https://en.wikipedia.org/w/index.php?title=M2PA&action=edit&redlink=1), [M2UA](https://en.wikipedia.org/w/index.php?title=M2UA&action=edit&redlink=1), [M3UA](https://en.wikipedia.org/wiki/M3UA) and [SUA](https://en.wikipedia.org/w/index.php?title=Signaling_Connection_Control_Part&action=edit&redlink=1).[[11]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-11)

SS7 protocol suite[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=5)]

|  |  |
| --- | --- |
| **SS7 protocol suite** | |
| SS7 protocols by OSI layer | |
| [**Application**](https://en.wikipedia.org/wiki/Application_layer) | [INAP](https://en.wikipedia.org/wiki/INAP), [MAP](https://en.wikipedia.org/wiki/Mobile_Application_Part), [IS-41](https://en.wikipedia.org/wiki/IS-41)... [TCAP](https://en.wikipedia.org/wiki/Transaction_Capabilities_Application_Part), [CAP](https://en.wikipedia.org/wiki/CAMEL_Application_Part), [ISUP](https://en.wikipedia.org/wiki/ISDN_User_Part), ... |
| [**Network**](https://en.wikipedia.org/wiki/Network_layer) | [MTP Level 3](https://en.wikipedia.org/wiki/Message_Transfer_Part) + [SCCP](https://en.wikipedia.org/wiki/Signalling_Connection_Control_Part) |
| [**Data link**](https://en.wikipedia.org/wiki/Data_link_layer) | [MTP Level 2](https://en.wikipedia.org/wiki/Message_Transfer_Part) |
| [**Physical**](https://en.wikipedia.org/wiki/Physical_layer) | [MTP Level 1](https://en.wikipedia.org/wiki/Message_Transfer_Part) |
| * [v](https://en.wikipedia.org/wiki/Template:SS7_stack) * [t](https://en.wikipedia.org/wiki/Template_talk:SS7_stack) * [e](https://en.wikipedia.org/w/index.php?title=Template:SS7_stack&action=edit) | |

The SS7 [protocol stack](https://en.wikipedia.org/wiki/Protocol_stack) may be partially mapped to the [OSI Model](https://en.wikipedia.org/wiki/OSI_Model) of a packetized digital protocol stack. OSI layers 1 to 3 are provided by the [Message Transfer Part](https://en.wikipedia.org/wiki/Message_Transfer_Part) (MTP) and the [Signalling Connection Control Part](https://en.wikipedia.org/wiki/Signalling_Connection_Control_Part) (SCCP) of the SS7 protocol (together referred to as the Network Service Part (NSP)); for circuit related signaling, such as the [BT IUP](https://en.wikipedia.org/wiki/Interconnect_User_Part), [Telephone User Part (TUP)](https://en.wikipedia.org/wiki/Telephone_User_Part_(TUP)), or the [ISDN User Part](https://en.wikipedia.org/wiki/ISDN_User_Part) (ISUP), the User Part provides layer 7. Currently there are no protocol components that provide OSI layers 4 through 6.[[1]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-q700-1) The [Transaction Capabilities Application Part](https://en.wikipedia.org/wiki/Transaction_Capabilities_Application_Part) (TCAP) is the primary SCCP User in the Core Network, using SCCP in connectionless mode. SCCP in connection oriented mode provides transport layer for air interface protocols such as BSSAP and [RANAP](https://en.wikipedia.org/wiki/RANAP). TCAP provides transaction capabilities to its Users (TC-Users), such as the [Mobile Application Part](https://en.wikipedia.org/wiki/Mobile_Application_Part), the [Intelligent Network Application Part](https://en.wikipedia.org/wiki/INAP) and the [CAMEL Application Part](https://en.wikipedia.org/wiki/Camel_Application_Part).[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

The Message Transfer Part (MTP) covers a portion of the functions of the OSI network layer including: network interface, information transfer, message handling and routing to the higher levels. Signaling Connection Control Part (SCCP) is at functional Level 4. Together with MTP Level 3 it is called the Network Service Part (NSP). SCCP completes the functions of the OSI network layer: end-to-end addressing and routing, connectionless messages (UDTs), and management services for users of the Network Service Part (NSP).[[12]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-12) Telephone User Part (TUP) is a link-by-link signaling system used to connect calls. ISUP is the key user part, providing a circuit-based protocol to establish, maintain, and end the connections for calls. Transaction Capabilities Application Part (TCAP) is used to create database queries and invoke advanced network functionality, or links to Intelligent Network Application Part (INAP) for intelligent networks, or Mobile Application Part (MAP) for mobile services.

**BSSAP**[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=6)]

**BSS Application Part** (**BSSAP**) is a protocol in [Signaling System 7](https://en.wikipedia.org/wiki/Signaling_System_7) used by the [Mobile Switching Center](https://en.wikipedia.org/wiki/Mobile_Switching_Center) (MSC) and the [Base station subsystem](https://en.wikipedia.org/wiki/Base_station_subsystem) (BSS) to communicate with each other using signalling messages supported by the [MTP](https://en.wikipedia.org/wiki/Message_Transfer_Part) and [connection-oriented services](https://en.wikipedia.org/wiki/Connection-oriented_communication) of the [SCCP](https://en.wikipedia.org/wiki/Signalling_Connection_Control_Part). For each active [mobile equipment](https://en.wikipedia.org/wiki/Mobile_station) one signalling connection is used by BSSAP having at least one active transactions for the transfer of messages.[[13]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-13)

BSSAP provides two kinds of functions:

* The BSS Mobile Application Part (BSSMAP) supports procedures to facilitate communication between the MSC and the BSS pertaining to resource management and [handover](https://en.wikipedia.org/wiki/Handover) control.
* The Direct Transfer Application Part (DTAP) is used for transfer of those messages which need to travel directly to a Mobile equipment from MSC by passing any interpretation by BSS. These messages are generally pertaining to [Mobility management](https://en.wikipedia.org/wiki/Mobility_management) (MM) or [Call Management](https://en.wikipedia.org/wiki/Call_Management) (CM).

Protocol security vulnerabilities[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=7)]

In 2008, several SS7 vulnerabilities were published that permitted the tracking of cell phone users.[[14]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-14) In 2014, the media reported a protocol vulnerability of SS7 by which anybody can [track](https://en.wikipedia.org/wiki/Cell_phone_tracking) the movements of cell phone users from virtually anywhere in the world with a success rate of approximately 70%.[[15]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-15) In addition, eavesdropping is possible by using the protocol to forward calls and also facilitate decryption by requesting that each caller's carrier release a temporary encryption key to unlock the communication after it has been recorded.[[16]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-16) The software tool *SnoopSnitch* can warn when certain SS7 attacks occur against a phone,[[17]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-17) and detect [IMSI-catchers](https://en.wikipedia.org/wiki/IMSI-catcher) that allow call interception and other activities.[[18]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-18)[[19]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-19)

In February 2016, 30% of the network of the largest mobile operator in Norway, [Telenor](https://en.wikipedia.org/wiki/Telenor), became unstable due to "Unusual SS7 signaling from another European operator".[[20]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-20)[[21]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-21)

The security vulnerabilities of SS7 have been highlighted in U.S. governmental bodies, for example when in April 2016 US congressman [Ted Lieu](https://en.wikipedia.org/wiki/Ted_Lieu) called for an oversight committee investigation.[[22]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-22)

In May 2017, [O2 Telefónica](https://en.wikipedia.org/wiki/Telef%C3%B3nica_Germany), a German mobile service provider, confirmed that the SS7 vulnerabilities had been exploited to bypass [two-factor authentication](https://en.wikipedia.org/wiki/Two-factor_authentication) to achieve unauthorized withdrawals from bank accounts. The perpetrators installed [malware](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) on compromised computers, allowing them to collect online banking account credentials and telephone numbers. They set up redirects for the victims' telephone numbers to telephone lines controlled by them. Confirmation calls of two-factor authentication procedures were routed to telephone numbers controlled by the attackers. This enabled them to log into victims' online bank accounts and effect money transfers.[[23]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-23)

In March 2018, a method was published for the detection of the vulnerabilities, through the use of [open-source](https://en.wikipedia.org/wiki/Open-source_software) monitoring software such as [Wireshark](https://en.wikipedia.org/wiki/Wireshark) and [Snort](https://en.wikipedia.org/wiki/Snort_(software)).[[24]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-24)[[25]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-25)[[26]](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_note-26) The nature of SS7 normally being used between consenting network operators on dedicated links means that any bad actor's traffic can be traced to its source.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=8)]

* [SS7 probe](https://en.wikipedia.org/wiki/SS7_probe)
* [Out-of-band data](https://en.wikipedia.org/wiki/Out-of-band_data)

References[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=9)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-q700_1-0) [***b***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-q700_1-1) [***c***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-q700_1-2) [ITU-T Recommendation Q.700](http://www.itu.int/rec/T-REC-Q.700/en)
  2. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Ronayne_2-0) [***b***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Ronayne_2-1) [***c***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Ronayne_2-2) *Ronayne, John P (1986). The Digital Network Introduction to Digital Communications Switching (1 ed.). Indianapolis: Howard W. Sams & Co., Inc.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*0-672-22498-4*](https://en.wikipedia.org/wiki/Special:BookSources/0-672-22498-4)*.*
  3. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-rfc2716_3-0) [RFC 2719](http://www.ietf.org/rfc/rfc2719.txt) - Framework Architecture for Signaling Transport
  4. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Russell_4-0) [***b***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Russell_4-1) [***c***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Russell_4-2) [***d***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Russell_4-3) [***e***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Russell_4-4) [***f***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Russell_4-5) *Russell, Travis (2002). Signaling System #7 (4 ed.). New York: McGraw-Hill.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-07-138772-9*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-07-138772-9)*.*
  5. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-5) [ITU-T Recommendation Q.700,03/93](http://www.itu.int/rec/T-REC-Q.700-199303-I/en/), Section 3.2.1, p. 7.
  6. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-6) [ITU-T Recommendation Q.700](http://www.itu.int/rec/T-REC-Q.700-199303-I/en/), p. 4.
  7. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-7) ([Dryburgh 2004](https://en.wikipedia.org/wiki/Signalling_System_No._7#CITEREFDryburgh2004), pp. 22–23).
  8. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-8) ([Dryburgh 2004](https://en.wikipedia.org/wiki/Signalling_System_No._7#CITEREFDryburgh2004), p. 23).
  9. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-9) [ITU-T Recommendation Q.700](http://www.itu.int/rec/T-REC-Q.700-199303-I/en/), Section 2.2.3, *"signaling modes"*, pp. 4-5.
  10. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Q.703_10-0) [***b***](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-Q.703_10-1) [*"ITU-T Recommendation Q.703, Annex A, Additions for a national option for high speed signaling links"*](http://www.itu.int/rec/T-REC-Q.703-199607-I/en/)*.*[*International Telecommunication Union*](https://en.wikipedia.org/wiki/International_Telecommunication_Union)*. pp. 81–86.*
  11. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-11) [*"Understanding the Sigtran Protocol Suite: A Tutorial | EE Times"*](http://www.eetimes.com/document.asp?doc_id=1203417)*. EETimes. Retrieved 2016-06-30.*
  12. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-12) [ITU-T Recommendation Q.711](http://www.itu.int/rec/T-REC-Q.711-200103-I/en/), Section 1, *"Scope and field of application"*, pp 1-2.
  13. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-13) [3GPP TS 48.008](http://www.3gpp.org/ftp/Specs/html-info/48008.htm) Mobile Switching Centre - Base Station System (MSC-BSS) interface; Layer 3 specification
  14. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-14) *Engel, Tobias (27 December 2008).*[*"Locating Mobile Phones using SS7"*](https://www.youtube.com/watch?v=OEcW4HlrpYE)*(Video). Youtube. 25th Chaos Communication Congress (25C3). Retrieved 19 April 2016.*
  15. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-15) *Timburg, Craig (24 August 2014).*[*"For sale: Systems that can secretly track where cellphone users go around the globe"*](https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html)*.*[*The Washington Post*](https://en.wikipedia.org/wiki/The_Washington_Post)*. Retrieved 27 December 2014.*
  16. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-16) *Timburg, Craig (18 December 2014).*[*"German researchers discover a flaw that could let anyone listen to your cell calls"*](https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/)*.*[*The Washington Post*](https://en.wikipedia.org/wiki/The_Washington_Post)*. Retrieved 19 December 2014.*
  17. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-17) SnoopSnitch is for [rooted](https://en.wikipedia.org/wiki/Rooting_(Android)) Android mobile phones with [Qualcomm chip](https://en.wikipedia.org/wiki/List_of_Qualcomm_Snapdragon_systems-on-chip)
  18. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-18) *Karsten Nohl (2014-12-27).*[*"Mobile self-defence"*](https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf)*(PDF). Chaos Communication Congress.*
  19. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-19) [*"SnoopSnitch"*](https://play.google.com/store/apps/details?id=de.srlabs.snoopsnitch)*.*[*Google Play*](https://en.wikipedia.org/wiki/Google_Play)*. August 15, 2016.*
  20. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-20) [*"Feilen i mobilnettet er funnet og rettet"*](http://www.mynewsdesk.com/no/telenor/pressreleases/feilen-i-mobilnettet-er-funnet-og-rettet-1322239)*(in Norwegian). Telenor ASA.*
  21. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-21) [*"SS7 signalering – Et ondsinnet angrep mot Telenor ville hatt samme konsekvens"*](http://www.digi.no/tele-kommunikasjon/2016/02/22/-et-ondsinnet-angrep-mot-telenor-ville-hatt-samme-konsekvens)*(in Norwegian). digi.no / Teknisk Ukeblad Media AS.*
  22. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-22) [*"US congressman calls for investigation into vulnerability that lets hackers spy on every phone"*](https://www.theguardian.com/technology/2016/apr/19/ss7-hack-us-congressman-calls-texts-location-snooping)*.*[*The Guardian*](https://en.wikipedia.org/wiki/The_Guardian)*. April 19, 2016.*
  23. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-23) *Khandelwal, Swati.*[*"Real-World SS7 Attack — Hackers Are Stealing Money From Bank Accounts"*](http://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html)*. The Hacker News. Retrieved 2017-05-05.*
  24. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-24) *Corletti Estrada, Alejandro.*[*"Análisis de ataques/vulnerabilidades SS7/Sigtran empleando Wireshark (y/o tshark) y Snort"*](http://darfe.es/joomla/index.php/descargas/viewdownload/5-seguridad/1353-analisis-de-ataques-vulnerabilidades-ss7-sigtran-empleando-wireshark-y-o-tshark-y-snort-es)*. Metodología de detección de vulnerabilidades SS7/Sigtran (in Spanish). Retrieved 2018-03-31.*
  25. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-25) *Corletti Estrada, Alejandro.*[*"Analysis of attacks/vulnerabilities SS7/Sigtran using Wireshark (and/or tshark) and Snort"*](http://darfe.es/joomla/index.php/descargas/viewdownload/5-seguridad/1354-analysis-of-attacks-vulnerabilities-ss7-sigtran-using-wireshark-and-or-tshark-and-snort-en)*. Vulnerability detection methodology SS7/Sigtran. Retrieved 2018-03-31.*
  26. [**^**](https://en.wikipedia.org/wiki/Signalling_System_No._7#cite_ref-26) [*"Definitive guide to SS7/Sigtran Attack and Preventive Measures"*](https://www.smtechub.com/ss7-attack/)*. Full Research on SS7/Sigtran Attack Vector, Exploits and Preventive Measures. Retrieved 2020-07-03.*

Further reading[[edit](https://en.wikipedia.org/w/index.php?title=Signalling_System_No._7&action=edit&section=10)]

* *Dryburgh, Lee; Hewitt, Jeff (2004). Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. Indianapolis: Cisco Press.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*1-58705-040-4*](https://en.wikipedia.org/wiki/Special:BookSources/1-58705-040-4)*.*
* *Ronayne, John P. (1986). "The Digital Network". Introduction to Digital Communications Switching (1st ed.). Indianapolis: Howard W. Sams & Co., Inc.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*0-672-22498-4*](https://en.wikipedia.org/wiki/Special:BookSources/0-672-22498-4)*.*
* *Russell, Travis (2002). Signaling System #7 (4th ed.). New York: McGraw-Hill.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-07-138772-9*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-07-138772-9)*.*