SIEMENS

Data sheet   **6GK5792-6MN00-0AA6**

product type designation	Antenna ANT792-6MN

ANT792-6MN IWLAN antenna with omnidirectional characteristic incl. N-female plug: 6 dBi IP67 (-40-+70 °C); 2.4 GHz; Wi-Fi compliance and national approvals to be observed; mounting on wall or mast, compact instructions as hard copy German/English, scope of delivery: 1x ANT792-6MN,

Technical Product Detail Page	https://i.siemens.com/1P6GK5792-6MN00-0AA6
radio frequencies	
type of wireless network / is supported	WLAN
operating frequency	
● for WLAN in 2.4 GHz frequency band	2.4 ... 2.5 GHz
electrical data	
antenna gain compared to spherical radiator	
● of the WLAN antenna / in the 2.4 GHz frequency band	6 dB
impedance	50 Ω
polarization	Linear Vertical
radiation characteristic	omnidirectional
standing wave ratio (VSWR) / maximum	1.8
radiating angle of the antenna	
● in the 2.4 GHz frequency band / horizontal	360°
● in the 2.4 GHz frequency band / vertical	30°
number of electrical connections / of the antenna	1
type of electrical connection / of the antenna	N-Connector
design of plug-in connection	female
angle of inclination / downward / maximum	0°
mechanical data	
material	
● of outer shell	Glass fiber
ambient conditions	
ambient temperature	
● during operation	-40 ... +80 °C
● during storage	-40 ... +80 °C
● during transport	-40 ... +80 °C
protection class IP	IP67
wind load / maximum	3 N; at 160 km/h
design, dimensions and weights	
width	50 mm
height	370 mm
depth	40 mm
net weight	300 g
fastening method	
● mast mounting	Yes
● wall mounting	Yes
● roof mounting	No

● directly on the device	No
product features, product functions, product components / general	
product feature / silicon-free	Yes
standards, specifications, approvals	
certificate of suitability	
● RoHS conformity	Yes
product conformity	UL 94-HB
wireless approval	Current national approvals can be found on the Internet under www.siemens.com/funkzulassungen
further information / internet links	
internet link	
● to website: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
● to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
● to web page: WLAN country approval	https://www.siemens.com/wireless-approvals
● to website: Industrial communication	https://www.siemens.com/simatic-net
● to web page: SiePortal	https://sieportal.siemens.com/
● to website: Image database	https://www.automation.siemens.com/bilddb
● to website: CAx-Download-Manager	https://www.siemens.com/cax
● to website: Industry Online Support	https://support.industry.siemens.com
security information	
security information	Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)

last modified: 11/11/2025 ↗