SIEMENS

Data sheet 6GK1900-0AB00

C-plug, removable data storage medium for simple device replacement in case of fault, for recording configuration or engineering and application data, can be used in the following SIMATIC NET products with C-plug slot: SCALANCE X-200, X-300, X-400, S-600, CP443-1Advanced, CP343-1Advanced, CP343-1 ERPC, IE/PB-Link PNIO, .

product type designation	
product type designation	C-PLUG
suitability for operation	SCALANCE XC-200, XP-200, XM-400, XR-500, M-800, W-700, SC-600 and S615 devices with PLUG slot
ambient conditions	
ambient temperature	
● during operation	-40 ... +75 °C
● during storage	-40 ... +80 °C
● during transport	-40 ... +80 °C
relative humidity	
● at 25 °C / without condensation / during operation / maximum	95 %
protection class IP	IP20
design, dimensions and weights	
width	24.3 mm
height	17 mm
depth	8.1 mm
net weight	5 g
design of the removable storage	
● C-PLUG	Yes
● KEY-PLUG	No
product feature / conformal coating	No
product features, product functions, product components / general	
storage capacity	256 Mibyte
standards, specifications, approvals	
reference code	
● according to IEC 81346-2:2019	CFA
standards, specifications, approvals / Environmental Product Declaration	
Environmental Product Declaration	Yes
Global Warming Potential [CO2 eq]	
● total	1264 kg
● during manufacturing	0.92 kg
● during operation	0.34 kg
● after end of life	0.0042 kg
further information / internet links	
internet link	
● to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
● 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)

Approvals / Certificates

General Product Approval

Declaration of Conformity	CE EG-Konf.	CCC CCC	EAC	Manufacturer Declaration	RCM

Environment

Confirmation	EPD

last modified:	6/3/2024