SIEMENS

Data sheet 6GT2890-0CA00

product type designation	**card holder for all RF1000 readers**
product description	Card holder for ISO cards and round transponder
	SIMATIC RF1000 card retainer for all access control readers of the RF1000 family; for clipping in.

suitability for use	plastic holder for latching onto the RF1000 reader
suitability for operation	holder for permanently keeping the transponder on the reader
mechanical data	
material	SAN
color	Transparent
ambient conditions	
ambient temperature	
● during operation	-25 ... +55 °C
● during storage	-25 ... +55 °C
● during transport	-25 ... +55 °C
design, dimensions and weights	
width	100 mm
height	42 mm
depth	15 mm
standards, specifications, approvals	
reference code	
● according to IEC 81346-2:2019	UQB
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 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:	1/28/2025