SIEMENS

Data sheet 6GT2831-6CA60

product type designation



Reader RF1040R USB/RS232

SIMATIC RF1000 access control reader RF1040R; LF 125 kHz, HITAG 1/2/S, EM41xx, HF, ISO 14443 A/B, ISO15693; USB port, including RS 232 interface; IP65 front, -25 to +55 °C; 90 x 62 x 25 mm LxWxH; with integrated antenna, including 1.8 m USB connecting cable .BLE

suitability for operation	HiTag 1/2/S, EM4xxx, ISO 15693 and ISO 14443 A/B transponder, for connecting to PC and control systems
radio frequencies	
operating frequency	0.125 13.56 MHz
range / maximum	0.03 m; Range is dependent on transponder type: observe http://support.automation.siemens.com/WW/view/en/67384964
protocol / with radio transmission	HiTag 1/2/S, EM41xx/45xx, EKS key, ISO 15693, ISO 14443 A/B, Felica, NXP NTAG21x, HID iClass
transfer rate / with radio transmission / maximum	424 kbit/s
product feature / multitag-capable	Yes
electrical data	
transfer rate / at the point-to-point connection / serial / maximum	115.2 kbit/s
interfaces	
standard for interfaces / for communication	USB 2.0, RS232
type of electrical connection	1.8 m connecting cable with USB 2.0 type A connector or RS232 connecting cable
mechanical data	
material	PC-GF
color	Ti gray
mounting distance / relating to metal surfaces / recommended / minimum	0 mm
supply voltage, current consumption, power loss	
supply voltage / at DC	
rated value	5 V
•	4.6 5.25 V
consumed current / at DC	
• at 5 V / typical	0.15 A
• at 5 V / maximum	0.3 A
ambient conditions	
ambient temperature	
during operation	-25 +55 °C
during storage	-25 +55 °C
during transport	-25 +55 °C
protection class IP	IP65; on front after cabinet installation, IP20 rear
shock resistance	EN 60721-3-7 Class 7 M2
shock acceleration	300 m/s²
vibrational acceleration	50 m/s²
design, dimensions and weights	
design, dimensions and weights width	90 mm

depth	23.5 mm	
net weight	0.12 kg	
fastening method	4 M4 screws for cabinet installation	
product features, product functions, product components / general		
display version	3-color LED	
product feature / silicon-free	Yes	
standards, specifications, approvals		
certificate of suitability	Radio according to R&TTE guidelines EN300 330 and EN 301489, FCC, cULus	
certificate of suitability		
• IECEx	No	
accessories		
accessories	card holder, USB cable 0.5 m, table/wall box, clean room cover, BLE license, HID license	
further information / internet links		
internet link		
• to website: Image database	https://www.automation.siemens.com/bilddb	
• to website: Industry Online Support	https://support.industry.siemens.com	
W 1.5 0		
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)	
	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	



Industry Canada (IC) other radio approvals other radio approvals

Radio Equipment Type Approval Certificate

<u>FCC</u>

last modified: 3/25/2024