

### product type designation

### PC adapter USB A2

PC adapter USB A2 USB adapter (USB V2.0) for connection of a PG/PC or notebook to SIMATIC S7 via PROFIBUS or MPI contain USB cable 5 m, MPI cable 0.3 m can be used under Windows XP/Vista/ Windows 7 32/64 bit and higher.



transfer rate	
transfer rate	
<ul style="list-style-type: none"> <li>at the 1st interface / according to PROFIBUS</li> </ul>	9.6 kbit/s ... 12 Mbit/s
interfaces	
number of electrical connections	
<ul style="list-style-type: none"> <li>at the 1st interface / according to PROFIBUS</li> </ul>	1
number of interfaces / according to USB	1
type of electrical connection	
<ul style="list-style-type: none"> <li>at the 1st interface / according to PROFIBUS</li> <li>of the USB interface</li> </ul>	9-pin Sub-D socket (RS 485) Standard-B socket
standard for interfaces / USB 2.0	Yes
supply voltage, current consumption, power loss	
type of voltage / of the supply voltage	DC
type of voltage supply / optional external power supply	No
supply voltage	
<ul style="list-style-type: none"> <li>from USB</li> <li>note</li> </ul>	5 V Supply direct from USB
relative symmetrical tolerance / at DC	
<ul style="list-style-type: none"> <li>at 5 V</li> </ul>	5 %
consumed current	
<ul style="list-style-type: none"> <li>from USB</li> </ul>	0.2 A
power loss [W]	1 W
ambient conditions	
ambient temperature	
<ul style="list-style-type: none"> <li>during operation</li> <li>during storage</li> <li>during transport</li> </ul>	0 ... 60 °C -40 ... +70 °C -40 ... +70 °C
relative humidity / at 30 °C / during operation / maximum	95 %
protection class IP	IP20
design, dimensions and weights	
module format	USB V2.0 adapter
width	58 mm
height	26 mm
depth	105 mm
net weight	0.365 kg
fastening method / 35 mm top hat DIN rail mounting	No
product features, product functions, product components / general	
number of plug-in cards of same design / plug-in / per PC station	1

number of units / note	-
<b>product functions / diagnostics</b>	
product function	
• port diagnostics	Yes
<b>standards, specifications, approvals</b>	
reference code	
• according to IEC 81346-2:2019	KEC
<b>further information / internet links</b>	
internet link	
• to website: Selection guide for cables and connectors	<a href="https://support.industry.siemens.com/cs/ww/en/view/109766358">https://support.industry.siemens.com/cs/ww/en/view/109766358</a>
• to web page: selection aid TIA Selection Tool	<a href="https://www.siemens.com/tstcloud">https://www.siemens.com/tstcloud</a>
• to website: Industrial communication	<a href="https://www.siemens.com/simatic-net">https://www.siemens.com/simatic-net</a>
• to web page: SiePortal	<a href="https://sieportal.siemens.com/">https://sieportal.siemens.com/</a>
• to website: Image database	<a href="https://www.automation.siemens.com/bilddb">https://www.automation.siemens.com/bilddb</a>
• to website: CAx-Download-Manager	<a href="https://www.siemens.com/cax">https://www.siemens.com/cax</a>
• to website: Industry Online Support	<a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
<b>security information</b>	
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 <a href="http://www.siemens.com/cybersecurity-industry">www.siemens.com/cybersecurity-industry</a> . 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 <a href="https://www.siemens.com/cert">https://www.siemens.com/cert</a> . (V4.7)

**Approvals / Certificates**

**General Product Approval**

[Declaration of Conformity](#)



General Product Approval	EMV	Marine / Shipping	Environment
<p>RCM</p>	<p><a href="#">KC</a></p>	<p>ABS</p> <p>PRS</p>	<p><a href="#">Confirmation</a></p> <p>EPD</p>

last modified:

8/8/2024