Security Guidebook Function List (Small Printers)

Y: Supported -: Not supported

Security Function	TM-m30II	TM-m30II-S/ TM-m30II-SL	TM-m50	TM-L100	TM-T88VII	TM-m30III/ TM-m30III-H	TM-m50II	TM-P20II/ TM-P80II Bluetooth	TM-P20II/ TM-P80II Wi-Fi	TM-T20IV	TM-H6000VI
Network Security											
TLS Communication	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TLS1.1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TLS1.2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TLS1.3	-	-	-	-	-	-	-	-	-	Y	-
Controlling Protocol Permissions and Exclusions	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IPsec/IP Filtering	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
IKEv1	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
IKEv2	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
ESP:AES-CBC-128/AES-CBC-192/AES-CBC-256/3DES	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
ESP:AES-GCM-128/AES-GCM-192/AES-GCM-256	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
ESP/AH:SHA-1/MD5	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
ESP/AH:SHA-256/SHA-384/SHA-512	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
IEEE802.1X Authentication	Y*1	Y*1	Y*1	Y*1	Y	Y	Y	Y	Y	Y	Y
EAP-TLS	Y*1	Y*1	Y*1	Y*1	Y	Y	Y	Y	Y	Y	Y
PEAP-TLS	Y*1	Y*1	Y*1	Y*1	Y	Y	Y	Y	Y	Y	Y
PEAP/MSCHAPv2	Y*1	Y*1	Y*1	Y*1	Y	Y	Y	Y	Y	Y	Y
EAP-TTLS	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
AES128/AES256/3DES/RC4	Y*1	Y*1	Y*1	Y*1	Y	Y	Y	Y	Y	Y	Y
SNMP	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SNMPv1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SNMPv2c	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
SNMPv3	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
Wi-Fi Security	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y
Bluetooth Security	Y	Y	Y	Y	Y	Y	-	Y	-	Y	-
CA Certificate	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Protecting Your Product											
Handling Viruses Introduced by USB Memory	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Print Security											
Secure Printing	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2
HTTPS Communication Protected by TLS	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	-	Y*2	Y*2	Y*2
Communication Using the TCP Port (8143/8043/TCPS) for ePOS-Device Protected by TLS	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y
Bluetooth Communication Protected by AES Encryption	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	-	Y*2	-	Y*2	-
User Data Protection											
Data Handling Processed by a Product	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Password Encryption	-	-	-	-	Y	Y	Y	Y	Y	Y	Y
Acquiring Receipt Information	-	-	-	-	Y	Y	-	-	-	Y	-
Operational Limitation											
Password Policy	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Audit Log	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2
Product Security											
Automatic Firmware Update Notification	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2
Protection Against Illegal Firmware Updates	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2
Administrator Password Authentication for Network Updating	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2
HTTPS Data Communication Protection	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2
Signature Verifying the Authenticity of F/W Update	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2	Y*2
Malware Infiltration Detection	-	-	-	-	-	Y	Y	Y	Y	Y	Y
Security Measures When You Dispose of Your Product											
Restore Factory Default	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

*1 Only supported for wireless LAN models.

*2 The feature is only available in Europe, the Middle East, and Africa. For details, see the Cybersecurity Enhancement Supplementary Guide or the product manual.