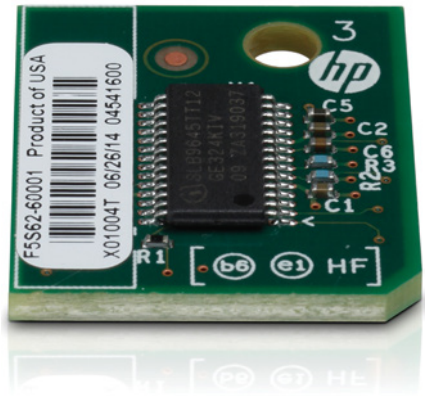
Data sheet

HP Trusted Platform Module

Plug in and protect

Add an extra level of security to safeguard sensitive information. The HP Trusted Platform Module (TPM) strengthens protection of encrypted credentials and data stored on your printer or MFP.[1]



Recognize and manage risks

The value of data to your organization can not be understated. The more data that you acquire and share, the more security risks and requirements you face. Your imaging and printing environment is not immune to costly security breaches.[2] And while security gaps can leave sensitive data dangerously exposed, the HP Trusted Platform Module (TPM) can help guard against such exposures.

With the TPM, you can:

- **Safeguard sensitive user data:** The TPM is an easy-to-install security chip that enables secure storage of information, such as passwords and security keys. By automatically sealing device encryption keys to the TPM, the printer or multifunction product (MFP) strengthens protection of encrypted credentials and data that it stores.[3] The TPM "wraps" encryption keys with its own storage root key, which is stored within the TPM.
- **Provide secure device identity:** Certificate private keys are both generated by and protected by the TPM, so you can be assured that even your most sensitive client information, data, and documents are safeguarded. The printer or MFP uses the created certificates to prove it is the device it claims to be. Because the certificate private keys never leave the TPM, the identity certificates cannot be spoofed or copied, helping ensure that information received from the device is genuine and that information sent to the device is going to the intended destination.
- **Gain peace of mind:** The TPM is designed to international industry standards, specifically the TPM 1.2 standard set by the Trusted Computing Group (TCG).[4] And when it comes time to dispose of your printer or MFP, you are able to make the printer or MFP stop using the TPM. When this happens, the TPM will permanently delete the storage root key, and any data that was protected by it cannot be retrieved by anyone who subsequently has access to the device.

Install quickly and easily

Start safeguarding your sensitive user data right away—installation requires minimal technical expertise. Simply attach the TPM accessory to the device formatter and turn on the device. The TPM automatically pairs with your printer or MFP upon installation. The relevant security keys, passwords, and certificates will automatically be secured by the TPM.

Installation

1 Snap in TPM

2 Turn on the device

3 Secure keys, passwords, and certificates

Product specifications

Part number	F5S62A
Supported printers and MFPs	Supported with the latest firmware update using HP FutureSmart 3.0: **HP LaserJet:** M806 **HP LaserJet MFP:** M630, M830 **HP Color LaserJet:** M651, M855 **HP Color LaserJet MFP:** M680, M880 **HP Officejet:** X555 **HP Officejet MFP:** X585
Dimensions	0.85 x 0.71 x 0.24 in (21.62 x 18.03 x 6.2 mm)
Weight	0.06 oz (1.71 g)
What's in the box	HP Trusted Platform Module, Install Guide
Warranty	One-year, onsite limited warranty
Environmental ranges	Recommended temperature: Operating: 56 to 86° F (13 to 30° C); Storage: 32 to 104° F (0 to 40° C) Humidity: Operating: 10 to 80% RH, Storage: 10 to 90% RH
Standards and certifications	Designed to the TPM 1.2 standard set by the Trusted Computing Group.[4]

Learn more at
hp.com/go/printsecurity

Notes

[1] Use of the HP Trusted Platform Module accessory may require a firmware upgrade.
[2] The cost of a single data breach averages $136 per record compromised, and $5.4M overall. Source: Ponemon 2013 Cost of a Data Breach: Global Analysis, May 2013.
[3] HP is not liable for maintaining recovery keys. Customers are strongly encouraged to perform the recommended procedures to back up customer keys and data.
[4] The Trusted Computing Group (TCG) is an international industry standards group that develops specifications amongst its members. The TCG publishes the specifications for use and implementation by the industry.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-4782ENW, September 2014