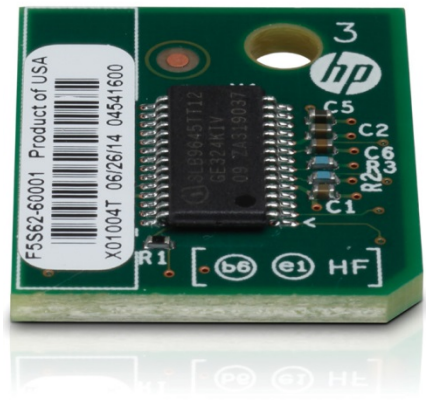
Технический документ

Чип HP Trusted Platform Module

Обеспечьте защиту данных сразу же после подключения устройства

Реализуйте дополнительный уровень системы безопасности для защиты конфиденциальной информации. Чип HP Trusted Platform Module (TPM) обеспечивает надежную защиту зашифрованных учетных данных и другой информации, хранящейся на принтере или МФУ[1].



Выявление и устранение рисков

Важность данных для организации невозможно переоценить. И чем больше данных накапливается, тем выше риски для безопасности и выше требования, предъявляемые к системе безопасности. Ваша инфраструктура печати и обработки изображений не защищена, что может обойтись весьма дорого[2]. Из-за брешей в системе безопасности конфиденциальные данные подвергаются серьезному риску, однако тут на помощь приходит чип HP Trusted Platform Module (TPM).

Чип TPM предоставляет следующие преимущества:

- **Защита конфиденциальных данных пользователей:** TPM — это удобный в установке чип, обеспечивающий безопасное хранение данных, в том числе паролей и ключей безопасности. Благодаря автоматической привязке к чипу TPM ключей шифрования принтера или МФУ обеспечивается надежная защита хранящихся на устройстве зашифрованных учетных данных и иной информации[3]. Чип TPM «заменяет» ключи шифрования собственным корневым ключом хранилища, который хранится в самом чипе.
- **Надежная идентификация устройств:** чип TPM создает закрытые ключи сертификатов и обеспечивает их защиту, поэтому вы можете быть абсолютно уверены в безопасности конфиденциальной информации, документов и иных данных клиентов. Созданные сертификаты используются принтером или МФУ для подтверждения подлинности. Поскольку закрытые ключи сертификатов никогда не выходят за пределы чипа TPM, удостоверяющие сертификаты невозможно подменить или скопировать, что гарантирует подлинность полученной с устройства информации, а также то, что эта информация попадет в нужные руки.
- **Уверенность в завтрашнем дне:** чип TPM соответствует международным стандартам, в частности стандарту TPM 1.2, разработанному Trusted Computing Group (TCG).[4] А когда придет время утилизировать принтер или МФУ, чип TPM на устройстве можно будет отключить. При этом корневой ключ хранилища будет безвозвратно удален, после чего прочитать хранящиеся на устройстве данные будет невозможно, даже если оно попадет в руки злоумышленников.

Удобство установки

Обеспечьте защиту конфиденциальных данных незамедлительно — для установки чипа требуются минимальные технические навыки. Просто подключите модуль TPM к плате форматирования устройства и включите устройство. Чип TPM автоматически начнет работать с принтером или МФУ. Защита ключей безопасности, паролей и сертификатов также будет обеспечена автоматически.

Установка

1 Подключение модуля TPM

2 Включение устройства

3 Защита ключей, паролей и сертификатов

Технические характеристики

Артикул	F5S62A
Поддерживаемые принтеры и МФУ	Поддерживаются следующие устройства с последней версией встроенного ПО, обновленного по технологии HP FutureSmart 3.0: HP LaserJet: M602, M603, M604, M605, M606, M712, M806 HP LaserJet MFP: M630, M830 HP Color LaserJet: M552, M553, M651, M855 HP Color LaserJet MFP: M680, M880 HP OfficeJet: X555 HP OfficeJet MFP: X585
Габариты	21,62 x 18,03 x 6,2 мм
Вес	1,71 г
Комплект поставки	Чип HP Trusted Platform Module, руководство по установке
Гарантия	Ограниченная гарантия сроком на один год с обслуживанием на месте установки оборудования
Диапазоны характеристик окружающей среды	Рекомендуемая температура: эксплуатация: 13–30 °C; хранение: 0–40 °C Относительная влажность: эксплуатация: 10–80%, хранение: 10–90%
Стандарты и сертификаты	Соответствует стандарту TPM 1.2, разработанному Trusted Computing Group[4].

Дополнительные сведения см. по адресу
hp.com/go/jetadvantage

Notes

[1] Для работы чипа HP Trusted Platform Module может потребоваться обновление встроенного ПО.

[2] Утечка данных обходится организации в среднем в 136 долларов за каждую запись, а общая сумма убытков достигает 5,4 млн долларов. Источник: «Цена утечки данных в 2013 г.: глобальный анализ», Ponemon, май 2013 г.

[3] HP не несет ответственности за обслуживание ключей восстановления. Клиентам настоятельно рекомендуется следовать предложенным процедурам по резервному копированию ключей и данных.

[4] Trusted Computing Group (TCG) — это международная группа, разрабатывающая отраслевые стандарты для входящих в нее организаций. Группа TCG публикует технические спецификации, предназначенные для использования и внедрения в конкретной отрасли.

Подписаться на обновления
hp.com/go/getupdated

4AA5-4782RUE, апрель 2015 г.