Advantech AE Technical Share Document

Date	1/11 /2023	**Release Ver.**	V1.0
Category	■ FAQ □ SOP	**Release Note**	□Internal ■External
Related OS			
Abstract	What is the difference between TPM IC and Intel PTT?		
Keyword	TPM, Intel PTT, fTPM		
Related Product	IASG products that support TPM IC or Intel PTT		

■ Solution:

Four types of TPM are popular today, offering different trade-offs between cost, features, and security.

DISCRETE TPM

Discrete TPM provides the highest level of security, as might be needed for a TPM used to secure the brake controller in a car. The intent of this level is to ensure that the device it's protecting does not get hacked via even sophisticated methods. To accomplish this, a discrete chip is designed, built and evaluated for the highest level of security that can resist tampering with the chip, including probing it and freezing it with all sorts of sophisticated attacks.

INTEGRATED TPM

Integrated TPM is the next level down in terms of security. This level still has a hardware TPM but it is integrated into a chip that provides functions other than security. The hardware implementation makes it resistant to software bugs, however, this level is not designed to be tamper-resistant.

FIRMWARE TPM

Firmware TPM is implemented in protected software. The code runs on the main CPU, so a separate chip is not required. While running like any other program, the code is in a protected execution environment called a trusted execution environment (TEE) that is separated from the rest of the programs that are running on the CPU. By doing this, secrets like private keys that might be needed by the TPM but should not be accessed by others can be kept in the TEE creating a more difficult path for hackers.

In addition to the lack of tamper resistance, the downside to the TEE or firmware TPM is that now the TPM is dependent on many additional aspects to keep it secure, including the TEE operating system, bugs in the application code running in the TEE, etc.

ADVANTECH
Enabling an Intelligent Planet

SOFTWARE TPM

Software TPM can be implemented as a software emulator of the TPM. However, a software TPM is open to many vulnerabilities, not only tampering but also the bugs in any operating system running it. It does have key applications: it is very good for testing or building a system prototype with a TPM in it. For testing purposes, a software TPM could provide the right solution/approach.

The five variations of TPM, discussed roughly in order of security level and decreasing cost, are shown in table. To get a better handle on the cost and security level impact, the TPM supplier needs to be consulted.

TRUST ELEMENT	SECURITY LEVEL	SECURITY FEATURES	RELATIVE COST	TYPICAL APPLICATION
DISCRETE TPM	HIGHEST	TAMPER RESISTANT HARDWARE	$$$	CRITICAL SYSTEMS
INTEGRATED TPM	HIGHER	HARDWARE	$$	GATEWAYS
FIRMWARE TPM	HIGH	TEE	$	ENTERTAINMENT SYSTEMS
SOFTWARE TPM	NA	NA	¢¢	TESTING & PROTOTYPING
VIRTUAL TPM	HIGH	HYPERVISOR	¢	CLOUD ENVIRONMENT

- **Reference**

http://www.springer.com/us/book/9783319087436