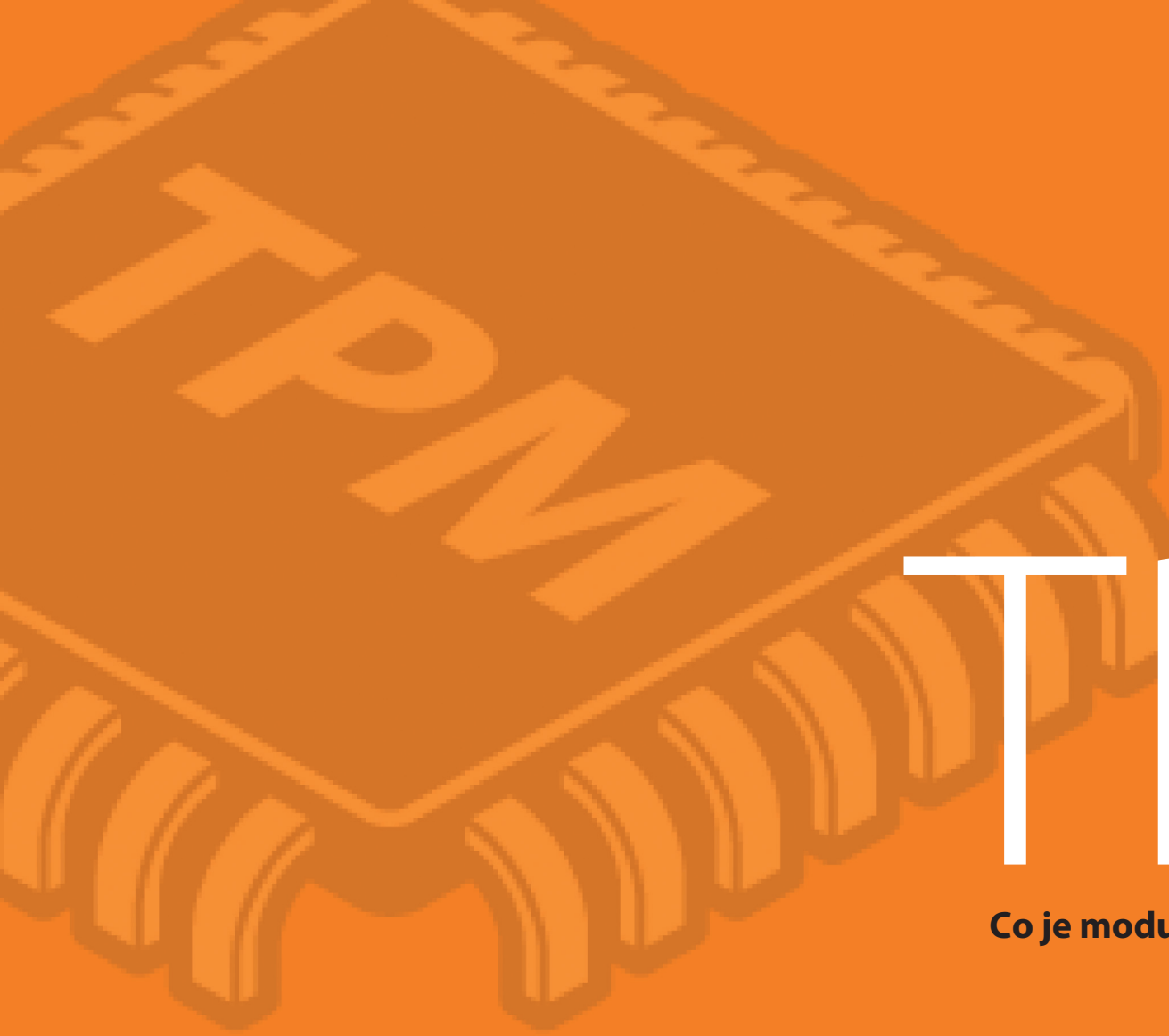


TPM

Co je modul s důvěryhodné platformy?

"Můžete zjistit, že se vaše organizace nachází v podobné situaci jako PwC, což vás může vést k využívání TPM pro silné ověřování."

- Karl Wagner, PwC, ředitel, Global IT

Co je TPM?

Modul s důvěryhodnou platformou (TPM - trusted platform module) je bezpečnostní čip založený na standardech, který je vestavěn do většiny vašich laptopů a stolních počítačů. Ve skutečnosti byl dodán ve více než 600 milionech laptopů a stolních počítačů od společností Acer, Dell, HP, Lenovo, Panasonic, Samsung a Toshiba.

TPM je bezpečný mikroprocesor s šifrovacími funkcemi, který poskytuje kořen důvěry (root of trust) a umožňuje bezpečné generování klíčů a omezení jejich používání (k podepisování / ověřování nebo šifrování / dešifrování). Slouží také jako bezpečný kontejner pro ukládání klíčů a může zabezpečit jiná data považovaná za příliš citlivá na to, aby byla použita jen softwarová ochrana.

Standard TPM vytvořila téměř před deseti lety skupina TCG (Trusted Computing Group); mezinárodní organizace pro bezpečnostní standardy.

Jak to funguje?

K základním výhodám TPM nad tradičním softwarem patří to, že TPM může generovat klíče, ukládat důvěrné informace a provádět měření v rámci bezpečné hranice fyzického hardwarového čipu – nezávislého na operačním systému PC a jeho procesoru. To znamená, že klíče TPM nelze kopírovat nebo exportovat, uložené důvěrné informace nelze ukrást nebo nevědomě použít a provedená opatření nemohou být změněna malwarem.

TPM mají navíc značné výhody oproti jiným zařízením s hardwarovým zabezpečením, jako jsou tokeny OTP, smart karty a tokeny USB. Na rozdíl od těchto technologií je TPM skutečně trvalou součástí PC: je připevněn k základní desce. A z toho důvodu je TPM jediným tokenem, který je schopen vytvořit jedinečnou a trvalou identitu pro každý počítač ve vaší síti. Protože se TPM nachází pod povrchem, který může být terčem útoku, jako je firmware, ovladače, zavaděč (boot loader) a operační systém, může bezpečně tvořit základní opatření, která lze používat k ověřování integrity PC před povolením jeho přístupu do vaší sítě.

Důvěřujte vašim mobilním stanicí

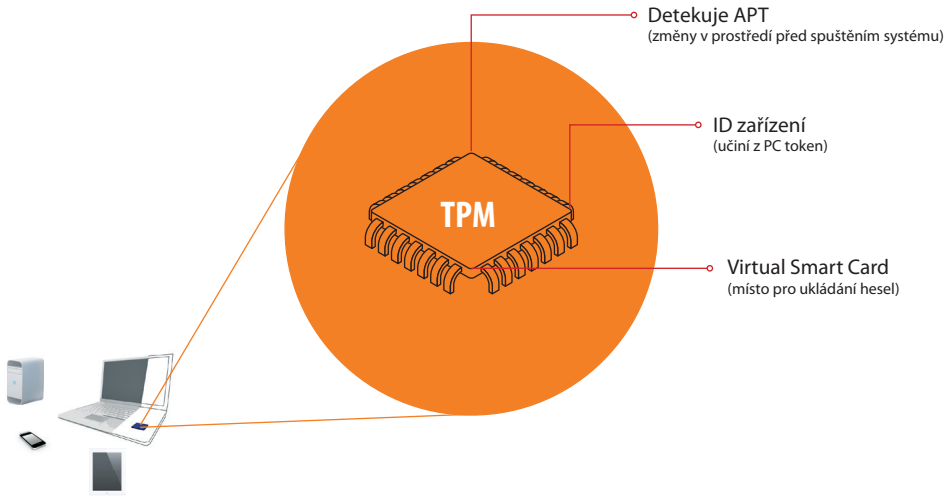
Špičková řešení pro ochranu dat od společnosti Wave jsou založena na velmi jednoduchém principu:

Zabezpečení začíná u zařízení.

Vestavěné zabezpečení zdaleka není nové nebo nevyzkoušené, již dlouho brání podvodnému používání mobilních telefonů a kabelových sítí, Xbox LIVE a iTunes. Důvěryhodné koncové zařízení je základním kamenem síťového zabezpečení.

Protože pokud zabezpečení začíná u zařízení, můžete:

- **Zajistit ochranu proti APT**
- **Důvěřovat počítačům, které přistupují k vašim službám v cloudu**
- **Zabezpečit vaše systém proti útokům malwaru**
- **Zjednodušit zabezpečení vašich sítí VPN a WiFi a eliminovat náklady za tokeny**
- **Zajistit integritu BIOS počítačů**
- **Umožnit BYOD (používání soukromých zařízení) při současném zajištění bezpečnosti sítě a informací**



Oficiální distributor pro ČR a SR
Genisoft, a.s.
Strakonická 6, Praha 5 - Lahovičky, 159 00, Česká republika
+420 723 885 032
info@genisoft.cz