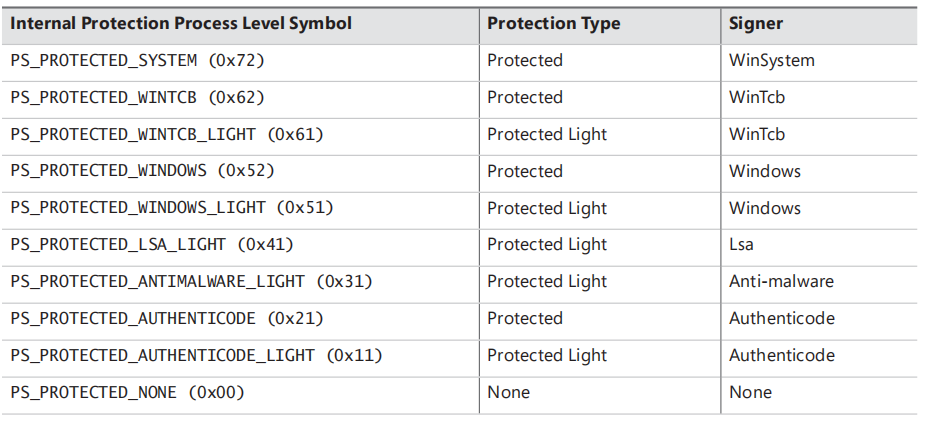
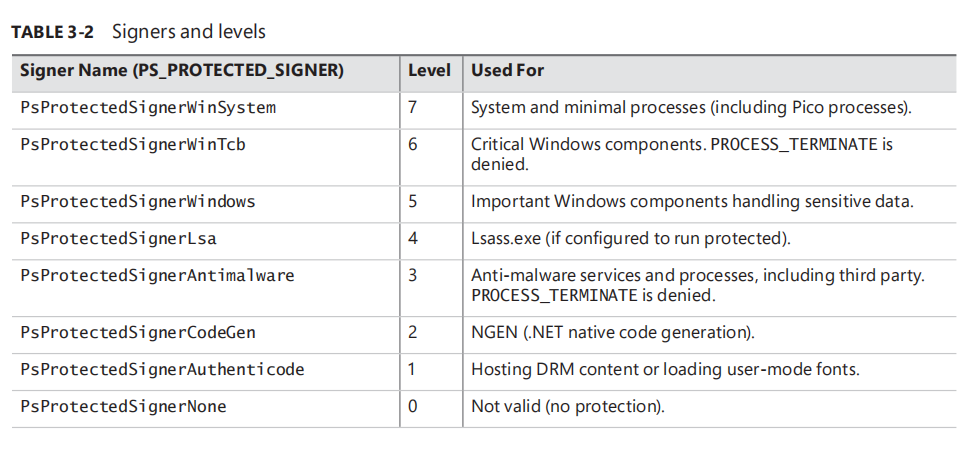
PPL是受保护进程轻型，Windows上的受保护程序中的一种，PPL可以受到与传统保护进程相同的保护，即用户模式代码（哪怕是提权后运行）无法通过注入线程的方式渗透进此类进程，也无法获取有关已加载DLL的详细信息。而PPL模型对可实现的保护增加了一个新的维度——属性值。不同签名房 (signer) 的信任程度各不相同，因此一个PPL可以实现比其他PPL更严格或更宽松的保护。

下表为EPROCESS结构中所存储的保护标记可用的值



上表显示了签名方及其级别。根据能力的大小，这里定义了多种签名方。WinSystem是最高优先级的签名方，主要供System进程以及Memory Compression进程等最小进程使用。对于用户模式进程，WinTCB(Windows Trusted Computer Base)是最高优先级的签名方，可用于保护关键进程。内核可能对此类进程有非常深入的了解，因而可能会降低其安全边界。

Protected > Protected Light；高级签名方可以访问低级签名方的进程，签名级别如下表



借助PPL机制，系统对进程的保护能力可扩展至由微软创建的可执行文件的范围之外。例如反恶意软件(Anti-Malware)程序。典型的AM产品通常包含下列三大组件。

1. 内核驱动程序：负责拦截文件系统或网络I/O请求，并使用对象、进程(PsSetCreateProcessNotifyRoutineEx函数)和线程回调(PsSetCreateThreadNotifyRoutine函数)实现阻止功能。
2. 用户模式的服务(通常用特权账户运行): 配置驱动程序的配置文件，从驱动程序处接收有关“值得关注”事件（例如有文件感染）的通知，并可能要与本地服务器或互联网通信。
3. 用户模式的GUI进程：向用户告知相关信息，让用户在必要时做出处理决策。

以防恶意软件攻击AM服务，AM服务一般会以PPL的方式运行，让AM服务无法被代码注入，且AM进程将无法终止，借此AM服务能够更好地防范针对内核级漏洞的恶意软件。

为了实现这种做法，AM内核驱动程序必须具备相应的预先启动反恶意软件(Early-Launch Anti Malware, ELAM)驱动程序。此类驱动需要微软提供的一种特殊反恶意软件证书。一旦安装了此类驱动，即可在自己的主PE文件中包含一个名为ELAMCERTIFICATEINFO的自定义资源节。该资源节可描述3个额外的签名方(由其公钥加以区分)，每个签名方最多可以具备3个额外的EKU(由OID加以区分)。当代码完整性系统确认由3个签名方中任何一个签名过的任何文件中包含3个EKU中的任意一个EKU后，即可允许该进程请求PS\_PROTECTED\_ANTIMALWARE\_LIGHT(0x31)这个PPL。Windows Defender就是这样做的。