Visão geral da tecnologia Trusted Platform Module

28/11/2018 • 5 minutos para ler •

Neste artigo

Descrição do recurso

Aplicações práticas

Funcionalidade nova e alterada

Atestado de integridade de dispositivo

Versões com suporte para atestado de integridade do dispositivo

Tópicos relacionados

Aplica-se a

- Windows 10
- Windows Server 2016
- Windows Server 2019

Este tópico para o profissional de TI descreve o TPM (Trusted Platform Module) e como o Windows o usa para controle de acesso e autenticação.

Descrição do recurso

A tecnologia TPM foi desenvolvida para fornecer funções relacionadas à segurança com base em hardware. Um chip TPM é um processador de criptografia seguro projetado para desempenhar as operações de criptografia. O chip inclui vários mecanismos de segurança física para torná-lo resistente a adulterações nas funções de segurança do TPM por software mal-intencionado. Algumas das principais vantagens do uso da tecnologia TPM são a possibilidade de:

- Gerar, armazenar e limitar o uso de chaves de criptografia.
- Usar a tecnologia TPM para autenticação de dispositivo de plataforma com a chave RSA de autogravação exclusiva do TPM.

- Ajudar a garantir a integridade da plataforma, executando e armazenando medidas de segurança.

As funções mais comuns do TPM são para medições de integridade do sistema e uso e criação de chaves. Durante o processo de inicialização de um sistema, o código de inicialização que é carregado (incluindo firmware e componentes do sistema operacional) pode ser medido e gravado no TPM. As medidas de integridade podem ser usadas como prova de como um sistema foi iniciado e como garantia de que uma chave baseada no TPM só foi usada com o software correto para inicializar o sistema.

As chaves baseadas no TPM podem ser configuradas de várias maneiras. Uma opção é tornar uma chave baseada no TPM indisponível fora do TPM. Isso é bom para reduzir ataques de phishing porque impede que a chave seja copiada e usada sem o TPM. As chaves baseadas no TPM também podem ser configuradas para exigir um valor de autorização de uso. Se ocorrerem muitas tentativas de autorização incorretas, o TPM ativará sua lógica de ataque de dicionário e evitará novas tentativas de valor de autorização.

Versões diferentes do TPM estão definidas nas especificações pelo TCG (Trusted Computing Group). Para obter mais informações, consulte o site do TCG.

Inicialização automática do TPM com o Windows 10

Desde o Windows 10, o sistema operacional é inicializado automaticamente e assume propriedade do TPM. Isso significa que, na maioria dos casos, recomendamos que você evite configurar o TPM por meio do console de gerenciamento do TPM, **TPM.msc**. Há algumas exceções, principalmente relacionadas à redefinição ou à realização de uma instalação limpa em um computador. Para obter mais informações, consulte Limpar todas as chaves do TPM. Não estamos mais desenvolvendo ativamente o console de gerenciamento do TPM a partir do windows Server 2019 e do Windows 10, versão 1809.

Em determinados cenários corporativos específicos limitados ao Windows 10, versões 1507 e 1511, a Política de Grupo pode ser usada para fazer backup do valor de autorização do proprietário do TPM no Active Directory. Como o estado do TPM é preservado em todas as instalações de sistema operacional, essas informações do TPM são armazenadas em um local separado dos objetos do computador no Active Directory.

Aplicações práticas

É possível instalar ou criar certificados em computadores usando o TPM. Depois que um computador é configurado, a chave privada RSA para obter um certificado é vinculada ao

TPM e não pode ser exportada. O TPM também pode ser usado como um substituto para cartões inteligentes, o que reduz os custos associados à criação e distribuição de cartões inteligentes.

O provisionamento automatizado no TPM reduz o custo de implantação do TPM em uma empresa. As novas APIs para gerenciamento do TPM podem determinar se as ações de provisionamento do TPM exigem a presença física de um técnico de serviço para aprovar solicitações de alteração de estado do TPM durante o processo de inicialização.

O software antimalware pode usar as medições de inicialização do estado inicial do sistema operacional para comprovar a integridade de um computador no qual o Windows 10 ou o Windows Server 2016 esteja em execução. Essas medições incluem a inicialização do Hyper-V para testar se os datacenters usando a virtualização não estão executando hipervisores não confiáveis. Com o Desbloqueio pela rede do BitLocker, os administradores de TI podem enviar por push uma atualização sem a preocupação de que um computador está esperando a entrada do PIN.

O TPM tem diversas configurações de Política de Grupo que podem ser úteis em determinados cenários corporativos. Para obter mais informações, consulte Configurações da Política de Grupo do TPM.

Funcionalidade nova e alterada

Para obter mais sobre as funcionalidades nova e alterada para Trusted Platform Module no Windows 10, consulte Novidades no Trusted Platform Module?.

Atestado de integridade de dispositivo

O atestado de integridade de dispositivo permite que as empresas tenham confiança nos componentes de hardware e software de um dispositivo gerenciado. Com o atestado de integridade de dispositivo, você pode configurar um servidor MDM para consultar um serviço de atestado de integridade que permitirá ou negará o acesso de um dispositivo gerenciado a um recurso seguro.

Algumas coisas que você pode verificar no dispositivo são:

- A Prevenção de Execução de Dados é compatível e está habilitada?
- A Criptografia de Unidade de Disco BitLocker é compatível e está habilitada?
- A Inicialização Segura é compatível e está habilitada?

> **Observação**
>
> O Windows 10, o Windows Server 2016 e o Windows Server 2019 dão suporte ao atestado de integridade do dispositivo com TPM 2,0. O suporte para o TPM 1,2 foi adicionado a partir da versão 1607 do Windows (RS1). TPM 2,0 requer firmware UEFI. Um computador com BIOS herdado e TPM 2,0 não funcionará conforme o esperado.

Versões com suporte para atestado de integridade do dispositivo

Versão do TPM	Windows 10	Windows Server 2016	Windows Server 2019
TPM 1.2	>= ver 1607	>= ver 1607	Sim
TPM 2.0	Sim	Sim	Sim

Tópicos relacionados

- Trusted Platform Module (lista de tópicos)
- Detalhes sobre o padrão TPM (tem links para recursos usando TPM)
- Portal de serviços base do TPM
- API de serviços base TPM
- Cmdlets do TPM no Windows PowerShell
- Preparar sua organização para o BitLocker: planejamento e políticas - configurações do TPM
- Provisionamento de dispositivo do Azure: atestado de identidade com TPM
- Provisionamento de dispositivo do Azure: uma linha do tempo de fabricação para dispositivos TPM
- Windows 10: Habilitando o vTPM (TPM virtual)
- Como fazer multi-inicialização com o BitLocker, TPM e um sistema operacional que não seja Windows