《使命召唤》安全认证失败

故障分析报告 · 动视支持工单材料

HP OMEN 17-ck2002TX ｜ 报告日期 2026-10-20 ｜ 证据版本 1.1

一、一句话结论

本机 TPM 2.0、安全启动、EK 证书、证书链、AIK 私钥全部正常，唯一缺失的是由微软 AIK 服务签发的 AIK 证书。证书申请在 GetCACaps 阶段即被微软以 HTTP 404 拒绝（KeyId 7fd50ee8...，该 authority 未在 microsoftaik.azure.net 预置）。

该失败发生在任何 TPM 操作之前（CreateRequest / SubmitRequest 均为 0 ms），属于服务端配置问题，用户侧不存在可修复的环节。

二、环境信息

项目	值
机型	OMEN by HP Laptop 17-ck2002TX（HP 官方维修板，板号 8BAD）
CPU	13th Gen Intel Core i9-13900HX
操作系统	Windows 11 26H2，Build 26300.9711
启动模式	UEFI / GPT
安全启动	已启用（UEFISecureBootEnabled = 1）
TPM	Intel PTT 2.0，固件 600.18.1040.2765，Spec 1.38
BIOS	F.16（2026-04-21，HP 当前最新版本）
VBS / HVCI	均已启用；IOMMU 可用且已启用
游戏平台	Steam — Call of Duty HQ

三、故障现象

界面	显示内容	含义
官方安全认证向导	TPM 2.0 通过、安全启动通过、认证未满足；「新密钥生成失败，建议更新 BIOS 固件」	基础项全部达标，失败在密钥生成阶段
向导可操作状态	「需要重新生成密钥」+「生成密钥」按钮	提示点击后出现 UAC 应选「是」；实际点击后依然失败
第三方工具（bufftool）	检测 9 项，通过 8、未满足 1；游戏 AIK 密钥「本次未返回」、AIK 密钥集「未满足」、AIK 证书「未判定」	调用 Windows 接口拿不到 AIK，与官方向导结论一致

四、关键证据

4.1 证书申请被拒（2026-10-20 18:45，管理员）

```
> certreq -enrollaik -config ""
GET https://INTC-KeyId-7fd50ee8ef6f5eb392ded861815e2d49b45c487b.microsoftaik.azure.net/templates/Aik/scep
GetCACaps: Not Found
{"Message":"The authority \"intc-keyid-7fd50ee8ef6f5eb392ded861815e2d49b45c487b.microsoftaik.azure.net\" does not exist."}
HTTP/1.1 404 Not Found
x-ms-request-id: 599dc7f3-48e8-41aa-abf9-f895077c5bf8
EnrollStage = 140  CreateRequest = 0 ms  SubmitRequest = 0 ms
0x80190194 (HTTP_E_STATUS_NOT_FOUND)
```

4.2 TPM 健康状态（全部通过）

```
-TPM Present: Yes                -Ready For Storage: True
-TPM Version: 2.0                -Ready For Attestation: True
-Manufacturer: INTC / Intel      -Is Capable For Attestation: True
-Firmware: 600.18.1040.2765      -Clear Needed To Recover: False
-PCR7 Binding State: Bound       -TPM Has Vulnerable FW: False
CheckEkCertState: EKCertState is Present
```

4.3 证书链对比

来源	元素数	信任状态	说明
ekchain（Windows 旧缓存）	4	0x10008	部分链 + 签名无效（旧主板残留）
ekchainNV（TPM NV 0x1C00100）	4	0x10000	签名有效，仅缺根（正常状态）
当前（导入 NV 正确链后）	4	0x10000	错链已替换，签名错误已消除

4.4 历史 400 与当前 404 的对比

动视向导导出的 certreq_output.txt 记录了一次更早的申请，使用的是另一个 KeyId：

```
INTC-KeyId-ea950d987bcff0df9aac1feffb8ab4803fef2ca2 (Intel ODCA 2 Issuing CA)
Submit(Request): Bad Request
{"Message":"No valid TPM EK/Platform certificate provided in the TPM identity request message."}
-> HTTP 400 / 0x80190190
```

阶段	KeyId	微软回应	含义
换板初期	ea950d98…（Intel ODCA 2）	400：EK 证书无效	该 authority 存在，但当时仍在用旧主板的 EK 证书
当前	7fd50ee8…（CSME ADL PTT 01SVN）	404：authority 不存在	已换为当前 TPM 的真实 EK 证书，微软未收录该 CA

五、动视向导报告解读（diagnostic_info.json）

共 9 项检查，8 项通过，唯一失败项为 BAD_KEYSET：

检查项	类别	级别	结果
COD_BROKER_INSTALLED	ATTESTATION	EXPECTED	通过
COD_BROKER_DISABLED	ATTESTATION	EXPECTED	通过
TPM2_PRESENT	TPM	REQUIRED	通过

检查项	类别	级别	结果
AMDFW_NEEDS_UPDATE	ATTESTATION	EXPECTED	通过
BAD_KEYSET	ATTESTATION	EXPECTED	未通过
TCG_LOG_PRESENT	ATTESTATION	EXPECTED	通过
EFI_MEASUREMENT_PRESENT	ATTESTATION	EXPECTED	通过
CAN_TURN_ON_SECURE_BOOT	SECURE_BOOT	REQUIRED	通过
SHOULD_TURN_ON_SECURE_BOOT	SECURE_BOOT	REQUIRED	通过

三个 REQUIRED 级别检查全部通过，唯一未通过项是 BAD_KEYSET（密钥集无效）。该项是 AIK 证书登记失败的直接后果，而非用户配置问题；PCR 表与 TCG 日志完整，证明度量启动链路正常。

六、已排除的本地因素

项目	检查结果	结论
安全启动 / UEFI / GPT	均已启用	正常
TPM 启用与所有权	Present / Ready / Enabled / Activated / Owned 均 True	正常
TPM 是否需清除	Clear Needed To Recover = False	无需清除
EK 证书	存在，签发者 CN=CSME ADL PTT 01SVN	正常
证书链（NV）	4 元素，dwErrorStatus=0x10000	签名有效
Windows 缓存错误链	已用 NV 正确链替换（0x10008 → 0x10000）	已修复
BIOS	F.16，HP 当前最新；Windows Update 无固件更新	无更新可用
网络 / 代理 / hosts	无代理、无劫持，返回的是微软真实 404 响应	正常
RSA / ECC 通道	三张 EK 证书（RSA/P256/P384）AKI 完全相同，均 404	无法绕过

项目	检查结果	结论
Intel EK 证书服务	GetEkCertFromWeb 返回 ASN.1 错误	无法换发 EK 证书
清 TPM / 重装系统	EK 证书由 endorsement seed 派生，Clear 不改变；重装仍需同一证书	无效

七、提交给动视支持的工单（中文）

标题：Call of Duty 安全认证失败：Windows AIK 证书登记被微软 AIK 服务以 HTTP 404 拒绝（KeyId 7fd50ee8），非本机配置问题

正文：

问题描述：启动 Call of Duty HQ 后，安全认证向导提示「新密钥生成失败，建议更新 BIOS 固件」；TPM 2.0 与安全启动两项均显示通过。认证向导标记系统为「临时合规状态」，匹配受到限制。

技术定位：COD 需要 Windows 的 AIK 证书来完成 TPM 远程认证。本机执行 certreq -enrollaik 时，微软 AIK 服务在 GetCACaps 阶段返回 HTTP 404：{"Message":"The authority intc-keyid-7fd50ee8ef6f5eb392ded861815e2d49b45c487b.microsoftaik.azure.net does not exist."}（x-ms-request-id: 599dc7f3-48e8-41aa-abf9-f895077c5bf8，错误码 0x80190194）。该请求在 CreateRequest / SubmitRequest 之前即失败，耗时 0 ms，说明服务端未预置该 CA 的 authority，与本地配置无关。

本机状态：TPM Present / Ready For Attestation=True / Is Capable For Attestation=True / Clear Needed To Recover=False；EK 证书存在（签发者 CN=CSME ADL PTT 01SVN，AKI 7FD50EE8…）；ekchainNV 四元素、dwErrorStatus=0x10000（签名有效，仅缺根）；RSA/ECC P256/P384 三张 EK 证书 AKI 相同，改用 ECC 通道同样返回 404；Intel EK 证书服务返回 ASN.1 错误，无法换发。

官方向导报告：diagnostic_info.json 中 9 项检查 8 项通过，三个 REQUIRED 项全部通过，唯一未通过项为 BAD_KEYSET；PCR 表与 TCG 日志完整。

影响范围：该问题自 2026-08 起在 ASUS / MSI / ASRock / 技嘉 / 联想 / HP 多平台、Windows 10/11 多版本上持续出现，Intel 社区与 Microsoft Q&A 均有大量记录。

请求：请协助向微软升级该 AIK authority 预置问题，或为受影响的玩家提供备用认证路径 / 临时豁免，避免玩家因上游服务端配置问题被长期限制游戏功能。

八、Support Ticket Text (English)

Subject: Call of Duty secure attestation fails — Windows AIK enrollment rejected by Microsoft AIK service with HTTP 404 (KeyId 7fd50ee8…), not a local misconfiguration

Summary: On launching Call of Duty HQ, the Secure Attestation wizard reports "New key failed to be generated / BIOS firmware update recommended". TPM 2.0 and Secure Boot both PASS. The system is flagged as temporary compliance and matchmaking is restricted.

Root cause: COD requires a Windows AIK certificate for TPM remote attestation. On this machine, certreq -enrollaik fails at the GetCACaps stage with HTTP 404: {"Message":"The authority intc-keyid-7fd50ee8ef6f5eb392ded861815e2d49b45c487b.microsoftaik.azure.net does not exist."} (x-ms-request-id: 599dc7f3-48e8-41aa-abf9-f895077c5bf8, error 0x80190194). CreateRequest and SubmitRequest both report 0 ms, i.e. the TPM is never used and the failure is entirely server-side.

Local state is healthy: TPM Present, Ready For Attestation = True, Is Capable For Attestation = True, Clear Needed To Recover = False; EK certificate present (issuer CN=CSME ADL PTT 01SVN, AKI 7FD50EE8…); ekchainNV builds a 4-element chain with dwErrorStatus = 0x10000 (signature valid, root only missing). The RSA, ECC P256 and ECC P384 EK certificates share the same AKI, so the ECC enrollment path returns the same 404. Intel's EK certificate service returns an ASN.1 error, so re-issuing an EK certificate is not possible.

Wizard report: diagnostic_info.json shows 8 of 9 checks passing; all three REQUIRED checks pass; the only failing entry is BAD_KEYSET. PCR table and TCG log are complete.

Scope: identical reports since August 2026 across ASUS / MSI / ASRock / Gigabyte / Lenovo / HP platforms and multiple Windows versions; widely documented on Intel Community and Microsoft Q&A.

Request: please escalate the missing AIK authority provisioning to Microsoft, or provide a fallback attestation path / temporary exemption for affected players, so that an upstream service-side configuration gap does not permanently restrict gameplay features.

九、附件与提交方式

- diagnostic_info.json —— COD 安全认证向导导出（9 项检查、PCR 表、TCG 日志）
- certreq_output.txt —— certreq 申请记录（含 x-ms-client-request-id）
- 微软反馈-提交文本.txt / 微软 Q&A-回帖文本.txt —— 给微软的中英文提交材料

提交渠道：动视支持工单（主渠道，附上述两个文件）；微软 Q&A 跟帖；HP 售后备档。

十、本地处置说明

本次排查以只读诊断为主：未清除 TPM、未修改 BIOS、未重装系统、未更换驱动；BitLocker 全程保持加密启用状态，TPM 内的 AIK 私钥未被删除。唯一的持久性改动是将 TPM NV 索引 0x1C00100 中正确的 Intel 中间证书链导入「本地计算机\中间证书颁发机构」，使本机 EK 证书链的信任状态由 0x10008（签名无效）修正为 0x10000（签名有效）。

结论：本地已无可执行的修复手段，需微软在 microsoftaik.azure.net 为 KeyId 7fd50ee8ef6f5eb392ded861815e2d49b45c487b 预置 AIK SCEP authority。