CÂMARA MUNICIPAL DE CANGUÇU
ESTADO DO RIO GRANDE DO SUL

Canguçu, 17 de maio de 2021

Memorando Nº 06/2021

De: Especialista em Informática
Para: Pregoeira

Assunto: Resposta ao recurso encaminhado por Verlin Soluções em TI

Prezada, segue as considerações:

- O requerente afirma que o equipamento ofertado (Lenovo SFF V50s 10100) no item 1 pela empresa Ana Carolina Haack de Castro, não atende as especificações do produto solicitado por esta casa nos seguintes aspectos:

> A – (...) Deverá possuir, integrado a placa mãe do computador (on board), sem adaptações, subsistema de segurança TPM (Trusted Plataform Module) compatível com a norma TPM 1.2 ou superior a especificada pelo TCG (Trusted Computing Group).
>
> B – (...) Deverá possuir Sistema de Controle de intrusão, compatível com o sensor de intrusão do gabinete.

Tendo em vista o prospecto do equipamento ofertado pela empresa Ana Carolina Haack de Castro e anexado a solicitação pelo requerente, considero:

No tocante ao item A, ressaltando que o TPM é um padrão para um processador criptográfico e como mostra o texto abaixo disponibilizado em https://www.minitool.com/, empresa parceira Microsoft, atualmente, existem 5 versões diferentes possíveis para o padrão TPM versão 2.0.

Types of TPM
TPM was conceived by a computer industry consortium named Trusted Computing Group (TCG) and was standardized by ISO and IEC in 2009 as ISO/IEC 11889. TCG has assigned TPM vendor IDs to AMD, IBM, Intel, Lenovo, Samsung, etc. companies.

There are 5 types of TPM 2.0 implementations:

- **Firmware TPM (fTPM):** fTPM is a software-only solution that runs in a CPU's trusted execution environment. So, it is more likely to be vulnerable to software bugs. AMD, Intel, and Qualcomm have implemented fTPMs.

- **Discrete TPM (dTPM):** dTPM is a dedicated chip that implements TPM functionality in their own tamper-resistant semiconductor package. So, it's the

most secure TPM type theoretically because the routines implemented in hardware should be more resistant to bugs compared to routines implemented in software.

- **Software TPM (sTPM):** sTPM is a software emulator of TPM that runs with only a regular program gets within an operating system (OS). It depends completely on the environment that it runs in. therefore, sTPM offers no more security than what can be provided by the normal execution environment; it is vulnerable to its own software bugs and attacks that are penetrating the normal execution environment. Yet, sTPM is useful for development purposes.

- **Integrated TPM (iTPM):** iTPM is a part of another chip. It uses hardware that resists software bugs, so it isn't required to implement tamper resistance. Intel includes iTPMs in some of its chipsets.

- **Hypervisor TPM (hTPM):** hTPM is a kind of virtual TPM provided by and rely on hypervisors. The hypervisor is an isolated execution environment that is hidden from the software running inside virtual machines to secure their code from the software in the virtual machines. hTPM can offer a security level similar to a fTPM.

Com atenção ao documento anexado, o mesmo mostra a existência de firmware TPM (fTPM) na versão 2.0 da norma de especificação e integrado ao chipset do equipamento (iTPM). Nesse sentido, está solução não apresenta chip dedicado para este propósito e integrado a placa-mãe, sem adaptações, NÃO estando, portanto, em conformidade com o solicitado em edital;

Com relação ao item B, segundo o prospecto anexado, o equipamento ofertado pela empresa Ana Carolina Haack de Castro, NÃO disponibiliza o dispositivo de intrusão de gabinete solicitado em edital, portanto, estando em desconformidade com o mesmo.

Atenciosamente.

André Marcelo Coelho da Silva
Especialista em Informática