
**ILUSTRÍSSIMO SENHOR PREGOEIRO DESIGNADO PELO TRIBUNAL REGIONAL
ELEITORAL DO ESTADO DO RIO GRANDE DO NORTE, PARA O PREGÃO
ELETRÔNICO DE Nº.: 030/2020-TRE-RN**

CINTE TELECOM COMÉRCIO E SERVIÇOS LTDA, pessoa jurídica de direito privado, com sede na rua Doutor Lauro Pinto, nº 610, Lagoa Nova, Natal/RN, CEP.: 59.064-250, inscrita no CNPJ/MF de nº 08.378.641/0001-96, vem, à presença de Vossa Senhoria, conforme intenção demonstra durante a sessão do Pregão Eletrônico supra referido, apresentar **RECURSO** contra a empresa **INTERJATO SERVIÇOS DE TELECOMUNICAÇÕES LTDA**, nos termos que abaixo seguem.

Nos termos do edital de nº.: 30/2020-TRE/RN, o objeto licitado foi dividido em cinco itens, estando os itens de 1 a 4 reunidos em um único lote, e o item 5, em separado, que correspondia ao enlace dedicado 10 Gigabit (COJE), conforme especificações contidas no Termo de Referência.

Pois bem.

Conforme disposto no Termo de Referência e no Edital, o item cinco (5) deveria atender às seguintes especificações:

1.3.1.19. Quanto ao link metropolitano (COJE): 1.3.1.19.1. O equipamento CPE deste deverá ter uma capacidade de pelo menos 10Gbps em túnel IPSec;

1.3.1.19.2. Em caso de utilização de enlace dedicado fisicamente (fibra apagada) entre o COJE e a secretaria do TRE-RN), não há necessidade de utilização de IPSec, sendo ainda de responsabilidade da CONTRATADA implementar medidas que garantam a segurança do enlace, não permitindo

interceptação, como MACSec, ou tecnologia equivalente.

1.3.1.19.3. O equipamento deverá ter porta SFP+, com os devidos cabos SFP+, compatíveis com os switches do TRE-RN, tanto no lado da CPE, quanto no lado da secretaria, em caso de utilização de fibra apagada.

Como forma de tentar atender ao requisito imposto pelo Edital, a empresa licitante Recorrida informou em seu projeto que a unidade receberá dois switches CPE Huawei S5720-28X-LI-AC para a integração da rede local com a rede de dados, cujos enlaces serão recebidos por fibra apagada, usando protocolo de segurança MACSec.

Salienta-se que o Protocolo de Segurança MACSec uma vez habilitado em um link Ethernet ponto-a-ponto, todo o tráfego que atravessa este *link* passa por verificação de integridade de dados e, se for configurado, criptografado, o MACsec é capaz de identificar e impedir a maioria das ameaças à segurança, incluindo negação de serviço, invasão, intermediário, mascaramento, escutas telefônicas passivas e ataques de reprodução.

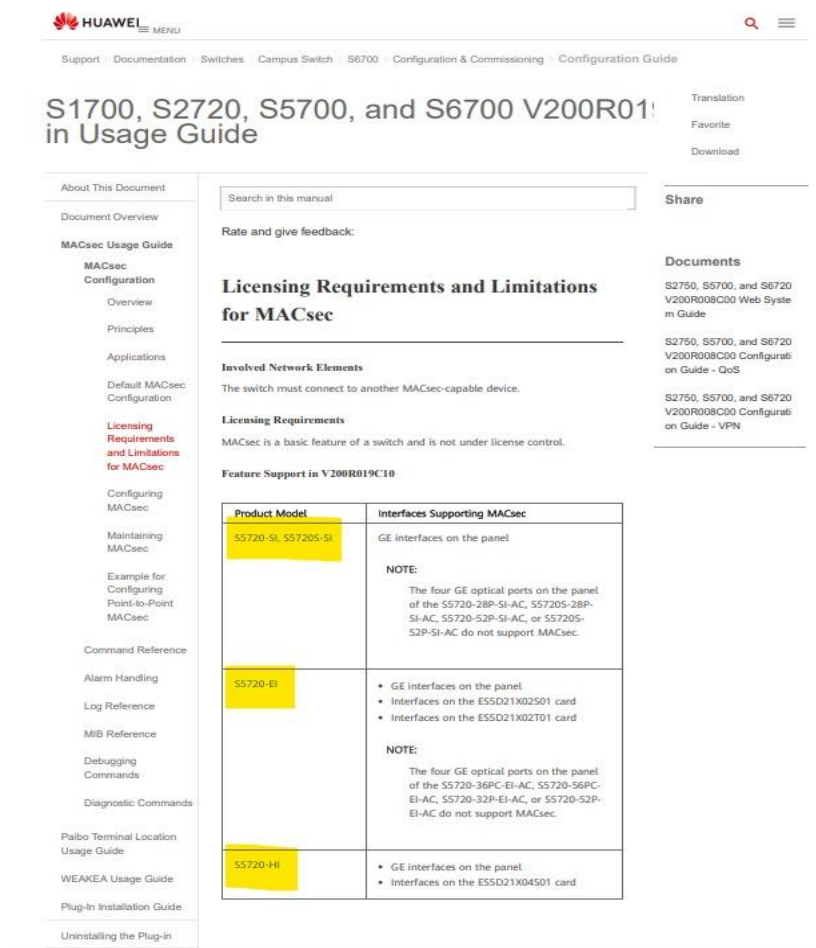
De acordo com a página 1 do documento *Licensing Requirements and Limitations for MACsec - S1700, S2720, S5700, and S6700 V200R019C10 Plug-in Usage Guide - Huawei*, anexo a este Recurso, o MACSec é um protocolo de *peering*, ou seja, precisa ser habilitado e configurado nas **duas** bordas do *link* ponto-a-ponto para que seja efetivo. Os equipamentos instalados tanto na Secretaria do TRE/RN como no COJE devem suportar e implementar MACSec, sob pena de não atendimento ao que se requer no Edital.

A licitante Recorrida definiu como switch concentrador o Huawei S5720-28x-SI-AC e como switch CPE (a ser instalado no COJE) o modelo Huawei S5720-28x-LI-AC. Apesar de serem do mesmo fabricante, o modelo **S5720-28x-LI-AC** não suporta MACSec e, como dito anteriormente, para utilização do protocolo MACSec é necessário que os equipamentos em ambas as bordas do *link* suportem o referido protocolo de segurança.

Desta forma, resta caracterizado o completo descumprimento do item 1.3.1.19.2. do termo de referência. O documento *Licensing Requirements and Limitations for MACsec - S1700, S2720, S5700, and S6700 V200R019C10 Plug-in Usage Guide - Huawei*¹, lista todos os

¹ Disponível em: <https://support.huawei.com/enterprise/en/doc/EDOC1100126488/6f7c2df0/licensing-requirements-and-limitations-for-macsec> Acesso em: 08 de julho de 2020.

equipamentos da série S5700 que dão suporte ao MACSec, sendo de fácil verificação a ausência do modelo S5720-28x-LI-AC neste documento da fabricante, o que denota a certeza da impossibilidade de implementação do MACSec e consequente descumprimento das normas e exigências editalícias. Anexa-se a este Recurso o referido documento.



The screenshot shows the Huawei documentation page for the S1700, S2720, S5700, and S6700 V200R011 in Usage Guide. The page is titled "S1700, S2720, S5700, and S6700 V200R011 in Usage Guide" and includes a search bar, a navigation menu, and a table of contents. The table of contents lists various sections such as "About This Document", "Document Overview", "MACsec Usage Guide", "Configuration", "Principles", "Applications", "Default MACsec Configuration", "Licensing Requirements and Limitations for MACsec", "Configuring MACsec", "Maintaining MACsec", "Example for Configuring Point-to-Point MACsec", "Command Reference", "Alarm Handling", "Log Reference", "MIB Reference", "Debugging Commands", "Diagnostic Commands", "Patbo Terminal Location Usage Guide", "WEAKEY Usage Guide", "Plug-In Installation Guide", and "Uninstalling the Plug-In".

Licensing Requirements and Limitations for MACsec

Involved Network Elements

The switch must connect to another MACsec-capable device.

Licensing Requirements

MACsec is a basic feature of a switch and is not under license control.

Feature Support in V200R019C10

Product Model	Interfaces Supporting MACsec
S5720-SI, S5720S-SI	<p>GE interfaces on the panel</p> <p>NOTE:</p> <p>The four GE optical ports on the panel of the S5720-28P-SI-AC, S5720S-28P-SI-AC, S5720-52P-SI-AC, or S5720S-52P-SI-AC do not support MACsec.</p>
S5720-EI	<ul style="list-style-type: none"> GE interfaces on the panel Interfaces on the ESSD21X02501 card Interfaces on the ESSD21X02T01 card <p>NOTE:</p> <p>The four GE optical ports on the panel of the S5720-36PC-EI-AC, S5720-56PC-EI-AC, S5720-32P-EI-AC, or S5720-52P-EI-AC do not support MACsec.</p>
S5720-HI	<ul style="list-style-type: none"> GE interfaces on the panel Interfaces on the ESSD21X04501 card



<p>HUAWEI</p>		<p>• GE and XGE interfaces on the panel</p> <p>• Interfaces on the ESSD21X08500 card</p> <p>NOTE:</p> <p>The four XGE optical interfaces on the panel of the S5730-44C-HI, S5730-44C-PWH-HI, S5730-44C-HI-24S, S5730-68C-HI, S5730-68C-PWH-HI, or S5730-68C-HI-48S do not support MACsec.</p>	<p>Translation</p> <p>Favorite</p> <p>Download</p> <p>Share</p>
S5731-HI		Interfaces on the S7X08000 card	
S5731S-H24T4XC-A, S5731S-H48T4XC-A		Interfaces on the S7X08000 card	
S5732-H24UM2CC, S5732-H48UM2CC		<p>• 25GE/40GE/100GE interfaces on the panel</p> <p>• Interfaces on the S7X08000 card</p> <p>• Interfaces on the S7Y08000 card</p>	
S5720-SI		Interfaces on the ESSD21X04501 card	
S5720-EI		<p>• Interfaces on the ESSD21X08500 card</p> <p>• Interfaces on the ESSD21X04501 card</p>	

Feature Limitations

- For the S7X08000 and S7Y08000 cards:
 - When MACsec is enabled on an interface, the actual maximum frame length allowed by this interface is the value specified by the **jumboframe enable** value command plus 32. When MACsec is disabled on an interface, the actual maximum frame length allowed by this interface is restored to the value specified by the **jumboframe enable** value command.
 - When MACsec is enabled on an interface and MACsec frame headers are not configured to contain an SCL, the maximum length of original packets (packets that are not encrypted by MACsec) that are allowed to pass through the interface is the value specified by the **jumboframe enable** value command plus 8 bytes.
- MACsec cannot be configured when an interface works in half-duplex mode, or the **auto duplex half** or **duplex half** command is executed on an interface, or a copper module is installed on an interface.
- After MACsec is configured on an interface:
 - MACsec fails if the local and peer interfaces work in half-duplex mode through negotiation.
 - MACsec configuration is cleared if a copper module is installed.
- If remote loopback is configured on an MACsec-enabled interface, MKA packets are looped on the peer device, causing an MKA session timeout. The MACsec function becomes invalid. Therefore, before configuring remote loopback on an interface, disable MACsec on it.
- Two devices are connected and MACsec is deployed on both devices. If a transparent transmission device is deployed between the two devices, deleting

Além disso, comparando os documentos Huawei S5720-SI Series Switches Brochure.pdf e Huawei S5720-LI Series Switches Brochure.pdf, é possível identificar que o modelo S5720-28x-SI suporta MACSec, mas o modelo S5720-28x-LI-AC não. A autenticidade do documento pode ser verificada a partir do QR Code ao lado.

Ademais, o que está descrito nos documentos do fabricante como MAC *address table* ou MAC address *authentication* nada tem a ver como a tecnologia MACSec, pois o primeiro trata de um IEEE 802.1X que é um padrão IEEE² para controle de acesso à rede com base em portas. O modo EAP do WPA e do WPA2 utiliza autenticação 802.1X em vez de chaves PSK, o que permite a possibilidade de dar a cada usuário ou cliente as suas próprias credenciais de *login*: nome de usuário e senha e/ou certificado digital. O MACsec, por seu turno, é utilizado para fornecer criptografia dos

² A rede IEEE possui como principal característica transmitir sinal sem fio através de ondas.

dados trafegados entre um meio físico e um meio lógico, bem como detectar, analisar e bloquear acessos indevidos e/ou externos à rede, quando for caso, tendo ainda a possibilidade de criptografar estes dados passantes de forma ativa e inteligente. Em comum com IPsec, tecnologia equivalente, o MACsec define uma infraestrutura de segurança para fornecer confidencialidade e integridade de dados e autenticação da origem dos dados. Como dito acima e frisa-se agora, o MACSec é um protocolo de *peering*, ou seja, precisa ser habilitado e configurado nas **duas** bordas do *link* ponto-a-ponto para que tal protocolo de segurança funcione, estando errado o projeto apresentado pela Recorrida por não cumprir os requisitos editalícios exigidos pela Administração.

É necessária a expertise mínima para a assunção de projetos técnicos como o que está sendo licitado, sob pena de levar a Administração a perigos técnicos imensuráveis. No caso, o não atendimento de critérios técnicos como esse põe em risco a segurança de dados da Administração. É cediço o entendimento de que falhas nos projetos levam à inabilitação da licitante, conforme se detrai da jurisprudência abaixo:

APELAÇÃO CÍVEL - AÇÃO ORDINÁRIA E CAUTELAR - LICITAÇÃO - HABILITAÇÃO TÉCNICA - PROPOSTA COMERCIAL - INVIABILIDADE - JULGAMENTO ANTECIPADO DA LIDE - Alegado prejuízo quanto à demonstração da exequibilidade do objeto da licitação. 1- O julgamento antecipado da lide é previsto no artigo 330, inciso I, que, conjugado com o [artigo 427 ambos do Código de Processo Civil](#), facultam ao magistrado dispensar a realização da perícia, desde que outros elementos técnicos encontrem-se disponíveis nos autos e sejam suficientes ao julgamento da matéria controvertida, razão pela qual se afasta a preliminar de cerceamento do direito de defesa. 2- Evidenciado que o objeto do certame, diferentemente do entendimento declinado pelo juízo a quo, comporta também a operação de sistema de bilhetagem eletrônica, além do serviço de transporte urbano municipal pelo segundo apelado, conforme projeto básico, que possui o poder de vincular tanto o poder concedente quanto os licitantes. **3- A falta de demonstração dos requisitos editalícios para a proposta técnica de qualquer dos licitantes é razão suficiente para a inabilitação da mesma ao certame.** 4[...]- Diante da constatação do não atendimento pelo consórcio licitante, aos requisitos mínimos dispostos no instrumento de chamamento do certame, bem como à inexecuibilidade da proposta apresentada, impõe-se a reforma do ato

objurgado para reconhecer a desclassificação da mesma, bem como sua impraticabilidade, nos termos do [artigo 48, incisos I e II da Lei 8.666/1993](#).
Apelação conhecida e provida. (TJGO - AC 201390711455 - 6ª C.Cív. - Rel. Des. Fausto Moreira Diniz - DJe 30.11.2015 - p. 434)

Assim, diante do descumprimento de critérios técnicos e a apresentação de proposta técnica/projeto falho, não alinhado aos requisitos do Edital, requer-se a inabilitação da empresa Recorrida e as medidas de estilo para a continuidade da licitação no que tange ao item 05 do Edital.

Nestes termos, CONFIA deferimento.

Natal, 10 de julho de 2020.



CINTE TELECOM COMÉRCIO E SERVIÇOS LTDA

CNPJ/MF de nº 08.378.641/0001-96