IBM BRASIL - Indústria, Máquinas e Serviços Ltda.
Av. Avenida República do Chile, nº 330, 11º e 12º andares, Bloco 1 - Salas 1101 e 1201 e Bloco 2 – Salas 1101 e 1201, Rio de Janeiro – RJ
CEP 20031-170
Internet: WWW.IBM.COM.BR
CNPJ: 33.372.251/0001-56

São Paulo, 17 de novembro de 2022

À

PROCEMPA - Companhia de Processamento de Dados de Porto Alegre

DECLARAÇÃO

A IBM Brasil Indústria, Máquinas e Serviços Ltda, inscrita no CNPJ n. 33.372.251/0001-56, declara o produto descrito abaixo, faz parte da família FlashSystem do qual faz uso do microcódigo (ou software) chamado Spectrum Virtualize e que a partir de dezembro de 2022, quando estará disponível uma nova versão, todos os modelos da família FlashSystem que fazem uso do referido microcódigo, passam a suportar a criação de até 32.000 (trinta e dois mil) snapshots por sistema. Este novo release do microcódigo Spectrum Virtualize, previsto para dezembro de 2022 será compatível com os modelos descritos nesta declaração e não possuem nenhum custo adicional para os usuários ou clientes que possuem equipamentos em garantia ou em contratos de manutenção. Possíveis atrasos podem ocorrer sem prévio aviso.

Produto	Descrição
4657924	IBM FlashSystem 7300

Esta declaração é válida por 60 (sessenta) dias a contar da data de emissão acima.

Atenciosamente,

e-Signed by FABRICIO LIRA DA SILVA
on 2022-11-17

Fabricio Lira da Silva
Ecosystem Director
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

IBM BRASIL - Indústria, Máquinas e Serviços Ltda.

Av. Avenida República do Chile, nº 330, 11º e 12º andares, Bloco 1 - Salas 1101 e 1201 e Bloco 2 – Salas 1101 e 1201, Rio de Janeiro – RJ

CEP 20031-170

Internet: WWW.IBM.COM.BR

CNPJ: 33.372.251/0001-56

São Paulo, 17 de novembro de 2022

À
COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

DECLARAÇÃO

A IBM Brasil - Indústria, Máquinas e Serviços Ltda., inscrita no CNPJ nº 33.372.251/0001-56, declara que os produtos IBM abaixo citados, ofertados pela IBM para o revendedor oficial IBM, O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA ,inscrita no CNPJ nº. 08.706.548/0001-63 ,são novos, sem uso anterior e estão em linha normal de produção ou em regime de OEM. Entretanto, o revendedor oficial IBM deverá confirmar se o produto que está ofertando para seu Cliente final, em cada caso específico, também é novo e sem uso anterior.

Produto	Descrição
4657924	FlashSystem 7300

Esta declaração é válida por 60 (sessenta) dias.

Atenciosamente,

e-Signed by FABRICIO LIRA DA SILVA
on 2022-11-17

Fabricio Lira
Ecosystem Director
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

IBM BRASIL - Indústria, Máquinas e Serviços Ltda.

Av. Avenida República do Chile, nº 330, 11º e 12º andares, Bloco 1 - Salas 1101 e 1201 e Bloco 2 – Salas 1101 e 1201, Rio de Janeiro – RJ

CEP 20031-170

Internet: WWW.IBM.COM.BR

CNPJ: 33.372.251/0001-56

São Paulo, 17 de novembro de 2022

À

COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

DECLARAÇÃO

A IBM Brasil - Indústria, Máquinas e Serviços Ltda., inscrita no CNPJ nº 33.372.251/0001-56, declara que os produtos IBM abaixo citados, ofertados pela IBM para o revendedor oficial IBM, O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA inscrita no CNPJ nº. 08.706.548/0001-63 são novos, sem uso anterior e estão em linha normal de produção. Entretanto, o revendedor oficial IBM deverá confirmar se o produto que está ofertando para seu Cliente final, em cada caso específico, também é novo e sem uso anterior.

Produto	Descrição
4657924	FlashSystem 7300

Esta declaração é válida por 60 (sessenta) dias.

Atenciosamente,

e-Signed by FABRICIO LIRA DA SILVA
on 2022-11-17

Fabricio Lira
Ecosystem Director
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

IBM BRASIL - Indústria, Máquinas e Serviços Ltda.
Av. Avenida República do Chile, nº 330, 11º e 12º andares, Bloco 1 - Salas 1101 e 1201 e Bloco 2 – Salas 1101 e 1201, Rio de Janeiro – RJ
CEP 20031-170
Internet: WWW.IBM.COM.BR
CNPJ: 33.372.251/0001-56

São Paulo, 17 de novembro de 2022

À

COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

DECLARAÇÃO

A IBM Brasil - Indústria, Máquinas e Serviços Ltda., inscrita no CNPJ nº 33.372.251/0001-56, declara que a empresa O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA inscrita no CNPJ nº. 08.706.548/0001-63 localizada na AV RIO BRANCO 1, n001, SAL 2005, Rio de Janeiro, RIO DE JANEIRO ,celebrou Contrato IBM Business Partner de Parceria Comercial – Revenda, número 631-EEAF7EE02696C6A0 em 20/06/2017 (vinte de junho de dois mil e dezessete) com a IBM Brasil - Indústria, Máquinas e Serviços Ltda., estando apta a comercializar o (s) produto(s) Storage Categoria(s) :1, 2 e 3)

Esta declaração é válida por 60 (sessenta) dias.

Atenciosamente,

e-Signed by FABRICIO LIRA DA SILVA
on 2022-11-17

Fabricio Lira
Ecosystem Director
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

IBM BRASIL - Indústria, Máquinas e Serviços Ltda.
Av. Avenida República do Chile, nº 330, 11º e 12º andares, Bloco 1 - Salas 1101 e 1201 e Bloco 2 – Salas 1101 e 1201, Rio de Janeiro – RJ
CEP 20031-170
Internet: WWW.IBM.COM.BR
CNPJ: 33.372.251/0001-56

São Paulo, 17 de novembro de 2022

À

PROCEMPA - Companhia de Processamento de Dados de Porto Alegre

DECLARAÇÃO

A IBM Brasil Indústria, Máquinas e Serviços Ltda, inscrita no CNPJ n. 33.372.251/0001-56, declara o produto descrito abaixo, faz parte da família FlashSystem do qual faz uso do microcódigo (ou software) chamado Spectrum Virtualize e que a partir de dezembro de 2022, quando estará disponível uma nova versão, todos os modelos da família FlashSystem que fazem uso do referido microcódigo, passam a suportar a criação de até 32.000 (trinta e dois mil) snapshots por sistema. Este novo release do microcódigo Spectrum Virtualize, previsto para dezembro de 2022 será compatível com os modelos descritos nesta declaração e não possuem nenhum custo adicional para os usuários ou clientes que possuem equipamentos em garantia ou em contratos de manutenção. Possíveis atrasos podem ocorrer sem prévio aviso.

Produto	Descrição
4657924	IBM FlashSystem 7300

Esta declaração é válida por 60 (sessenta) dias a contar da data de emissão acima.

Atenciosamente,

e-Signed by FABRICIO LIRA DA SILVA
on 2022-11-17

Fabricio Lira da Silva
Ecosystem Director
IBM Brasil - Indústria, Máquinas e Serviços Ltda.

SERVIÇO REGISTRAL - RIO DE JANEIRO - CAPITAL

FINALIDADE EXCLUSIVA declarada pelo requerente:

CONCORRENCIA.

07/10/2022>12/10/2022 [2]

20221031512572-001/001

Ato: 20221034914775

1º Oficio do Registro de Distribuição

RUA DO OUVIDOR, 63 - 2º ANDAR - CENTRO - RJ

Delegatário: Lélio Gabriel Heliodoro dos Santos

CERTIDÃO DE REGISTRO DE DISTRIBUIÇÃO DE FEITOS AJUIZADOS

O REGISTRADOR DO 1º OFICIO DO REGISTRO DE DISTRIBUIÇÃO DA CIDADE E COMARCA DO RIO DE JANEIRO, CAPITAL DO ESTADO DO RIO DE JANEIRO.

C E R T I F I C A

com referência aos assuntos abaixo mencionados, e DÁ FÉ QUE, revendo em seu poder e Serviço os livros e/ou assentamentos das distribuições em curso ou andamento relativos a:

A) FALÊNCIAS, CONCORDATAS, INSOLVÊNCIAS E RECUPERAÇÕES JUDICIAIS DISTRIBUIDAS A UMA DAS VARAS EMPRESARIAIS.

DESDE QUATRO DE OUTUBRO DE DOIS MIL E DOIS ATÉ QUATRO DE OUTUBRO DE DOI S MIL E VINTE E DOIS(04/10/2002 ATÉ 04/10/2022), dele(s)**********

_*_*_*_*_*_*_*_*_NADA_CONSTA_*_*_*_*_*_*_*_

Relativamente ao nome de O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA - CNPJ: 08.706.548/0001-63**********

Rio de Janeiro, Capital em 10/10/2022. QUALIFICAÇÃO conf. o requerido. Emolumentos Tab.01. Ato 01: R$ 47,84, Tab.04-Ato 08: R$ 49,30, LEI 6.37 0 Art.2 §4: R$ 0,98, FETJ: R$ 19,42, FUNDPERJ: R$ 4,85, FUNPERJ: R$ 4,8 5, FUNARPEN: R$ 3,88, ISS: R$ 5,16. TOTAL: R$ 136,28. EU, RICARDO DA CO STA MEIRELES (Mat.94/1867),Oficial Substituto a assino digitalmente.

CERTIDÃO ESPECIAL - (ART.21, § 1°, IV CNCGJERJ)
ESTA CERTIDÃO REFERE-SE ÚNICA E
EXCLUSIVAMENTE AO ASSUNTO REQUERIDO.

Poder Judiciário - TJERJ
Corregedoria Geral da Justiça
EEHQ 42819 PRF
Consulte a validade do selo em:
https://www3.tjrj.jus.br/sitepublico

- Esta certidão eletrônica estará disponível para download e validação no Portal Extrajudicial da Corregedoria Geral da Justiça (acesso pela página do TJRJ/Corregedoria/Extrajudicial/Portal Extrajudicial) pelo período de 90 (noventa) dias após a sua emissão.

CERP: CDF95A4F-C103-4E3D-92F8-2653DFADABB6

Senhor usuário, se necessário, é possível obter certidão que abranja outros períodos de consulta para além do pesquisado. Informe-se com o cartório do distribuidor.

2o. Ofício do Registro de Distribuição

RUA DA ASSEMBLÉIA, 19 - 7o. ANDAR - CEP 20011-020

CERP: 2cc6048f-de5d-4040-8705-d9e9854315d2

REQUERIDA EM: 07/10/2022 **914776**

00/33 Pag: 0001

MODELO(C)>> CERTIFICA A a B <<

PARA FINS DE: CONCORRÊNCIA E LICIT

Jorge Constancio Cassas - Responsável pelo Expediente

CERTIDÃO DE REGISTRO DE DISTRIBUIÇÃO DE FEITOS AJUIZADOS

O REGISTRADOR DO 2o. OFÍCIO DO REGISTRO DE DISTRIBUIÇÃO DA CIDADE E COMARCA DO RIO DE JANEIRO, CAPITAL DO ESTADO DO RIO DE JANEIRO.

C E R T I F I C A e D Á F É

QUE REVENDO OS LIVROS E ASSENTAMENTOS DAS DISTRIBUIÇÕES EM CURSO OU ANDAMENTO SOBRE:

A - Ações de Falência ou Concordata distribuídas as Varas Competentes, bem como, Inquéritos Judiciais Falimentares ou Falências Dolosas as Varas Criminais ou outras (art.186 da Lei de Falências), Recuperações Judiciais;

B - Interdições previstas pela Lei no. 6024 desde 13/03/1974, que trata da intervenção e Liquidação Extrajudicial de Instituições Financeiras pelo Banco Central,do Brasil ou Ministério da Fazenda, desde:

QUATRO DE OUTUBRO DE DOIS MIL E DOIS ATÉ QUATRO DE OUTUBRO DE DOIS MIL E VINTE E DOIS (04/10/2002 a 04/10/2022) dele(s).-

.-.-.-.-.-.-.-.NADA CONSTA.-.-.-.-.-.-.-

Relativamente ao Nome de O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA Qualificação: 08706548000163 (conforme requerido).-.-.-.-.-.-.-.-.-.-

EMITIDA EM: 10/10/2022, RIO DE JANEIRO, COMARCA DA CAPITAL

EU REGISTRADOR ASSINO. **T O T A L R$: 136.28**

EMOL R$: 97.14 - PMCMV(2%)R$: 0.98 - FETJ(20%)R$: 19.42 - FUNDPERJ(5%)R$: 4.85 - FUNPERJ(5%)R$: 4.85 - FUNARPEN(4%)R$: 3.88 - ISS(5%)R$: 5.16

Senhor usuário, se necessário, é possível obter certidão que abranja outros períodos de consulta para além do pesquisado. Informe-se com o cartório do distribuidor.

Poder Judiciário - TJERJ
Corregedoria Geral de Justiça
Selo de Fiscalização Eletrônico
EEGZ54589-KQZ
Consulte a validade do selo em:
https://www3.tjrj.jus.br/sitepublico

Esta certidão eletrônica estará disponível para download e validação no Portal Exrtajudicial (acesso pela página do TJRJ/Corregedoria/Extrajudicial/Portal Extrajudicial) pelo período de 90 (noventa) dias após sua emissão.

Requerida em 07/10/2022

Finalidade declarada CONCORRÊNCIA / LICITAÇÃO

8360636/2022-1.00

Modelo ESPECIAL folha 01

0903321943

3º Ofício de Registro de Distribuição da Capital

Av. Erasmo Braga, 227 - Grupo 201 - CEP: 20020-902

CERTIDÃO DO REGISTRO DE DISTRIBUIÇÃO DE FEITOS AJUIZADOS

CERP: 02a14552-5399-4fe3-be13-2e15473ed2f4

Esta certidão eletrônica estará disponível para download e validação no Portal Extrajudicial da Corregedoria Geral da Justiça(acesso pela página do TJRJ / Corregedoria / Extrajudicial / Portal Extrajudicial) pelo período de 90(noventa) dias após a sua emissão.

O REGISTRADOR DO 3º OFÍCIO DE REGISTRO DE DISTRIBUIÇÃO DA CIDADE DO RIO DE JANEIRO CAPITAL DO ESTADO DO RIO DE JANEIRO, AO VERIFICAR OS LIVROS E/OU ASSENTAMENTOS DE SEU OFÍCIO RELATIVOS A FEITOS EM ANDAMENTO NO PERÍODO REQUERIDO E NO QUE CONCERNE AOS ASSUNTOS ABAIXO DISCRIMINADOS, CERTIFICA E DÁ FÉ

a) Falências, Concordatas, Recuperações Judiciais e demais ações e precatórias distribuídas às varas com competência Empresarial;
b) Inventários, testamentos, arrolamentos, arrecadações, administrações provisórias, tutelas, interdições, curatelas, declarações de ausência e outras ações e precatórias distribuídas às varas com competência em Órfãos e Sucessões;
c) Ações distribuídas às Varas da Infância, da Juventude e do Idoso mencionadas nos parágrafos 1° e 3º do artigo 33 da Consolidação Normativa da CGJ, desde
QUATRO DE OUTUBRO DE DOIS MIL E DOIS ate QUATRO DE OUTUBRO DE DOIS MIL E VINTE E DOIS (04/10/2002 ate 04/10/2022) deles **NADA CONSTA** contra o nome de: **O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA**, qualificacao: CNPJ 08.706.548/0001-63 (conforme requerido)
Emitida em: 07/10/2022 Rio de Janeiro, RJ. OBS: Demais requisitos obrigatórios previstos na Lei 11.971/09: NÃO CONSTAM.
EMOLUMENTOS R$ 97,23 (Tab1, Ato1 e Tab4, Ato8) + R$ 0.98 (Lei 6.370/2012) + R$ 19.42 (FETJ) + R$ 4.85 (FUNDPERJ) + R$ 4.85 (FUNPERJ) + R$ 3.88 (FUNARPEN) + R$ 5.16 (LEI 7128/2015) valor total R$ 136,28
"Senhor usuário, se necessário, é possível obter certidão que abranja outros períodos de consulta para além do pesquisado. Informe-se com o cartório do distribuidor."

Poder Judiciário - TJERJ
Corregedoria Geral da Justiça
Selo de Fiscalização Eletrônico
EEHB68564 HKW
Consulte a validade do selo em:
https://www3.tjrj.jus.br/sitepublico

Cert. Proc. p/ /POSSEBON

3º Ofício de Registro de Distribuição da Capital

Av. Erasmo Braga, 227 - Grupo 201 - CEP: 20020-902
CNPJ: 27.532.571/0001-23
Contatos: (21) 2262-9543 | E-mail: 3ord@3ord.com.br

DATA DA CERTIDÃO: 07/10/2022 **RECIBO: 615414/2022** **FUNCIONARIO: POSSEBON**

Nº SEDE: 0903321943 | 8360636/2022 **Nº E-CARTORIO: 20221031512572**

Valores detalhados do Ato

Nº ATO	SELO	SERVIÇO	EMOLUMENTOS	LEI 6.370/2012	FETJ	FUNDPERJ	FUNPERJ	FUNARPEN	LEI 7.128/2015
20221034914777	EEHB 068564 HKW	C	R$ 97,14	R$ 0,98	R$ 19,42	R$ 4,85	R$ 4,85	R$ 3,88	R$ 5,16

Valor Certidão: R$ 136,28

4º Ofício do Registro de Distribuição

CERTIDÃO MODELO ESPECIAL DE FALÊNCIA

DESTINA-SE EXCLUSIVAMENTE À CONCORRENCIA E LICITACAO

20221034914778

Emolumentos:Tab 16 Item 01 R$47,84Tab 19 Item 08 R$49,30 (FETJ) R$:19,42 (FUNPERJ) R$:4,85 (FUNDPERJ) R$:4,85 (FUNARPEN) R$:3,88 (CG - PORTARIA 17/13) R$:0,98 (I.S.S.Q.N.) R$:5,16 = Total R$:136,28

4º Ofício do Registro de Distribuição

Rua do Carmo, 8 - 3º andar

Hermes Valverde da Cunha Vasconcellos Filho — Titular

Hermes Valverde da Cunha Vasconcellos Netto — Substituto do Titular

O OFICIAL REGISTRADOR DO 4º OFÍCIO DO REGISTRO DE DISTRIBUIÇÃO DA CIDADE DO RIO DE JANEIRO, CAPITAL DO ESTADO DO RIO DE JANEIRO, NOMEADO NA FORMA DA LEI,

RAFAELLL
(0)
07/10/2022

C E R T I F I C A

folha: 1
10:29:00
EHL43620

e DÁ FÉ QUE, ao verificar os livros e/ou assentamentos de seu Serviço Registral, relativos a feitos em curso ou andamento, no periodo requerido, no que concerne aos assuntos abaixo:

I - Ações de FALÊNCIAS, CONCORDATAS, RECUPERAÇÕES JUDICIAIS e demais ações e precatórias distribuídas às varas com competência Empresariais;

II - Inqueritos Judiciais Falimentares ou falências dolosas as varas criminais ou outras (art. 186 da Lei de Falências);

III - INTERDIÇÃO e/ou INDISPONIBILIDADE de BENS, previstas pela lei nº 6024 de 13/03/1974, que trada da intervenção e liquidação extrajudicial de instituições financeiras pelo Banco Central do Brasil ou Ministerio da Fazenda;

IV - INVENTÁRIOS, TESTAMENTOS, ARROLAMENTOS, ARRECADAÇÕES, ADMINISTRAÇÕES PROVISÓRIAS, TUTELAS, INTERDIÇÕES, CURATELAS, DECLARAÇÕES de AUSÊNCIA e outras ações e precatórias distribuídas às varas com competência em Órfãos e Sucessões afetos a este Ofício;

V - Ações distribuídas às varas da infância, da juventude e do idoso, mencionadas no parágrafo primeiro e terceiro do artigo 33 desta Consolidação, desde:

SEIS DE OUTUBRO DE DOIS MIL E DOIS xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx ate SEIS DE OUTUBRO DE DOIS MIL E VINTE E DOIS xxxxxxxxxxxxxxxxxxxxxxxxxxx
que dele (s) NADA CONSTA contra o (s) nome (s) de
O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
CNPJ:08.706.548/0001-63//
REQUERIDA E EMITIDA EM 07/10/2022,RIO DE JANEIRO.//////////////////////
FINALIDADE DECLARADA PELO REQUERENTE:CONCORRENCIA E LICITACAO.////////

DOCUMENTO EMITIDO POR PROCESSAMENTO ELETRÔNICO. QUALQUER EMENDA OU RASURA SERÁ CONSIDERADA COMO INDÍCIO DE ADULTERAÇÃO OU TENTATIVA DE FRAUDE.

Poder Judiciário - TJERJ
Corregedoria Geral da Justiça
Selo de Fiscalização Eletrônico
EEHL43620 WMK
Consulte a validade do selo em:
https://www3.tjrj.jus.br/sitepublico

Esta certidão eletrônica estará disponível para download e validação no Portal Extrajudicial da Corregedoria Geral da Justiça (acesso pela página do TJRJ /Corregedoria/Extrajudicial/Portal Extrajudicial) pelo período de 90 (noventa) dias após a sua emissão.

Senhor usuário, se necessário, é possível obter certidão que abranja outros períodos de consulta para além do pesquisado. Informe-se com o cartório do distribuidor.

9222809466473001

CERP: 85fe618f-707f-475f-8f48-6541f7fc27be

CONFERIDO POR:FABIO

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DO ESPÍRITO SANTO
R. Des. Homero Mafra, 60 Enseada do Suá, Vitória - ES | CEP: 29.050-275 | Tel: (27) 3334-2000.

CERTIDÃO NEGATIVA DE PRIMEIRA INSTÂNCIA
NATUREZA DE RECUPERAÇÃO JUDICIAL E EXTRAJUDICIAL (FALÊNCIA E CONCORDATA)

Dados da Certidão

Razão Social: O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA

CNPJ:	08.706.548/0003-25		
Data de Expedição:	31/10/2022 11:29:25	**Validade:**	30 DIAS
N° da Certidão:	**** 2021007242 ****		
-- ENDEREÇO --			
Município:	SERRA	**Bairro:**	JACUHY
Logradouro:	ROD GOVERNADOR MARIO COVAS	**Número:**	KM279
Complemento:	*- NÃO INFORMADO -*	**CEP:**	29.161-230
-- CONTATO --			
Email:	ADM@O2SISTEMAS.COM	**Telefone Fixo:**	(21) 2042-0406
		Telefone Celular:	*- NÃO INFORMADO -*

CERTIFICA que, consultando a base de dados do Sistema de Gerenciamento de Processos do Poder Judiciário do Estado do Espírito Santo (E-Jud, SIEP, PROJUDI e PJe) até a presente data e hora, **NADA CONSTA** contra o solicitante .

Observações

a. Certidão expedida gratuitamente através da Internet;
b. Os dados do(a) solicitante acima informados são de sua responsabilidade, devendo a titularidade ser conferida pelo interessado e/ou destinatário;
c. O prazo de validade desta certidão é de 30 (trinta) dias, contados da data da expedição, conforme disposto no art. 467 do Código de Normas da Corregedoria Geral da Justiça. Após essa data será necessária a emissão de uma nova certidão;
d. A autenticidade desta certidão poderá ser confirmada na página do Tribunal de Justiça do Estado do Espírito Santo - www.tjes.jus.br -, utilizando o número da certidão acima identificado;
e. Em relação as comarcas da entrância especial (Vitória/Vila Velha/Cariacica/Serra/Viana), as ações de: execução fiscal estadual, falência e recuperação judicial, e auditoria militar, tramitam, apenas, no juízo de Vitória;
f. As ações de natureza cível abrangem inclusive aquelas que tramitam nas varas de Órfãos e Sucessões (Tutela, Curatela, Interdição,...), Juizado Especial Cível, Juizado Especial da Fazenda Pública, Execução Fiscal e Execução Patrimonial (observado o item **e**);
g. As ações de natureza criminal abrangem, dentre outras: as de auditoria militar e de juizados especiais criminais;
h. As matérias atinentes as varas de família e infância e juventude são objeto de certidão específica;
i. A base de dados do sistema de gerenciamento processual (1ª INSTÂNCIA: eJUD, SIEP, PROJUDI, PJe-1G; 2ª INSTÂNCIA: Sistema de Segunda Instância, PJe-2G) contém o registro de todos os processos distribuídos no Judiciário do Estado do Espírito Santo, com exceção do SEEU;
j. A certidão negativa referente ao Sistema Eletrônico de Execução Unificado – SEEU deverá ser requerida ao Cartório do Ofício de Distribuidor da Comarca, conforme Ato Normativo Conjunto n°. 009/2021.

ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
CONTADORIA E AUDITORIA-GERAL DO ESTADO - CAGE
Rua Siqueira Campos, nº 1044 - Sala 426-B - Centro
90010-001 - Porto Alegre - RS
Fones: 51 3214-5215 ou 3214-5218
E-mail: dcce.cage@sefaz.rs.gov.br

CERTIFICADO DE CAPACIDADE FINANCEIRA RELATIVA DE LICITANTE

Certificado Nº: 90686 **Processo**: 000000-00.00/00-0

Período de Validade: 02/06/2022 até 30/06/2023

CNPJ Nº: 08.706.548/0003-25

Razão Social: O2 SOLUCOES EM TECNOLOGIA DIGITAL

Endereço: RODOVIA GOVERNADOR MARIO COVAS, KM 279 / SALA 186
JACUHY - 29161-230 - SERRA - ES

Atividade Principal: 46.51-6-01 - Comércio atacadista de equipamentos de informática

A Contadoria e Auditoria-Geral do Estado - CAGE, com base nas demonstrações contábeis assinadas por **VINICIUS CORREA DE SOUZA** , CRC **RJ-076771/O-5**, concede o presente Certificado, atestando, na forma que dispõe o Decreto Estadual 36.601/96, que a empresa acima identificada possui capacidade financeira relativa para participar de licitações promovidas pela Administração Pública Estadual.

Para fins do disposto no art. 31 da Lei 8.666/93 e conforme as demonstrações contábeis do exercício social encerrado em 31/12/2021, a empresa ora certificada apresenta:

- Receita Bruta Anual no valor de $ 12.923.268,01 *.
- Capital Social Integralizado no valor de $ 1.603.600,00.
- Patrimônio Líquido no valor de $ 2.706.601,98.

Este Certificado substitui,no seu período de validade, a apresentação das Demostrações Contábeis, do Parecer de Auditoria e do Anexo II, de que tratam o Decreto estadual nº 36.601/96 e a Instrução Normativa CAGE nº 2/96.

CAGE 70 ANOS
CUIDANDO DO PRESENTE, ORIENTANDO PARA O FUTURO.

* Excluídas as vendas canceladas e os descontos incondicionais concedidos nos termos do § 1º do art. 3º da LC 123/2006.

Constatando-se, a qualquer tempo, irregularidades nas informações fornecidas pela empresa, este certificado perderá imediatamente sua validade.

Código de Autenticação: **5675013394**

Confira a autenticidade deste documento em **http://www.sisacf.sefaz.rs.gov.br**

ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

Certidão Negativa de Débitos para com a Fazenda Pública Estadual - MOD. 2

Certidão Nº 20220000998678

Identificação do Requerente: CNPJ N° 08.706.548/0003-25

Certificamos que, até a presente data, não existe débito contra o portador do Cadastro de Pessoa Jurídica acima especificado, ficando ressalvada à Fazenda Pública Estadual o direito de cobrar quaisquer dívidas que venham a ser apuradas.

Certidão emitida via Sistema Eletrônico de Processamento de Dados, nos termos do Regulamento do ICMS/ES, aprovado pelo Decreto nº 1.090-R, de 25 de outubro de 2002.

Certidão emitida em **11/11/2022**, válida até **09/02/2023**.

A autenticidade deste documento poderá ser confirmada via internet por meio do endereço **www.sefaz.es.gov.br** ou em qualquer Agência da Receita Estadual.

Vitória, 11/11/2022.

Autenticação eletrônica: **0023.2C35.FB70.A579**

PREFEITURA DA SERRA
SECRETARIA MUNICIPAL DA FAZENDA

29176-439 - R MAESTRO ANTÔNIO CÍCERO, 111 CAÇAROCA SERRA ES

CERTIDÃO NEGATIVA DE DÉBITOS

Número 11457477/2022 **Data Geração: 03/10/2022** **Data Validade: 03/12/2022**

Certificamos que não constam em nome do sujeito passivo identificado, nesta data, débitos com a Fazenda Pública Municipal, ressalvando o direito do município de cobrar quaisquer débitos que vierem a ser conhecidos e apurados após a expedição desta certidão.

Identificação	
Crc	8430722
Contribuinte	O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA
CNPJ / CPF	08.706.548/0003-25
IE / RG	
Endereco	29161-382 - ROD GOVERNADOR MÁRIO COVAS, KM 279
Bairro	TERMINAL INTERMODAL DA SERRA Cidade: SERRA Estado: ES

Data Emissão: 03/10/2022

Tanto a veracidade da informação quanto a manutenção da condição de não devedor poderá ser verificada na seguinte página da Internet:

http://www.serra.es.gov.br

Número: 11457477/2022

Inscrição: 8430722

ATENÇÃO: Qualquer rasura ou emenda **INVALIDARÁ** este documento.

Certidão Emitida Gratuitamente

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 08.706.548/0003-25
Razão Social: O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA
Endereço: ROD GOVERNADOR MARIO COVAS KM279 SALA 186 / TM INTERMODAL SERRA / SERRA / ES / 29161-382

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade:03/11/2022 a 02/12/2022

Certificação Número: 2022110300500515461040

Informação obtida em 07/11/2022 13:30:16

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA (MATRIZ E FILIAIS)
CNPJ: 08.706.548/0003-25
Certidão nº: 24458670/2022
Expedição: 02/08/2022, às 11:25:30
Validade: 29/01/2023 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **08.706.548/0003-25**, **NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.° 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
08.706.548/0003-25 **FILIAL**		**14/08/2020**

NOME EMPRESARIAL
O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
********	**DEMAIS**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
46.51-6-01 - Comércio atacadista de equipamentos de informática

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
62.01-5-01 - Desenvolvimento de programas de computador sob encomenda
62.01-5-02 - Web design
62.02-3-00 - Desenvolvimento e licenciamento de programas de computador customizáveis
62.03-1-00 - Desenvolvimento e licenciamento de programas de computador não-customizáveis
62.04-0-00 - Consultoria em tecnologia da informação
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
63.11-9-00 - Tratamento de dados, provedores de serviços de aplicação e serviços de hospedagem na internet
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios
85.99-6-04 - Treinamento em desenvolvimento profissional e gerencial

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
ROD GOVERNADOR MARIO COVAS	**KM 279**	**SALA 186**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
29.161-230	**JACUHY**	**SERRA**	**ES**

ENDEREÇO ELETRÔNICO	TELEFONE
FINANCEIRO@O2SISTEMAS.COM	**(21) 2042-0406**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**14/08/2020**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia **25/10/2022** às **10:13:36** (data e hora de Brasília). Página: **1/1**

IBM® NVMe FlashCore™ Module 2
FIPS 140-2 Non-proprietary Security Policy
Security Level 2

Rev. 1.2 – Jan 13th, 2021

IBM® Corporation

Table of Contents

1 Introduction 3

1.1 Scope 3

1.2 Security Levels 3

1.3 References 3

1.4 Acronyms used in this document 4

2 Cryptographic Module Description 4

2.1 Overview 4

2.2 Logical to Physical Port Mapping 5

2.3 Hardware and Firmware Versions 5

2.4 FIPS Approved and Allowed Algorithms 6

2.5 Self-Tests 7

2.6 FIPS 140-2 Approved Mode of Operation 7

2.6.1 FIPS mode 8

2.6.2 SUM Locking Ranges (SLRs) 8

2.7 Crypto-Erase of User Data 9

2.8 Revert via OFS 9

3 Identification and Authentication Policies 9

3.1 Operator Roles 9

3.1.1 Cryptographic Officer (CO) Roles 9

3.1.2 Users (1 – 8) in LockingSP 10

3.1.3 Unauthenticated Role 10

3.2 Authentication 10

3.2.1 Authentication Type 10

3.2.2 Authentication in FIPS mode 10

3.2.3 Authentication Mechanism, Data and Strength 10

3.2.4 Personalizing Authentication Data 11

4 Access Control Policy 11

4.1 FIPS 140-2 Services....11
4.2 Non-FIPS Mode Services....14
4.3 Cryptographic Keys and CSPs....14
5 Physical Security....17
5.1 Mechanisms....17
5.1.1 Figure 1 – TEL1....17
5.1.2 Figure 2 – TEL2....18
5.1.3 Figure 3 – TEL3 and TEL4....20
5.2 TELs on ends of FCM2....20
5.2.1 Figure 4 – tampered TEL1....20
5.2.2 Figure 5 – tampered TEL2....21
5.2.3 Figure 6 – tampered TEL3....21
5.2.4 Figure 7 – tampered TEL4....21
5.3 Operator Requirements....22
6 Operational Environment....22
7 Security Rules....23
7.1 Establishing FIPS mode and exit conditions....23
7.2 Ongoing Policy Restrictions....23
8 Mitigation of Other Attacks Policy....23

1 Introduction

1.1 Scope

This is the security policy associated with the IBM NVMe FlashCore Module 2, a NVMe-connected self-encrypting non-volatile storage module, a Cryptographic Module which is being validated per FIPS 140-2.

This document is designed to meet the FIPS 140-2 standard (Appendix C) and Implementation Guidance (section 14.1) requirements. It is not intended to provide the type of interface details required to develop a compliant application.

1.2 Security Levels

Requirement Area	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interface / Electromagnetic Compatibility (EMI / EMC)	2
Self – Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

1.3 References

1. FIPS PUB 140-2, issued May 25, 2001
2. Derived Test Requirements for FIPS PUB 140-2, issued Jan. 4, 2011
3. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, last updated Dec 3, 2019
4. TCG Storage Architecture Core Specification, Specification Version 2.01
5. TCG Storage Security Subsystem Class: Opal, Specification Version 2.01
6. TCG Storage Opal SSC Feature Set: PSID Version 1.00
7. TCG Storage Opal SSC Feature Set: Single User Mode, Specification Version 1.00
8. NVM Express Revision 1.2.1

1.4 Acronyms used in this document

AdminSP	Administrative security partition, a TCG term
AES	Advanced Encryption Standard (FIPS 197)
CBC	Cipher Block Chaining, an encryption mode
CO	Crypto-Officer
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FCM2	FlashCore Module 2
LBA	Logical Block Address
KAT	Known Answer Test
LockingSP	Locking Range security partition, a TCG term
MEK	Media Encryption Key
MSID	Manufactured SID, TCG term for a unique per FCM2 public value used as the default PIN
POST	Power on Self-Test
PSID	Physical SID, TCG term for a unique per FM value public value
SID	Security ID, TCG term for Drive Owner CO role's PIN
SLR	SUM Locking Range
SP	Security Policy (per FIPS 140-2)
SUM	Single User Mode
XTS	XEX-based tweaked-codebook mode with ciphertext stealing, an encryption mode

2 Cryptographic Module Description

2.1 Overview

The cryptographic module is the IBM NVMe FlashCore Module 2 (FCM2) in its entirety. The cryptographic module will be referred to as the FCM2 throughout this document. This FCM2 uses FIPS approved algorithms to provide a number of cryptographic services. Those services include encryption and decryption of user data in hardware, support for cryptographic erase, support for multiple user data Locking Ranges (each of which can be configured for independent access control and protection), and authentication checking of code downloads. The services are provided via FCM2 support of the TCG Opal SSC interface.

The FCM2 is a multiple-chip embedded cryptographic module implementation. The outside surfaces of the FlashCore Module 2 Assembly are the physical cryptographic boundary. The module's logical boundary is comprised of all hardware and firmware components contained within the module's physical boundary. The host interface to the FCM2 is physically a PCIe connector, over which the industry-standard NVMe protocol [8] is supported. Through the NVMe logical interface the FCM2 supports the TCG SWG Core [4] and TCG Opal SSC [5] protocols. All control of the FCM2 via its interfaces is typically through an application on a host system. All human control of an FCM2 is assumed to be through such an application.

The primary cryptographic service supported by the FCM2 is encryption of user data at rest: encrypting user data written to the FCM2 before the resultant ciphertext is written to the FCM2's non-volatile solid-state memory. The FCM2 also supports the complementary decryption function, decrypting that ciphertext from solid-state memory when it is read back. Storing user data in encrypted form enables another cryptographic service the FCM2 supports: cryptographic erase, which nearly instantly renders all previously encrypted user data to be effectively destroyed. The FCM2 supports TCG Opal access controls, which restrict access to use of, and administration of, the encryption and cryptographic erase services.

2.2 Logical to Physical Port Mapping

FIPS 140-2 Interface	Module Ports
Data In	NVMe connector
Data Out	NVMe connector
Control Input	NVMe connector
Status Output	NVMe connector
Power Input	NVMe connector

2.3 Hardware and Firmware Versions

The following FCM2 configurations have been validated:

Native Capacity	Hardware Part #	Firmware Version
38.4 TB	02CL181	2.0.9.67
19.2 TB	02CL183	2.0.9.67
9.6 TB	02CL185	2.0.9.67
4.8 TB	02CL187	2.0.9.67

The configurations vary with respect to the memory integrated circuits (ICs) used. The number of parts, part numbers, and storage capacity of those ICs varies between configurations, but these ICs have no cryptographic capability and do not alter the FIPS services provided.

2.4 FIPS Approved and Allowed Algorithms

Algorithm (implementation in)	Certificate #	Associated Standard	Usage
AES-KEY-WRAP (F/W)*	AES #5898	SP 800-38F	Only used as part of self-test at POST
AES-KEY-UNWRAP (F/W)*	AES #5898	SP 800-38F	Only used as part of self-test at POST
XTS-AES-256 Encrypt (F/W)**	AES #5898	SP 800-38E	To check XTS-AES-256 Encrypt in H/W
ECB-AES-256 (F/W)	AES #5898	FIPS 197	A primitive used by XTS-AES-256 Encrypt, and by AES key wrap & unwrap
CBC-AES-128 (F/W)	AES #5898	SP 800-38A	Whitening performed as part of entropy processing
CKG (F/W)	Vendor Affirmed *5	SP 800-133	Cryptographic Key Generation
NDRNG (H/W)	Allowed	SP 800-90B	Seeding the DRBG
DRBG-SHA-512 (F/W)	DRBG #2454	SP 800-90A	Random number generation
SHA2-512 (F/W)	SHA #4648	FIPS 180-4	A primitive used by DRBG-SHA-512
KDF	KBKDF #244	SP 800-108	Key derivation
HMAC-SHA-256 (F/W)	HMAC #3872	FIPS 198-1	A primitive used by the KDF
SHA2-256 (F/W)	SHA #4648	FIPS 180-4	Hash of PINs used to authenticate, as well as a primitive used by HMAC-SHA-256
XTS-AES-256 Encrypt/Decrypt (H/W)**	AES #5897	SP 800-38E	User Data written by a host application is encrypted; decryption is performed on read
ECB-AES-256 (H/W)	AES #5897	FIPS 197	A primitive used by XTS-AES-256
SHA3-384 (H/W)	SHA-3 #62	FIPS 202	As part of verification of a code load's digital signature (4 byte aligned only *3)
RSA-4096 (H/W)	Vendor Affirmed *4	FIPS 186-4	As part of verification of a code load's digital signature

* No claim of any service or cryptographic protection associated with use of AES Key Wrap and Unwrap is made

** XTS-AES-256 is only used by the FCM2 in the context of storage applications

*3 Only 4-byte aligned inputs are supported, so only 4-byte aligned inputs were verified by CAVP

*4 In accordance with FIPS 140-2 IG A.11, the cryptographic module performs digital signature checking using SHA3-384 as specified in FIPS PUB 202 (Vendor Affirmed)

*5 In accordance with FIPS 140-2 IG D.12, the cryptographic module performs cryptographic key generation per SP 800-133 (Vendor Affirmed)

2.5 Self-Tests

Function Tested	Self-Test	KAT Implementation	If this KAT test fails
SHA2-256	Power-On	Hash KAT performed	Enters FIPS Self-Test Fail State
AES-KEY-WRAP	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
AES-KEY-UNWRAP	Power-On	Decrypt KAT performed	Enters FIPS Self-Test Fail State
DRBG (SHA-512)	Power-On	DRBG KAT performed	Enters FIPS Self-Test Fail State
HMAC-SHA-256	Power-On	HMAC KAT performed	Enters FIPS Self-Test Fail State
AES-256	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
XTS-AES-256	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
CBC-AES-128	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
SHA3-384 (H/W)	Power-On	Digest KAT performed	Enters FIPS Self-Test Fail State
RSA-4096 (H/W)	Power-On	Verify KAT performed	Enters FIPS Self-Test Fail State
AES-256 (H/W)	Power-On	Encrypt/Decrypt performed	Enters FIPS Self-Test Fail State
XTS-AES-256 (H/W)	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
SP 800-108 KDF	Power-On	KDF KAT performed	Enters FIPS Self-Test Fail State
XTS Key1 != XTS Key 2	Conditional*	Not a KAT	Enters FIPS Self-Test Fail State

* This check is made each time a Root Key is expanded, by two key derivations, into XTS's Key1 and Key2.
The Non-Approved but Allowed Non-Deterministic Random Number Generator (NDRNG) is continuously tested by a Repetition Count Test (RCT).

A new SP 800-90A DRBG Instantiate and Generate Health Tests are addressed by destructing the existing instance and instantiating a new one each time a random number is to be generated. A KAT test is run against the new SP 800-90A instantiation to assure it is sound before it is used. The DRBG is then used to generate a random number by processing NDRNG samples.

A Continuous Random Number Generator Test (CRNGT) is performed on the output of the DRBG. The first random number generated after power up is not used, and SHA2-256 hash of each subsequently generated new random number is compared to the SHA2-256 of the immediately previous generated random number. The continuous test fails if the two numbers match indicating the output of the DRBG has not changed (i.e. is stuck).

A firmware download test which checks the authenticity of the firmware download, is performed on any attempted firmware update to the FCM2. If the SHA3-384/RSA-4096 digital signature of the firmware update does not check, the firmware download is aborted.

A firmware integrity check is performed as part of the power on process using the same SHA3-384/RSA-4096 digital signature. The CPU cores are not allowed to run until and unless the firmware integrity check is run successfully.

2.6 FIPS 140-2 Approved Mode of Operation

The FCM2 will operate in a non-FIPS mode until the Secure Initialization steps detailed in Section 7.1 are performed. Before FIPS mode is established, the FCM2 is in, what will be called here, an "unestablished state".

From this non-FIPS mode, the FCM2 may be securely initialized so that it operates in FIPS 140-2 Mode of operation (hereafter "FIPS Mode"). After the FCM2 has been Securely Initialized and operated per the Security Rules detailed in Section 7.1, the FCM2 will remain in FIPS Mode of operation until either an important error or failure has been detected or a "Revert via OFS" service is performed. An operator controlling the FCM2 can use the "FIPSmode?" service, if it does not return the expected status (see Section 4.1), then the FCM2 is not operating in FIPS mode.

An operator can cause an FCM2 operating in FIPS Mode to quit FIPS Mode by use of the FCM2's "Revert via OFS" service. This service will zeroize the FCM2's keys and CSPs and transition it through its Original Factory State

(OFS) to its unestablished state. The operator can then cause that FCM2 to return to FIPS Mode by following the Secure Initialization procedure detailed in Section 7.1 again.

To operate the FCM2 is in its FIPS Mode, it must be configured properly and it must be operated in accordance with the associated policy restrictions (detailed in Section 7.2). Violating the ongoing policy restrictions would mean that the FCM2 is no longer being operated in its FIPS Mode of operation.

2.6.1 FIPS mode

When operated in this mode the FCM2 provides cryptographic services via industry-standard NVMe commands, TCG Opal commands addressed to the TCG AdminSP, and TCG Opal commands addressed to the TCG LockingSP. To operate in FIPS mode, the Drive Owner must invoke the Activate method on the LockingSP starting from an unestablished state which itself must start afresh from an OFS state.

Keys and CSPs established in FIPS mode cannot be used in non-FIPS mode. This is accomplished by the key zeroization which performed as part of the "Revert via OFS" service.

Similarly, Keys and CSPs established in non-FIPS mode cannot be used in FIPS mode. If an FCM2 had been previously operated with a non-FIPS code load, a Locking Range may have been established, though that FCM2 would not have been in FIPS mode because of the non-FIPS code load. In this case some keys (e.g. the Locking Range's MEK) would have been established with a non-FIPS code load and they cannot be used in FIPS mode. If the code on that FCM2 is then updated to the FIPS code load, then the FCM2 must be put back into the OFS state by use of one of the Opal methods specified in the "Revert via OFS" service. This service will cause cryptographic erase of all data written to those Locking Ranges as the Locking Range's MEKs are zeroized. Then the drives can be put back into FIPS mode if all requirements are met.

The FCM2 only supports Single User Mode (SUM), so only a single User has independent access control to read/write/erase a given Locking Range. By default, there is a single "Global Range" that encompasses the whole user data area. "Locking Ranges", when established, are configured to be subsets of the LBA range initially established as a Global Range.

2.6.2 SUM Locking Ranges (SLRs)

When invoking the Activate method to enter FIPS mode, the Drive Owner creates a Locking Range (LR). All LRs created within the FCM2 must be of the Single User Mode (SUM) type. The FCM2 does not support creation of non-SUM LRs, or reclassification of SUM LRs into non-SUM LRs, and any TCG Opal methods attempting either of those will fail with the appropriate error code returned. So, all LRs created in an FCM2 will be, and will remain, "SUM Locking Ranges" (SLRs). SLRs conform to the SUM feature set [7]. Each SLR is controlled and administered solely by the single User role it is associated with per [5] and [7], e.g. SLR1 by User2.

TCG Opal implements multiple Cryptographic Officer (CO) roles which operate cooperatively to establish, configure, and administer these SLRs. These roles include, at a minimum, the Drive Owner, the User(s), and the LockingSP Admin(s). While in FIPS mode, this cooperative operation includes:

1. Creating one or more SLRs (by the Drive Owner)
   - the FCM2 supports a Global Range and the additional creation of up to 3 SLRs
2. Customize the User PIN and LBA range associated with each created SLR (by User(s) only)
3. Lock and Unlock SLRs (by User(s) only)
4. Crypto-Erase of SLRs (by User(s) or Locking SP Admin(s))
5. Crypto-Erase of Global Range (by Locking SP Admin(s))

2.7 Crypto-Erase of User Data

Because all user data written to the FCM2 is encrypted when stored to its internal solid-state media, the data can be cryptographically erased (crypto-erased). The encrypted data, ciphertext, stored is effectively erased when the media encryption key (MEK) used to encrypt it is overwritten (with a fresh MEK) or erased (overwritten with a fixed value such as all zeroes). Because the FCM2 supports the ability to "zeroize" all keys and CSPs, per the FIPS 140-2 key management requirement, the FCM2 supports the capability to "zeroize" any and all MEKs, which in turn crypto-erases all the user data encrypted with those MEKs. The FCM2 supports the capability to zeroize any and all MEKs whether it is in FIPS Mode or not.

It should be noted that user data stored to the FCM2 cannot be reliably destroyed by overwrite from the host because the actual storage space where a given LBA's data is stored moves over time within the FCM2 for multiple reasons including support for wear-leveling. But user data can be reliably destroyed by crypto-erase of the associated MEK. Alternately, all private keys and CSPs can be zeroized at once via Opal methods which cause Revert via OFS (see Section 2.8).

2.8 Revert via OFS

Whether in FIPS mode or not, the TCG Revert and RevertSP methods may be invoked by an appropriately authenticated Role to put the FCM2 into an unestablished state (non-Approved) mode. This corresponds to the "Revert via OFS" service and is akin to a "restore to factory defaults" operation. This operation causes zeroization of all CSPs and private (or secret) cryptographic keys. Subsequently, the FCM2 has to be reinitialized before it can return to a FIPS Mode of operation. These Revert and RevertSP methods may be invoked by the Drive Owner, by the AdminSP's Admin, by the LockingSP's Admins, or by an unauthenticated role using the public PSID value [6].

3 Identification and Authentication Policies

3.1 Operator Roles

The following explains the Cryptographic Officer and User roles with a *general* description of the purpose and authority of each role. For further details of the services performed by each role while the FCM2 is in FIPS mode, see section 4.1.

3.1.1 Cryptographic Officer (CO) Roles

3.1.1.1 Drive Owner

This role corresponds to the SID (Secure ID) Authority on the AdminSP as defined in Opal SSC [5]. This role is used to transition the FCM2 to FIPS mode. It should be noted that to operate in FIPS Mode, a FIPS validated code version (i.e. FIPS code) must be loaded into the FCM2, and the FCM2 must have booted to that code level. If the FCM2 is not running FIPS code, it cannot be operating in FIPS mode.

3.1.1.2 Admins (1-4) in LockingSP

When in FIPS mode, these roles' Authority corresponds to the LockingSP's Admin roles as defined in Opal SSC [5].

3.1.1.3 Admin1 in AdminSP

When in FIPS mode, this role's Authority corresponds to the AdminSP's Admin1 role defined in Opal SSC [5]. This role is enabled by default, but can be disabled by the Drive Owner, if desired. When enabled, an authenticated AdminSP Admin1 can invoke the "Revert via OFS" service.

3.1.2 Users (1 – 8) in LockingSP

When in FIPS mode, these roles' Authority corresponds to the LockingSP's User roles as defined in Opal SSC [5]. These roles can unlock (and also lock) the corresponding SLR in the FCM2, so that an operator can read and write data to that SLR. This role can also invoke the Crypto-Erase service of the associated SLR.

When operating in FIPS Mode, there can be up to 8 separate Users (User IDs) and the role corresponds to the same named TCG Authority on the LockingSP. Because SUM assigns a single fixed User to a given SLR, the three SLRs supported are all associating with a given User. Because the FCM2 only supports three SLRs, only the three associated Users (2-4) can actually be used at present.

3.1.3 Unauthenticated Role

Anyone who has the ability to remove and then restore power to a FCM2 can cause a power cycle which will cause a reset of the FCM2, that is one type of unauthenticated service. Note that since both the MSID and 26-byte PSID are public credentials, "authenticating" with either to gain MSID authority or PSID authority, respectively, amounts to operation in an unauthenticated role. Thus, entering the public PSID value enables unauthenticated invocation of some services (e.g. to invoke the "Revert via OFS" service). No authentication is required to perform the "FIPScode?" and "FIPSmode?" services.

3.2 Authentication

3.2.1 Authentication Type

Role-based authentication of operators is supported. For example, the Drive Owner role has its own unique ID which is associated with a dedicated PIN. The Drive Owner's PIN can be personalized such that it is unique for that role.

For some cases, the authentication is performed in a separate associated service. For example, the Read Unlock service is the authentication required to enable subsequent User Data Read service. If an attempt is made to use the User Data Read service without prior authentication, then the User Data Read will fail.

Authentications which use the TCG interface can provide the operator and PIN in the StartSession method invocation. Or, an operator may use the Authenticate method to authenticate to a role within a Session that has already been started. Authentications persist until the associated session is closed.

3.2.2 Authentication in FIPS mode

Operators can authenticate by use of either the TCG Authenticate or StartSession methods. The host application can have only a single session open at a time. During a session the application can invoke services for which the authenticated operator(s) have authority. One of security rules enforced by the FCM2 is that the host must not authenticate to more than two operators' roles while in a session.

The host application can authenticate to the "Anybody" authority, which does not have a private credential, for the invocation of some services. Accordingly, the invoked services are effectively unauthenticated services.

3.2.3 Authentication Mechanism, Data and Strength

Operators authenticate with the FCM2 by providing a PIN. The provided PIN is hashed and compared to the hash non-volatilely stored when that PIN was established. Per the TCG SWG Core [4] specification, PINs have an associated retry attribute ("TryLimit") that controls the number of unsuccessful attempts before the authentication is blocked. The default value of the TryLimit and Persistence settings are 0 (which specifies unlimited retries) and FALSE (which means that any count of incorrect authentications will be reset on reboot), respectively. Neither the TryLimit nor the Persistence settings can be changed, both have their respective Writeable Flags permanently set to FALSE.

The PINs have a maximum length of 32 bytes. Per the policy security rules, the FCM2 only allows programming of PINs that are of length 8 bytes or longer (see Section 7.1's Rule 4). This PIN length results in a probability of at most $1/2^{64}$ (i.e. less than 10^{-19}) for the PIN to be guessed in a single random attempt. This far exceeds the FIPS 140-2 authentication strength requirements of less than $1/10^{6}$ (= 10^{-6}).

Each authentication attempt requires 39ms on average for the FCM2 to complete. This means that at most (60*1000)/39 (= 1538) attempts can, on average, be made in one minute. So the probability of multiple random attempts succeeding in guessing a PIN in a one minute period is about $1538/2^{64}$ = 8 x 10^{-17} which far exceeds the FIPS requirement of $1/10^{5}$ (= 10^{-5}).

3.2.4 Personalizing Authentication Data

The SID is initially set to the value of the manufactured value (MSID). This is a device-unique public value which is 32 ASCII characters long. The Security Rules (Section 7) for the FCM2 requires that the PIN values must be "personalized" to private values using the "Set PIN" service. The Drive Owner PIN can be set to a different value by use of the TCG Set Method.

4 Access Control Policy

4.1 FIPS 140-2 Services

The following tables details the FIPS 140-2 services the FCM2 provides when in FIPS Mode. It shows which services (Approved Security Functions) can be invoked or used by which authenticated operators (Access Control). in terms of the and operator access control. Note the following:

- Use of the services described below is compliant only when the FCM2 is in FIPS mode.
- Not shown are the security functions which underlie the higher-level algorithms shown below (e.g. DRBG-SHA-512 as part of NDRBG)
- Operator authentication is not shown in this table, but an operator must have appropriately authenticated to the role shown in the Operator Access Control column to use/invoke the service shown in the Service Name column of the same row
- Some security functions listed are used solely to protect / encrypt keys and CSPs.
- Input and output details of TCG Opal (or NVMe) methods used to invoke the services below are defined by the TCG Opal (or NVMe) standards.
- Unauthenticated services (e.g. FIPScode?) do not provide access to private keys or CSPs
- Some services such as User data read / write have indirect access control provided through enable, disable, lock, and unlock services used by an authenticated operator.

Table 2.1 - FIPS 140-2 Authenticated Services – FIPS mode				
Service Name	**Description**	**Operator Access Control**	**Security Function**	**Command(s)/Event(s)**
Set PIN	Change operator authentication data.	AdminSP Admin1, LockingSP Admin1- 4, User1-8, Drive Owner	SHA2-256 Hashing	TCG Set Method
Activate SLR	Allocate a SUM Locking Range (SLR)	Drive Owner	SHA2-256 Hashing	TCG Activate Method
Firmware Download	Load firmware image. If the downloaded firmware image signature checks, then the FCM2 will boot to the new code at next reboot. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.	None	Digital Signature (RSA 4096 with SHA3-384) Check	NVMe Firmware Image Download
Enable / Disable AdminSP Admin	Enable / Disable the AdminSP Admin1	Drive Owner	None	TCG Set Method
Enable / Disable LockingSP Admin(s)	Enable / Disable a LockingSP Admin	LockingSP Admin1- 4	None	TCG Set Method
Set Geometry	Set the starting LBA and size of the SLR.	User1-8 (if User Ownership (Policy 0))	None	TCG Set Method
Lock / Unlock SLR for Rd/Wr	Block or allow read (decrypt) / write (encrypt) of user data in a range.	User1-8 (only one of these users is authorized for each LR created, per SUM restrictions)	Key Derivation Function (KDF)	TCG Set Method
User Data Read / Write	Encryption/decryption of user data to/from a SLR. Access control to this service is provided through Lock/Unlock SLR for Rd/Wr	None	XTS-AES-256 Decryption/ Encryption (Symmetric Key)	NVMe Read / Write Commands
Crypto-Erase of SLR	Erase user data in a SUM Locking range by changing its associated MEK	LockingSP Admin1- 4	DRBG, Symmetric Key	TCG Erase Method
		LockingSP User1-8		TCG GenKey Method, TCG Erase Method
Revert via OFS	Exit FIPS mode. Note: FCM2 will enter unestablished state.	Drive Owner	DRBG, Hashing, Symmetric Key	TCG LockingSPObj.Revert(), TCG AdminSPObj.Revert()

		AdminSP Admin1		TCG AdminSPObj.Revert()
		LockingSP Admin1- 4		TCG LockingSP.RevertSP()

Table 2.2 - FIPS 140-2 Unauthenticated Services – FIPS mode				
Service Name	**Description**	**Operator Authentication Required**	**Security Function**	**Command(s)/Event(s)**
Cold Boot	Firmware integrity check on boot	None	RSA-4096/ SHA3-384 signature	Power On Reset
Unblock PIN	Resets password attempt counters	None	None	Power On Reset
Reset Module	Runs all POSTs and zeroizes keys & CSPs in RAM	None	None	Power On Reset, NVMe reset (NSSR)
FIPSmode?	Reports whether, from a drive perspective, the drive is in FIPS mode	None	None	NVMe Identify: Controller Identify, bytes 3600-3607 (set to “FIPSmode”?)
FIPScode?	Reports whether the code level in operation was FIPS validated	None	None	NVMe Identify: Controller Identify, bytes 3616-3623 (set to “FIPScode”?)
DRBG Generate Bytes	Returns a SP800-90A DRBG Random Number of # of bytes requested up to 50	None	DRBG	TCG Random()
Revert via OFS	Exit FIPS mode. Note: FCM2 will enter unestablished state.	None (e.g. by use of PSID)	DRBG, Hashing, Symmetric Key	AdminSP.RevertSP(), AdminSPObj.Revert()

4.2 Non-FIPS Mode Services

In the unestablished state, the FCM2 supports the following services:

1. The ability to transition the FCM2 to FIPS Mode of operation
2. The ability to update firmware
3. The ability to crypto-erase user data
4. The ability to reset the FCM2 via NVMe Reset (NSSR) or Power On Reset
5. The ability to report status.

All cryptographic algorithms used in FIPS Mode of operation are also available in this security unestablished state.

4.3 Cryptographic Keys and CSPs

The following table defines the keys / CSPs and the operators / services which use them.

Note that:

- The use of PIN CSPs to authenticate is implied by the operator access control
- The Set PIN service is shown in this table though it is generally only used at FCM2 setup
- All non-volatile storage of keys and CSPs is internal to the FCM2 and to which there is no logical or physical access from outside of the FCM2
- The FCM2 uses a SP 800-90A DRBG and adopts the Hash_DRBG mechanism
- Non-critical security parameters are not shown in this table
- Read access of private values is kept internal to the FCM2 and so are not represented in this table.
- There is no audit feature supported which is security-relevant.

	Table 3 - Key Management					
Name	**Description / Non-volatile Storage**	**Type (Pub / Priv, key / CSP (e.g. PIN)), size**	**Operator Role**	**Establishment**	**Services Used In**	**How accessed**
SID (Security Identifier), a.k.a. Drive Owner PIN	Auth. Data / Hash	Secret, PIN, 32 bytes	Drive Owner	This PIN is setup or changed by the drive owner	Set PIN, Activate SLR, Enabl / Disbl AdminSP Admin(s), Revert via OFS	Entered into FCM2 (in plaintext)
LockingSP Admin1-4 Passwords	LockingSP Admins Auth. Data / Hash	Secret, PIN, 32 bytes	LockingSP Admins	These PINs are setup or changed by the corresponding admins	Set PIN, Enabl / Disbl LockingSP Admin(s), Crypto-erase of SLR, Revert via OFS	Entered into FCM2 (in plaintext)
AdminSP Admin1 Passwords	AdminSP Admin Auth. Data / Hash	Secret, PIN, 32 bytes	AdminSP Admin	These PINs are setup or changed by the corresponding admin	Set PIN, Revert via OFS	Entered into FCM2 (in plaintext)
User1-8 Passwords	Users Auth. Data / Hash	Secret, PIN, 32 bytes	LockingSP User	These PINs are setup or changed by the corresponding users	Set PIN, Set Geometry, Lock/Unlock SLR for Rd/Wr	Entered into FCM2 (in plaintext)
LBA Range Root Key (unmodified DRBG Output)	Root Key / Obfuscated	Secret, AES Key, 256 bits	LockingSP Admins, Users	This key is generated using the output from the module's DRBG	Encrypt / Decrypt User Data	Use allowed during Execution only
LBA Range MEKs (each 'MEK' is comprised of two 256-bit keys)	Media Encryption Key / No*	Secret, 2 AES keys, 2 x 256 bits	LockingSP Admins, Users	These 2 keys are derived from the LBA range root key using the approved SP800-108 KDF	Encrypt / Decrypt User Data	Use allowed during Execution only
DRBG Entropy Input String	String of bits that contains entropy, input to a	Private, 128 bytes (providing full entropy)	None	Generated using the module's NDRNG	Services which use the DRBG (e.g. crypto-erase)	Use allowed during Execution only

	SP 800-90A DRBG / No*					
DRBG Seed	String of bits that is used as input to a SP 800-90A DRBG / No*	Private, 888 bits**, seed	None	Generated using the module's NDRNG	Services which use the DRBG (e.g. crypto-erase)	Use allowed during Execution only
DRBG Internal State	Collection of stored information about a SP 800-90A DRBG / No*	Private, DRBG intermediate values V and C (888 bits each)	None	Generated using the module's NDRNG	Services which use the DRBG (e.g. crypto- erase)	Use allowed during Execution only
FW Verification Key	Firmware Load Test Signature Verify Key / hardcoded in firmware	Public, RSA-4096 key, 4096 bits	None	This key is generated externally to the module and is hard-coded at build time	FW Download	Use allowed during Execution only

* Not stored non-volatilely

** per https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf; Table 2, seedlen

5 Physical Security

5.1 Mechanisms

The FCM2 has the following physical security:

1. Built of production-grade components which have standard passivation
2. Four opaque tamper-evident labels (TELs) on the FCM2. Two of the TELs are on the top (lid) of the FCM2. Additionally there is one TEL on each the front and back of the FCM2. The TELs are applied during IBM's manufacturing process. They protect against physical access to the electronics by board removal and prevent electronic design visibility.
3. Tamper-evident security labels applied by IBM manufacturing prevent FlashCore Module 2 Assembly cover removal for access to or visibility of the solid-state memory
4. Exterior of the FCM2 is opaque
5. The tamper-evident labels (TELs) cannot be penetrated, or removed and reapplied, without that tamper being readily evident
6. The TELs cannot be easily replicated with a low attack time

5.1.1 Figure 1 – TEL1

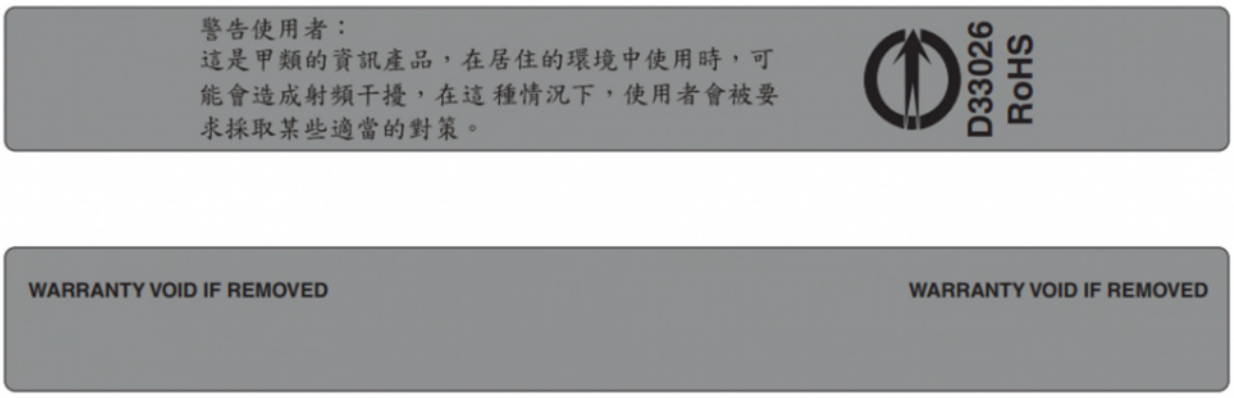
Figure shows TEL1 (black Agency Label)

5.1.2 Figure 2 – TEL2

Figure shows TEL2 (blue Counterfeit Label)

5.1.3 Figure 3 – TEL3 and TEL4

Figure shows TEL3 the BSMI label and TEL4 Warrantee Label



5.2 TELs on ends of FCM2

To provide tamper-evidence of FlashCore Module 2 Assembly cover removal:

5.2.1 Figure 4 – tampered TEL1

Showing tamper-evidence on TEL1

Where the folding and general distress are seen, and the TEL's shape has been distorted.

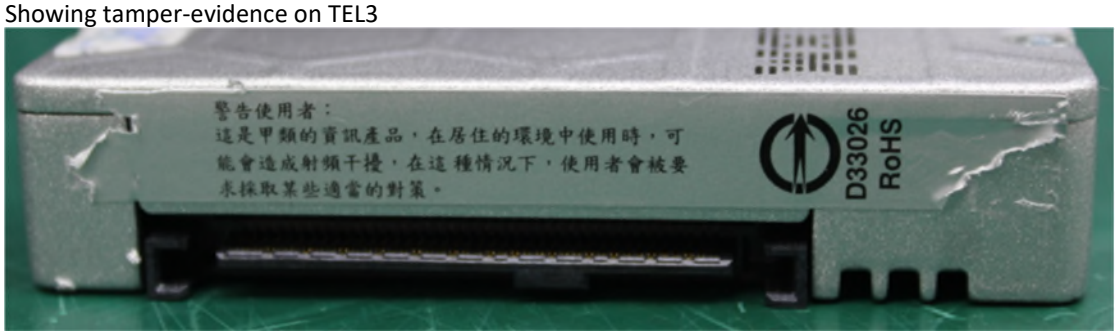
5.2.2 Figure 5 – tampered TEL2

Showing tamper-evidence on the holographic TEL2

Where the folding and general distress are seen, and the TEL's shape has been distorted.

5.2.3 Figure 6 – tampered TEL3

Showing tamper-evidence on TEL3



Where flaking and general distress are seen at each end of the label

5.2.4 Figure 7 – tampered TEL4

Showing tamper evidence of TEL4

Where flaking and general distress are seen at each end of the label

5.3 Operator Requirements

The operator is required to inspect the FCM2 periodically for any of the following types of tamper evidence:

- Flaking, folding, or ripping of TELs or metal case
  - Figures 4 illustrates tamper evidence on TEL3
- Security label over screws is missing or penetrated
- Text attributes (e.g. size, font, orientation, etc.) on security label does not match the original TEL
- TEL label cutouts do not match original
- General distress or discoloration of the TELs
  - Figures 5 illustrates tamper evidence on TEL4
- FCM2 assembly lid does not sit evenly or looks deformed

If evidence of tampering is apparent, the operator must assume the FCM2 has been compromised and so should decommission that FCM2. At a minimum the operator must discontinue using that FCM2 in any way that relies on that FCM2's cryptographic capabilities. Once tampering of a TEL has been detected, the FCM2 cannot thereafter ever be considered to be in FIPS mode.

6 Operational Environment

The FCM2 operates in a "non-modifiable operational environment" and so the FIPS 140-2, Section 6, Operational Environment requirements do not apply. Specifically, the operational environment cannot be modified while the FCM2 is in operation, and no code can be added or deleted. Firmware can be replaced or upgraded with a signed firmware download operation. If the code download's digital signature checks as authentic, then the FCM2 will boot to it following the next cold boot and so will begin operating with the new firmware image.

7 Security Rules

7.1 Establishing FIPS mode and exit conditions

The FCM2 does not typically change mode across power cycles and resets. However, certain operations can result in the FCM2 exiting FIPS Mode. In some of these situations (e.g. failure of the Power On Self Test), the FCM2 cannot be restored to FIPS mode and in that case could not provide any further FIPS service.

The following are the security rules for establishment and operation of the FCM2 in a FIPS 140-2 Approved manner. Further detail is available in the appropriate sections of this document.

1. Cryptographic Officer(s): At receipt of the product examine the shipping packaging and the product packaging to ensure it has not been accessed during shipping by the trusted courier.
2. Cryptographic Officers and Users: At installation, and periodically thereafter, examine the Tamper Evident Labels (TELs) installed at time of manufacture for tamper evidence.
3. Cryptographic Officers and Users: At installation, and periodically thereafter, query the FCM2's firmware's code level to be sure it matches the FIPS validated firmware level (see section 2.3). Additionally, use the "FIPScode?" service to assure the firmware identifies itself as "FIPScode" (i.e. that the proper compile time options were used when it was built).
4. Cryptographic Officers: At installation, determine if the FCM2 has been used previously (e.g. has a SLR already been established?). If so, then invoke the "Revert via OFS" service to zeroize all previously established secret keys and CSPs and remove any SLRs.
5. Transition the FCM2 to FIPS mode: The Drive Owner invokes the Activate method for each SLR to be created
6. Cryptographic Officers and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 8 bytes length by use of FIPS mode: Drive Owner, Admins, and Users
7. Cryptographic Officers (specifically LockingSP Admins) to operate in FIPS mode: Set ReadLockEnabled and WriteLockEnabled to "True" on each activated SLR. Periodically thereafter the ReadLockEnabled and WriteLockEnabled settings should be checked to be sure they have not been modified.
8. Use the "FIPSmode?" service to assure the firmware sees itself as being in FIPS mode.
9. Drive Owner: At installation, disable the "Makers" authority by use of the TCG Set method.
10. After secure establishment is complete, do a power-on reset to clear authentications established during establishment.
11. Users: do a GenKey of each SLR's Media Encryption Key (MEK)

If all of these steps are followed correctly, the FCM2 will be in FIPS Mode of operation. It should be noted that all of the conditions detailed above must continue to be met to remain in FIPS mode.

7.2 Ongoing Policy Restrictions

Each time a new CO role is to be assumed, the current Session must be closed, and a new Session started (or do a power-on reset), so that the previous authentication to the previous CO authority is cleared.

8 Mitigation of Other Attacks Policy

The FCM2 does not claim to mitigate against any other attacks relevant to FIPS 140-2 validation.

Cryptographic Module Validation Program CMVP

PROJECT LINKS

Overview

News & Updates

Publications

Certificate #3879

Details

Module Name
IBM® NVMe FlashCore™ Module 2

Standard
FIPS 140-2

Status
Active

Sunset Date
3/31/2026

Overall Level

2

Caveat

When operated in FIPS mode. When installed, initialized and configured as specified in Section 7 of the Security Policy

Security Level Exceptions

- Mitigation of Other Attacks: N/A

Module Type

Hardware

Embodiment

Multi-Chip Embedded

Description

The IBM® NVMe FlashCore™ Module2 is a NVMe-connected self-encrypting non-volatile storage module.

Tested Configuration(s)

- N/A

Approved Algorithms

AES	Certs. #5897 and #5898
CKG	vendor affirmed
DRBG	Cert. #2454
HMAC	Cert. #3872
KBKDF	Cert. #244
RSA	SHA-3 Cert. #62, vendor affirmed
SHA-3	Cert. #62
SHS	Cert. #4648

Allowed Algorithms

NDRNG

Hardware Versions

02CL181, 02CL183, 02CL185, 02CL187

Firmware Versions

2.0.9.67

Vendor

IBM® Corporation
10777 Westheimer Rd
Houston, TX 77042
USA

Glen Jaquette
jaquette@us.ibm.com
Phone: 713-278-6279

Related Files

Security Policy
Consolidated Certificate

Validation History

Date	Type	Lab
4/1/2021	Initial	LEIDOS CSTL

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Canadian Centre for Cyber Security

April 2021

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Gavin O'Brien

Dated: 05/04/2021

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 2021-05-03

Director, Risk Mitigation Programs
Canadian Centre for Cyber Security

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3879	04/01/2021	IBM(R) NVMe FlashCore(TM) Module 2	IBM(R) Corporation	Hardware Version: 02CL181, 02CL183, 02CL185, 02CL187; Firmware Version: 2.0.9.67
3880	04/03/2021	Cisco FTD FX-OS on 4K/9K Cryptographic Module	Cisco Systems, Inc.	Hardware Version: FPR4110[1], FPR4115[1], FPR4120[1], FPR4125[1], FPR4140[1], FPR4145[1], FPR4150[1], FPR9K-SM-24[2], FPR9K-SM-36[2], FPR9K-SM-40[2], FPR9K-SM-44[2], FPR9K-SM-48[2] and FPR9K-SM-56[2] with FIPS Kit (Cisco_TEL.FIPS_Kit), and opacity shield 69-100250-01[1] or 800-102843-01[2]; Firmware Version: 2.6
3881	04/03/2021	BeyondTrust Cryptographic Module	BeyondTrust Corporation	Software Version: 2.2
3882	04/05/2021	HID Global Applets v3.0 on NXP JCOP 3 SecID P60 CS (OSB)	HID Global	Hardware Version: P6022y VB with product identifier J3H145C; Firmware Version: 19790400 and HID Global ActivID Applet Suite v3.0 with factory configuration FIPS 140-2-L3
3883	04/06/2021	Cisco Catalyst 9800 (40/80/L) Wireless Controllers running IOS-XE 16.12	Cisco Systems, Inc.	Hardware Version: 9800-40, 9800-80 and 9800-L; Firmware Version: IOS-XE 16.12

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3884	04/06/2021	PAN-OS 9.0 Firewalls PA-220, PA-220R, PA-800 Series, PA-3000 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series	Palo Alto Networks, Inc.	Hardware Version: PA-220 P/N 910-000128 Rev. A with [1], PA-220R P/N 910-000147 Rev. B with [2], PA-820 P/N 910-000120 Rev. A with [3], PA-850 P/N 910-000119 Rev. A with [3], PA-3020 P/N 910-000017 Rev. J with [4], PA-3050 P/N 910-000016 Rev. J with [4], PA-3060 P/N 910-000104 Rev. C with [5], PA-3220 P/N 910-000162 Rev. A with [6], PA-3250 P/N 910-000163 Rev. A with [6], PA-3260 P/N 910-000164 Rev. A with [6], PA-5220 P/N 910-000132 Rev. A with [7], PA-5250 P/N 910-000131 Rev. A with [7], PA-5260 P/N 910-000125 Rev. A with [7], PA-5280 P/N 910-000157 Rev. A with [7], PA-5280-K2-EXP: P/N: 910-000257 Rev. A with [7], PA-5280-K2-SEC: P/N: 910-000357 Rev. B with [7], PA-7050 P/N 910-000102 Rev. B with [8], [12], [14] and at least one from [10]; PA-7080 P/N 910-000122 Rev. A with [9], [12], [15] and at least one from [10]; PA-7050 P/N 910-000102 Rev. B with [8], [13], one from [11] and one from [17]; PA-7080 P/N 910-000122 Rev. A with [9], [13], one from [11] and one from [16]; FIPS Kit: P/Ns 920-000084 Rev. A [1], 920-000226 Rev. A [2], 920-000185 Rev. A [3], 920-000081 Rev. A [4], 920-000138 Rev. A [5], 920-000212 Rev. A [6], 920-000186 Rev. A [7], 920-000112 Rev. A [8] and 920-000119 Rev. A [9]; Network Processing Cards [10]: P/Ns 910-000028-00B, 910-000117-00A, 910-000137-00A, 910-000136-00A, 910-000156-00A, 910-000256-00A and 910-000356-00B; Network Processing Cards [11]: P/Ns 910-000156-00A, 910-000256-00A, and 910-000356-00B; Log Processing Card [12]: P/N 910-0000014-00A; Log Forwarding Card [13]: P/N 910-000183-00A; Switch Management Card [14]: P/N 910-000013-00P; Switch Management Card [15]: P/N 910-000012-00L; Switch Management Cards [16]: P/Ns 910-000186-00A, 910-000286-00D, 910-000386-00D; Switch Management Cards [17]: P/Ns 910-000185-00A, 910-000285-00C, 910-000385-00C; Firmware Version: 9.0.9-h1

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3885	04/06/2021	AT-SBx908 Gen2, AT-x950, AT-x550, AT-x530 Secure Management Module	Allied Telesis	Hardware Version: AT-SBx908 Gen2, 990-007222-F00 with [1], [2], [3], [4] [Tamper Label Kit: 066-000080 x 10, 056-000658 x 1] [A], AT-x950-28XTQm, 990-007221-F00 with [2], [5], [Tamper Label Kit: 066-000080 x 4, 056-000658 x 1] [B], AT-x950-28XSQ, 990-007712-F00 with [3], [5], [Tamper Label Kit: 066-000080 x 4, 056-000658 x 1] [B], AT-x550-18XTQ, 990-007217-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x550-18XSQ, 990-007218-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x550-18XSQ, 990-007724-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x550-18XSPQm, 990-007219-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [C], AT-x530-52GTXm, 990-007725-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530-52GPXm, 990-007726-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530-28GTXm, 990-007220-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530-28GPXm, 990-007727-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530L-52GTX, 990-007728-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530L-52GPX, 990-007729-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D], AT-x530L-28GTX, 990-007730-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D] and AT-x530L-28GPX, 990-007731-F90, [Tamper Label Kit: 066-000080 x 1, 056-000658 x 1] [D]; XEM2 Modules [1] 990-005492-00, 990-005490-00, 990-005493-00, 990-006024-00, 990-005491-00, XEM2 Module [2] 990-006242-00 and XEM2 Module [3] 990-006018-00; Power Supply Unit [4] 990-004783-10 and Power Supply Unit [5] 990-006195-10; Firmware Version: 5.4.9.APCERT-2.3; Bootloader Versions bl-6.2.7-SBx908NG-39A8-D2D8.bin [A], bl-6.2.20-x950-1D0D-2BC3.bin [B], bl-6.2.21-x550-2FC1-A0F1.bin [C], bl-7.0.3-x530-noecc-B495-8AEE.kwb [D]
3886	04/07/2021	CryptoServer CSe-Series	Utimaco IS GmbH	Hardware Version: CryptoServer CSe-Series 4.00.5.0 and CryptoServer CSe-Series 4.00.5.1; Firmware Version: SecurityServer-CSe-Series-4.32.0.3-FIPS
3887	04/07/2021	Integral Crypto AES 256 Bit USB 3.0	Integral Memory Plc	Hardware Version: INFD4GCRY3.0140-2, INFD8GCRY3.0140-2, INFD16GCRY3.0140-2, INFD32GCRY3.0140-2, INFD64GCRY3.0140-2, INFD128GCRY3.0140-2, INFD256GCRY3.0140-2, INFD512GCRY3.0140-2, INFD1TCRY3.0140-2, INFD2TCRY3.0140-2, INFD4GCRYDL3.0140-2, INFD8GCRYDL3.0140-2, INFD16GCRYDL3.0140-2, INFD32GCRYDL3.0140-2, INFD64GCRYDL3.0140-2, INFD128GCRYDL3.0140-2, INFD256GCRYDL3.0140-2, INFD512GCRYDL3.0140-2, INFD1TCRYDL3.0140-2, INFD2TCRYDL3.0140-2, INFD4GENVDL3.0-140, INFD8GENVDL3.0-140, INFD16GENVDL3.0-140, INFD32GENVDL3.0-140, INFD64GENVDL3.0-140, INFD128GENVDL3.0-140, INFD256GENVDL3.0-140, INFD512GENVDL3.0-140, INFD1TENVDL3.0-140, INFD2TENVDL3.0-140; Firmware Version: 4.06.10

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3888	04/09/2021	PAN-OS 9.0 VM-Series	Palo Alto Networks, Inc.	Software Version: 9.0.9-h1
3889	04/12/2021	Fortress Mesh Points	General Dynamics Mission Systems	Hardware Version: ES2440, ES520v1, ES520v2 and ES820; Firmware Version: 5.4.6
3890	04/12/2021	TippingPoint Crypto Core OpenSSL	Trend Micro Inc.	Software Version: 1.0.2l-fips
3891	04/12/2021	Red Hat Enterprise Linux 7 OpenSSH Server Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190626
3892	04/12/2021	Red Hat Enterprise Linux 7 OpenSSH Client Cryptographic Module	Red Hat(R), Inc.	Software Version: rhel7.20190626
3893	04/15/2021	Oracle Linux Unbreakable Enterprise Kernel (UEK 5) Cryptographic Module	Oracle Corporation	Software Version: R7-5.0.0
3894	04/15/2021	Panorama Virtual Appliance 9.0	Palo Alto Networks, Inc.	Software Version: 9.0.9
3895	04/15/2021	WildFire 9.0 WF-500	Palo Alto Networks, Inc.	Hardware Version: 910-000097-00G; FIPS Kit P/N: 920-000145-00A; Firmware Version: 9.0.9-h1
3896	04/15/2021	Panorama 9.0 M-100, M-200, M-500 and M-600	Palo Alto Networks, Inc.	Hardware Version: P/Ns 910-000030 Version 00D [1], 910-000092 Version 00D [1], 910-000176 Version 00A [2], 910-000073 Version 00D [3], and 910-000175 Version 00A [4]; FIPS Kit P/Ns 920-000140 Version 00A [1], 920-000208 Version 00A [2], 920-000145 Version 00A [3], and 920-000209 Version 00A [4]; Firmware Version: 9.0.9
3897	04/16/2021	FortiWLM-100D and FortiWLM-1000D	Fortinet, Inc.	Hardware Version: FWM-100D (C1AE82) and FWM-1000D (C1AE83) with Tamper Evident Seal Kit: FIPS-SEAL-RED; Firmware Version: FortiWLM 8.5-2fips-1
3898	04/17/2021	Luna T7 Cryptographic Module	Thales Trusted Cyber Technologies	Hardware Version: 872-500024-001 and 872-500025-001; Firmware Version: 7.11.1 with Boot Loader version 2.0.1
3899	04/19/2021	Aruba IAP-303H, IAP-304, IAP-305, IAP-314, IAP-315, IAP-324, IAP-325, IAP-334, and IAP-335 Wireless Access Points with Aruba Instant Firmware	Aruba, a Hewlett Packard Enterprise company	Hardware Version: [IAP-303H-US TAA (HPE SKU JY681A), IAP-304-US TAA (HPE SKU JX944A), IAP-305-US TAA (HPE SKU JX950A), IAP-314-US TAA (HPE SKU JW808A), IAP-315-US TAA (HPE SKU JW814A), IAP-324-US TAA (HPE SKU JW322A), IAP-325-US TAA (HPE SKU JW328A), IAP-334-US TAA (HPE SKU JW820A), IAP-335-US TAA (HPE SKU JW826A)] with FIPS Kit 4011570-01 (HPE SKU JY894A); Firmware Version: ArubaInstant 8.5.0.12
3900	04/19/2021	Samsung BoringSSL Android	Samsung Electronic Co. Ltd.	Software Version: 1.5
3901	04/19/2021	FIPS AP43	Mist Systems	Hardware Version: AP43-FIPS-US [REV. AA] and AP43E-FIPS-US [REV. AA]; Firmware Version: fips_apfw-0.8.20681-master-5ce6

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3902	04/20/2021	Ubuntu 20.04 Libgcrypt Cryptographic Module	Canonical Ltd.	Software Version: 3.0
3903	04/22/2021	MonoCrypt AES Enhanced Crypto Library	Focus Systems Corporation	Software Version: 2.0.0
3904	04/22/2021	TASS Crypto Engine	Beijing JN TASS Technology Co., Ltd.	Hardware Version: CE2-A2H0O4; Firmware Version: H1.00.00
3905	04/22/2021	CN Series Encryptors	Senetas Corporation Ltd., distributed by Thales SA (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. & SafeNet Inc. CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc. CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Senetas Corp. Ltd. & Thales CN4000 Series: A4010B (DC) and A4020B (DC); Senetas Corp. Ltd. & Thales CN6000 Series: A6010B (AC), A6011B (DC), A6012B (AC/DC), A6140B (AC), A6141B (DC) and A6142B (AC/DC); Senetas Corp. Ltd. & Thales CN9000 Series: A9100B (AC), A9101B (DC), A9102B (AC/DC), A9120B (AC), A9121B (DC) and A9122B (AC/DC); Firmware Version: 5.1.1
3906	04/22/2021	CN6000 Series Encryptors	Senetas Corporation Ltd., distributed by Thales SA (SafeNet)	Hardware Version: Senetas Corp. Ltd. CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & SafeNet Inc CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Senetas Corp. Ltd. & Thales CN6000 Series: A6040B (AC), A6041B (DC), A6042B (AC/DC), A6100B (AC), A6101B (DC) and A6102B (AC/DC); Firmware Version: 5.1.1
3907	04/22/2021	YubiKey 5 Cryptographic Module	Yubico, Inc.	Hardware Version: SLE78CLUFX3000PH and SLE78CLUFX5000PH; Firmware Version: 5.4.2
3908	04/23/2021	Juniper Networks NFX250 Network Services Platform	Juniper Networks, Inc.	Hardware Version: NFX250-S1, NFX250-S1E and NFX250-S2; Firmware Version: Junos OS 20.1R1
3909	04/26/2021	IBM(R) z/OS(R) Version 2 Release 4 ICSF PKCS #11 Cryptographic Module	IBM Corporation	Software Version: ICSF level HCR77D0 with APAR OA58593; Hardware Version: COP chips integrated within processor unit [1] and COP chips integrated within processor unit and P/N 01PP167 [2]; Firmware Version: Feature 3863 (aka FC3863) with System Driver Level 32L [1], and Feature 3863 (aka FC3863) with System Driver Level 32L and CCA 6.0.8z [2]

http://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
3910	04/27/2021	FSM-2 Flash Storage Cryptographic Module	Curtiss-Wright Defense Solutions	Hardware Version: A8; Firmware Version: 4.0

In recognition of the commitment to achieve professional excellence

Alexandre Alvarenga

Has successfully satisfied the requirements for:

IBM Business Partner Storage - Enterprise Storage - Technical Advocate V2

Issued on: 04 JUL 2022

Issued by IBM

Verify: https://www.credly.com/go/E9NdBtK8

IBM

In recognition of the commitment to achieve professional excellence

Alexandre Alvarenga

Has successfully satisfied the requirements for:

IBM Systems Business Partner - Storage for Data Resilience - Technical Advocate V2

Issued on: 04 JUL 2022

Issued by IBM

Verify: https://www.credly.com/go/PcMhOyJS

ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
CONTADORIA E AUDITORIA-GERAL DO ESTADO - CAGE
Rua Siqueira Campos, nº 1044 - Sala 426-B - Centro
90010-001 - Porto Alegre - RS
Fones: 51 3214-5215 ou 3214-5218
E-mail: dcce.cage@sefaz.rs.gov.br

CERTIFICADO DE CAPACIDADE FINANCEIRA RELATIVA DE LICITANTE

Certificado Nº: 90680 **Processo**: 000000-00.00/00-0

Período de Validade: 02/06/2022 até 30/06/2023

CNPJ Nº: 08.706.548/0002-44

Razão Social: O2 SOLUCOES EM TECNOLOGIA DIGITAL

Endereço: RUA AFRANIO MELO FRANCO, 333 / L 4 A 9 E 5 BIS
QUITANDINHA - 25651-000 - PETROPOLIS - RJ

Atividade Principal: 46.51-6-01 - Comércio atacadista de equipamentos de informática

A Contadoria e Auditoria-Geral do Estado - CAGE, com base nas demonstrações contábeis assinadas por **VINICIUS CORREA DE SOUZA** , CRC **RJ-076771/O-5**, concede o presente Certificado, atestando, na forma que dispõe o Decreto Estadual 36.601/96, que a empresa acima identificada possui capacidade financeira relativa para participar de licitações promovidas pela Administração Pública Estadual.

Para fins do disposto no art. 31 da Lei 8.666/93 e conforme as demonstrações contábeis do exercício social encerrado em 31/12/2021, a empresa ora certificada apresenta:

- Receita Bruta Anual no valor de $ 12.923.268,01 *.
- Capital Social Integralizado no valor de $ 1.603.600,00.
- Patrimônio Líquido no valor de $ 2.706.601,98.

Este Certificado substitui,no seu período de validade, a apresentação das Demostrações Contábeis, do Parecer de Auditoria e do Anexo II, de que tratam o Decreto estadual nº 36.601/96 e a Instrução Normativa CAGE nº 2/96.

CAGE 70 ANOS
CUIDANDO DO PRESENTE, ORIENTANDO PARA O FUTURO.

* Excluídas as vendas canceladas e os descontos incondicionais concedidos nos termos do § 1º do art. 3º da LC 123/2006.

Constatando-se, a qualquer tempo, irregularidades nas informações fornecidas pela empresa, este certificado perderá imediatamente sua validade.

Código de Autenticação: **9807485113**

Confira a autenticidade deste documento em **http://www.sisacf.sefaz.rs.gov.br**

PROCURADORIA GERAL DO ESTADO

CERTIDÃO NEGATIVA DE DÉBITOS EM DÍVIDA ATIVA

Certifico que, em consulta ao Sistema da Dívida Ativa no dia 01/08/2022 , em referência ao pedido **172801/2022 , NÃO CONSTA DÉBITO INSCRITO** em Dívida Ativa para o CPF ou CNPJ informado abaixo:

RAZÃO SOCIAL: **O2 SOLUÇÕES EM TECNOLOGIA DIGITAL LTDA**

CNPJ: **08.706.548/0002-44** INSCRIÇÃO ESTADUAL: **12.02777.0**

A certidão negativa de Dívida Ativa e a certidão negativa de ICMS ou a certidão para não contribuinte do ICMS somente terão validade quando apresentadas em conjunto.

Fica ressalvado o direito da Fazenda Estadual de inscrever e cobrar débitos que vierem a ser apurados posteriormente à emissão da presente certidão.

A aceitação desta certidão está condicionada a verificação de sua autenticidade na INTERNET, no endereço: https://pge.rj.gov.br/divida-ativa/certidao-de-regularidade-fiscal

CÓDIGO CERTIDÃO: **0KS6.5210.6211.L075**

PESQUISA CADASTRAL realizada em: **01/08/2022 às 17:24:45.8**

Esta certidão tem validade até 28/01/2023 , considerando 180 (cento e oitenta) dias após a pesquisa cadastral realizada na data e hora acima, conforme artigo 11 da Resolução nº 2690 de 05/10/2009.

Para maiores informações: https://pge.rj.gov.br/divida-ativa

Emitida em 11/08/2022 às 13:47:51.5

GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE FAZENDA

CERTIDÃO DE REGULARIDADE FISCAL Nº: 10-2022/1283045

Código de verificação de autenticidade: 27156193ec0ded93825994874b91421c

CERTIDÃO NEGATIVA DE DÉBITOS - CND

IDENTIFICAÇÃO DO REQUERENTE	
CPF / CNPJ: 08.706.548/0002-44	CAD-ICMS: Ativo
NOME / RAZÃO SOCIAL: O2 SOLUÇÕES EM TECNOLOGIA DIGITAL LTDA	

CERTIFICAMOS, para os fins de direito, e de acordo com as informações registradas nos Sistemas Corporativos da Secretaria de Estado de Fazenda e Planejamento, que, até a presente data,
NÃO CONSTAM DÉBITOS perante a RECEITA ESTADUAL para o requerente acima identificado, ressalvado o direito de a Receita Estadual cobrar e inscrever as dívidas de sua responsabilidade, que vierem a ser apuradas.

EMITIDA EM: 11/10/2022 ÀS 13:51:03

VÁLIDA ATÉ: 09/01/2023

Certidão emitida com base na Resolução SEFAZ nº 109 de 04/08/2017

OBSERVAÇÕES

Esta certidão deve estar acompanhada da Certidão Negativa da Dívida Ativa, emitida pelo órgão próprio da Procuradoria Geral do Estado, nos termos da Resolução Conjunta PGE/SER nº 33/2004.

A autenticidade desta certidão pode ser confirmada pela Internet (http://www10.fazenda.rj.gov.br/SATI-FiscoFacil/publico/autenticidadeHashCertidao/consultaAutenticidadeHash.xhtml).

A verificação de débitos é efetuada pelo CNPJ do requerente, abrangendo sua regularidade fiscal e de estabelecimentos que porventura possuir com mesma raiz de CNPJ. A razão social, quando indicada, é informação apenas ilustrativa.

O campo CAD-ICMS atesta a situação do CNPJ do requerente no Cadastro Estadual de Contribuintes do ICMS: ATIVO - estabelecimento inscrito e ativo; DESATIVADO - estabelecimento inscrito e desativado; NÃO INSCRITO - estabelecimento sem qualquer inscrição. No caso de estabelecimento inscrito no CAD-ICMS, sua identificação deveráser obtida pelo Comprovante de Inscrição e de Situação Cadastral (www.fazenda.rj.gov.br).

A condição de não-inscrito ou desativado não desobriga o requerente de possuir inscrição ativa no Cadastro de Contribuintes do ICMS do Estado do Rio de Janeiro caso exerça atividade relacionada no artigo 20 do Anexo I da Parte II da Resolução SEFAZ nº 720/2014.

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 08.706.548/0002-44
Razão Social: O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA
Endereço: RUA AFRANIO DE MELO 333 LJ 4 A 9 E 5 BIS / QUITANDINHA / PETROPOLIS / RJ / 25651-000

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade: 03/11/2022 a 02/12/2022

Certificação Número: 2022110300500515461040

Informação obtida em 18/11/2022 15:07:29

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

Prefeitura Municipal de Petrópolis

Secretaria Municipal de Fazenda
Departamento de Receita

CERTIDÃO NEGATIVA DE TRIBUTOS MUNICIPAIS

Número Certidão: 202202407

CPF/CNPJ: 08.706.548/0002-44

Contribuinte: O2 SOLUÇÕES EM TECNOLOGIA DIGITAL LTDA

Endereço: RUA AFRÂNIO MELO FRANCO - Nº: 333 - QUITANDINHA - CEP: 25651000

Certificamos, de acordo com informações apuradas nos sistemas de controle de Tributos Municipais, que não constam débitos referente aos dados informados acima.

Requerente: Marcos Arino Motta de Oliveira

CPF: 711.177.337-34

Data da Emissão: 06/06/2022

Validade: 03/12/2022 - 180 dias (Decreto n° 758 de 14/05/2019)

Esta Certidão refere-se a Débitos de natureza tributária ou não tributária, IPTU, ISS, ITBI, Taxas Diversas, Autos de Multa, Notas de Débito, inscritos ou não em Dívida Ativa.

Fica ressalvado, entretanto, o direito de a Fazenda Municipal cobrar as dívidas, que porventura venham a ser apuradas

Qualquer rasura ou emenda invalidará este documento

Autenticação

Av. Koeler, 260 (Anexo "B") – Centro - CEP: 25685-060 - Petrópolis - RJ / Telefones: (24) 2246-8522 / 2242-8892

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA (MATRIZ E FILIAIS)
CNPJ: 08.706.548/0002-44
Certidão nº: 24458794/2022
Expedição: 02/08/2022, às 11:25:59
Validade: 29/01/2023 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **O2 SOLUCOES EM TECNOLOGIA DIGITAL LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **08.706.548/0002-44**, **NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.° 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.