TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Ata de Registro de Preços Nº 02/2021

Pregão Eletrônico nº 07/2021	**Processo SEI nº 0018160-27.2020.6.18.8000**

O TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, inscrito no CNPJ/MF sob o n° 05.957.363/0001-33, situado no endereço Praça Des. Edgar Nogueira, S/N - Centro Cívico - Bairro Cabral - CEP 64000-920 - Teresina (PI), neste ato representado por seu Presidente, Des. JOSÉ JAMES GOMES PEREIRA, com fundamento na Lei n° 8.666/93 e no Decreto n° 7.892/2013, emite a presente Ata de Registro de Preços com o objetivo de formalizar o Registro de Preços para contratação de certificados digitais e emissão de tokens USB, em decorrência das propostas apresentadas no Pregão Eletrônico n° 07/2021 e em conformidade com os Anexos do Edital do referido Pregão Eletrônico.

1. Os dados relativos ao licitante vencedor e aos itens registrados estão especificados nos quadros a seguir:

1.1. Dados referentes ao licitante vencedor:

Empresa: AR RP CERTIFICAÇÃO DIGITAL EIRELI	**CNPJ:21.308.480/0001-22**
Endereço: Rua Marechal Rondon, N° 401, Sala 03, Setor Jardim América, Ribeirão Preto - SP, CEP: 14.020-220	**Telefone:** (11) 3504-8750 **E-mail:** licitacoes@rpcd.com.br
Representante legal: Juliana Cristina Moreira Guimarães	**CPF:**

1.2. Dados relativos aos itens registrados, em conformidade com as especificações constantes nos Anexos do Edital licitatório:

Item	Especificação	Quantidade	Valor unitário (R$)	Valor total (R$)
1	**CERT-JUS INSTITUCIONAL A3 - 3 ANOS** Certificado digital do tipo A3 para pessoa física, padrão ICP-Brasil, compatível com a AC-JUS, com prazo de validade de 3 (três) anos;	70	R$ 23,27	R$ 1.628,90
2	**VISITA TECNICA LOCAL** As visitas para emissão dos certificados digitais deverão ser realizadas na sede do Tribunal Regional Eleitoral do Piauí, na cidade de Teresina-PI	5	R$ 51,00	R$ 255,00
3	**TOKEN (SAFENET)** Token criptográfico USB capaz de armazenar certificados, chaves e cadeias de certificados aderentes às normas do Comitê Gestor da ICP-Brasil. MARCA:SAFENET MODELO: ETOKEN 5110	70	R$ 36,00	R$ 2.520,00

2. A presente Ata de Registro de Preços terá vigência de 12 (doze) meses, a contar da data de sua publicação.

3. A existência de preços registrados não obriga o TRE-PI a efetuar as aquisições, facultando-se a realização de licitação específica para as aquisições pretendidas. Nesse caso, o beneficiário do registro de preços terá preferência de fornecimento, em igualdade de condições.

4. As quantidades constantes do Anexo I do edital licitatório são estimativas máximas para eventual fornecimento, durante o prazo de vigência da Ata de Registro de Preços.

4.1. As aquisições ocorrerão em conformidade com as necessidades e conveniências do TRE-PI, facultada a aquisição parcial, total ou mesmo a não aquisição dos materiais licitados.

5. O licitante vencedor deverá atender às solicitações de fornecimento dos produtos, entregando-os em perfeitas condições de uso e armazenamento, no prazo máximo estipulado na Ordem de Fornecimento, a contar do recebimento da respectiva Ordem de Fornecimento e Nota de Empenho, conforme especificado no Termo de Referência.

5.1. O licitante vencedor será responsável pela confirmação do local e horário de entrega dos materiais mediante contato telefônico com a Seção de Almoxarifado e Patrimônio, pelo telefone (86) 2107-9811.

5.2. O licitante deverá atender aos pedidos formalizados durante a vigência da Ata de Registro de Preços, ainda que a entrega seja prevista para data posterior a sua vigência.

6. O eventual fornecimento, objeto da presente Ata de Registro de Preços, obedecerá ao estipulado neste instrumento, bem como às disposições do Pregão Eletrônico nº 07/2021, além das disposições constantes da proposta apresentada pelo licitante vencedor, que independentemente de transcrição, fazem parte integrante e complementar deste documento, no que não o contrarie.

7. O licitante vencedor tem obrigação de manter, durante toda a vigência da Ata de Registro de Preços, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

E, por estarem justos e contratados, foi lavrado o presente instrumento no Sistema Eletrônico de Informações que, após lido e achado conforme vai assinado pelas partes.

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Des. JOSÉ JAMES GOMES PEREIRA
Presidente

AR RP CERTIFICAÇÃO DIGITAL EIRELI
Juliana Cristina Moreira Guimarães
Representante

Documento assinado eletronicamente por **JULIANA CRISTINA MOREIRA GUIMARAES**, **Usuário Externo**, em 28/04/2021, às 20:59, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **José James Gomes Pereira**, **Presidente**, em 29/04/2021, às 10:14, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1233598** e o código CRC **514B52BD**.

Neg.: 24238

AO,
TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

REFERENTE:

Pregão Eletrônico N.º: 07/2021
Modalidade: Menor Preço Por Item
Processo SEI Nº: 0018160-27.2020.6.18.8000
Data da negociação: 02/03/2021 às 14:00 horas

RAZÃO SOCIAL: AR RP CERTIFICACAO DIGITAL EIRELI
IE: 35.600.746.401 **CNPJ:** 21.308.480/0001-22
Ins. Municipal: 20026631 **Ins. Estadual:** 797.089.188.110
Endereço: Rua Marechal Rondon, N° 401, Sala 03, Setor Jardim América, Ribeirão Preto - SP, Cep: 14.020-220
Fone: 11 3504-8750 **E-mail:** licitacoes@rpcd.com.br
Banco: Caixa Econômica Federal **Agência nº** 003 **OP**: **Conta Corrente nº** 587-0
Banco: Santander **Agência nº** 910 **Conta Corrente nº** 13000741-0
Contato: Juliana Cristina Moreira Guimarães

PROPOSTA COMERCIAL

DO OBJETO: O objeto pretendido por esta contratação é o registro de preços para contratação de serviços de emissão de Certificados Digitais A3 padrão ICP-Brasil para pessoa física e fornecimento de dispositivos tokens USB para armazenamento.

Item	Especificação	Quant.	Valor Unitário	Valor Total
1	CERT-JUS INSTITUCIONAL A3 - 3 ANOS Certificado digital do tipo A3 para pessoa física, padrão ICP-Brasil, compatível com a AC-JUS, com prazo de validade de 3 (três) anos;	70	$ 23,27	R$ 1.628,90
2	VISITA TECNICA LOCAL As visitas para emissão dos certificados digitais deverão ser realizadas na sede do Tribunal Regional Eleitoral do Piauí, na cidade de Teresina- PI;	5	R$ 51,00	R$ 255,00
3	TOKEN (SAFENET) Token criptográfico USB capaz de armazenar certificados, chaves e cadeias de certificados aderentes às normas do Comitê Gestor da ICP-Brasil;	70	R$ 36,00	R$ 2.520,00
Valor total: Quatro Mil e Quatrocentos e Três Reais e Noventa Centavos				**R$ 4.403,90**

- **Marca do Certificado:** AC SOLUTI;
- **Marca / Modelo do Equipamento:** MARCA: SAFENET MODELO: ETOKEN 5110;

A **AR RP CERTIFICACAO DIGITAL EIRELI**, declara inteira submissão aos preceitos legais em vigor, especialmente aos da Lei 10.520/02, do Decreto nº 5.450/05, da Lei nº 8.666/93, e às cláusulas e condições constantes do **Pregão Eletrônico n° 07-2021 TRIBUNAL REGIONAL ELEITORAL – PI ,** tem plena ciência do conteúdo e aceita todas as exigências do Edital e seus anexos, O valor do preço unitário e o valor total estão detalhados nesta proposta de preço, nos quais estão incluídas todas as despesas diretas e indiretas, inclusive impostos, taxas de qualquer natureza, contribuições, alvarás, mão de obra, salários, encargos sociais, previdenciários e trabalhistas, embalagens, transportes, seguros, peças de reposição, materiais utilizados na manutenção e quaisquer outras despesas necessárias que incidam ou venham a incidir sobre a execução do objeto desta licitação, propondo sua execução pelo valor **R$ 4.403,90 (Quatro Mil e Quatrocentos e Três Reais e Noventa Centavos)** observados os valores unitários cotados na planilha acima.

1. **VALIDADE DA PRPOSPOTA:**

- O prazo de validade desta proposta é de 90 (noventa) dias corridos, a contar da data prevista para sua abertura, esteja expressamente indicado ou não na proposta.

2. **DA ENTREGA DOS SERVIÇOS**

- **Prazo e entrega dos matérias:** 30 (trinta) dias corridos, contados a partir da data de recebimento da ordem de fornecimento. Os produtos deverão ser entregues na **Seção de Almoxarifado e Patrimônio**, Sede do Tribunal Regional Eleitoral do Piauí, CNPJ Nº 05.957.363/0001-33, localizado na Praça. Des. Edgar Nogueira, S/N, Centro Cívico, bairro Cabral, em Teresina-PI, CEP: 64000-920, em dia de expediente normal, no horário de 7h às 13h.

- **Prazo e entrega dos serviços:** As visitas técnicas para validação e emissão de certificados digitais serão realizadas conforme agendamento de data e horário pelo Tribunal, em conformidade com os dispositivos constantes do edital e seus anexos, e encaminhado junto à Central de Serviços da contratada, por meio de Ordem de Serviço, com antecedência mínima de 5 (cinco) dias úteis.

3. **DA GARANTIA**

- **Garantia: Pagamento:** Conforme previsto no Edital e Termo de Referência do Pregão Eletrônico n° 07/2021 Tribunal Regional Eleitoral – PI.

4. SUPORTE TÉCNICO

- **Suporte Técnico:** Conforme previsto no Edital e Termo de Referência do Pregão Eletrônico n° 07/2021 Tribunal Regional Eleitoral – PI.

5. PAGAMENTO

- **Pagamento:** Conforme previsto no Edital e Termo de Referência do Pregão Eletrônico n° 07/2021 Tribunal Regional Eleitoral – PI.

6. DAS DECLARAÇÕES:

- O preço proposto abrange todos os tributos (impostos, taxas, emolumentos, contribuições fiscais e para fiscais), mão-de-obra, prestação do serviço, leis sociais, administração, lucros, equipamentos e ferramental, transporte de material e de pessoal, translado, seguro do pessoal utilizado nos serviços contra riscos de acidente de trabalho, cumprimento de todas as obrigações que a legislação trabalhista e previdenciária impõem ao empregador e qualquer despesa acessória e/ou necessária, não especificada no edital.

Dados da Autoridade competente que assinará o Contrato:
Nome: Juliana Cristina Moreira Guimarães
Cargo: Procuradora
Documento de Identidade: nº 5466356 Órgão Expedidor: SPTC-GO
CPF nº 035.827.821-07
Residente e domiciliado em: Goiânia-GO

Goiânia, 05 de março de 2021.

Atenciosamente,

21.308.480/0001-22
AR RP CERTIFICAÇÃO DIGITAL EIRELI
Rua Marechal Rondon, nº 401, Sala 03
Jardim América CEP 14.020-220
RIBEIRÃO PRETO - SP

Juliana Cristina Moreira Guimarães
Procuradora

Digitally signed by: JULIANA CRISTINA MOREIRA GUIMARAES
JULIANA CRISTINA MOR 05/03/2021 09:45:25

ID: 3GU2TMMJY-GEZDMMJRHE-XSALAYTWB55YO

AO,
TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

REFERENTE:

Pregão Eletrônico N.º: 07/2021
Modalidade: Menor Preço Por Item
Processo SEI Nº: 0018160-27.2020.6.18.8000
Data da negociação: 02/03/2021 às 14:00 horas

RAZÃO SOCIAL: AR RP CERTIFICAÇÃO DIGITAL EIRELI	**CNPJ:** 21.308.480/0001-22
NOME FANTASIA: AR RP CERTIFICAÇÃO DIGITAL	
ENDEREÇO: Rua Marechal Rondon, N° 401, Sala 03, Setor Jardim América	
BAIRRO: Jardim America	**CIDADE:** Riberão Preto
UF: SP	**CEP:** 14.020.220
TELEFONE: (11) 3504-8750	**E-mail:** licitacoes@rpcd.com.br
Banco: Caixa Econômica Federal **Agência nº** 003 **OP**: **Conta Corrente nº** 587-0 **Banco:** Santander **Agência nº** 910 **Conta Corrente nº** 13000741-0	
Responsável Contratual: Juliana Cristina Moreira Guimarães **Função:** Procuradora **Telefone:** (11) 3504-8750 **E-mail:** licitacoes@rpcd.com.br **RG:** 5466356 STPC/GO **CPF:** 035.827.821-07	

Goiânia, 05 de março de 2021.

Atenciosamente,

Juliana Cristina Moreira Guimarães

Juliana Cristina Moreira Guimarães
Procuradora

Digitally signed by:
JULIANA CRISTINA MOR
JULIANA CRISTINA MOREIRA GUIMARAES
05/03/2021 09:45:25

ID: 3GU2TMMJY-GEZDMMJRHE-XSALAYTWB55YO

21.308.480/0001-22
AR RP CERTIFICAÇÃO DIGITAL EIRELI
Rua Marechal Rondon, nº 401, Sala 03
Jardim América CEP 14.020-220
RIBEIRÃO PRETO - SP

PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Instituto Nacional de Tecnologia da Informação

ATO DECLARATÓRIO EXECUTIVO Nº 08/2013 ITI/PR, DE 03/04/2013

Divulga o resultado do Processo 00100.0000107/2013-52 relativo à homologação, no âmbito da ICP-Brasil, de Token Criptográfico – Modelo eToken 510x

O DIRETOR DE INFRAESTRUTURA DE CHAVES PÚBLICAS DO ITI, no uso da atribuição que lhe confere o item 3.3.1 do Anexo à Resolução 36 do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, de 21 de outubro de 2004,

DECLARA:

Art. 1º - Este Ato Declaratório se refere ao Processo 00100.0000107/2013-52, relativo à homologação de dispositivo do tipo Token Criptográfico – Modelo eToken 510x, Versão do COS "Athena IDProtect 0106.0113.2109", Chipset "Inside AT90SC25672RCT-USB", da empresa SAFENET, INC.

Art 2° - O equipamento acima foi avaliado pelo Laboratório de Ensaios e Auditoria – LEA, com relação aos requisitos técnicos de segurança e interoperabilidade exigidos pelo Manual de Condutas Técnicas nº 3 - Volume I - versão 3.0, considerando o Nível de Segurança de Homologação 1, e apresentou-se em conformidade com tais requisitos, conforme Laudo de Conformidade emitido por aquele Laboratório em 25 de março de 2013.

Art 3° - Face ao exposto, o equipamento avaliado está homologado pelo ITI, no Nível de Segurança de Homologação 1, em estrita observância à legislação aplicável, atendendo em especial aos seguintes normativos:

I - Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil – v.2.0 (DOC-ICP-10) – aprovado pela Resolução 36 do Comitê Gestor da ICP-Brasil, em 21.10.2004;

II - Estrutura Normativa Técnica e Níveis de Segurança de Homologação a serem utilizados nos Processos de Homologação de Sistemas e Equipamentos de Certificação Digital no âmbito da ICP-Brasil – v 3.0 (DOC-ICP-10.02) - aprovado pela Instrução Normativa 02-2007 do ITI, em 11.12.2007;

III - Padrões e Procedimentos técnicos a serem observados nos processos de homologação de cartões inteligentes (smart cards), leitoras de cartões inteligentes e tokens criptográficos no âmbito da ICP-Brasil – v.3.0 (DOC-ICP-10.03) – aprovado pela Instrução Normativa 03-2007 do ITI, em 11.12.2007;

IV - Manual de Condutas Técnicas nº 3 (MCT-3) – Volume I – v.3.0 – publicado no sítio www.iti.gov.br.

Art 4° Em decorrência da presente homologação a parte interessada poderá utilizar, no equipamento homologado, o Selo de Homologação, na forma prevista no item 4 do DOC-ICP-10, adotando a seguinte numeração: **0008-13-0003-07.**

MAURÍCIO AUGUSTO COELHO

CONTROLE DE ALTERAÇÕES

Documento que aprovou alteração	*Item Alterado*	*Descrição da Alteração*

SafeNet eToken 5100

PRODUCT BRIEF

Benefits

- Improves productivity by allowing employees and partners to securely access corporate resources
- Enables advanced certificate-based applications such as digital signature and pre-boot authentication
- Common Criteria certified
- Portable USB token: no special reader needed
- Simple and easy to use – no training or technical know-how needed
- Expand security applications through on-board Java applets
- Enhance marketing and branding initiatives with private labeling and color options
- Offers combined physical and logical access

To protect identities and critical business applications in today's digital business environment, organizations need to ensure that access to online and network resources is always secure, while maintaining compliance with security and privacy regulations.

SafeNet eToken 5100 offers two-factor authentication for secure remote and network access as well as certificate-based support for advanced security applications including digital signature and pre-boot authentication.

Two-Factor Authentication you can Trust

SafeNet eToken 5100 is a portable two-factor USB authenticator with advanced smart card technology. It utilizes certificate based technology to generate and store credentials, such as private keys, passwords and digital certificates inside the protected environment of the smart card chip. To authenticate, users must supply both their personal SafeNet authenticator and password, providing a critical second level of security beyond simple passwords to protect valuable digital business resources.

Future Proofed and Scalable with Centralized Management Control

SafeNet eToken 5100 integrates seamlessly with third party applications through SafeNet Authentication development tools, supports SafeNet PKI and password management applications and software development tools, and allows customization of applications and extension of functionality through on-board Java applets. It is also supported by SafeNet Authentication Manager, which reduces IT overhead by streamlining all authentication operations including deployment, provisioning, enrollment and ongoing maintenance, as well as offering support for lost tokens.

Supported Applications

- Secure remote access to VPNs and Web portals
- Secure network logon
- Digital signing
- Pre-boot authentication

Technical Specifications

Supported operating systems	Windows Server 2003/R2, Windows Server 2008/ R2, Windows 7, Windows XP/Vista, Mac OS X; Linux
API & standards support	KCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
Memory size	72K
On-board security algorithms	RSA 1024-bit / 2048-bit, DES, 3DES (Triple DES), SHA1, SHA256
Security certifications	Common Criteria EAL4+
Dimensions	5100 - 16.4mm x 8.4mm x 40.2mm (Mini) 5105 - 16.4mm x 8.4mm x 53.6mm (Midi)
ISO specification support	Support for ISO 7816-1 to 4 specifications
Operating temperature	0º C to 70º C (32º F to 158º F)
Storage temperature	-40º C to 85º C (-40º F to 185º F)
Humidity rating	0-100% without condensation
Water resistance certification	IP X7 – IEC 529
USB connector	USB type A; supports USB 1.1 and 2.0 (full speed and high speed)
Casing	Hard molded plastic, tamper evident
Memory data retention	At least 10 years
Memory cell rewrites	At least 500,000

The SafeNet Family of Authentication Solutions

Offering flexible management platforms, the broadest range of strong authentication methodologies and form factors, transaction verification capabilities as well as identity federation and Single Sign-on, SafeNet solutions create a future ready security foundation that allows organizations to adopt a modular, forward looking identity management strategy, ensuring that their security needs are met as new threats, devices and use cases evolve. To learn more about SafeNet's complete portfolio of authentication solutions, please visit our website at www.safenet-inc.com/authentication

2009 SC Magazine "Best Buy" 5-Star Rating

Network Product Guide's Best in Tokens

2009 WindowSecurity.com Reader's Choice 1st Runner Up

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected

Certificados

Resultado da Consulta:
21 Certificado(s)
21 Produtos(s)
0 Serviços(s)

Página 1

Certificador: NCC **Nº Certificado:** NCC 16.04488 **Tipo:** Produto **Emissão:** 12/12/2016 **Validade:** 12/12/2022 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
10206543000113	CIS ELETRÔNICA DA AMAZÔNIA LTDA	CIS ELETRÔNICA DA AMAZÔNIA LTDA	AVENIDA AÇAÍ,, 875 - BL.A - DISTRITO INDUSTRIAL - MANAUS, AM - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
CIS	SCR 3310 V2.0 RD1-X	NÃO	LEITORA DE CARTÕES INTELIGENTES PARA USO NO ÂMBITO DA ICP-BRASIL - HARDWARE: V3.0 / FIRMWARE: SMARTOS / SEGURANÇA: NSC 1

Certificador: NCC **Nº Certificado:** NCC 17.04547 **Tipo:** Produto **Emissão:** 30/01/2017 **Validade:** 30/01/2023 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
01586633000196	GEMALTO DO BRASIL CARTOES E TERMINAIS LTDA.	GEMALTO DO BRASIL	AV. NOSSA SENHORA DA BOA ESPERANÇA, 367 - - CENTRO - PINHAIS, PR - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
GEMALTO	IDBRIDGE CT30	NÃO	LEITOR / GRAVADOR DE CARTÃO INTELIGENTE - NSC 1 / FIRMWARE: V3.1

Certificador: NCC **Nº Certificado:** NCC 17.04618 **Tipo:** Produto **Emissão:** 14/03/2017 **Validade:** 14/03/2025 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
03514896000115	THOMAS GREG & SONS, GRÁFICA E SERVIÇOS, INDÚSTRIA E COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO DE EQUIPAMENTOS LTDA.	THOMAS GREG & SONS DO BRASIL	RUA GENERAL BERTOLDO KLINGER, 69, 89, 111, 131 - E FUNDOS - VILA PAULICÉIA - SÃO BERNARDO CAMPO, SP - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
NXP	JCOP 2.4.2 R2	NÃO	CARTÃO CRIPTOGRÁFICO (SMART CARD) PARA USO NO ÂMBITO DA ICP-BRASIL - SOFTWARE: SAFESIGN 3.0.45 | FIRMWARE: JCOP 2.4.2 R2 MASK ID 59 | NÍVEL DE SEGURANÇA: NSC 1

Certificador: NCC **Nº Certificado:** NCC 17.04636 **Tipo:** Produto **Emissão:** 28/03/2017 **Validade:** 28/03/2023 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa

01586633000196	GEMALTO DO BRASIL CARTOES E TERMINAIS LTDA.	GEMALTO DO BRASIL	AV. NOSSA SENHORA DA BOA ESPERANÇA, 367 - - CENTRO - PINHAIS, PR - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
SAFENET GEMALTO	ETOKEN 5110	SIM	TOKEN CRIPTOGRÁFICO PARA USO NO ÂMBITO DA ICP-BRASIL - HARDWARE: STM32F042K6U6TR | SOFTWARE: SAFENET AUTHENTICATION CLIENT V10.2.19.0 | FIRMWARE: IDCORE30-REVBBUILD06 | NSC1

Certificador: NCC **Nº Certificado:** NCC 17.04848 **Tipo:** Produto **Emissão:** 01/09/2017 **Validade:** 01/09/2023 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
04400995000309	GIESECKE & DEVRIENT AMÉRICA DO SUL INDÚSTRIA E COMÉRCIO DE SMART CARDS S/A	GIESECKE & DEVRIENT	AV. PAPA JOÃO PAULO I, 5627 - - RES. PARQUE CUMBICA - GUARULHOS, SP - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
G&D	SCE 3.2 80K	NÃO	CARTÃO CRIPTOGRÁFICO (SMART CARD) PARA USO NO ÂMBITO DA ICP-BRASIL - SAFESIGN STANDARD V3.0.112/ CPDIXJC_RSEFI-025CD80V100/ NSC1

Certificador: NCC **Nº Certificado:** NCC 17.04870 **Tipo:** Produto **Emissão:** 19/09/2017 **Validade:** 19/09/2023 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
17423726000130	DINAMO NETWORKS - SERVIÇOS, DESENVOLVIMENTO E PARTICIPAÇÕES OU EMPRESAS LTDA.	DINAMO NETWORKS	ST SCN - QD 05 / BL. A (ED.EMPR.BRASÍLIA SHOPPING), 50 - SL.416 - ASA NORTE - BRASÍLIA, DF - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
DINAMO	DINAMO POCKET	NÃO	MÓDULO DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL - HARDWARE: 4.1.19A | SOFTWARE: 3.2.3.0 | FIRMWARE: 3.10.0.3 | NSC1

Certificador: NCC **Nº Certificado:** NCC 17.04935 **Tipo:** Produto **Emissão:** 23/10/2017 **Validade:** 23/10/2023 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
06137098000100	IDEMIA DO BRASIL - SOLUCOES E SERVICOS DE TECNOLOGIA LTDA		AV BRIGADEIRO FARIA LIMA, 1336 - 5º/51,52 - JD. PAULISTANO - SÃO PAULO, SP - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
ID-ONE COSMO	ID-ONE COSMO V7.0.1	NÃO	CARTÃO CRIPTOGRÁFICO (SMART CARD) PARA USO NO ÂMBITO DA ICP-BRASIL - SOFTWARE: AWP MANAGER V5.1.8 SR1| FIRMWARE: COSMOV701 V077121| NSC1

Certificador: NCC **Nº Certificado:** NCC 17.04984 **Tipo:** Produto **Emissão:** 24/11/2017 **Validade:** 24/11/2023 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
04400995000309	GIESECKE & DEVRIENT AMÉRICA DO SUL INDÚSTRIA E COMÉRCIO DE SMART CARDS S/A	GIESECKE & DEVRIENT	AV. PAPA JOÃO PAULO I, 5627 - - RES. PARQUE CUMBICA - GUARULHOS, SP - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
G&D	STARSIGN CRYPTO USB-TOKEN S	NÃO	TOKEN CRIPTOGRÁFICO PARA USO NO ÂMBITO DA ICP-BRASIL - HARDWARE: SLE78CUFX5000PH (M7893 B11) | SOFTWARE: 3.0.124 | FIRMWARE: SM@RTCAFÉ EXPERT 7.0,

	DEMONSTRATION APPLET V1.0 | NSC1

Certificador: NCC Nº Certificado: NCC 18.05104 Tipo: Produto Emissão: 15/02/2018 Validade: 15/02/2024 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
92080035000104	PERTO S.A. PERIFÉRICOS PARA AUTOMAÇÃO.	PERTO S.A. PERIFÉRICOS PARA AUTOMAÇÃO.	RUA NISSIN CASTIEL, 640 - - DISTRITO INDUSTRIAL - GRAVATAÍ, RS - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
PERTO	CCID	NÃO	LEITORA DE CARTÕES INTELIGENTES PARA USO NO ÂMBITO DA ICP-BRASIL - HARDWARE: ACS AC1038SAM (204.04.753 REVISÃO D) | FIRMWARE: 112C | NSC1 | OBS: ESTE MODELO TAMBÉM PODE SER IDENTIFICADO COMO PERTOSMART PS-1000_CCID E PERTOSMART CCID

Certificador: NCC Nº Certificado: NCC 18.05201 Tipo: Produto Emissão: 18/04/2018 Validade: 18/04/2024 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
92702067000196	BANCO DO ESTADO DO RIO GRANDE DO SUL SA	BANRISUL	R CAPITAO MONTANHA, 177 - - CENTRO - PORTO ALEGRE, RS - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
BANRISUL	BANRISUL CARTÃO MÚLTIPLO	NÃO	CARTÃO CRIPTOGRÁFICO (SMART CARD) PARA USO NO ÂMBITO DA ICP-BRASIL - SOFTWARE: 3.1.00 | FIRMWARE: MULTOS V4.2.1 | NSC1

Certificador: NCC Nº Certificado: NCC 18.05455 Tipo: Produto Emissão: 30/10/2018 Validade: 30/10/2024 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
01586633000196	GEMALTO DO BRASIL CARTOES E TERMINAIS LTDA.	GEMALTO DO BRASIL	AV. NOSSA SENHORA DA BOA ESPERANÇA, 367 - - CENTRO - PINHAIS, PR - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
GEMALTO	IDPRIME MD 830B	NÃO	CARTÃO CRIPTOGRÁFICO (SMART CARD) PARA USO NO ÂMBITO DA ICP-BRASIL - HARDWARE: SLE78CFX3000PH I FIRMWARE: IDCORE30 VER B I NSC1

Certificador: NCC Nº Certificado: NCC 18.05527 Tipo: Produto Emissão: 12/12/2018 Validade: 12/12/2026 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
05761098000113	KRYPTUS SEGURANCA DA INFORMACAO S.A.	KRYPTUS SOLUCOES EM SEGURANCA DA INFORMA	RUA MARIA TEREZA DIAS DA SILVA, 270 - - CIDADE UNIVERSITÁRIA - CAMPINAS, SP - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
KRYPTUS	ASI-HSM AHX5 KNET CRYPTOGRAPHIC MODULE	NÃO	MÓDULO DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL - VERSÃO DE HARDWARE: 1.0.1 I VERSÃO DE SOFTWARE: 1.0.0 I VERSÃO DE FIRMWARE: 1.0.1 I NSC: 3

Certificador: NCC Nº Certificado: NCC 19.05644 Tipo: Produto Emissão: 13/03/2019 Validade: 13/03/2027 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
33113309000147	VALID SOLUÇÕES S.A.		PETER LUND, 146 - - - RIO DE JANEIRO, SP - BRASIL	ATIVO	SOLICITANTE

33113309004800	VALID SOLUÇÕES S.A. – UNIDADE SOROCABA		LAURA MAIELLO KOOK, - - - SOROCABA, - BRASIL	ATIVO	FABRICANTE

Marca	Modelo	Importado	Descrição
NXP	JCOP 3 SECID P60 CS	NÃO	CARTÃO CRIPTOGRÁFICO (SMART CARD) PARA USO NO ÂMBITO DA ICP-BRASIL

Certificador: NCC Nº Certificado: NCC 19.05710 Tipo: Produto Emissão: 13/05/2019 Validade: 13/05/2025 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
01586633000196	GEMALTO DO BRASIL CARTOES E TERMINAIS LTDA.	GEMALTO DO BRASIL	AV. NOSSA SENHORA DA BOA ESPERANÇA, 367 - - CENTRO - PINHAIS, PR - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
GEMALTO	IDCORE 30	NÃO	CARTÃO CRIPTOGRÁFICO (SMART CARD) PARA USO NO ÂMBITO DA ICP-BRASIL I VERSÃO DE HARDWARE: SLE78CFX3009P I VERSÃO DE SOFTWARE: SAFESIGN STANDARD 3.0.87 I VERSÃO DE FIRMWARE: IDCORE30 BUILD 1.16

Certificador: NCC Nº Certificado: NCC 19.05730 Tipo: Produto Emissão: 24/05/2019 Validade: 24/05/2027 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
05761098000113	KRYPTUS SEGURANCA DA INFORMACAO S.A.	KRYPTUS SOLUCOES EM SEGURANCA DA INFORMA	RUA MARIA TEREZA DIAS DA SILVA, 270 - - CIDADE UNIVERSITÁRIA - CAMPINAS, SP - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
KRYPTUS	AHX4 NSF2 R1	NÃO	MÓDULO DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL I VERSÃO DE HARDWARE: 1.0.0 I VERSÃO DE SOFTWARE: 2.4 I VERSÃO DE FIRMWARE: 2.4 I NÍVEL DE SEGURANÇA DE CERTIFICAÇÃO (NSC): 3

Certificador: NCC Nº Certificado: NCC 19.05811 Tipo: Produto Emissão: 23/07/2019 Validade: 23/07/2025 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
01586633000196	GEMALTO DO BRASIL CARTOES E TERMINAIS LTDA.	GEMALTO DO BRASIL	AV. NOSSA SENHORA DA BOA ESPERANÇA, 367 - - CENTRO - PINHAIS, PR - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
GEMALTO	IDBRIDGE K50	NÃO	TOKEN CRIPTOGRÁFICO PARA USO NO ÂMBITO DA ICP-BRASIL I VERSÃO DE HARDWARE: SHELL TOKEN V3 I VERSÃO DE SOFTWARE: SAFESIGN IDENTITY CLIENT I VERSÃO DE FIRMWARE: IDCORE30 BUILD 1.17

Certificador: NCC Nº Certificado: NCC 19.05842 Tipo: Produto Emissão: 05/08/2019 Validade: 05/08/2025 Status do Certificado: Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
01586633000196	GEMALTO DO BRASIL CARTOES E TERMINAIS LTDA.	GEMALTO DO BRASIL	AV. NOSSA SENHORA DA BOA ESPERANÇA, 367 - - CENTRO - PINHAIS, PR - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
GEMALTO	GRK-13	NÃO	NOME COMERCIAL: LUNA SA6 I MÓDULO DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL I VERSÃO DE HARDWARE: 6 I VERSÃO DE SOFTWARE: 6.3 I VERSÃO DE FIRMWARE: 6.27.0

Certificador: NCC **Nº Certificado:** NCC 19.05850 **Tipo:** Produto **Emissão:** 12/08/2019 **Validade:** 12/08/2025 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
01586633000196	GEMALTO DO BRASIL CARTOES E TERMINAIS LTDA.	GEMALTO DO BRASIL	AV. NOSSA SENHORA DA BOA ESPERANÇA, 367 - - CENTRO - PINHAIS, PR - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
GEMALTO	GRK-16	NÃO	NOME COMERCIAL: LUNA SA7 I MÓDULO DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL I VERSÃO DE HARDWARE: 7 I VERSÃO DE SOFTWARE: 7.3 I VERSÃO DE FIRMWARE: 7.3.0

Certificador: NCC **Nº Certificado:** NCC 19.05920 **Tipo:** Produto **Emissão:** 24/09/2019 **Validade:** 24/09/2025 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
17423726000130	DINAMO NETWORKS - SERVIÇOS, DESENVOLVIMENTO E PARTICIPAÇÕES OU EMPRESAS LTDA.	DINAMO NETWORKS	ST SCN - QD 05 / BL. A (ED.EMPR.BRASÍLIA SHOPPING), 50 - SL.416 - ASA NORTE - BRASÍLIA, DF - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
DINAMO	DINAMO ST	NÃO	MÓDULO DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL | VERSÃO DE HARDWARE 6.04F | VERSÃO DE SOFTWARE 4.0.2 | VERSÃO DE FIRMWARE 4.0.2 | NSC3

Certificador: NCC **Nº Certificado:** NCC 19.05921 **Tipo:** Produto **Emissão:** 24/09/2019 **Validade:** 24/09/2025 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
17423726000130	DINAMO NETWORKS - SERVIÇOS, DESENVOLVIMENTO E PARTICIPAÇÕES OU EMPRESAS LTDA.	DINAMO NETWORKS	ST SCN - QD 05 / BL. A (ED.EMPR.BRASÍLIA SHOPPING), 50 - SL.416 - ASA NORTE - BRASÍLIA, DF - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
DINAMO	DINAMO XP	NÃO	MÓDULO DE SEGURANÇA CRIPTOGRÁFICA (MSC) NO ÂMBITO DA ICP-BRASIL VERSÃO HARDWARE 6.03A | VERSÃO SOFTWARE 4.0.2 | VERSÃO FIRMWARE 4.0.2 | NSC3

Certificador: NCC **Nº Certificado:** NCC 19.05960 **Tipo:** Produto **Emissão:** 02/10/2019 **Validade:** 02/10/2027 **Status do Certificado:** Ativo Doc.Normativo

CNPJ/CPF	Razão Social / Nome (PF)	Nome fantasia	Endereço	Status	Papel da empresa
07771064000135	DEXON TECNOLOGIAS DIGITAIS LTDA		AVENIDA UNISINOS, 950 - SALA 36 - CRISTO REI - SAO LEOPOLDO, RS - BRASIL	ATIVO	SOLICITANTE/FABRICANTE

Marca	Modelo	Importado	Descrição
DEXON	E-SMARTDX	NÃO	LEITORA DE CARTÕES INTELIGENTES PARA USO NO ÂMBITO DA ICP-BRASIL - VERSÃO DE HARDWARE: H004.PCB-C I VERSÃO DE SOFTWARE: H004.PCB-C I VERSÃO DE FIRMWARE: 1.0

eToken 5110

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy Level 3

Table of Contents

Table of Tables

Table of Figures

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment D, Sept 2009
[ISO 7816]	ISO/IEC 7816-1:2003 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2013 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[ISO 14443]	*Identification cards – Contactless integrated circuit cards – Proximity cards* ISO/IEC 14443-1:2008 Part 1*: Physical characteristics* ISO/IEC 14443-2:2010 Part 2: *Radio frequency power and signal interface* ISO/IEC 14443-3:2011 Part 3: *Initialization and anticollision* ISO/IEC 14443-4:2008 Part 4: *Transmission protocol*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* *Java Card 3.0.5 Application Programming Interface [only for ECDSA with SHA2, AES-CMAC]* Published by Sun Microsystems
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 1, November 2015
[SP 800-90A]	NIST Special Publication 800-90, *Recommendation for the Random Number Generation Using Deterministic Random Bit Generators,* - revision 1, June 2015.
[SP 800-108]	NIST Special Publication 800-108, *Recommendation for Recommendation for Key Derivation Using Pseudorandom Functions,* October 2009.
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (Triple-DES) Block Cipher*, - revision 1, January 2012.
[FIPS 113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS 197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[PKCS#1]	*PKCS #1 v2.2: RSA Cryptography Standard*, RSA Laboratories, October 27, 2012.
[FIPS 186-4]	NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013

Acronym	Full Specification Name
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, revision 2, May 2013.
[FIPS 180-3]	NIST, *Secure Hash Standard*, FIPS Publication 180-3, October 2008
[AESKeyWrap]	NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key Triple-DES in lieu of AES is described in [IG] D.2.
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 10 May 2016.
[USB 2.0]	USB.org, Universal Serial Bus Revision 2.0 specification

Table 1 – References

Acronyms and definitions

Acronym	Definition
GP	Global Platform
CVC	Card Verifiable Certificate
MMU	Memory Management Unit
OP	Open Platform
RMI	Remote Method Invocation
SC	Secure Controller

Table 2 – Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the Gemalto SafeNet eToken 5110 which comprises the 5110 USB MCU FW, the IDCore 30-revB platform and the eToken Applet 1.8 and herein denoted as Cryptographic Module. The Cryptographic Module or CM, validated to FIPS 140-2 overall Level 3, is a USB token that contains a secure controller (SC) module implementing the Global Platform operational environment, with Card Manager, the eToken Applet 1.8.

The CM is a limited operational environment under the FIPS 140-2 definitions. The CM SC includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation. The CM also includes the USB MCU FW firmware load service to support necessary updates of the USB controller FW.

The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 3 – Security Level of Security Requirements

The CM implementation is compliant with:

- [ISO 7816] Parts 1-4
- [JavaCard]
- [GlobalPlatform]
- [USB 2.0]

1.1 eToken Applet

eToken Applet (v1.8) is a Java applet that provides all the necessary functions to integrate a smart card in a public key infrastructure (PKI) system, suitable for identity and corporate security applications. It is also useful for storing information about the cardholder and any sensitive data. eToken Applet implements state–of–the–art security and conforms to the latest standards for smart cards and PKI applications. It is also fully compliant with digital signature law.

The eToken is designed for use on JavaCard 2.2.2 and Global Platform 2.1.1 compliant smart cards.

The main features of eToken Applet are as follows:

- Digital signatures—these are used to ensure the integrity and authenticity of a message. (RSA, ECDSA)
- Storage of sensitive data based on security attributes
- Secure messaging based on the Triple-DES 3 Keys algorithms.
- Public key cryptography, allowing for RSA keys and ECDSA keys
- Storage of digital certificates—these are issued by a trusted body known as a certification authority (CA) and are typically used in PKI authentication schemes.
- Decryption RSA , ECDH
- On board key generation (RSA, ECDSA)
- Support of integrity on data to be signed based on the Secure messaging protocol.

1.2 eTPnP applet is associated to eToken applet and offers:

- GUID tag reading, defined in Microsoft Mini Driver specification.

2 Hardware and Physical Cryptographic Boundary

eToken 5110 is a multiple-Chip standalone cryptographic module. Two (2) ICs are mounted on a PCB assembly with a connector and passive components, covered by epoxy on both sides, exposing only the LED and USB connector. The Module is intended to be covered within a plastic enclosure. Physical inspection inside the Module boundary is not practical, as the epoxy layer is opaque.

The Module meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations.

2.1 eToken 5110 Crypto Boundary

Figure 1 – eToken 5110 Crypto Boundary (Top and Bottom)

Figure 2 – Shows the Module with the outer enclosure, which is not within the cryptographic boundary

2.2 Ports and Interfaces

The Module functions as a slave device to process and respond to commands.

This module provides a contact interface that is fully compliant with USB 2.0.

Interface	Description
USBDM	USB D- differential data
USBDP	USB D+ differential data
V_{Bus}	Power supply input
GND	Ground (reference voltage)
LED	LED indicator

Table 4 – USB Physical Interfaces

The I/O ports of the platform provide the following logical interfaces:

Interface	USB
Data In	USBDM, USBDP
Data Out	USBDM, USBDP
Status Out	USBDM, USBDP, LED
Control In	USBDM, USBDP

Table 5 – USB Logical Interfaces

3 Cryptographic Module Specification

3.1 USB MCU Firmware and Logical Cryptographic Boundary

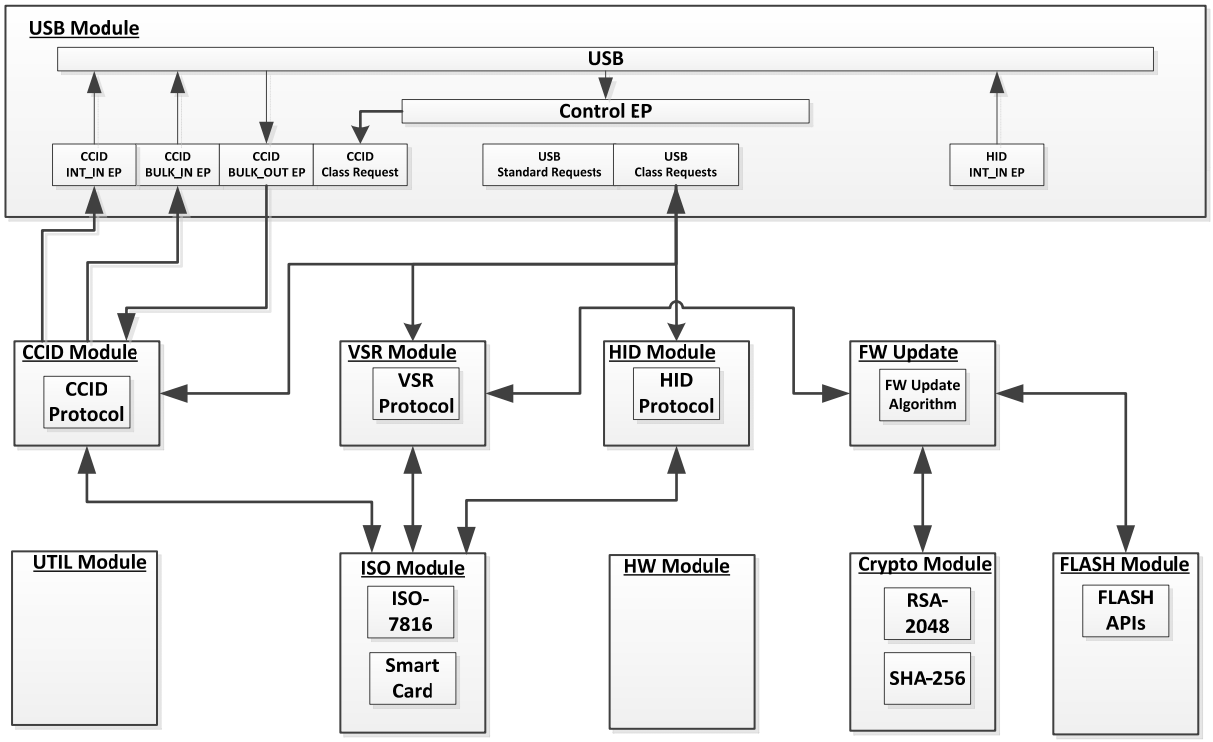

Figure 3 – USB MCU Block Diagram

The CM provides framework for the USB Standard and Class requests including the API dedicated to the CCID protocol, VSR propriety protocol, and the HID propriety protocol. The CM defines an interface for USB MCU firmware update service secured with RSA-2048 PKCS#1 RSASSA-PKCS1-v1_5 signature. The USB MCU FW communicates with the SC OS using ISO-7816 T1 protocol.

3.2 SC OS Firmware and Logical Cryptographic Boundary

Figure 4 below depicts the Module operational environment and applets.

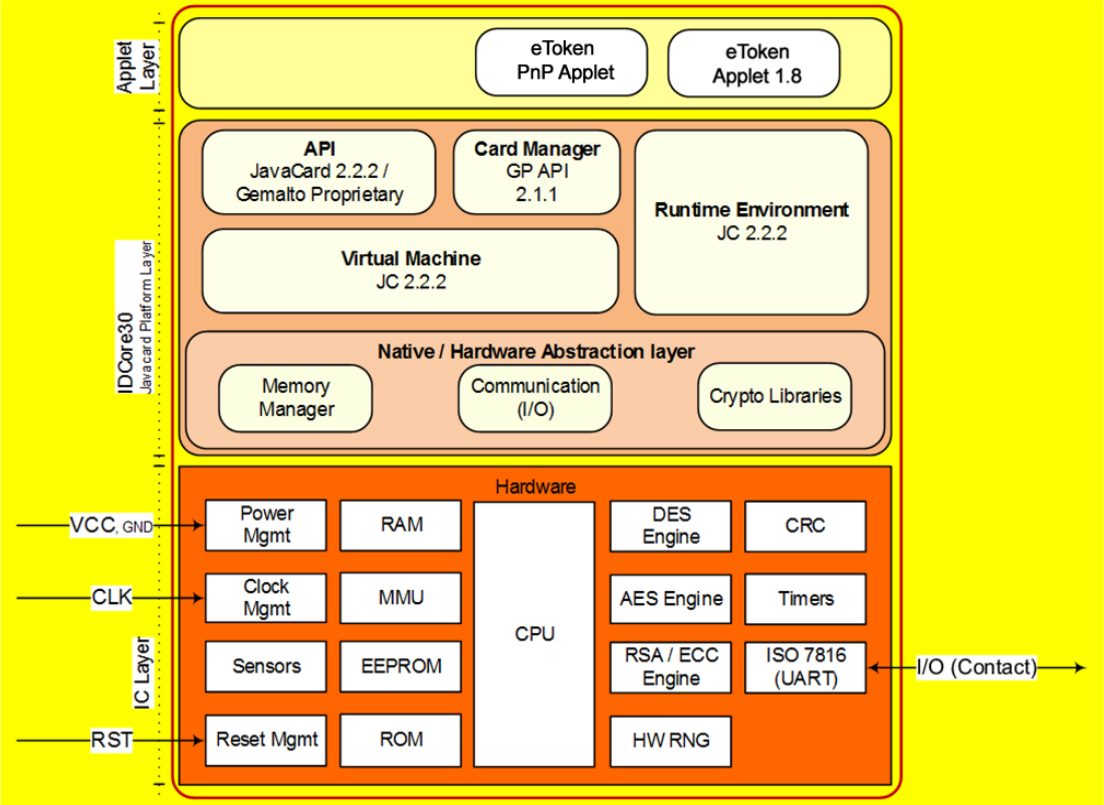

Figure 4 – SC Module Block Diagram

The CM supports [ISO7816] T=1 communication protocols.

The CM provides services to both external devices and internal applets as the eToken Applet 1.8.

Applets, as eToken Applet 1.8, access module functionalities via internal API entry points that are not exposed to external entities. External devices have access to CM services by sending APDU commands.

The CM provides an execution sandbox for the eToken Applet and performs the requested services according to its roles and services security policy.

The CM inhibits all data output via the data output interface while the module is in error state and during self-tests.

The *JavaCard API* is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

The *Javacard Runtime Environment* implements the dispatcher, registry, loader, logical channel and RMI functionalities.

The *Virtual Machine* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

The *Card Manager* is the card administration entity – allowing authorized users to manage the card content, keys, and life cycle states.

The *Memory Manager* implements services such as memory access, allocation, deletion, garbage collector.

The *Communication* handler deals with the implementation of ATR, PSS, and T=1 protocols.

The *Cryptography Libraries* implement the algorithms listed in Section 3.5.

3.3 USB MCU FW Versions and mode of operation

Hardware: STM32F042K6U6TR

Firmware: 5110 FIPS FW ver-15.0

The MCU FW version is retrieved via VSR 0xA0; The FW version is encoded in the

kernelVerMajor, **kernelVerMinor**, **kernelBuild** Fields.

3.3.1 Get Descriptors (VSR 0xA0) Device to Host

- This command is being implemented in the **KERNEL** for Kernel Info
- One Stage command – Only CTRL Read.
- Each Descriptor starts with a fixed Header, and might have a string descriptor.

Field	Offset	Length	Value	Description
Request type	0	1	0xC0	Device to Host VSR
Request	1	1	0xA0	Get Descriptor
Value	2	2		0x0 – For Kernel Info 0x6 – For String descriptor (not implemented)
Index	4	2	Index	If wValue == 6 then it's the Index of requested string descriptor: • VENDOR 0x01 • PRODUCT 0x02
Data Length	6	2	According to the descriptor	

Table 6 - Get Descriptors (VSR 0xA0) Device to Host

3.3.1.1 Get Descriptors - Header

Get Descriptors Header has a fixed structure with fixed size common to all Descriptors.

Offset	Length	Value	Field Name	Description
0	2	N	size	Descriptor size including the header
2	1	1	version	Descriptor Version set to 1
3	1	0	stringIndex	Index of string descriptor, 0 value means that there is no string descriptor

Table 7 - Get Descriptors – Header

3.3.1.2 Kernel Info (Index 0)

Offset	Length	Value	Field Name	Description
0	4		descriptorHeader	Descriptor Header
4	1		kernelLocation	0x0 - Low, 0x1 - High
5	2	2	kernelType	0x0 – NG PRO T1 CARDOS 0x1 - PRO T0 JAVA 0x2 - NG PRO T1 JAVA
7	2	15	kernelVerMajor	Kernel Version – firmware major version, changing the protocol will affect the FW major version.
9	2	0	kernelVerMinor	Kernel Version – Firmware minor version
11	4	X	kernelBuild	Firmware build
15	2	1	microController	Micro Controller type: 0 - Micro Controller C8051F320/1 with 16K EE 1 - Micro Controller C8051F387 2 - Microcontrollers ST STM32F042
17	4		tokenId	Token Id
21	2		tokenIdEx	Token Id Extender
23	1	0	status	status

Table 8 – Kernel Info (Index 0)

3.4 SC Versions and mode of operation

Hardware: SLE78CFX3000PH
Firmware: IDCore30-revB - Build 06, eToken Applet version 1.8 and eTPnP Applet V1.0

The CM is always in the approved mode of operation. To verify that a CM is in the approved mode of operation, select the Card Manager and send the GET DATA commands shown below:

Field	CLA	INS	P1-P2 (Tag)	Le (Expected response length)	Purpose
Value	00	CA	9F-7F	2A	Get CPLC data
			01-03	1D	Identification information (proprietary tag)

Table 9 - GET DATA Command

The CM responds with the following information:

IDC30-revB - CPLC data (tag 9F7F)			
Byte	**Description**	**Value**	**Value meaning**
1-2	IC fabricator	**4090h**	Infineon
3-4	IC type	**7901**	SLE78CFX3000PH
5-6	Operating system identifier	**1291**	Gemalto
7-8	Operating system release date (YDDD) – Y=Year, DDD=Day in the year	**5356**	Operating System release Date
9-10	Operating system release level	**0200h**	V2.0
11-12	IC fabrication date	xxxxh	Filled in during IC manufacturing
13-16	IC serial number	xxxxxxxxh	Filled in during IC manufacturing
17-18	IC batch identifier	xxxxh	Filled in during IC manufacturing
19-20	IC module fabricator	xxxxh	Filled in during module manufacturing
21-22	IC module packaging date	xxxxh	Filled in during module manufacturing
23-24	ICC manufacturer	xxxxh	Filled in during module embedding
25-26	IC embedding date	xxxxh	Filled in during module embedding
27-28	IC pre-personalizer	xxxxh	Filled in during smartcard preperso

29-30	IC pre-personalization date	xxxxh	Filled in during smartcard preperso
31-34	IC pre-personalization equipment identifier	xxxxxxxxh	Filled in during smartcard preperso
35-36	IC personalizer	xxxxh	Filled in during smartcard personalization
37-38	IC personalization date	xxxxh	Filled in during smartcard personalization
39-42	IC personalization equipment identifier	xxxxxxxxh	Filled in during smartcard personalization

Table 10 - Versions and Mode of Operations Indicators (tag 9F7F)

IDC30-revB - Identification data (tag 0103)			
Byte	**Description**	**Value**	**Value meaning**
1	Gemalto Family Name	**B0**	Javacard
2	Gemalto OS Name	**84**	IDCore family (OA)
3	Gemalto Mask Number	**56**	G286
4	Gemalto Product Name	**51**	IDCore30-revB
5	Gemalto Flow Version	**XY**	**X** is the type of SCP: ▪ 2xh for SCP0300 flows ▪ 3xh for SCP0310 flows **Y**: is the version of the flow (x=1 for version 01). For instance: ▪ **21h** = SCP0300 - flow 01 (version 01) ▪ **31h** = SCP0310 - flow 01 (version 01)
6	Gemalto Filter Set	**00**	▪ Major nibble: filter family = 00h ▪ Lower nibble: version of the filter = 00h
7-8	Chip Manufacturer	**4090**	Infineon
9-10	Chip Version	**7901**	SLE78CFX3000PH
11-12	FIPS configuration	**8D00**	MSByte: b8 : 1 = **conformity to FIPS certificate** b7 : 0 = not applicable b6 : 0 = not applicable b5 : 0 = not applicable

			b4 : 1 = ECC supported b3 : 1 = RSA CRT supported b2 : 1 = RSA STD supported b1 : 1 = AES supported LSByte: b8 .. b5 : 0 = not applicable b4 : 0 = not applicable (ECC in contactless) b3 : 0 = not applicable (RSA CRT in contactless) b2 : 0 = not applicable (RSA STD in contactless) b1 : 0 = not applicable (AES in contactless) For instance: **8F 00** = FIPS enable (CT only)–AES-RSA CRT/STD-ECC **(Full FIPS)** **8D 00** = FIPS enable (CT only)–AES-RSA CRT-ECC **(FIPS PK CRT) *** **85 00** = FIPS enable (CT only)–AES-RSA CRT **(FIPS RSA CRT)** **00 00** = FIPS disable (CT only)–No FIPS mode **(No FIPS)** **(* default configuration)**
13	FIPS Level for IDPrime MD product	**00**	03 = FIPS Level 3
14-29	RFU	**xx..xxh**	-

Table 11 – Versions and Mode of Operations Indicators (tag 0103)

The **eToken Applet 1.8** is identified with an applet version

Field	CLA	INS	P1-P2 (Tag)	Le (Expected response length)	Purpose
Value	**00**	**CA**	**01-11**	**06**	Get Data Applet Version

Table 12 – Get Data Applet Version

The **eToken Applet 1.8** Version is returned in TLV format as follows:

Tag	Length	Value	Value meaning
11	04	1.8.XX	VerMajor (one byte), VerMinor (one byte), Build (two bytes);

Table 13 – eToken Version Returned Values

3.5 Cryptographic Functionality

The Module operating system implements the FIPS Approved and Non-FIPS Approved cryptographic function listed in Tables below.

Algorithm	Description	Cert #
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128, 192, and 256-bit key lengths with ECB and CBC modes.	3779
AES CMAC	AES CMAC The Module supports 128-, 192- and 256-bit key lengths.	3779
CVL (ECC-CDH)	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive. The Module is CAVP validated for the NIST defined P-224, P-256, P-384 and P-521 curves.	719
CVL (RSASP1)	[FIPS 186-4] RSA PKCS1-v1.5 signature generation primitive	803
CVL (RSADP)	[SP 800-56B] RSA PKCS#1 v2.1 decryption operation primitive component as specified in Section 7.1.2.Section 5.1.2 decryption primitive	804
DRBG	[SP 800-90] Deterministic Random Number Generators [CTR_DRBG mode based on AES]	1045
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm: signature generation, verification and key pair generation. The Module is CAVP validated for the NIST defined P-224, P-256, P-384 and P-521 curves. (Note: Sig Ver P-192 is not used by the module.)	814
KBKDF	[SP 800-108] KDF for AES CMAC. The Module supports 128-, 192- and 256-bit key lengths.	81
KTS	[SP800-38F] Symmetric Key wrapping using 128, 192, or 256 bit keys (based on AES and AES CMAC Cert. #3779), meets the SP800-38F §3.1 ¶3. Key establishment methodology provides 128, 192, or 256 bits of strength.	3779
KTS	[SP800-38F] Symmetric Key wrapping using 3-key Triple-DES Cert. #2100 and Triple-DES MAC Vendor Affirmed), meets the SP800-38F §3.1 ¶3. Key establishment methodology provides 112 bits of strength.	2100
RSA	[FIPS 186-4] RSA signature generation, verification, and key pair generation. The Module follows PKCS#1 and is CAVP validated for 2048 bit key length. (Note: Sig Ver 1024 is not used by the module.)	1946
RSA CRT	[FIPS 186-4] RSA signature generation, verification, CRT key pair generation. The Module follows PKCS#1 and is CAVP validated for 2048 bit key length.	1947
RSA Signature Verification	[FIPS 186-4] USB FW implementations of RSA Signature Verification	2037
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms.	3146
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The Module supports the 3-Key options; CBC and ECB modes. Note that the Module does not support a mechanism that would allow collection of plaintext / ciphertext pairs aside from authentication, limited in use by a counter.	2100

Triple -DES MAC	[FIPS 113] Triple-DES Message Authentication Code. Vendor affirmed, based on validated Triple-DES.	Vendor Affirmed
SHA 256	[FIPS 180-4] USB FW implementations of Secure Hash Standard compliant one-way (hash) algorithms	3276

Table 14 – FIPS Approved Cryptographic Functions

Algorithm	Description
EC Diffie-Hellman key agreement	SP 800-56A; non-compliant - key agreement using NIST defined, P-224, P-256, P-384 and P-521 curves. Key establishment methodology provides 112, 128, or 192 bits of strength.
NDRNG	Used to initialize the CTR DRBG. Provides more than 112 bits of entropy.

Table 15 – Non-FIPS Approved But Allowed Cryptographic Functions

The CM includes an uncallable DES implementation. This algorithm is not used and no security claims are made for its presence in the Module.

FIPS approved security functions used specifically by the **eToken Applet** are:

- **DRBG**
- **AES**
- **RSA**
- **ECDSA**
- **SHA-256,**
- **ECDH**
- **Triple-DES 3 Key**

(Note: no security function is used in **eTPnP applet**)

4 Platform Critical Security Parameters

All CSPs used by the CM are described in this section. All usages of these CSPs by the CM are described in the services detailed in Section 5.

Key	Description / Usage
OS-RNG-SEED-KEY	256-bit random drawn by the NDRNG HW chip (AIS-31PTG.2), used as a seed key for the [SP 800-90A] DRBG implementation.
OS-RNG-STATE	16-byte random value and 16-byte counter value used in the [SP 800-90] DRBG implementation. 16-byte AES state V and 16-byte AES key used in the [SP800-90A] CTR DRBG implementation.
OS-GLOBALPIN	6 to 16 bytes Global PIN value managed by the ISD. Character space is not restricted by the module.

OS-MKDK	AES-128/192/256 (SCP03) key used to encrypt OS-GLOBALPIN value
SD-KENC	AES-128/192/256 (SCP03) Master key used by the CO role to generate SD-SENC
SD-KMAC	AES-128/192/256 CMAC (SCP03) Master key used by the CO role operator to generate SD-SMAC
SD-KDEK	AES-128/192/256 (SCP03) Sensitive data decryption key used by the CH role to decrypt CSPs for SCP03.
SD-SENC	AES-128/192/256 (SCP03) Session encryption key used by the CO role to encrypt / decrypt secure channel data.
SD-SMAC	AES-128/192/256 CMAC (SCP03) Session MAC key used by the CO role to verify inbound secure channel data integrity.
SD-SDEK	AES-128/192/256 (SCP03) Session DEK key used by the CO role to decrypt CSPs.
DAP-SYM	AES-128/192/256 (SCP03) key optionally loaded in the field and used to verify the signature of packages loaded into the Module.

Table 16 - Platform Critical Security Parameters

Keys with the "SD-" prefix pertain to a Global Platform Security Domain key set. The module supports the Issuer Security Domain at minimum, and can be configured to support Supplemental Security Domains.

4.1 eToken Applet Critical Security Parameters

Key	Description / Usage
ID_AUTH_OP	Triple-DES 3 Key MAC key used to authenticate the ESO or CH role using a challenge-response protocol.
ID_SM_ENC_IN_OP	Triple-DES 3 SM Decryption key used to decrypt data sent by the host application as a part of the operator operations.
ID_SM_MAC_IN_OP	Triple-DES 3 SM MAC key used to guarantee integrity on any data sent by the host application as a part of the operator operations. This also prevents replay attack as each MAC calculation uses an incrementing counter.
ID_SM_ENC_OUT_OP	Triple-DES 3 SM Encryption key used to encrypt data sent by the Module as a part of the operator operations.
ID_SM_MAC_OUT_OP	Triple-DES 3 SM MAC key used to guarantee integrity on any data sent by the Module as a part of the operator operations. This also prevents replay attack as each MAC calculation uses the host challenge.
ASK_MAC / ASK_ENC	The Applet Start key (ASK) comprises two 3-key Triple-DES keys – ASK_MAC key and ASK_ENC encryption Key. The ASK_MAC Key is used to protect the integrity and authenticate the File System Re-initialization and Change Applet Key services. The ASK_ENC key encrypts the new Key Applet Start Key Set during the Change Applet Key service. It is possible to perform File System Re-Initialization using the Applet Start Key Set.
SEC_AUTH	This CSP is a 3-key Triple-DES MAC key for use in a challenge response protocol. The Secondary Authentication Secret is used as the second level of authentication for cryptographic operations with AES and Triple-DES keys and RSA key pairs.
CH_RSA_KEY_PRIVATE / CH_RSA_KEY_PUBLIC	The eToken Applet Suite implements 0 to n (limited only by available memory) RSA-2048 key pairs used by the CH role in the *Perform Security Operation* service. RSA keys may be used for digital signatures as well as for key decapsulation. However, the key decryption mechanism is not used to establish keys into the module, only to provide key decryption as a service to the caller.
CH_ECDSA_KEY_PRIVATE / CH_ECDSA_KEY_PUBLIC	The eToken Applet Suite implements 0 to n (limited only by available memory) ECDSA key pairs (P-256, P-384 curves) used by the CH role in the *Perform Security Operation* service. ECDSA is used for signature generation.
CH_ECDH_KEY_PRIVATE / CH_ECDH_KEY_PUBLIC	The eToken Applet Suite implements 0 to n (limited only by available memory) ECDH key pairs (P-256, P-384 curves) used by the CH role in the *Perform Security Operation* service. ECDH is used for shared key mechanism
CH_SYMMETRIC	The eToken Applet Suite implements 0 to n (limited only by available memory) AES-128, AES-192, AES-256 or 3-key Triple-DES keys for use by CH role in the *Perform Security Operation* service.

Table 17 – eToken Applet Critical Security Parameters

4.2 USB MCU FW Critical Security Parameters

Key	Description / Usage
ID_FW_DOWNLOAD_RSA_KEY_PUBLIC	2048 bit RSA Public key embedded in the USB MCU FW – used by the FW to validate the new FW signature during FW Download.

Table 18 – USB MCU FW Critical Security Parameters

5 Roles, Authentication and Services

Table 15 lists all operator roles supported by the Module. This Module does not support a maintenance role. The Module clears previous authentications on power cycle. The Module supports GP logical channels, allowing multiple concurrent operators. Authentication of each operator and their access to roles and services is as described in this section, independent of logical channel usage. Only one operator at a time is permitted on a channel. Applet de-selection (including Card Manager), card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services. Authentication data is encrypted during entry (by SD-SDEK), is stored encrypted (by OS-MKDK) and is only accessible by authenticated services.

Role ID	Role Description
CO	(Cryptographic Officer) This role is responsible for card issuance and management of card data via the Card Manager applet. Authenticated using the SCP authentication method with SD-SENC.
CH	Card Holder (User role for FIPS 140-2 validation purposes). The Card Holder role is defined in the context of the eToken Applet Suite and is used to protect keys and data owned by the Card Holder.
ESO	eToken Security Officer This role is responsible for managing the life cycle of the Card Holder (CH).
FSI	File System Initializer This role is responsible for the eToken Applet Suite File System Re-initialization. In additional to the File System initialization, this role is capable of changing the Applet Start Key Set values.
FWU	USB MCU FW Updater; This role is responsible to sign the New FW package with a dedicated RSA 2048 private key to allow updating the 5110 USB MCU FW.
UA	Unauthenticated role

Table 19 - Role Description

5.1 Secure Channel Protocol (SCP) Authentication

The Open Platform Secure Channel Protocol authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command. These two commands operate as described next.

The SD-KENC and SD-KMAC keys are used along with other information to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the CO role).

For SCP03, AES-128, AES-192 or AES-256 keys are used for Global Platform secure channel operations, in which the Module derives session keys from the master keys and a handshake process, performs mutual authentication, and decrypts data for internal use only. The Module encrypts a total of one block (the mutual authentication cryptogram) over the life of the session encryption key; no decrypted data is output by the Module. AES key establishment provides a minimum of 128 bits of security strength. The Module uses the SD-KDEK key to decrypt critical security parameters, and does not perform encryption with this key or output data decrypted with this key.

The strength of GP mutual authentication relies on AES key length, and the probability that a random attempt at authentication will succeed is:

- $\left(\frac{1}{2^{128}}\right)$ for AES 16-byte-long keys;
- $\left(\frac{1}{2^{192}}\right)$ for AES 24-byte-long keys;
- $\left(\frac{1}{2^{256}}\right)$ for AES 32-byte-long keys;

Based on the maximum count value of the failed authentication blocking mechanism, the minimum probability that a random attempt will succeed over a one minute period is 255/2^128.

5.2 eToken Applet Authentication

The ESO or CH authenticates by opening a SM session with the eToken Applet using a challenge response mechanism with the ID_AUTH_OP key, which has an associated error counter in the range one to 15 with default value 15.

The FSI role is authenticated using the ASK_MAC key and utilizing a challenge response mechanism. In all cases, the minimum challenge size is a single 64-bit block, therefore the probability of false authentication is 1/2^64 or approximately 5.4E-20.

For ESO or CH authentication, the error counter limits the probability of false authentication in a one minute period to 15/2^64 or approximately 8.1E-19.

For FSI authentication, the serial communications rate limits the maximum rate of authentication attempts in a one minute period to 1000 attempts, therefore the probability of false authentication is 1000/2^64 or approximately 5.4E-17.

5.3 FW Updater Authentication

The FW updater utilizes RSA 2048-bit signature verification to authenticate new signed firmware to be loaded. According to NIST SP 800-57 and NIST SP 800-131A Rev 1, the RSA 2048-bit signature verification method provides an estimated security strength of 112-bits.

5.4 Platform Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. The *Card Reset* service will invoke the power on self-tests described in Section §10-Self-test. Moreover, on any card reset, the Module overwrites with zeros the RAM copy of, OS-RNG-STATE, SD-SENC, SD-SMAC and SD-SDEK. The Module can also write the values of all CSPs stored in EEPROM as a consequence of restoring values in the event of card tearing or a similar event. During the self-tests, the module generates the RAM copy of OS-RNG-STATE and updates the EEPROM copy of OS-RNG-STATE.
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. Uses SD-SENC and SD-SMAC.
INITIALIZE UPDATE	Initializes the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. Uses the SD-KENC, SD-KMAC and SD-KDEK master keys to generate the SD-SENC, SD-SMAC and SD-SDEK session keys, respectively.
GET DATA	Retrieve a single data object. Optionally uses SD-SENC, SD-SMAC (SCP).
MANAGE CHANNEL	Open and close supplementary logical channels. Optionally uses SD-SENC, SD-SMAC (SCP).
SELECT	Select an applet. Does not use CSPs.

Table 20 - Unauthenticated Services and CSP Usage

Service	Description	CO
DELETE	Delete an applet from EEPROM. This service is provided for the situation where an applet exists on the card, and does not impact platform CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET STATUS	Retrieve information about the card. Does not use CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
INSTALL	Perform Card Content management. Optionally uses SD-SENC, SD-SMAC (SCP). Optionally, the Module uses the DAP-SYM key to verify the package signature.	X
LOAD	Load a load file (e.g., an applet). Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT DATA	Transfer data to an application during command processing. Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT KEY	Load Card Manager keys The Module uses the SD-KDEK key to decrypt the keys to be loaded. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET STATUS	Modify the card or applet life cycle status. Optionally uses SD-SENC, SD-SMAC (SCP).	X
STORE DATA	Transfer data to an application or the security domain (ISD) processing the command. Optionally, updates OS-GLOBALPIN. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET MEMORY SPACE	Monitor the memory space available on the card. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET ATR	Change the card ATR. Optionally uses SD-SENC, SD-SMAC (SCP).	X

Table 21 – Authenticated Card Manager Services and CSP Usage

All of the above commands use the SD-SENC and SD-SMAC keys for secure channel communications, and SD-SMAC for firmware load integrity.

The card life cycle state determines which modes are available for the secure channel. In the SECURED card life cycle state, all command data must be secured by at least a MAC. As specified in the GP specification, there exist earlier states (before card issuance) in which a MAC might not be necessary to send Issuer Security Domain commands. Note that the LOAD service enforces MAC usage.

5.5 eToken Applet Services

All services implemented by the eToken Applet 1.8 applet are listed in the table below.

All services that are related to Key import/gen or Key Crypto Operations are Secure Messaging Protected.

Service	Description	ESO	CH	FSI	UA
Operator Logon	Authenticate the CH or ESO role. Uses ID_AUTH_OP key from Secure Messaging Key Set to authenticate operator.	X	X		
Credential Change	Change the current Secure Messaging Key Set. Uses ID_SM_ENC_IN_OP and ID_SM_MAC_IN_OP from Secure Messaging Key Set to decrypt and verify MAC value on new credentials.	X	X		
CH Unlocking	Unlock the CH Key Set. The ESO provides the new CH key set. All CH data and other keys remain untouched. Uses ID_SM_ENC_IN_OP and ID_SM_MAC_IN_OP from Secure Messaging Key Set to decrypt and verify MAC value on new CH key set.	X			
File System Re-initialization	The data in the SafeNet eToken Applet are cleared and the eToken file system is re-initialized. Deleting all keys stored in the eToken file system. This service executed from the FSI role. ASK_ENC key from Applet Start Key set is used to authenticate FSI role.			X	
Generate CH RSA Key Pair	Generate a CH RSA Key Pair. Generates RSA Key Pair, including CH_RSA_KEY_PRIVATE and CH_RSA_KEY_PUBLIC keys.		X		
Generate CH ECDSA Key Pair	Generate a CH ECDSA Key Pair, including CH_ECDSA_KEY_PRIVATE and CH_ECDSA_KEY_PUBLIC keys.		X		
Generate CH ECDH Key Pair	Generate a CH ECDH Key Pair, including CH_ECDSA_KEY_PRIVATE and CH_ECDSA_KEY_PUBLIC keys.		X		

Create Secondary Authentication Secret	Import Secondary Authentication Secret SEC_AUTH. Updates SEC_AUTH. Uses ID_SM_ENC_IN_OP and ID_SM_MAC_IN_OP from Secure Messaging Key Set to decrypt and authenticate the new value.		X		
Perform Security Operation	Use a CH RSA Key Pair to generate/verify signatures or decryption of symmetric keys. Use a CH ECDSA Key Pair to generate, compute/verify signatures or compute a shared secret. Use a CH ECDH Key pair for shared key mechanism. Use AES and Triple-DES keys for encryption/decryption. Key decryption does not establish a CSP into the Module. Uses CH_RSA_KEY_PRIVATE, CH_RSA_KEY_PUBLIC, CH_ECDSA_KEY_PRIVATE, CH_ECDSH_KEY_PRIVATE, CH_ECDSA_KEY_PUBLIC, CH_ECDH_KEY_PUBLIC or CH_SYMMETRIC keys, depending on operation type.		X		
Store and read data	Store and read data objects. Uses the Secure Messaging key set to encrypt/decrypt and authenticate data on input/output.		X		
Import RSA\ECC key pair and import TDEA \AES symmetric keys	Import RSA\ECC key pair. Writes CH_RSA_PRIVATE_KEY, CH_RSA_PUBLIC_KEY or CH_ECDSA_PRIVATE_KEY, CH_ECDSA_PUBLIC_KEY or CH_ECDH_PRIVATE_KEY, CH_ECDH_PUBLIC_KEY or CH_SYMMETRIC Uses the Secure Messaging key set to encrypt/decrypt and authenticate keys on input/output.		X		
Manage file system	Create files, delete files, admin files, list directories, resize filesystem, wipe filesystem. Uses the Secure Messaging key set to encrypt/decrypt and authenticate commands on input/output.	X	X		
Manage objects	Admin object, get object info, list objects. Uses the Secure Messaging key set to encrypt/decrypt and authenticate commands on input/output.	X	X		

Export public key	Export public key. The service does not utilize any CSPs.				X
Set/read volatile data	Set or read application-specific volatile data for the applet.				X

Table 22 – eToken Applet Services and CSP Usage

5.6 USB MCU FW Services

All services implemented by the USB MCU FW are listed in the table below.

Service	Description	UA	FWU
USB	This module provides framework for the USB Standard and Class requests, such as VSR, CCID protocols, to allow either ISO7816 communication with the SC or Commands which are directed to the FW such as FW Update, FW get Info, etc.	X	
FW Update	This module defines an interface for firmware update process; FW is protected by an RSA 2048 signature. The signature verification is for the purposes of authenticating the USB FW download.		X
Crypto Module	This module includes the API dedicated to using SHA-256 and RSA-2048 verify (RSA PKCS#1-v1_5 format).	X	

Table 23 – USB MCU FW applet Services

5.7 eTPnP Applet Services

In addition to the authenticated services, the module provides the Minidriver Information Service when the Minidriver eTPnP Applet is selected. This service is available without authentication. It provides non-security relevant information used by the host operating system to recognize the module.

The Minidriver Information Service does not utilize any CSPs.

Service	Description	UA
GET DATA	Retrieves the following information: • GUID	X

Table 24 – eTPnP applet Services

6 Finite State Model

The CM is designed using a finite state machine model that explicitly specifies every operational and error state.

The CM includes Power on/off states, Cryptographic Officer states, User services states, applet loading states, Key/PIN loading states, Self-test states, Error states, and the GP life cycle states.

An additional document (Finite State Machine document) identifies and describes all the states of the module including all corresponding state transitions.

7 Physical Security Policy

eToken 5110 is a multiple-chip standalone cryptographic module. Two (2) ICs are mounted on a PCB assembly with a connector and passive components, covered by epoxy on both sides, exposing only the LED and USB connector. The Module is intended to be covered within a plastic enclosure. Physical inspection inside the Module boundary is not practical, as the epoxy layer is opaque.

8 Operational Environment

This section does not apply to CM. No code modifying the behavior of the CM operating system can be added after its manufacturing process.

Only authorized applets can be loaded at post-issuance under control of the Cryptographic Officer. Their execution is controlled by the CM operating system following its security policy rules.

9 Electromagnetic Interference and Compatibility (EMI/EMC)

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

10 Self-test

10.1 Power-on Self-test

Each time the CM is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-on self–tests are available on demand by power cycling the CM.

On power-on or reset, the CM performs the self-tests described in table below. All KATs must be completed successfully prior to any other use of cryptography by the CM. If one of the KATs fails, the CM enters the Card Is Mute error state.

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in Flash memory (for OS and Applets).
DRBG	Performs DRBG SP 800-90 Section 11.3 instantiate and generate health test KAT with fixed inputs (no derivation function and no reseeding supported)
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
AES	Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC.
KBKDF AES-CMAC	Performs a KDF AES-CMAC KAT using an AES 128 key and 32-byte derivation data. The KAT computes session keys and verifies the result. Note that KDF KAT is identical to an AES-CMAC KAT; the only difference is the size of input data.
RSA	Performs separate RSA PKCS#1 signature and verification KATs using an RSA 2048 bit key, and a RSA PKCS#1 signature KAT using the RSA CRT implementation with a 2048 bit key.
ECC CDH	Performs an ECC CDH KAT using an ECC P-224 key.(same crypto engine than for ECDSA KAT)
SHA-1	Performs a SHA-1 KAT.
SHA-256	Performs a SHA-256 KAT.
SHA-512	Performs a SHA-512 KAT.
USB MCU FW Integrity	32 bit CRC performed over all FW executable code, located in MCU Flash memory. 32 bit CRC performed over FW configuration block, located in MCU Flash memory.
USB MCU FW RSA Signature Verification	Perform RSA 2048 PKCS#1 v1.5 Sig Verification KAT.
USB MCU FW SHA-256	Performs a SHA-256 KAT.

Table 25 – Power-On Self-Test

10.2 Conditional Self-tests

On every call to the [SP 800-90] DRBG, the CM performs the FIPS 140-2 Continuous RNG test to assure that the output is different than the previous value.

When any asymmetric key pair is generated (for RSA or ECC keys) the CM performs a pair-wise consistency test.

When new firmware is loaded into the CM using the LOAD command, the CM verifies the integrity and authenticity of the new firmware (applet) using the SD-SMAC key for MAC process.

USB MCU FW design includes a firmware load service to support necessary updates. Updatable MCU FW code is signed by RSA-2048 SHA-256 private key to avoid non-authorized FW update.

When new MCU FW is loaded into the USB MCU, the MCU FW verifies the integrity and authenticity of the new firmware using the RSA Signature verify method.

The RSA-2048 Modulus and Public Exponent data are hardcoded in firmware code. Firmware does not provide interface to change or read this key.

11 Design Assurance

The CM meets the Level 3 Design Assurance section requirements.

11.1 Configuration Management

An additional document (Configuration Management Plan document) defines the methods, mechanisms and tools that allow to identify and place under control all the data and information concerning the specification, design, implementation, generation, test and validation of the card software throughout the development and validation cycle.

11.2 Delivery and Operation

Some additional documents ('Delivery and Operation', 'Reference Manual', 'Card Initialization Specification' documents) define and describe the steps necessary to deliver and operate the CM securely.

11.3 Guidance Documents

The Guidance document provided with CM is intended to be the 'Reference Manual'. This document includes guidance for secure operation of the CM by its users as defined in the section: Roles, Authentication and Services.

11.4 Language Level

The CM operational environment is implemented using a high level language. A limited number of software modules have been written in assembler to optimize speed or size.

The eToken Applet is a Java applet designed for the Java Card environment.

12 Mitigation of Other Attacks Policy

The Module implements defenses against:

- Fault attacks
- Side channel analysis (Timing Analysis, SPA/DPA, Simple/Differential Electromagnetic Analysis)
- Probing attacks
- Card tearing

13 Security Rules and Guidance

The Module implementation also enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The Module does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
- In accordance to NIST guidance, operators are responsible for ensuring that a single Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit data blocks.

END OF DOCUMENT

SECRETARIA DE ORÇAMENTO, FINANÇAS E CONTABILIDADE

EXTRATO DE NOTA DE EMPENHO

Notas de Empenho Ordinário. TRE-PE n.º 2021NE285 e 2021NE286, emitidas em 26/04/2021. SEI nº 0013728-89.2020.6.17.8000. CONTRATADA: MACHADO ARMARINHOS LTDA - EPP. Valor: R$ 4.170,00 e 335,50. OBJETO: Aquisição de Material de Copa e Cozinha e Material de Limpeza e Produtos de Higienização. FUNDAMENTO LEGAL: ARP nº 15/2020, vinculada ao Pregão Eletrônico nº 01/2020 deste TRE-PE. PTRES: 167661. Elemento de despesa: 3390.30.21 e 3390.30.22, respectivamente.

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

SECRETARIA DE ADMINISTRAÇÃO, ORÇAMENTO E FINANÇAS
COORDENADORIA DE MATERIAL E PATRIMÔNIO

EXTRATO DE PREÇOS REGISTRADOS

Procedimento Licitatório nº 07/2021- Pregão Eletrônico - Sistema de Registro de Preços (SEI nº 0018160-27.2020.6.18.8000
Ata nº 02/2021: CONTRATADA: AR RP CERTIFICAÇÃO DIGITAL EIRELI (CNPJ: 21.308.480/0001-22). ITEM 1 - CERT-JUS INSTITUCIONAL A3 - 3 ANOS. Quantidade: 70 unidades, valor unitário: R$ 23,27 (vinte e três reais e vinte e sete centavos); ITEM 2 - VISITA TECNICA LOCAL. Quantidade: 5 unidades, valor unitário: R$ 51,00 (cinquenta e um reais); ITEM 3 - TOKEN (SAFENET). Quantidade: 70 unidades, valor unitário: R$ 36,00 (trinta e seis reais);

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL

DIRETORIA-GERAL

AVISO DE PREÇOS REGISTRADOS

O Tribunal Regional Eleitoral do Rio Grande do Sul, com fundamento no Decreto n. 7.892/2013, torna público os preços registrados para eventual aquisição de publicações nacionais, empresa, item, descrição resumida, quantidade estimada e percentual de desconto abaixo mencionados, obtidos como resultado do Pregão n. 02/2021, com vigência de 12 meses, a contar da data desta publicação: MD Distribuidora de Livros Ltda, item 1, publicações nacionais, 250 títulos, 36,02%.

JOSEMAR DOS SANTOS RIESGO
Diretor-Geral

TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA

DIRETORIA-GERAL
SECRETARIA DE ADMINISTRAÇÃO, ORÇAMENTO, FINANÇAS E CONTABILIDADE
COORDENADORIA DE MATERIAL DE PATRIMÔNIO
SEÇÃO DE LICITAÇÕES E COMPRAS

AVISO DE LICITAÇÃO FRACASSADA
PREGÃO Nº 6/2021

Na fase de julgamento, a única proposta foi recusada e o item foi cancelado. Certame fracassado.

ANDERCLEDSON REIS
Pregoeiro

(SIDEC - 29/04/2021) 070024-00001-2021NE000001

AVISO DE LICITAÇÃO
CONVITE Nº 1/2021 - UASG 70024

Nº Processo: 0003199-70.2020. Objeto: Contratação de empresa especializada de engenharia para EXECUÇÃO DE OBRA DE ESCORAMENTO REFORÇO ESTRUTURAL de Pilares do Edifício Sede do Tribunal Regional Eleitoral do Estado de Rondônia - TRE-RO, localizado no município de Porto Velho-RO, nos termos e condições estabelecidos no instrumento convocatório e seus anexos integrantes.. Total de Itens Licitados: 1. Edital: 30/04/2021 das 08h00 às 17h59. Endereço: Av Presidente Dutra, 1889, Baixa União, - Porto Velho/RO ou https://www.gov.br/compras/edital/70024-1-00001-2021. Entrega das Propostas: 07/05/2021 às 09h30. Endereço: Av Presidente Dutra, 1889, Baixa União, - Porto Velho/RO.

ANDERCLEDSON REIS
Presidente da CPL

(SIASGnet - 29/04/2021) 70024-00001-2021NE000001

TRIBUNAL REGIONAL ELEITORAL DE RORAIMA

DIRETORIA-GERAL

AVISO DE REGISTRO DE PREÇOS

O Tribunal Regional Eleitoral de Roraima, com fundamento no Decreto 7.892/2013, torna pública a Ata de Registro de Preços nº 16/2021, referente ao Pregão Eletrônico nº 09/2021 - Procedimento Administrativo SEI nº 0000978-24.2019.6.23.8000, assinada em 26.04.2021, com vigência de 1(um) ano a contar da assinatura, para eventual contratação de empresa para prestação dos serviços de limpeza de terreno pertencente ao Tribunal Regional Eleitoral de Roraima. O valor da Ata ficou definido em R$ 7.336,32 (sete mil, trezentos e trinta e seis reais e dois centavos), com BDI a ser aplicado no percentual 28,00%, cujo objeto foi adjudicado ao fornecedor M V COMÉRCIO E SERVIÇO EIRELE, CNPJ n.º 11.144.330/0001-77.

Assinam: pelo TRE/RR, Adriano Nogueira Batista, Diretor-Geral, e pela Beneficiária, Adriana Barbosa da Silva Oliveira. A especificação completa do objeto encontra-se no Edital do referido pregão, disponibilizado no sítio www.tre-rr.jus.br.

ADRIANO NOGUEIRA BATISTA
Diretor-Geral

AVISO DE REGISTRO DE PREÇOS

O Tribunal Regional Eleitoral de Roraima, com fundamento no Decreto 7.892/2013, torna pública a Ata de Registro de Preços n.° 19, referente ao Pregão Eletrônico nº 06/2021 - Procedimento Administrativo SEI nº 0002190-46.2020.6.23.8000, assinada em 27.04.2021, com vigência de 1(um) ano a contar da assinatura, para uma futura e eventual contratação de empresa especializada na prestação de serviços de lavagem, polimento e lubrificação automotiva para os veículos que compõem a frota do TRE/RR, cujo o objeto foi adjudicado ao fornecedor conforme a seguir: ARP n.° 19 - GONÇALVES E BORGES LTDA - ME, CNPJ n.º 21.785.298/0001-62. GRUPO 1, itens de 1 a 42. Valor total da Ata: R$ 100.000,00.

Assinam: pelo TRE/RR, Adriano Nogueira Batista, Diretor-Geral, e pela Beneficiária, Igor Thiago Borges Leonel. A especificação completa do objeto encontra-se no Edital do referido pregão, disponibilizado no portal do comprasnet ou no sítio www.tre-rr.jus.br.

ADRIANO NOGUEIRA BATISTA
Diretor-Geral

TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA

EXTRATO DE TERMO ADITIVO

Contratada: Mapfre Seguros Gerais S/A. CNPJ da Contratada: 61.074.175/0001-38. Objeto: Termo Aditivo n. 035/2021, referente ao Contrato n. 037/2018, cujo objeto é o seguro para 14 (quatorze) veículos que compõem a frota do TRESC (prorroga o prazo de vigência da apólice de seguro até as 24h do dia 08/05/2022 e registra a emissão de novo empenho). Valor total: R$ 6.312,55. Fundamento legal: Lei n. 8.666/1993. Data da assinatura: 13/04/2021. Pregão n. 029/2018.

EXTRATO DE TERMO ADITIVO

Contratada: Grabin Obras e Serviços Urbanos EIRELI. CNPJ da Contratada: 08.058.662/0001-24. Objeto: Termo Aditivo n. 046/2021, referente ao Contrato n. 048/2020, cujo objeto é a prestação de serviços continuados e especializados de telefonistas (repactuação). Novo valor mensal estimado: R$ 9.825,39, a partir de 01/01/2021. Fundamento legal: Lei n. 8.666/1993. Data da assinatura: 27/04/2021. Pregão n. 029/2020.

RESULTADO DE JULGAMENTO
PREGÃO Nº 11/2021

Objeto: Contratação de empresa para a prestação de serviços especializados e continuados de telefonia móvel pessal, no Estado de Santa Catarina, com fornecimento de 174 (cento e setenta e quatro) aparelhos móveis celulares, a título de comodato. Data do julgamento: 26/04/2021. Empresa vencedora: TELEFÔNICA BRASIL S.A.

HELOÍSA HELENA BASTOS SILVA LÜBKE
Pregoeira

(SIDEC - 29/04/2021) 070020-00001-2021NE999999

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 21/2021 - UASG 70020

Nº Processo: 8.473/2021. Objeto: Contratação de empresa especializada para execução de desinsetização e desratização dos imóveis próprios e locados sob responsabilidade do TRESC. Total de Itens Licitados: 6. Edital: 30/04/2021 das 12h00 às 17h00. Endereço: Rua Esteves Junior, 80, Centro - Florianópolis/SC ou https://www.gov.br/compras/edital/70020-5-00021-2021. Entrega das Propostas: a partir de 30/04/2021 às 12h00 no site www.gov.br/compras. Abertura das Propostas: 13/05/2021 às 14h00 no site www.gov.br/compras. Informações Gerais: O Edital, o Projeto Básico / Termo de Referência e demais documentos também estão disponíveis no site www.tre-sc.jus.br (Transparência - Contas públicas - Licitações - Pregões - 2021).

HELOISA HELENA BASTOS SILVA LUBKE
Coordenadora de Julgamento de Licitações

(SIASGnet - 28/04/2021) 70020-00001-2021NE999999

TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 33/2021 - UASG 70018

Nº Processo: 075631-13.2019. Objeto: Prestação de serviços de coffee break.. Total de Itens Licitados: 1. Edital: 30/04/2021 das 08h00 às 12h00 e das 13h00 às 17h00. Endereço: Rua Francisca Miquelina, 123, Bela Vista - São Paulo/SP ou https://www.gov.br/compras/edital/70018-5-00033-2021. Entrega das Propostas: a partir de 30/04/2021 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 12/05/2021 às 13h00 no site www.gov.br/compras. Informações Gerais: .

ALESSANDRO DINTOF
Secretário de Administração de Material

(SIASGnet - 28/04/2021) 70018-00001-2021NE000169

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 32/2021 - UASG 70018

Nº Processo: 079925-11.2019. Objeto: Aquisição de material de impermeabilização. . Total de Itens Licitados: 8. Edital: 30/04/2021 das 08h00 às 12h00 e das 13h00 às 17h00. Endereço: Rua Francisca Miquelina, 123, Bela Vista - São Paulo/SP ou https://www.gov.br/compras/edital/70018-5-00032-2021. Entrega das Propostas: a partir de 30/04/2021 às 08h00 no site www.gov.br/compras. Abertura das Propostas: 12/05/2021 às 13h00 no site www.gov.br/compras. Informações Gerais: .

ALESSANDRO DINTOF
Secretário de Administração de Material

(SIASGnet - 27/04/2021) 70018-00001-2021NE000068

TRIBUNAL REGIONAL ELEITORAL DE SERGIPE

SECRETARIA
SECRETARIA DE ADMINISTRAÇÃO E ORÇAMENTO

RESULTADO DE JULGAMENTO
PREGÃO Nº 3/2021

Fica homologado o processo licitatório nº 0003951-24.2021.6.25.8000, referente ao Pregão 03/2021 - Eletrônico, destinado à contratação de empresa especializada na gestão de mão-de-obra para prestação de serviços continuados de telefonista, a serem executados na sede do Tribunal Regional Eleitoral de Sergipe, tendo como adjudicatário o licitante vencedor do respectivo item do certame, conforme ata constante dos autos e disponível no site www.comprasgovernamentais.gov.br.

WALKELINE FRAGA DIAS
Analista Judiciário

(SIDEC - 29/04/2021) 070012-00001-2021NE100000

TRIBUNAL REGIONAL ELEITORAL DO TOCANTINS

AVISO DE LICITAÇÃO FRUSTRADA
PREGÃO ELETRÔNICO Nº 10/2021

O Tribunal Regional Eleitoral do Tocantins torna público o resultado do Pregão Eletrônico nº 10/2021, Processo Administrativo Eletrônico nº 0001117-91.2021.6.27.8000. O pregão restou frustrado

Palmas-TO, 29 de abril de 2021.
CARLOS HENRIQUE DRUMOND SOARES MARTINS
Secretário de Administração e Orçamento