ANEXO III
ESPECIFICAÇÕES TÉCNICAS DOS DISPOSITIVOS ELETRÔNICOS EMBARCADOS NA CARTEIRA DE IDENTIDADE FUNCIONAL MILITAR (CHIPS DE CONTATO E SEM CONTATO)

I - Serão inseridos dois chips na carteira de identidade funcional militar, um sem contato e outro com contato, este para questões de PKI certificação digital e suporte a multiaplicação.

II - São as seguintes as especificações do **chip** sem contato:

a) seguir as recomendações de interfaces (ISO/IEC 14443A), transmissão de dados sem contato e suprimento de energia (sem necessidade de bateria);

b) operação à distância: até 100 mm;

c) frequência de operação: 13.56 MHz;

d) transferência de dados: 106 kB/s;

e) anticolisão verdadeira;

f) EEPROM no mínimo de 1 (um) kB;

g) tempo de retenção de dados de até 10 (dez) anos;

h) suporte de gravação de 100.000 (cem mil) ciclos;

i) encriptação (Crypto1);

j) conjunto individual de duas chaves por setor (por aplicação) com derivação de chaves;

k) número serial único para cada módulo de **chip**; e

l) suporte à multiaplicação com chaves individuais para acesso dos setores de EEPROM.

III - São as seguintes as especificações do **chip** com contato:

a) características eletromagnéticas, químicas, físicas, mecânicas e de ordenamento lógico de acordo com as recomendações:

b) ISO/IEC 7816 - **Identification Cards**, **Integrated Circuit Cards**; e

c) ISO/IEC 19784 - **Information Technology**.

IV - As características e recomendações físicas em relação à luz ultravioleta, raios-X, superfície de contato, resistência mecânica e elétrica, interferência eletromagnética, estática, temperatura de operação, torção e flexibilidade do **chip** com contato devem estar no formato da ISO/IEC 7816-1, ISO/IEC 7810 e ISO/IEC 10373.

V - As características de dimensão e acoplamento elétrico devem seguir as normas estabelecidas na ISO/IEC 7816-2.

VI - As normas em relação a sinais e protocolos de transmissão sobre contatos elétricos, classes de operação (A, B e C, o **chip** deve suportar mais de uma classe; o cartão não deve ficar inoperável caso seja aplicada uma classe não suportada por esse), sinal de **reset** e **clock**, I/O, devem estar de acordo com o estabelecido na ISO/IEC 7816-3.

VII - Os procedimentos operacionais, tais quais de ativação, seleção de classe e **reset**, seleção de transmissão e protocolos, **clock stop** e desativação, devem estar de acordo com o estabelecido na ISO/IEC 7816-3.

VIII - As características assíncronas sobre ETU, **frame** de transmissão, erros do sinal e pergunta/resposta devem seguir as normas estabelecidas na ISO/IEC 7816-3.

IX - Os parâmetros e escolha do protocolo de transmissão T=0 (**half-duplex transmission**) e T=1 (**half-duplex transmission blocks**) devem conter todas as normas e regras dispostas na ISO/IEC 7816-3.

X - Os padrões estabelecidos na ISO/IEC 7816-4 para interoperabilidade entre os dispositivos leitores e o **chip** devem ser seguidos, assim como os comandos básicos de **reading**, **writing** e **updating**, para comunicação entre os dispositivos de todas as empresas que fornecem esse tipo de solução.

XI - As normas estabelecidas para os procedimentos de registro (RID) devem seguir a norma ISO/IEC 7816-5.

XII - Os padrões estabelecidos nas ISO/IEC 7816-6, ISO/IEC 7816-7 e ISO/IEC 7816-8 sobre as definições da transferência física e dados operacionais (seleção do protocolo de transmissão T=0 e T=1, o **chip** deve suportar os dois - não simultaneamente), comandos de interoperabilidade para dispositivos de leitura e questões sobre o controle da segurança do **chip**, principalmente em relação aos algoritmos de criptografia que podem ser usados, devem ser obedecidos para o **chip** com contato.

XIII - A arquitetura do **chip** com contato deve conter:

a) pelo menos 100.000 (cem mil) ciclos leitura/escrita sem erros; e

b) capacidade para retenção dos dados de até 10 (dez) anos.

XIV - O fornecedor do **chip** com contato deverá disponibilizar a especificação do sistema operacional embarcado, detalhando o tipo de sistema operacional, as interfaces de entrada e saída de dados e rotinas internas do sistema operacional, observadas as seguintes exigências:

a) suporte a 3DES e AES;

b) EEPROM de, no mínino, 72 kB; e

c) suporte a multiaplicação conforme Tabelas 1 e 2.

XV - O sistema cartão/**chip** deve possuir homologação da ICP-Brasil para as questões do certificado digital, assim como contemplar todos padrões para algoritmos criptográficos vigentes (mínimo RSA 2048 ou superior, como ECDSA) e de **hash** (mínimo SHA, família 2) determinadas pela ICP-Brasil.

XVI - As considerações relatadas abrangem somente aspectos técnicos básicos da arquitetura do **chip** com contato, estabelecidos em normas técnicas.

Tabela 1
Tabela de aplicação dos chips da Carteira de Identidade Funcional Militar

Interface	Aplicação	Finalidade	Serviço	Objetos externos necessários	Condições para acesso ao serviço
Sem contato	Aplicação sem contato			Cartão	Controle de Acesso; leitor de **chip** sem contato
Com contato	Aplicação com contato	Autenticação do Cartão e identificação do portador	Leitura dos dados de controle do Cartão, autenticação eletrônica dos Dados (verificação se não é falso)	Cartão	
			Leitura de dados de identificação do portador	Cartão	Autenticação do portador
	Aplicação ICP-Brasil	Utilização de chaves e certificados digitais ICP- Brasil	Uso de chaves ICP-Brasil: propiciar ao portador a utilização de sua chave privada em atividades de autenticação e de assinatura digital na ICP-Brasil.	Cartão	Autenticação do portador
			Leitura de certificados digitais, utilização do certificado digital em sistemas computacionais para autenticação, assinatura digital, sigilo de dados, entre outros.	Cartão	

Tabela 2
Tabela de objetos eletrônicos presentes nos chips da Carteira de Identidade Funcional Militar

Interface	Aplicação	Objetos	Descrição
Sem contato	Controle de Acesso		
Com contato	ICP-Brasil	Certificado digital	Cadeia de certificados digitais associada ao certificado de assinatura do portador
			A geração e armazenamento do certificado digital de assinatura e da cadeia de certificação são de responsabilidade da autoridade certificadora (AC)
		Chave privada de assinatura do portador	Chave privada de assinatura do portador
			A geração do par de chaves assimétricas de assinatura é de responsabilidade do portador A geração das chaves assimétricas de autenticação do cartão é realizada de forma que seja gerada pelo próprio CHIP do cartão A chave pública é exportada, porém, a chave privada nunca é exportada do cartão
		PIN de uso da chave privada	PIN para autorização de uso da chave privada de assinatura, gerado pelo usuário

ANEXO IV
MODELOS DE CARTEIRA DE IDENTIDADE FUNCIONAL MILITAR E DE CARTÃO DE SERVIÇO MILITAR INICIAL
1 - POLÍCIA MILITAR DO ESTADO DO PARÁ (PMPA)
A) CARTEIRA DE IDENTIDADE FUNCIONAL MILITAR
A.1) PARA MILITARES DA ATIVA