ANEXO VI

Especificação da Tecnologia SINIAV

Requisitos de Segurança Física de Equipamentos da *Geração Zero* (G0)

Índice

1 Escopo

Este documento especifica, para equipamentos do SINIAV da *Geração Zero* (G0):

- Requisitos de segurança para leitores (SLP e ECS) e transponders (PIVE) do SINIAV.

2 Referências a Normas

Os seguintes documentos são indispensáveis para a aplicação desta especificação. Para as referências datadas, aplica-se somente a edição citada. Para referências não datadas, aplica-se a última edição do documento referenciado (incluindo as respectivas emendas).

[1] Centro de Pesquisas Avançadas Wernher von Braun: *Especificação do Protocolo IAV DENATRAN na* Geração Zero *(G0)*

[2] Centro de Pesquisas Avançadas Wernher von Braun: *Especificação do ECS e Procedimentos de Gravação*

[3] Centro de Pesquisas Avançadas Wernher von Braun: *Procedimentos e Requisitos Técnicos para a Personalização e Ativação do Modo SINIAV em PIVEs pelo ECS* [2]

3 Abreviações

AVI	Automatic Vehicle Identification – Identificação Automática de Veículos

DENATRAN	National Department of Transportation – Departamento Nacional de Trânsito
ECS	SINIAV Configuration Equipment – Equipamento Configurador do SINIAV. Obs.: Equipamento de leitura e escrita de PIVES DENATRAN, cuja operação é de responsabilidade dos DETRANs [2]. São os equipamentos utilizados durante a implantação e outras manipulações da placa eletrônica. O ECS deve estar em ambiente seguro e controlado, e todas as suas operações são dependentes de conexão segura com o DENATRAN.
IAV	vide AVI
OBU	On Board Unit – Unidade de Bordo (vide Transponder e PIVE)
PIVE	Electronic Vehicle Identification Plate – Placa Eletrônica de Identificação Veicular DENATRAN. Obs.: È termo oficial do DENATRAN para o Transponder do SINIAV (vide Transponder e OBU).
RSU	Roadside Unit – Unidade de Pista. No âmbito do SINIAV, é chamado também de SLP (vide SLP).
SINIAV	National System for Automated Vehicle Identification – Sistema Nacional de Identificação Automática de Veículos
SLP	Subsystem for Electronic License Plate Identification – Sub-Sistema de Leitura de Placa Eletrônica. Obs.:Conjunto de equipamentos (leitores RFID, antenas, computadores, etc) implantados em um ponto de circulação de veículos com o objetivo essencial de coletar dados de passagem de todos os veículos circulantes naquele ponto, além de realizar processamento da informação com o objetivo de identificar rapidamente veículos que estejam cadastrados na Lista de Exceção de Segurança. Em sistemas de IAV internacionais, este equipamento é chamado também de RSU.
Transponder	Dispositivo, baseado na tecnologia RFID, a ser instalado nos veículos como uma "placa eletrônica". Obs.: No âmbito do SINIAV, é chamado também de PIVE (vide PIVE) ou de OBU (vide OBU).

4 Requisitos de Segurança Física de Equipamentos da Geração Zero (G0) do SINIAV

O presente documento define requisitos de segurança física para os equipamentos Leitor (incluindo os equipamentos SLP e ECS) e Transponder (também conhecido como PIVE DENATRAN ou OBU), da *Geração Zero* (G0) do SINIAV, que implementam e reivindicam conformidade com o Protocolo IAV DENATRAN G0 [1].

5 Requisitos de Leitor SINIAV G0

REQ#1 O equipamento Leitor SINIAV G0 deve prover chassi opaco e resistente à violação e manipulação física indevida (*tampering*), com caixa que evidencie qualquer tentativa de violação física (ex: resultados permanentemente visíveis no caso de abertura do chassi).

REQ#2 Sensores para detecção de tentativa de violação do equipamento leitor, incluindo hardware do sensor e modulo de controle em software no firmware do leitor,

resultando em apagamento (zeroização[1], ou *zeroization* em inglês) de todos os dados relacionados à segurança e confidencialidade da memória do leitor (incluindo chaves secretas, *tokens*, *black-lists*, etc.) e na incapacitação do dispositivo. Exemplos da violação do equipamento leitor incluem abertura física de chassi, bem como abertura física de qualquer porta do equipamento (ex: porta de comunicação, porta de I/O, porta de ventilação, etc.).

REQ#3 Entre outros, a utilização de um ou mais dos seguintes sensores é RECOMENDADA para atender o REQ#2:

i. Um ou mais sensores de nível de *energia* e/ou *tensão* para detecção de falha temporária de energia, ou de variação de energia indevida (detectar potência inferior ou superior ao limiar, flutuação indevida, ou ausência de energia).

ii. Um ou mais sensores de *detecção de movimento interno* (ex: detectar tentativas de inserção física de sondas).

iii. Um ou mais sensores de *detecção de luz interna* para detectar a abertura completa ou parcial do encapsulamento do equipamento.

iv. Um ou mais sensores de *pressão atmosférica* para detectar violações do encapsulamento do equipamento.

v. Um ou mais sensores de *temperatura* internos para monitoramento de faixa de temperatura aceitáveis.

vi. Um ou mais sensores de *deslocamento* para detecção de remoção não autorizada de dispositivos (ex: sensor de aceleração).

REQ#4 Fonte de alimentação interna de emergência para alimentação dos sensores anti-falsificação e para permitir que o leitor realize o apagamento (zeroização) da memória e a incapacitação do dispositivo quando uma tentativa de adulteração/violação é detectada. Em particular, deve ser garantido que o processo de apagamento da memória e a incapacitação do dispositivo sejam realizados antes que a alimentação interna de emergência acabar.

REQ#5 Registro persistente interno do histórico da segurança física, disponível para uma análise posterior no caso de detecção de uma tentativa de violação (com zeroization de memória e incapacitação do dispositivo).

REQ#6 Todos os meios de proteção (eletrônico e mecânico) devem ser habilitados antes da primeira inicialização e operação do leitor no modo SINIAV e somente poderão ser desabilitados depois que todas as informações relevantes á segurança SINIAV estejam seguramente apagadas do leitor, sem meio de recuperação.

REQ#7 Toda e qualquer característica ou funcionalidade relacionada à segurança física do equipamento leitor deve estar presente e descrita de forma quantitativa e mensurável na documentação que obrigatoriamente deve acompanhar o leitor, tais como: condições nominais de operação, limiares, tolerâncias, ocorrência, condições de ativação e utilização (ex: especificar o limiar mensurável de ativação de um sensor de aceleração, incluindo todas as tolerâncias aplicáveis, bem como demais características pertinentes).

[1] Na presente especificação foi adotado o termo *zeroização* como neologismos por transferência de vocábulo estrangeiro da língua inglesa, notadamente *zeroization*.

6 Requisitos de Transponder SINIAV G0

REQ#8 O equipamento Transponder SINIAV G0 deve prover encapsulamento opaco e duro, com selagem do invólucro e sem entrada para ventilação ou monitoração de qualquer espécie.

REQ#9 O equipamento transponder não pode permitir qualquer tipo de manutenção, inclusive a troca de bateria, e qualquer tentativa de acesso físico deve ser considerada violação devendo ser evidenciada por destruição visível do encapsulamento.

REQ#10 No caso de um equipamento transponder com fonte própria de energia (transponder semi-ativo ou ativo), o equipamento deve prover sinalização eletrônica de tentativa de violação e/ou descolamento do local de fixação por ativação do seu *tamper flag* **TF** de forma irreversível, considerando também a especificação e os demais requisitos funcionais do *tamper flag* definidos no documento *Procedimentos e Requisitos Técnicos para a Ativação do Modo SINIAV em PIVEs pelo ECS* [3].

REQ#11 No caso de um equipamento transponder com fonte própria de energia (transponder semi-ativo ou ativo), o equipamento deve garantir apagamento imediato (zeroização) de todos os dados relacionados à segurança do transponder (incluindo quaisquer chaves secretas, usadas para a autenticação, controle de acesso, encriptação ou decriptação de dados, ou para qualquer outra finalidade, mas excluindo o *tamper flag* **TF**), contidos na memória volátil e não volátil, no primeiro caso de violação e/ou descolamento do local de fixação detectado, juntamente com acionamento do *tamper flag*.

REQ#12 Uma vez que o tamper flag **TF** foi ativado, o transponder deve ignorar qualquer comando de leitor que envolve criptografia e/ou uso de chaves secretas.

REQ#13 No caso de um equipamento transponder sem fonte própria de energia (transponder passivo), o equipamento deve prover um encapsulamento altamente resistente, que protege, de forma efetiva, a confidencialidade de todos os dados relacionados à segurança do transponder (incluindo quaisquer chaves secretas, usadas para a autenticação, controle de acesso, encriptação ou decriptação de dados, ou para qualquer outra finalidade), contidos na memória volátil e não volátil do equipamento, contra tentativas da extração destes dados confidenciais.

REQ#14 No caso de um equipamento transponder com fonte própria de energia (transponder semi-ativo ou ativo), o equipamento deve ter um sensor de monitoramento da vida útil desta, que detecta um tempo de vida útil restante limitado (ex: poucas semanas ou meses restantes), e bem como uma falha iminente da bateria (ex: poucas horas ou dias restantes). A determinação de limiares adequados para a detecção correta do estado de carregamento da fonte própria de energia, e da sua vida útil restante esperada, está sob responsabilidade do fabricante do equipamento transponder.

REQ#15 No caso de um equipamento transponder com fonte própria de energia (transponder semi-ativo ou ativo), se o equipamento detectar que a sua fonte (ex: bateria) tem pouco tempo de vida restante (ex: poucas semanas ou meses), o equipamento deve permanentemente e de forma irreversível acionar o seu *battery*

flag **BF** (vide a definição e utilização do *battery flag* especificada no Protocolo IAV DENATRAN G0 [1]).

REQ#16 No caso de um equipamento transponder com fonte própria de energia (transponder semi-ativo ou ativo), se o equipamento detectar que a sua fonte de energia (ex: bateria) tem tão pouco tempo de vida restante que uma falha de operação esteja iminente (ex: poucas horas ou dias de operação restantes), o equipamento deve imediatamente apagar (zerar, ou *zeroize* em inglês) a sua memória da mesma maneira que especificada pelo requisito REQ#11.

REQ#17 O mecanismo de fixação do equipamento transponder deve suportar a vibração do veículo e esforços leves, como os oriundos de limpeza do local, sem se soltar, danificar, ou ativar o *tamper flag*.

REQ#18 Todos os meios de proteção (eletrônicos e mecânicos) devem ser habilitados antes da primeira inicialização e operação do equipamento transponder no modo SINIAV, e não mais poderão ser desabilitados em seguida, até o fim da vida útil do equipamento transponder.

REQ#19 Toda e qualquer característica ou funcionalidade relacionada à segurança física do equipamento transponder deve estar presente e descrita de forma quantitativa e mensurável na documentação que obrigatoriamente deve acompanhar o transponder, tais como: condições nominais de operação, limiares, tolerâncias, ocorrência, condições de ativação e utilização (ex: especificar o limiar mensurável de ativação de um sensor de aceleração, incluindo todas as tolerâncias aplicáveis, bem como demais características pertinentes).

7 Proteção contra a Remoção Ilegal do Transponder

REQ#20 A partir do momento que o transponder seja permanentemente instalado em um veículo, e assim fixado numa superfície aprovado pelo DENATRAN, todos os demais requisitos supracitados, listados nas Seções 5 e 6 do presente documento, na extensão que são aplicáveis, valem também para o conjunto de transponder e daquela área do substrato que tem contato físico com o transponder.

8 Aviso Legal

O DENATRAN se reserva o direito de alterar os requisitos e métodos de testes. Qualquer alteração de requisito e/ou método de teste será comunicado a todos os fabricantes de equipamentos e implantadores do sistema SINIAV que estiverem registrados no DENATRAN, através dos canais próprios de comunicação.