

República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI 1101244-7 A2**

(22) Data de Depósito: 22/03/2011
(43) Data da Publicação: 15/01/2013
(RPI 2193)



(51) *Int.Cl.:*

G06K 7/00

G11B 5/10

G11B 5/40

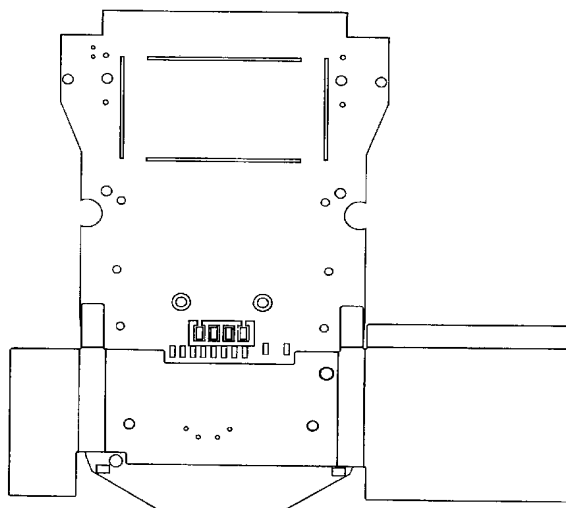
H05K 5/00

(54) Título: SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS

(73) Titular(es): TECVAN INFORMÁTICA LTDA.

(72) Inventor(es): JORGE RIBEIRO PEREIRA

(57) Resumo: SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS. Apresenta um sistema que protege as partes internas e terminais externos de Conector para Cartão Inteligente (SmartCard) com processo de envolvimento físico com circuito impresso maleável (FPC) conectado à Placa de Circuito Impresso (PCI) com sensoriamnto. A proteção é em todas as direções, exceto na face frontal do Conector para Cartão Inteligente (SmartCard) para possibilitar a inserção do Cartão Inteligente (SmartCard) ao equipamento. O Circuito Impresso Maleável (FPC) envolve o Conector para Cartão Inteligente (SmartCard), sendo que o suporte de proteção é sobreposto, total ou parcialmente, sobre o Conector para Cartão Inteligente (SmartCard) impedindo que o FPC seja retirado. No suporte de proteção há um alojamento conector tipo Zebra que é reposável pelo sensoriamnto entre as PCIs presentes nas faces superior e inferior do Conector para Cartão Inteligente (SmartCard) e também impede acesso aos terminais traseiros do conector que está sendo protegido. Na ocorrência de uma invasão ao Conector para Cartão Inteligente (SmartCard), o acionamento de qualquer um dos sensores comunica ao processador que destrói todas as chaves de segurança que criptografam as informações sigilosas armazenadas em uma memória eletrônica.



"SISTEMA PARA PROTEÇÃO DE
CONECTOR PARA CARTÕES INTELIGENTES EM
EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS"

Refere-se o presente relatório descritivo ao

- 5 Privilégio de Invenção de um dispositivo de proteção eletrônico-
mecânico de conectores para Cartão Inteligente (SmartCard)
utilizados em equipamentos que exigem altos níveis de segurança,
dotado de sensores de circuitos de alta segurança, de modo a
proteger informações sigilosas, contra intrusão e acessos não
10 autorizados.

- Os Equipamentos Seguros como Terminais
de Pontos de Venda (PDV ou em inglês POS – Point Of Sales),
Terminais PINPAD, Teclado Encriptado, este último normalmente
utilizado em equipamentos de autoatendimento e até mesmo
15 Equipamentos Leitores de Cartões Inteligentes, permitem
aplicações como pagamentos de despesas utilizando diversos
meios de pagamento tais como: cartões de crédito, cartões de
débito, cartões inteligentes, transações bancárias, validações
eletrônicas, etc.. O uso de cartões inteligentes (SmartCards) tem se
20 tornado bastante frequente devido aos recursos que possui e
também por sua segurança maior que cartões magnéticos apenas.
Para assegurar que as informações lidas do cartão inteligente
(SmartCard) não sejam interceptadas ou capturadas quando o
cartão inteligente estiver inserido no conector próprio presente nos
25 equipamentos seguros, faz-se necessário o uso de disposição
construtiva segura.

O presente sistema de proteção baseia-se no
envolvimento físico de toda superfície externa do conector para
cartões inteligentes (SmartCard), exceto a face que permite a

inserção do cartão inteligente (SmartCard) no conector, presentes em Terminais de Pontos de Venda, POS, PINPAD, Leitores de Cartões Inteligentes (SmartCard) ou Teclado Encriptado, com a utilização de circuito impresso maleável (FPC – Flexible Printed Circuit), que protege mecanicamente, não apenas parte traseira do conector para cartão inteligente (SmartCard), mas suas duas laterais, a parte superior e a parte inferior do mesmo, podendo ou não conter adesivos ou resinas depositados em áreas específicas do circuito impresso maleável, para que fiquem totalmente inacessíveis, impossibilitando ataques externos. Além disso, o sistema de proteção é complementado através de monitoração de sensores ativos através de pontos de conexão do circuito impresso maleável com circuitos de alarme implantados em Placa de Circuito Impresso, cuja descrição detalhada segue abaixo.

Um Circuito Impresso Maleável (FPC) é um circuito eletrônico impresso sobre material flexível não condutor. Esse circuito eletrônico é impresso nas faces externas, podendo ser em apenas uma das faces ou em duas faces ou em suas camadas intermediárias, caso seja um Circuito Impresso Maleável com múltiplas camadas, podendo também ser sobrepostos formando várias camadas de circuitos. Estes circuitos possuem a forma de mosaicos randômicos cobrindo toda a superfície do FPC, de tal sorte que, ao serem rompidas ou perfuradas, são detectadas por circuitos especializados de segurança que indicam uma tentativa de invasão do sistema.

A solução proposta também possui a proteção contra ataques químicos de ablação, ataques mecânicos de delaminação e perfuração da FPC, através do uso de uma malha randômica eletrônica que é ligada ao circuito de segurança que

detecta qualquer tentativa de ataque.

A solução de envolver o conector para Cartão Inteligente (SmartCard) desta forma é, do ponto de vista de montagem, bastante simples, e conseqüentemente, de custo baixo, mas extremamente eficiente. Como o Circuito Impresso Maleável pode ser posteriormente adesivado ou resinado, a tentativa de acesso interno do conector para Cartão Inteligente (SmartCard) torna o processo destrutivo.

A solução proposta para detecção de ataque utiliza trilhas múltiplas, dispostas em passos milimétricos, ou em frações de milímetros, formando uma malha randômica, conectadas à Placa de Circuito Impresso, através de contatos soldados presentes na face do Circuito Impresso Maleável abaixo do conector de Cartão Inteligente (SmartCard), portanto esses contatos ficam protegidos em todas direções, pois fica presente na FPC entre a Placa de Circuito Impresso e o Conector para Cartão Inteligente. Estas trilhas são confeccionadas em material, como por exemplo, o cobre, que permite trilhas de espessuras da ordem de 6 mils ou menores ainda.

Como resultado da análise do estado da técnica, o Privilégio de Invenção aqui descrito pretende propor uma técnica inovadora com recursos de proteção para impedir o acesso não autorizado ao interior do Conector para Cartão Inteligente (SmartCard) presente em Terminal de Ponto de Venda, POS, PINPAD, Leitores de Cartão Inteligente e Teclado Encriptado e com custos reduzidos.

Assim sendo, a fim de permitir uma melhor elucidação do objeto em questão, proceder-se-á à sua descrição pormenorizada com referência aos desenhos seguintes, onde:

A figura 1 - ilustra a vista da área reservada para o conector para Cartão Inteligente (SmartCard) que deseja-se proteger, com o sistema de proteção por envolvimento físico (Circuito Impresso Maleável – FPC), e já apresentando a infraestrutura necessária, que é composta por 1 PCI (Placa de Circuito Impressa) com contatos para a FPC, por onde é injetado o sinal eletrônico do circuito de proteção na malha randômica presente na FPC (Circuito Impresso Maleável), sendo que é possível a utilização de FPCs adicionais para elevar o grau de proteção da solução, contatos na PCI para conector do tipo Zebra, encaixe para suporte de proteção da parte traseira do Conector para SmartCard, protegendo acessos aos pinos com sinais do Conector para SmartCard da Zebra e conector para interligação da PCI inferior e da PCI superior, incorporando maior proteção de acesso ao Conector SmartCard nessas duas direções, sendo que essas PCIs podem apresentar circuitos de mechas nelas próprias ou as mechas estarem presentes em FPCs adicionais, sendo possível também a combinação de PCIs e FPCs nessa solução;

A figura 2 - ilustra o início da montagem do envolvimento do Conector SmartCard pelo Circuito Impresso Maleável - FPC. Observa-se que o FPC é projetado para envolver a área abaixo do Conector SmartCard, suas laterais direita e esquerda, sua parte traseira e a área superior do mesmo, lembrando que o FPC é conectado à PCI, através de solda nos respectivos contatos do FPC, por onde é injetado o sinal eletrônico do circuito de proteção na malha randômica.

A figura 3 - ilustra o FPC montado e envolvendo todo o Conector SmartCard, exceto a abertura para inserção do Cartão SmartCard propriamente dito. A fita FPC é

caracterizada por um desenho específico, para envolver três laterais e as superfícies inferior e superior do Conector SmartCard, entremeada com circuitos randômicos de proteção, que é conectado à PCI, sendo que suas partes são adesivadas ou
5 resinadas de modo a impedir que o FPC seja retirado sem antes ser danificado e gerar alarmes correspondentes. Desta forma, na figura pode-se visualizar o processo de envolvimento físico do Conector SmartCard pelo FPC;

A figura 4 - ilustra a montagem do suporte de
10 proteção dos contatos traseiros do Conector de SmartCard. Esse suporte de proteção também possui um conector do tipo Zebra que realiza o contato entre as Placas de Circuito Impresso inferior e superior, lembrando que essas PCIs possuem uma de suas camadas como circuito em forma de mechas, circuitos randômicos,
15 por onde sinais de monitoramento estão ativos. Dessa forma, se houver tentativa de separar as PCIs o sistema irá gerar alarmes. O Conector do tipo Zebra também impede acessos pela parte traseira do Conector SmartCard, pois se houver tentativa de rompimento do mesmo para se atingir os contatos do Conector SmartCard o
20 sistema gerará alarme imediatamente. O suporte de proteção sobrepõe-se ao FPC que envolve o Conector SmartCard, impedindo que a parte traseira seja acessada bem como protegendo as laterais direita e esquerda e a superfície superior do Conector contra remoção do adesivo ou resina que fixa o FPC após montado,
25 garantindo nível de proteção adicional ao sistema;

A figura 5 - ilustra o sistema de proteção do Conector SmartCard completamente montado, utilizando proteção adicional de mecha com circuito randômico sobre a PCI superior. Nota-se visualmente que o Conector SmartCard fica protegido em

todas direções, além do que há a proteção do gabinete do equipamento que pode ser Terminal Ponto de Venda, POS, PINPAD, Leitor de Cartão Inteligente (SmartCard) ou Teclado Encriptado que possui o não sistema de proteção de abertura
5 (tamper proof) inserindo maior dificuldade de acesso ao Conector SmartCard., isto garante um nível de proteção muito maior nesta solução apresentada;

A figura 6 - ilustra o sistema de proteção do Conector SmartCard em perspectiva contendo todas as suas parte
10 e peças.

Em conformidade com o quanto ilustram as figuras acima mencionadas, o sistema de envolvimento físico do Conector SmartCard é constituído por no mínimo 1 Circuito Impresso Maleável (FPC) montado envolvendo as laterais direita e
15 esquerda do Conector SmartCard bem como suas superfícies superior e inferior e também sua parte traseira, podendo ou não utilizarem adesivo ou resina para proteção adicional contra remoção da FPC, por 2 PCIs que protegem a parte superior e a parte inferior do Conector SmartCard, uma vez que essas PCIs possuem
20 circuitos randômicos de proteção, interligados, podendo ou não adicionalmente utilizar 1 ou mais FPS com circuitos randômicos de proteção sobre essas PCIs, por 1 suporte de proteção da parte traseira do Conector SmartCard, por 1 conector tipo Zebra que além de proteger acessos aos terminais do Conector SmartCard também
25 geram alarme quando houver tentativa de separação das PCIs, formando, o sistema todo, uma blindagem formidável sobre o Conector SmartCard.

Cada Circuito Impresso Maleável - FPC possui pelo menos dois circuitos com assinaturas diferentes e os

FPCs possuem, pelo menos, 1 circuito com assinatura diferente entre si, impedindo também o curto-circuito dos circuitos de proteção.

As camadas externas do circuito impresso maleável (FPC) são projetadas de forma a apresentar em toda a sua superfície trilhas condutoras finas, distribuídas de forma randômica e bastante densa, na forma de uma serpentina. As terminações destas trilhas são conectadas aos circuitos de segurança que ficam monitorando o rompimento dos mesmos. Com isso, se houver uma tentativa de se delaminar mecanicamente o circuito externo, para ter acesso às trilhas internas, as trilhas externas de proteção são rompidas, ativando o sistema de segurança. O mesmo acontece se houver uma tentativa de perfurar mecanicamente as camadas externas para acessar as trilhas internas, que provocam o rompimento de uma ou mais trilhas de proteção.

Outra característica importante do Circuito Impresso Maleável – FPC utilizado é sua fragilidade, proposital, pois não possui funcionalidade estrutural e qualquer tentativa de manipulação mais enérgica do mesmo, provoca o rompimento das trilhas físicas de proteção inseridas no circuito. Pode-se ainda utilizar a deposição de adesivo ou resina sobre o FPC para dificultar ainda a invasão, pois o adesivo ou a resina adere ao FPC e qualquer tentativa de manipulação rompe o mesmo devido à sua fragilidade e causa alarme do sistema.

O circuito do sistema de segurança, ao detectar a invasão à área do Conector SmartCard, aciona o sensor que comunica ao processador que atua destruindo todas as chaves de segurança que criptografam as informações sigilosas,

armazenadas em memória eletrônica. Sem as chaves de segurança, não é possível a recuperação das informações sigilosas da memória e a execução dos processos sigilosos, tornando o equipamento inoperante. Internamente ao processador existe um

5 gerador de números randômicos verdadeiros. Os valores aleatórios desse gerador são utilizados para criar as formas dos sinais dos sensores, servindo para os parâmetros de amplitude, frequência e fase. Esses sinais percorrem o conjunto de sensores e retornam ao microprocessador, cujos circuitos comparadores conferem os

10 referidos parâmetros em relação aos sinais originais. Detectando-se diferenças nos parâmetros, o circuito de alarme de invasão é acionado e imediatamente as chaves criptográficas são destruídas tornando o equipamento inoperante e impossibilitando a recuperação das informações.

REIVINDICAÇÕES:

1. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS"
5 **caracterizado** por um ou mais circuitos impressos maleáveis (FPCs) montados de forma a envolver todas as faces do Conector para Cartão Inteligente (SmartCard), exceto sua face frontal que permanece acessível para inserção do Cartão Inteligente (SmartCard) no conector, que abriga um circuito interno de proteção
10 contra ataques mecânicos, elétricos ou eletrônicos, podendo ser protegidos por adesivo ou resina, que deve ser conectado a um circuito de monitoramento de segurança.
2. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM
15 EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS", de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) forma parte de um Terminal PIN PAD.
3. "SISTEMA PARA PROTEÇÃO DE
20 CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS", de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) forma parte de um Terminal POS (Point Of Sale – PDV
25 = Ponto De Venda).
4. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS", de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito

sistema de proteção de Conector para Cartão Inteligente (SmartCard) forma parte de um Teclado Encriptado.

5. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS", de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) forma parte de um Leitor de Cartão Inteligente (SmartCard).

6. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS", de acordo com a reivindicação 1, e em que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) é **caracterizado** pela introdução de um ou mais circuito impresso maleável, contendo circuito em forma de mosaico com padrão randômico para detectar o rompimento de trilhas, que é analisado por um circuito externo de monitoramento de segurança, utilizado para monitorar qualquer tentativa de invasão ao Conector para Cartão Inteligente (SmartCard) a ser protegido.

7. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS" de acordo com a reivindicação 6, e em que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) é **caracterizado** de modo que cada circuito do mosaico possui assinaturas eletrônicas distintas entre si, que são padrões de corrente, forma de onda e frequências diferentes, permitindo caracterizar univocamente cada circuito detector pelo circuito externo de

monitoramento de segurança.

8. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS" de acordo com a reivindicação 6, e em que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) é **caracterizado** por proteção mecânica traseira através de suporte de proteção dos terminais de contatos do Conector SmartCard e por um conector tipo Zebra que além de proteger acessos aos terminais do Conector para Cartão Inteligente (SmartCard) gera alarme quando houver tentativa de invasão ao Conector para Cartão Inteligente (SmartCard).

9. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS" de acordo com a reivindicação 8, e em que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) é **caracterizado** por proteção adicional nas faces superior e inferior do mesmo por Placas de Circuito Impresso (PCI) que possuem circuito em forma de mosaico randômico em pelo menos uma de suas faces ou camadas, além do que podem possuir proteção extra através de um ou mais Circuito Impresso Maleável (FPC).

10. "SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS" de acordo com a reivindicação 9, e em que o dito sistema de proteção de Conector para Cartão Inteligente (SmartCard) é **caracterizado** por proteção contra separação das Placas de Circuito Impresso (PCI), gerando alarme imediato e tornando o equipamento

inoperante.

FIG. 1

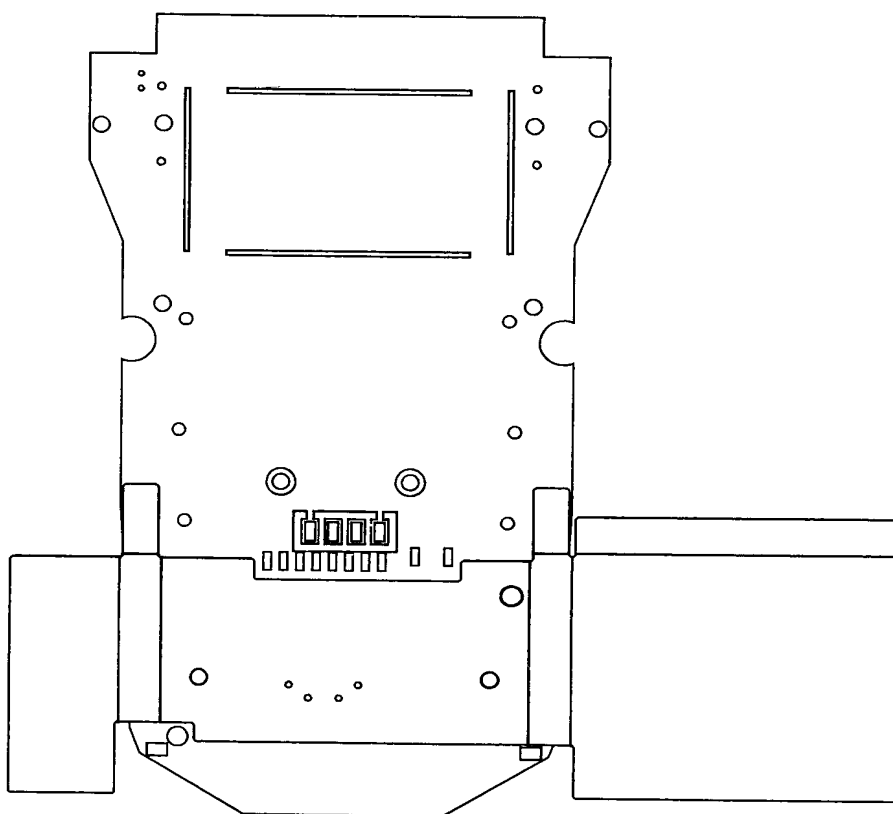


FIG. 2

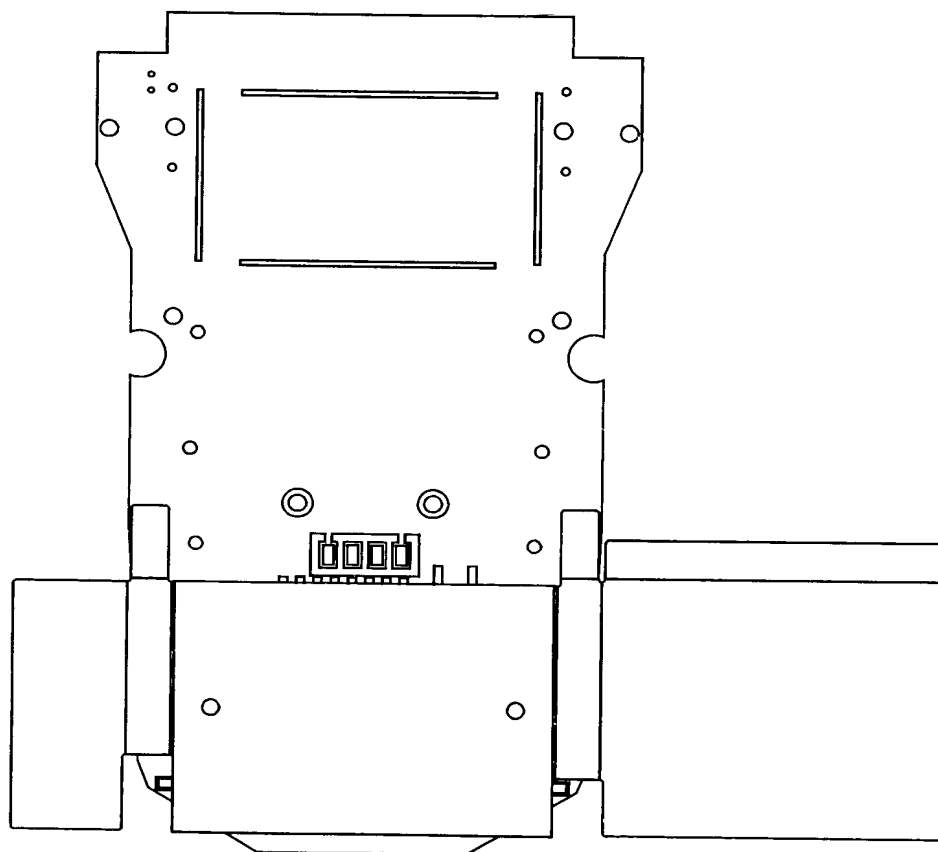


FIG. 3

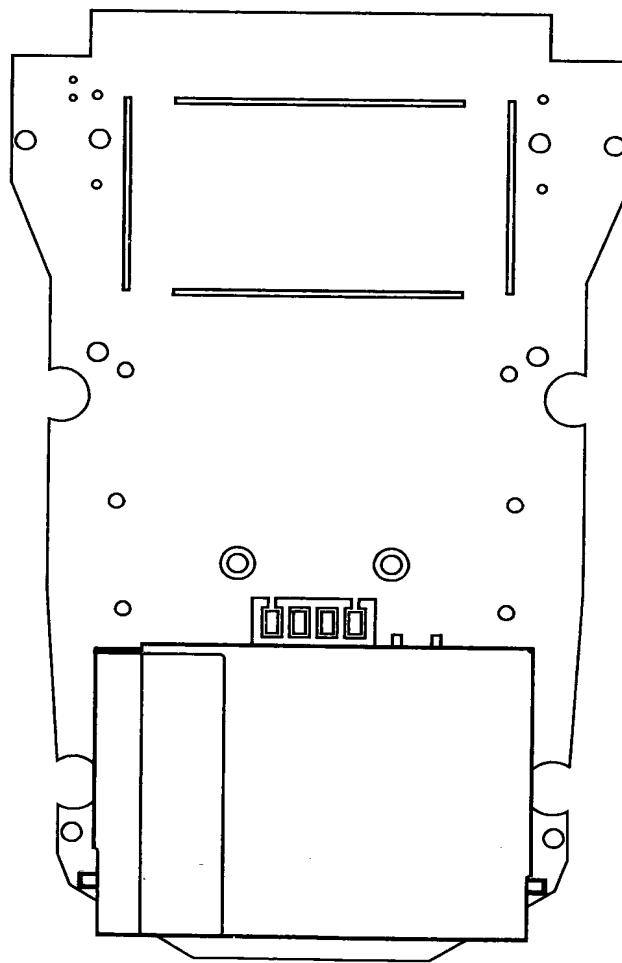


FIG. 4

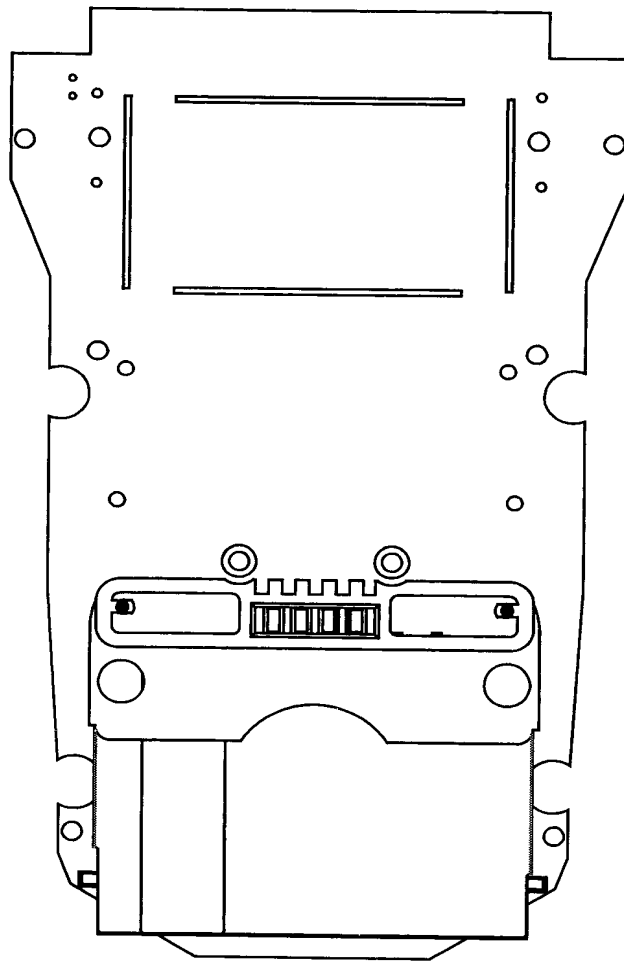
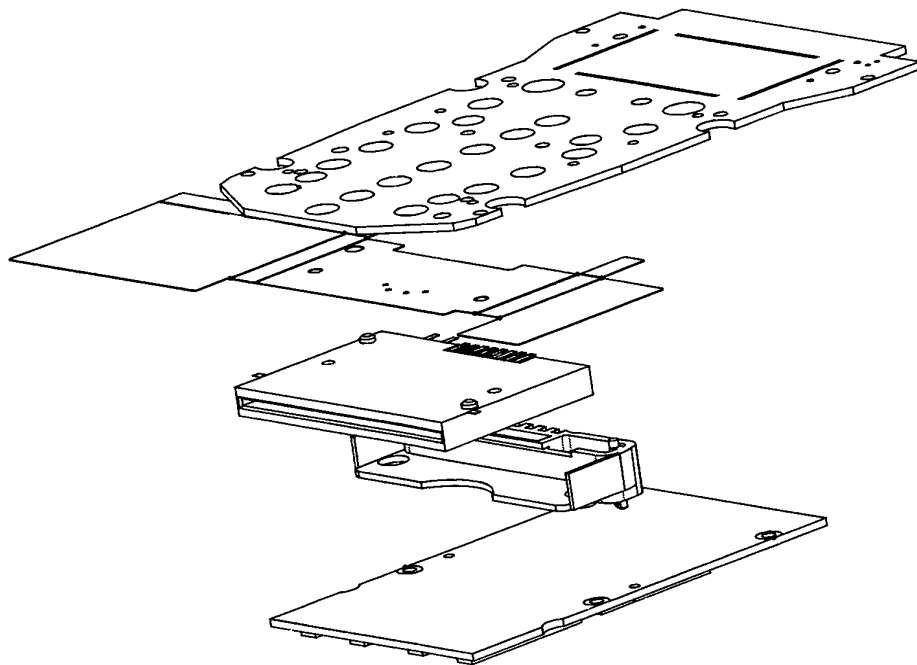


FIG. 5



FIG. 6



RESUMO:

"SISTEMA PARA PROTEÇÃO DE CONECTOR PARA CARTÕES INTELIGENTES EM EQUIPAMENTOS QUE EXIGEM SEGURANÇA DE DADOS"

5 apresenta um sistema que protege as partes internas e terminais externos de Conector para Cartão Inteligente (SmartCard) com processo de envolvimento físico com circuito impresso maleável (FPC) conectado à Placa de Circuito Impresso (PCI) com sensoramento. A proteção é em todas as direções, exceto na face

10 frontal do Conector para Cartão Inteligente (SmartCard) para possibilitar a inserção do Cartão Inteligente (SmartCard) ao equipamento. O Circuito Impresso Maleável (FPC) envolve o Conector para Cartão Inteligente (SmartCard), sendo que o suporte de proteção é sobreposto, total ou parcialmente, sobre o Conector

15 para Cartão Inteligente (SmartCard) impedindo que o FPC seja retirado. No suporte de proteção há um alojamento para conector tipo Zebra que é responsável pelo sensoramento entre as PCIs presentes nas faces superior e inferior do Conector para Cartão Inteligente (SmartCard) e também impede acesso aos terminais

20 traseiros do conector que está sendo protegido. Na ocorrência de uma invasão ao Conector para Cartão Inteligente (SmartCard), o acionamento de qualquer um dos sensores comunica ao processador que destrói todas as chaves de segurança que criptografam as informações sigilosas armazenadas em uma

25 memória eletrônica.