Brazilian Journal of Development

Mudança da Identidade Funcional da PMPR: Proposta de um modelo mais moderno e seguro

PMPR Functional Identity Change: Proposal for a more modern and secure model

DOI:10.34117/bjdv5n9-125

Recebimento dos originais: 20/08/2019
Aceitação para publicação: 18/09/2019

Welby Pereira Sales,
Especialista em Direito Penal
Casa Militar da Governadoria
Endereço:Praça Nossa Senhora Salete, s/n, 5° andar
Email:welbycasamilitar@gmail.com

RESUMO

Este artigo tem como objetivo presentar as novas tecnologias para a adoção de uma nova identidade para a Polícia Militar do Paraná. A pesquisa consiste no uso de cartões de cloreto de polivinila (PVC) – Cartões Inteligentes, moldados à realidade da administração da PMPR. Nesse contexto, objetiva-se apresentar um novo modelo, um *layout* diferenciado, integrado aos sistemas existentes, e consoante o que há de mais moderno na utilização de cartões, produzindo-se assim um sistema mais eficiente de identificação. O modelo atualmente utilizado se revela muito frágil, suscetível aos desgastes do tempo e à possiblidade de falsificações, além de ser usado unicamente para identificação, uma vez que sua criação data de 1974. Apesar de a nova identidade ter um custo um pouco superior, está ajustada à perspectiva contemporânea de novos parâmetros de identificação, sendo sua segurança consideravelmente superior, aliando-se ainda à maior durabilidade e aos fatores estéticos. Desse modo, a proposta de identidade funcional poderá ser usada como autenticadora com o uso de certificação digital e em todos os setores da PMPR.

Palavras-chave:Identidade Funcional. Inovação Tecnológica. Segurança. Certificação Digital.

ABSTRACT

This article aims to present the new technologies for the adoption of a new identity for the Paraná Military Police. The research consists of the use of polyvinyl chloride (PVC) - Smart Cards, molded to the reality of PMPR management. In this context, the objective is to present a new model, a differentiated layout, integrated with existing systems, and depending on what is most modern in the use of cards, thus producing a more efficient identification system. The model currently used is very fragile, susceptible to time wasting and the possibility of forgery, and is only used for identification, since its creation dates from 1974. Although the new identity has a slightly higher cost, it is adjusted to the contemporary perspective of new identification parameters, and its security is considerably superior, coupled with greater durability and

aesthetic factors. This way, the functional identity proposal can be used as an authenticator with the use of digital certification and in all PMPR sectors.

Keywords: Functional Identity. Tecnologic innovation. Safety. Digital certification.

1 INTRODUÇÃO

Vivemos na era digital, em que os recursos o avanço da Tecnologia a Informação vêm sendo o centro da revolução científica no mundo em expansão, trocando-se as sociedades que antes eram industriais para as sociedades da informação. Dentre as áreas nessa nova sociedade temos destaques na microeletrônica, informática, tecnologia da comunicação e tecnologia de imagem. A partir do século 20, a tecnologia da informação se transformou em um sistema digital de alta velocidade, baseada em rede integrada e inteligente rapidamente. Pierre Lévy (1999, p. 92) afirma que "a perspectiva da digitalização geral das informações provavelmente tornará o ciberespaço o principal canal de comunicação e de suporte de memória da humanidade, a partir do início do próximo século", e foi exatamente o que aconteceu. Em nossos dias o papel cada vez mais vai perdendo espaço para o "virtual", termo amplo que se refere a elementos de computação virtual, em vez da base real (física); todos os dados encontram-se em dispositivos magnéticos, instrumentos esses capazes de aperfeiçoar a administração e otimizar recursos.

Não há que se discutir que hoje o momento é de transformação, nossas rotinas e costumes foram totalmente modificados, e os padrões rotineiros de vida foram impulsionados com novos conceitos e atitudes repletas de informações. A Internet é uma das causadoras dessas modificações, em que palavras novas foram incorporadas em nosso dicionário e sem dúvida todos sofreram essa nova roupagem digital.

Os padrões da publicidade e a maneira de se negociar e interagir foram completamente transformados pela era digital, alterando radicalmente os paradigmas da comunicação mundial, rompendo velhos modelos de negócio, escrita, interação, fazendo assim uma passagem do modelo físico para o virtual. A maioria da população tem acesso ao computador, tornando-se a informática fundamental para a nossa cultura. Cultura essa baseada na digitalização, que se "[...] conecta no centro de um mesmo tecido eletrônico o cinema, o rádio, a televisão, o jornalismo, a edição, a música, as telecomunicações e a informática" (LÉVY,1999, p. 92).

O imediatismo do mundo virtual, que é a combinação de rapidez e a agilidade unidas ao dinamismo e as situações do mundo atual, transforma a Internet no meio de comunicação mais eficiente da atualidade. A digitalização conseguiu alcançar o objetivo de levar conhecimento a inúmeros lugares antes nunca mensurados ou conhecidos. A consequência

dessa rapidez é prejudicial, uma vez que temos que desenvolver um senso crítico, filtrando o grande número de informações que nos é despejado todos os dias, através de mídia social e eletrônica, e, ao mesmo tempo em que hoje nós estamos mais atualizados que antigamente, temos uma gama maior de conhecimento do que gerações passadas.

> A Tecnologia da Informação começou a modificar radicalmente o trabalho – sua localização, rapidez, qualidade e outras características-chave [...]. Os computadores apressam o ritmo de muitas atividades de trabalho e, ao mesmo tempo, reduzem drasticamente a necessidade de mão-de-obra (DAVENPORT, 1994, p. 92).

A Polícia Militar do Paraná (PMPR) vem acompanhando esse processo de "virtualização", com o desenvolvimento contínuo de sistemas em todos os setores necessários e imprescindíveis à economia de meios e recursos, agilidade no processo e uma busca rápida e eficaz com relatórios fidedignos à realidade, como exemplo tem-se a intranet[4] da instituição, com um rol de sistemas desenvolvidos pela Diretoria de Desenvolvimento Tecnológico e Qualidade, possibilitando ao público interno inserção, edição e consulta de dados *online*.

O tema proposto pelo presente artigo é a inovação da Identificação Funcional do Policial Militar do Paraná, que advém do Decreto Estadual n.º 6.147, de 11 de novembro 1974, o qual já não corresponde mais aos anseios e nem se adequa à nova realidade de tecnologia.

Do mesmo modo, se alinha ao Programa Nacional de Qualidade de Vida para Profissionais de Segurança Pública (Pró-Vida), em seu art. 8.º, inciso II, alínea "e" da Lei Federal n.º 13.675, de 11 de junho de 2018, que disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública e institui o institui o Sistema Único de Segurança Pública (Susp).

Com os meios disponíveis hoje, qualquer pessoa pode copiar e imprimir o modelo atual de identificação funcional, que não possui uma proteção efetiva, além do papel que pode ser confeccionado por meios não oficiais, estando, portanto, suscetível à falsificação.

2 CRIAÇÃO DA IDENTIDADE FUNCIONAL NA PMPR

O Decreto Estadual n.º 6.147, de 11 de novembro de 1974, institui efetivamente a Cédula de Identidade Funcional Policial Militar do Paraná. No ato normativo está definida a cor, forma, tamanho, impressões e marca d´agua que devem conter, assim como tipo de fontes e escritas. O art. 7.º da norma estabelece que a aquisição seja sem ônus para os Soldados de 1.ª

[4] Página acessada internamente na corporação: http:// http://intranet.pmpr.parana/.

Brazilian Journal of Development

Classe e para os alunos da Escola de Formação de Oficiais do 1.º ano, sendo que para os demais integrantes, assim como uma segunda via, deverá ser recolhido valor, não discriminado, ao Tesouro do Estado.

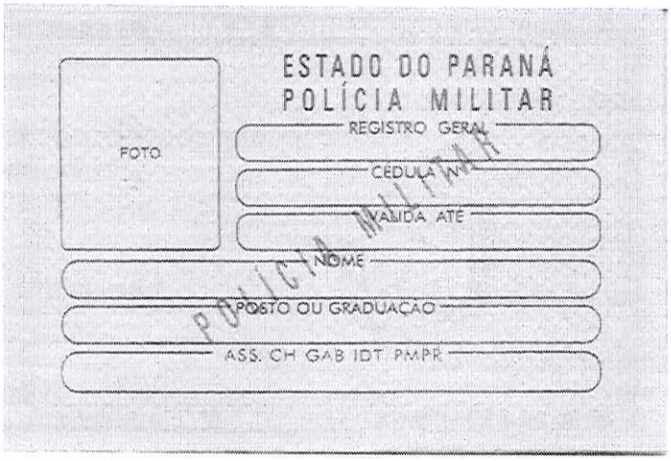

FIGURA 1 – Cédula Atual de Identidade Funcional.

O modelo atual somente atende às necessidades de identificação funcional, como já dito, podendo ser facilmente falsificado, além de estar suscetível às ações do tempo, desgastes e perda de impressão.

O Governo Federal já começou a trocar os antigos RG (Registro-Geral), que são confeccionados pelos Estados da Federação, por um novo modelo chamado RIC (Registro de Identidade Civil), um número de cadastro único em todo o território nacional[5]. Essa preocupação vem ao encontro das novas tecnologias e com o principal foco na segurança, uma vez que hoje um cidadão pode ter vários Registros Gerais, em vários estados brasileiros. Estão sendo inseridos neste novo "RG" dados como CPF (Cadastro de Pessoas Físicas), Título de Eleitor, PIS (Programa de Integração Social), Pasep (Programa de Formação do Patrimônio do Servidor Público), Carteira de Trabalho e Carteira Nacional de Habilitação, além de dados referentes à pessoa e se a mesma é doadora de órgãos ou não.

Com relação ao RIC, cabe salientar que o projeto foi suspenso sem data para retorno. Foi substituído pelo DNI (Documento Nacional de Identificação), projeto piloto em

[5] Projeto do Governo Federal: http://www.brasil.gov.br/cidadania-e-justica/2010/12/conheca-o-novo-registro-de-identidade-civil-ric
[6] Projudi: http://www.jurisway.org.br/v2/dhall.asp?id_dh=9722
[7] Certificado digital é um arquivo de computador que contém um conjunto de informações em chave pública ou privada criando o conceito de "Identidade digital".

05/05/2018. Em 11 de fevereiro de 2019, o então secretário de Governo Digital do Ministério da Economia, Luis Felipe Salin Monteiro, anunciou o uso do CPF como número geral, sendo um primeiro passo para implantação geral do DNI no Brasil. Além disso, ao contrário da proposta de lei aprovada, o governo pretende manter alguns documentos como Passaporte, Certificado de Alistamento Militar, Carteira do Bolsa Família e Carteira de Motorista (inclusive aumentando a validade deste último), em razão de leis que proíbem que esses documentos sejam unificados em um outro.

É certo que a mudança poderá causar antagonismo, seguida da desconfiança do incerto e duvidoso, sendo que, numa fase inicial, como retrata Almeida e Coelho:

> [...] O comportamento e o desempenho poderão ser desconfiados numa fase inicial, sendo, no entanto no domínio da aprendizagem técnica que se justifica o sucesso imediato do processo de mudança pelos bons resultados que em geral são alcançados. A resistência à mudança que as novas tecnologias introduzem encontra terreno fértil na ameaça percepcionada à segurança no emprego [...] Por outro lado, personalidades avessas ao risco resistirão pela desconfiança quanto ao desconhecido e também pela mudança estrutural de magnitude global que a reforma integral de crenças e valores implica. O desconhecimento técnico funciona em geral como fator chave que sustenta a resistência [...] (ALMEIDA; COELHO, 2000, p. 3).

Vários setores públicos e privados trocaram suas identificações acompanhando a nova tecnologia, uma delas foi a OAB (Ordem dos Advogados do Brasil) que passou por este processo, seguindo as tendências de digitalização de processos fomentados pela informatização dos Tribunais de Justiça. Hoje, os processos judiciais especiais cíveis, no Paraná, são 100% digitais[6] e acessados através de Certificação Digital[7] por advogados, juízes e promotores.

No ano em que o Decreto instituiu a Identidade Funcional da PMPR, não se estimava que esse aparato poderia ser usado de outra forma, senão como identificação pessoal. A partir dos novos, com O processo de irradiação da informatização, as tendências se alavancaram para uma nova era, a qual denominamos de "Era Digital".

3 CARTÕES INTELIGENTES *(SMART CARDS)*

Cartão inteligente *(smart card)* é um cartão de plástico de forma retangular, semelhante a um cartão de crédito, que pode encapsular um chip para armazenar e processar dados no padrão ISO (*International Organization for Standardization*). Neste encapsulamento, pode ainda existir um circuito eletrônico integrado com ou sem a presença de uma targeta magnética.

O *smart card* (SC) pode ser composto por um ou mais chips de circuitos integrados, sendo que seu formato facilita o transporte e a utilização. Com capacidade de armazenamento temporário ou permanente de dados, o conteúdo está disponível para leitura externa ou interna e tem a capacidade de executar operações de processamento, objetivando identificar e responder às informações a ele solicitadas externamente e armazenar certificados de chaves públicas e privadas.

Algumas das características do cartão inteligente é um nível mais elevado de segurança, impresso sobre a sua superfície uma assinatura pessoal com impressão de imagem holográfica. O cartão inteligente é composto por três partes: um substrato de plástico (com ou sem tarja magnética), uma superfície de contato e um circuito integrado.

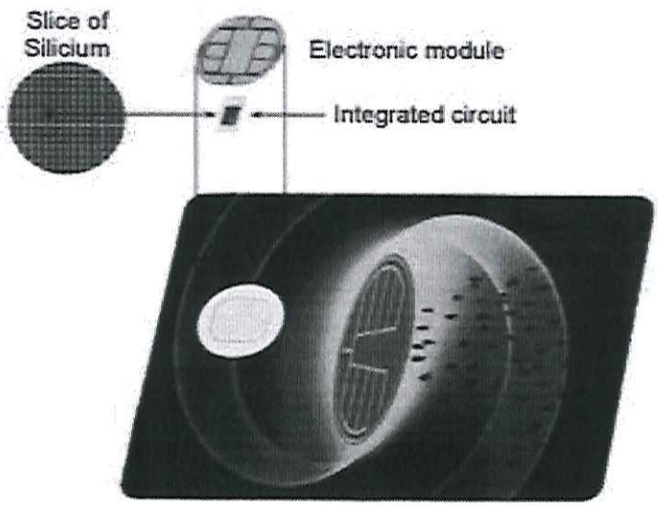

Figura 2 – Estrutura *Smart Card*

Os objetivos do cartão inteligente são basicamente a autenticação de usuários e o armazenamento de chaves de informações e operações criptográficas em um ambiente confiável.

Nesse contexto, questiona-se o porquê do uso do *smart card* como base para esta transformação do "papel para o plástico"? Dentre as justificativas, pode-se relatar que o *smart card* oferece segurança de dados (só autorizados), integridade dos dados (transações não completadas), criptografia e resistência a fraudes. Além disso, detém capacidade de processamento com cálculos flutuantes e coprocessador, capacidade de armazenamento, baixo consumo de energia, elevada vida útil, confiabilidade, resistência e grande volume de produção.

3.1 TIPOS DE CARTÕES INTELIGENTES

Todo o cartão inteligente pode ser dividido pelo processo de troca com o leitor:

a) Cartão de contato com interface de cartão inteligente com ISO 7816;
b) Cartão de contato com USB de interface;
c) Cartão sem contato (RFID[8] cartão inteligente).

Sobre a funcionalidade do cartão, pode ser dividido em:

a) Cartão de memória (contendo uma certa quantidade de dados e do mecanismo de controle de acesso);
b) Cartão inteligente (contendo um microprocessador e a capacidade de gerir os dados no mapa).

3.1.1 Cartão de Contato Interface ISO 7816

Os cartões de contato inteligentes têm uma zona de contato contendo alguns terminais pequenos de contato. Quando o cartão é inserido no leitor o chip entra em contato com conectores eléctricos, e um leitor pode ler e/ou escrever a informação do chip.

Os SC são regidos pelas normas da ISO / IEC 7816 e ISO / IEC 7810. A norma ISO / IEC 7816 também regula os protocolos de comunicação e alguns aspectos dos dados que são usados para outros cartões inteligentes. O cartão de contato não contém uma bateria, sendo a energia fornecida pelos leitores.

3.1.2 Cartão de Contato com interface USB

Normalmente, um cartão com chip padrão ISO 7816 é combinado com o USB - Reader[9] em um pacote pequeno. Isso faz com que a utilização de cartões inteligentes para autenticação de computador seja muito mais conveniente, como, por exemplo, o *eToken*.

[8] A tecnologia de RFID (*radio frequency identification* – identificação por radiofrequência) nada mais é do que um termo genérico para as tecnologias que utilizam a frequência de rádio para captura de dados.
[9] Leitor USB (*Universal Serial Bus*) – Conexão de periféricos ao computador

Figura 3 – eToken.

3.1.3 Cartões inteligentes sem contato

Esses são os cartões que se comunicam com o leitor de cartão por meio da tecnologia RFID. Tal modalidade requer a aproximação acentuada do cartão ao leitor, para que se procedam às operações necessárias. Esses cartões são muitas vezes utilizados em áreas em que é necessária a rápida execução e operação, por exemplo, em transportes públicos.

O padrão para cartões inteligentes sem contato é o ISO / IEC 14443, raramente ISO / IEC 15693.

A tecnologia do cartão inteligente sem contato é a RFID, sendo que, igualmente aos cartões com contato, eles não possuem baterias. Um indutor é incorporado para armazenar a energia de RF[10] para o pulso inicial, que é então retificado e usado para operar a placa.

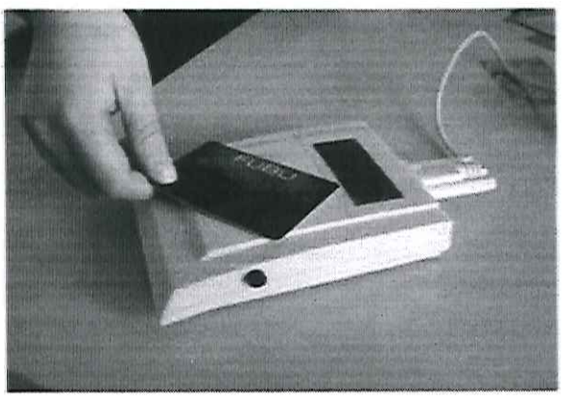

Figura 4 – Leitor RFID

[10] Rádio Frequência.

Os Cartões Inteligentes com a característica memória podem conter dados de acesso fixo. Normalmente, este cartão é usado para pagamentos de transporte, telefones públicos, ingressos, recreação e cartões de fidelização.

Como um mecanismo para restringir o acesso, o cartão pode funcionar com autenticação mútua, usando o padrão de criptografia simétrica, algoritmos simples (uma única conta, uma senha, um número único) ou mais complexos, como a criptografia DES/AES[11] .

Já os Cartões Inteligentes, cuja principal característica não seja o armazenamento de dados fixos, contém um microprocessador e algoritmos que são capazes de fazer *upload* de seu trabalho. Possíveis ações desses cartões incluem ações integradas para autenticação, protocolos de comunicações complexas e o registro de casos de acesso.

Além da criptografia simétrica (AES, DES) conhecidas, pode existir também a assimétrica (RSA)[12], que são algoritmos de infraestrutura de chave pública (ICP)[13] e hardware gerador de números aleatórios, com proteção melhorada contra-ataques físicos.

3.2 LEITORES DE CARTÕES INTELIGENTES

Apesar do nome, o dispositivo para leitura de cartões inteligentes pode ler e escrever somente se for permitida essa possibilidade e direitos de acesso. Os leitores *smart card* podem se conectar ao computador de três maneiras: porta serial, ranhura PCMCIA e *serial bus USB.*

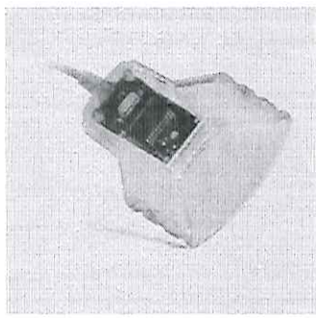

Figura 5 - Leitor Ranhura PCMCIA.

[11] DES (*Data Encryption Standard*) é um tipo de cifra em bloco, ou seja, um algoritmo que toma uma *string* de tamanho fixo de um texto plano e a transforma através de uma série de complicadas operações, em um texto cifrado de mesmo tamanho. AES (*Advanced Encryption Standard*) – Chave criptográfica mais avançada.

[12] RSA (um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto MIT (fundadores da atual empresa RSA Data Security, Inc.), Ronald Rivest, Adi Shamir e Leonard Adleman) envolve um par de chaves, uma chave pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo.

[13] ICP (*public-key infrastructure*) Infraestrutura de Chave Pública, sistema que utiliza mecanismos de segurança baseados na criptografia de chaves públicas.

Alguns fabricantes produzem outros tipos de dispositivos de hardware que fazem a integração com o contato do SC, elas são propriedades de memória, capacidade e processamento. Os *hardwares* mais populares – chaves – usam a porta USB. As chaves USB são atraentes para algumas organizações, porque USB é o padrão de comunicação com o Computador, sem a necessidade de um leitor especifico. Os dispositivos de leitor de cartão inteligente podem ser integrados no teclado, conforme apresentamos abaixo.

Figura 6 – Leitor *Smart Card* Embutido no TecladO.

3.3 PRINCIPIOS BÁSICOS DE FUNCIONAMENTO

O princípio de funcionamento dos Cartões Inteligentes é simples, através de determinado sistema instalado ou apenas aberto em um computador, requisita as informações da leitora e quando inserido o cartão com a autenticação do usuário se obtém a resposta. Esse método funciona através do APDUs (*Application Protocol Data Units*) Protocolo de Aplicação de Unidade de Dados, que é a unidade de comunicação entre um leitor de cartão inteligente e um cartão inteligente.

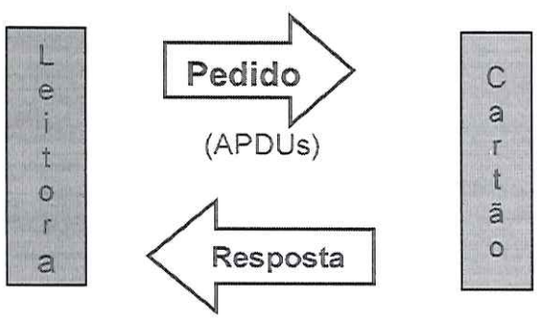

Figura 7 – Funcionamento *Smart Card*

4 INFRAESTRUTURA DE CHAVE PÚBLICA E CERTIFICAÇÃO DIGITAL

É um conjunto de serviços para o gerenciamento de chaves e certificados digitais, usuários, programas e sistemas.

A infraestrutura de chaves públicas é usada para a identificação do EDI partes (usuários, programas, sistemas), garantir a confidencialidade das informações, realizar o controle sobre a integridade da informação e determinar a origem das informações.

4.1 COMPONENTES DA ICP

a) Centro de Certificação (*Certificate Authority*) parte de uma chave pública que emite um certificado para confirmar os direitos dos usuários ou solicitantes de sistemas. Ele cria um certificado e assina com a chave privada. Devido à sua função para criar um certificado, o centro de certificação é uma parte central da ICP;

b) Repositório de Certificado (*Certificate Store*): armazenamento de certificados válidos e lista de revogação (CRLs). As aplicações verificam a adequação do certificado e o nível de acesso deles, verificando a amostra contida no repositório;

c) Chaves de recuperação do servidor (*Recovery Key Server*): o servidor executa as chaves de recuperação automática se o serviço está instalado;

d) Aplicações para leitura de ICP: são aplicações que podem utilizar o ICP para a segurança. Gerencia certificados ICP digitais e chaves usadas para criptografar as informações contidas nos servidores da web, usando *e-mail*, troca de mensagens, quando da visualização de páginas web e transferência de dados. Alguns aplicativos podem utilizar inicialmente uma ICP, outros requerem alterações na programação;

e) Centro de Registro (*Registration Authority*): módulo responsável pelo registro do usuário e as solicitações de certificados;

f) Servidor de Segurança (*Security Server*): um servidor que fornece controle de acesso do usuário, certificados digitais e as relações de confiança entre o ICP. O *Security Server* gerencia centralmente todos os usuários, certificados, títulos com um centro de certificação, relatórios e verifica a lista de certificados revogados.

Brazilian Journal of Development

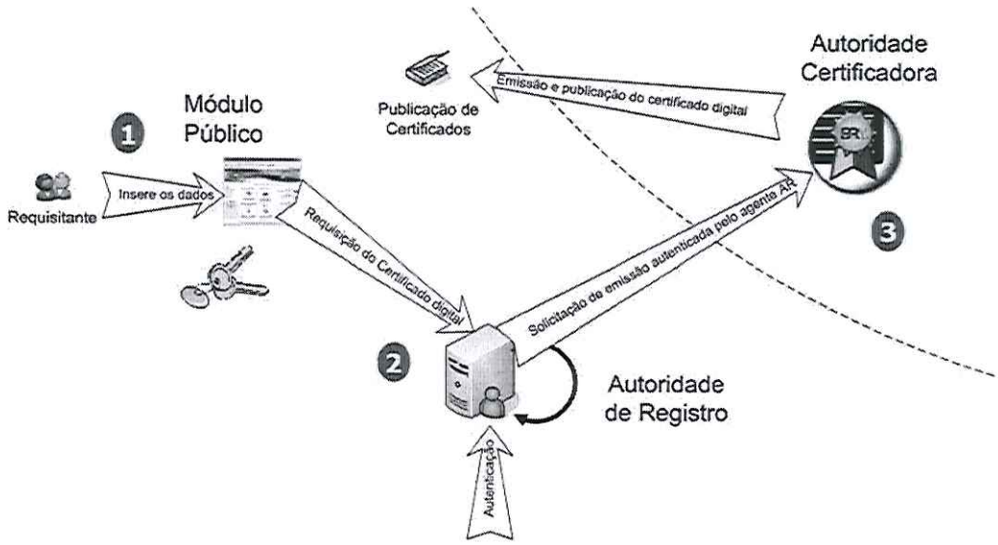

Figura 8 – Infraestrutura de Chave Pública (ICP).

4.2 FUNÇÕES DE ICP

a) Registro (inscrição): o processo de coleta de informações sobre o usuário e verificação de sua autenticidade, que é então usada quando o usuário faz de acordo com as regras de segurança;

b) Emissão de um certificado: uma vez que a CA[14] assinou o certificado, é emitido para o requerente e/ou enviados para o armazenamento de certificados. É inserida CA sobre a validade dos certificados, exigindo, portanto, a renovação periódica do certificado;

c) Cancelamento do certificado (Certificados Revogados). O certificado pode ser invalidado antes da expiração por uma variedade de razões, como exemplo:

- o usuário deixou a empresa;

- mudança de matrícula;

- chave privada foi comprometida. Nestas circunstâncias, o certificado da CA é nulo, registrando o número de série no CRL[15];

d) Chave de recuperação (*Recovery Key*). Função adicional ICP permite que você recupere dados ou mensagens em caso de perda da chave;

e) Controle do Ciclo de Vida (*Lifecycle Management*): apoio contínuo dos certificados ICP, incluindo atualização, recuperação e arquivamento de chaves.

[14] CA (Certificate Authority) – Autoridade Certificadora
[15] CRL (Certificate Revocation List) – Lista de Certificados revogados

Estas funções são realizadas periodicamente e não em resposta a solicitações específicas uma vez que o gerenciamento de chaves automatizado é a função mais importante para a ICP e o gerenciamento de chaves, sendo que, se realizado manualmente, pode limitar a escalabilidade do ICP.

4.3 CERTIFICADOS DIGITAIS

Certificado Digital é a estrutura de dados usada para associar um determinado módulo com uma chave pública específica. Os certificados digitais são usados para autenticar usuários, aplicativos, serviços e controle de acesso (autorização). Os certificados digitais são emitidos e distribuídos pela CA em consulta a uma Lista de Revogação de Certificados (CRL); os usuários podem verificar esta lista, antes de conceder acesso, de acordo com o certificado.

Assinatura digital é o método de utilização de criptografia de chave pública para garantir a integridade de dados. O bloco de dados é criptografado e descodificado pelo destinatário; o remetente identifica e confirma a segurança dos dados. Por exemplo, o documento "comprimido" e criptografado com a chave privada do remetente e anexado ao documento (na verdade, isso significa fazer a "impressão digital" deste documento) quando chega ao seu destino o receptor utiliza a chave pública para decifrar a mensagem recebida que é então comparada com a chave privada e, se ambas não corresponderem, isso significa que o documento foi alterado ou corrompido durante a transmissão.

Existem dois tipos básicos de criptografia utilizados: chave pública e uma chave privada (simétrica). A pública é disponível gratuitamente e a chave privada é conhecida apenas por um usuário específico, aplicativo ou serviço que mantenha este sistema. Este par de chaves está ligado de tal forma que a chave privada cifrada apenas pode ser decifrada pela chave pública, e vice-versa.

O algoritmo RSA foi o primeiro sistema de criptografia com uma chave pública, em homenagem a seus inventores: Ronald Rivest, Adi Shamir e Leonard Adleman.

A maior empresa brasileira de tecnologia com foco exclusivo em soluções que utilizam certificação digital é a Certisign. Fundada em 1996, foi a primeira autoridade certificadora a entrar em operação no Brasil e a terceira no mundo.

A Medida Provisória nº 2.200-2, de 24 de agosto de 2001, define as regras para a criação da ICP-Brasil, bem como a utilização de certificados digitais no Brasil, aspectos legais e necessários para uma entidade se tornar uma AC intermediária e, assim, emitir certificados digitais para outras entidades garantindo autenticidade, integridade, não repúdio e validade

jurídica de trâmites eletrônicos por essas entidades realizados. A Lei n.º 11.419, de 19 de dezembro de 2006, fundamenta os processos judiciais eletrônicos no Brasil, que recentemente foi alterada pela Lei 13.793, de 3 de janeiro de 2019.

5 OS CARTÕES INTELIGENTES E AS ICP

Há muitas vantagens em se combinar o uso de *smart cards* em uma ICP. Em contrapartida, verificam-se algumas desvantagens, mas que são superadas pelos benefícios decorrentes do uso dos cartões.

Algumas vantagens que podem ser citadas são:

a) Assinatura, criptografia, decriptografia e geração de chaves assimétricas realizadas pelo coprocessador criptográfico do cartão;
b) Garantia de confidencialidade da chave privada, uma vez que esta nunca deixa o cartão;
c) Portabilidade e armazenamento seguro de chaves e certificados;
d) Múltiplas aplicações em um mesmo cartão;
e) Duplo fator de segurança, "o que você tem" mais "o que você sabe";
f) Múltiplas formas de identificação em um único dispositivo: chip, foto, código de barras, tarja magnética, assinatura, além de identificação textual do nome indivíduo e/ou empresa;
g) Fácil aceitação da tecnologia por parte das pessoas, uma vez que estas já estão acostumadas a portar diversos tipos de cartões.

Algumas desvantagens também podem ser citadas:

a) Aumento dos custos de desenvolvimento, manutenção e gerenciamento da ICP;
b) Necessita de leitores especiais ainda não disponíveis em todos os computadores;
c) Em caso de perda, roubo ou danificação do cartão, documentos encriptados com a chave pública podem nunca mais serem recuperados (se a ICP não implementar um esquema de recuperação de chaves).

Assim como os *smart cards* intensificam a infraestrutura de chave pública, a ICP também intensifica o uso dos *smart cards*, pois pode utilizar a totalidade das suas capacidades, usufruindo ao máximo dos benefícios que esta tecnologia pode oferecer (FIGUEIREDO; RIBEIRO, 2004. p. 6).

6 A NOVA IDENTIDADE FUNCIONAL DA PMPR

A seguir se apresenta uma proposta de *layout* para a nova Identidade Funcional do Policial Militar do Paraná. Ressalte-se que, como etapas preliminares são necessárias as seguintes providências:

- mudança do Decreto Estadual n.º 6.147, de 11 de novembro de 1974;

- estudo por parte da Diretoria de Desenvolvimento Tecnológico e Qualidade da PMPR para integrar os sistemas existentes à nova tecnologia de identificação;

- escolha do tipo de criptografia se a PMPR será uma Autoridade Certificadora (interno) ou a certificação será Certsign (maior custo), ou ainda ambos, ou por interno e externo;

- escolha do tipo de cartão, capacidade de armazenamento, entre outros detalhes técnicos.

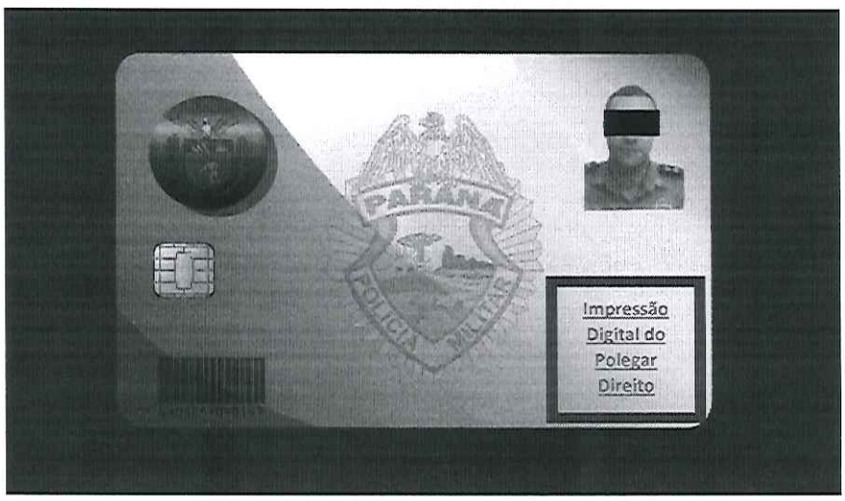

Figura 15 – Modelo Nova identidade Funcional.

Os seguintes campos serão digitados da nova Identidade Funcional: posto/Graduação, nome, registro geral, número do porte de arma e o tipo sanguíneo do titular. A identificação datiloscópica deve ser digitada e impressa juntamente com esses outros dados.

Dependendo do tipo de CHIP escolhido e conforme seu tamanho de armazenamento, poderá conter também as seguintes informações: ficha completa do Policial Militar, identificação datiloscópica, prontuário médico, chaves de Criptografia para a assinatura digital e outros dados que se julguem necessários.

Discutir a importância da inserção da impressão digital do dedo polegar da mão direita para a identificação inequívoca do servidor. Este é um dos maiores erros encontrados nos

modelos atualmente existentes que já utilizam os cartões com chip na identificação funcional: a ausência da impressão digital visível de fácil confronto pelos peritos técnicos em papiloscopia. Questão imprescindível para que essa nova Identidade Funcional seja realmente utilizada para identificação: a impressão digital do polegar direito deve ser impressa juntamente com os outros dados, tendo em vista que somente desta forma poderá ser realmente utilizada em qualquer situação para identificação inequívoca do servidor (tanto em concursos públicos, quanto em vestibulares, ou ainda em eventuais problemas nos leitores do SC em qualquer local ou mesmo por falta deste no momento da identificação).

6.1 UTILIDADES DA NOVA CARTEIRA FUNCIONAL NA PMPR

6.1.1 Logística

Na Logística da PMPR, a nova Identidade Funcional será uma autenticadora de materiais e equipamentos que o policial militar terá em seu poder. Não serão mais necessárias cautelas em papel, como sistema de controle de material. Ao chegar ao setor de patrimônio de material bélico de sua Unidade, o PM precisará apenas inserir seu cartão (ID Funcional) em um leitor e digitar sua senha no teclado para que seja confirmado e autenticada a cautela de determinado material.

Quanto ao fardamento, poderá ser inserido em alguma parte da farda um código de barras, que será automaticamente entregue ao policial já autenticado no sistema, tendo assim o registro que aquela farda pertence àquele policial militar e o próprio romaneio poderá estar inserido na carteira. Em um futuro próximo, até ao assumir a direção, o policial poderá se autenticar à viatura comprovando que o mesmo estava na direção.

O controle de entrada e saída dos aquartelamentos será mais eficaz, uma vez que poderá ser utilizado o método de autenticação em catracas para a entrada do policial militar. Enfim, podem ser vislumbradas inúmeras utilizações desse método de autenticação, inserção e busca de dados na área da logística.

6.1.2 Pessoal

Na área pessoal da Corporação, dentro do CHIP será possível o cadastro completo do policial militar, incluindo sua identificação datiloscópica. Ao se apresentar de férias ou em outra Unidade Policial Militar, bastará o policial se dirigir ao setor de recursos humanos da unidade e por meio de um leitor de cartão autenticará sua presença e automaticamente será inserido no sistema, podendo até já constar no Boletim Interno da Unidade, sem a necessidade

de se digitar novamente seu comparecimento. Os requerimentos e solicitações poderão ser feitos todos digitalmente sem a necessidade de papel, ou seja, a autenticação será a base para todos os atos.

Com a certificação digital, através dos leitores de cartões, os comandantes poderão ter autenticidade em seus atos publicados digitalmente, enviar documentos certificados e que não restarão dúvidas quanto à autenticidade de nenhum documento. Essa nova tecnologia poderá se aliar ao Certificado Digital (*e*-Token USB) atualmente utilizado para assinaturas de e-protocolos em vigência no Estado do Paraná.

6.1.3 Saúde

Na Saúde, além de perícias autenticadas pelos pacientes, também será possível a inserção do prontuário médico dentro do CHIP na carteira funcional, e com relação ao Prontuário Médico inserido no s*mart card.*

Sobre o tema, em uma pesquisa realizada por dois professores do Departamento de Ciência da Computação/Grupo de Pesquisa em Informática Médica e Telemedicina da Universidade do Extremo Sul Catarinense (UNESC), constatou-se que é possível armazenar 62 anos de registros de prontuário médico, considerando 2 atendimentos mensais em um *smart card* de 1 *mbytes*. (JARACESKI; NICOLEIT, 2008).

6.1.4 Outros setores da PMPR

Quando se trata em autenticação de documentação, a nova identidade junto com a certificação digital irá influenciar todos os setores da PMPR, sendo que os custos poderão ser absorvidos pela própria instituição, que poderá criar sua certificação, ou mesmo contratar empresa especializada do ramo, de acordo com processos formais de compras públicas, segundo a legislação vigente.

7 EQUIPAMENTOS NECESSÁRIOS PARA A IMPLANTAÇÃO DA NOVA IDENTIDADE FUNCIONAL

Para que seja implementado o processo da nova identidade será necessária a aquisição de equipamentos capazes de realizar a leitura e gravação de dados, bem como a tecnologia em programação necessária para integrar o que existe hoje nos sistemas da PMPR e à identidade proposta.

7.1 CARTÕES PVC E CARTÕES INTELIGENTES

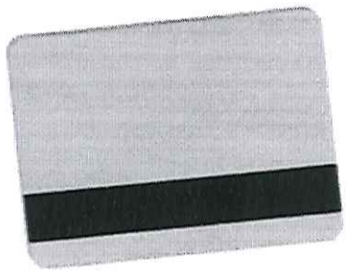

Figura 9 – Cartão PVC com Tarja Magnética

O cartão representado na figura 09 é um cartão em branco em PVC pronto para a impressão. Esta seria uma solução para uma escolha sem o chip *smart card*, em que a autenticação aconteceria por tarja magnética em leitores magnéticos, cujo custo médio de R$ 0,60 por unidade (para compras médias de até 500 cartões), valor que pode ser diminuído conforme o volume de aquisições.[16]

Figura 10 – Cartão PVC com chip *Smart Card*

O Cartão representado na figura 10 é o objeto da presente proposta. Seu material também é PVC e o custo médio é de R$2,00, sendo sua cotação feita em US$ (dólar americano). Dependendo da capacidade de gravação pode ser aumentado o custo unitário, pois necessitaria de maior capacidade do CHIP que começa em 1K (K Byte).

[16] https://www.stockprint.com.br/catalog/product/view/id/106/s/cartao-pvc-tarja-magnetica/.

7.2 IMPRESSORA PARA CARTÕES EM PVC

Modelo de impressora ideal para a impressão dos cartões:

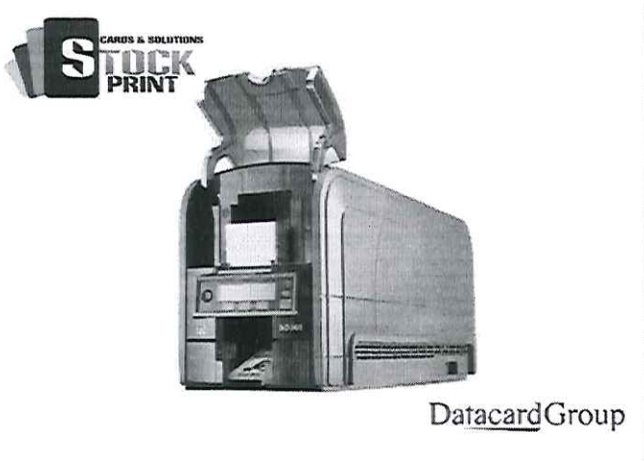

Figura 11 - Impressora Datacard SD260

A impressora acima tem resolução de impressão de 300 dpi, 256 combinações por painel, velocidade de impressão, *Full-color* de até 200 cartões por hora e monocromático até 850 cartões por hora.

A impressora alimenta automaticamente 100 cartões (0.76mm) e em um compartimento de saída de 25 cartões, na alimentação manual um cartão por vez (0.76mm) em um compartimento de Saída de 5 cartões. O custo médio é de R$ 4.400,00.[17]

7.3 LEITORES E GRAVADORES DE CARTÕES

Para que ocorra o processo de integração entre a identidade em cartão e os sistemas da PMPR será necessário um equipamento, de preferência em unidade USB, responsável pela autenticação ou busca de dados como os apresentados abaixo:

[17]https://www.stockprint.com.br/catalog/product/view/id/230/s/impressora-datacard-sd-260/category/116/

Figura 12 - Leitor de Cartão Magnético USB

Na figura acima (12) tem-se um leitor somente para cartões com tarjas magnéticas, cujo custo está em torno de R$168,00.[18]

Figura 13 – Leitor de Código de Barras

Acima mais um modelo que poderá ser usado para leitura da identidade e materiais pertencentes a PMPR, ao custo médio de R$99,00.[19]

Utilizado para a leitura e gravação do certificado digital do tipo A3 e-CPF, e-CNPJ, NF-e, Conectividade Social®, em Cartões *Smart Card.*

[18] http://www.mvnet.com.br/prod,IDLoja,12266,Amp,True,IDProduto,2317424,magneticos-leitores-de-cartao-leitor-de-cartao-magnetico-minimag-duo
[19] http://www.leitor-optico.com/