white paper

O padrão aberto

CIPURSE

Mamede Lima–Marques

2019.WP.0425

Instituto MODAL

Brasília, DF
Setembro de 2019 – Versão 1.1

Identificação

Título: White Paper: O padrão aberto CIPURSE
iD: 2019.WP.0425
Autor: Mamede Lima–Marques
Projeto: Difusão do Conhecimento
Data: Setembro de 2019
Local: Brasília, DF
Versão: 1.1

Revisões

Data	Versão	Alterações / Comentário	Revisor
2018.04.25	1.0	Criação do documento.	Mamede Lima–Marques
2019.09.23	1.1	Revisão geral. Inclusão de resumo e considerações finais. Atualização do layout.	Bruno Souza

Ficha catalográfica

O padrão aberto CIPURSE / Mamede Lima–Marques; Bruno Carvalho Castro Souza. – : Brasília, DF: Instituto Modal, Setembro de 2019.
20 p. : il. (algumas color.) : 21,0x29,7 cm

White Paper – Instituto Modal de Ciência, Tecnologia e Inovação, Setembro de 2019. Versão final.

1. microprocessadores 2. CIPURSE 3. padrão aberto I. Título

CDD 001.42

Autores

Mamede Lima–Marques (pesquisador líder)

Bruno Carvalho Castro Souza

white paper

Sumário

Resumo

O CIPURSE é um padrão aberto de segurança mantido pela OSPT ALLIANCE e que está disponível para qualquer empresa. A definição conjunta das especificações dos produtos e os procedimentos independentes de testes asseguram que os produtos baseados CIPURSE são compatíveis entre si. Os dados dos usuários são transmitidos usando tecnologias sem contato e podem, portanto, ser carregados não só para cartões inteligentes sem contato, mas também para *smartphones* ou relógios inteligentes – ou qualquer dispositivo com a tecnologia NFC. Independentemente de se usar um cartão inteligente ou um dispositivo móvel, os dados do usuário estão efetivamente protegidos. O padrão de segurança é baseado na criptografia AES (Padrão de Criptografia Avançada), sendo criptografados tanto para armazenamento no cartão ou dispositivo móvel quanto para envio ou recepção de informações do leitor.

Palavras-chave: microprocessadores. CIPURSE. padrão aberto.

Abstract

CIPURSE is an open security standard maintained by OSPT ALLIANCE and available to any company. The joint definition of product specifications and independent testing procedures ensure that CIPURSE based products are compatible with each other. User data is transmitted using contactless technologies and can therefore be uploaded not only to contactless smart cards, but also to smartphones or smart watches – or any device with NFC technology. Regardless of whether using a smart card or mobile device, user data is effectively protected. The security standard is based on Advanced Encryption Standard (AES) encryption and is encrypted for either storage on the card or mobile device or for sending and receiving inforation to the reader.

Keywords: microprocessors. CIPURSE. open standard.

Introdução

Desde a sua criação em 2010 até hoje, o padrão CIPURSE evoluiu da especificação para a realidade com um número significativo de implantações de membros globais. Hoje, CIPURSE é considerado aberto, não proprietário, e o padrão para serviços de mobilidade. Possui fator de forma integralmente agnóstica, suporta diferentes tipos de mídias, incluindo sem-contato, *wearables* e móveis. São soluções desenvolvidas com ambas metodologias: elementos seguros no dispositivo e *Host Card Emulation* (HCE). Como o CIPURSE é independente tanto do *hardware* quanto do provedor de *hardware*, ele pode perfeitamente, com segurança e custo acessível, efetivamente ser integrado a qualquer solução existente do MaaS. Isso permite aos provedores ir além de fornecedores de fonte única e capitalizar em vários projetos de parceiros que podem melhor apoiar serviços digitais e serem mais flexíveis para o que o mercado futuro exige.

No Brasil, o CIPURSE está sendo utilizado também para verificação de identificação de pessoas, como proposto para a nova Carteira Nacional de Habilitação (CNH) com base em cartão inteligente. O projeto usa CIPURSE para proteger dados pessoais do motorista – como uma fotografia e impressões digitais – para que possa ser usado como ID e verificação. A tecnologia capacita policiais ler os dados no cartão via um aplicativo NFC de smartphone, em qualquer localização, e rapidamente coordenar com outras agências em todos os sistemas relacionados. Além disso, os bancos podem usar impressão digital como autenticação para conceder acesso a serviços e crédito, e serviços locais de soluções de transporte público também podem ser implementados em o cartão. A nova CNH será lançada para o 66 milhões de motoristas no Brasil, levando o País a se afastar do modelo tradicional baseado em papel pela primeira vez.

1 Breve histórico

A proliferação de cartões de plástico começou nos EUA no início dos anos 50. O baixo preço do material sintético PVC tornou possível a produção de cartões de plástico robustos e duráveis, que eram muito mais adequados para o uso diário do que os cartões de papel e demais cartões anteriormente utilizados, que não resistiam adequadamente a tensões mecânicas e efeitos climáticos.

O primeiro cartão de pagamento totalmente plástico para uso geral foi emitido pelo *Diners Club* em 1950. Destinava-se a uma classe exclusiva de indivíduos e, por-

tanto, também servia como símbolo de status, permitindo que o titular pagasse com o seu bom nome "em vez de dinheiro". Inicialmente, apenas os restaurantes e hotéis mais selecionados aceitavam esses cartões, levando-os a ficarem conhecidos como cartões de viagem e entretenimento (RANKL; EFFING, 2010).

Os cartões inteligentes chegaram no final da década de 60. O primeiro modelo foi publicado em 1968 por dois inventores alemães, Dethloff e Grotrupp, que desenvolveram o conceito de um cartão plástico contendo um microchip (SHELFER; PROCACCINO, 7 2002). Em 1970, os japoneses seguiram a liderança dos alemães e registraram uma patente para a sua própria versão do cartão inteligente (ATTOH-OKINE; SHEN, 1995). Moreno (1976) obteve uma patente em 1974 sobre o conceito de um cartão inteligente semelhante ao que é utilizado hoje e também patentes sobre como produzir cartões inteligentes de forma eficiente (HUSEMANN, 2001).

No final de 1970, a Motorola desenvolveu o primeiro microcontrolador de *chip* único seguro, que foi utilizado pelo sistema bancário francês para melhorar a segurança nas transações. No entanto, foi desde 1990 que o uso do cartão inteligente tornou-se significativo, com o crescimento exponencial da Internet e a crescente sofisticação das tecnologias de comunicação móvel (BLYTHE, 2004).

A tecnologia de cartão inteligente começou a entrar no mercado e tentativas estão sendo feitas para usá-lo em muitas áreas da atividade comercial. Attoh-Okine e Shen (1995) lembram que a Alemanha vem usando o cartão inteligente para cuidados de saúde desde 1992; na França, foi adotado para serviços postais, telefônicos e telégrafo em 1982. De fato, o cartão inteligente (sem contato ou de outra forma) é usado em muitos setores: saúde, banco, governo, recursos humanos e, claro, transporte.

O cartão é usado para armazenar identificação, biometria, fotos, impressões digitais, dados médicos, resultados de DNA, afiliação religiosa, dados bancários, tarifas de transporte e outros dados individuais. Atualmente usa-se cartões inteligentes em um sentido muito mais amplo. Eles se tornaram facilitadores para uma ampla gama de soluções (usos), serviços e sistemas de comércio eletrônico.

Os principais recursos que os tornam tão atraentes para os desenvolvedores de aplicativos são:

a) seu tamanho pequeno, viabilizando sua portabilidade;

b) sua capacidade de armazenar dados de forma segura; e

c) executar programas.

Nos últimos anos, o avanço da tecnologia digital criou a necessidade de dotar os documentos e impressos de recursos gráficos e elementos anti-falsificação, capazes de garantir a segurança dos mesmos.

Até o início dos anos 90, o foco principal da indústria havia sido no desenvolvimento e na melhoria de *software*, especialmente no sistema operacional embutido na arquitetura dos cartões, na sua integração com os computadores e nos padrões de segurança e criptografia (PRACA; BARRAL, 2001). Os avanços demandaram aumento significativo no poder de processamento e na capacidade de memória, enquanto os demais elementos mantiveram-se relativamente estáveis.

A partir dos anos 90, os cartões passaram a permitir multiaplicações, ou seja, mais de uma aplicação sendo executada em um único cartão. Isso foi possível devido ao desenvolvimento da tecnologias de *multithreading*, que viabilizaram seu uso como objeto de real computação, com características de segurança para um grande número de domínios (SAUVERON, 2009).

2 Cartões Inteligentes

Cartões inteligentes estão disponíveis em diversos formatos, incluindo plásticos (PVC e policarbonato sendo os mais comuns no Brasil), *tokens* USB, relógios inteligentes e módulos de identificação, que seguem o padrão definido pela Norma ISO 7816, que determina:

a) suas característica físicas (ISO 7816-1);

b) a localização e dimensão dos contatos (ISO 7816-2);

c) os sinais elétricos e os protocolos de transmissão de baixo nível (ISO 7816-3); e

d) a comunicação de alto nível (ISO 7816-4).

A norma também especifica outros aspectos (partes 5 a 15).

Em termos gerais, os cartões inteligentes podem ser divididos em dois grupos (European Railway Agency, 2012):

a) *Cartões de contato*, que requerem algum tipo de contato físico entre o cartão e o leitor, tecnologia ainda muito comum no Brasil (como os atuais cartões de crédito com chip, que precisam ser inseridos nas leitoras); e

b) *Cartões sem contato, ou* contactless, que possuem circuitos integrados que processam e armazenam informação, comunicando-se remotamente por ondas de rádio. Esses cartões podem ser usados como documentos de identificação e se comunicam de maneira inteligente com os dispositivos de leitura, inclusive *smartphones* e dispositivos com tecnologia NFC. Esses cartões tem sua comunicação definida pela Norma ISO 14443.

A Figura 1 mostra um exemplo de cartão inteligente típico.

Figura 1 – Modelo de Cartão em Policarbonato

Fonte: CFM (2017)

2.1 Vantagens e desvantagens dos tipos de cartões

A opção por adotar cartões com ou sem *chip* depende fundamentalmente da finalidade do cartão. É possível listar vantagens e desvantagens para cada situação.

A principal vantagem do cartão sem *chip* é o custo menor do que os cartões com *chip*. Além disso, a gestão do ciclo de vida do cartão é mais simples, uma vez que não é possível fazer atualizações. Seu tempo útil, no entanto, é limitado pela eventual necessidade de alterar informações, o que requer a emissão de novo cartão.

As desvantagens dos cartões sem *chip* incluem:

a) não é possível incluir certificações digitais no cartão devido ao volume de informações, que ultrapassa as possibilidades tecnológicas atuais de armazenamento no suporte. Consequentemente, a verificação da autenticidade

eletrônica requer o uso de uma base de dados acessível pelo encarregado (pessoa física) por verificar a informação do portador;

b) por não ser possível atualizá-los, é necessária a emissão mais frequente de novos cartões – na prática, cada vez que houver atualização de qualquer das informações incorporadas ao cartão será necessária nova emissão;

c) a falta de *chip* inviabiliza transações eletrônicas seguras, por não permitir a identificação inequívoca do portador.

Os cartões com *chip* ampliam as funcionalidades do cartão sem *chip*, tendo como principais vantagens:

a) permitem armazenar informações adicionais, como certificados digitais, biometria, histórico e outros dados;

b) é possível atualizar eletronicamente as informações armazenadas no *chip*, permitindo o aumento da vida útil do cartão;

c) permitem ao portador participar de transações eletrônicas por meio da autenticação da identidade através de biometria – tecnologia *Match on Card*) e outras técnicas de segurança;

d) viabiliza a adoção de medidas de segurança mais sofisticadas, embutidas no *chip*, criando melhor proteção contra falsificações;

e) possibilita o uso de chaves criptográficas e certificados, tanto do cartão quanto do portador.

Uma outra vantagem dos cartões com *chip* é a possibilidade de integrar serviços de terceiros, o que traz benefícios adicionais ao portador.

Como desvantagens, os cartões com *chip* possuem um processo de gerenciamento mais sofisticado, tornando-os mais caros. Além disso, os desenvolvedores de aplicativos precisam realizar um planejamento detalhado sobre os serviços que podem vir a ser oferecidos, incluindo questões de segurança.

Outra característica dos cartões com *chip* é a necessidade de manter a informação armazenada sincronizada com a base de dados do emissor, o que é possível por meio do uso de equipamentos adequados e processos bem definidos. Idealmente, a cada uso as informações armazenadas no cartão deveriam ser validadas (e, quando for o caso, atualizadas) pelo emissor.

2.1.1 Cartões de contato

Cartões de contato fazem uso de contatos físicos do cartão com os terminais de leitura, que provêm energia para ativar o seu *chip*.

Outra característica dos cartões de contato traduz-se na confiabilidade da própria conexão, menos suscetível a interferências entre o cartão e o terminal. Isso, no entanto, não se traduz necessariamente em aumento da segurança, uma vez que existem dispositivos que podem ser inseridos entre o cartão e o terminal de leitura sem que o portador se dê conta.

Uma vez que os cartões de contato possuem mais tempo de uso e maior base implantada em relação aos cartões sem contato, há mais fabricantes, o que tende a reduzir os custos e aumentar a competitividade.

Por outro lado, a principal desvantagem do cartão de contato é a necessidade de inseri-lo fisicamente em um dispositivo de leitura, o que toma algum tempo e pode ser inconveniente para o portador.

Além disso, por haver uma ação física de inserção e retirada do cartão nos dispositivos de leitura, há um desgaste nos contatos do cartão, o que faz com que a vida útil desse tipo de cartão seja, em média, cinco anos.

Informações da indústria de *chips* dão conta que haverá a desativação das linhas de produção de *chips* de contato em um período de sete a dez anos (Silicon Trust, 2017).

2.1.2 Cartões sem contato

A principal vantagem do cartão sem contato é a conveniência e a facilidade de uso pelo portador, uma vez que não há necessidade da inserção em terminais de leitura – basta que o cartão se aproxime do dispositivo de leitura para que a comunicação seja estabelecida. Consequentemente, esse tipo de cartão tem vida útil superior aos de contato – alguns fabricantes estimam que seus cartões tenham durabilidade de até dez anos.

Outro aspecto a ser considerado é o tamanho da base instalada: a indústria vem gradativamente aumentando a participação do *chip* sem contato, que hoje já representa quase 40% do mercado, reforçado pela chegada de leitores incorporados a *smartphones* comuns.

3 Tecnologia de *Hardware* Embarcada

Uma das principais características que distingue os tipos de cartões inteligentes é o *chip* de Circuito Integrado (CI) presente nesse cartão, como mostra a Figura 1.

Sua CPU pode comportar microcontroladores, que utilizam conjuntos de instruções para acesso e escrita em memória, manipulações de registradores, modos de endereçamento e operações de I/O. Alguns fabricantes estenderam o conjunto básico de instruções particularmente desenvolvidas para uso em CPU dos cartões inteligentes.

Algumas das características dos cartões sem contato são:

a) *Interface física:* O canal de I/O em um cartão inteligente é um canal serial unidirecional. Ou seja, só se pode passar um bit por vez, e os dados podem unir apenas em um sentido por vez. A capacidade de transmissão do cartão inteligente é geralmente bem superior àquela suportada pela leitora, isto é, a velocidade de transmissão dos dados será determinada pela capacidade de transmissão/recepção de dados da leitora. O protocolo de comunicação entre o cartão inteligente e a leitora é baseado em uma relação de mestre (leitora) e escravo (cartão inteligente). A leitora (ou um *host* conectado a ela) envia solicitações de dados para o cartão inteligente e espera por uma resposta. O cartão inteligente nunca envia dados sem a solicitação do *host*.

b) *Energia:* É suprida da leitora para o cartão. A maioria dos cartões inteligentes opera entre 3,5V e 5V.

c) *I/O:* Duas interfaces são utilizadas para carregar tráfego I/O entre a leitora e o cartão. Uma linha, a linha de I/O, carrega os bits de dados. Esta linha pode assumir dois estados, 1 ou 0. A segunda linha, o *clock*, indica quando a linha de I/O deve ser amostrada para determinação do bit de dados.

d) *Sincronização:* Os protocolos típicos que são utilizados para comunicação entre a leitora e o cartão são os protocolos *half-duplex*. Ou seja, os dados são tanto escritos na linha de I/O pela leitora e lidos pelo cartão quanto escritos pelo cartão e lidos pela leitora. Dessa maneira, cada final da linha de comunicação determina qual dispositivo está em um estado de leitura ou escrita. Como esses protocolos não são muito sofisticados, é possível que ocorram erros que deixem um ou ambos os terminais do canal em um estado ambíguo. Quando isso ocorre, é responsabilidade da leitora reiniciar toda a sequência do protocolo. Isso pode ser realizado com o pino iniciar.

e) *Memória:* Existem basicamente quatro tipos de memória amplamente utilizadas em um cartão inteligente: ROM (*Read-Only Memory*), EEPROM (*Electrically Erasable Programmable Read-Only Memory*), NVM (*Nonvolatile Memory*) e RAM (*Random Access Memory*).

Cartões sem contato não necessitam de nenhum contato físico entre o cartão e o terminal, para transferência de energia ou de dados. Existem três principais tecnologias em uso atualmente: Tecnologia 125kHz, ISO/IEC 14443 e ISO/IEC 15693.

Vários de padrões internacionais definem especificações para implementação de cartão inteligente direcionadas para a indústria e para desenvolvimento de aplicações com o foco nestes dispositivos. Cabe salientar que, para as definições do arcabouço tecnológico utilizado para o desenvolvimento dos requisitos técnicos definidos neste documento, foram provenientes dos estudos técnicos realizados nestes padrões. A ISO 7816 é um padrão internacional relacionado com cartões de identificação eletrônicos, especialmente cartões inteligentes microprocessados.

4 Tecnologia de *Software* Embarcada

Em contraste com todos os outros tipos de cartões, as propriedades específicas de um cartão inteligente são determinadas pelo microcontrolador implantado no cartão. A função principal do corpo do cartão de plástico é manter o microcontrolador. Claro, outros componentes podem estar presentes além do microcontrolador, mas eles não são essenciais para as funções reais do cartão inteligente. Uma compreensão básica de certos aspectos da tecnologia da informação é necessária para entender as características desses pequenos computadores e os mecanismos de tecnologia da informação baseados neles.

Dentre os aspectos essenciais, merece destaque o sistema operacional (SO), que é definido como "os programas de um sistema de computador digital que, juntamente com as propriedades do sistema de computação, forma a base de modos de operações possíveis do sistema de computação pessoal, particularmente no controle e monitoração da execução do programa". Um SO provê uma interface entre o *hardware* do computador e o *software* de aplicação utilizado no momento, de maneira que torna desnecessário que o *software* de aplicação acesse diretamente o *hardware*, o que provê à aplicação a característica de portabilidade.

Os sistemas operacionais para cartões inteligentes são desenvolvidos para operar como uma interface serial bidirecional para o terminal.

Nos anos 90, de acordo com Rankl e Effing (2010), havia poucos sistemas operacionais de cartões inteligente. A capacidade de memória dos cartões era pequena. A situação usual não era a presença de um sistema operacional como uma coleção bem estruturada de rotinas na memória ROM, que era utilizada quando necessário por uma aplicação particular quando o cartão estava completo. A estrutura desses sistemas era muito monolítica, e somente poderia ser modificada a altos custos. As próximas gerações começaram a ser construídas como um sistema operacional em camadas, e, nos dias de hoje, os sistemas operacionais possuem, além dessa estrutura em camadas, inumeráveis refinamentos. A base para a padronização dos sistemas operacionais para cartões inteligente é formada pela família ISO/IEC 7816, além de especificações *Universal Integrated Circuit Card* UICC (ETSI TS 102 221).

4.1 CIPURSE™

CIPURSE[1] é um padrão aberto não-proprietário com segurança forte (sistema AES de criptografia), utilizado principalmente para sistemas de cobrança de tarifa de transporte. Usa tecnologias de cartões inteligentes e medidas de segurança adicionais.

A *OSPT Alliance* (OSPT) definiu o padrão CIPURSE para fornecer uma plataforma aberta para proteger as novas e legadas operações de cobrança de tarifa de trânsito (CLARY, 2010). Dentre os sistemas que utilizam o endereço de segurança aberto CIPURSE incluem-se serviços de transporte público, coleta de tarifas de transporte e transações relacionadas a micropagamentos e identificação.

O padrão de segurança CIPURSE foi estabelecido pela OSPT para atender às necessidades das autoridades de transporte e para os sistemas de cobrança de tarifas automáticas baseadas em tecnologias de cartões inteligentes e medidas de segurança avançadas.

Os produtos desenvolvidos em conformidades com o padrão CIPURSE são concebidos para:

a) incluírem tecnologia de segurança avançada;

b) suportarem múltiplas aplicações;

c) ajudarem a garantir a compatibilidade com sistemas legados; e

[1] CIPURSE™ é marca registrada da *Open Standard for Public Transportation Alliance (OSPT ou OSPT Alliance)*

d) estarem disponíveis em uma variedade tamanhos, formatos e outras características físicas de *hardware* (*Form Factor*).

O padrão aberto e não-proprietário CIPURSE é pretendido para:

a) promover a neutralidade de fornecedor;

b) habilitar a interoperabilidade de sistemas de diferentes fornecedores;

c) reduzir o risco de adotar uma nova tecnologia; e

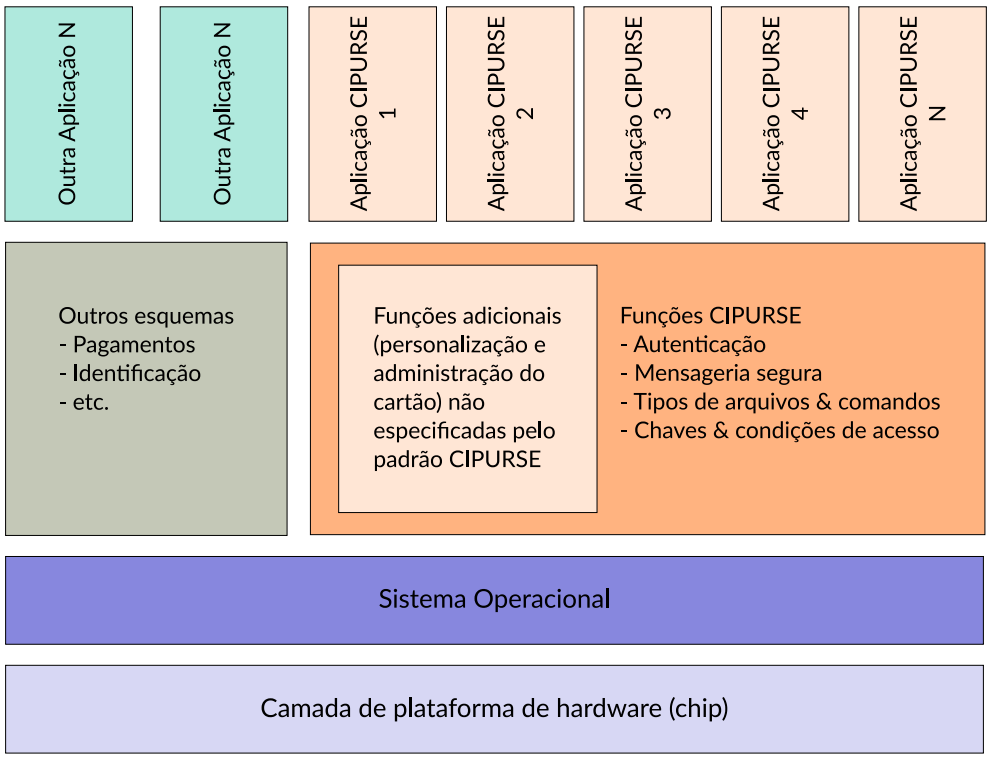
d) melhorar a receptividade do mercado.

Todos esses fatores destinam-se a reduzir os custos de operação e a aumentar a flexibilidade para operadores de sistemas de transporte.

A transição para uma plataforma de padrão aberto cria oportunidades para adotar padrões também abertos para partes importantes do sistema de coleta de tarifas, incluindo gerenciamento de dados, interface de mídia e segurança, o que torna os sistemas mais econômicos, seguros, flexíveis, escaláveis e extensíveis.

O padrão CIPURSE permite a utilização simultânea de outras aplicações, incluindo para soluções de identificação. A Figura 2 apresenta o esquema genérico de integração do *hardware* com uma solução CIPURSE.

Figura 2 – Integração CIPURSE – visão em camadas



4.2 Especificações

Em dezembro de 2010, a OSPT Alliance apresentou o primeiro rascunho do padrão CIPURSE. Ele empregava padrões abertos existentes e comprovados, incluindo o padrão do cartão inteligente ISO/IEC 7816, bem como o Padrão de Criptografia Avançada de 128 bits (AES 128) e a camada de protocolo ISO/IEC 14443. Projetado para implementações de silício de baixo custo, o conceito de segurança CIPURSE usava um esquema de autenticação que é resistente à maioria dos ataques eletrônicos de hoje.

Seus mecanismos de segurança incluem um protocolo criptográfico exclusivo para implementações rápidas e eficientes com proteção robusta e inerente contra ataques de análise de energia diferencial (DPA) e Diferencial de falhas. Como o protocolo é inerentemente resistente a esses tipos de ataques e não requer medidas de *hardware* dedicadas, ele deve ser mais seguro e menos oneroso. Pretende-se proteger contra a falsificação, a clonagem, a espionagem, os ataques do homem no meio e outras ameaças à segurança.

O padrão CIPURSE também:

a) define um protocolo de mensagens seguro;

b) identifica quatro tipos de arquivos mínimos obrigatórios e um comando mínimo obrigatório para acessar esses arquivos;

c) especifica chaves de criptografia e condições de acesso;

d) define a camada de radiofrequência (RF) como agnóstica;

e) inclui personalização e gerenciamento do ciclo de vida, bem como a funcionalidade do sistema para fornecer interoperabilidade e rápida adoção;

f) fornece um conceito de segurança e diretrizes.

Os provedores de tecnologia da OSPT Alliance podem adicionar funcionalidades fora do núcleo comum (que é definido no padrão) para diferenciar seus produtos, desde que não prejudiquem a interoperabilidade das funções principais (OSPT Alliance, 2017).

A versão 2.0 foi introduzida no final de 2012. Projetado como uma arquitetura modular em camadas com perfis específicos da aplicação, o padrão CIPURSE v2 aberto e não-proprietário compreende um conjunto único e consistente de especificações para todas as funções de gerenciamento de segurança, personalização, administração e vida útil necessárias para criar uma ampla gama de aplicativos interoperáveis.

Três perfis específicos da aplicação – subconjuntos do padrão CIPURSE v2 adaptados para diferentes casos de uso – foram definidos, os quais devem ser seguidos pelos fornecedores quando criam produtos visando essas aplicações:

a) CIPURSE T – Aproveita os novos mecanismos de transação incluídos na especificação para suportar o uso de transações baseadas em microprocessadores de alto nível usando cartões inteligentes, telefones celulares e dispositivos similares para aplicações de tarifa de trânsito mais complexas, como ingressos mensais ou anuais, bilhetes multi-sistema e programas de fidelidade.

b) CIPURSE S – Suporta bilhetes que podem ser recarregados para um número específico de passeios ou bilhetes semanais e é essencialmente equivalente e substitui a corrente CIPURSE 1.1 especificação.

c) CIPURSE L – Suporta aplicações que utilizam bilhetes de bilhete único ou de bilhete barato, descartáveis.

Os produtos com base em diferentes perfis podem ser adicionados aos sistemas de coleta de tarifas a qualquer momento e podem ser usados em paralelo para fornecer aos operadores de trânsito a maior flexibilidade, com uma variedade de opções de tarifa de trânsito. Como eles são derivados do mesmo conjunto de especificações, todos os perfis são interoperáveis, refletem o mesmo critério de *design* e têm a mesma aparência, permitindo que os desenvolvedores criem produtos de acordo com um conceito de família.

Com o seu *design* modular *"onion-layered"*, o padrão CIPURSE pode ser facilmente aprimorado com funcionalidades adicionais e novos perfis criados para abordar mudanças em tecnologia e negócios.

No início de 2013, a OSPT ALLIANCE apresentou as diretrizes do CIPURSE v2 *Mobile*, um conjunto abrangente de requisitos e casos de uso para o desenvolvimento e implantação de aplicativos móveis de tarifa de trânsito seguro do CIPURSE para *smartphones*, *tablets* e outros dispositivos inteligentes habilitados para comunicação de campo próximo (NFC). Essa nova derivação fornece tudo o que os desenvolvedores precisam para implementar e usar o padrão de segurança aberto CIPURSE v2 quando incorporado em um dispositivo móvel NFC, permitindo que os operadores aprimorem seus sistemas para suportar a emissão de bilhetes de cartões com esses novos formatos.

Considerações finais

Um padrão aberto simplifica as conexões entre os provedores de serviços, uma vez que a interoperabilidade acontece no nível do aplicativo ao invés de no nível da plataforma.

A participação diversificada e crescente da OSPT Alliance é um fator para tornar o CIPURSE um padrão aberto viável para emissão de bilhetes seguros e além. Os principais *players* de tecnologia do setor de transporte são membros ativos, participando de seus grupos de trabalho e impulsionando o padrão CIPURSE. Membros de todo o mundo e de todo o ecossistema de trânsito trazem diversas perspectivas de atuação, tendo como resultado maior robustez e flexibilidade em relação a outras soluções proprietárias disponíveis 0atualmente.

Como uma solução independente de hardware, o CIPURSE abre opções para aceitação de diferentes tipos de cartões e mídias. Os mercados locais podem impulsionar a evolução do programa, dependendo do valor trazido por cada proposição, assim como aceitar um caminho de múltiplas opções também é mais econômico.

A especificação CIPURSE oferece escalabilidade, o que facilita a introdução de novos produtos e evita modificações caras e complexas no sistema. Além disso, graças à compatibilidade os diferentes perfis, é possível introduzir serviços complementares praticamente sem nenhum custo extra.

A integração de soluções baseadas em CIPURSE é relativamente simples e rápida, uma vez que o padrão é aberto. Qualquer leitor de cartão compatível com ISO 14443 pode acomodar uma solução CIPURSE, atualizando para ISO 14443-4 e integrando uma funcionalidade CIPURSE *Secure Access Module* (SAM) ou CIPURSE ao SAM ou *firmware* existente.

Referências

ATTOH-OKINE, N. O.; SHEN, L. D. Security issues of emerging smart cards fare collection application in mass transit. In: *Pacific Rim TransTech Conference. Vehicle Navigation and Information Systems Conference Proceedings. 6th International VNIS. A Ride into the Future*. [S.l.: s.n.], 1995. ISBN 0-7803-2587-7. Citado na página 7.

BLYTHE, P. Improving public transport ticketing through smart cards. In: *Proceedings*

of the Institute of Civil Engineers: Municipal Engineer. [S.l.: s.n.], 2004. v. 157, p. 47–54. Citado na página 7.

CFM. *Certificação Digital Do Médico No Brasil*. [S.l.: s.n.], 2017. Citado na página 9.

CLARY, R. Ospt alliance debuts at cartes, announces open standard for fare collection. 2010. Disponível em: <https://www.secureidnews.com/news-item/*ospt-alliance-debuts-at-cartes-announces-open-standard-for-fare-collection/>. Citado na página 14.

European Railway Agency. *Report on the Use of Smartcards*. France, 2012. 72 p. Citado na página 8.

HUSEMANN, D. Standards in the smart card world. *Computer Networks*, v. 36, n. 4, p. 473–487, jul. 2001. ISSN 1389-1286. Citado na página 7.

MORENO, R. *Methods of Data Storage and Data Storage Systems*. [S.l.]: Google Patents, 1976. Citado na página 7.

OSPT Alliance. *An Open Standard For Next-Generation Transit Fare Collection*. 2017. Disponível em: <http://www.osptalliance.org/assets/pdf/ospt_transit_fare_collection.pdf>. Citado na página 16.

PRACA, D.; BARRAL, C. From smart cards to smart objects: The road to new smart technologies. *Computer networks*, v. 36, n. 4, p. 381–389, 2001. Citado na página 8.

RANKL, W.; EFFING, W. *Smart Card Handbook*. 4. ed. Germany: John Wiley & Sons, Ltd., 2010. ISBN 978-0-470-74367-6. Citado 2 vezes nas páginas 7 e 14.

SAUVERON, D. Multiapplication smart card: Towards an open smart card? *Information Security Technical Report*, v. 14, n. 2, p. 70–78, maio 2009. ISSN 13634127. Citado na página 8.

SHELFER, M.; PROCACCINO, J. D. Smart card evolution. *Communications of the ACM*, v. 7, n. 45, p. 83–88, 7 2002. Citado na página 7.

Silicon Trust. *Silicon Trust*. 2017. Disponível em: <https://silicontrust.wordpress.com/>. Citado na página 11.

Sobre o Instituto Modal

O Instituto Modal é uma *Instituição de Ciência e Tecnologia* (ICT), de natureza privada e sem fins lucrativos, que surgiu da convergência entre pesquisadores da área de informação e de tecnologia, empresários e profissionais com larga experiência no setor privado. Essa junção permitiu construir pontes entre fundamentação teórica e soluções reais, viabilizando a o uso da experiência científica às necessidades do mercado e da sociedade e encontrando soluções para problemas dos mais diversos tipos.

O Instituto Modal tem por objeto a realização de pesquisa básica e aplicada de caráter científico ou tecnológico e o desenvolvimento de novos produtos, serviços ou processos voltados prioritariamente ao objeto "informação", zelando pelo reconhecimento da importância da inovação no sistema produtivo nacional.

Para saber mais, visite institutomodal.org.br.

Contatos podem ser feitos pelo e-mail modal@modal.org.br.