Lucas Leite Cesar

Análise comparativa de uma transação de eletronic referral no POS, PDV, E-Commerce e Mobile

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para conclusão do curso de MBA em Tecnologia de Software.

São Paulo
2017

Lucas Leite Cesar

Análise comparativa de uma transação de eletronic referral no POS, PDV, E-Commerce e Mobile

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a conclusão do curso de MBA em Tecnologia de Software.

Área de Concentração: Tecnologia de Software

Orientador: Prof. Dr. Marco Antonio Torrez Rojas.

São Paulo
2017

Catalogação-na-publicação

Cesar, Lucas
Análise comparativa de uma transação de eletronic referral no POS, PDV, E-Commerce e Mobile / L. Cesar -- São Paulo, 2017.
98 p.

Monografia (MBA em Tecnologia de Software) - Escola Politécnica da Universidade de São Paulo. PECE – Programa de Educação Continuada em Engenharia.

1.CARTAO DE CREDITO I.Universidade de São Paulo. Escola Politécnica. PECE – Programa de Educação Continuada em Engenharia II.t.

DEDICATÓRIA

Dedico este trabalho a minha família, pois sem ela não estaria concluindo este trabalho, minha noiva minha grande motivadora, a minha irmã que sempre acreditou no meu esforço, meu orientador que sempre mostrou o melhor caminho para geração deste trabalho e aos meus guias tantos espirituais como carnais que me guiaram a conclusão deste trabalho.

AGRADECIMENTOS

À Universidade de São Paulo – USP que forneceu conhecimento teórico e técnico para o desenvolvimento da pesquisa realizada por este trabalho, que será levado ao longo da minha carreira.

À Escola Politécnica da Universidade de São Paulo – forneceu o espaço físico para o desenvolvimento e estudo focado.

Ao PECE – Programa de Educação Continuada em Engenharia que forneceu as aulas e o apoio dos professores e colaboradores para o desenvolvimento do aluno nas linhas de raciocínio de pesquisa e desenvolvimento.

Aos meus pais que zelaram e mantiveram a confiança na conclusão desta etapa da minha carreira e da minha vida.

A Minha irmã que sempre motivou e acreditou na capacidade técnica que pode ser utilizada e entregue a sociedade afim de sempre auxiliar o desenvolvimento continuo da tecnologia nos meios de pagamentos.

A Minha Noiva por sempre me motivar e me auxiliar no desenvolvimento do raciocínio lógico, incrementando as ideias e as contribuições de correções quando desviei do foco e toda a força espiritual que ela me transmitiu nos meses de trabalho de esforço e entrega

RESUMO

O mercado de pagamentos eletrônicos, especificamente o mercado de cartões brasileiros esta em uma constante evolução. Este trabalho visa apresentar uma explicação ampla de como é feita uma transação de cartão, envolvendo as empresas participantes em toda a cadeia em que ocorre a transação eletrônica. Para auxiliar no entendimento as necessidades de comunicação de dados e criptografia exigidos pelas empresas reguladoras do mercado, bem como pelo protocolo ISO 8583 responsável pela padronização da comunicação entre as empresas são apresentados. Os detalhes que envolvem os meios de captura mais populares do mercado brasileiro (TEF, *E-Commerce* e *Mobile*), bem como o processo de geração da transação e comunicação entre as partes envolvidas serão apresentados e discutidos. Com base nos conceitos apresentados com relação à meios de pagamento, a transação do tipo de *eletronic referral*, empregada para a prevenção de fraudes será apresentada para os principais meios de captura discutidos. Para a utilização deste tipo de transação existe a necessidade de adequação dos meios de captura, demandando um esforço técnico de implementação. Desta forma, este trabalho visa comparar os meios de captura apresentados, utilizando como critérios de avaliação o método de criptografia, tempo de resposta e a usabilidade do meio de captura. Assim, cada cenário apresentado e comparado é classificado de acordo com o impacto para o lojista ou para o portador do cartão, resultando em uma análise de esforço de implementação ou adequação deste tipo de transação para este meio de captura, com foco no contexto do mercado de cartões brasileiro.

ABSTRACT

The electronic market payments, specific, Brazilian market is evolution day by day. This study shows explanation of how a card transaction is made, involving the participating companies throughout the chain in which the electronic transaction occurs. To assist in understanding the data communication and encryption requirements required by the regulatory companies of the market, as well as by the protocol ISO 8583 responsible for the stander of communication between companies. The details that involve the most popular means of capture of the Brazilian market (TEF, E-Commerce and Mobile), as well as the process of generating the transaction and communication between the parties involved will be presented and discussed. Based on the concepts presented with respect to the means of payment, the transaction of the type of electronic referral used for the prevention of fraud will be presented for the main means of capture discussed. In order to use this type of transaction there is a need to adapt the capture means, requiring a technical implementation effort. This work compare the capture means presented, using as evaluation criteria the method of cryptography, response time and the usability of the capture medium. Each presented and compared scenario is classified according to the impact to the merchant or the cardholder, resulting in an analysis of the implementation effort or adequacy of this type of transaction for this capture medium, focusing on the context of the market Cards

LISTA DE ILUSTRAÇÕES

Pág.

Figura 1 – Infográfico trimestral de transações de credito e débito 12

Figura 2: Transações capturadas por tarja magnética e Chipcard Trimestral…...14

Figura 3 – Modelo Macro de comunicação entre as empresas.…….....17

Figura 4 – Especificação POS ICT250 .....…….....19

Figura 5 – Arquitetura de um POS.....…….....21

Figura 6 – Interação do portador com um cartão sem senha ... ……...……....22

Figura 7 – Interação do portador com um cartão com senha.....22

Figura 8 – Comunicação realizada entre *checkout* e pinpad 24

Figura 9 – Conexão entre a empresa A e B com *FailOver* 25

Figura 10 – Representação do X25 na cadeia de meios de pagamento.....26

Figura 11 – Representação da comunicação discada de um POS 27

Figura 12 – Representação da largura dos canais ADSL 28

Figura 13 – Representação da comunicação realizada de um POO 30

Figura 14 – Arquitetura do DES.....32

Figura 15 – Criptografia 3DES.....33

Figura 16 – Modelo de criptografia DUKPT 34

Figura 17 – Arquitetura ISO 8583.....42

Figura 18 – Exemplo de transação no modelo da ISO 8583.....43

Figura 19 – Envio de informações em uma transação *referral* no POS 49

Figura 20 – Trafego de uma transação de referral negada no POS.....47

Figura 21 – Exemplo do *checkout* de uma loja com a tecnologia de TEF.....54

Figura 22 – Estrutura do TEF para realização de transações 56

Figura 23 – Fases da transação de *referral* em um Pinpad.....56

Figura 24 – Estrutura mobile para realização de transações 60

Figura 25 – Protótipo de exemplificação do agente de conexão.....67

Figura 26 – Protótipo de exemplificação do *device* de captura.....68

Figura 27 – Ecossistema do E-Commerce brasileiro.....70

Figura 28 – Integração de pagamento de um e-commerce.....71

LISTA DE TABELAS

Pág.

Tabela 1: Significado de cada byte do MTI..... 37
Tabela 2: Variação do bit 1 da MTI..... 38
Tabela 3: Significado do bit 2 do MTI..... 43
Tabela 4: Significado do bit 3 do MTI..... 39
Tabela 5 – Significado do bit 4 do MTI..... 40
Tabela 6 – Exemplos do MTI..... 40
Tabela 7 – Definição da ISO 8583 com os principais bits utilizados..... 98
Tabela 8 –Variação do Processing Code..... 50
Tabela 9 – Sub elemento 1 do BIT 48 – Definição de consulta referral.....50
Tabela 10 – Sub elemento 8 do BIT 48 48
Tabela 11 - Sub elemento 9 do BIT 48..... 49
Tabela 12 – Pontuação pelo número de empresas para integração..... 79
Tabela 13 – Pontuação pelo tempo de resposta das transações..... 80
Tabela 14 – Pontuação pela facilidade de o portador inserir as informações..... 82
Tabela 15 – Pontuação pela possibilidade de *FailOver*..... 83
Tabela 16 – Pontuação pelo envio sem cifragem..... 84
Tabela 17 – Analise comparativa dos meios de captura..... 85

LISTA DE ABREVIATURAS E SIGLAS

POS	Point of Sale
TEF	Transferencia Eletronica de Fundos
EMV	Europay Mastercard and Visa
CPF	Cadastro de pessoa fisica
RG	Registro Geral
PCI	Payment Card Industry Security Standards
DES	Data Encryption Standard
SO	Sistema Operacional
GSM	Global System Mobile
ADSL	Assymmetric Digital Subscriber Line
MSISDN	Mobile Service ISDN Number
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity
GT	Global Title
DUKPT	Derived Unique Key Per Transaction
MTI	Message Type Indicator
TCP	Transmission Control Protocol
STAN	System Audit Transaction Number
NII	Network International Identifier
MAC	Message authentication code
XML	eXtensible Markup Language
Wi-FI	Wireless Fidelity

SUMÁRIO

Pág.

1. INTRODUÇÃO 12

1.1 MOTIVAÇÕES 13

1.2 OBJETIVO 15

1.3 JUSTIFICATIVA 15

1.4 ESTRUTURA DO TRABALHO 16

2. MEIO DE PAGAMENTOS BRASILEIROS 17

2.1 EXECUÇÃO DE VENDA 21

2.2 MEIOS DE COMUNICAÇÃO 23

2.1.1 Conexão Direta 23
2.1.2 Link dedicado 24
2.1.3 Conexão via X25 25
2.1.4 Conexão discada 27
2.1.5 Conexão ADSL 28
2.1.6 Sistema Global para comunicação móvel (GSM). 29

2.2 CRIPTOGRAFIA 31

2.3.1 DES 31
2.3.2 Triplo DES 33
2.3.3 DUKPT 33
2.3.4 RSA 34

2.4 APLICAÇÃO DO POS 35

3 NORMA ISO (FORMATO DE MENSAGENS DE TRANSAÇÕES FINANCEIRAS) 8583 37

3.1 TRANSAÇÃO DE *REFERRAL* EM UM POS 44

4. ANÁLISE COMPARATIVA DOS MEIOS DE CAPTURA 53

4.1 TRANSFERÊNCIA ELETRÔNICA DE FUNDOS (TEF) 53

4.1.1 Transação de eletronic referral no TEF 54

4.2 TRANSAÇÃO MOBILE 59

4.2.1 Transação de eletronic referral no mobile 60

4.3 TRANSAÇÃO DE *E-COMMERCE* 69

4.3.1 Transação de eletronic referral no E-Commerce 71

4.4 ANÁLISE COMPARATIVA DA TRANSAÇÃO DE *REFERRAL* 77

4.4.1 Integração do Lojista 77
4.4.2 Tempo de resposta 78
4.4.3 Experiência do Usuário 79
4.4.4 Fail Over de conexão 81
4.4.5 Cifragem da transação 82
4.4.6 Análise comparativa 84

5. CONSIDERAÇÕES FINAIS 87

5.1 CONTRIBUIÇÕES DO TRABALHO 88

5.2 TRABALHOS FUTUROS 88

REFERÊNCIAS 89

APÊNDICE 1 94

1. INTRODUÇÃO

O mercado de pagamentos eletrônicos, especificamente de cartões (crédito e débito) vem crescendo cada vez no Brasil, tornando-se um mercado competitivo para empresas financeiras ou facilitadoras de pagamento. O número de transações empregando cartões mantém-se em constante progressão ano após ano, como exemplificado pela Associação Brasileira das Empresas de Cartões de crédito e Serviço (ABECS) na Figura 1.

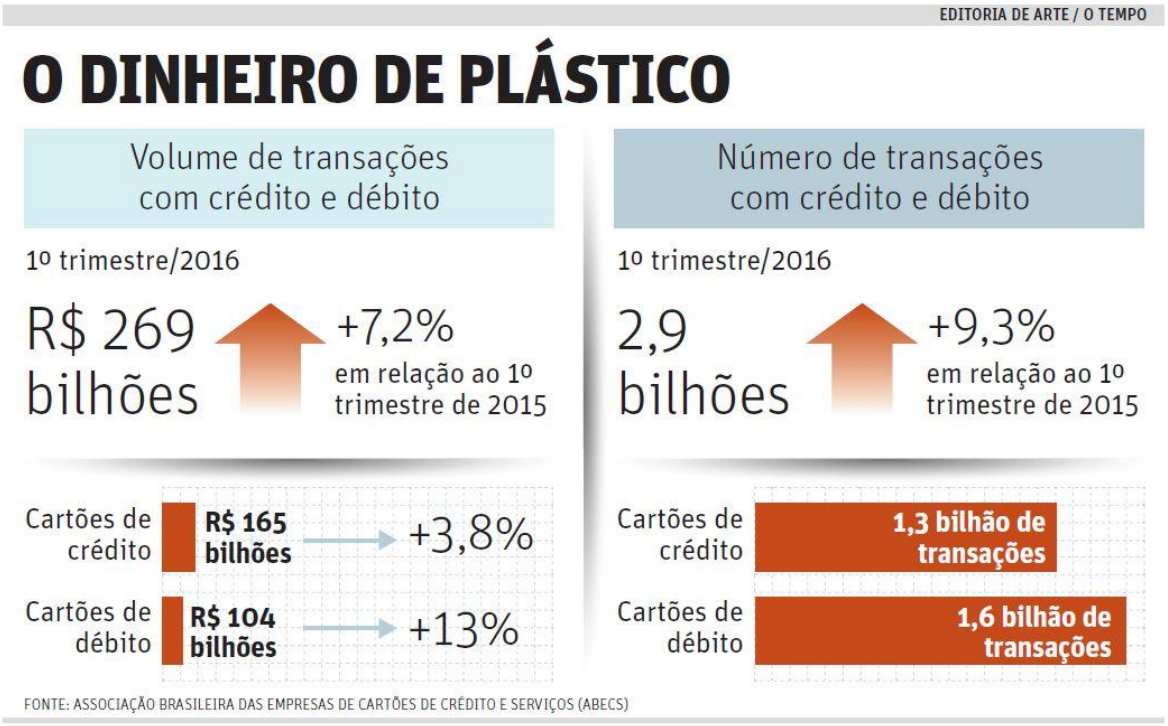


Figura 1: Infográfico trimestral de transações de credito e débit
Autor: ABECS, Maio, 2016

Por conta deste crescimento, o sistema de pagamentos brasileiro está adotando novas tecnologias e *softwares* para facilitar a implementação do dinheiro eletrônico (cartão de crédito e débito), tornando tais métodos acessíveis e populares. Segundo (ABECS, 2016) apenas no 1º trimestre de 2016 o volume de transações de cartões de crédito e débito atingiu a marca de R$ 269 bilhões, um valor 7,2% maior que no ano anterior. No mesmo período, o número total de transações foi de 2,9 bilhões, um aumento de 9,3% com relação ao ano anterior.

Esse constante crescimento de transações eletrônicas de pagamentos, teve por consequência à própria evolução em seu sistema, onde, por meio de pagamento utilizando um cartão plástico (cartão de crédito ou débito), o lojista possuía um novo

canal de pagamento para oferecer ao seu cliente. Onde o credenciamento (cadastro do lojista na facilitadora de pagamentos) é mais fácil e menos burocrático, com relação aos serviços de auto-credenciamento oferecido pelas empresas de pagamentos atualmente. A facilidade e velocidade na emissão de cartões de pagamentos (cartão de crédito ou débito) no Brasil aumentou a oferta, tornando-se um meio de pagamento popular (Emalta, 2016). O sistema de pagamento está adotando novas tecnologias e novos *softwares* com o objetivo de facilitar o uso de dinheiro eletrônico (cartão de crédito e débito), garantindo a própria atualização dos sistemas, aumentando as margens de lucro e fortalecendo sua capacidade de prevenir tentativas de fraudes.

Em 2009 uma adquirente brasileira chamada Redecard S.A, lançou um produto que visa trabalhar no âmbito de prevenção a fraudes e ao mesmo tempo uma transação rápida, o nome do produto chama-se *Eletronic Referral*; este produto possui como diferencial a solicitação de informações do portador do cartão no ato da compra, por exemplo (CPF/Data de nascimento/etc.), na qual ao responder essas questões o sistema executa uma dupla autenticação, garantindo maior segurança na transação (Cliente SA, Outubro, 2016).

1.1 Motivações

O Mercado brasileiro com o seu crescimento em relação ao número de transações atrai pessoas que tentam buscar brechas no sistema para tirar proveito próprio através de fraudes. Brechas tanto no tipo de transação *on-line* (*E-Commerce*/POS) como no modelo *off-line* (autorização posterior).

Levando a empresas a monitorar a movimentação de transações *e-commerce* e seus compradores a fim de construir indicadores para estudos, como da 2Checkout (2Checkout, 2014), com o objetivo de montar uma base histórica, na qual é empregada para a prevenção de fraudes.

O serviço utilizado para auxiliar na mitigação das fraudes relacionadas a transações de crédito e débito ocorre executando uma dupla autenticação, a fim de garantir que o portador que está realizando uma venda fidedigna. Atualmente os plásticos de cartão de crédito e débito estão com suporte maior da tecnologia para auxiliar na mitigação de fraudes.

A tecnologia de tarja magnética está sendo substituída pelo o tipo EMV (*Chipcard*) pelas instituições financeiras, o cartão com chip possui data gramas com objetivo de auxiliar no combate as fraudes. O número de transações utilizando tarja magnética diminuiu de 8% em 2014 para 2,6% em 2015, em contrapartida as transações utilizando o EMV subiu de 82,6% em 2014 para 87,2% em 2015, conforme exemplificado pelo Figura 2.

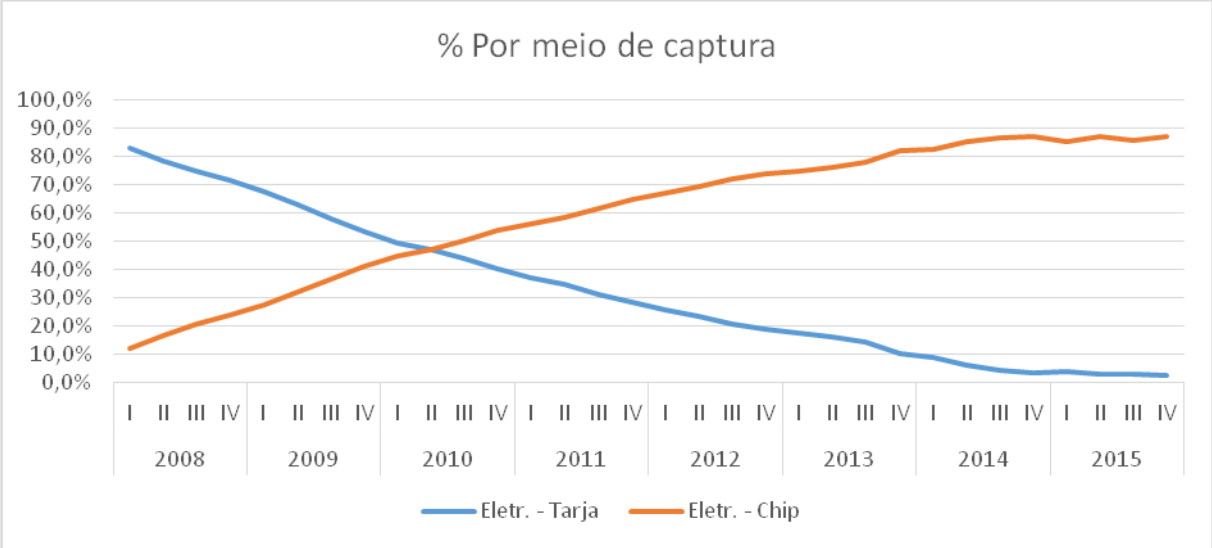


Figura 2: Transações capturadas por tarja magnética e *Chipcard* Trimestral
Autor: (BACEN, 2016)

A última fraude registrada no território brasileiro sobre cartões utilizando EMV foi em Maio de 2016, onde uma quadrilha informava aos portadores, simulando a instituição financeira que o portador possui relação, informando que seus cartões foram bloqueados por tentativa de fraudes e pediam para cortá-los e em seguida entregar para um funcionário do banco (fraudador) o cartão triturado. Porém, com o chip em perfeito estado; os fraudadores conseguiam incluir o chip em um plástico do tamanho de um cartão e decifrar os data gramas e a senha, sendo possível clonar o chip e o cartão e executar novas transações (G1, 2016).

O mercado trabalha em um ritmo constante a fim de prevenir as novas fraudes que ocorrem dentro do mercado de cartões brasileiro, assim como métodos de estudo heurísticos de analisar e definir se uma transação é fraudulenta através de algoritmos (Kovach, Stephan; 2011), como o estudo sobre a utilização de transações de *eletronic referral* como uma alternativa para prevenção a fraudes, seguindo a tendência do mercado.

O mercado é composto por meios de captura além do POS, como o TEF, *Mobile* e *E-Commerce*, por tanto este trabalho visa exemplificar a implementação da transação de *eletronic referral* em cada meio de captura, seguindo suas características de comunicação e usabilidade, apresentando o esforço de implementação de cada meio de captura, sendo este um motivador para este trabalho.

1.2 Objetivo

O objetivo deste trabalho é apresentar um tipo de transação específica chamada *eletronic referral*. Utilizando como premissa os meios de captura do mercado brasileiro mais populares de cartões (POS/Mobile/TEF/E-Commerce) e contextualizando as empresas que fazem parte para aprovação de uma transação (adquirentes, bandeiras, estabelecimentos e emissor.

A partir deste contexto será realizado a comparação das tecnologias de meios de captura, a fim de avaliar o grau de dificuldade de integração da ISO 8583 de cada meio de captura com o adquirente e apresentar a comparação a partir de cada categoria derivada de normas regulatórias e boas práticas de mercado. Para que a comparação seja concisa é necessário apresentar em detalhes a implementação do *eletronic referral* em cada meio de captura.

1.3 Justificativa

Com a velocidade do desenvolvimento do mercado de cartões brasileiro, bem como os diversos tipos de serviços que são oferecidos ao portador, existe um tipo específico de transação que tem por objetivo executar uma segunda camada de segurança em uma transação financeira, chamada de *eletronic referral.* A transação de *eletronic referral* é mais utilizada nas máquinas de POS, portanto o estudo do trabalho visa discutir a possibilidade de ampliar a gama de utilização desta transação para outros meios de caputra, em especial o PDV, *E-Commerce* e *Mobile*.

1.4 Estrutura do Trabalho

Os capítulos sequentes deste trabalho foram estruturados da seguinte maneira. O Capitulo 1 apresenta a introdução do mercado brasileiro de vendas de cartão de crédito e débito e motivações da construção deste trabalho. O Capitulo 2 os meios de pagamento brasileiros, contendo a estrutura geral para realização de uma venda e os requisitos que os meios de captura precisam se adequar. O Capítulo 3 apresenta a Norma ISO 8583 que contempla a especificação dos bits empregados na troca de mensagens entre os membros participantes do processo de transação eletrônica. O Capítulo 4 apresenta a análise comparativa dos meios de captura e a sua aplicação no contexto da transação do tipo *eletronic referral.* Para finalizar, o Capítulo 5 contendo a conclusão, contribuições e trabalhos futuros e apresentado.

2. Meio de pagamentos brasileiros

O mercado brasileiro de pagamentos eletrônicos (cartões) contempla empresas com papéis e responsabilidades próprias, na qual, em conjunto constituem uma cadeia sistêmica interdependente. Pois, necessitam de todas as empresas se comunicando em um intervalo curto de tempo para prover um serviço conhecido como pagamento eletrônico.

No sistema brasileiro de pagamentos eletrônicos as transações são realizadas por meio de transações. Esta transação é composta pelos seguintes participantes: um portador do cartão, que efetua o pagamento/compra em uma máquina POS sigla para *Point of Sale* (Ponto de Venda) que captura as informações desta transação.; Um fornecedor de comunicação de dados entre as empresas, a empresa adquirente de cartões, a empresa responsável pela bandeira do cartão e por fim o emissor do cartão. A empresa adquirente tem como função credenciar os estabelecimentos comerciais (lojas) e fornecer o canal de comunicação para realizar as transações de crédito e débito, pagar o estabelecimento pelas vendas realizadas e enviar todas as requisições de transações para bandeira. A empresa responsável pela bandeira tem como função gerenciar a comunicação entre os adquirentes e os emissores, credenciar as adquirentes e os emissores, regularizar a maneira como é feita a comunicação de cada transação. O emissor do cartão é o banco financeiro que emite o cartão para o portador (cliente), aprova as transações de crédito e débito, cadastra o portador no produto da bandeira e paga as bandeiras pelas transações realizadas.

Todas as informações desde a inserção do cartão no POS são trafegadas por um canal cifrado. A Figura 3 exemplifica o modelo macro de comunicação entre as empresas para realização de um pagamento.

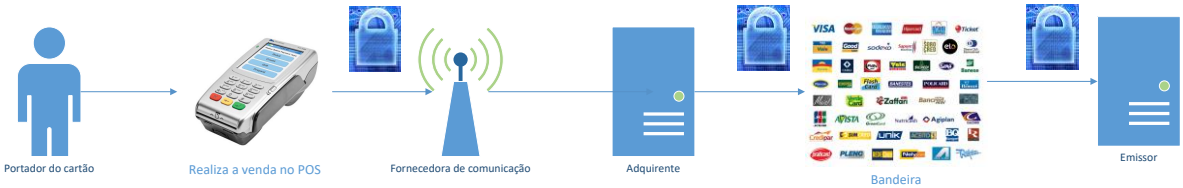


Figura 3: Modelo Macro de comunicação entre as empresas.
Fonte: elaborado pelo próprio autor.

Esta comunicação é realizada por meio de um circuito de comunicação de dados pertencente às operadoras de comunicação, que fornecem soluções para essas empresas. O contrato varia de acordo com a necessidade de cada empresa e esta fora do escopo desse trabalho. Os meios de comunicação variam de acordo com a solução adequada para cada cliente segundo a necessidade de negócio de cada lojista. Segundo o manual da Transferência Eletrônica de Fundos (TEF) escrito pela empresa Auditor, temos alguns exemplos de meios de comunicação entre as empresas (Auditor, 2016), são eles:

- Conexão direta;
- *Link* dedicado;
- Conexão via X25;
- Conexão discada;
- Conexão de banda larga; e
- Sistema Global para comunicação móvel (GSM).

Como a comunicação de dados efetuada entre as empresas envolve informações sigilosas e privadas, se faz necessário a aplicação de criptografia em todo o canal de comunicação. A criptografia exerce o papel de manter as informações financeiras trafegadas entre as empresas atendendo os requisitos de segurança necessários. Determinado pelo PCI (*Payment Card Industry Security Standards*) órgão que define as regras de segurança do mercado de pagamentos eletrônicos, a qual exige a criptografia de todo o canal de comunicação empregando o DES (*Data Encryption Standard*) (PCI, 2016). No entanto, fica a cargo da empresa financeira utilizar o DES ou algoritmo de criptografia superior oferecido no mercado.

Atualmente os algoritmos de criptografia disponíveis para o mercado, constituem-se dos algoritmos que utilizam a mesma chave de cifragem e decifragem conhecidas como simétricas e os algoritmos que utilizam uma composição de chaves, sendo uma pública e outra privada, é conhecida como assimétrica (Ronielton, Oliveiraon, 2012).

No mercado, a tecnologia comum referente aos meios de pagamento é o POS sistema configurado das populares “maquininhas” que possuem um sistema operacional básico fornecido pelos seus fabricantes. O sistema operacional básico tem como função testar a comunicação entre os componentes de hardware, a fim de

verificar se todos os componentes estão em modo operacional. Exemplos de fabricantes atuantes no mercado brasileiro são a Ingenico, Verifone e Perto.

Os componentes de *hardware* de um POS reunidos possuem semelhança com os de um microcomputador, como processador, memória e placa de rede. Exemplificando a composição de um POS, temos a especificação técnica do POS da Fabricante Ingenico modelo ICT 250 ilustrada pela Figura 4:

Feature		Description
Processor		ARM 9 & ARM 7, 450 MIPS & 50 MIPS
Memory	RAM	32 MB
	Flash	128 MB
	µSD Card	•
SAM		2
Card reader	Smart card	1
	Magstripe	Track 1/2/3
	Contactless	•
Display	Size & Resolution	TFT color 2.7" QVGA 320 x 240 pixels
Keypad	Backlit operational keys	15
	Navigation keys	4
Thermal printer	Speed in lines/second	18 l/s
Connections on terminal	RS232	1
	USB host, USB slave	1
	Ethernet	1
	Power supply connector	1
Power supply	External power supply	110 V, 60 Hz
Terminal size	L x W x H	7.28" x 3.26" x 2.48"
Weight	Terminal without paper roll/cable	11.46 oz
Privacy shield		Option
Customization	Lens marking	Option
	Printer cover flap	Option
	Top casing	Option
Connections on Magic Box (optional)	Power supply connector	1
	RS232	1
	Line in	1
	Ethernet	1
Environment	Operating temperature	41°F to 113°F
	Storage temperature	-4°F to 131°F
	Relative humidity, non-condensing	85% HR at +104°F
Security	Online & offline	PCI PTS 3.x

Figura 4 – Especificação POS ICT250

Fonte: Ingenico, 2016

A Fabricante do POS entrega o sistema operacional (SO) com funcionalidades básicas do equipamento (ligar, desligar, validação de memória e processador) para a empresa detentora do equipamento. Apenas o SO fornecido pela fabricante não é o suficiente para realizar uma transação, se faz necessário à instalação do *software* de pagamento oferecido pela empresa detentora, no caso deste trabalho a adquirente. Este *software* entregue pela adquirente executa as funções comumente realizadas para operação de um POS, como por exemplo, sincronização da rede GSM (*Global System Mobile*), interpretação do cartão inserido no POS, emissão de impressão (Cielo, 2016). O POS possui virtualização em uma camada superior ao sistema operacional, que é a aplicação oferecida pelo proprietário do POS. O versionamento, instalação e uso são de propriedade intelectual da empresa dona do POS (Adquirente), incluindo o meio de pagamento e as funcionalidades disponibilizadas.

Os POS suportam uma série de protocolos, responsáveis principalmente para gerar e administrar a conexão, por exemplo, o protocolo TCP/IP para conexão de rede, ou conexão via rádio frequência. Todos estes protocolos possuem uma camada reservado e específica dentro do POS, para assim ser melhor administrada.

Utilizando como base no sistema virtualizado fornecido pela adquirente, o acesso a hardware é possível, via acesso do sistema ou via chamada com a camada física existente no próprio POS. Com base nas informações Geradas por Elizer Pimentel, 2016, sobre as propriedades de um POS é possível exemplificar na Figura 5 o modelo de arquitetura de um POS.

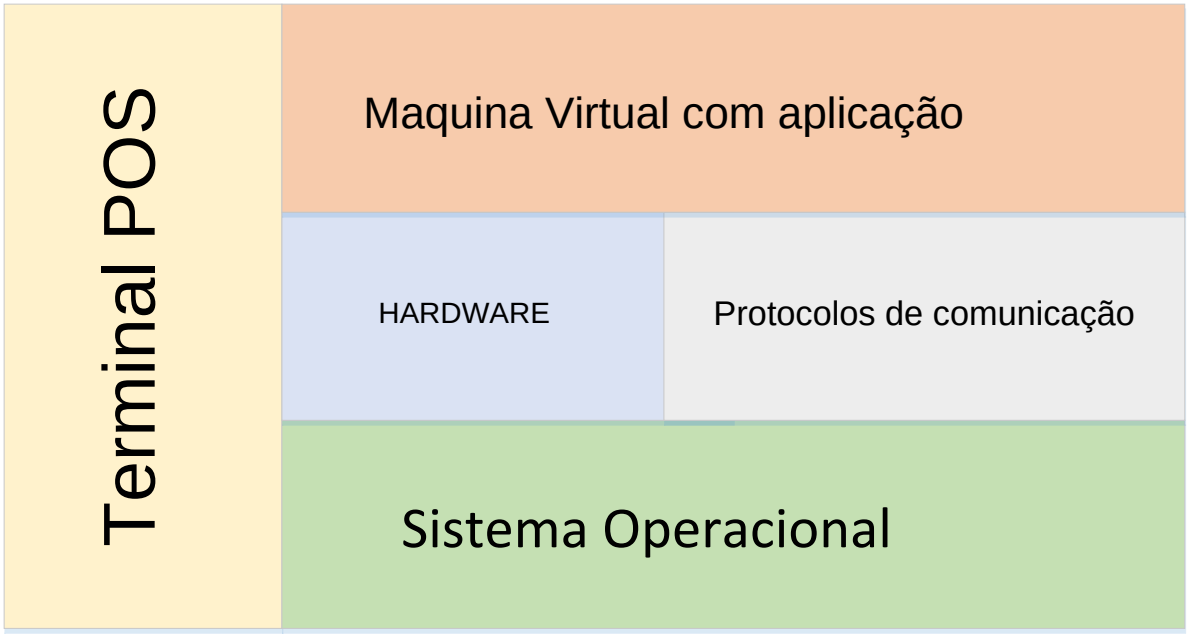


Figura 5 – Arquitetura de um POS

Fonte: Pimentel, 2009

A Partir de um POS é possível realizar transações de crédito e débito também conhecido como vendas, às vendas são transferências de crédito entre o pagador e o beneficiário, por intermédio de um sistema de liquidação (Sebrae, 2016).

2.1 Execução de venda

Para a execução de uma venda, o portador do cartão insere o cartão e seleciona o tipo de transação de crédito ou débito, a interação com o terminal varia de acordo com o tipo do produto do cartão, como exemplo, Cartão Black, Gold, Infinite, Cliente Mais. Dependendo do produto do cartão, sendo como produto o informado pela bandeira e emissor no cartão, exemplo Visa Platinum, Elo Ruby, Mastercard Gold; onde é informado o nome da bandeira do cartão (Visa, Elo, Mastercard) e o produto referenciado (Platinum, Ruby, Gold). O produto tem por definição a segregação de benefícios, cada cartão pode possuir não sendo necessariamente uma obrigação, varia da decisão do portador e do emissor do cartão, além de definir o valor aquisitivo do portador.

As funcionalidades fornecidas pelo emissor também são uma variável de interação para o terminal, temos como funcionalidades do emissor os exemplos, Cartão Débito e Crédito (Múltiplo), Parcelado Emissor, Pagamento por fidelidade, Pagamento Pré

Datado. Existem tipos de cartões que precisam apenas da assinatura do ato da compra como meio de comprovante, ou existe tipo de cartão que exige a segunda interação (inserção de senha) para conclusão de uma venda, sendo variantes na interação do portador com o POS. Para determinar o tipo de cartão é a composição do produto oferecido pelo cartão, funcionalidade do emissor.Exemplificando como a variação do cartão pode alterar as interações que o portador executa com o terminal, serão utilizados dois cenários de pagamento. A Figura 6 ilustra um pagamento utilizando a tarja magnética como meio de entrada no POS e a assinatura como forma de autenticidade de compra presente.

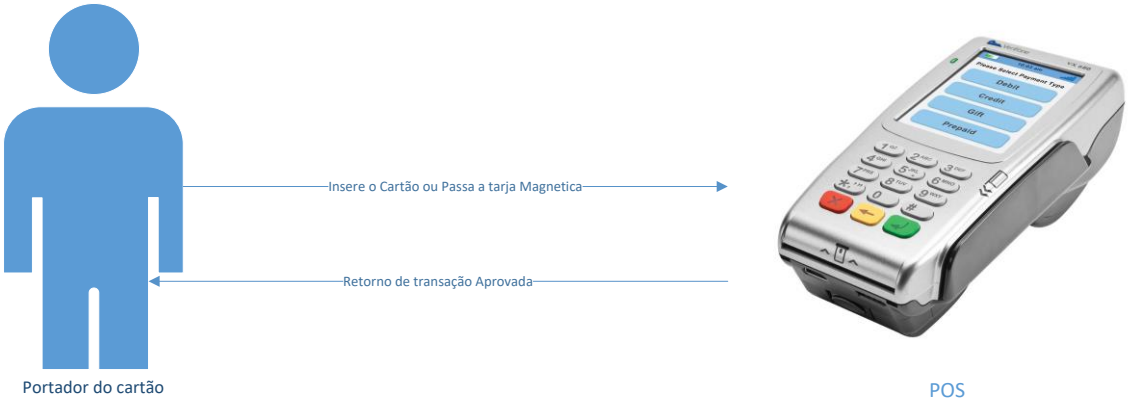


Figura 6: Interação do portador com um cartão sem senha

Fonte: elaborado pelo próprio autor

Na Figura 7 é ilustrado o segundo cenário, onde o meio de entrada do POS continua sendo a tarja magnética, no entanto o modelo de autenticidade é a senha do cartão.

Figura 7: Interação do portador com um cartão com senha

Fonte: elaborado pelo próprio autor

2.2 Meios de comunicação

Para realizar uma transação existem diferentes meios de comunicação. Dentre eles destacamos os seguintes meios.

2.1.1 Conexão Direta

O termo conexão direta consiste na comunicação entre dois sistemas interoperantes, neste caso, a da comunicação entre duas empresas. A conexão direta utiliza o protocolo de rede TCP/IP nas versões 4 e 6 (Shultz, Greg; 2003). O recurso de conexão direta utilizado em uma transação garante um maior nível de segurança, visto que a comunicação é feita *end-to-end* sem interferência de empresas ou entidades não pertencentes a esta comunicação.

Além de uma comunicação privada, sem necessidade de compartilhamento com empresas terceiras, podendo variar nos seguintes meios de transmissão:

- Fibra Ótica;
- Cabo Elétrico; e
- Conexão via Satélite.

Para exemplificação de uma aplicação da conexão direta, será utilizado o exemplo do fluxo de informação da ISO 858 variando de acordo com a solução instalada pelo lojista ou o serviço prestado, utilizando como transferência de informações uma venda realizada por meio de um POS *Wireless*:

- Meio de captura para o Roteador: o meio de captura (POS) captura as informações do cartão e envia para a torre de distribuição.
- Torre para o servidor de distribuição: a Torre de distribuição envia as informações o servidor de distribuição.
- Servidor de distribuição entre a adquirente: o Servidor de distribuição por sua vez, captura as informações e as envia cifrada para o adquirente.
- Adquirente com a Bandeira: a adquirente responsável pelo estabelecimento recebe as informações e por sua vez envia para bandeira via canal cifrado.
- Bandeira com o Emissor: a Bandeira responsável pelo estabelecimento recebe as informações e por sua vez envia para o emissor via canal cifrado.

- Emissor com a Bandeira: o Emissor recebe as informações da bandeira, aprova ou nega dependendo da regra de negócio do emissor para o cartão, devolvendo o retorno para a bandeira. Concluído o retorno para a bandeira oriunda do emissor o fluxo de retorno é executado até a chegada ao POS.

As formas de comunicação do tipo conexão direta variam de acordo com o contrato entre as duas empresas que estarão executando o serviço, utilizando como exemplo a conexão de um equipamento de captura de cartão. Este tipo de equipamento será nomeado de PinPad, integrado ao servidor de pagamento da loja conhecido como *Checkout*, conforme o modelo apresentado na Figura 8.

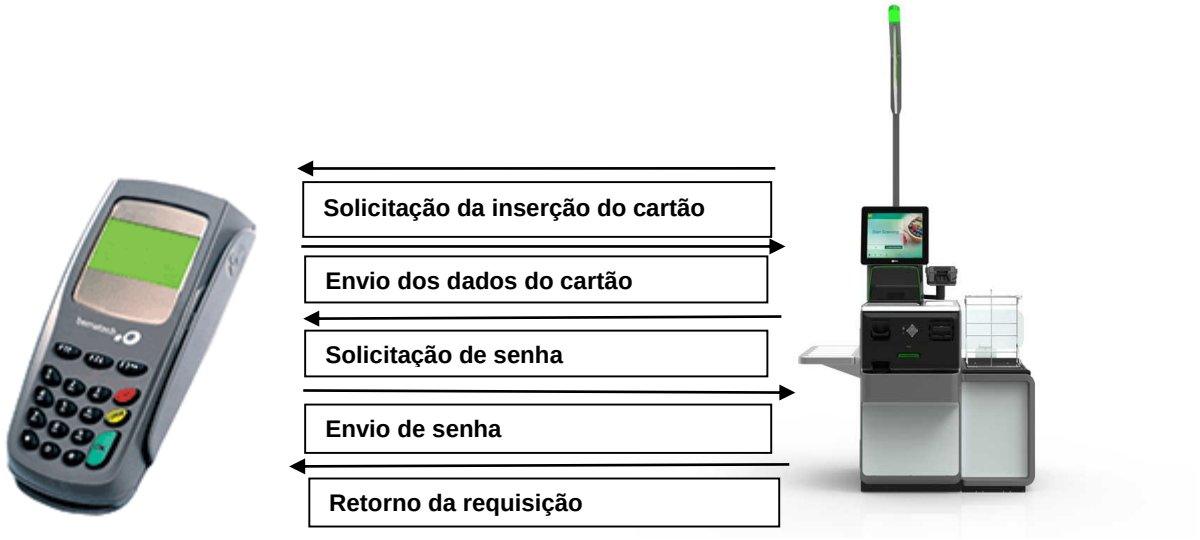


Figura 8: Comunicação realizada entre checkout e PinPad

Fonte: Software Express - 2016

2.1.2 Link dedicado

O *link* dedicado trata-se de um circuito de comunicação contratado a partir de uma empresa de telecomunicações, onde se garante um canal de roteamento único e exclusivo provido pela contratante (Embratel, 2016). Em um *link* dedicado existe apenas um usuário utilizando o canal de comunicação, assim a concorrência do canal de rede é mínima, garantindo a velocidade contratada informada pelo fornecedor. O *link* dedicado possui um controle maior de segurança, pois, o cliente tem a possibilidade de contratar o serviço com a restrição dos IPs (*Internet Protocol*)

de acesso ao canal sobre a velocidade de banda, garantindo e configurando a velocidade do *download e upload* no modelo contratado.

O *link* dedicado é utilizado pelas corporações, visto que na conexão realizada, não pode existir latência ou instabilidade, além de uma necessidade de suporte por eventuais instabilidades que podem existir de alguns minutos, item que impacta todo o sistema que depende desta conexão. Algumas empresas utilizam o *failover* de conexão, método de contingência automática, onde um segundo sistema assume automaticamente o lugar do primário quando o mesmo apresenta alguma falha pré-determinada, (FailOver, 2016). A principal diferença entre a conexão direta e o *link* dedicado; no cenário do *link* dedicado a empresa que realiza a conexão é responsável por toda manutenção e suporte, enquanto para o *link* direto este serviço é terceirizado para uma empresa de telecomunicações. A Figura 9 ilustra o modelo de link direto com *failover*.

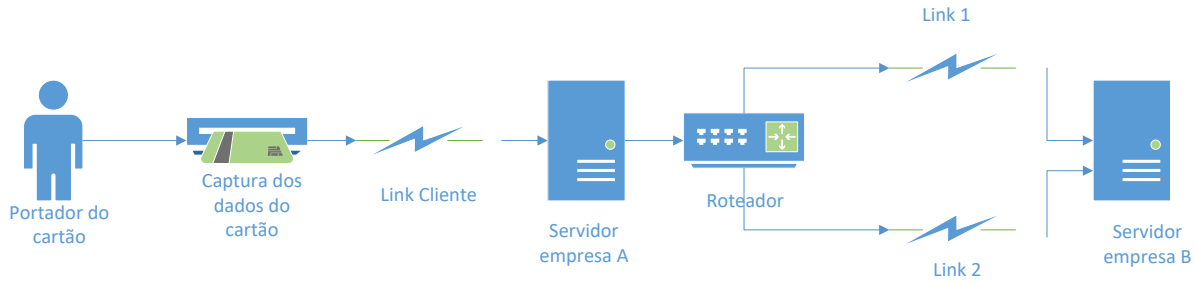


Figura 9 - Conexão entre a empresa A e B com FailOver

Fonte: elaborado pelo próprio autor.

2.1.3 Conexão via X25

O protocolo de comunicação X25, consiste de um protocolo de comunicação de tecnologia baseada na comutação de pacotes, utilizando sempre o mesmo canal, adotando uma abordagem de transmissão *full duplex*, ou seja, envio e recebimento pelo mesmo canal. O X25 foi baseado nas três camadas do modelo OSI (X25, 2016), tendo fácil compatibilidade com outras camadas do protocolo como TCP/IP, sendo elas:

- Camada Física: define as características mecânicas e elétricas da interface do Terminal e da Rede. A transmissão é feita de modo síncrono e *full duplex*;

- Camada de Enlace: responsável por iniciar, verificar e encerrar a transmissão dos dados na ligação física. Também é responsável pelo sincronismo, detecção e correção de erros durante a transmissão; e
- Camada de Rede: responsável pelo empacotamento dos dados. Define se a transmissão será realizada por Circuito Virtual (conexões temporárias, estabelecidas somente no momento da comunicação) ou por Circuito Virtual Permanente (conexões permanentes, não existe a necessidade de realizar uma chamada para estabelecer conexão) (Tektonia, 2016).

O endereçamento utilizado pelas redes X25 é dado por um padrão chamado X.121, similar ao número empregado nos telefones. Uma atribuição que um provedor de acesso fornece baseado na geolocalização do cliente, um exemplo de número de endereçamento X.21 é *[1235431441]*.

O principal objetivo de uma conexão X25 é fornecer uma comunicação sem erros, pois, o cliente que executa a requisição nem sempre está preparado para tratamento de erros. Uma conexão de um serviço X25 para o sistema de pagamentos eletrônicos é utilizado para conectar o roteador das empresas parceiras com as empresas adquirentes, esta rede é de uso exclusivo do trafego de informações dos dados do cartão, não sendo utilizado para outros fins. Na Figura 10 é apresentado o cenário de pagamentos de uma loja, onde existe um servidor concentrador que centraliza as transações. O X25 foi implementado entre a *Software House* (empresa contratada para envio das transações) e a Adquirente de cartões, no entanto não existe impedimento para se utilizar em toda a cadeia.

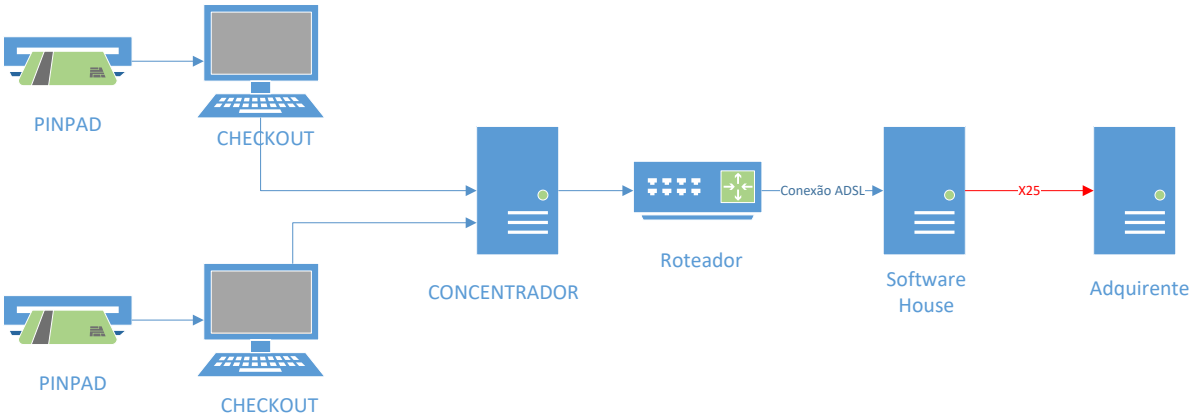


Figura 10 – Representação do X25 na cadeia de meios de pagamento

Fonte: Auditor, 2016

2.1.4 Conexão discada

A conexão discada consiste na utilização da linha telefônica como meio de conexão entre o cliente e o provedor de Internet, a comunicação é feita através do modem do cliente (Cisco Support, 2016). Esta infraestrutura de comunicação é apropriada para a voz, a Internet discada não consegue alcançar maior velocidade, mantendo com o seu padrão de 56kbps. Este tipo de comunicação possui uma largura de banda limitada, ou seja, não suportando um alto volume de conexões além de ser uma conexão simétrica, logo, quando o aparelho se conectava na Internet não é mais possível utilizar o canal de voz. Existe a possibilidade de aumentar a velocidade como agregação de outras linhas telefônicas para conexão, multiplicando conforme a quantidade de linhas telefônicas, no entanto, este modelo consome como se fosse feita uma ligação de voz por cada linha, tornando-se um modelo caro para a velocidade fornecida. Uma das configurações que as empresas fornecedoras aplicam especificamente para este tipo de conexão é o *time out*, onde durante tempo de inatividade o cliente tinha sua conexão com o provedor interrompida.

O principal equipamento no contexto das transações financeiras que utiliza a linha discada é o POS de conexão discada. Quando o POS é instalado no lojista, o técnico configura dentro do POS o número de telefone que se deve discar para conexão, semelhante a um provedor de acesso a Internet. O POS quando conectado na Internet entra na Rede da Adquirente e segue o caminho transacional, limitando ao conteúdo da velocidade máxima que a infraestrutura de comunicação discada pode oferecer. A Figura 11 ilustra o modelo de conexão discada de um POS.

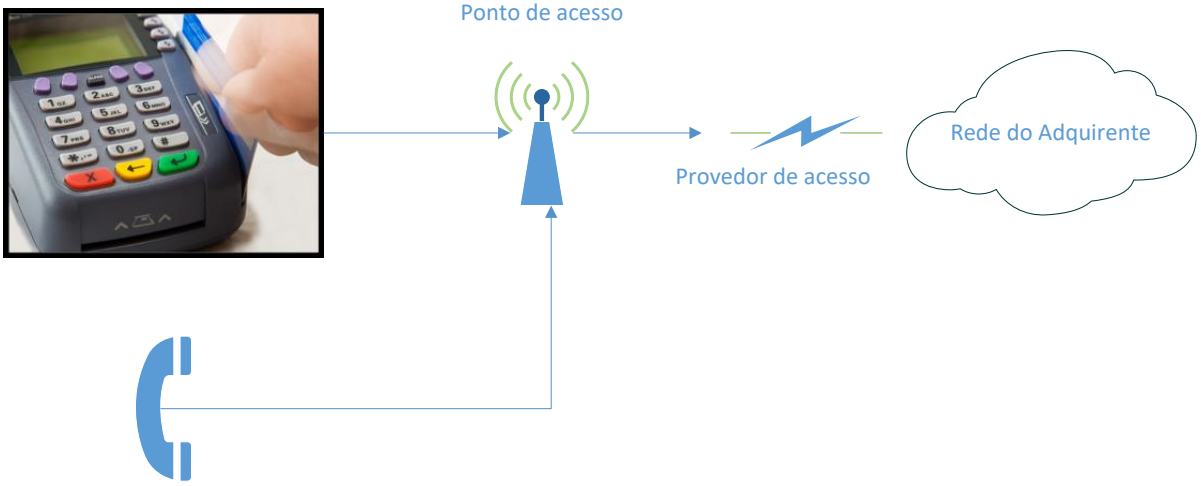


Figura 11 – Representação da comunicação discada de um POS

Fonte: elaborado pelo próprio autor.

2.1.5 Conexão ADSL

A conexão ADSL (*Assymmetric Digital Subscriber Line*) ou (linha digital assimétrica para assinante) tem por meio de comunicação a linha telefônica, porém, diferentemente da conexão discada. O ADSL divide o canal de comunicação em três canais distintos:

- Canal de *download*;
- Canal de *upload*; e
- Canal de voz.

Cada canal tem por função estabelecer a comunicação própria definida, onde o canal de voz será utilizado exclusivamente para a conexão de voz, o canal de *download* apenas o recebimento de informações e o canal de *upload* apenas para o envio de informações (Teleco ADSL, 2010). O ADSL possui como diferencial a assimetria, pois o canal de banda não são os mesmos, tendo por definição um canal maior para *download* e os dois menores para *upload* e voz. A conexão ADSL apresenta maior velocidade em comparação a conexão discada, assim, dependendo da qualidade da infraestrutura da companhia de telecomunicações e a distância de conexão, esta velocidade pode ser alterada batendo um limite de 9Mbit/s, conforme exemplificado na Figura 12.

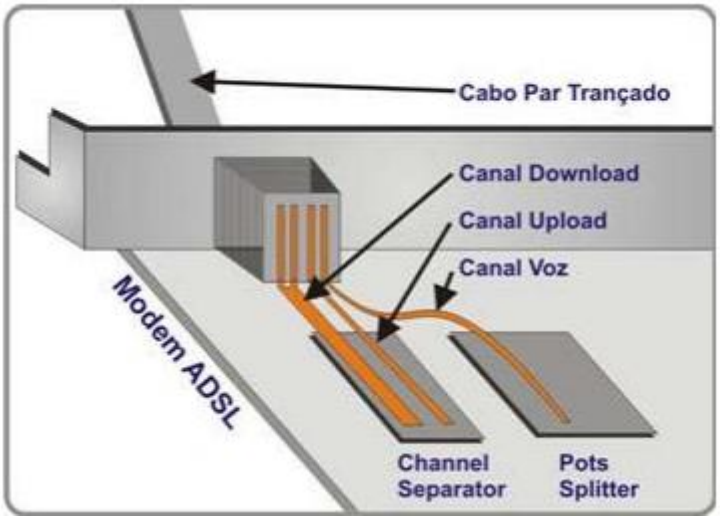


Figura 12 – Representação da largura dos canais ADSL

Fonte: Teleco ADSL, 2010.

Existem tecnologias compatíveis com o protocolo PPPoE de autenticação, onde é possível por meio de um cabo RJ45 (cabo de par trançado para conexões através de

impulsos elétricos) a conexão de um canal de captura de uma transação. Utilizando um POS com conexão Ethernet, o mesmo tem uma entrada para conexão telefônica (RJ11) e a entrada para Ethernet (RJ45). Diferentemente da configuração realizada em um terminal POS de conexão discada. Para esta configuração o operador configura o IP fixo do POS para um roteador ou modem, na qual ao enviar uma transação, o pacote de dados irá consumir a banda de *upload* para envio da transação e a banda de *download* para recebimento dos pacotes de resposta, não sendo necessário o consumo da banda de voz semelhante ao POS discado.

2.1.6 Sistema Global para comunicação móvel (GSM).

O primeiro sistema global de comunicação móvel teve inicio na Europa após um grupo de estudos se unirem a fim de padronizar os protocolos de comunicação e permitir a interoperabilidade entre os países da Europa (Teleco GSM, 2008).
Um GSM e composto pelas seguintes informações:

- MSISDN - *Mobile Service ISDN Number*

  Representa o número discado associado ao assinante. É provido para o assinante pela operadora na hora da compra e é gravado no SIM *card* (Chip de autenticidade do numero do celular), é formado da seguinte maneira: MSISDN = Código do País + Código da região + Numero do assinante. Exemplo: 55 + 11 + 99999 9999.

- IMSI - *International Mobile Subscriber Identity*

  Quando um usuário assina o serviço de uma operadora uma identificação única de assinante é fornecida, essa identificação é gravada no SIM card do assinante e também no HLR (Base de dados de assinantes na operadora), é formado da seguinte maneira: IMSI = Código do país do celular + Código da Rede do celular + Numero da identificação do celular. Exemplo: 311 + 030 + 000001258.

- IMEI - *International Mobile Equipment Identity*

  É um número de série único alocado no hardware do aparelho móvel, registrado pela operadora e opcionalmente gravado na AUC (Central de

Autenticação da rede) para propósito de validação. Exemplo: 354150-06-173363-5.

- GT – *Global Title*

Todo equipamento na rede GSM recebe uma identificação única internacional, para que possa ser identificado por qualquer operadora GSM no mundo. Funciona como um endereço IP, através desse GT que uma operadora consegue comunicação entre equipamentos dentro da rede e comunicação com outras operadoras também.

Para meios de pagamentos a tecnologia GSM é utilizada com os modelos de máquinas de POS conhecidas como PO**O**, acrônimo adicionado o segundo O por significar *outdoor* (sem conexão fixa). Neste caso o POO recebe um chip de um celular, na qual entrará na rede GSM, ao executar uma venda o POO envia para antena da operadora que por sua vez direciona para a rede de distribuição que por fim chega na rede da adquirente. A Figura 13 ilustra este tipo de conexão.

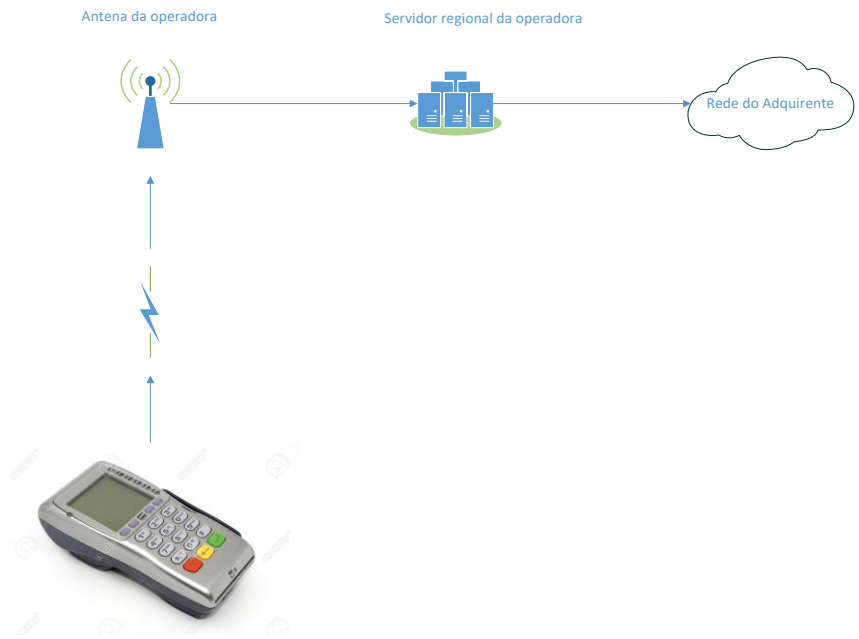


Figura 13 – Representação da comunicação realizada de um POO

Fonte: elaborado pelo próprio autor.

2.2 Criptografia

A criptografia das transações oriundas de pagamentos utilizadas no padrão da ISO8583 responsável pelo trafego de informações financeiras, varia de acordo com cada instituição, o PCI atualmente exige a criptografia DES ou superior nas transações.

2.3.1 DES

O modelo de criptografia mínimo requisitado pelo PCI para se adequar as regras de segurança de informação de uma transação financeira é o DES. O Significado de DES (*Data Encryption Standard*) Criptografia de Padrão de Dados, criado pela NSA (Agencia Nacional de Segurança Americana) em 1977 (STALLINGS, 1998). O modelo de funcionamento do DES consiste em três partes: permutação inicial, cifragem com operações de chave e permutação final. As permutações iniciais e finais são processos de transposição dos blocos de entrada, executando a leitura da esquerda para direita. Já a cifragem com operações de chave onde se é trocado os bytes iniciais com finais é executada repetindo dezesseis vezes a mesma operação. Inicialmente o bloco de entrada e a chave são divididos em duas partes de mesmo tamanho, é executado processos de permutação, transformação e expansão de chave, a expansão da chave consiste em um tamanho máximo de 56 bits, onde ‘K’ é a chave e ‘F’ é a função de cifragem composta, ao final é executado a permutação inversa afim de apresentar os dados cifrados anteriormente. A cada bloco executado, uma nova chave é gerada, a Figura 14 ilustra a operação de permutação do DES.

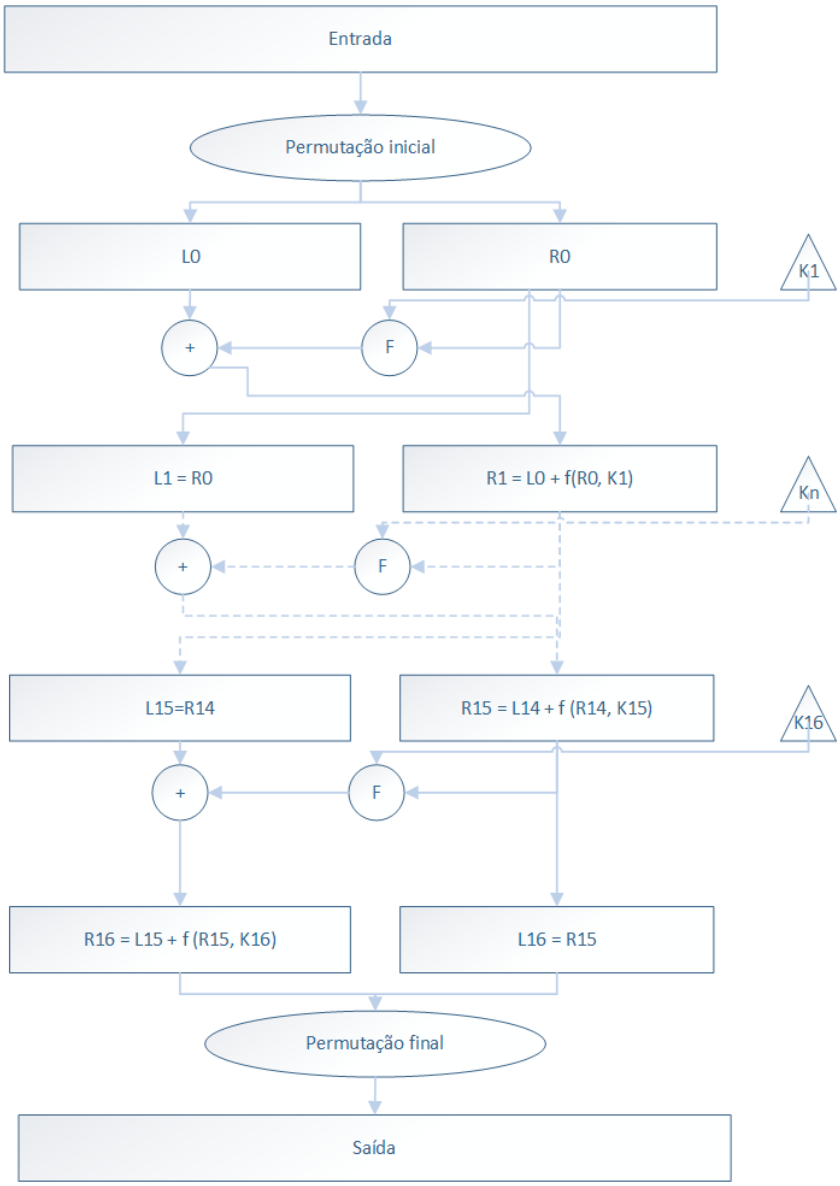


Figura 14 – Arquitetura do DES

Fonte: Gargallo, 2016

2.3.2 Triplo DES

O triplo DES (3DES), uma variação da criptografia do DES, onde a chave de criptografia varia dentro do próprio modelo de cifragem do DES e pode ser cifrado em três etapas. O processo de cifragem do 3DES ocorre na seguinte sequência:

- Primeira etapa ocorre em um processo de cifragem de informação através do processo do DES;
- Segunda etapa ocorre o processo de cifragem do DES, porém utilizando a chave invertida do que realizada na primeira etapa; e
- Na terceira etapa ocorre um novo processo de cifragem utilizando o processo do DES.

As chaves de criptografia compatível no 3DES varia entre 2^112 ou 2^168 (Alanazi, Hamdan, 2010).

O modelo de cifragem do 3DES é exemplificado na Figura 15.

Figura 15 – Criptografia 3DES

Fonte: elaborado pelo próprio autor

2.3.3 DUKPT

A criptografia de chave única derivada por transação (*Derived Unique Key Per Transaction*) foi criada pela Visa na década de 80, no entanto começou a ser implementada somente na década de 90, para cifrar as informações entre os bancos emissores de cartões e os POS (Visa, 2013).

O algoritmo DUKPT trabalha utilizando três informações que são oriundas do POS, sendo elas:

- Base de chaves de derivação (*Base Derivation Key*): São as chaves internas do POS;
- Chave de criptografia de senha Inicial (*Initial PIN Encryption key*): São as senhas inseridas no ato da compra pelo portador e cifradas pelo terminal a cada sessão; e

- Chave de numero de serial (*Key Serial Number*): chave de criptografia derivada do numero do serial gerado automaticamente a cada nova transação.

Com essas três informações reunidas, gera-se a chave de sessão (*Session Key*) que é enviada ao receptor (Bandeira ou Emissor) para que utilize para decifrar a informação enviada (Global Insurence, 2016).

No receptor o sistema possui uma copia das chaves de derivação do POS, onde utiliza o *Session Key* como chave de cifragem semelhante; a chave de cifragem é a comparação do *hash* cifrado das informações enviadas pelo meio de captura (POS/PDV/Mobile) com o existente na base do sistema receptor, se os dois *hash* estiverem corretos, o sistema receptor executa o processo de decifragem. Na figura 16 é apresentado o modelo de cifragem do DUKPT com base de uma transação oriunda do POS.

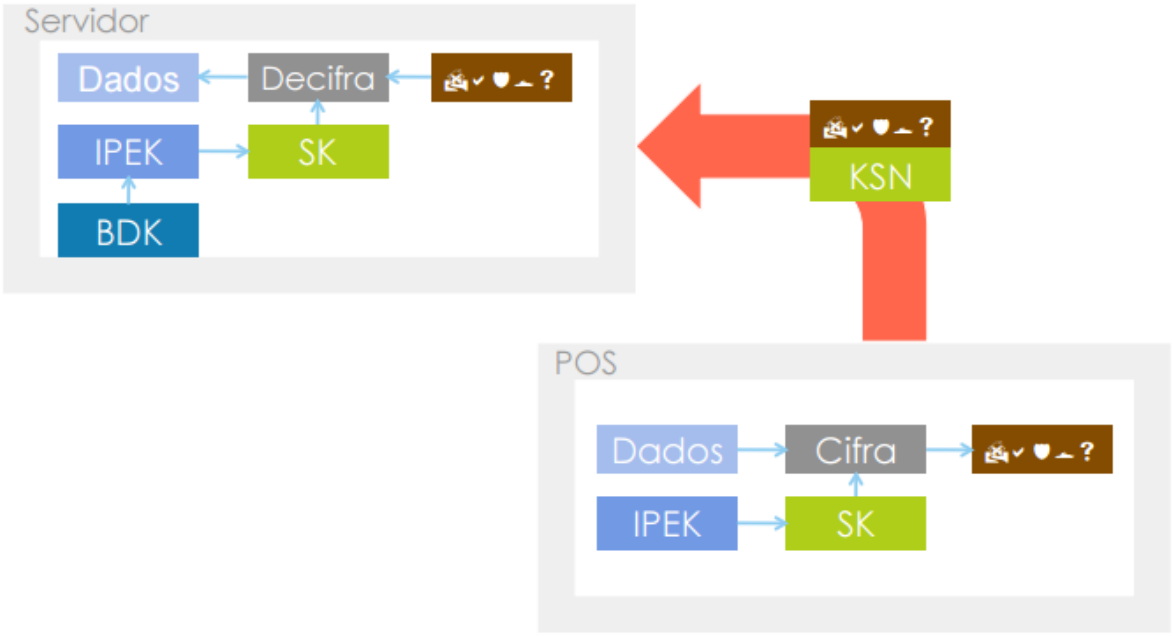


Figura 16 – Modelo de criptografia DUKPT

Fonte: Guimares, Moises, 2016

2.3.4 RSA

O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: **R**on Rivest, Adi **S**hamir e Len **A**dleman, que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento.

O RSA utiliza números primos grandes como base de sua segurança. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, onde é muito difícil de recuperar os dois primos a partir daquele terceiro número. Este processo é conhecido como fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de fatoração de números grandes em um tempo razoável. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo (Oliveira, Roneilton, 2016).

2.4 Aplicação do POS

Uma aplicação de POS pode ser escrita de diversas maneiras e linguagens, por possuir uma arquitetura semelhante a um computador pessoal, no entanto em menor escala, chegando à similaridade de um *smartphone*.

A máquina virtual instalada junto com os pacotes binários básicos da empresa responsável pelo POS tem como função utilizar o *hardware* fornecido pela fabricante e utilizar suas funções em um nível que a máquina virtual que a aplicação do POS utilize tenha total acesso sem restrições a camadas baixa do *hardware* e sistema operacional nativo.

Os sistemas desenvolvidos pelos fornecedores de pagamentos podem ser desenvolvidos em linguagens de nível intermediário de acesso ao hardware como o C, C++, Java (Desenvolvimento de software, 2016) dependendo da aplicação com acesso ao banco de dados, caso a necessidade de gerar um relatório ou necessidade da aplicação para funções especificas. Para atualização da versão, o POS recebe as informações diretamente via conexão remota da empresa onde esta conectada (Adquirente, Servidor, Concentrador) e inicia o *download* de pacotes, instalando e definindo como nova versão na máquina virtual.

Com base da aplicação as empresas conseguem desenvolver ferramentas e ou serviços para os clientes finais, podendo variar desde a impressão de um comprovante fiscal até um novo modelo de pagamentos (Desenvolvimento de software, 2016). Com a semelhança de um microcomputador é possível gerar

aplicações, desde a criação de um *smart terminal* (Poynt, 2016) como uma criação de uma aplicação de jogos de tabuleiro no terminal. O terminal desde que possua *hardware* para aplicação que se é escrita, consegue executar como esperado semelhante à aplicação de um computador, com um *software* de desenvolvimento simulado, o pacote entregue com os binários compilados e depois entregue para o terminal instalá-lo na máquina virtual da aplicação.

3 Norma ISO (Formato de mensagens de transações financeiras) 8583

A ISO 8583 é o principal protocolo de comunicação de sistemas financeiros para transações de pagamentos eletrônicos (transações de cartão de crédito e débito). Foi criado pela Organização Internacional de Padrões (ISO), a qual tem por objetivo manter uma comunicação eficaz, com um uma informação sucinta, protocolado e padronizado nos diversos sistemas financeiros do mundo (ISO 8583, 2003). O objetivo da ISO é padronizar a comunicação entre os sistemas. O protocolo consiste de manter a rastreabilidade da informação em todo fluxo transacional. A ISO permite o controle por meio de um código de controle de filiação saber quais as instituições financeiras participantes possuem um número de filiação e controle, tendo a rastreabilidade da informação trafegada em todas as instituições participante da transação.

A ISO é formada por vários *bytes* a fim de manter uma troca concisa de informações sistêmicas entre as instituições, contudo existem alguns *bytes* iniciais que determinam e classificam uma transação, o primeiro é o indicador da mensagem (em inglês MTI [*Message Type Indicator*]), formado por 4 bits. Conforme a Tabela 4.

MTI	
Conteúdo do BIT	**Significado**
0XXX	**Versão da ISO 8583**
X0XX	**Classificação da mensagem**
XX0X	**Função da mensagem**
XXX0	**Quem está se comunicando**

Tabela 1: Significado de cada byte do MTI

Fonte: ISO 8582, 2003

No primeiro bit nós temos a versão da ISO, conforme a versão implementada em 1987, algumas empresas como o caso da PRODESP (PRODESP**,** 2007) e do Banco Postal (Banco Postal, 2011). No entanto a mesma possui três variações como o objetivo de determinar como será feito a troca de mensagens informando a sua versão. Na tabela 5, temos as possíveis versões que podem ser utilizadas para realização de uma transação financeira utilizando a ISO 8583.

Posição	Significado
0xxx	ISO 8583:1987
1xxx	ISO 8583:1993
2xxx	ISO 8583:2003

Tabela 2 – Variação do bit 1 da MTI

Fonte: ISO, 2003

O segundo bit, tem como significado a classificação da mensagem, neste bit define-se qual a finalidade da troca da comunicação realizada, variando qual o objetivo da conexão a ser realizada, se é para envio de informações sobre uma transação financeira ou se é uma troca de arquivo entre duas ou mais instituições ou cobrança de taxas. Desta forma, a ISO 8583 varia de acordo com o objetivo da mensageria, a Tabela 6 exemplifica as variações que podem ser realizadas.

Posição	Significado
x0xx	Reservado para ISO
x1xx	Mensagem de autorização
x2xx	Mensagem Financeira
x3xx	Mensagem de arquivos
x4xx	Mensagem de reversão ou *chargeback*
x5xx	Mensagem de reconciliação
x6xx	Mensagem Administrativa
x7xx	Mensagem de *fee collection* (Ajuste financeiro)
x8xx	Mensagem de Rede
x9xx	Reservado para ISO

Tabela 3 – Significado do bit 2 do MTI

Fonte: ISO, 2003

O terceiro Bit possui como objetivo informar a função da troca de mensagens, visando o ponto de vista da origem da transação, o momento em que se envia a requisição e que se recebe a resposta. Tomando como exemplo uma requisição que o adquirente realiza com a bandeira do cartão de crédito, o sistema envia o bit preenchido xx0x e espera receber xx1x. Conforme Tabela 7 é possível exemplificar todas as possíveis funções deste elemento, para assim interpretar a resposta da transação.

Posição	Significado
xx0x	Requisição
xx1x	Resposta da requisição
xx2x	Aviso
xx3x	Resposta do Aviso
xx4x	Notificação
xx5x	Reconhecimento de notificação
xx6x	Instrução (ISO 8583:2003)
xx7x	Reconhecimento da Instrução (ISO 8583:2003)
xx8x	Reservado para ISSO
xx9x	Reservado para ISSO

Tabela 4 – Significado do bit 3 do MTI

Fonte: ISO, 2003

O quarto bit, apresenta a origem da transação, ou seja, como a ISO irá identificar de quem é a propriedade da mensagem, se é o adquirente ou emissor e o complemento para total rastreabilidade, se é a primeira requisição ou se é uma retentativa de comunicação. Com base na Tabela 8 é possível verificar as possíveis variações do quarto bit.

Posição	Significado
xxx0	Adquirente
xxx1	Repetição Adquirente
xxx2	Emissor
xxx3	Repetição do Emissor
xxx4	Outro
xxx5	Repetição Outro

Tabela 5 – Significado do bit 4 do MTI

Fonte: ISO, 2003

Com a composição das informações citada na Tabela 2, Tabela 3 e Tabela 4, é possível gerar o primeiro bit, definição da mensagem e o seu objetivo na troca de informações entre os sistemas das empresas participantes da ISO 8583. Na Tabela 9 são apresentados alguns exemplos da composição do MTI (M*essage Type Indicator*).

Message Type Indicator	Significado	Usado
0100	Requisição de autorização	Requisição executada de um POS para uma transação financeira
0110	Resposta da requisição	Resposta da requisição da transação financeira realizada por um POS
0120	Aviso de autorização	Quando um terminal POS quebra e precisa ser enviado um aviso de compra
0121	Repetição de aviso de autorização	Ocorre quando a primeira requisição sofre time out

Tabela 6 – Exemplos do MTI

Fonte: ISO, 2003

Com a composição para geração do cabeçalho da mensagem, é possível gerar uma transação financeira, portanto pode-se dizer que o bit 1 é o MTI (*Message Type Indicator*) de uma transação. Os bits da ISO são compostos de variáveis, alguns são variáveis numéricas onde trafegam apenas números no campo, outras são

hexadecimal onde são trafegados letras e números. As definições de variáveis têm como função construir os mapas de bits, para que as empresas que irão utilizar a ISO (Adquirente; Emissor; Software *House*; Bandeira) consiga interpretar as informações trafegadas. As variáveis da ISO podem ser compostas da seguinte maneira:

- Numérico (n);
- Alfanumérico (ans);
- Valores (x+n);
- Byte (b); e
- Rastreio (z).

Com base nesta variação de definição, a Tabela 10 exibe a definição dos campos conforme a ISO.

Campo	Tipo	Usado
2	n ..19	Cartão
3	n 6	Código do processo
4	n 12	Valor da transação

Maiores detalhes dentro do Apêndice 1 deste trabalho

Existem as definições especiais, como o campo de rastreio (z), esse campo determinado pela ISO 8583, tem como objetivo rastreio e auditoria da informação por ele trafegado, este campo é reservado para trilha 1 e trilha 2 dos cartões.

Assim como *header* e complemento do MTI, existe o *processing code* (Código do Processo) na qual auxilia a definição de transação, conforme definição especifica da ISO presente na Tabela 11.

Transação	MIT	*Processing code*
Autorização	100	**00 a0 0x**
Balanço de inquérito	100	**31 a0 0x**
Venda	200	**00 a0 0x**
Dinheiro	200	**01 a0 0x**
Estorno	200	**02 a0 0x**
Complemento de mobile	200	**57 a0 0x**

Tabela 8 – Variação do *Processing Code*

Fonte: ISO, 2003

A Estrutura da ISO é formada pelo cabeçalho da mensageria (*Header*) que tem por objetivo enviar os primeiros bits do cabeçalho (podendo ser enviado o IP de origem ou data, variando de acordo com o contrato das duas empresas). O *Message Type Indicator* (MTI), a primeira camada de bits (inicia no bit 001 e vai ate o bit 064) chamados (*Primary Bitmap*), a segunda camada de bits (inicia no bit 065 e vai ate o bit 128) chamados (Secondary Bitmap) e o conteúdo da informação da mensageria (*Message Data Fields*). Conforme ilustrado na Figura 19.

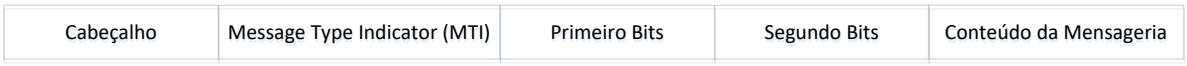
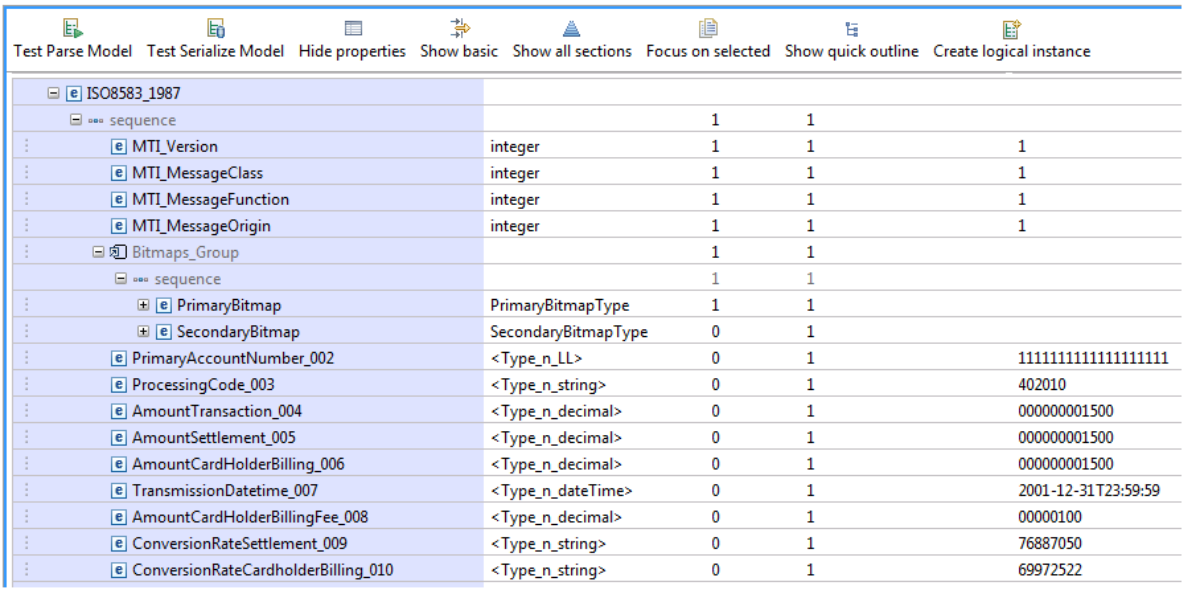


Figura 17 Arquitetura ISO 8583

Fonte: IBM, 2016

Quando é gerado a comunicação de transação entre as empresas financeiras, seguem a estrutura definida pela ISO 8583. O objetivo da transação, define-se através do MTI, na qual possui como objetivo a troca de informações entre duas empresas financeiras. O conteúdo da mensageria pode ser diferenciado, com alguns bits obrigatórios e outros não. A Figura 20 apresenta um exemplo fornecido pela IBM da ISO 8583 em um separador e mapa de bits.



Test Parse Model | Test Serialize Model | Hide properties | Show basic | Show all sections | Focus on selected | Show quick outline | Create logical instance

ISO8583_1987				
sequence		1	1	
MTI_Version	integer	1	1	1
MTI_MessageClass	integer	1	1	1
MTI_MessageFunction	integer	1	1	1
MTI_MessageOrigin	integer	1	1	1
Bitmaps_Group		1	1	
sequence		1	1	
PrimaryBitmap	PrimaryBitmapType	1	1	
SecondaryBitmap	SecondaryBitmapType	0	1	
PrimaryAccountNumber_002	<Type_n_LL>	0	1	1111111111111111111
ProcessingCode_003	<Type_n_string>	0	1	402010
AmountTransaction_004	<Type_n_decimal>	0	1	000000001500
AmountSettlement_005	<Type_n_decimal>	0	1	000000001500
AmountCardHolderBilling_006	<Type_n_decimal>	0	1	000000001500
TransmissionDatetime_007	<Type_n_dateTime>	0	1	2001-12-31T23:59:59
AmountCardHolderBillingFee_008	<Type_n_decimal>	0	1	00000100
ConversionRateSettlement_009	<Type_n_string>	0	1	76887050
ConversionRateCardholderBilling_010	<Type_n_string>	0	1	69972522

Figura 18 Exemplo de transação no modelo da ISO 8583

Fonte: IBM, 2016

3.1 Transação de *Referral* em um POS

Uma transação de *eletronic referral* é um tipo de transação que possui como propósito mitigar as fraudes em transações financeiras de cartões de crédito. A transação consiste no envio das informações financeiras e depois uma confirmação dos dados do portador do cartão para conclusão da compra. A Transação de *eletronic referral* é atividade de acordo com o produto do cartão e o emissor. Ao informar o valor de uma venda e inserir o cartão para transacionar, o POS envia as informações da transação para a bandeira realizar a aprovação que por sua vez envia para o emissor, no retorno da transação o emissor envia a informação que deve ser questionada ao portador. O POS traduz a mensagem e questiona para o portador através do *display* do POS, com a resposta, o POS envia os dados ao emissor que retorna se a informação esta correta ou incorreta. Para exemplificar serão utilizadas empresas fictícias no processo da transação de *eletronic referral*, enviando todas as mensagens, com detalhes dos bits da ISO 8583, geradas desde a interação do portador com o terminal até a ultima resposta que é enviada para o terminal com objetivo de demonstrar no *display* do POS, portanto os nomes das empresas serão:

- POSFast – Como fornecedora de POS;
- CapturaCartão – Como Adquirente;
- CardSupreme – Como Bandeira; e
- DinheiroRapido – Como Emissor.

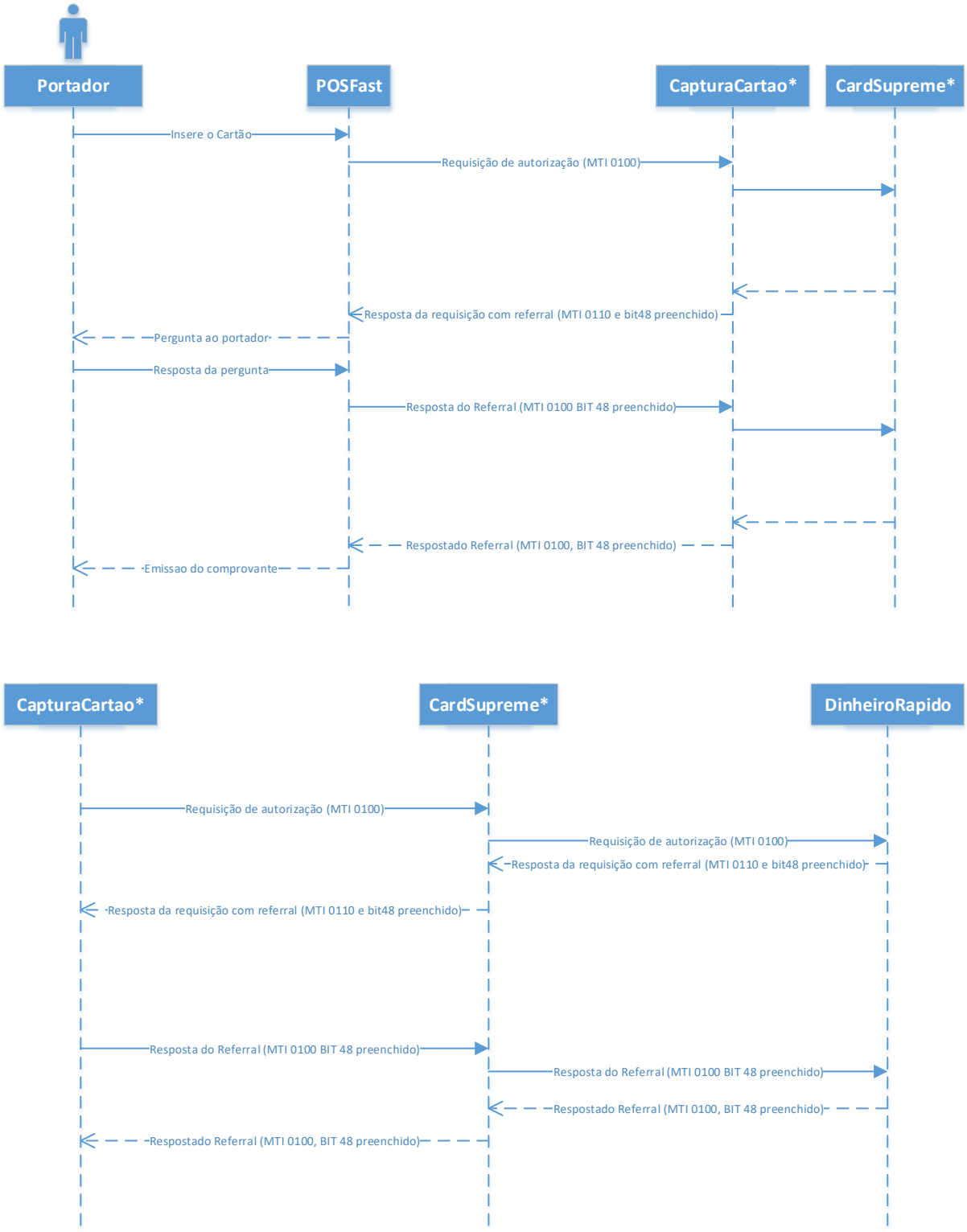


Figura 19: Envio de informações em uma transação *Referral* no POS

Fonte: Autoria Própria

Uma transação de *eletronic referral* negada ocorre quando o portador digita a resposta incorreta para o POS. O adquirente recebe a informação que por sua vez envia para bandeira que por fim entrega ao emissor; este informa dentro do bit 48 da

ISO8583. No exemplo ilustrado na Figura 16, um *byte* que a informação esta incorreta. Ao chegar no terminal POS, o sistema apresenta transação negada e o POS envia uma reversão para o emissor a fim de devolver o saldo ao cartão. A Reversão é enviada ao emissor que por sua vez efetiva o retorno do saldo ao portador, evitando qualquer ônus no saldo financeiro. Na Figura 16 o mesmo contexto de empresas participantes para realização de uma transação utilizado na Figura 15 é empregada para a apresentação de uma transação de *eletronic referral* com reversão no terminal por conta de uma informação do *referral* inserida de maneira incorreta.

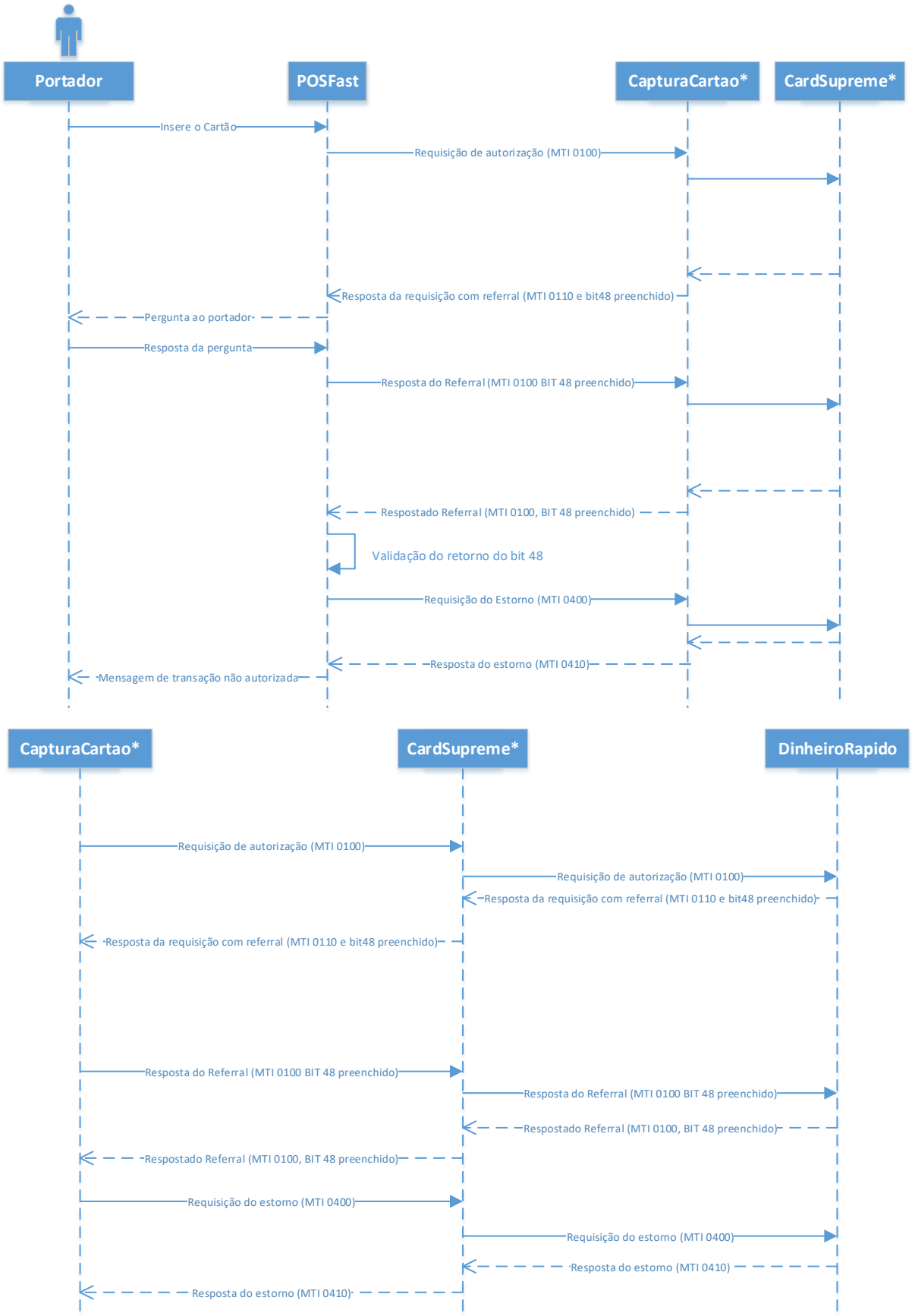


Figura 20: Trafego de uma transação de *referral* negada no POS
Fonte: Autoria Própria

Com a troca de mensagens entre as empresas é gerado empregando a ISO 8583, de uma transação comum, no retorno do emissor o bit 48 com seus sub elementos, sub elemento é a definição de uma posição definida dentro de um bit, um bit pode possuir N sub elementos, de acordo com a especificação da ISO 8583, portanto em uma transação de referral o bit 48 é preenchido conforme especificação elaborada pela CapturaCartão (Adquirente) e DinheiroRapido (Emissor). Conforme definição na Tabela 1:

BIT 48 Sub elemento 1	Definição
0	Transação Financeira
1	Consulta de *Referral*

Tabela 9: Sub elemento 1 do BIT 48 – Definição de consulta referral, CapturaCartão

Fonte: autoria própria

O subelemento 8 do bit 48 é a variável de questões oriundas do emissor, são apresentados 5 exemplos para este trabalho, no entanto as combinações variam em 30 maneiras diferentes. Conforme Tabela 2.

BIT 48 Sub elemento 8	Definição
U	CPF
F	Data de nascimento
T	RG
A	Nome da Mãe
C	Placa do Carro

Tabela 10: Sub elemento 8 do BIT 48 – Definição das questões de *referral*

CapturaCartão

Fonte: autoria própria

Conforme a Tabela 3 o retorno oriundo do emissor ao se enviar a resposta do questionamento do sub elemento 9, este retorno determina se a transação de *eletronic referral* obteve todas as suas informações corretamente preenchidas ou não. Com esta informação o meio de captura esta apto para realizar o estorno da venda em caso de retorno negativo.

BIT 48 Sub elemento 9	Definição
N	Nada coincidem
B	Dados Compatíveis
Z	Consulta Indisponível

Tabela 11: Sub elemento 9 do BIT 48 – Definição de retorno de consulta de *Referral*, CapturaCartão

Fonte: autoria própria

Para a empresa CapturaCartão é possível detalhar a mensagem trocada, utilizando como exemplo o mínimo necessário para aprovação de uma transação na mensageria ISO8583 usando a especificação esperada pela CardSupreme (Bandeira).

Mensagem de requisição:

<field id="0" value="0100"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="00000000000000"/>
<field id="63" value="WRSTE45587"/>

Mensagem de resposta:

<field id="0" value="0110"/>

<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="37" value="0001228546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="48" value="0000000**U**000000"/>
<field id="63" value="WRSTE45587"/>

Sendo o retorno **U** do emissor a pergunta para “Qual o CPF do portador do cartão” conforme definição entre DinheiroRapido (Emissor) e CapturaCartão (Adquirente). Com a inserção da resposta é enviado uma nova requisição para o emissor inserindo a informação dentro do bit 48.

Mensagem de Requisição:
<field id="0" value="0100"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=2110110$¨%$#%000015324"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="43" value="SAO PAULO BRA"/>

<field id="48" value="**1**000000**U**000000"/>
<field id="63" value="WRSTE45587"/>

Mensagem de Resposta:
<field id="0" value="0110"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="37" value="0001328546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="48" value="0000000**UN**00000"/>
<field id="63" value="WRSTE45587"/>

O Retorno **N** do emissor na definição da DinheiroRapido (Emissor) e CapturaCartão (Adquirente) seria dados não coincidem. Automaticamente o terminal enviaria a requisição de reversão da transação, conforme exemplo:

Requisição:
<field id="0" value="0400"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201221"/>
<field id="11" value="101216"/>
<field id="14" value="2110"/>

<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="00000000000000"/>
<field id="63" value=" WRSTE45587"/>
<field id="90" value="0100101214000000001018201021"/>

Mensagem de Resposta:
<field id="0" value="0410"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201221"/>
<field id="11" value="101216"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="37" value="0001248546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="48" value="00000000000000"/>
<field id="63" value="WRSTE45587"/>
<field id="90" value="0100101214000000001018201021"/>

O Papel da CardSupreme (Bandeira) neste tipo de transação, consiste as validações apenas da requisição da transação financeira e na requisição de estorno, para a consulta *de referral transaction* a bandeira entende que é uma nova requisição e envia para o emissor, sem executar nenhuma validação ou intervenção no tipo diferencial da transação.

4. Análise comparativa dos meios de captura

A transação de *Referral* pode ser implementada em diferentes meios de captura, os quais serão discutidos neste trabalho para as transações de autorização financeira, pois, sua especificação altera apenas no conteúdo do mapa de bits (ISO 8583). No entanto este tipo de transação não é utilizado em todos os canais de captura. Um canal de captura tem por definição o meio por onde é realizado a transação (Redecard, 2010) no caso deste trabalho focando no (TEF, POS, E-Commerce e Mobile) no entanto existem outros meios como URA (Telefone), Arquivo Eletrônico, Papel, Leitor de trilha, ATM (Caixa eletrônico bancário).

Assim, o objetivo desta análise é apresentar a comparação e mensurar o grau de dificuldade de implementação entre os canais de captura para possível utilização nos meios de captura citados neste trabalho.

4.1 Transferência Eletrônica de Fundos (TEF)

A TEF possui a grande maioria de funcionalidades que um POS (Executar venda, estornar, emitir comprovante, executar recarga de celular, etc) pode ter, logo, uma transação feita na máquina POS pode transacionar no TEF sem problemas, isso é possível por conta de uma tecnologia chamada POS TEF (Auditor, 2016). O TEF existe por conta de nichos de mercado e da necessidade do governo por fiscalizar a movimentação de transações financeiras nos lojistas, pois, o TEF possui uma funcionalidade que não existe no POS atual. Uma funcionalidade importante que é a vinculação da venda em conjunto com o comprovante fiscal, atendendo os tributos federais, estaduais e municipais (Bematch, 2017).

O TEF diferente do POS possui algumas empresas para efetivar a transação, além das já conhecidas na cadeia (Lojista, Adquirente, Bandeira, Emissor), as empresas adicionais são, a *Software House* e o Integrador (Auditor, 2016). O Integrador tem como função instalar o *software* no lojista e realizar a comunicação com o *Software House*, ficando também como responsável pela versão do *checkout*, atualização do sistema operacional e controle da licença instalada no lojista. A *Software House* por sua vez, tem como objetivo certificar os integradores que estão utilizando os seus sistemas, concentrar as transações e enviar para o adquirente via conexão X25. A *Software House* também pode auxiliar no controle de transações, gerenciamento de

cartões de fidelidade e o processo de multiadquirencia, ou seja, envio de uma mesma transação para varias adquirentes.

Todas as transações são realizadas no *checkout*, termo intitulado para o ponto de venda onde se é feito o registro da compra, pagamento e emissão do cupom fiscal (Definição de TEF, 2016), dependendo do cliente. Um cliente pode possuir um ou mais *checkouts*. Na Figura 21 tempos ilustrado dois pontos de vendas com os pinpads e impressoras fiscais conectados ao servidor da aplicação do TEF.

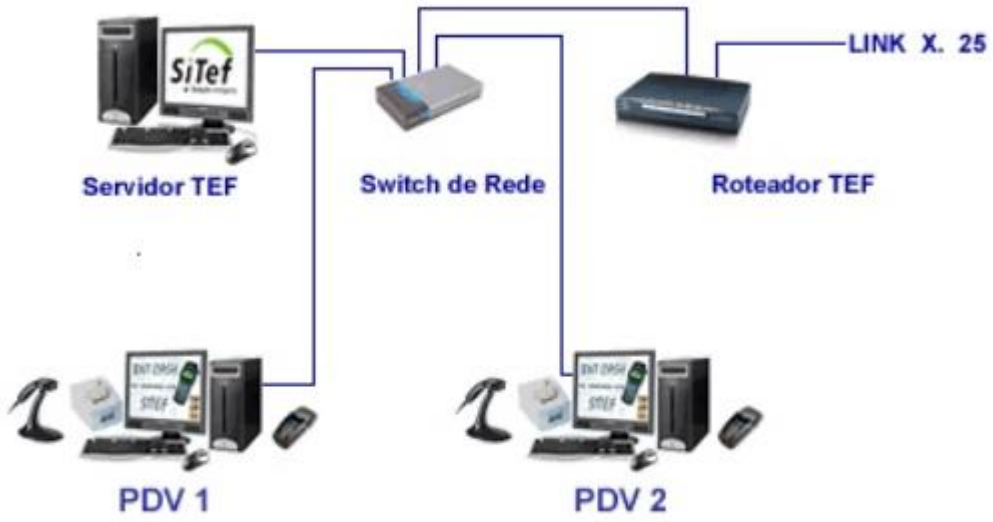


Figura 21 Exemplo do *checkout* de uma loja com a tecnologia de TEF

Fonte: Auditor, 2016

A Chave de criptografia de cada transação esta baseado na chave do terminal, semelhante ao que existe no POS, onde cada pinpad possui sua chave de criptografia para realização de uma transação, no entanto fica a definição do lojista qual tipo de cifragem ele pode utilizar em conjunto com a *software house*.

4.1.1 Transação de *eletronic referral* no TEF

Para que uma transação de *eletronic referral*, possa ser efetivada, o mesmo comportamento de tratativa de resposta que é adotada no POS precisa ser adotado no TEF. Para que este cenário possa ser realizado, as empresas integradoras de *Software House* precisam implementar esta tratativa. Para a *Software House* a implementação seria o tratamento da ISO 8583, trafegada com a adquirente nos seus múltiplos canais, tratando a resposta oriunda do adquirente e preparar o canal

para reversão da transação, além de habilitar o serviço oferecido para o cliente. Para a integradora, a empresa precisa da licença da *Software House* e deve implementa-la ao serviço do cliente e preparar o sistema para trocas de mensagens financeiras (autorização de crédito e débito), bem como no serviço de questionamento ao cliente.

No TEF o formato da ISO 8583 é empregado da mesma forma que no POS. A diferença se encontra apenas na interface com o lojista, pelo lado bandeira e emissor, não existe diferença, mantendo o mesmo formato de mensageria. Para exemplificar um cenário de aplicação será utilizado empresas fictícias a fim de melhor apresentar o papel e responsabilidade de cada empresa envolvida no processo:

- IntegraFacil – Integrador da automação comercial

A loja executa a requisição de venda para o servidor interno responsável pela realização da transação, integrada via IntegraFacil, esta requisição de transação pode ser feita da maneira definida pelo integrador e lojista, porem comumente é utilizado o protocolo da ISO 8583. O servidor concentra as informações e envia para a *Software House* com as informações de uma transação do serviço de *eletronic referral*.

Para os clientes com um maior volume de transações e com um maior aporte financeiro, é aplicado um *firewall* na saída do servidor da aplicação do lojista para o *link* da *Software House*, a fim de incluir uma camada de segurança nas informações enviadas e recebidas.

A Figura 22 apresenta um exemplo de modelo da infraestrutura de um lojista com três *checkouts*, com troca de mensagens utilizando a ISO 8583 em todas as pontas da cadeia.

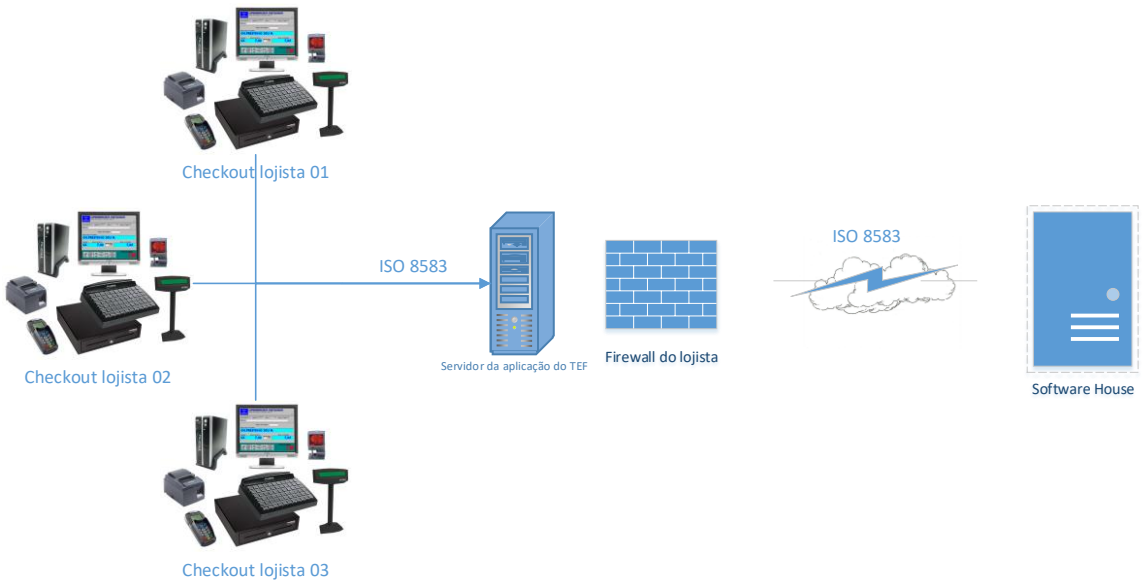


Figura 22 Estrutura do TEF para realização de transações

Fonte: elaborado pelo próprio autor

O pinpad precisa tratar tanto o recebimento do questionário, conseguindo exibir de maneira legível para o portador, como o tratamento da resposta, possibilitando a inserção de caracteres alfanuméricos. Como exemplo a Figura 23 apresenta o protótipo da exibição do questionamento e da inserção da resposta que o portador possa incluir no momento de uma transação realizada em algum meio de captura.

Figura 23 Fases da transação de *referral* em um Pinpad

Fonte: elaborado pelo próprio autor

A *Software House* por sua vez envia a requisição para adquirente de uma maneira semelhante a que um POS envia para a Adquirente, com o adicional apenas do bit 24, o *NII* (*Network International Identifier)* em português, rede de identificação internacional), com base neste bit a Adquirente consegue identificar na troca de mensagens qual a origem da transação.
A mensagem de uma transação financeira é desta forma.

Requisição do adquirente para a bandeira:

<field id="0" value="0100"/> → MTI da transação
<field id="2" value="5555555555555555"/> → Cartão
<field id="3" value="03000"/> → Requisição de credito
<field id="4" value="9999999999999"/> → Valor da transação
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/> → Validade do cartao
<field id="22" value="0051"/> → Metodo de entrada do cartao
<field id="24" value="251"/> → NII
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="00000000000000"/>
<field id="63" value="PVSTE45287"/>

Resposta da bandeira para o adquirente:

<field id="0" value="0110"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/>

<field id="22" value="0051"/>
<field id="24" value="251"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="37" value="0001228546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="48" value="0000000**C**000000"/>
<field id="63" value=" PVSTE45287"/>

Com cadastrado no emissor as mensagens variam de acordo o **C** do emissor a pergunta para “Placa do carro do portador do cartão” conforme definição entre DinheiroRapido (Emissor) e CapturaCartão (Adquirente). Com a inserção da resposta é enviado uma nova requisição para o emissor inserindo a informação dentro do bit 48.

Requisição do PinPad para o Adquirente:

<field id="0" value="0100"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=21101100¨%$%*000015324"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="**1**000000**U**000000"/>
<field id="63" value="WRSTE45587"/>

Resposta do Adquirente para o PinPad:

<field id="0" value="0110"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="37" value="0001328546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value="TERMINAL"/>
<field id="42" value="Filiação"/>
<field id="48" value="0000000**UB**00000"/>
<field id="63" value="WRSTE45587"/>

Sendo o B conforme Tabela 2, os retornos de dados coincidem, para que o processo seja concluído, o tratamento da mensagem tem que ser feito pela automação comercial, pois o *checkout* do lojista necessita das informações para exibir as informações necessárias no *display* do PinPad.

4.2 Transação Mobile

Transações *mobile*, são caracterizadas desta forma as transações realizadas através de um dispositivo móvel (Bacen, 2010). Os dispositivos móveis utilizados no contexto de pagamento *mobile*, são *tablets*, celulares ou celulares digitais. As transações de *mobile* surgiram com uma alternativa de menor custo para o lojista, sem a necessidade de pagar aluguel no dispositivo POS e no TEF, assim ele (lojista) poderia realizar transações financeiras com uma maior facilidade e mobilidade (Exemplo: Taxista), sem utilizar o pagamento com um POS ou um TEF.

Para a transação de *mobile* são necessários dois atores, sendo eles: o dispositivo de captura dos dados de cartão e o agente de gerenciamento de conexão (exemplo: celular ou *tablet*). O dispositivo de captura é conectado ao celular e este utiliza a rede para enviar dados para a adquirente, por meio da conexão da Internet do dispositivo. A conexão do dispositivo de captura com o agente de conexão varia de modelo para modelo, como por exemplo, os tipos fornecidos pelas empresas (Izettle, Mercado pago e Payeleven) aos lojistas Brasileiros, onde o meio de conexão pode ser Bluetooth ou entrada de fone do dispositivo (P2).

O protocolo de transferência entre o dispositivo de captura para o agente de conexão varia de empresa para empresa, podendo ser binário, ou em uma estrutura XML. Após o recebimento das informações o agente de conexão gera a mensagem de acordo com a ISO 8583 cifrada, de acordo com a exigência do PCI e envia para adquirente através de um canal da Internet. Os comprovantes das compras são exibidos de diferentes meios, dependendo da empresa que fornece serviço, em geral as duas possibilidades são o envio do comprovante da compra por meio de SMS para o portador cadastrado no ato da compra ou para o e-mail do portador, também cadastrado no ato da compra.

A Adquirente trata a transação semelhante a tratativa de um POS, utilizando o bit 42 e bit 41 para identificação da transação *mobile*. A Figura 24 ilustra uma transação financeira oriunda de um dispositivo móvel e enviado para o Adquirente.

Figura 24 Estrutura mobile para realização de transações,

Fonte: Elaborado pelo próprio autor

4.2.1 Transação de *eletronic referral* no mobile

Para o *mobile* uma transação de *eletronic referral* tem o comportamento semelhante a de um POS visando o lado Adquirente, pois a estrutura da ISO 8583 seria

semelhante diferenciando apenas o conteúdo dos bits 42 e bit 41. As transações de *eletronic referral* no *mobile* ocorreriam de uma forma semelhante as demais tecnologias, no entanto, o agente administrador teria uma função adicional de tratar as mensagens de retorno negativo, pois ficaria a cargo do agente montar a mensagem do estorno e enviar para o adquirente.

Para os *devices* sem *display* eletrônico, onde a transação possui uma maior dependência do agente, o modelo de *eletronic referral* não é adequado, pois, o agente teria que fazer uma interpretação do retorno do adquirente no próprio aplicativo, item que tem que estar transparente e ser tratado no dispositivo.

O caso de uma transação negativa para o portador quanto para o lojista é totalmente transparente, sendo exibida no agente de comunicação como transação negada e no dispositivo de captura, transação não autorizada.

Empegando as mesmas empresas DinheiroRapido como emissor e CapturaCartão como adquirente na exibição da mensagem padrão ISO 8583 para pagamento *móbile*, segue exemplo de troca de mensagens.

Mensagem de Requisição do *mobile* para o Adquirente:

```
<field id="0" value="0100"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="41" value="MOBILE"/>
<field id="42" value="MOFILIAC"/>
<field id="43" value="SAO PAULO  BRA"/>
<field id="48" value="00000000000000"/>
<field id="63" value="WRSME45587"/>
```

Mensagem de Resposta recebida pelo Adquirente para o mobile:

<field id="0" value="0110"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="37" value="0001228546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value="MOBILE"/>
<field id="42" value=" MOFILIAC"/>
<field id="48" value="0000000**T**000000"/>
<field id="63" value="WRSME45587"/>

Sendo o retorno **T** do emissor a pergunta para o portador “Qual o RG do portador do cartão” conforme definição entre DinheiroRapido (Emissor) e CapturaCartão (Adquirente). Com a inserção da resposta é enviado uma nova requisição para o emissor inserindo a informação no bit 48

.

Mensagem de Requisição do Mobile para o Adquirente:

<field id="0" value="0100"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000&¨%&00015324"/>

<field id="41" value=" MOBILE "/>
<field id="42" value=" MOFILIAC"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="**1**000000**U**000000"/>
<field id="63" value=" WRSME45587"/>

Resposta do Adquirente para o Mobile:

<field id="0" value="0110"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=211011000000000015324"/>
<field id="37" value="0001328546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value=" MOBILE"/>
<field id="42" value=" MOFILIAC"/>
<field id="48" value="0000000**UN**00000"/>
<field id="63" value=" WRSME45587"/>

O Retorno **N** do emissor na definição da DinheiroRapido (Emissor) e CapturaCartão (Adquirente) seria dados não coincidem. Automaticamente o agente enviaria a requisição de reversão da transação, conforme exemplo:

Mensagem de Requisição:

<field id="0" value="0400"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>

<field id="4" value="9999999999999"/>
<field id="7" value="1018201221"/>
<field id="11" value="101216"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=21101100000000000015324"/>
<field id="41" value=" MOBILE"/>
<field id="42" value=" MOFILIAC"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="00000000000000"/>
<field id="63" value=" WRSME45587"/>
<field id="90" value="0100101214000000001018201021"/>

Mensagem de Resposta:

<field id="0" value="0410"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201221"/>
<field id="11" value="101216"/>
<field id="14" value="2110"/>
<field id="22" value="0051"/>
<field id="35" value="5555555555555555=21101100000000000015324"/>
<field id="37" value="0001248546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value=" MOBILE"/>
<field id="42" value=" MOFILIAC"/>
<field id="48" value="00000000000000"/>
<field id="63" value=" WRSME45587"/>
<field id="90" value="0100101214000000001018201021"/>

Em paralelo a mensagem ISO 8583 é enviado para a Adquirente o dispositivo de conexão tem etapas de mudança com interação do portador no envio da transação, sendo elas:

- Primeira Etapa: onde esta aguardando o portador incluir a senha no dispositivo de captura;
- Segunda Etapa: no aguardo do retorno da adquirente e tratamento do *referral*, ou seja, caso a transação retorne que os dados inseridos pelo portador estejam incorretos, o agente manterá esta mensagem como aguardando retorno do emissor; e
- Terceira Etapa: a transação é aprovada nos dois passos ou a transação é negada. Na Figura 25 é ilustrado o protótipo do agente gerenciador das três etapas.

Etapa 1 – Aguardando o preenchimento da senha.

Etapa 2 – Aguardando retorno da consulta de *referral*.

Etapa 3 – Retorno da transação.

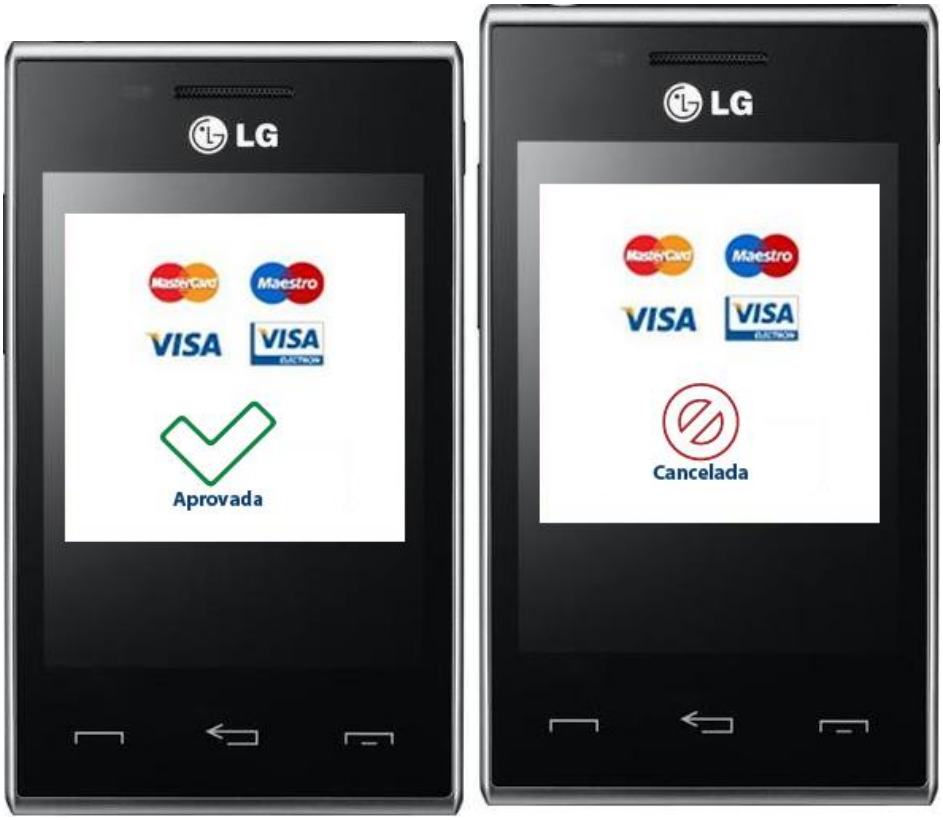


Figura 25: Protótipo de exemplificação do agente de conexão

Fonte: elaborado pelo próprio autor

Para que o agente possa realizar a execução do *eletronic referral*, o dispositivo de captura da venda tem que prover os dados de captura. Apresentando como exemplo de um protótipo a Figura 26 de como o dispositivo de captura efetuas as interações do portador do cartão.

- Na primeira etapa o *device* de captura questiona o portador para realização da transação de *referral*;
- Na segunda etapa ocorre a inserção da resposta; e
- Na terceira etapa ocorre o retorno do emissor para a transação.

Etapa 1 – Questionamento do *Eletronic Referral.*

Etapa 2 – Inserção da Resposta.

Etapa 3 – Retorno da transação.

Figura 26 Protótipo de exemplificação do *device* de captura

Fonte: elaborado pelo próprio autor

4.3 Transação de *E-Commerce*

Transação de *e-commerce*, são transações na qual o portador não está presente, também conhecidas como transações realizadas pelo canal da Internet (Batha, Tej; 2003). Estas transações oriundas do canal de *e-commerce* possuem algumas características diferentes dos outros canais citados anteriormente, pois, em todas as transações o portador não está presente, ou seja, a venda não precisa do cartão físico no meio de captura e nem mesmo da inserção de senha para sua efetivação.

Para a execução de uma venda empregando *e-commerce* o lojista pode executar a integração do canal de comunicação diretamente com a Adquirente ou com uma empresa facilitadora de pagamento como *gateway* ou plataformas. Os facilitadores de pagamento têm como função simplificar a integração com a adquirente além de fornecer serviços adicionais para o cliente como relatório de vendas, relatório de conversão, entre outros. Na Figura 27 são representadas as empresas participantes da cadeia de e-commerce, para realizar a venda é necessário apenas o quadrante de pagamentos, no entanto o lojista pode integrar com outros serviços para garantir a venda, como por exemplo, as empresas de soluções anti fraude.

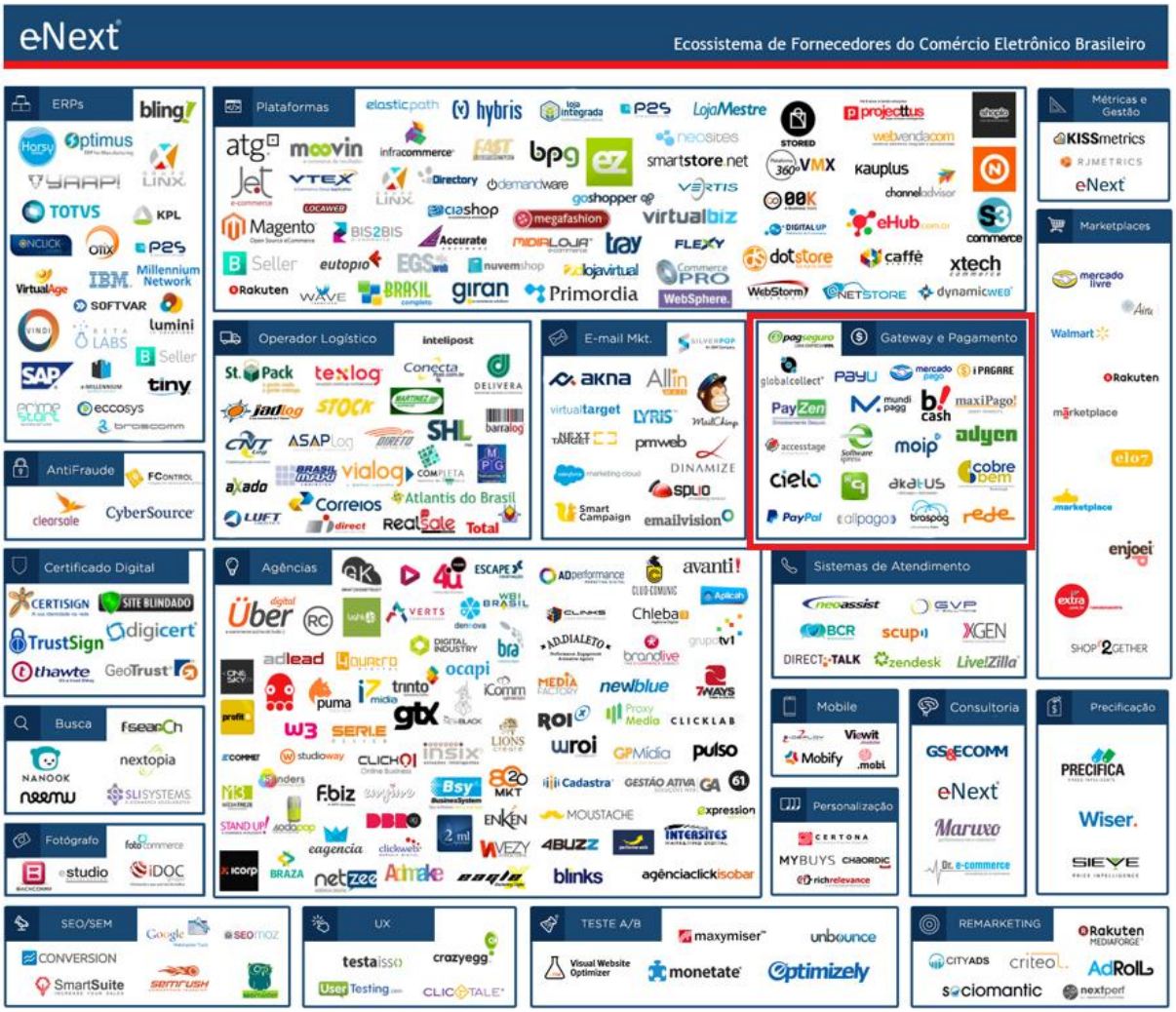


Figura 27: Ecossistema do E-Commerce brasileiro
Fonte: Enext, 2017

Para as transações de *e-commerce*, o lojista se integra com os facilitadores ou com os Adquirentes empregando o *XML* (e**X**tensible **M**arkup **L**anguage) ou com o *Rest* (**Re**presentational **S**tate **T**ransfer), variando a definição de cada empresa. A partir desta comunicação o lojista envia a transação com os dados do cartão do portador para efetivação da venda. Após o envio das informações, o sistema aguarda o retorno do adquirente de maneira síncrona em um tempo curto de resposta, pois, o lojista tem como premissa de aguardar o retorno da adquirente enquanto o portador está na página de pagamento aguardando um retorno, diferente dos outros meios de captura, o portador pode fechar a página de pagamento e ir para outra loja, abandonando a transação.

Todas as informações são trafegadas pelo canal da Internet até o endereço do adquirente ou do *gateway*, onde o retorno é executado em poucos segundos no endereço de origem do cliente, exibindo o retorno tanto para o lojista quanto para o portador. A Figura 28 ilustra um exemplo do modelo de pagamento de *e-commerce* com as duas integrações, a feita diretamente com a Adquirente e com a facilitadora de pagamento com a intermediaria.

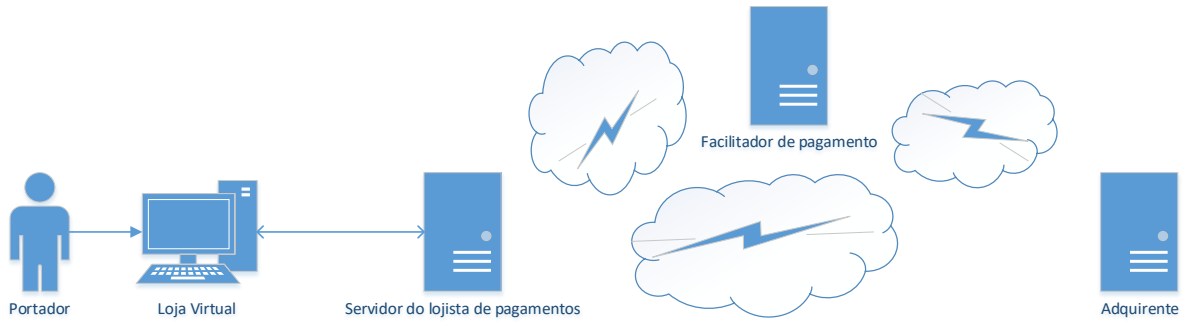


Figura 28: Integração de pagamento de um e-commerce
Fonte: Gateway de pagamento, 2017

As informações trafegadas podem ser executadas através do canal comum da Internet, ou seja, sem nenhuma cifragem ou utilizando um canal seguro cifrado por uma empresa terceira. A segurança do trafego das informações são baseados de acordo com a integração do lojista com o Adquirente ou com o *gateway*.

4.3.1 Transação de *eletronic referral* no E-Commerce

Para o *e-commerce* uma transação de *eletronic referral* teria o comportamento diferente dos outros meios de captura visando o lado adquirente, pois a estrutura da

ISO 8583 teria diferença dos bits 42 e bit 41 alem do bit 22 (*Entry mode*) que teria o valor fixo de 810 mitigando o bit 35 que é a trilha do cartão, pois, o cartão não foi capturado por meio magnético e sim digital, o código 810 significa transações eletrônicas (ISO 8583, 2003). Caso o cliente tenha algum facilitador de pagamento, o mesmo deverá estar preparado para receber os retornos do adquirente para tratar o questionamento que será feito para o portador do cartão, semelhante processo com o TEF e as S*oftware House*. A diferença é que a *Software House* trataria a ISO 8583, o facilitador teria de tratar o retorno em XML ou REST do adquirente. O lojista terá que criar o formulário para apresentação do questionário para o cliente, para que o portador inclua as informações que o emissor esta solicitando para executar a transação de *referral*. O sistema que trataria o retorno para montar o estorno em caso de retorno negativo seria a própria adquirente, pois, se fosse aberto um novo serviço para o lojista executar aumentaria o tempo de conclusão da transação.
Para ilustra é apresentado o exemplo de uma requisição ISO 8583 uma transação oriunda do canal de e-commerce com a execução do serviço de *referral*, utilizando o mesmo cenário de empresas fictícias, as empresas DinheiroRapido como emissor e CapturaCartão como adquirente na exibição da ISO para pagamento *e-commerce*.

Requisição da Loja para Adquirente:

```
<Ecommerce>
<LojaFeliz>
<Filiacao>12335</Filiacao>
<Cartao>5555555555555555</Cartao>
<valor>9999999999999</valor>
<parcelas>0</parcelas>
</LojaFeliz>
</Ecommerce>
```

Requisição da Adquirente para Bandeira:

```
<field id="0" value="0100"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
```

<field id="4" value="9999999999999"/>
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/>
<field id="22" value="0810"/>
<field id="41" value="ECOMER"/>
<field id="42" value="ECFILIAC"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="00000000000000"/>
<field id="63" value="WRSEE45587"/>

Resposta da Bandeira para Adquirente:

<field id="0" value="0110"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201021"/>
<field id="11" value="101214"/>
<field id="14" value="2110"/>
<field id="22" value="0810"/>
<field id="37" value="0001228546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value=" ECOMER"/>
<field id="42" value=" ECFILIAC"/>
<field id="48" value="0000000**F**000000"/>
<field id="63" value=" WRSEE45587"/>

Sendo o retorno **F** do emissor a pergunta para “Qual a data de nascimento do portador do cartão” conforme definição entre DinheiroRapido (Emissor) e CapturaCartão (Adquirente), apresentando o seguinte conteúdo do XML.

<Ecommerce>

<LojaFeliz>
<Filiacao>12335</Filiacao>
<autorizacao>R12345</autorizacao>
<valor>9999999999999</valor>
<parcelas>0</parcelas>
<Pergunta>Qual a data de nascimento do portador do cartão</Pergunta>
</LojaFeliz>
</Ecommerce>

Com a inserção da resposta é enviado uma nova requisição para o emissor inserindo a informação dentro do bit 48 é gerada.

Requisição da loja para o Adquirente:

<Ecommerce>
<LojaFeliz>
<Filiacao>12335</Filiacao>
<autorizacao>R12345</autorizacao>
<valor>9999999999999</valor>
<parcelas>0</parcelas>
<Pergunta>Qual a data de nascimento do portador do cartão</Pergunta>
<resposta>01011990</resposta>
</LojaFeliz>
</Ecommerce>

Requisição do Adquirente para Bandeira
<field id="0" value="0100"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0810"/>

<field id="41" value=" ECOMER"/>
<field id="42" value=" ECFILIAC"/>
<field id="43" value="SAO PAULO BRA"/>
<field id="48" value="**1**000000**U**0##@00"/>
<field id="63" value=" WRSEE45587"/>

Resposta da Bandeira para o Adquirente:

<field id="0" value="0110"/>
<field id="2" value="5555555555555555"/>
<field id="3" value="03000"/>
<field id="4" value="9999999999999"/>
<field id="7" value="1018201121"/>
<field id="11" value="101215"/>
<field id="14" value="2110"/>
<field id="22" value="0810"/>
<field id="37" value="0001328546"/>
<field id="38" value="AUTORI"/>
<field id="39" value="00"/>
<field id="41" value=" ECOMER"/>
<field id="42" value=" ECFILIAC"/>
<field id="48" value="0000000**UB**00000"/>
<field id="63" value=" WRSME45587"/>

Resposta do Adquirente para loja:

<Ecommerce>
<LojaFeliz>
<Filiacao>12335</Filiacao>
<autorizacao>R12345</autorizacao>
<valor>9999999999999</valor>
<parcelas>0</parcelas>
<codigoderetorno>30<codigoderetorno>
<mensagem>Transacao nao autorizada<mensagem>

</LojaFeliz>
</Ecommerce>

O Retorno **B** do emissor na definição da DinheiroRapido (Emissor) e CapturaCartão (Adquirente) seria “dados coincidem”.

4.4 Análise comparativa da transação de *referral*

Após a apresentação dos meios de captura onde a transação de *referral* pode ser executada, será realizada a análise comparativa dos meios de captura apresentados (POS, TEF, Mobile, E-Commerce). Para a análise comparativa, será utilizado o meio de integração do lojista com a solução, o risco do tempo de resposta elevado em perder a venda, interação com o portador, características externas de conexão, e também se a cifragem é transparente ao lojista ou se precisa ser implementada na solução.

A Analise atende 3 pontos principais do mercado de pagamentos, Segurança, Infraestrutura e Experiência do Usuário. Sendo que o ponto de Infraestrutura foi quebrado em implementação da solução, conexão e tempo de resposta, pois segundo consultorias contratadas para avaliar as necessidades de melhoria de pagamentos, esses elementos representam 70%, os outros 30% são compostos por facilidades que o portador exige que vai contra as regras do PCI, como cadastro do cliente no meio de pagamento sem a necessidade de digitar a senha.

A análise será avaliada em quesito de soma de pontuação, por padrão todo impacto que possa existir para o lojista será adicionado 10 pontos de esforço e em paralelo os impactos que possa existir para o portador será adicionado 15 pontos de esforço.

O impacto no lojista ficou definido como 10 pontos, pois caso o lojista decida melhorar ou eliminar o problema relatado, o mesmo pode contratar uma consultoria e melhorar sem o impacto financeiro. O impacto no portador ficou definido como 15 pontos, pois caso o problema pontuado ocorra no momento da transação o portador pode desistir da compra causando impacto financeiro ao lojista.

Segundo algumas consultorias especializadas em pagamentos, alegam que a falta de investimento em um pagamento ágil e descomplicado para o portador pode aumentar o índice de perda de vendas em 18%, para o e-commerce este item chega ao limite de 43%.

4.4.1 Integração do Lojista

O método de integração do lojista refere-se ao esforço que o lojista precisa executar para poder existir uma integração com o Adquirente, podendo existir entrar os tipos de conexão (X25, *Ethernet e Wireless*) com a solução de infraestrutura. Este ponto

é relevante na comparação, pois, quando o Adquirente ou emissor alterar alguma parte da mensagem, existe o esforço do lojista com as empresas prestadoras ou o próprio lojista do tempo de implementação para usufruir do novo serviço. Dependendo da alteração que possa existir no meio de captura, a lojista precisa reexecutar a homologação do seu serviço com a Adquirente.

O Tratamento da mensagem ISO 8583 tem que ser compartilhada com todas as empresas que participarão da solução para o lojista, pois, todas tem que estar cientes dos bits obrigatórios e opcionais, bem como do tratamento do bit 48 para transações de *referral* e criação do método automático para realização de estorno caso a mensagem retorne informando dados não coincidem. O lojista também precisa integrar o estorno automático o MTI 0400 de estorno com o tratamento do bit 90, caso a empresa desconheças de realizar estes tratamentos de troca de mensagens, maior o risco da implementação também estar errada, causando transtornos ao portador e ao lojista.

Dependendo do numero de empresas envolvidas na entrega da solução uma nova implementação no serviço troca de mensagem torna-se mais complexo, consequentemente, aumentando o esforço de entrega do novo serviço. A Tabela 8 apresenta o número de empresas e a pontuação de 10 pontos por empresa intermediaria presente na solução de pagamentos, a pontuação é relativa a complexidade da integração.

Meio de integração do lojista com a solução	
Empresas necessárias	Pontuação
0	0
1	10
2	20
3	30

Tabela 12 – Pontuação pelo número de empresas para integração
Fonte: Elaborado pelo próprio autor

4.4.2 Tempo de resposta

O tempo de resposta é fator determinante de toda a transação, seguindo a especificação da CardSupreme tanto para DinheiroRapido quanto para CapturaCartão, é de um tempo de resposta de 120 segundos, no entanto o padrão de resposta é de ate 2 segundos. Devido a necessidade do mercado de transações

instantâneas, os lojistas esperam transações com um tempo mínimo de resposta. Utilizando o cenário de uma transação *E-Commerce*, onde o portador após o preenchimento dos dados do cartão, a loja demore um tempo superior a 40 segundos para retorno, consequentemente o portador fechará a janela para executar uma nova tentativa ou desistira da venda, associando ao tempo de resposta a imagem da loja. Utilizando o mesmo cenário em uma transação POS, o portador possui uma maior compreensão que a responsabilidade não e da loja e sim de fatores externos, sendo a possibilidade de executar uma nova tentativa superior ao de um *e-commerce.*

Uma nova implementação de serviço sem alterar o tempo de resposta está sujeita a causar impactos financeiros para o lojista, com base nesta premissa a Tabela 9 foi elaborado, apresentando o impacto do tempo. Pois é um fator determinante para perda de transação, logo a empresa que utilizar o serviço caso tenha uma solução de uma empresa precisa elaborar o software de leitura e requisição para o sistema seja performático, levando mais tempo para implementação, caso o meio de captura dependa apenas da adquirente, a mesma tem que deixar os sistemas internos do POS em total sincronia com o servidor da aplicação interno, aumentando a performance de pagamento, caso seja necessário, segundo estudo onde a premissa tem que ser uma transação autorizada em real time (Ferreira, 2017).

A pontuação de complexidade aumenta em 15 pontos, para os meios de pagamento onde o tempo de resposta seja necessária pois o lojista irá perder a confiança em utilizar este tipo de serviço, diminuindo o uso da transação tendenciado a não utilização.

O tempo de resposta pode fazer o lojista perder a venda	
Resposta	Pontuação
Não	0
Sim	15

Tabela 13 – Pontuação pelo tempo de resposta das transações
Fonte: Elaborado pelo próprio autor.

4.4.3 Experiência do Usuário

A experiência do usuário esta baseado na facilidade do portador do cartão digitar as informações que a transação de *eletronic referral* pode solicitar e a facilidade de

corrigi-las em caso de falhas. Baseado na dimensão das teclas de preenchimento e o método de inserção, utilizando o cenário do dispositivo móvel, onde as teclas são menores em comparação com um pinpad, logo dependendo do portador, se for uma pessoa de uma idade elevada com um óculo não apropriado, esta transação possivelmente não seria realizada, conforme análise realizada pela tecnoblog para usuários com problemas visuais (tecnoblog, 2017).

Os níveis de complexidade são quebrados em quatro níveis

- Simples: facilidade na inserção das informações onde o portador pode alterar o tamanho do zoom caso necessário, corrigir erros em apenas um comando;
- Médio: botões com tamanho de no mínimo três centímetros, botões de cores diferentes e display colorido;
- Complexo: botões com tamanho de no mínimo três centímetros, botões de cores diferentes e display preto e branco; e
- Muito Complexo: botões menor de três centímetros, botões da mesma cor e display preto e branco

Com base nesta necessidade a Tabela 10 foi criada, onde cada grau de dificuldade recebeu o incremento de 15 pontos, pois, infere na gama de pessoas com dificuldade visual, onde o nível mais complexo exige uma pessoa com visão qualificada para execução da venda

Facilidade do portador ao inserir as informações	
Nível de facilidade	Pontuação
Simples	0
Médio	15
Complexo	30
Muito Complexo	45

Tabela 14 – Pontuação pela facilidade de o portador inserir as informações
Fonte: Elaborado pelo próprio autor

4.4.4 *Fail Over* de conexão

O *Fail Over* de conexão, em outras palavras backup de conexão, se baseia no meio de captura que possa utilizar uma segunda rota caso a primaria sofra com uma indisponibilidade, a fim de evitar a perda da transação. Utilizando o cenário de um celular para uma transação *mobile*, o celular conectado na Rede Wifi do proprietário para realizar as transações, caso o roteador sofra um desligamento repentino, cortando o sinal Wireless, o *mobile* automaticamente troca o método de conexão para os dados da operadora, a fim de concluir utilizando o segundo canal de transação, o FailOver utilizado para transações criticas, assume o serviço afim de não perder a conexão inicial, determinado com situação critica, situação onde pode paralisar o processo ou negocio do lojista que esta utilizando-o (Moser, 2004).

Seguindo um cenário parecido, como um servidor do TEF possui conexão através do X25 com a Adquirente é possível existir uma conexão *backup* utilizando a tecnologia ADSL, para garantir o envio da transação em caso de falha repentina.

A Existência de um *FailOver* implica em 10 pontos pois caso ocorra uma indisponibilidade da operadora que execute o serviço de Rede no momento do retorno da transação de *eletronic referral*, pode causar a negativa da transação no terminal, porém a aprovação da mesma no emissor, causando uma insatisfação do portador para o lojista devido a situação.

Com base nas tecnologias que possam executar este tipo de troca de canal de comunicação foi gerada a Tabela 11, onde a complexidade da solução esta relacionada a existência ou não da funcionalidade.

Característica da conexão	
Existência de backup	Pontuação
Sim	0
Não	10

Tabela 15 – Pontuação pela possibilidade de *FailOver*
Fonte: Elaborado pelo próprio autor

4.4.5 Cifragem da transação

Segundos a norma do PCI (PCI, 2016), toda a transação tem que ser cifrada com o nível de criptografia do DES ou superior, no entanto a criptografia depende do terminal como visto no DUKPT. Porém, nem todos os terminais possuem chave de criptografia, existem alguns poucos terminais legados de pinpad que conseguem enviar a ISO 8583 sem nenhuma cifra, sendo o risco para segurança da transação. Para este cenário o lojista precisaria atuar atualizando o seu parque por novos terminais PinPad, garantindo que todos suportam chave de criptografia DES ou superior. Não diferente do PinPad, o *e-commerce*, também possui um nível de segurança a ser respeitado, conforme demanda da CardSupreme toda a transação de *e-commerce* tem que ser trafegada através de um canal SSL de 128 bits. No entanto, fica a cargo do lojista implementar esta regra, pois, nem a bandeira e nem o Adquirente tem formas de homologar através do seu canal de origem, diferentemente das outras cifras. Por ser uma transação utilizando um serviço *web* o tempo de resposta tem que ser mínimo, a Adquirente precisa receber os dados abertos para tratamento da autorização e resposta imediata para o lojista. No caso

de uma transação POS a responsabilidade é do Adquirente, além de certificar o terminal com bandeira, todos os terminais possuem um nível de cifragem, bem como de nenhuma dependência da ação do lojista para atendimento desta determinação.

Com base no cenário de cifragem, caso seja responsabilidade da Adquirente, a facilidade por certificar a cifragem em todos os terminais tem que ser feito como normativa da bandeira, no entanto, se a responsabilidade for por conta do lojista do terminal estar cifrado ou a solução. A Tabela 12 apresenta este critério de possibilidade de envio de transação cifrada, a pontuação reflete a o grau de complexidade para implementação de uma transação de *referral*.

Possibilidade de enviar transação sem cifragem	
Resposta	Pontuação
Não	0
Sim	10

Tabela 16 – Pontuação pelo envio sem cifragem
Fonte: Elaborado pelo próprio autor

4.4.6 Análise comparativa

Na análise comparativa entre as soluções avaliadas será pontuado cada meio de captura, onde a solução que possuir uma menor pontuação consistirá na solução de melhor adequação e aceitação pelo portador no momento da utilização. A que possuir uma maior pontuação será a solução com um maior grau de dificuldade para implementação e pior aceitação no mercado. A Tabela 13 apresenta esta análise comparativa dos meios de captura.

	Meio de captura			
Perguntas	POS 	E-commerce 	Mobile 	TEF 
Meio de integração do lojista com a solução	0 (0)	1 (10)	0 (0)	2 (20)
O tempo de resposta pode fazer o lojista perder a venda	Não (0)	Sim (15)	Não (0)	Não (0)
Facilidade do portador ao inserir as informações	Médio (15)	Simples (0)	Muito Complexo (45)	Complexo (30)
Característica da conexão	Não(10)	Sim (0)	Sim (0)	Sim (0)
Possibilidade de enviar transação sem cifragem	Não (0)	Sim (10)	Não (0)	Sim (10)
Total	25	35	45	60

Tabela 17 – Analise comparativa dos meios de captura
Fonte: Elaborado pelo próprio autor

Com base nos resultados apresentados pela tabela 13 pode-se considerar:

- O POS é o meio de captura com maior facilidade de integração e utilização do *eletronic referral* em sua cadeia de aprovação
- O E-Commerce é o único meio de captura que pode perder uma venda por conta de tempo de resposta, logo as transações de *eletronic referral* tem que ser performáticas para implementação e utilização
- O Mobile possui como maior impactado a usabilidade por conta da concepção do mobile em si (máquina de captura do cartão), portanto para uma

implementação do *eletronic referral* possa atingir a maior gama de portadores, seria necessária uma melhoria no método de inserção das informações no quesito de usabilidade.

Com base na Tabela 13 podemos destacar:

- O TEF ficou com a somatória do meio de pagamento mais complexo, tendo como mais agravante em comparação aos outros meios de captura, o número de empresas necessárias para implementação de uma solução de pagamentos, pois cada alteração executada precisa ser compartilhada com todos no processo;
- Na categoria “Meio de integração do lojista com a solução” o TEF obteve a maior pontuação, pois, uma solução do TEF é mais complexa, precisa de pelo menos duas empresas (Integrador e *Software House*) para que a integração com a Adquirente seja realizada, além das aplicações fiscais que não podem sofrer alteração com a aplicação de um novo serviço ou atualização da versão;
- O *e-Commerce* foi pontuado nesta categoria, pois, a integração com o adquirente pode ser realizada em dois métodos, tanto integração direto com o adquirente como a integração realizada por empresas terceiras. O número de lojistas integrados com uma empresa terceira para realização de uma transação é superior a 60% (e-commerce, 2016). Portanto foi utilizado como verdade que todo lojista de e-commerce utiliza 1 empresa para integração do seu e-commerce, pois supera a maioria de lojista em número bruto;
- Na categoria de “Tempo de Resposta” o *e-commerce* foi pontuado, pois caso uma transação aumente o tempo de resposta consideravelmente, o portador pode fechar a janela (Loja Virtual) e ir buscar o mesmo produto em outra loja, sendo que o tempo de resposta tem um maior peso para conversão da venda em comparação com outros meios de captura;
- Para a categoria de “Usabilidade do portador em preencher os dados de *referral*”, o Mobile recebeu a maior pontuação, pois, o dispositivo de captura de cartão possui os botões reduzidos de tamanho, logo dificulta os portadores com um problema de visão ou que não possuem óculos corretivos no momento, diferentemente de um POS que possui os botões com um maior tamanho;

- Para a categoria de “Conexão”, o meio de captura de POS foi pontuado, pois o mesmo não possui um *FailOver* de conexão, sendo assim, para um POS GSM, quando a antena da operadora sofre indisponibilidade temporária, os POS da região não conseguem realizar vendas, pois não consegue montar a conexão com a adquirente. As outras tecnologias conseguem executar um *FailOver* sendo mudando de canal de conexão do X25 para um *link* dedicado ou de dois *links* de conexão com a Adquirente; e
- Para categoria de “Cifragem” tanto o *e-commerce* quanto o TEF foi pontuado, pois, são meios de captura que podem enviar uma transação diretamente para adquirente sem executar uma cifragem, transacionando com os dados abertos, saindo da especificação da bandeira, sendo um risco para o lojista que pode ser descredenciado previamente como para o portador que pode ter seus dados interceptados.

Com base nas cinco categorias avaliadas o POS é o meio de captura com um grau de dificuldade menor para o lojista, sem a necessidade do lojista executar alterações para utilização de uma transação de *referral*, além de maior velocidade na disponibilidade do produto final para o portador. Na outra ponta o meio de captura mais complexo é o TEF, pois para a implementação deste serviço as empresas contratadas pelo lojista precisam ter uma maior adequação do sistema para disponibilidade do produto para o portador, garantindo a ponta de cifragem que o terminal possui, o tipo do terminal para inserção das informações e a implementação da ISO 8583 para estorno em caso necessário.

5. CONSIDERAÇÕES FINAIS

O mercado de uma maneira macro consiste de um grupo de empresas com o propósito de entregar um serviço final para o cliente, definido de pagamento, este serviço precisa de uma conexão entre o meio de captura e a adquirente, uma aplicação para o suporte da funcionalidade e a criptografia da transação como um todo, portanto toda transação precisa atender estes requisitos para que seja efetuada.

O protocolo de comunicação entre todas as empresas é a ISO 8583, tendo seus bits definidos em um comum padrão para geração da transação, interessante da transação de *eletronic referral* que é um acordo entre as empresas para troca de informações no bit 48 e a bandeira apenas trafega as informações, portanto a ISO 8583 é protocolo de comunicação base, no entanto ele pode ser alterado a qualquer momento para adequação ou execução de um novo serviço, sendo um protocolo mutável.

O método de implementação da ISO 8583 da transação de *eletronic referral* para cada meio de captura, possui suas características de implementação, variando o nível de dificuldade de disponibilizar o produto para o portador na ponta final do processo, este tipo de transação não pode ser utilizado para portadores que possuam ausência da visão de maneira total, pois os meios de captura citados neste trabalho não estão aptos para atender este nicho de clientes para transação de *eletronic referral*, com exceção do e-commerce onde o cliente pode utilizar um dispositivo de narração da página navegada.

Com base no estudo conclui-se que a implementação do *eletronic referral* possui um maior nível de dificuldade para o meio de captura onde existe a necessidade de adequação por parte do lojista, aumentando a dificuldade de implementação como um todo, pois precisa tratar as mensagens, atender o mínimo de criptografia, executar um processo performático. Por outro lado existe uma maior facilidade para os meios de captura onde a adquirente tem por responsabilidade, pois ao ser implementado o serviço, a adquirente já consegue adequar os seu parque de maquinas para o serviço executando a atualização remota e por possuir um maior expertise no tratamento da troca de mensagens da ISO 8583, executando a atualização remota para todo o parque de maquinário, na qual o lojista precisaria apenas executar uma atualização da aplicação para que o serviço esteja disponível.

A transação de *eletronic referral* é uma alternativa de prevenção a fraude pois executa a segunda camada por ela proposta e garante um nível de segurança maior ao portador, pois entende que dependendo da situação, será feita a segunda camada de avaliação de integridade do portador do cartão e para o lojista que não terá problemas com fraude, é um tipo de transação que executa uma garantia para ambas as partes interessadas no processo de uma transação.

5.1 Contribuições do Trabalho

O trabalho contribuiu abordando os seguintes temas:

- O trabalho trata de em um serviço de implementação de um serviço que auxilia a mitigação de fraudes em transações eletrônicas oriundas de cartões de crédito e debito em pode uma transação;
- Implementação de integração de meios de captura para inserção de vendas com a adquirente e diversas plataformas de meios de pagamentos;
- Tratamento de envio e retorno da ISO 8583 em suas requisições em seus diversos pontos de origem, tratando diretamente cada bit de requisição e resposta; e
- Entendimento do mercado de pagamentos de uma maneira mais técnica tratado diretamente na troca de mensagens no protocolo da ISO 8583.

5.2 Trabalhos Futuros

Este trabalho contribui para o entendimento dos meios de captura de transações no ecossistema como um todo, auxiliando a possibilidade de melhorias diretamente nas empresas participantes com o tratamento da ISO 8583. Também no melhor tratamento para performance de uma transação de *eletronic referral* para o meio de captura de *e-commerce*, onde o tempo de resposta é um item vital para realização de vendas. E finalmente, na comparação dos serviços de *eletronic referral* com outras ferramentas do mercado para mitigar a fraude, realizando analise SWOT de cada produto

REFERÊNCIAS

2Checkout, Fraud Index 2014. Disponível em <http://go.2checkout.com/fraud-index> Acesso em 30 de Agosto de 2016

4ward, Desenvolvimento de software. Disponível em <https://www.4ward.com.br/produtos/aplicacao-pos/> Acesso em 11 de Dezembro de 2016

ABECS, Associação Brasileira das empresas de cartões de credito e serviço. Disponível em < **http://www.abecs.org.br/**> Acesso em 01 de Outubro de 2016

ALANAZI, Hamdan. New Comparative Study Between DES, 3DES and AES within Nine Factors. 2010. Journal Of Computing. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1003/1003.4085.pdf>. Acesso em: 27 nov. 2016

Auditor, Definição de TEF. Disponível em <http://www.auditornet.com.br/Manuais/aud_TEF.html> Acesso em 10 de Outubro de 2016

BACEN, Relatório de sistemas de pagamentos. Disponível em <http://www.bcb.gov.br/htms/novaPaginaSPB/Relatório_de_Vigilancia_do_SPB_2014.pdf>. Acesso em 21 de Agosto de 2016

BACEN, Relatório de incluso financeira. Disponível em <http://www.bcb.gov.br/Nor/relincfin/Relatório_inclusao_financeira.pdf>. Acesso em 22 de Agosto de 2016

Bematech, Meios de pagamento. Disponível em <http://www.slideshare.net/acimaq/bematech-bematef-turbo-automao-comercial-pafecf-8546028> Acesso em 10 de Janeiro de 2017

BHATLA, Tej Paul; PRABHU, Vikram; DUA, Amit. Understanding Credit Card Frauds. 2003. Tata Consultancy Services, 2003

Brasil, 1990 (BRASIL. Superior Tribunal de Justiça. Súmula 479, publicada no DJe de 01 agosto de 2012. Disponível em: http://www.stj.jus.br/SCON/sumulas/toc.jsp?t

Cielo, Manual de aplicação POS <https://www.cielo.com.br/live/documents/a96f4f850d6d4b199dc1f2c9e0caa89a.pdf> Acesso em 30 de Setembro de 2016

Cisco Support, Definição de conexão. Disponível em <https://search.cisco.com/search> Acesso em 01 de Novembro de 2016

Cliente SA, Referral Transaciton. Disponível em <http://www.clientesa.com.br/servicos/7480/prevencao-de-fraudes-com-cartao-de-credito/imprimir.aspx>. Acesso em 21 de Agosto de 2016

Datacash, Tempo de Resposta aceitável pelo gateway, Disponível em <https://datacash.custhelp.com/app/answers/detail/a_id/68> Acesso em 30 de Setembro de 2016.

Desenvolvimento de software, linguagens para o POS, Disponível em <**http://www.comprason-line.com/software-pos/**> Acesso em 15 de Setembro de 2016

Stephan Kovach Divisão de Biblioteca – EPUSP. Diretrizes para Apresentação de Dissertações e Teses. 4ª. Edição. São Paulo. 2013. 91p. http://www.poli.usp.br/images/stories/media/download/bibliotecas/DiretrizesTesesDissertacoes.pdf

E-Commerce News, MarkShare metodo de pagamento, Disponível em <http://ecommercenews.com.br/noticias/pesquisas-noticias/cartao-de-credito-e-meio-de-pagamento-usado-em-73-das-compras-no-comercio-eletronico> Acesso em 15 de Julho de 2016

E-Commercenews, Share de plataforma. Disponível em <https://ecommercenews.com.br/noticias/pesquisas-noticias/magento-lidera-entre-as-plataformas-mais-populares-do-mundo> Acesso em 15 de Janeiro de 2017

E-Commercepordentro, Gateway de pagamento. Disponível em <http://ecommercepordentro.com/intermediarios-x-gateways-pagamentos/> Acesso em 15 de Janeiro de 2017

Elizer Pimentel, Camadas de um POS. Disponível em <https://commons.wikimedia.org/wiki/File:Camadas_ptBr.png> Acesso em 13 de Dezembro de 2016

Emalta, Historia de cartões de credito no Brasil. Disponível em <http://emalta.com.br/historia-dos-cartoes-de-credito/>. Acesso em 20 de Agosto de 2016

Embratel, Link dedicado. Disponível em <http://www.embratel-linkdedicado.com.br/>. Acesso em 15 de Outubro de 2016

Enext, Ecossistema do E-Commerce. Disponível em http://nextecommerce.com.br/ecossistema-ecommerce-brasileiro-2014 Acesso em 15 de Janeiro de 2017

Ferreira Tiago, Aprovação de transação de credito. Disponível em < **http://200.17.137.109:8081/novobsi/Members/taef**

/graduacao/algoritmos-e-estrutura-de-dados/aulas/ProjetoFinal2011-2.pdf>. Acesso em 01 de março de 2017

G1, Novo fraude de cartões. Disponível em <http://g1.globo.com/bom-dia-brasil/noticia/2016/05/donos-de-cartoes-de-credito-sao-vitimas-de-novo-tipo-de-golpe.html> Acesso em 02 de Julho de 2016

Global Information Assurance Certification. Disponível em <https://www.giac.org/paper/gsec/4068/3des-secure-pin-based-electronic-transaction-processing/106500>, Acesso em 27 de Novembro de 2016.

Greg Shultz, Conexão direta. Disponível em <http://www.techrepublic.com/article/configure-it-quick-link-different-windows-versions-using-xps-direct-cable-connection/> Acesso em 6 de Outubro de 2016

Guimares, Moises, Segurança em transações eletrônicas. Disponível em <https://www.owasp.org/images/6/6c/Seguran%C3%A7a_em_Transa%C3%A7%C3%B5es_Eletr%C3%B4nicas_-_Mois%C3%A9s_Guimar%C3%A3es.pdf> Acesso em 01 de Dezembro de 2016

Jose Gargallo Tuzón, Arquitetura DES. Disponível em <**http://www.spi1.nisu.org/recop/al02/jgargallo/index.html**> Acesso em 15 de Outubro de 2016

IBM, Exemplo do MTI da ISO 8583. Disponível em <http://www.ibm.com/support/knowledgecenter/pt-br/SSMKHH_9.0.0/com.ibm.etools.mft.samples.iso8583.doc/doc/background.htm>. Acesso em 5 de Outubro de 2016

Informável, Autorização via TEF. Disponível em <https://informatavel.wordpress.com/2013/07/23/como-funciona-seu-cartao-de-credito/> Acesso em 10 de Janeiro de 2017

Ingenico, Especificação POS ICT250. Acesso em <https://ingenico.us/smart-terminals/countertop-terminals/ict-250.html> Acesso em 5 de Dezembro de 2016

ISO 8583, Norma técnica. Disponível em <https://www.iso.org/obp/ui/#iso:std:iso:8583:-1:ed-1:v1:en> <https://www.iso.org/obp/ui/#iso:std:iso:8583:-3:ed-2:v1:en>. Acesso em 5 de Outubro de 2016

IZettle, leitor de cartões. Disponível em <https://www.izettle.com/br/card-readers> Acesso em 11 de Janeiro de 2017

Mercado Pago, Produtos. Disponível em <https://www.mercadopago.com/mp-brasil/point/#!/products> Acesso em 12 de Janeiro de 2017

Moser Sergio, Alta Disponibilidade, um estudo de caso em um ambiente único de imagem única em produção <**https://projetos.inf.ufsc.br/arquivos_projetos/projeto_71/TCC.pdf**>. Acesso em 05 de Março de 2017

MTB, Fluxo X25. Disponível em <http://www.mtb.ind.br/tef.htm> Acesso em 01 de Novembro de 2016

Oliveira Ronielton, Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. Disponível em <www.ronielton.eti.br/publicacoes/artigorevistaseguranca digital2012.pdf> Acesso em 20 e Novembro de 2016

Payeleven, Tipos de equipamentos. Disponível em <https://payleven.com.br/maquininhas> Acesso em 13 de Janeiro de 2017

PCI, Regras do PCI. Disponível em <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_3_pt-BR.pdf?agreement=true&time=1478390605934>. Acesso em 30 de Setembro de 2016

Poynt, Terminal Inteligente, Disponível em <**https://poynt.com/**> Acesso em 20 de Novembro de 2016

Redecard, Meios de Captura. Disponível em < **http://relatorioweb.com.br/redecard/10/node/80**>. Acesso em 27 de Fevereiro de 2017

Rethinkdb, FailOver. Disponível em <https://www.rethinkdb.com/docs/failover/>. Acesso em 20 de Outubro de 2016

Sebrae, conceito de pagamentos. Disponível em <http://www.sebrae.com.br/sites/PortalSebrae/artigos/o-que-sao-meios-eletronicos-de-pagamentos,3a085415e6433410VgnVCM1000003b74010aRCRD> Acesso em 10 de Julho de 2016.

Software Express, Comunicação entre o Chekout e Pinpad. Disponível em < **https://www.softwareexpress.com.br/produtos/**> Acesso em 08 de Setembro de 2016

Tektonia, Protocolo de comunicação. Disponível em <http://tektonia.com/tecno.htm> Acesso em 25 de Outubro de 2016

Teleco, Rede GSM Conceitos. Disponível em <http://www.teleco.com.br/pdfs/tutorialredegsm.pdf> Acesso em 20 de Novembro 2016

Teixeira Damazio, As Tecnologias da Internet na Telefonia Fixa.

Disponível em <http://www.teleco.com.br/pdfs/tutorialadsltec.pdf>. Acesso em 20 de Novembro de 2016

Tecnoblog, Como não fazer uma máquina de cartão “moderninha”. Disponível em <https://tecnoblog.net/191099/maquina-cartao-acessibilidade-cegos/>. Acesso em 01 de Março de 2017

Visa, Criptografia POS. Disponível em <**https://www.visa.com.br/**>. Acesso em 30 de outubro de 2016

X25, Definição do X25. Disponível, em <http://x25.com.br/> Acesso em 20 de Outubro de 2016

YAZAKI, Marcos Tadeu; COSTA, Oswaldo Jaime da. Ambiente Online de Pagamentos de Tributos de IPVA, Licenciamento Eletrônico, Multas de Trânsito e Seguro Obrigatório. 2007. Prodesp, 2007

Apêndice 1

A Tabela abaixo referência a ISO 8583 com os principais campos, o tipo e o tamanho

Campo	Tipo	Usado
2	n ..19	Cartão
3	n 6	Código do processo
4	n 12	Valor da transação
5	n 12	Valor aceito
6	n 12	Valor da conta
7	n 10	Data e hora da transmissão
8	n 8	Valor da taxa da conta
9	n 8	Taxa de conversão aceita
10	n 8	Taxa de conversão da conta
11	n 6	Número de rastreamento (em Inglês System Audit Transaction Number(STAN))
12	n 6	Hora local da transmissão (hhmmss)
13	n 4	Data local da transmissão (MMDD)
14	n 4	Data de expiração
15	n 4	Data do aceite
16	n 4	Data da conversão
17	n 4	Data da captura
18	n 4	Tipo de estabelecimento
19	n 3	Código do país da Adquirente
20	n 3	Extensão do cartão, código do País
21	n 3	Instituição de encaminhamento, código do País
22	an 12	POS entrada do cartão
23	n 3	Aplicação do número de sequência do cartão
24	n 3	Rede internacional de identificação (em inglês Network International Identifier (NII))
25	n 2	Condição do ponto de serviço
26	n 2	Ponto de serviço código de captura

27	n 1	Identificação da autorização, tamanho de resposta
28	x+n 8	Valor taxa da transação
29	x+n 8	Valor taxa de aceite
30	x+n 8	Valor do processo de taxa
31	x+n 8	Valor da aceitação da taxa
32	n ..11	Número de identificação da adquirente
33	n ..11	Número de identificação do roteador
34	ns ..28	Extensão do cartão
35	z ..37	Dados da trilha 2
36	n ...104	Dados da trilha 3
37	an 12	Número de referência de recuperação
38	an 6	Número de autorização
39	an 2	Código de resposta
40	an 3	Código do serviço restrito
41	ans 8	Número de identificação do terminal
42	ans 15	Número de identificação do código de aceitação
43	ans 40	Nome do portador do cartão, endereço, cidade, estado, país
44	an ..25	Dados adicionais
45	an ..76	Trilha 1
46	an ...999	Dados adicionais - ISSO
47	an ...999	Dados adicionais - Nacional
48	an ...999	Dados adicionais - private
49	a or n 3	Código da moeda transacionada
50	a or n 3	Código da moeda aceita
51	a or n 3	Código da moeda da conta
52	b 64	Número de identificação pessoal
53	n 16	Dados seguros de controle de informação
54	an ...120	Valor adicional
55	ans ...999	Reservado ISO

56	ans ...999	Reservado ISO
57	ans ...999	Reservado Nacional
58	ans ...999	Reservado Nacional
59	ans ...999	Reservado Nacional
60	ans ...999	Reservado Nacional
61	ans ...999	Reservado Privado
62	ans ...999	Reservado Privado
63	ans ...999	Reservado Privado
64	b 16	Código de mensagem de autenticação em inglês (Message authentication code (MAC))
65	b 1	Extensão do BITMAP
66	n 1	Código de aceitação
67	n 2	Código do pagamento estendido
68	n 3	Recebendo da instituição o código do país
69	n 3	Código do país aceito
70	n 3	Código de administração da rede
71	n 4	Número da mensagem
72	n 4	Número da mensagem, ultimo
73	n 6	Data da ação
74	n 10	Número do credito
75	n 10	Reversão do número de crédito
76	n 10	Número de débito
77	n 10	Reversão do número de débito
78	n 10	Número de transferência
79	n 10	Reversão do número de transferência
80	n 10	Número da consulta
81	n 10	Número de autorização
82	n 12	Processo de *fee* de crédito
83	n 12	Valor do *fee* de crédito
84	n 12	Processo de *fee* de débito
85	n 12	Valor do *fee* de débito

86	n 16	Valor de crédito
87	n 16	Reversão do valor de crédito
88	n 16	Valor de débito
89	n 16	Reversão do valor de débito
90	n 42	Dados originais

Tabela 7 – Definição da ISO 8583 com os principais bits utilizados

Fonte: ISO, 2003