ABECS
INTEGRAÇÃO CTF COM AUTORIZADORAS CLASSE 3
CAPTURA DE SENHAS COM CHAVES 3DES

VERSÃO 1.1

27/08/2019

Histórico do Documento

Versão	Data	Autor	Descrição
1.0	19/02/2019	Emerson Polesi Magnum Lyra Tânia Alves Magro	Criação da primeira versão do documento.
1.1	27/08/2019	Emerson Polesi	Inclusão de fluxos do processo para cadastramento e validação de chaves de homologação e de produção. Substituição dos termos KEK por ZMK e Working Key por ZPK, mais relevantes para o contexto da integração em questão. Atualização do Glossário.

Índice

1 Introdução

Este documento define critérios para a geração e manipulação de chaves criptográficas relacionadas à captura de senhas em transações TEF e estabelece procedimentos para a integração do Sistema CTF Auttar com Autorizadoras Classe 3, as quais não possuem Master Key própria cadastrada nos dispositivos de captura, com a utilização de chaves 3DES.

O objetivo é aumentar a proteção de senhas capturadas através de dispositivos PINpads e POS, evitando que as mesmas sejam abertas (descriptografadas) e manipuladas por entidades não autorizadas, atendendo aos requisitos de segurança e boas práticas estabelecidos pela Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS).

Não é intenção deste documento descrever de forma abrangente a integração entre os sistemas da Auttar com os da Autorizadora mas, tão somente, esclarecer o processo seguro para geração e distribuição de chaves criptográficas, bem como a captura e distribuição segura de senhas de cartões de crédito e débito entre a Auttar e a Autorizadora.

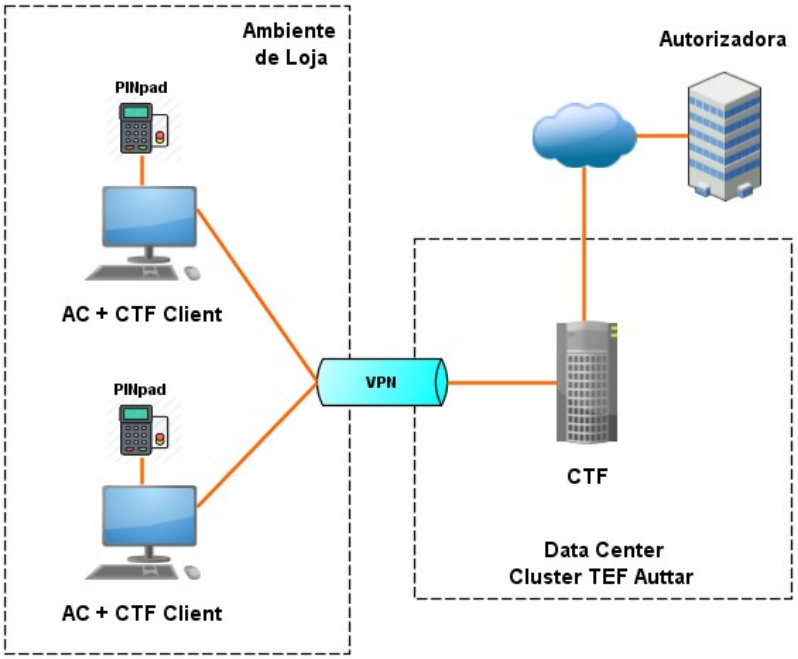
O Apêndice A apresenta um glossário com termos comuns utilizados neste documento.

2 Visão geral

A seguir, são apresentados alguns conceitos básicos para facilitar o entendimento da proposta de integração que será apresentada no capítulo 3.

2.1 Arquitetura Geral da Solução de Pagamento Auttar

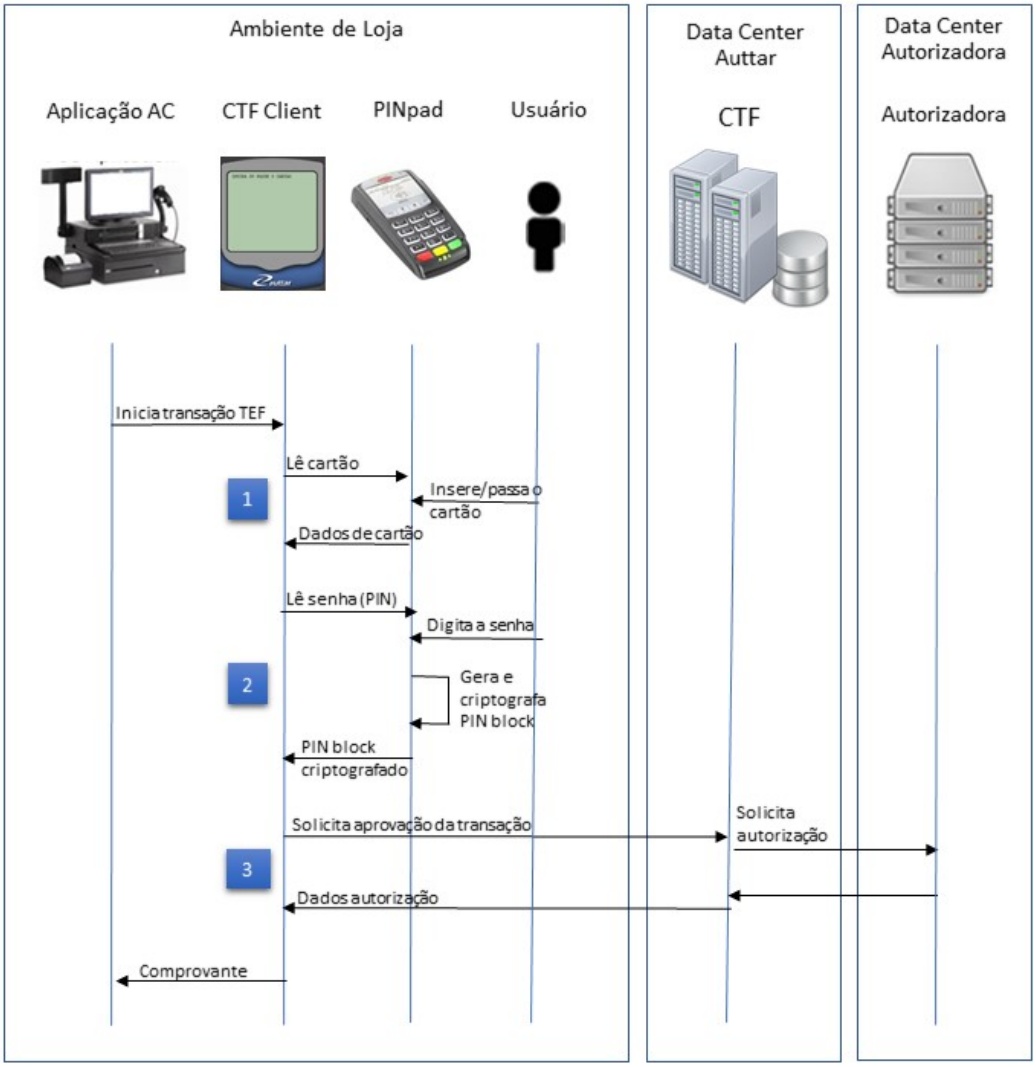
O diagrama abaixo apresenta uma visão resumida da arquitetura típica da solução de pagamento Auttar:



Componente	Descrição
AC	Aplicativo de automação comercial, usuária do CTF Client.
CTF Client	Disponibiliza acesso às funções de pagamento (TEF) para a AC, controla a interação com o PINpad e comunica-se com o CTF para autorizar transações.
PINpad	Dispositivo seguro para leitura de cartões e captura de senhas.
CTF	Sistema integrador TEF que atende às demandas do CTF Client por transações de pagamento, interagindo com a Autorizadora para efetivar as autorizações de pagamento.
Autorizadora	Responsável por validar e autorizar transações de pagamentos.

2.2 Fluxo de Autorização de Pagamentos

O diagrama abaixo apresenta a interação entre os diversos componentes da solução, durante um fluxo de autorização de pagamento:



Nota 1: **A senha é criptografada dentro do dispositivo PINpad e só pode ser descriptografada pela Autorizadora**.

Nota 2: Todas as mensagens entre CTF Client e CTF Server são inteiramente protegidas por criptografia forte ao nível de aplicação, bem como utiliza-se criptografia adicional no canal de comunicação (VPN) entre o CTF Client e o CTF.

Nota 3: As estações de trabalho (AC + CTF Client) nunca armazenam dados sensíveis da transação, tais como senhas ou dados de cartões, criptografados ou não.

Descrição do fluxo de autorização:

Leitura do Cartão (caso seja requerido para a transação)

1. O CTF Client solicita ao PINpad que inicie a leitura do cartão.
   1.1. O cliente passa ou insere o cartão no dispositivo PINpad.
   1.2. O PINpad lê o cartão e retorna para o CTF Client as trilhas 1 e 2 e o PAN.

Captura de PIN (senha)

2. O CTF Client solicita ao PINpad que inicie a captura da senha.
   2.1. O CTF Client solicita a leitura da senha, informando o PAN, a chave de trabalho da Autorizadora (ZPK criptografada com a MK da Auttar) e o índice da MK da Auttar no Mapa de Chaves do PINpad.
   2.2. O cliente digita a senha no dispositivo PINpad.
   2.3. O PINpad retorna para o CTF Client o *PIN block* (contendo a senha), criptografado com a chave de trabalho (ZPK) da Autorizadora.

Autorização da Transação

3. O CTF Client solicita a autorização da transação.
   3.1. O CTF Client formata uma mensagem contendo o *PIN block* criptografado, dados da trilha 1 e 2 criptografados, PAN criptografado e outros dados da transação.
   3.2. O CTF Client criptografa toda a mensagem e a envia para o CTF.
   3.3. O CTF recebe a mensagem e a descriptografa.
   3.4. O CTF Server valida a transação de acordo com parâmetros de configuração do lojista e da Autorizadora.
   3.5. O CTF Server formata uma mensagem de transação utilizando o padrão ISO 8583 e a envia para a Autorizadora através de um link privado ou HTTPS.
   3.6. A Autorizadora executa os procedimentos de autorização e responde ao CTF.
   3.7. O CTF formata a mensagem de resposta da transação com dados da transação, incluindo: comprovantes, código de aprovação, código de resposta, etc.
   3.8. O CTF criptografa a mensagem de resposta e a envia para o CTF Client.

2.3 Processo de Captura de Senha pelo PINpad

O processo de criptografia da senha, realizado pelo PINpad, não é o foco deste documento, porém, o seu conhecimento é importante para compreensão da interação entre o CTF e a Autorizadora, uma vez que algumas das informações utilizadas no processo são fornecidas pelo CTF e estabelecidas de comum acordo com a Auttar e a Autorizadora.

De modo resumido, o PINpad captura a senha através do seu teclado, formata um bloco de dados contendo a senha, chamado *PIN block*, e criptografa este bloco com uma chave de sessão (ZPK) conhecida na forma aberta apenas pela Autorizadora.

Obs.: O *PIN block* criptografado é encaminhado à Autorizadora na forma original em que foi gerado pelo *PINpad*, **sendo apenas ela capaz de descriptografá-lo e obter a senha aberta**.

Componentes utilizados no processo de captura de senha pelo *PINPad*:

Componente	Descrição
PIN	A senha aberta digitada pelo usuário no teclado do PINpad.
PIN block	Bloco de dados contendo a senha formatada. O formato segue o padrão ANSI X9.8 (ou simplesmente ANSI). Este formato também é conhecido como ISO-0.
PAN	Número da conta associada ao cartão. Normalmente são os últimos 12 dígitos do número de um cartão, sem o dígito verificador (último dígito), conforme ilustrado abaixo: XXXP PPPP PPPP PPPX
ZPK	Chave de trabalho (ou chave de sessão), utilizada para criptografar *PIN block*.
ZPK(*PIN block*)	*PIN block* criptografado com chave de trabalho (ZPK).
MK	Master Key (chave) utilizada para criptografar ZPK.
MK(ZPK)	ZPK criptografada com Master Key.
MK[]	Tabela de Master Keys do PINpad, contendo a MKs das principais Adquirentes e Integradoras. Estas chaves são previamente cadastradas nos equipamentos pelos fabricantes, em parceira com as entidades proprietárias das chaves. A Auttar é uma das integradoras que possui MK cadastrada nos *PINpads*.
Ind_{mk}	Índice (posição) de uma MK na Tabela de Master Keys do PINpad. No caso, o índice da MK utilizada para criptografar a ZPK.

Os componentes PAN, Ind_{mk} e MK(ZPK) são passados ao *PINpad*, pelo CTFClient, no momento da captura da senha, tendo sidos o MK(ZPK) e o Ind_{mk} recebidos do servidor CTF.

Após capturar a senha do usuário, o PINpad realiza internamente as seguintes operações para gerar o *PIN block* criptografado:

1) Obtém o *PIN block* a partir da senha e do PAN abertos, de acordo com o seguinte:
   - É criado um bloco de dados (A) composto de 16 dígitos hexadecimais, contendo a senha, no formato: 0 T senha padding
     Onde: 0 é um dígito zero fixo
     T é um dígito hexadecimal com o tamanho da senha
     senha são os dígitos que compõe a senha (PIN)
     padding são dígitos F completando os 16 bytes do bloco
     Para uma senha "1234", por exemplo, este bloco (A) seria: **041234FFFFFFFFFF**
   - É criado um bloco de dados (B) composto de 16 dígitos hexadecimais contendo 4 dígitos zeros fixos seguidos do PAN (12 dígitos). Ou seja, para um PAN "123456789012", por exemplo, este bloco (B) seria: **0000123456789012**
   - É criado o *PIN block* realizando-se um XOR (ou exclusivo) entre (A) e (B). Considerando os exemplos acima, o *PIN Block* seria o resultado de:
     041234FFFFFFFFFF xor 0000123456789012
     Ou seja:
     041226CBA9876FED

2) Obtém a MK no mapa MK[] do *PINpad*, a partir da posição especificada por Ind_{mk}.

3) Obtém a ZPK, descriptografando MK(ZPK) com a chave obtida no passo 2.

4) Obtém o ZPK(*PIN block*), criptografando o *PIN block* (do passo 1) com a ZPK (do passo 3).

O ZPK(*PIN block*) é retornado pelo PINpad para o CTF Client e repassado para o servidor CTF.

3 Integração CTF com Autorizadora

Antes de prosseguir com a leitura deste capítulo, recomenda-se a leitura do item 2.3 (Processo de Captura de Senha pelo PINpad), deste documento.

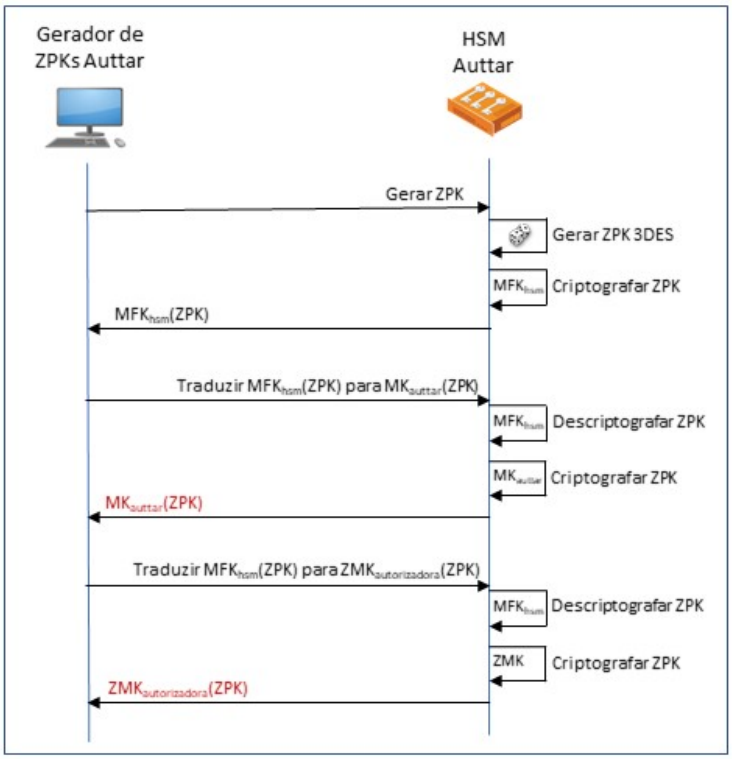
3.1 Funcionamento Geral da Integração

Uma vez que a Autorizadora não possui MK própria cadastrada no mapa de chaves dos PINpads, a **Auttar fará uso da sua MK para viabilizar a captura de senhas para a Autorizadora**.

A MK_{auttar} (Master Key da Auttar) está inserida no HSM da Auttar e também nos dispositivos *PINpads* e *POS* de mercado. **Esta chave foi gerada aleatoriamente pelo HSM e é desconhecida por pessoas e por sistemas da Auttar, incluindo o CTF.**

A MK_{auttar} é a chave que o *PINpad* utilizará para "abrir" a ZPK da Autorizadora a partir de $MK_{auttar}(ZPK)$, sendo esta ZPK posteriormente utilizada pelo próprio *PINpad* para criptografar o *PIN block*. Faz-se necessário, portanto, que as ZPKs da Autorizadora estejam criptografadas com a MK_{auttar}. No cenário atual, a única forma de se obter $MK_{auttar}(ZPK)$ é gerando e criptografando as ZPKs no HSM da Auttar.

Como o HSM não exporta ZPKs abertas, e considerando que a Autorizadora não possui a MK_{auttar}, para que ela tenha acesso às ZPKs no formato aberto, de maneira que possa descriptografar ZPK(*PIN block*), **ela deve estabelecer uma ZMK (Zone Master Key) 3DES própria e cadastrá-la previamente no HSM da Auttar**. Assim, o HSM será capaz de gerar tanto $MK_{auttar}(ZPK)$ quanto $ZMK_{autorizadora}(ZPK)$. A título informativo, o diagrama abaixo ilustra o procedimento que a Auttar utilizará para a gerar as ZPKs criptografadas:



Obs.: A MFK_{hsm}, citada no diagrama, é uma chave interna do HSM, conhecida apenas pelo próprio dispositivo.

Tendo a posse da sua ZMK, a Autorizadora será capaz de obter a ZPK aberta a partir de $ZMK_{autorizadora}(ZPK)$.

Em resumo, cada ZPK gerada através do HSM da Auttar será disponibilizada nos formatos $MK_{auttar}(ZPK)$ e $ZMK_{autorizadora}(ZPK)$, sendo que as $MK_{auttar}(ZPK)$ serão utilizadas pela Auttar e a as $ZMK_{autorizadora}(ZPK)$ pela Autorizadora. Ao todo serão geradas 10 ZPKs, ou seja, um conjunto de 10 $MK_{auttar}(ZPK)$ e outro conjunto equivalente de 10 $ZMK_{autorizadora}(ZPK)$.

Lembrando e reforçando que:

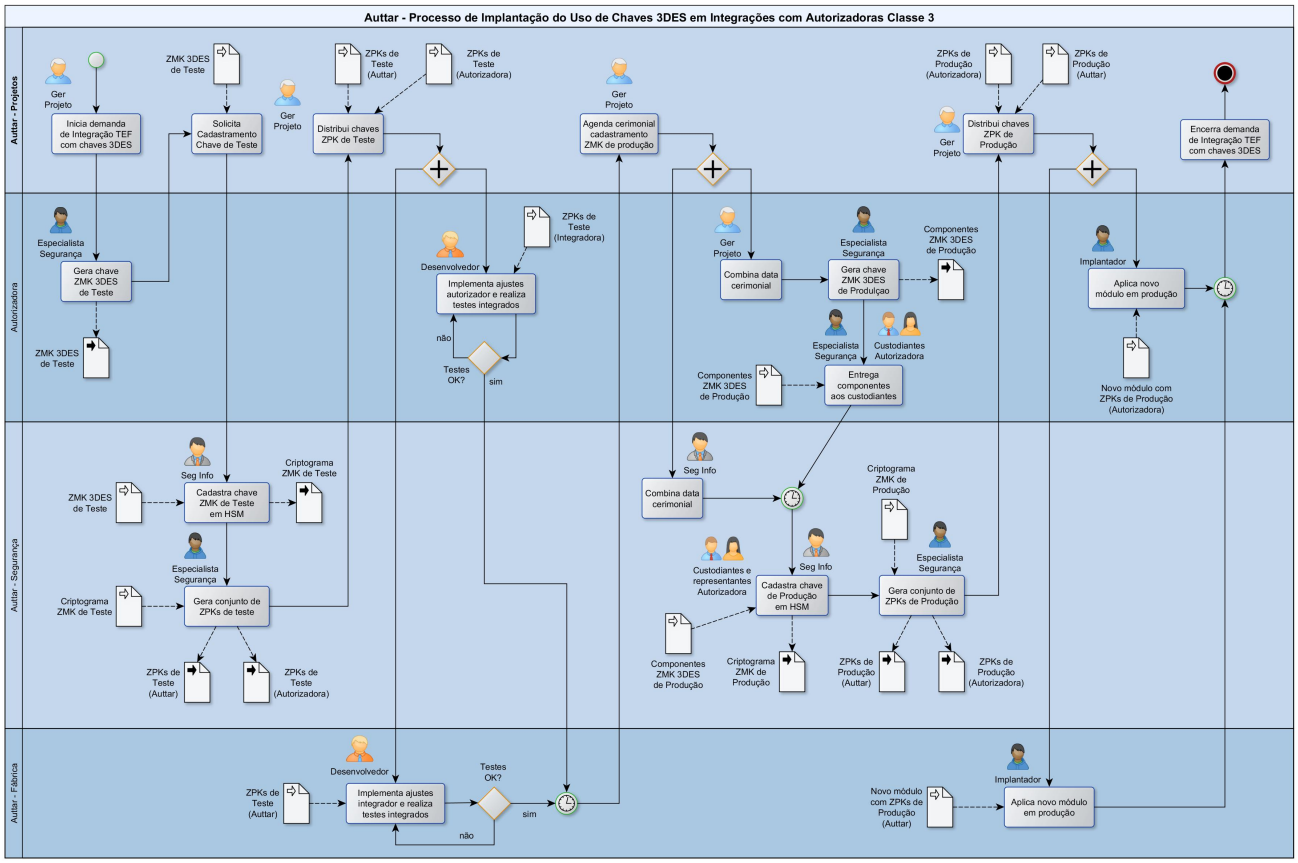
1) No momento da captura da senha, o *PINpad* descriptografa $MK_{auttar}(ZPK)$ e utiliza ZPK para gerar ZPK(*PIN block*);
2) Para obter o *PIN block* aberto, **a Autorizadora, com sua ZMK, descriptografa $ZMK_{autorizadora}$(ZPK) para obter a ZPK e utiliza-a para descriptografar ZPK(*PIN block*)**;
3) O *PIN block* só pode ser aberto pela Autorizadora, pois, só ela tem condições de obter a ZPK aberta, através da sua ZMK;
4) A Auttar não tem conhecimento da MK_{auttar}, portanto, não consegue obter ZPK a partir de $MK_{auttar}(ZPK)$.

A Autorizadora deverá adotar, em seu ambiente, procedimentos para garantir a criação, armazenamento e guarda da sua chave ZMK de produção de maneira segura.

3.2 Processo para Implantação da Integração

O processo completo de integração entre CTF e Autorizadora, pode ser dividido em duas principais etapas: homologação e produção. Na etapa de homologação, são criadas chaves de teste e validados os procedimentos e sistemas envolvidos, da Auttar e da Autorizadora. Na fase de produção, são geradas as chaves de produção e implantados os sistemas em ambientes produtivos.

O diagrama abaixo ilustra o processo completo:



O cadastramento de chaves (ZMK) de produção da Autorizadora no HSM da Auttar ocorre de forma segura, através da realização de cerimonial, o qual deve ser previamente agendado com a equipe de segurança da Auttar, quando serão fornecidos detalhes sobre os requisitos e procedimentos para do cerimonial.

A chave de produção só poderá ser cadastrada no HSM após terem sido realizados testes prévios (com sucesso) com chaves de teste/homologação.

Obs.: As chaves $ZMK_{autorizadora}$ de homologação poderão ser criadas pela Autorizadora ou pela Auttar, e o seu cadastramento no HSM de homologação da Auttar não demanda cerimonial.

3.3 Mensageria

Quando os sistemas estiverem integrados, a cada transação, o CTF utilizará uma das ZPKs do conjunto de 10 ZPKs geradas, a critério da Autorizadora. Para tanto, o índice da chave a ser utilizada (na referida tabela) deverá ser passado da Autorizadora para o CTF, junto com outros dados da transação, conforme ilustrado pelos fluxos dos diagramas a seguir:

1) Fluxo 3DES padrão (novo)

FLUXO 3DES PADRÃO NOVO

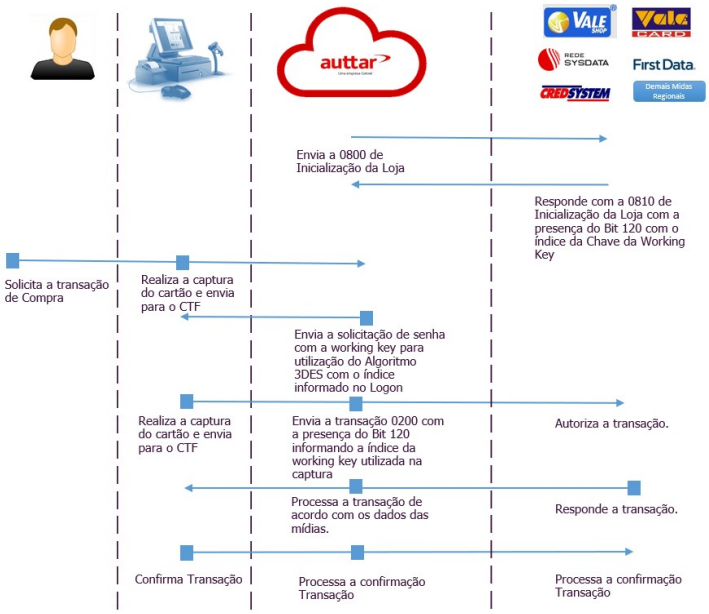
No fluxo de demonstrado ao lado, temos a condição ideal de funcionamento.

Como pré-requisitos para este fluxo temos:

0 – Cerimonial de chaves da autorizadora junto a Auttar.
1 – Presença da chave 3DES da Auttar no pinpad do varejista.

Fluxo:

A autorizadora informa qual o índice que a loja usará naquele dia através da mensagem de logon (0800), após isso o CTF Server, faz o uso da working key de referencia e envia o pinblock para a autorizadora conforme regra citada no item 2 deste documento.



2) Fluxo Alternativo 1

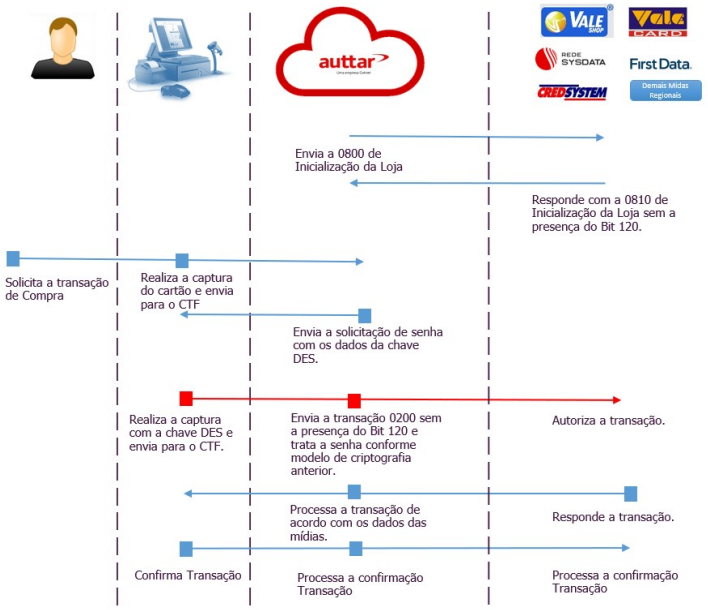
FLUXO ALTERNATIVO 1

Uma vez que o fluxo padrão não seja possível porque o pré-requisito da cerimonia de chaves não tenha sido realizado ainda.

A solução CTF tratará com o modelo anterior e realizará a captura do pin utilizando o modelo anterior onde o CTF manipula o PIN para envio a administradora conforme orientação.

Como pré-requisitos para este fluxo temos:

0 – Presença da chave DES da Auttar no pinpad do varejista.

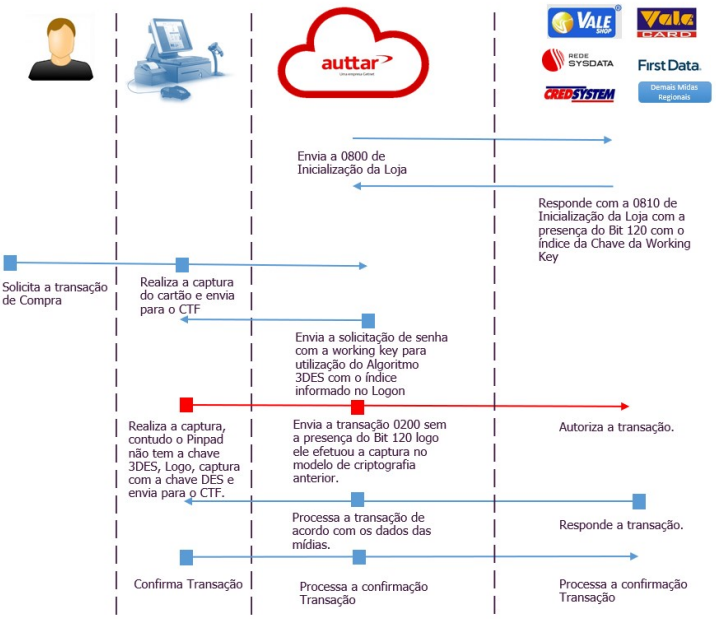


3) Fluxo Alternativo 2

FLUXO ALTERNATIVO 2

Uma vez que o fluxo padrão não seja possível porque o pré-requisito da presença da chave 3DES do PINPAD não seja atendido.

A solução CTF tratará com o modelo anterior e realizará a captura do pin utilizando o modelo anterior onde o CTF manipula o PIN para envio a administradora conforme orientação.



Apêndice A - Glossário

Abaixo, a descrição de alguns termos comuns utilizados neste documento:

Termo	Descrição
3DES	Vide Triple-DES.
AC	Sistema de Automação Comercial, normalmente localizado em uma loja de varejo.
Autorizadora	Empresa responsável por autorizar ou negar transações financeiras. Mantém o cadastro com informações de cartões e clientes.
CTFClient	Componente cliente do CTF, integrado às Automações Comerciais, responsável por se comunicar com os servidores CTF e viabilizar a realização de transações TEF, bem como controlar o aceso ao dispositivo PINPad.
CTF	O Concentrador de Transações Financeiras (CTF) é a aplicação da Auttar responsável por: comunicar-se com o CTFClient e com as Autorizadoras; atender às requisições de transações financeiras e de resgate de pontos do CTFClient; manter as regras de negócio da Autorizadora; armazenar os dados das transações; inicializar os terminais; atender as demandas de outros serviços como consultas, relatórios, arquivos de saída, etc.
EC	Estabelecimento Comercial, para se referir a uma loja de uma empresa que tenha um aplicativo de AC instalado.
HSM	*Hardware Security Module* é um equipamento criado especificamente para guardar e gerenciar, de forma segura, chaves utilizadas em processos criptográficos.
Integradora	Empresa responsável por desenvolver o Sistema de Pagamento Eletrônico o qual utiliza o PINPad. O mesmo que Software House de TEF. A Auttar se enquadra nesta categoria.
LMK	Local Master Key. Uma Master Key para uso restrito local. Normalmente utilizada internamente em HSMs para proteger outras chaves.
Master Key	Chave criptográfica normalmente utilizada para criptografar outras chaves as quais são utilizadas por algoritmos de criptografias simétricos, como 3DES, para criptografar senhas e/ou dados.
MFK	Vide *LMK*.
MK	Vide *Master Key*.
PAN	*Primary Account Number* é número quer identifica a conta de um cartão de crédito ou débito junto à Autorizadora. Em outras palavras, é um número de cartão.
PINPad	Equipamento seguro responsável por ler dados de cartões magnéticos e com chip EMV, bem como capturar senhas.
Triple-DES	*Triple Data Encryption Standard* (3DES) é um método de criptografia baseado em algoritmo de criptografia simétrica.
Working Key	Chave de trabalho utilizada para criptografar informações durante uma transação (sessão).
ZMK	Zone Master Key. Uma Master Key utilizada para criptografar ZPKs. Considerada como chave de transporte para ZPKs.
ZPK	Zone PIN Key. É um tipo de Working Key, utilizada para criptografar *PIN blocks* que trafegam entre diferentes instituições.