

Distribuição de Serviços de Comércio Eletrônico

Interações

- Servidores de comércio eletrônico interagem com:
 - clientes
 - prestadores de serviço
- Questões:
 - como altera o comportamento do servidor
 - como ocorre a interação

Prestadores de Serviço

- Executam tarefas que contribuem, total ou parcialmente, para o atendimento às requisições submetidas ao servidor.
- Motivação:
 - diminuição da carga de trabalho
 - execução mais eficiente das tarefas
- Exemplo: autenticação e verificação de crédito

Comércio Eletrônico Móvel

- Aplicação recente resultante da proliferação de dispositivos de acesso pessoal
- Tecnologias
 - Internet
 - computação móvel
 - comunicação sem fio
- Definição
 - conjunto de atividades e processos de comércio eletrônico que é realizado utilizando terminais sem fio por pelo menos um dos participantes

Tipos de comunicação

- Comunicação com fio
 - fibra ótica
- Comunicação sem fio
 - celulares com novos protocolos e maiores velocidades
- São complementares
- Devem continuar a crescer

Computação Móvel

- Processamento
 - Dispositivo portátil
 - Transportável
 - Autônomo em termos de energia
- Mobilidade
 - Não importa a localização do usuário
- Comunicação sem fio
 - Uso de tecnologias rádio

Atributos da Computação Móvel

- Ubiquidade
- Alcance
- Segurança
- Conveniência
- Georeferenciamento
- Conectividade instantânea
- Personalização

Computação Móvel

- Questões
 - Como usaremos os dispositivos portáteis?
 - Que aplicações serão úteis?
 - Que tipo de interface vai predominar?
 - Teremos ambientes parecidos aos PCs?

Telefones Celulares

- 1G
 - Transmissão analógica
 - Taxa: 9600bps
- 2G
 - Transmissão digital (TDMA, CDMA, GSM)
 - Taxa: 9600 bps a 14400 bps
 - Objetivo é suportar o WAP
- 2.5G
 - Objetiva disponibilizar aplicações pré 3G
 - Taxa: até 150kbps

Telefones Celulares

- 3G
 - Objetiva a transmissão de dados multimídia
 - Taxas:
 - 140 kbps a mais de 120 km/h
 - 400 kbps a menos de 120 km/h
 - 2000 kbps a menos de 10 km/h

Telefones Celulares

- Serviços 3G
 - vídeo sob demanda
 - acesso a dados multimídia
 - acesso à Internet
 - execução de aplicações diversas
 - interoperabilidade entre ambientes em escala possivelmente mundial

Telefones Celulares

- 4G
 - eliminação da comutação por circuito
 - transmissão de dados multimídia em redes baseadas em pacotes
 - serviços previstos
 - localização inteligente de serviços
 - siga-me
 - disseminação de informação push.

Adaptação

- Questão central em computação móvel
- Considera características físicas
 - mobilidade
 - características do ambiente (ruído, perda)
 - energia
- Outras características
 - pessoais, culturais e lógicas WAP
- Solução para ligar PDAs e celulares à Internet
- O padrão WAP especifica um ambiente de aplicação, e os protocolos para comunicação para dispositivos sem fio, como telefones celulares, pagers e PDAs.

WAP

Interoperabilidade

- Aplicações desenvolvidas para um dispositivo devem poder operar em outros dispositivos
 - Não devem existir versões diferentes para dispositivos diferentes
 - Um componente WAP deve interoperar com outros componentes

Desafios

- Comunicação transparente
 - utilizar diferentes infra-estruturas de forma imperceptível
 - não existe tal conceito na prática
 - Soluções baseadas em pacotes e software radio

Desafios

- Localização e informação
 - Pessoas e entidades em lugares diferentes vão desejar ter informações dependentes da sua localização
 - localização de serviços e servidores
 - adaptação da informação
 - personalização
 - aspectos culturais

Tecnologias de Computação Móvel

Sumário

- ambiente móvel oferece recursos aquém daqueles da Internet fixa
- plataforma atraente pela sua comodidade
- já oferece condições para execução de transações, que têm demandas de conectividade usualmente baixas
- novas possibilidades em termos de aplicações e serviços

Transações de Comércio Eletrônico Móvel

Ambientes móveis se diferenciam pelos seguintes aspectos:

- Hostilidade do ambiente aberto
- Vulnerabilidade dos dispositivos móveis
- Autonomia de comunicação dos dispositivos
- Autonomia de processamento
- Hostilidade e vulnerabilidade são relacionados à segurança e integridade dos dados, e à identificação dos clientes
- Autonomia de comunicação e processamento afetam o projeto dos serviços

Transações Distribuídas

Transações distribuídas são caracterizadas pela execução concorrente de operações em várias unidades de processamento que cooperam para a realização de transações.

Como garantir as propriedades transacionais em um ambiente distribuído?

Atomicidade

- todos participantes devem sinalizar conclusão
- protocolos de duas fases
 - operações concorrentes são executadas
 - coordenador verifica se as operações foram executadas
 - coordenador conclui a transação e notifica participantes

Distribuição: Serviço de Pagamento

- Autorização
 - verificação de crédito
- Despacho
 - atualização de estoque e logística
- Débito
 - confirma aquisição de bem
- Geração de anúncio
 - selecionar anúncio para inclusão na página resposta

Critérios

- Distribuição:
 - quais serviços são distribuídos e por que.
- Segurança:
 - procedimentos de segurança para a troca de informações
- Atomicidade:
 - como manter a atomicidade em transações distribuídas.

Requisitos de Distribuição

- Cliente-servidor:
 - tarefa é delegada e servidor aguarda resposta para continuar
- Paralelização:
 - tarefas independentes são executadas ao mesmo tempo

Requisitos de Segurança

- Privacidade dos dados:
 - qual participante acessa qual dado
- Segurança dos dados:
 - mecanismos para manutenção da privacidade e integridade dos dados
- Tolerância a falhas:
 - como evitar que falhas nos prestadores de serviço ou na comunicação comprometam as tarefas

Requisitos de Atomicidade

- Atomicidade Robusta:
 - não é possível criar ou destruir informações, bens digitais ou moedas
 - transações em moeda real são robustas
 - concentração em instituições financeiras é uma estratégia comum para garantir atomicidade robusta em transações eletrônicas

Requisitos de Atomicidade

- Atomicidade recíproca:
 - execução de transações distribuídas inter-dependentes só se completa se ambas são executadas
 - exemplo: cliente recebe bens se e somente se pagamento foi efetuado
 - essencial para bens digitais
 - demanda infra-estrutura de logística para bens físicos

Requisitos de Atomicidade

- Atomicidade certificada:
 - permite demonstrar com precisão as interações para a venda, incluindo comprovação de quais bens foram entregues
 - exige entidades certificadoras para bens digitais
 - é normalmente impraticável para bens físicos

Café: Transações Distribuídas

Nível de Aplicação

- Todos os prestadores de serviço são agentes
- Conseqüências:
 - número de estados aumenta
 - ações assumem granulação mais fina
 - um único serviço implica em várias transições de estado

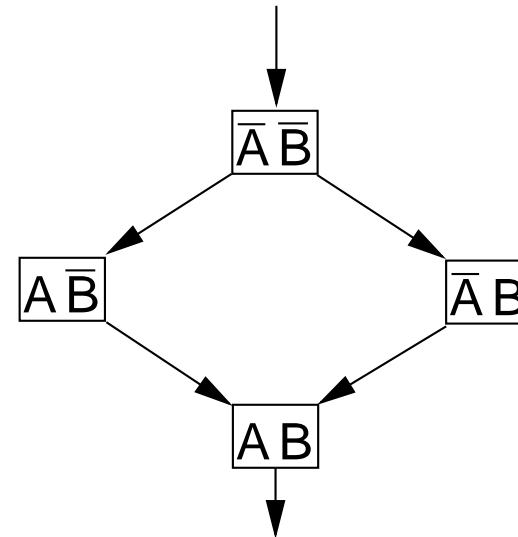
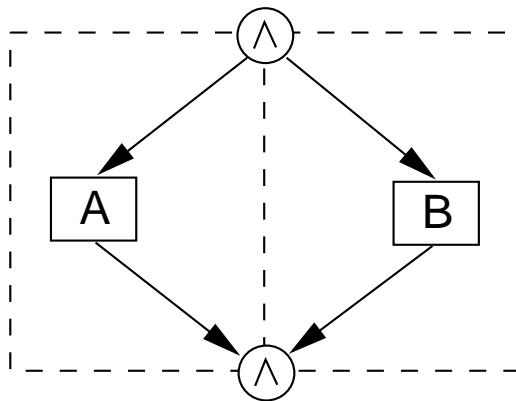
Café: Transações Distribuídas

Nível de Aplicação

- Execução de serviços distribuídos
 - Seqüencial: tarefas executadas em uma ordem pré-determinada (seriada)
 - Paralelo: mais de uma tarefa pode ser executada simultaneamente, mas o servidor deve estabelecer a estratégia de sincronização

Café: Transações Distribuídas Nível de Aplicação

Transações distribuídas são representadas por arestas conjuntivas.



Café: Transações Distribuídas

Nível de Aplicação

- Agentes:
 - incluem os prestadores de serviço
- Estados:
 - refletem ações executadas em cada agente
- Ações:
 - desmembradas de acordo com agentes
- Função de transição:
 - deve contemplar novos estados e ações

Café: Transações Distribuídas

Nível de Aplicação

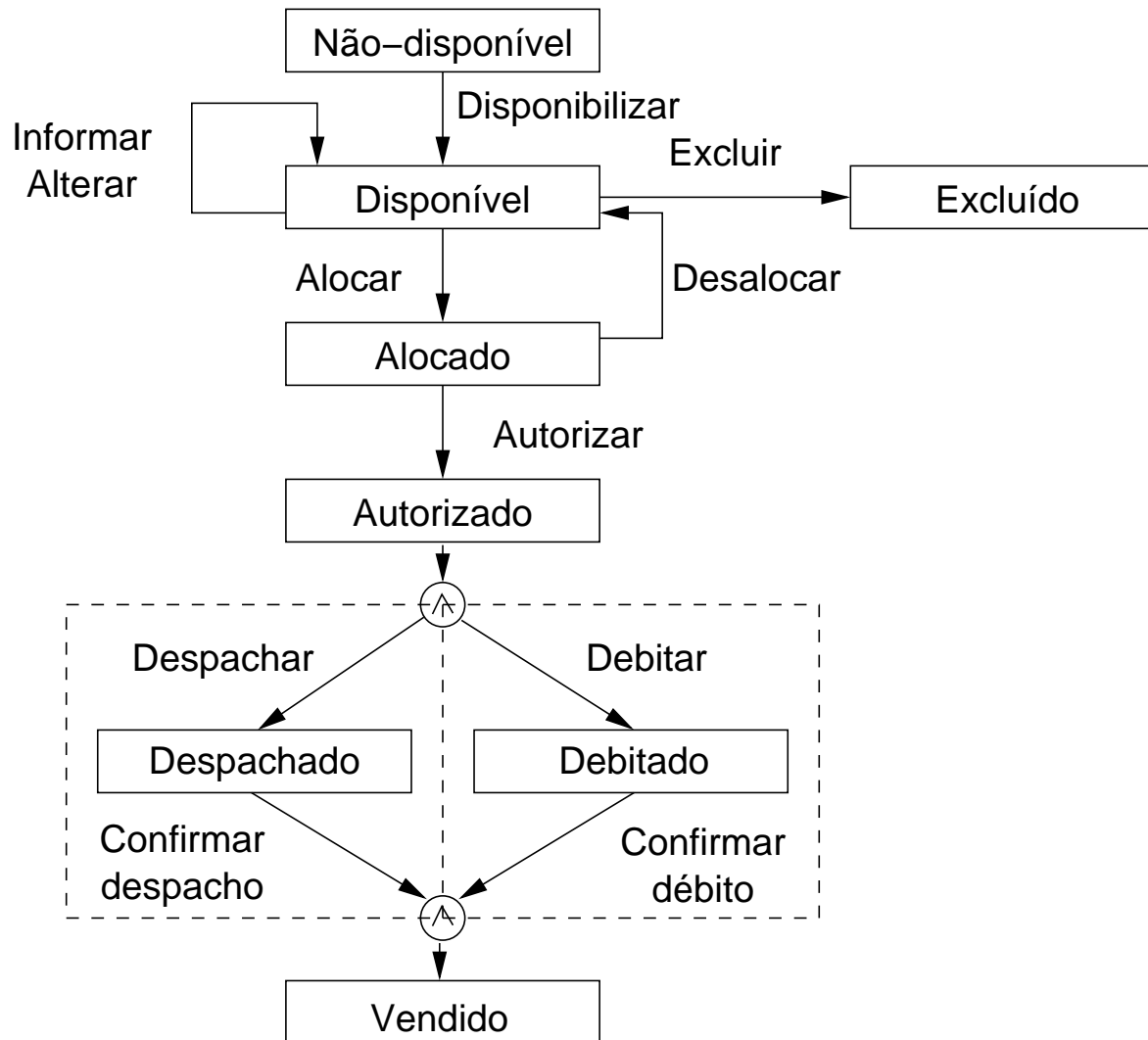
Exemplo: distribuição do serviço de pagamento

- Autorizado
- Despachado
- Debitado

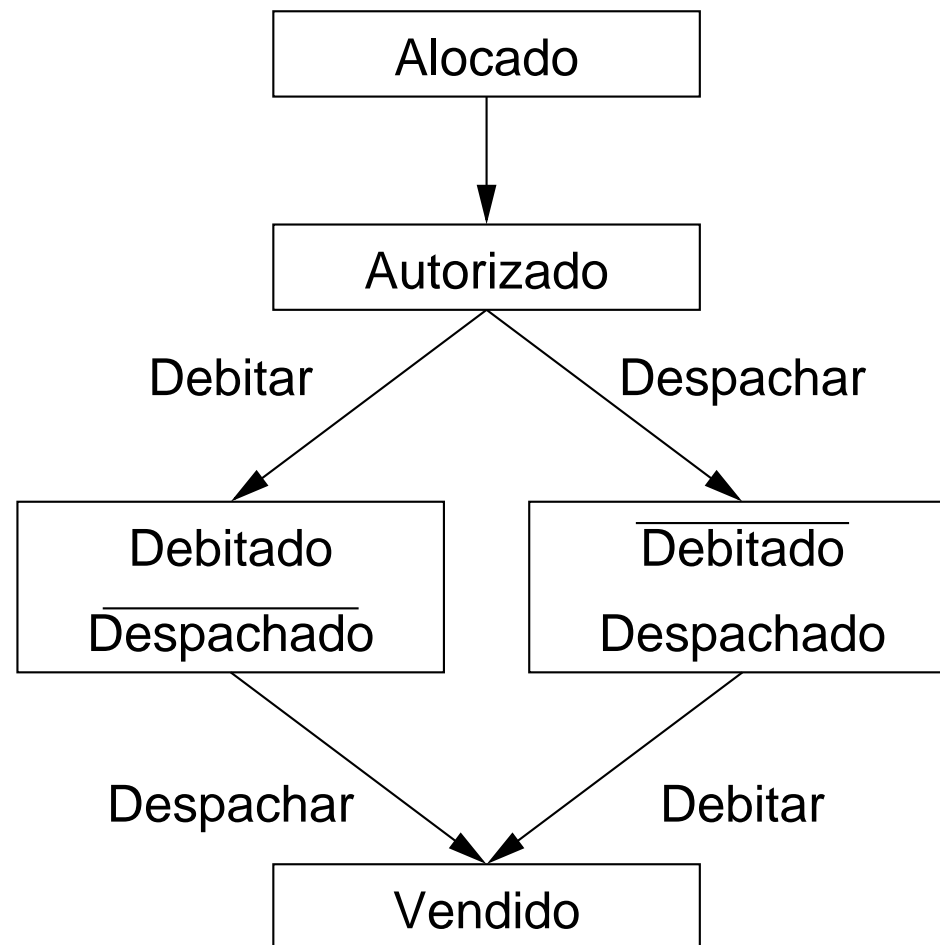
Regras

- Pagamento deve ser autorizado antes de ser debitado e a compra despachada
- Débito e despacho podem ocorrer simultaneamente

Café: Transações Distribuídas Nível de Aplicação

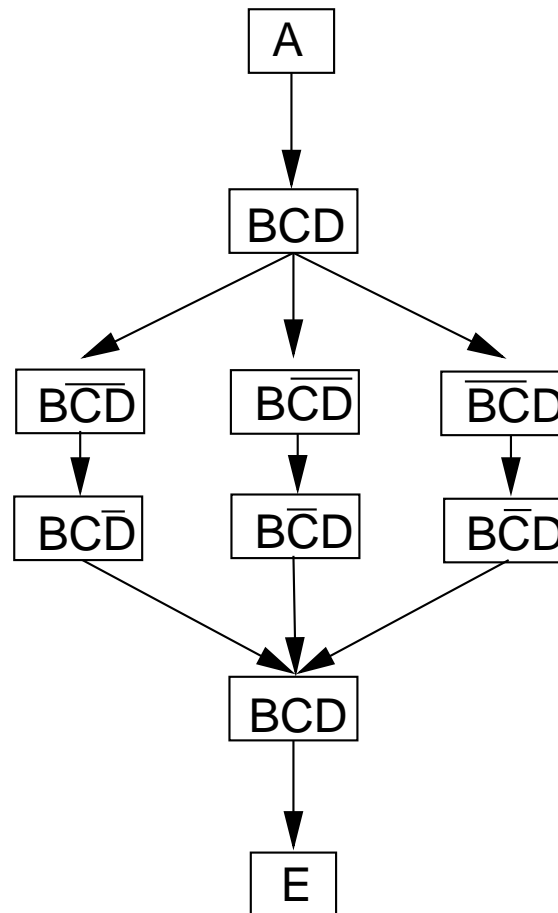
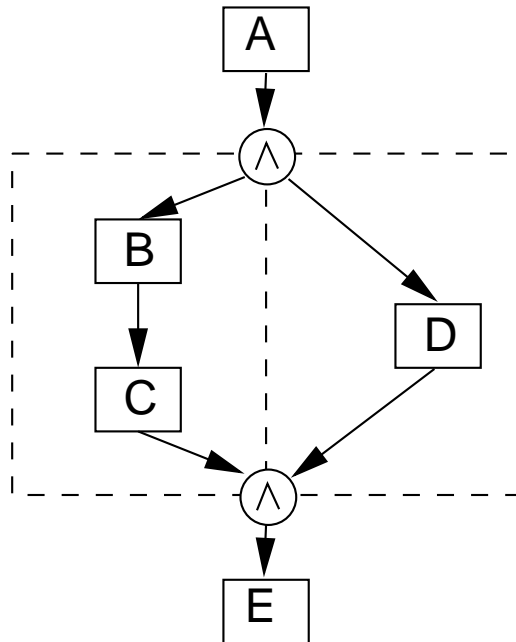


Café: Transações Distribuídas Nível de Aplicação



Café: Transações Distribuídas Nível de Aplicação

Não-determinismo associado a paralelismo,



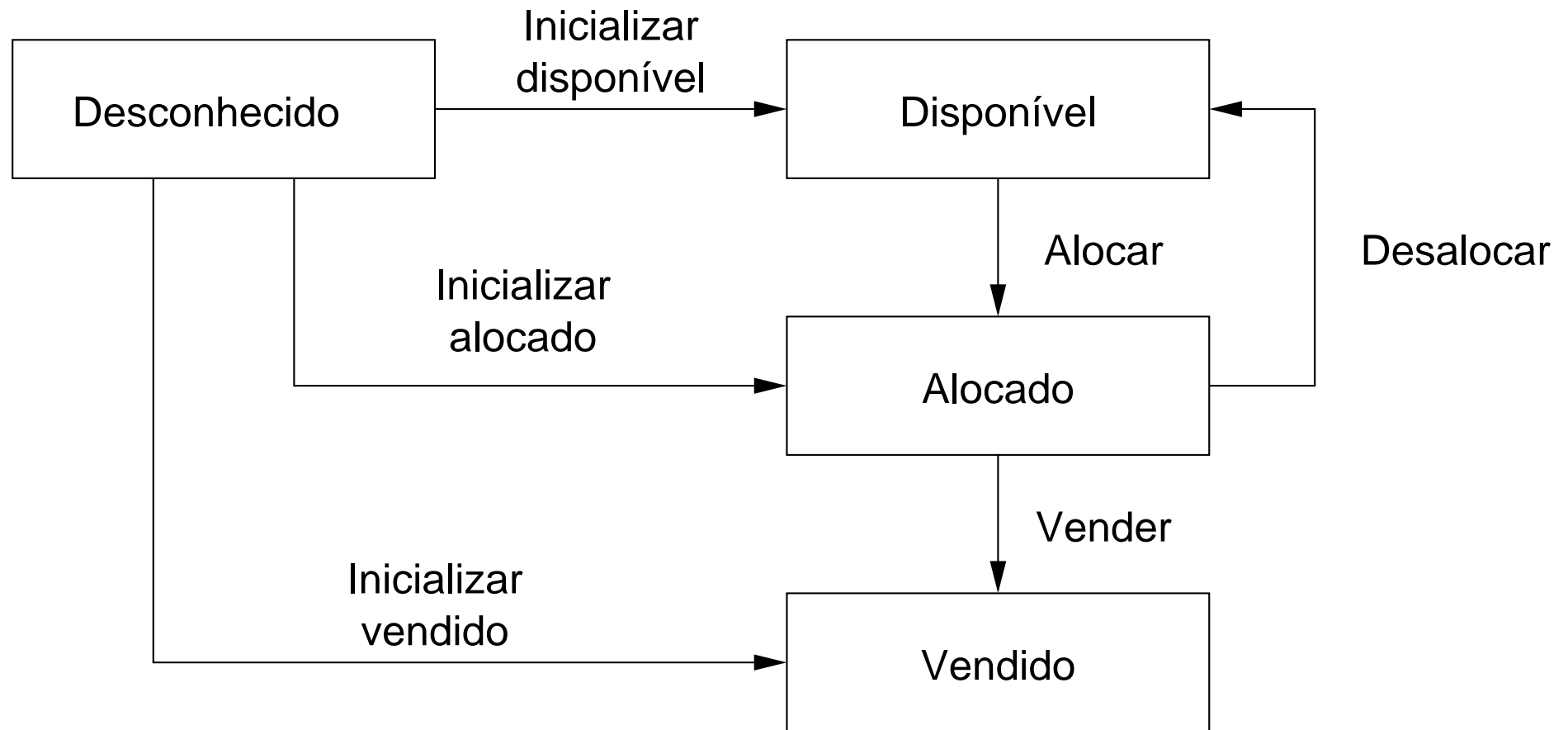
Manutenção de Estado Compartilhado

Cliente Autônomo

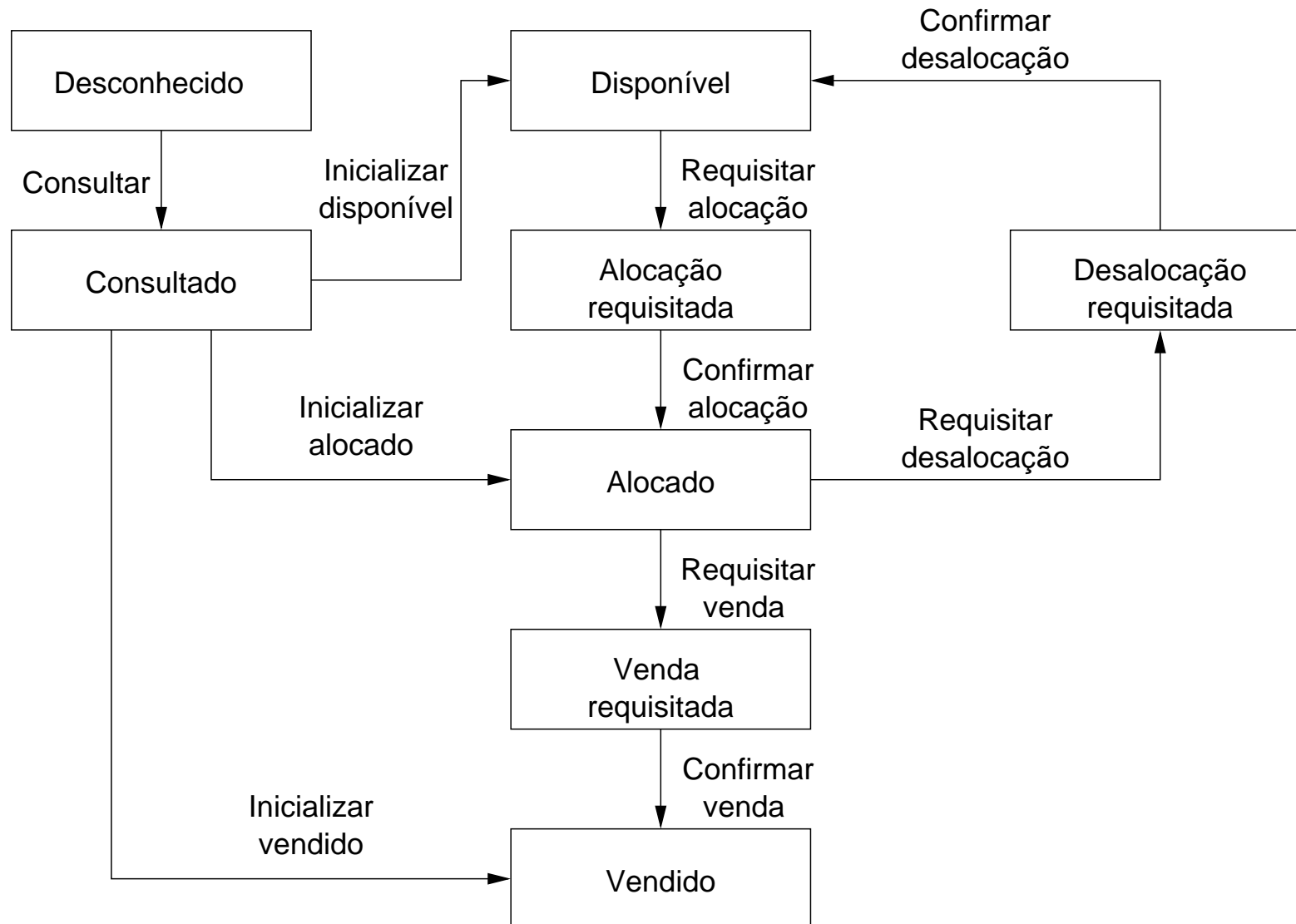
Uma opção para distribuição de aplicações é o cliente armazenar o estado da sessão do cliente e ter autonomia para executar serviços.

- No caso do cliente com itens alocados perder a comunicação:
 - mantém a alocação por tempo indefinido
 - detecta perda de comunicação e cancela
 - altera estado do produto para refletir a nova situação

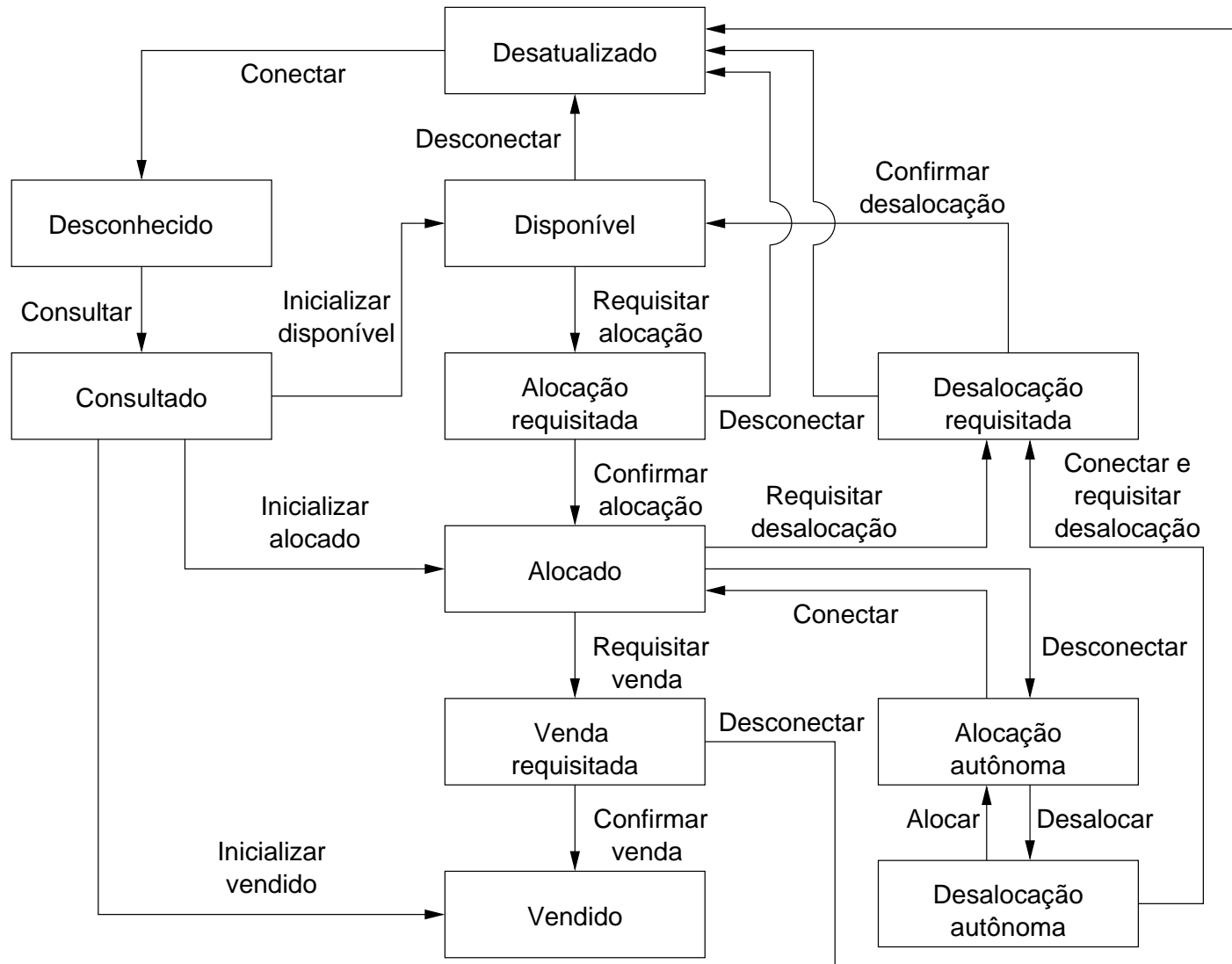
Nível de Aplicação Cliente Autônomo



Nível de Aplicação Cliente Autônomo



Nível de Aplicação Cliente Autônomo



Nível Funcional

- Para cada serviço distribuído:
 - Deve identificar prestadores de serviço e justificar a sua utilização
 - Estratégia de segurança deve indicar quais dados são transmitidos e como.
 - Definir e justificar o nível de atomicidade garantido pelo serviço distribuído

Nível de Execução

- Especifica os mecanismos de segurança a serem utilizados
- Protocolos e endereçamento devem contemplar os prestadores de serviço
- Ferramentas devem incluir aquelas necessárias à interação segura

Nível de Execução Tolerância a Falhas

- Mecanismos de recuperação:
 - repetição temporizada
 - servidores redundantes
- Política de tratamento de falhas:
 - define as respostas em caso de falhas
 - execução local
 - cancelamento da transação
 - envio parcial
 - adiamento

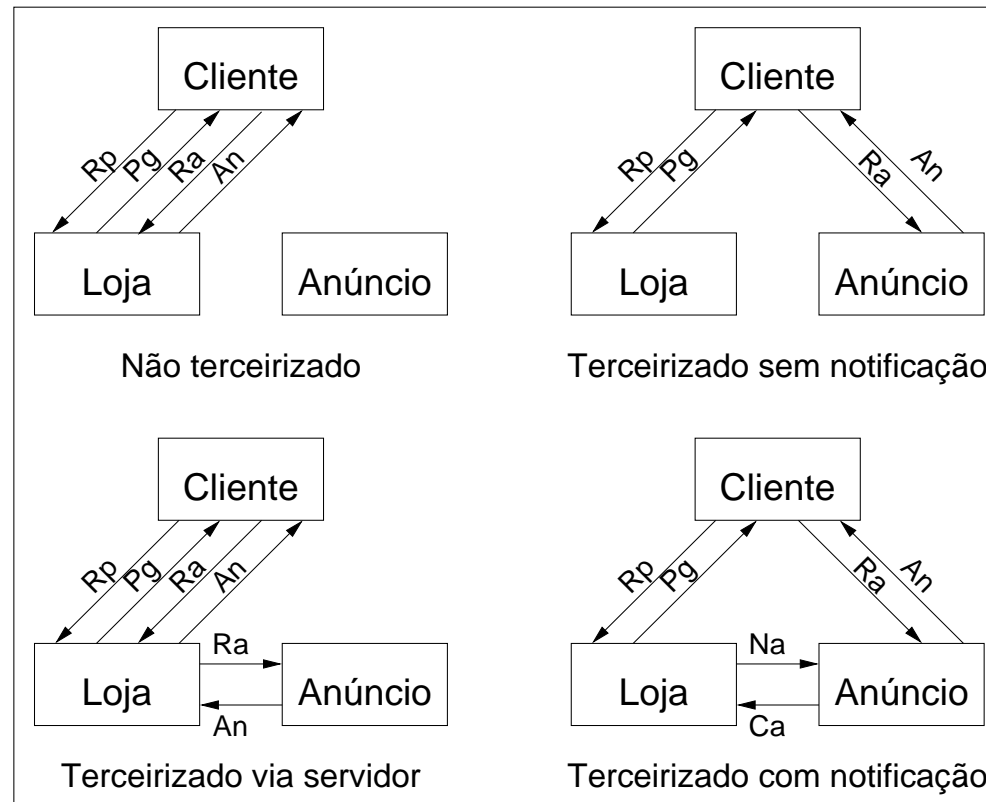
Servidor de Anúncios

- Explora a delegação da geração de anúncios eletrônicos
- Características:
 - anúncios são imagens binárias
 - tarifação por impressão
 - requisição via protocolo HTTP
 - não há autenticação

Servidor de Anúncios

- Protocolo
 - Fatores
 - nível de controle do contratante:
 - agente requisitante
 - Tipos de requisições
 - Notificação de anúncio
 - Requisição de anúncio

Servidor de Anúncios: Estratégia de Integração



Rp – Requisição de Página

Pg – Página resposta

Na – Notificação de anúncio

Ra – Requisição de anúncio

An – Anúncio

Ca – Confirmação anúncio

Servidor de Anúncios

Nível de Execução

- Ambiente de execução:
 - WWW
- Protocolo:
 - HTTP
 - Mensagens
 - Notificação
 - Confirmação
 - Requisição
 - Anúncio

Servidor de Anúncios

Nível de Execução

- Endereçamento:
 - `http://servidor/tiporeq?p1=v1&p2=v2...`
- Tolerância a falhas
 - ausência de resposta:
repetição das requisições até que seja atingida um limite
 - servidor retorna erro:
repete requisição, persistindo não insere anúncio.

Exemplo: Pagamento utilizando SET

- Secure Electronic Transactions
 - provê canal de comunicação seguro
- inacessível a agentes externos às transações
 - suporta relações de confiança
- utiliza certificados digitais
 - garante a privacidade das partes
- apenas informações necessárias são disponibilizadas para participantes

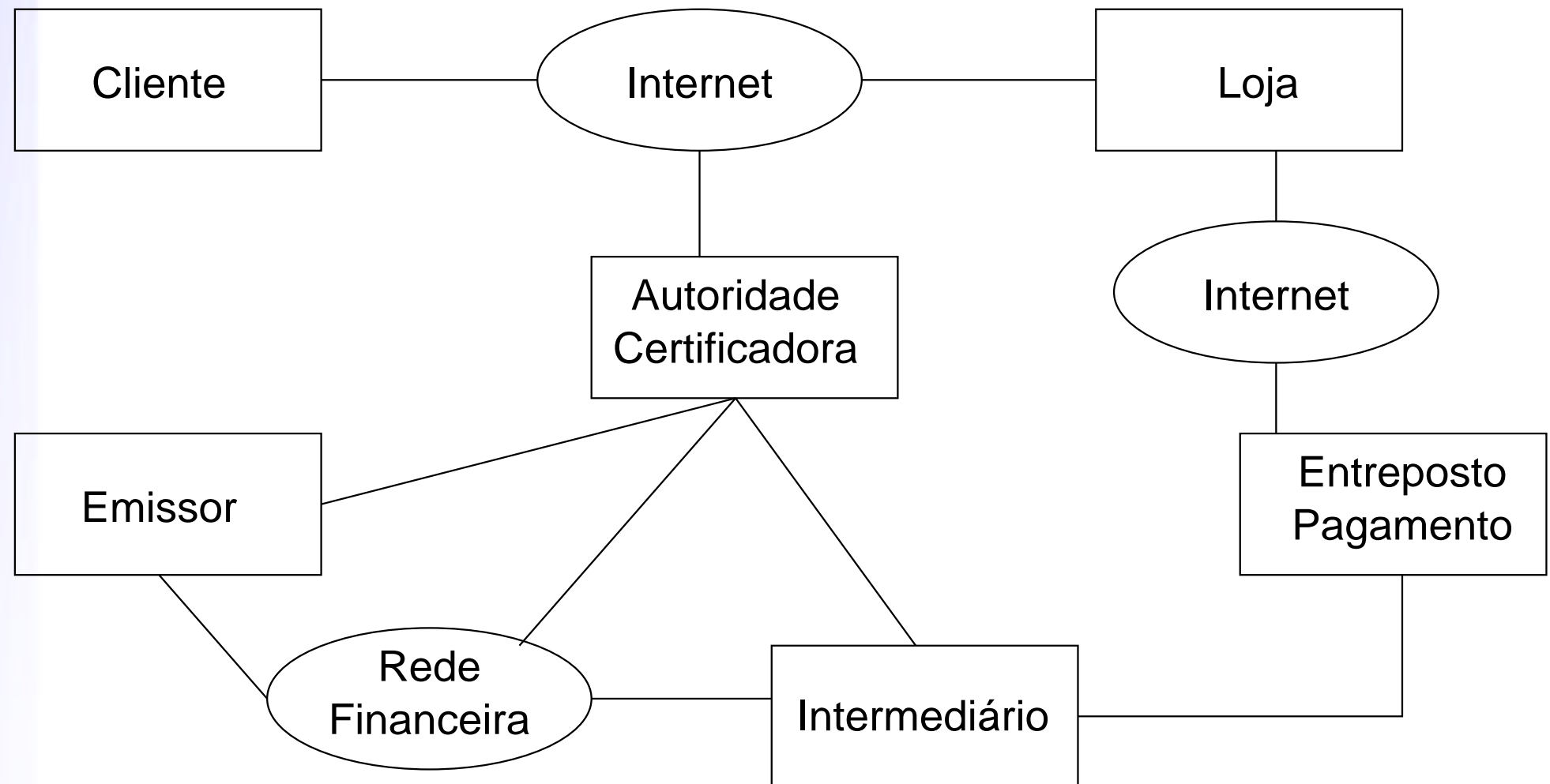
SET

Propriedades Fundamentais

- Confidencialidade da informação
 - dados de cartão são transmitidos de forma segura e loja não tem acesso a eles
- Integridade de dados
 - uma única mensagem, não alterável e contendo todas as informações
- Identificação positiva
 - todos os participantes utilizam certificados digitais

SET

Participantes



Transação de Pagamento

- Estabelecimento de relação comercial
 - cliente obtém cartão de crédito
 - cliente recebe certificado
 - loja recebe certificados
- assinar mensagens
- se identificar junto aos clientes

Transação de Pagamento

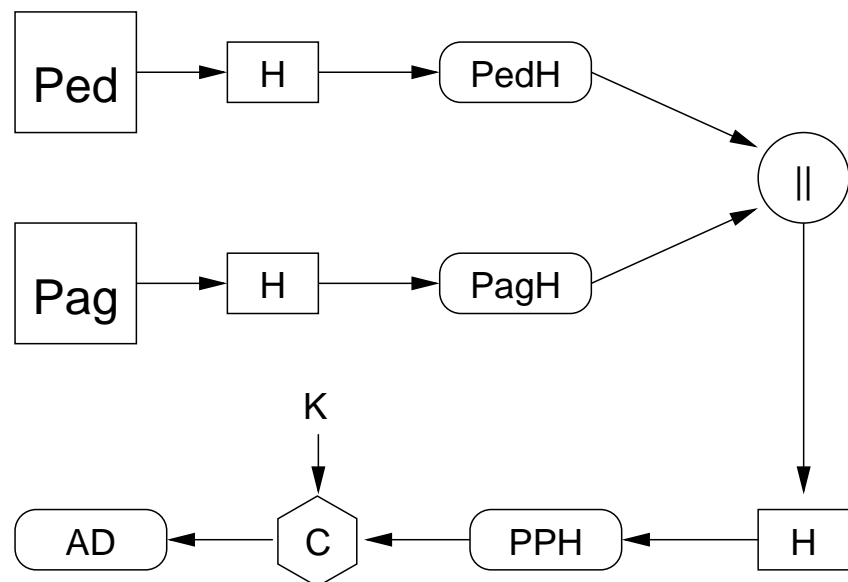
- Compra
 1. cliente coloca pedido
 2. loja é verificada
 3. pedido e pagamento são enviados
 4. loja requisita autorização de crédito
 5. loja confirma pedido
 6. loja entrega bens e serviços
 7. loja requisita o pagamento

SET

Requisição de Compra

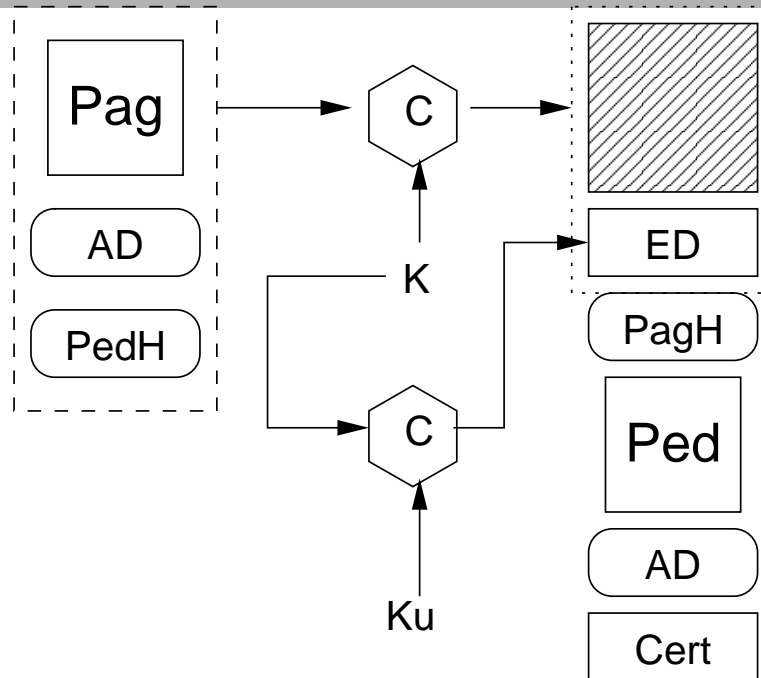
- Início requisição
 - cliente requisita certificados
- Resposta inicial
 - certificados são enviados criptografados
- Pedido
 - informações de pedido e de pagamento assinadas digitalmente
- Confirmação do pedido

Assinatura Dual



Ped	Info pedido	Pag	Info pagamento
H	Função hash	C	Cifragem
PedH	Sumário pedido	PagH	Sumário pagamento
	Concatenação	K	Chave cifragem
PPH	Sumário pagamento e pedido		
AD	Assinatura digital		

Mensagem de Pedido



Ped Info pedido

AD Assinatura digital

ED Envelope digital

PedH Sumário pedido

Ku Chave pública banco

Pag Info pagamento

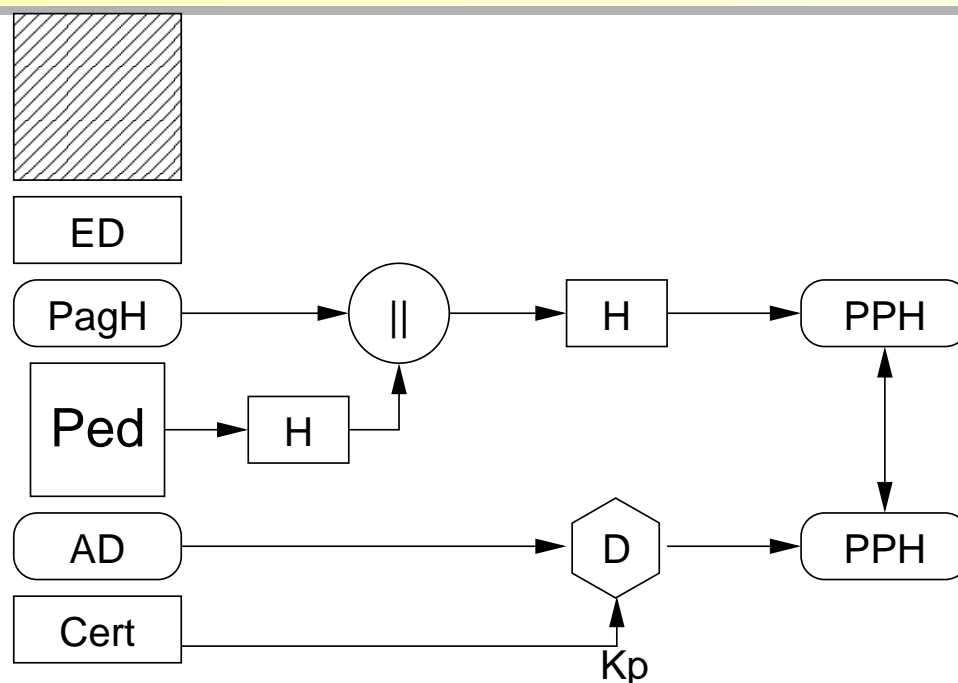
Cert Certificado cliente

C Cifragem

PagH Sumário pagamento

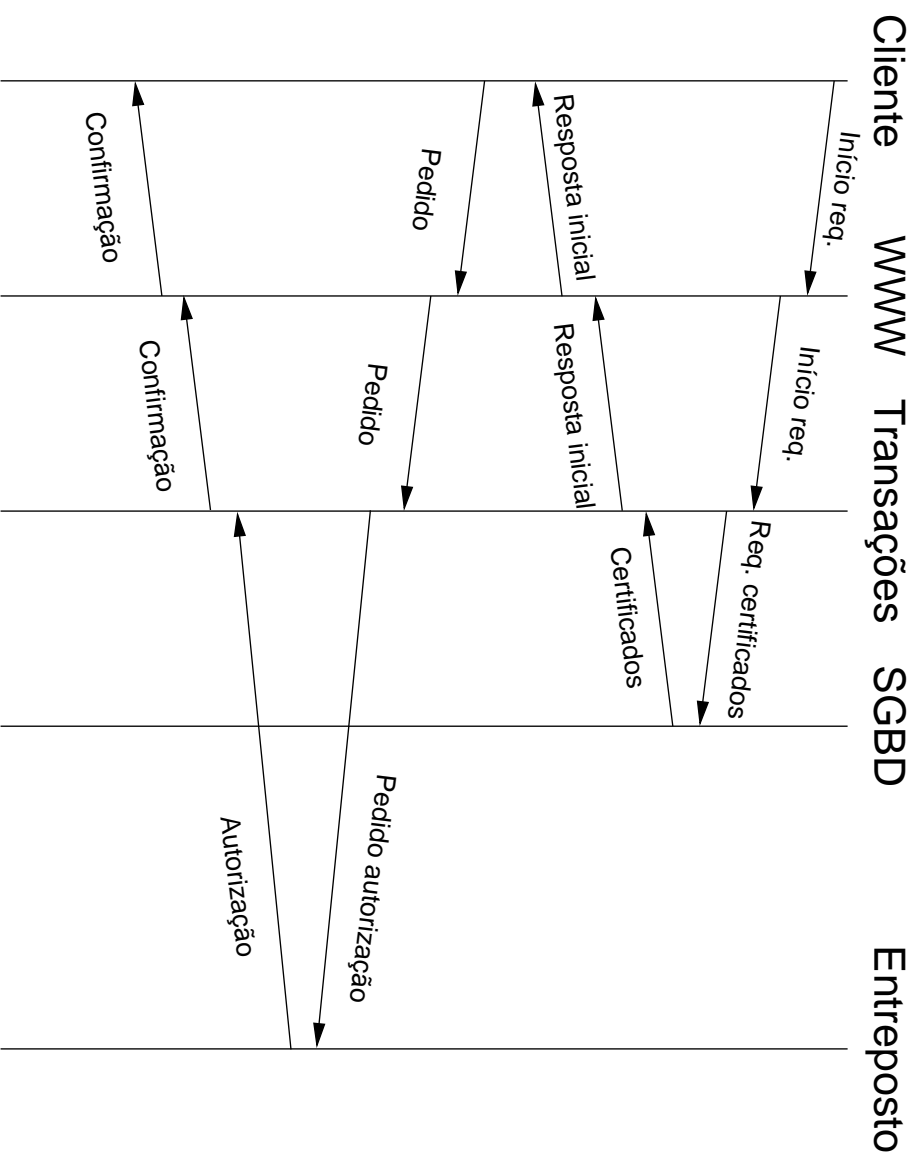
K Chave cifragem cliente

Verificação da Mensagem de Pedido



Ped	Info pedido	PPH	Sumário pagamento e pedido
D	Decifragem	Cert	Certificado cliente
ED	Envelope digital	AD	Assinatura digital
H	Função hash	PagH	Sumário pagamento
	Concatenação	Kp	Chave pública cliente

Protocolo para Requisição de Compra



Requisição de Compra

Nível Funcional

- Ação: autorizar
- Atributos: preço, dados do cliente e dos produtos adquiridos
- Distribuição: motivada pela legitimidade da administradora de cartões de crédito
- Meio: transmissão segura e certificada
- Atomicidade: robusta
- Processamento: aritmética, processamento de cadeias de caracteres, acesso Internet

Requisição de Compra

Endereçamento

- Utiliza requisições POST [http://entrepasto.com.br/autpag= <info pagamento> env= <envelope digital> certcli= <certificado cliente> certloja= <certificado loja>](http://entrepasto.com.br/autpag=<info%20pagamento>env=<envelope%20digital>certcli=<certificado%20cliente>certloja=<certificado%20loja>)

SET Tolerância a Falhas

- Falhas de comunicação
 - retransmissão até um número máximo de tentativas
 - no caso de erro, loja posterga confirmação ao cliente