Segurança em Transações Eletrônicas

A criptografia e o gerenciamento de chaves em terminais POS

Eu: Moisés Guimarães de Medeiros

- Especialista em Segurança da Informação – FATEC JP;
- Tecnólogo em Sistemas para Internet – IFPB;
- Desenvolvedor C na Phoebus Tecnologia desde 2006;
- Fascinado por criptografia;
- Músico, Atleta e N3rd.

Terminais POS

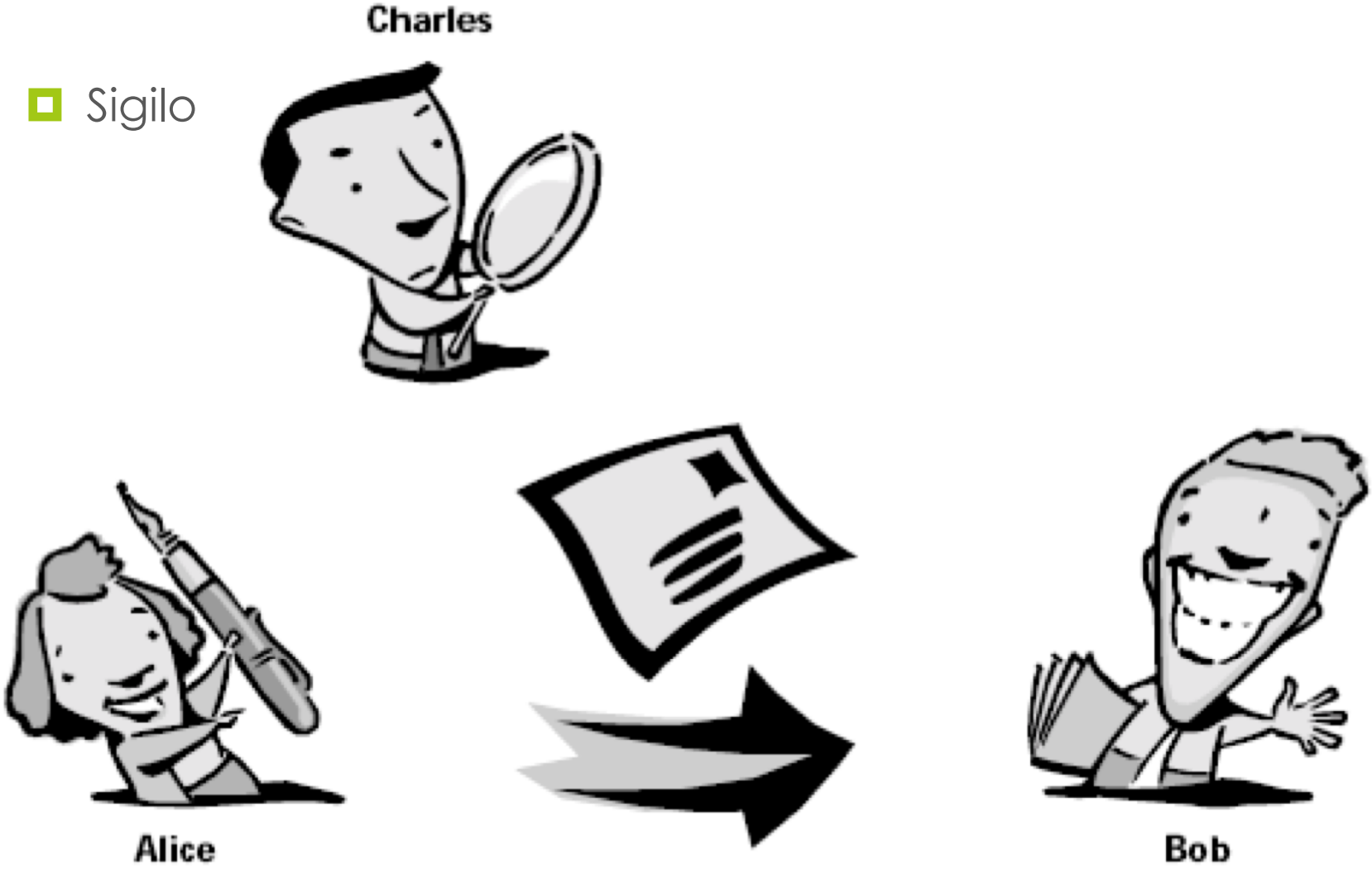
- Aprox. de 512KB a 16MB de RAM
- Impressora Térmica
- Display LCD
- Teclado integrado com **PinPad**
- Comunicação:
  - Ethernet
  - GPRS
  - Dial
- Lê cartões magnéticos e com chip

Cenário

- Recursos limitados
  - Baixa capacidade de processamento.
  - Pouca quantidade de RAM disponível.
  - Conectividade precária ou limitada.
- Tempo de resposta é crucial
  - O consumidor quer pagar e ir embora.
  - O lojistas quer atender mais consumidores/min.
  - O nosso cliente quer a transação aprovada em segundos.
- Segurança
  - Os dados do consumidor devem ser preservados.

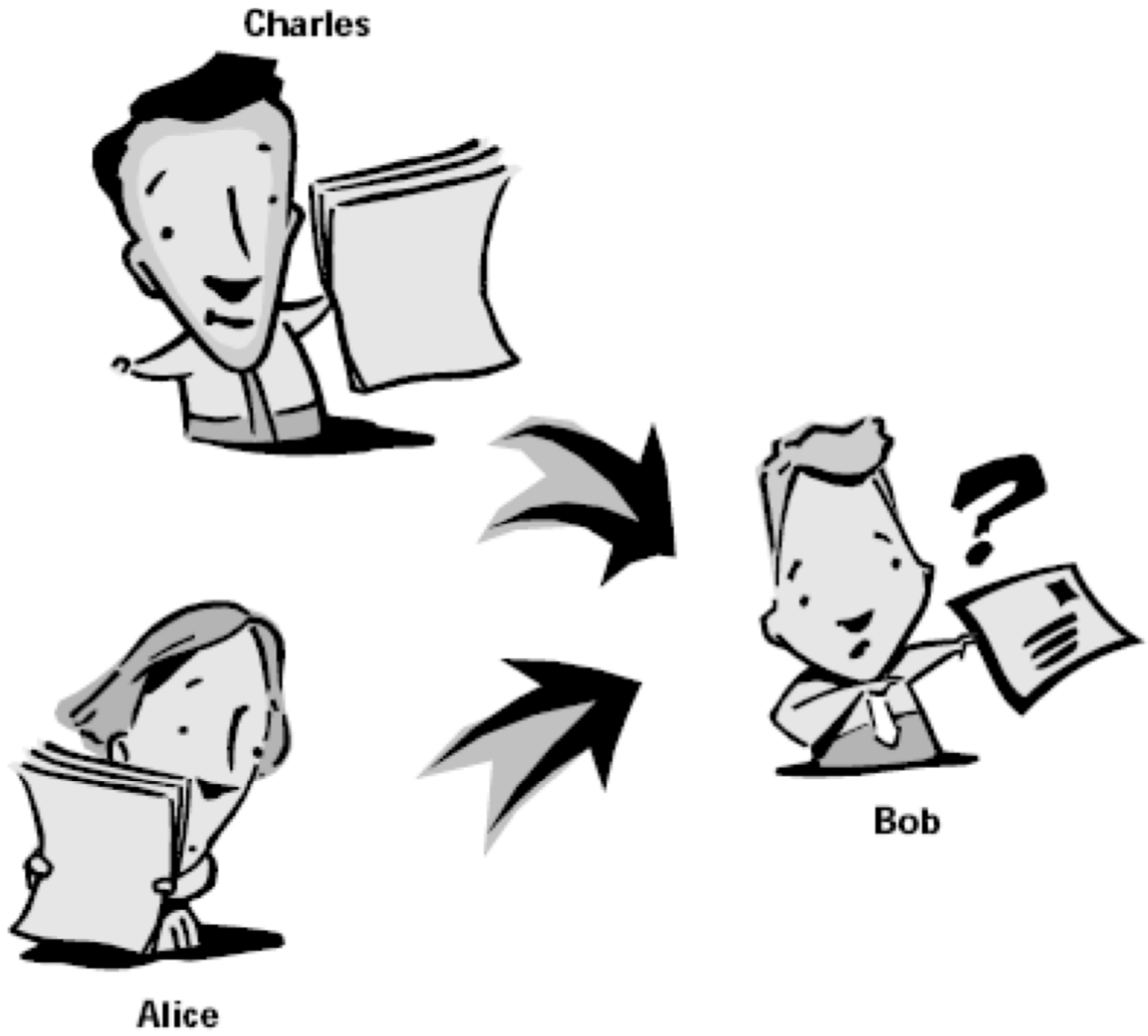
Comunicação Segura

- Sigilo



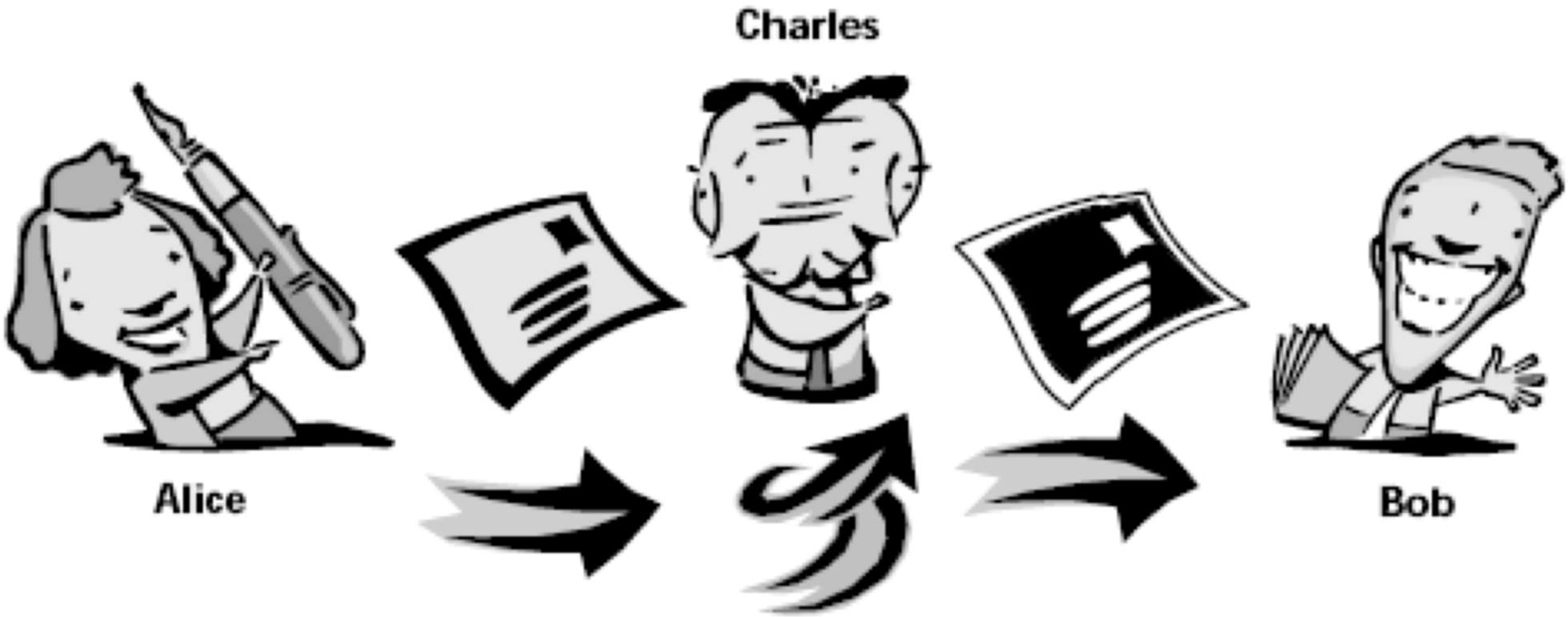
Comunicação Segura

- Autenticidade

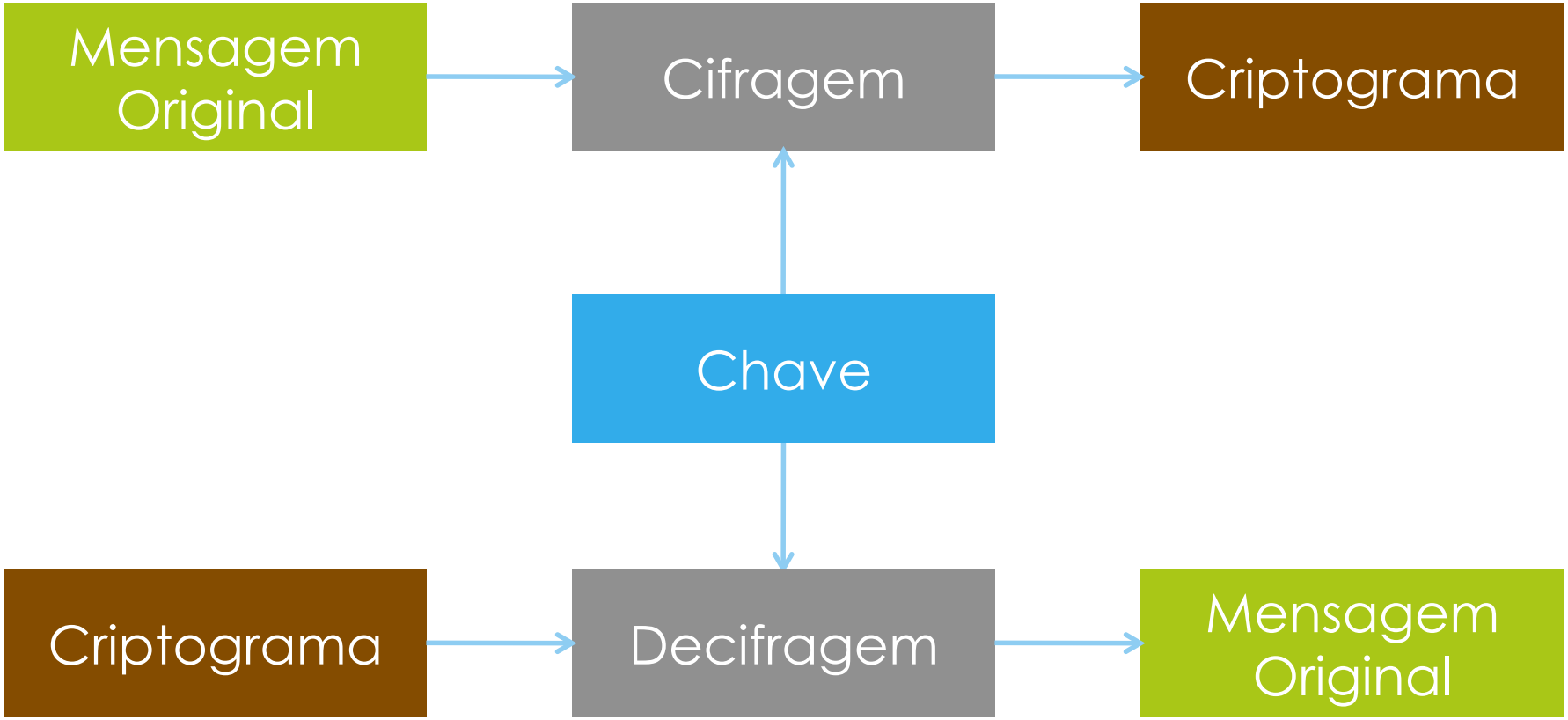


Comunicação Segura

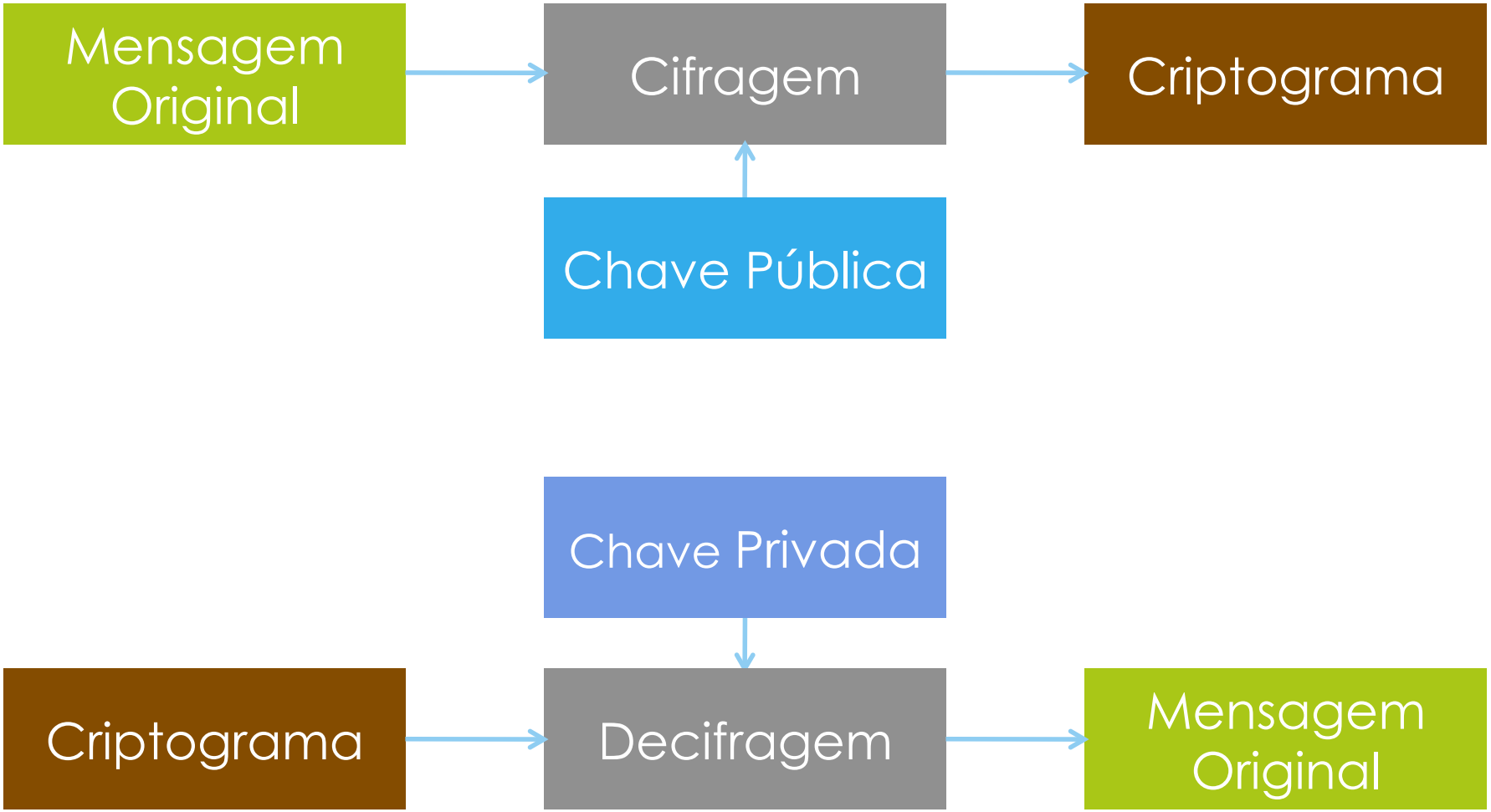
- Integridade



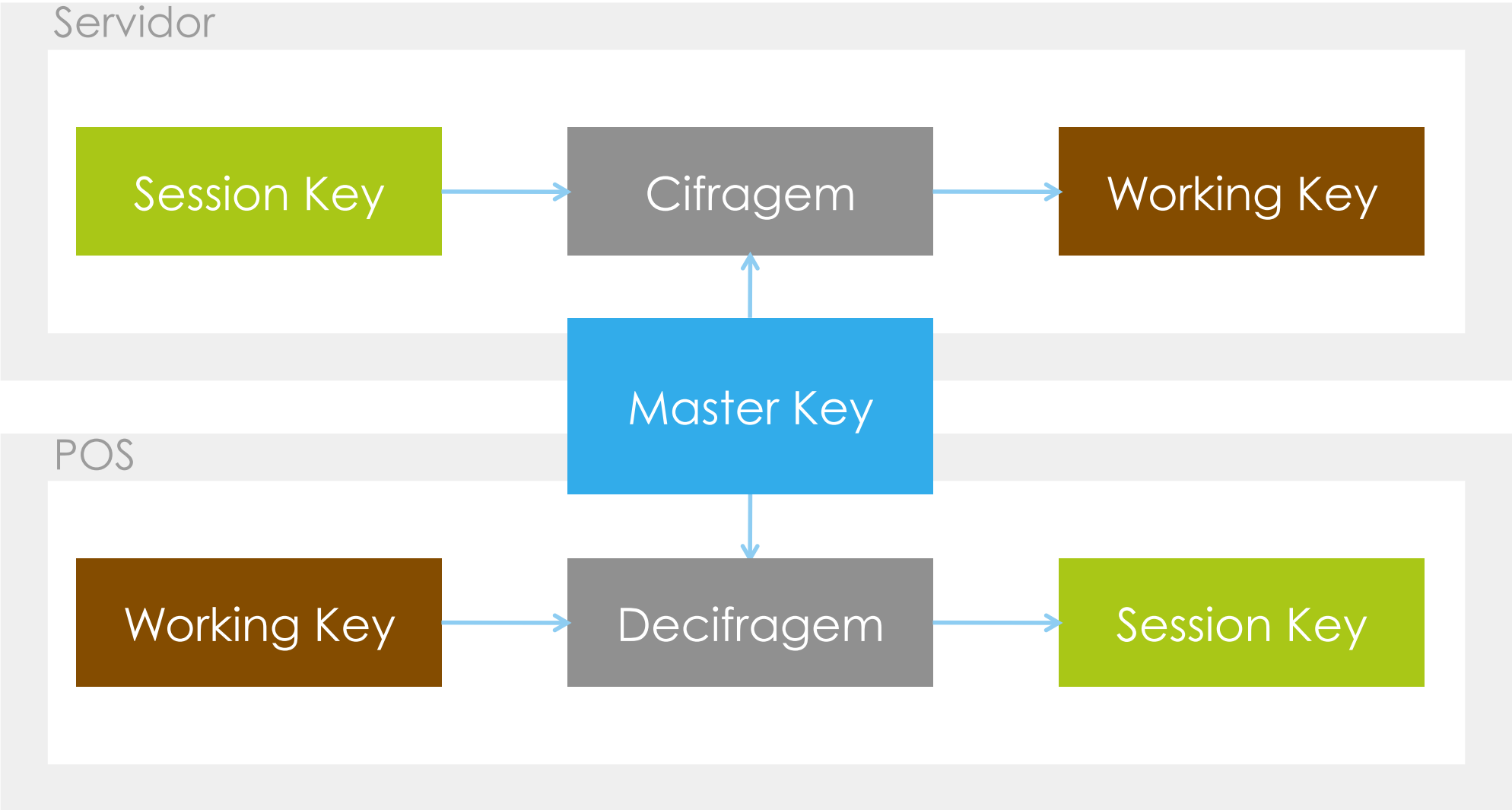
Criptografia Simétrica



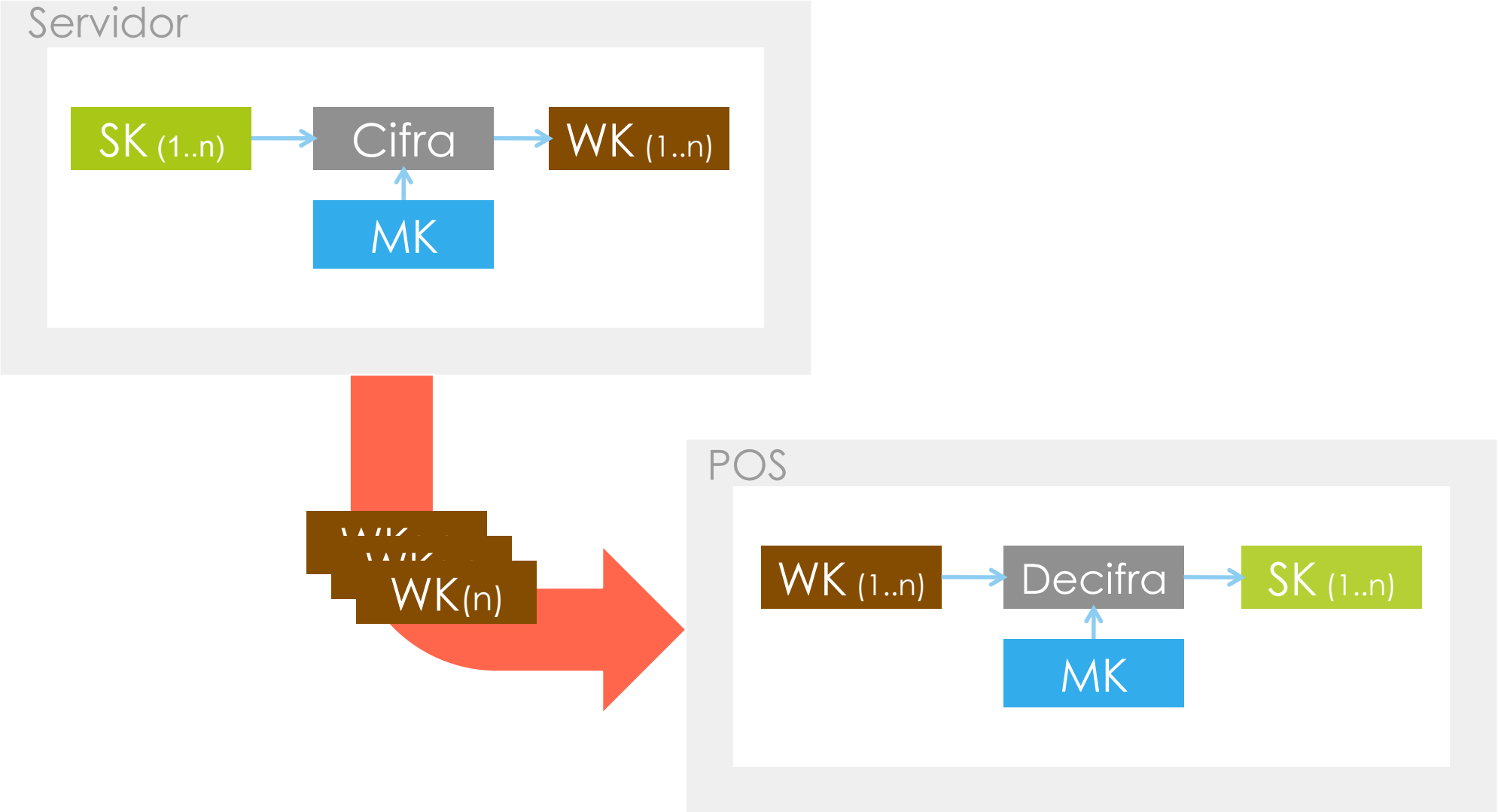
Criptografia Assimétrica



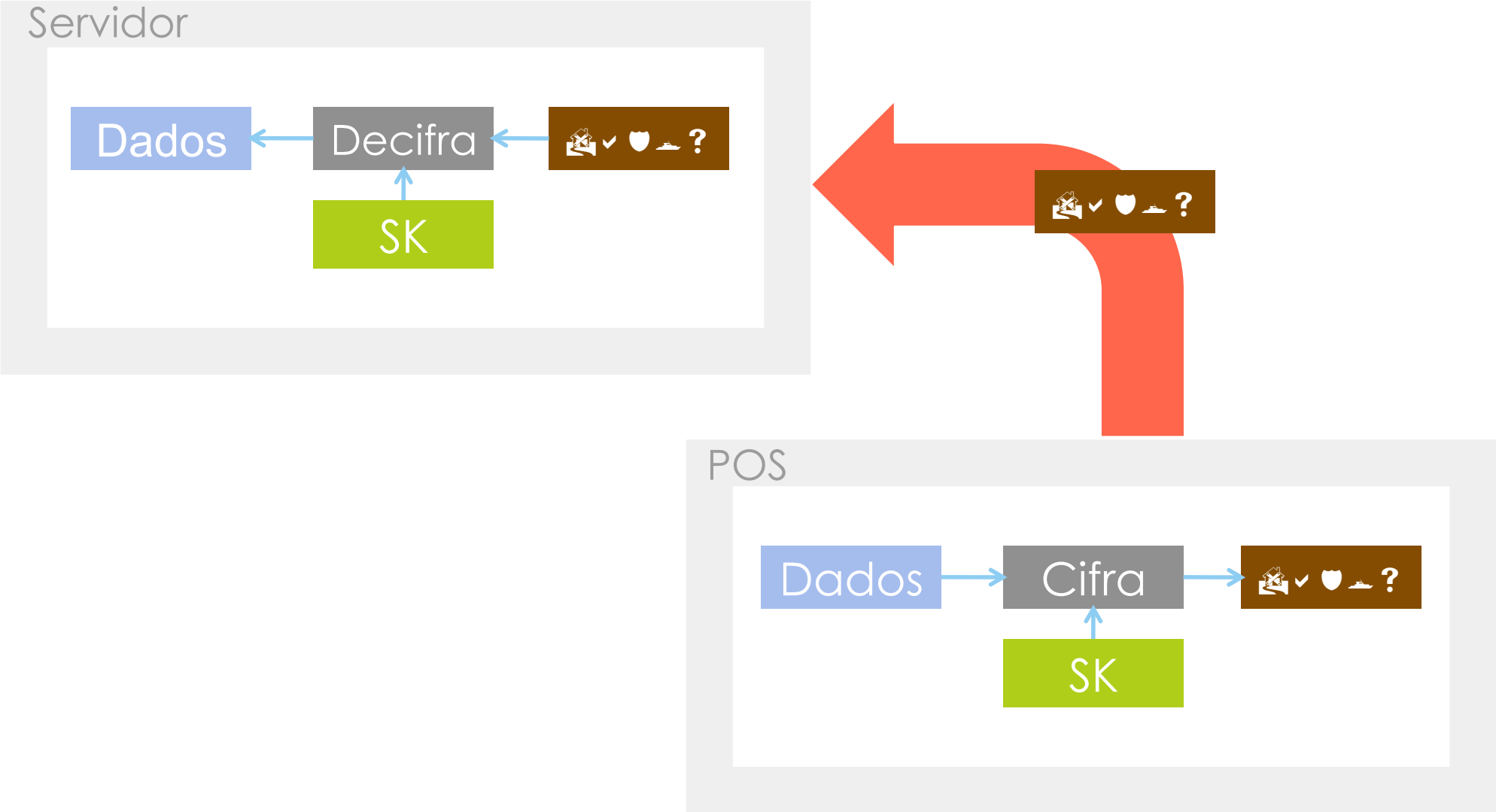
Master Session



Master Session

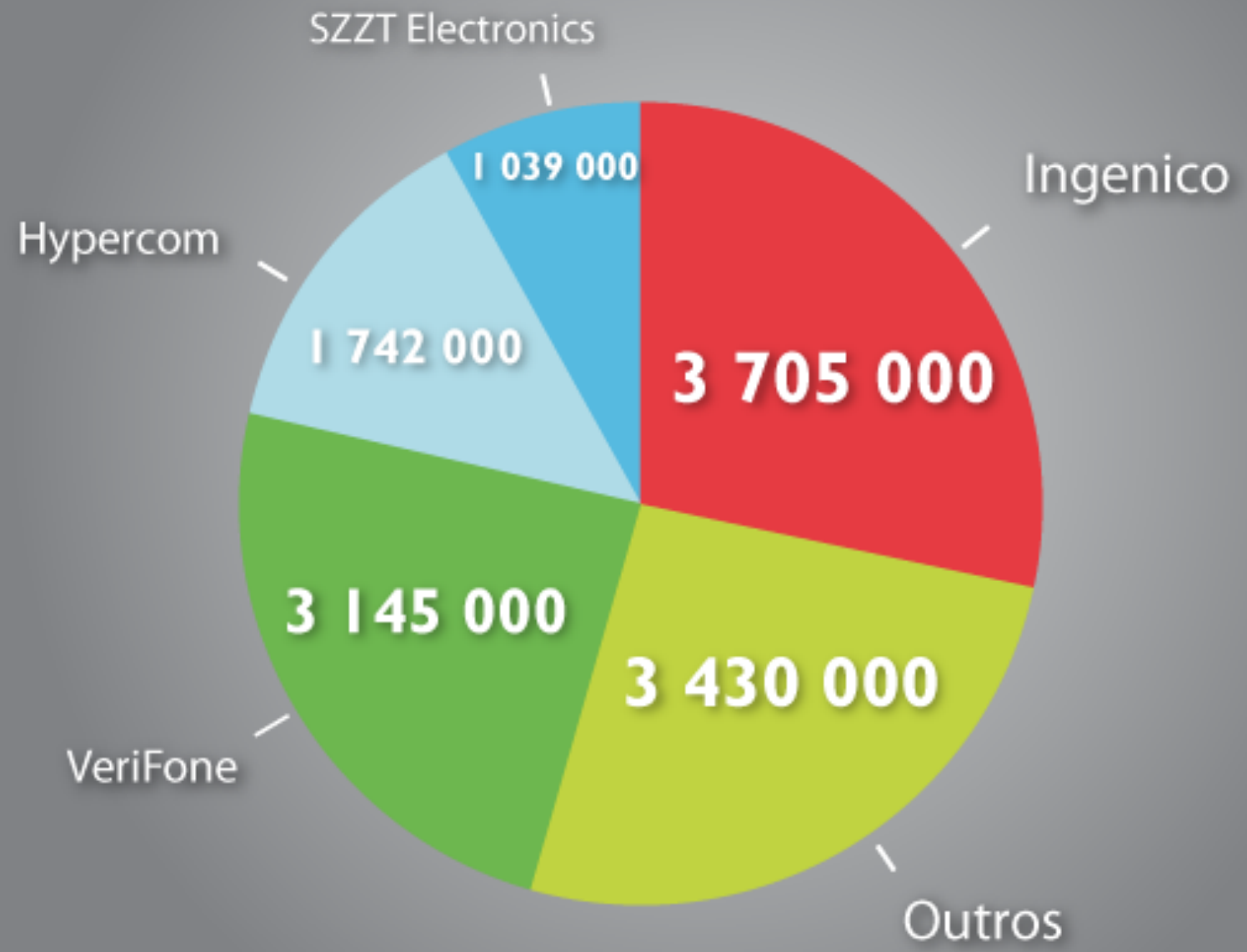


Master Session



Marcas de terminais POS vendidos em 2009

Mundialmente



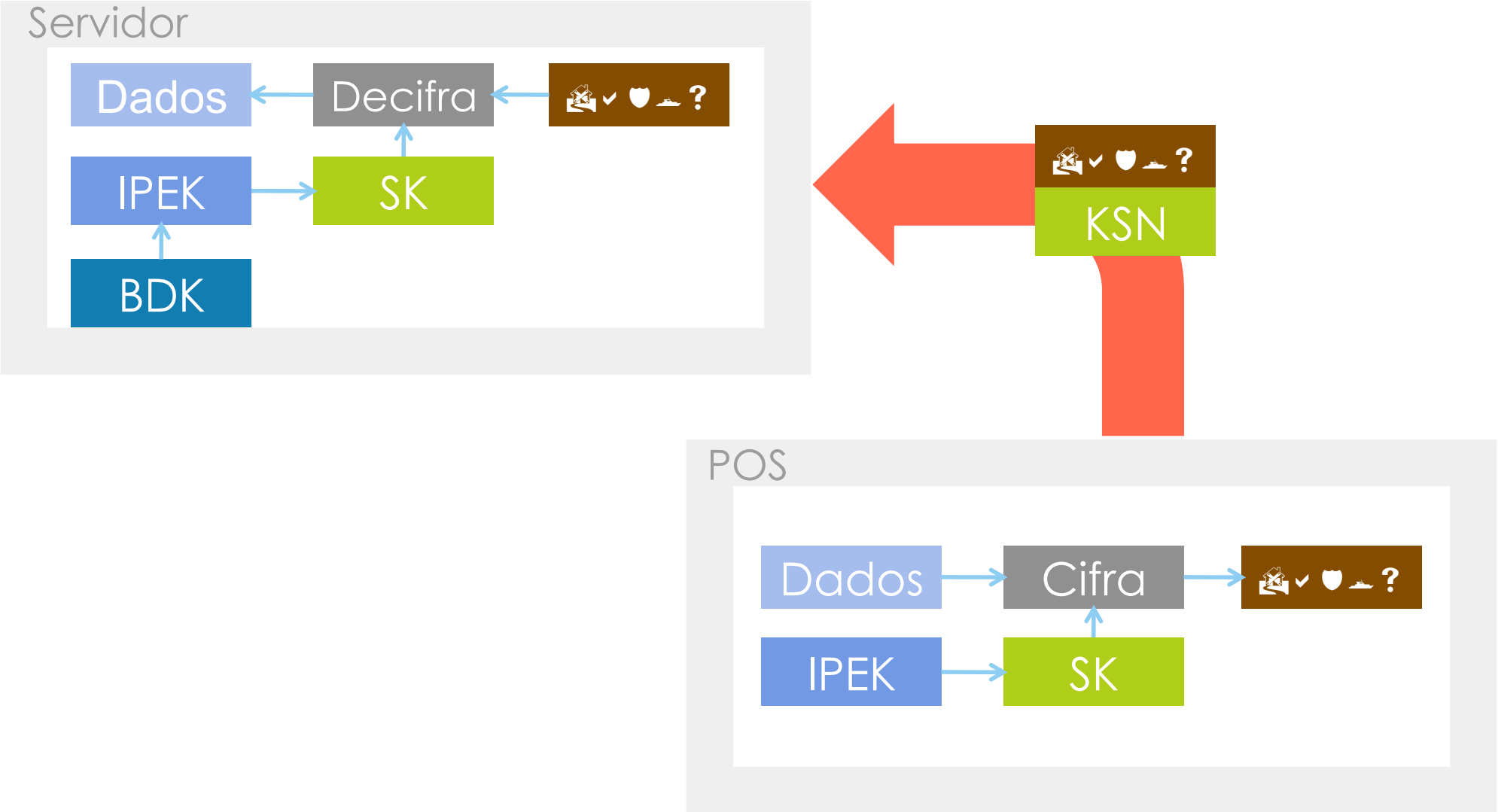
http://blog.plataformawalk.com.br

Fonte: The Nilson Report

DUKPT - Derived Unique Key Per Transaction

- BDK – Base Derivation Key
- IPEK – Initial PIN Encryption Key
- KSN – Key Serial Number

DUKPT


Servidor
Dados
Decifra
?
IPEK
SK
BDK
?
KSN
POS
Dados
Cifra
?
IPEK
SK

Perguntas

Contato

- @moisesguimaraes