

# Novidades em ICP

Mudanças Silenciosas e Profundas

Dr. Roberto GALLO

gallo@kryptus.com

FORUM RNP 2017

# Empresa

**kNET** network  
HSM



## Alguns destaques

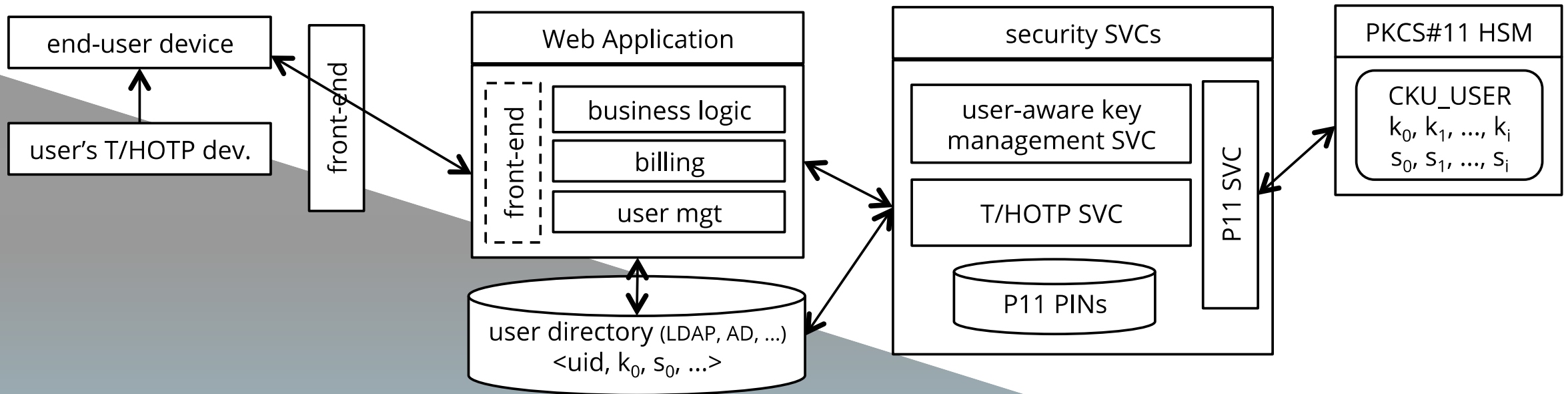
- Gartner Cool Vendor;
- Empresa Estratégica de Defesa - EED;
- Especialista em Criptografia há 14 anos;
- Presente em mais de 50% das ACs ICP-Brasil'

## O Que Refreia o Uso de Certificação Digital?

- Inconveniência do uso de smart cards e tokens físicos
- A insegurança da manutenção de chaves em software
- A complexidade de integração no *end-point* de usuário
- A complexidade de integração no *back-end*

# Exemplo

## Assinatura em Nuvem com P11

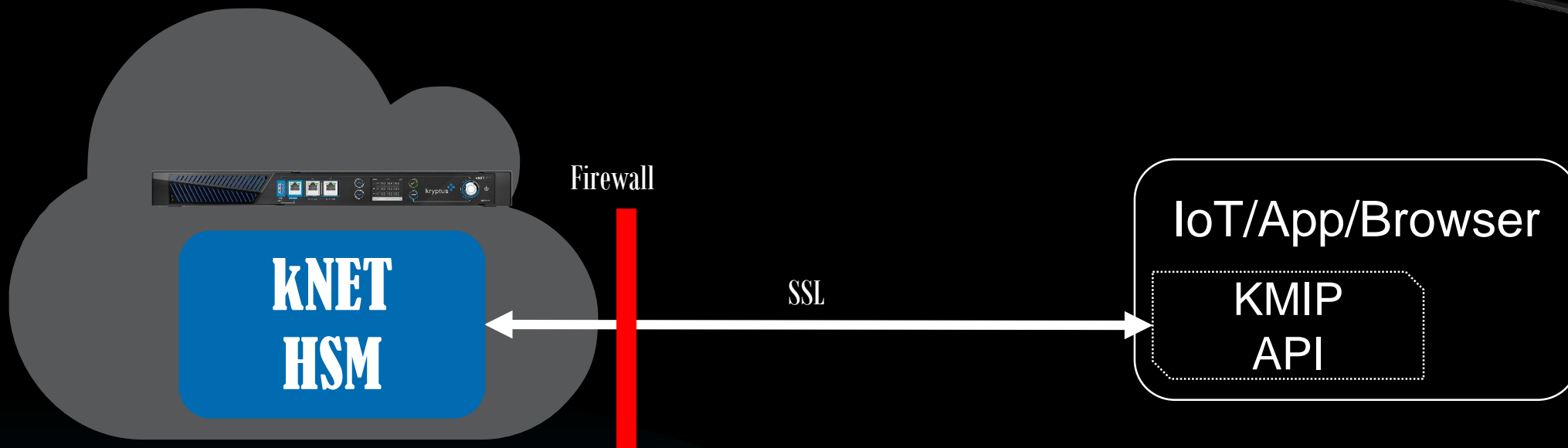


### KMIP/OASIS muda o jogo

- Protocolo de gestão de chaves e de serviços criptográficos
- Pensado em nuvem, com mensagens XML, JSON
- Extremamente fácil de integrar
- Viabiliza certificação digital em múltiplos cenários (nuvem, IoT)
- Extensível, facilidade para Criptografia Pós Quântica

# Caso de **Uso**

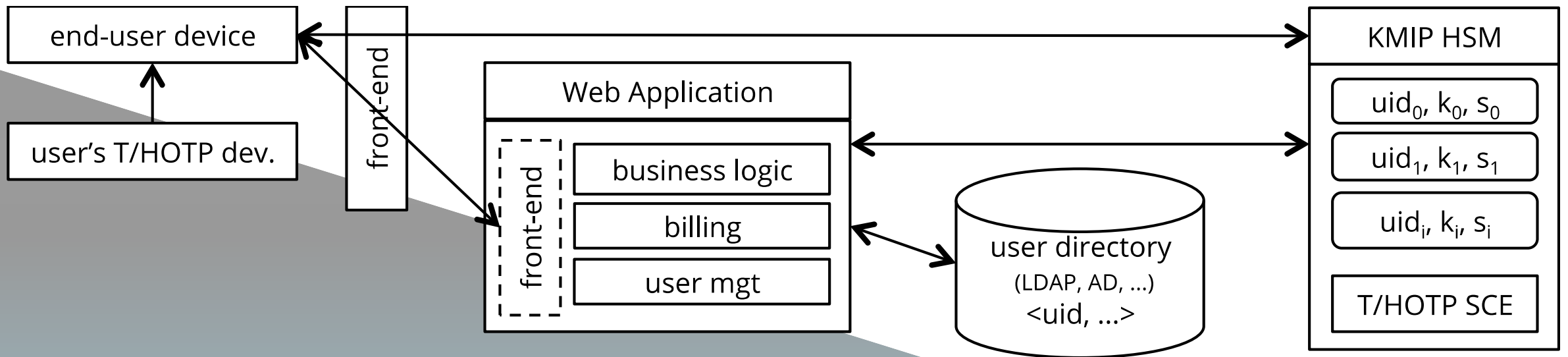
**kNET** network  
HSM



Conexão direta entre o HSM e o dispositivo, sem necessidade de drivers via Socket em formatos como JSON e XML.

# Exemplo

## Assinatura em Nuvem com KMIP



# KMIP

## Benefícios

kNET network  
HSM



### Principais Benefícios

- Unificação de proteção serviços de nuvem;
- Segurança no uso de nuvens externas;
- Blindagem de nuvens privadas;
- Blindagem de aplicações de missão crítica
  - Via execução segura de software;
- Alta interoperabilidade;
- Facilidade no desenvolvimento de software;
- Interface KMIP
  - Interoperabilidade;
  - Facilidade no desenvolvimento de apps;
  - Elimina infraestrutura;

### Aplicações

- Assinatura em nuvem
- Cifração de bancos de dados:
  - Amplo suporte (FLOSS e comerciais);
  - Gestão segura de chaves;
- Cifração de disco de servidores Linux;
- Proteção no uso de serviços de nuvem;
  - Como Google Drive e Dropbox
- Plataforma segura via OpenStack;
- Aprovisionamento seguro de máquinas virtuais;



# KMIP

## Quem Usa?

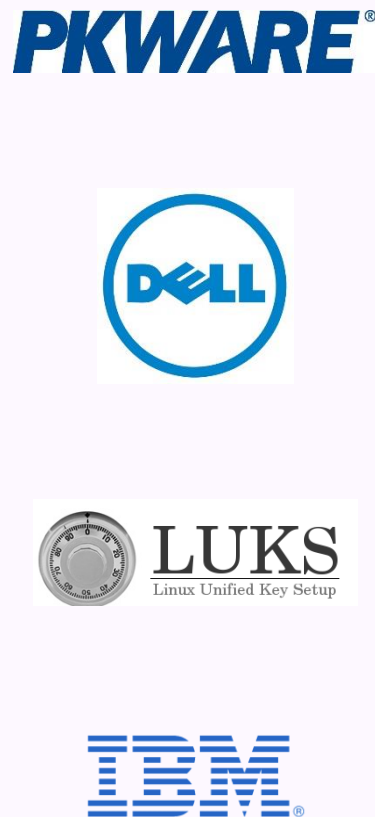
kNET network  
HSM



### Cifração de banco de dados



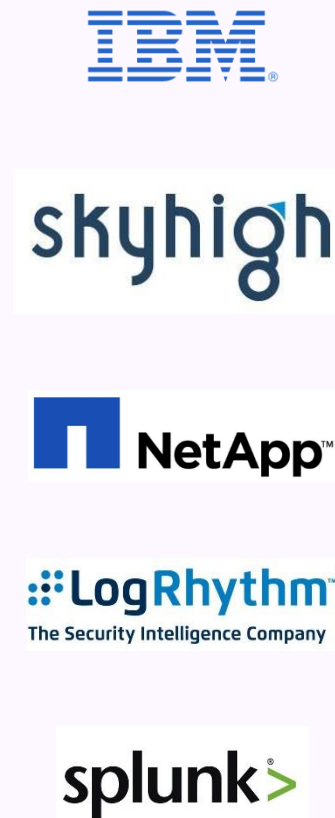
### Cifração de Disco e Arquivos



### Serviços em Nuvem



### Outros



# KRYPTUS kNET HSM

Plataforma de Segurança Criptográfica para a Nuvem

