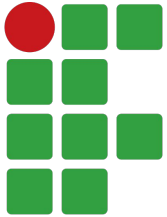


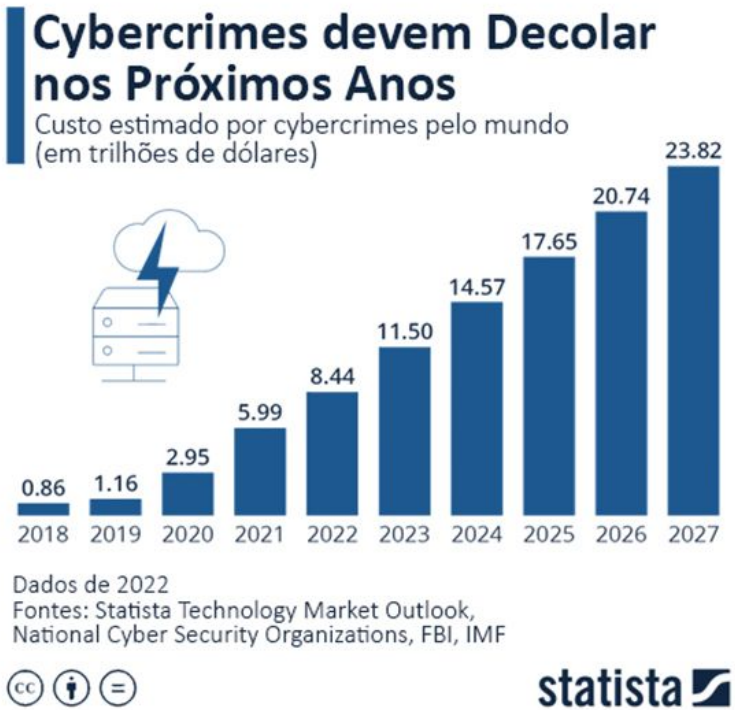
INSTITUTO FEDERAL
Fluminense

Instrumentos de Medição Seguros Baseados em Ambientes de Execução Confiáveis

Eduardo Valente, Eduardo Machado, Gustavo Martins e Wilson Melo Jr.

Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)

Introdução



Com o aumento da frequência e complexidade dos ataques digitais, empresas enfrentam riscos crescentes à segurança de suas operações.

Sistemas de Medição Distribuídos

O que é?

O conceito de DMS é variável. No nosso caso, trata-se de um dispositivo com múltiplos sensores de medição.

Quais os riscos?

DMS podem ser alvo de ataques cibernéticos que alteram as medições coletadas para fins maliciosos.

Trusted Execution Environment

O que é?

É um ambiente seguro dentro de um processador protegido contra acesso não autorizado.

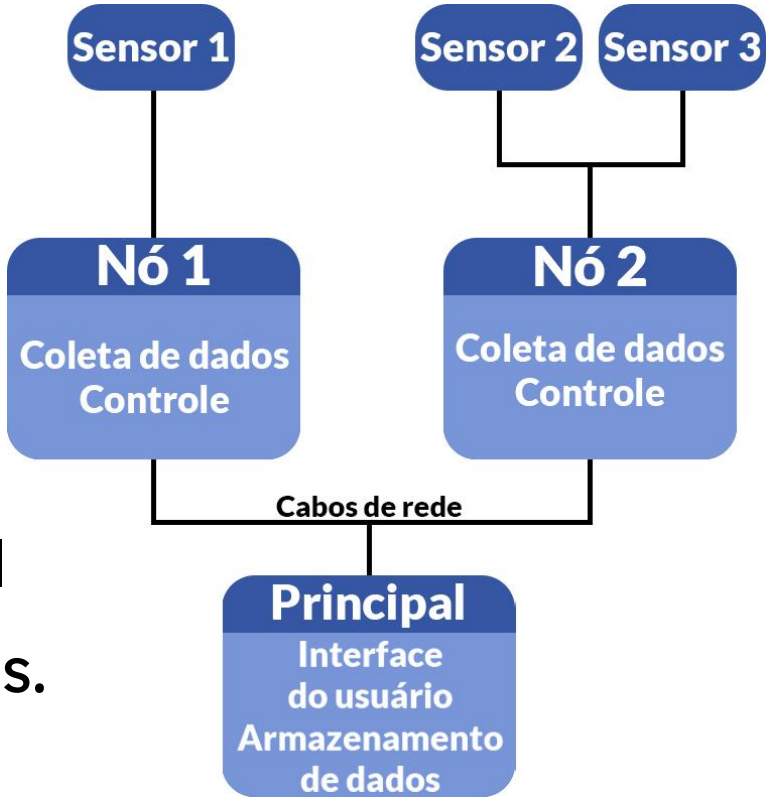
Por que usar um TEE?

Por sua característica de proteção contra adulteração, o TEE permite a execução segura de operações críticas.

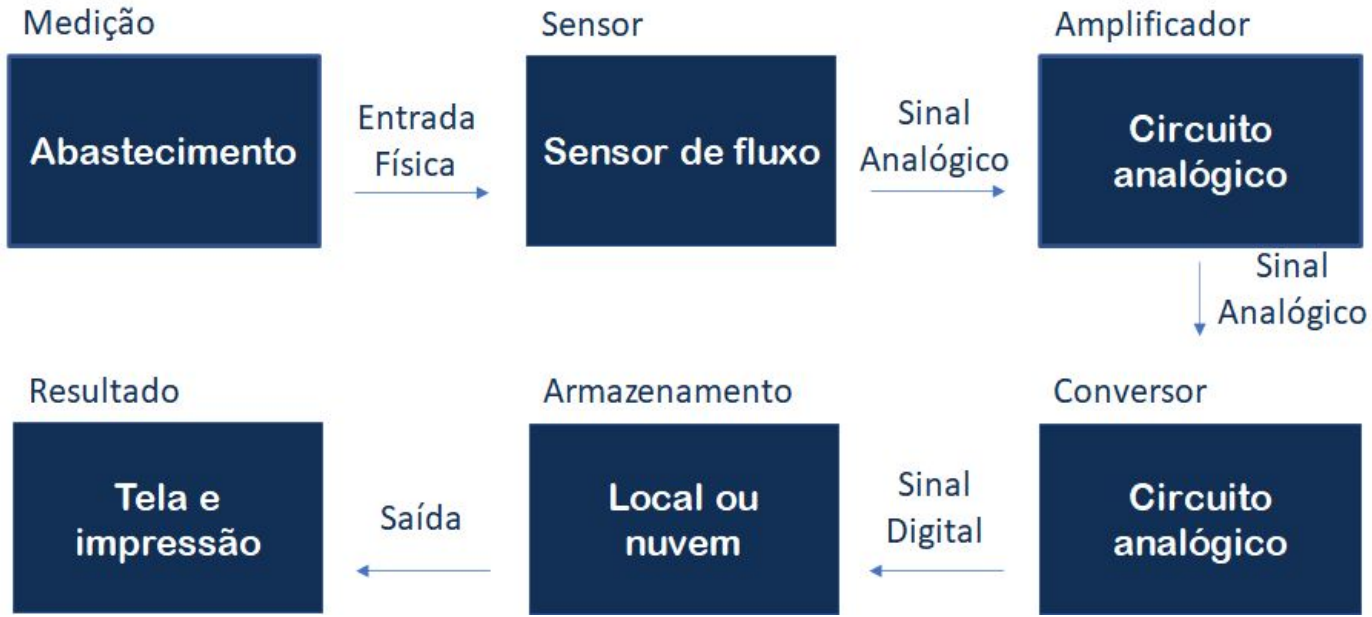
Assinatura de Chave Pública em Ambiente Confiável

Arquitetura que utiliza TEE para aumentar a segurança dos DMS.

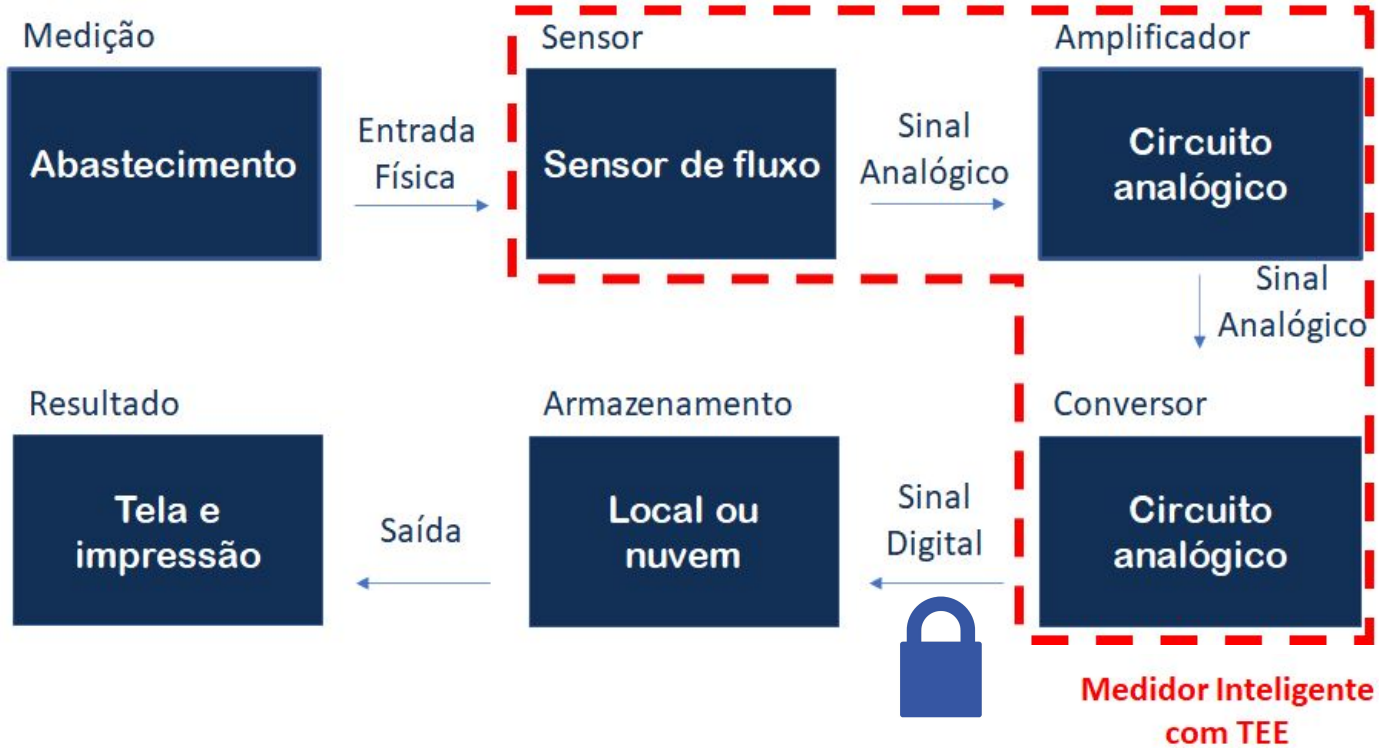
No TEE ocorre a assinatura digital das medições que foram coletadas.



Exemplo de implementação - BMC



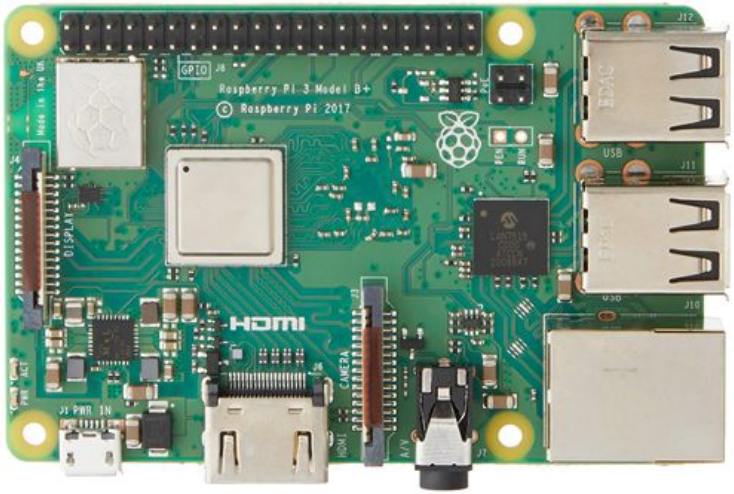
Exemplo de implementação - BMC



Experimento com assinaturas RSA

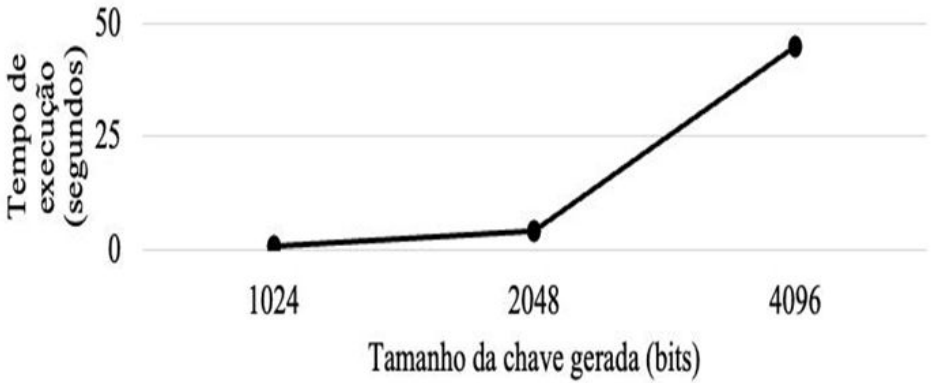
O teste foi realizado em um Raspberry Pi 3B+, que possui a tecnologia Arm TrustZone, usando criptografia RSA, por meio de um script do OP-TEE.

Testamos diferentes tamanhos de chave e registramos seus tempos de assinatura.



Resultados

Percebe-se o aumento considerável no tempo de geração de chaves e assinatura digital.



Um novo script está sendo desenvolvido para utilizar uma chave gravada no TEE.

Próximos passos

- **Criação de um script próprio**
  Remover a geração de chaves do processo;
- **Alteração do script de criptografia**
  Utilizar ECC no lugar de RSA;
- **Realização de mais experimentos**
  Avaliar a repetibilidade dos resultados;

Obrigado!

- Eduardo Valente, Eduardo Machado, Gustavo Martins e Wilson Melo Jr.

- evmartins@colaborador.inmetro.gov.br
- egmachado@colaborador.inmetro.gov.br
- gjmachado@colaborador.inmetro.gov.br
- wsjunior@inmetro.gov.br

MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

INMETRO 50 anos

CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico

INSTITUTO FEDERAL Fluminense

Patrocinadores do SBSeg 2024!

nic.br

cgi.br

Google

Tempest

CAPES

SiDi

FAPESP

zscaler™

BugHunt

CNPq

C.E.S.A.R

FACULDADE IBPTECH