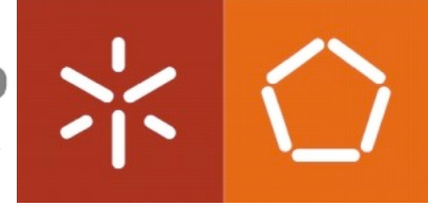
Universidade do Minho
Departamento de Informática



Segurança de Sistemas Informáticos

Vitor Fonte
vff@di.uminho.pt

João Marco Silva
joaomarco@di.uminho.pt

Apresentação

- Avaliação
  - Teóricas (50%) + Práticas laboratoriais(50%)
    - Nota mínima:

8.0 teóricas

10.0 práticas laboratoriais

- Avaliação teórica
  - Um teste final com questões de ambas as componentes

Apresentação

- Práticas laboratoriais
  - Grupos de trabalho - 2 membros
    - Constituição: https://bit.ly/2H4fan4
- 3 trabalhos práticos
  - Trabalhos com igual cotação
  - Submissão via e-learning
    - após o prazo estipulado, o grupo será penalizado em 10% da nota obtida por cada dia de atraso

Apresentação

- Práticas laboratoriais
  - TP 1 - Security awareness
    - Key concepts
    - Vulnerability & Exploits
    - Threat Modelling
    - Risk analysis

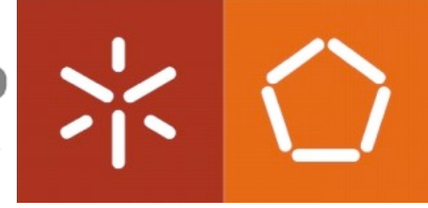
Apresentação

- Práticas laboratoriais
  - TP 2 - Security assessment & tools
    - Data gathering
      - Footprinting / Reconnaissance
      - Active Vs. Passive scanning
      - Assessment tools
        - Scanners; Logging analysis

Apresentação

- Práticas laboratoriais
  - TP 3 - Security technologies & protection
    - Exploitation
    - Protection tools
      - IDS/IPS; Firewalls; ACL; FUSE

Universidade do Minho
Departamento de Informática



Segurança de Sistemas Informáticos

Vitor Fonte
vff@di.uminho.pt

João Marco Silva
joaomarco@di.uminho.pt

Sistema referência

mID

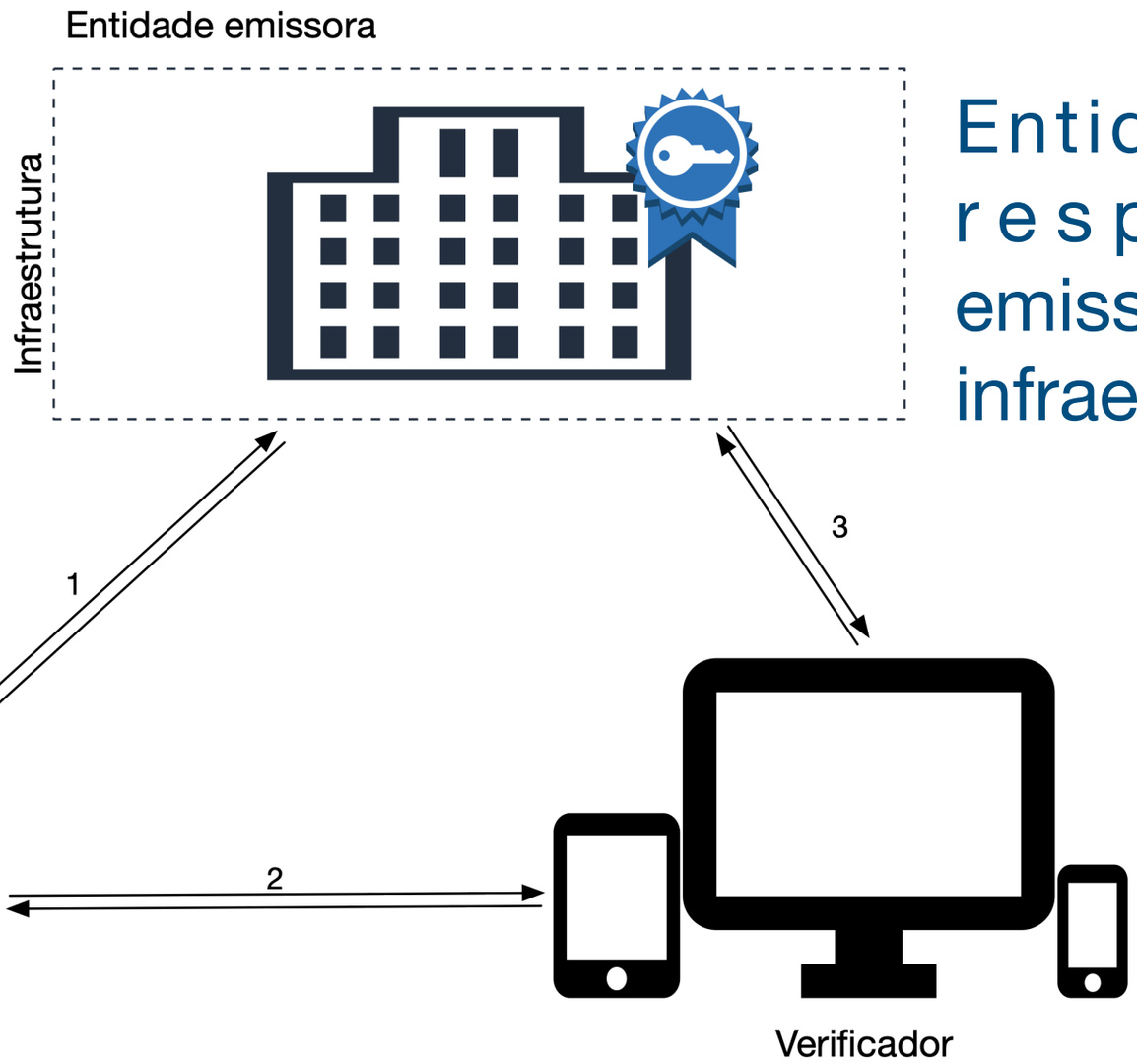
Sistema confiável de identificação pessoal digital e móvel.

- Solução de identificação pessoal para *smartphones*
- Arquitetura orientada a serviços
- Sustentado por protocolos abertos e *standards*

Principais requisitos

- *Secure by design*
- Confiável
- Interoperável
  - Controlo do utilizador sobre o que é revelado em transações
    - Privacidade
  - Funcione em ambiente sem conectividade com a infraestrutura
  - Flexível
    - Suporte a novas funcionalidades e serviços ao longo do ciclo de vida

Entidades envolvidas

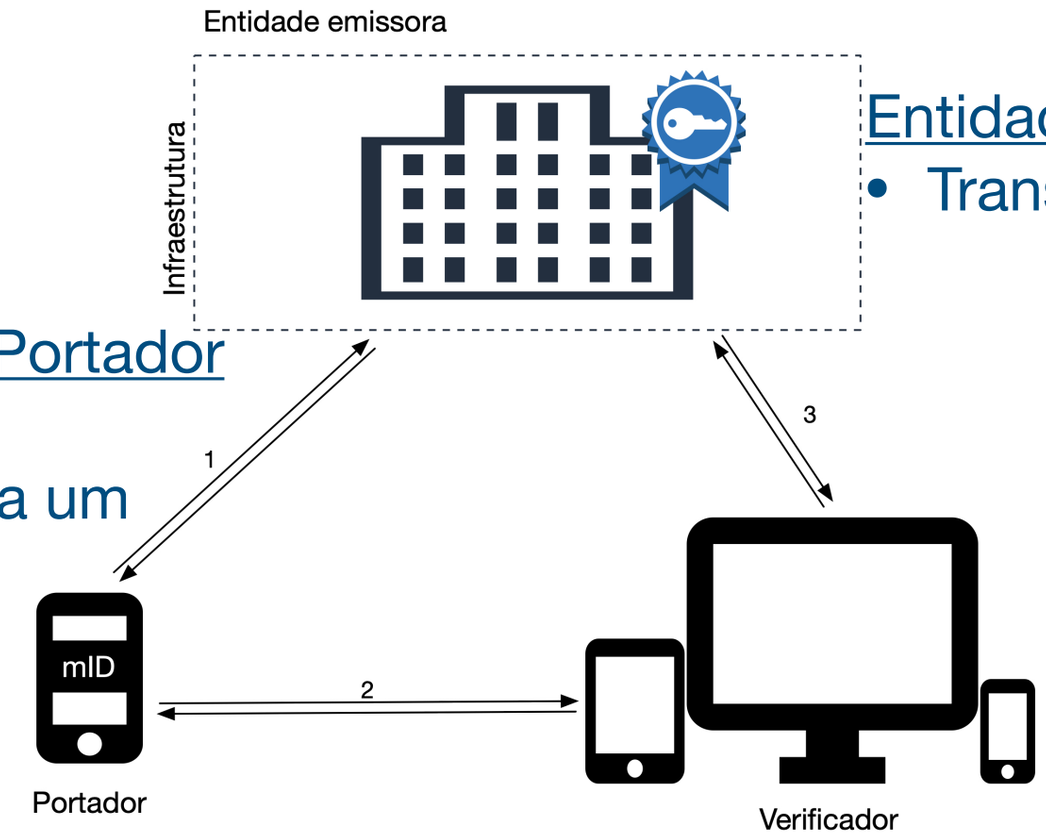


Entidade autoritativa responsável pela emissão da mID e pela infraestrutura de suporte

Cidadão com acesso a um smartphone que armazena a mID

Entidade terceira com acesso a um leitor de mID

Principais interações



[Entidade emissora <-> Portador]

- Adesão
- Associação de uma mID a um dispositivo móvel
- Atualização de dados

[Entidade emissora <-> Verificador]

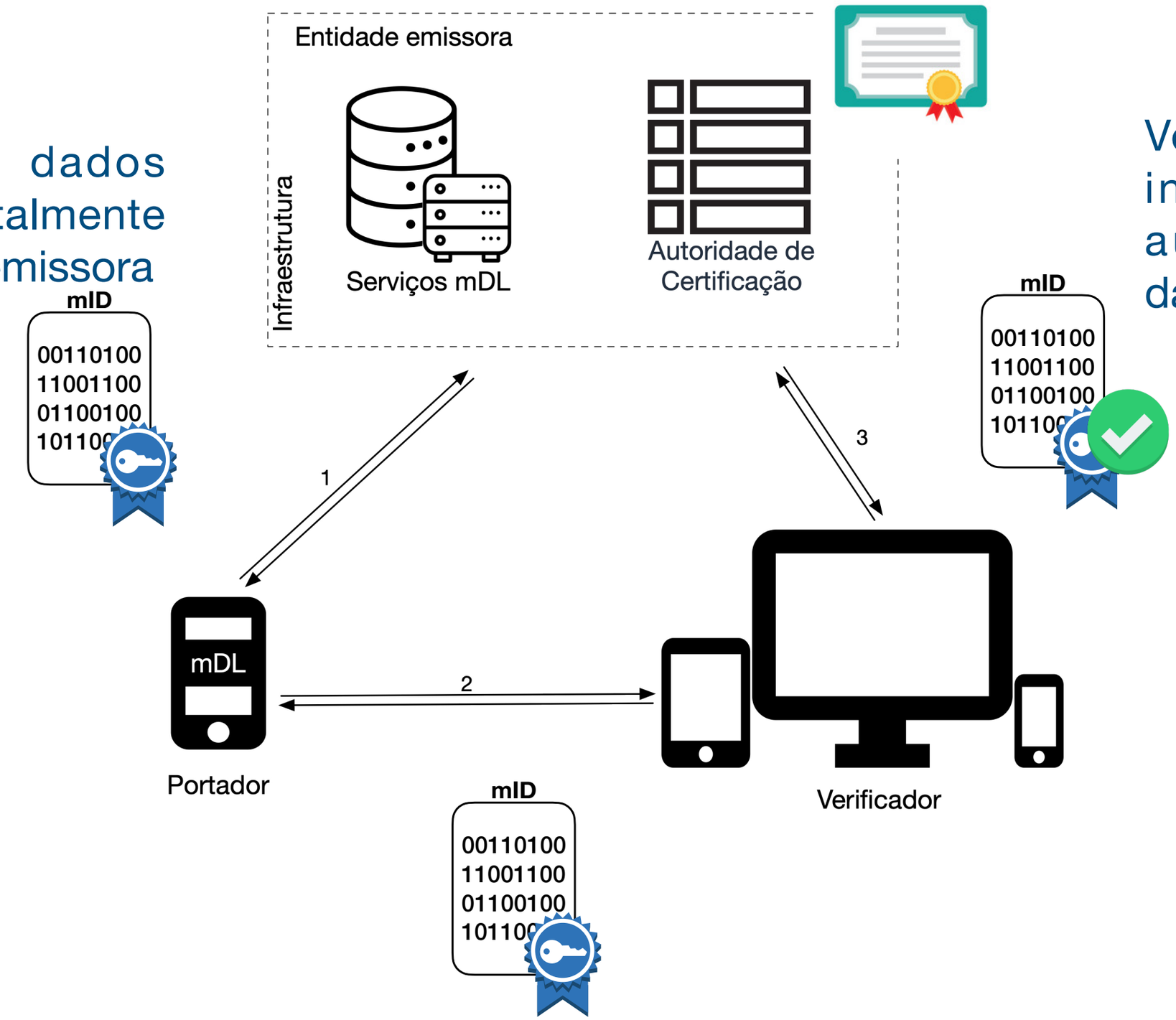
- Transmissão online de atributos

[Portador <-> Verificador]

- Transmissão de atributos
  - Modo *offline* (dados)
  - Modo *online* (*token*)

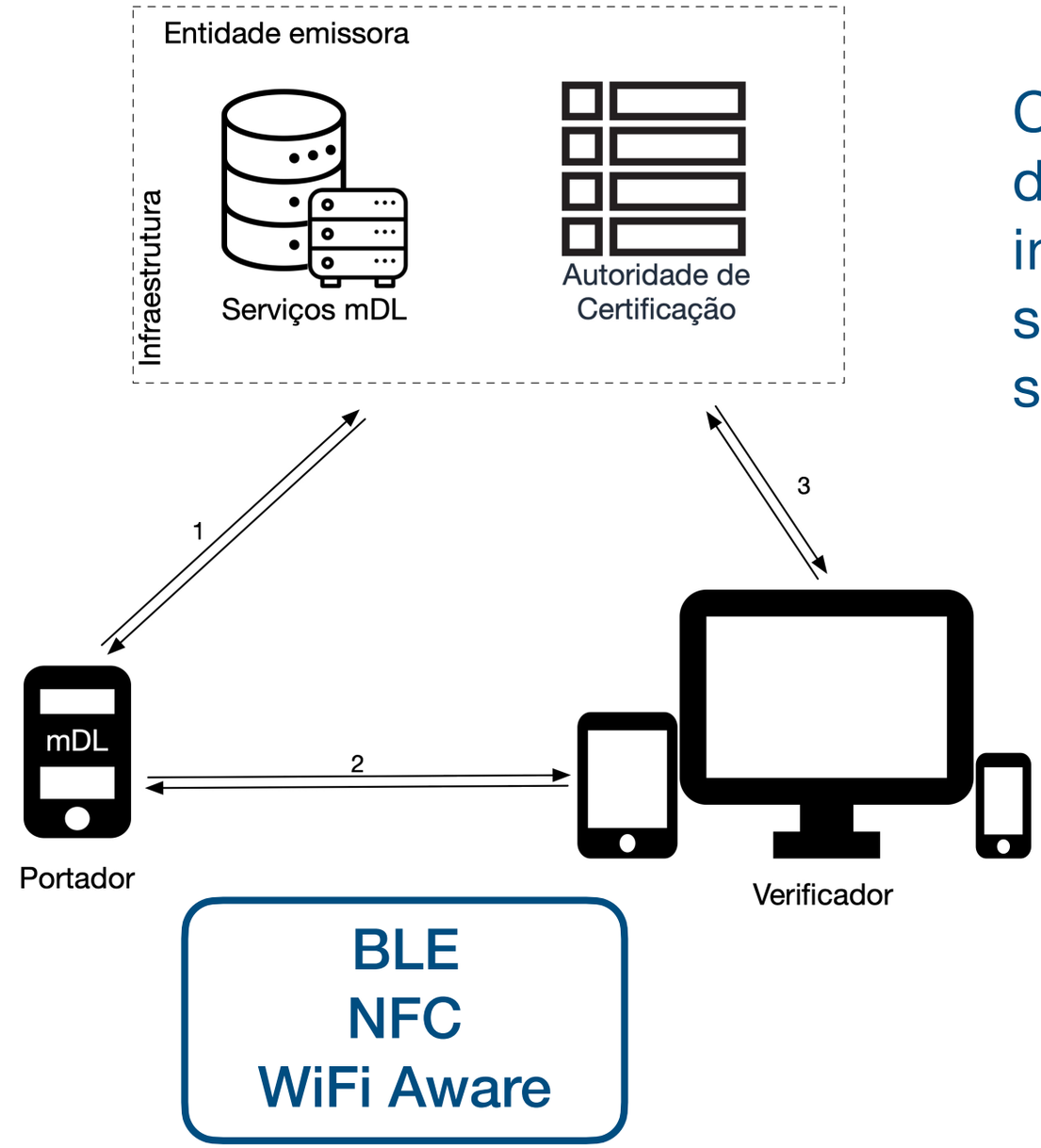
Esquema de confiança

Estrutura de dados assinada digitalmente pela entidade emissora



Verificação da integridade e autenticidade da mID

Estratégias de segurança



Comunicação entre os dispositivos móveis e infraestrutura é feita sobre protocolos seguros

Canal de comunicação entre os dispositivos móveis é cifrado com chaves derivadas

Opcional: entidades que controlam os dispositivos podem ser autenticadas por assinatura de mensagens

Controlo do utilizador

- Uma transação entre dispositivos móveis é **sempre** iniciada pelo portador
  - QR Code
  - NFC
- Transmissão seletiva de dados
  - O portador define quais atributos de identificação são transmitidos para o verificador
    - Tanto no modo *online* quanto no modo *offline*
- Limita funções de rastreio de utilizadores

Interoperabilidade

- Representação de dados em formato aberto
  - Entre infraestrutura e dispositivos móveis
    - JSON - *JavaScript Objet Notation*
    - JWS - *JSON Web Signature*
  - Entre dispositivos móveis
    - CBOR - *Concise Binary Object Representation*
    - COSE - *CBOR Object Signing and Encryption*
- Os leitores podem não ter relação com a entidade emissora
  - Devem suportar o formato de dados e o protocolo das transações

Conectividade

- Modos de operação
  - *Offline*
    - Transmissão direta dos atributos de identificação entre portador e leitor
    - Requer certificados de raíz instalados no leitor
    - Os dados podem não estar atualizados
  - *Online*
    - Requer conectividade do leitor com a infraestrutura
    - Garante que os dados da mID são atuais
    - A depender do número e tipo de serviços suportados, pode gerar carga significativa na infraestrutura