Universidade do Minho
Departamento de Informática

Tecnologia de Segurança

João Marco Silva
joaomarco@di.uminho.pt

Sistema referência

mID

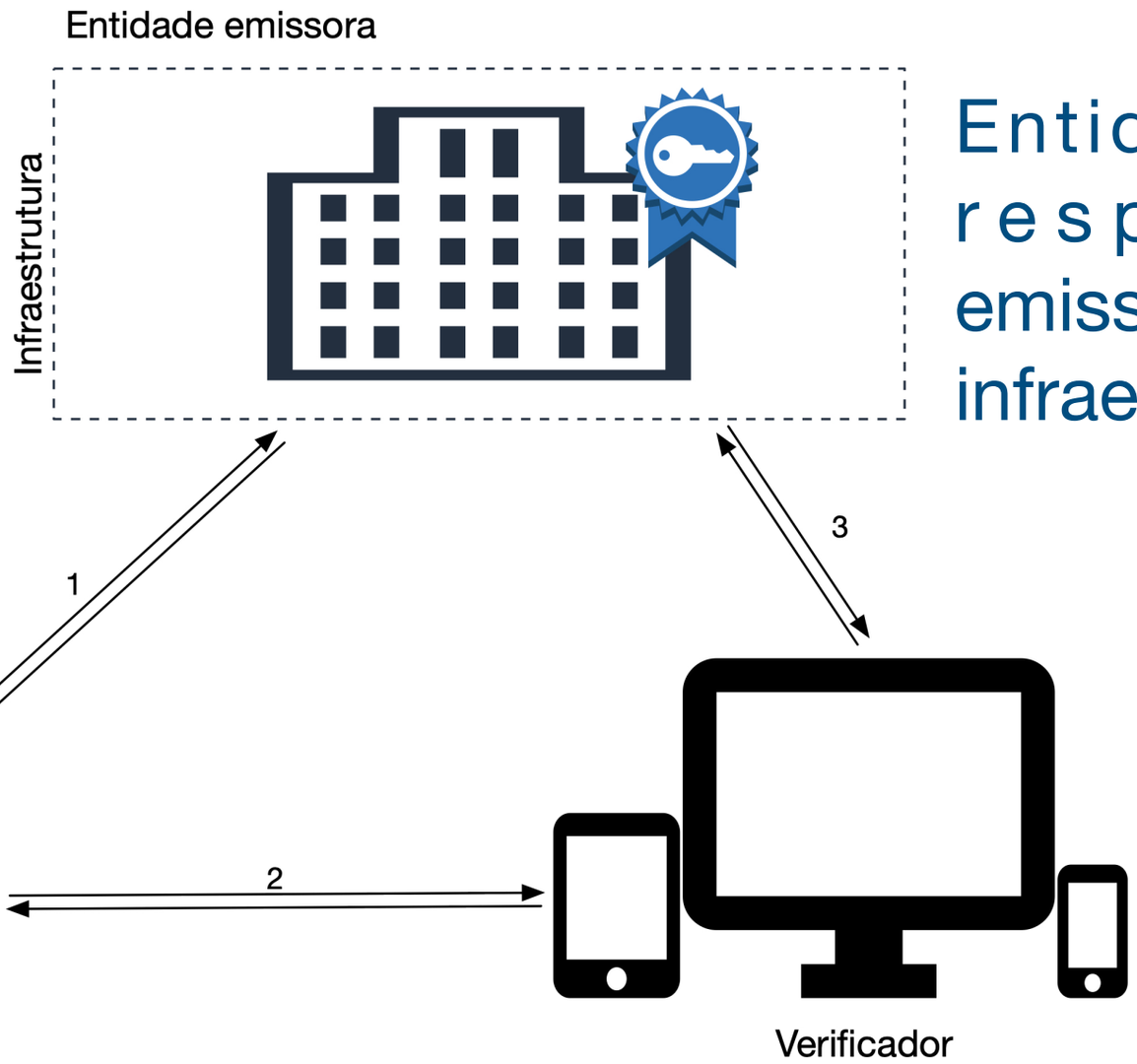
Sistema confiável de identificação pessoal digital e móvel. ISO/IEC 18013-5:2021

- 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

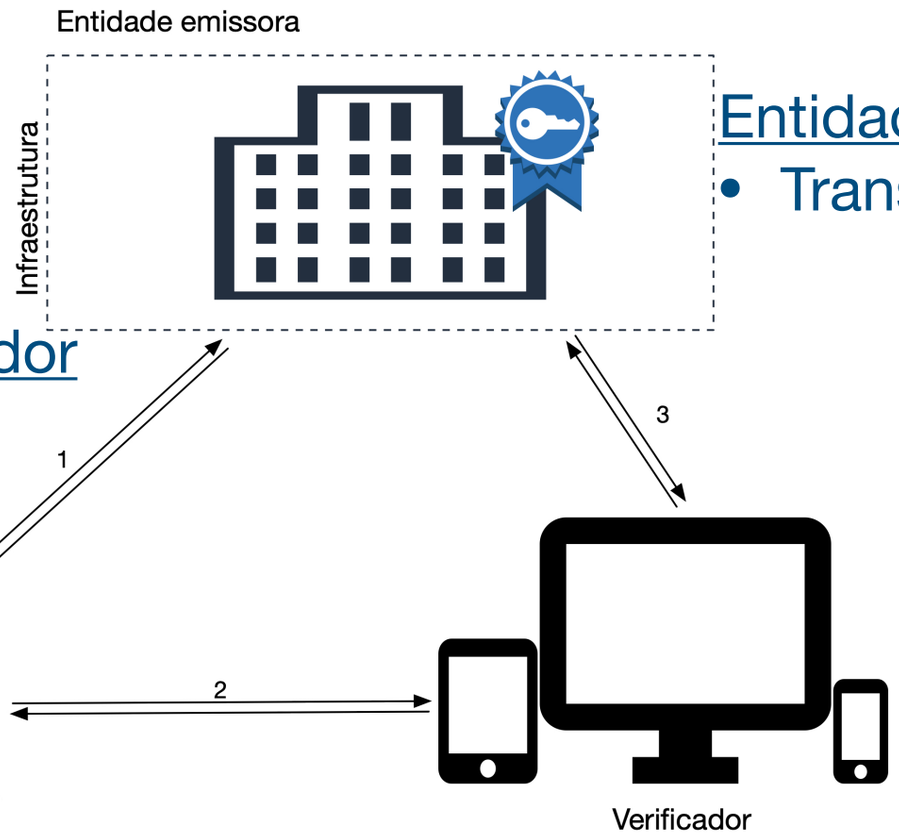


Entidade autoritativa responsável pela emissão da mID e pela infraestrutura de suporte

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

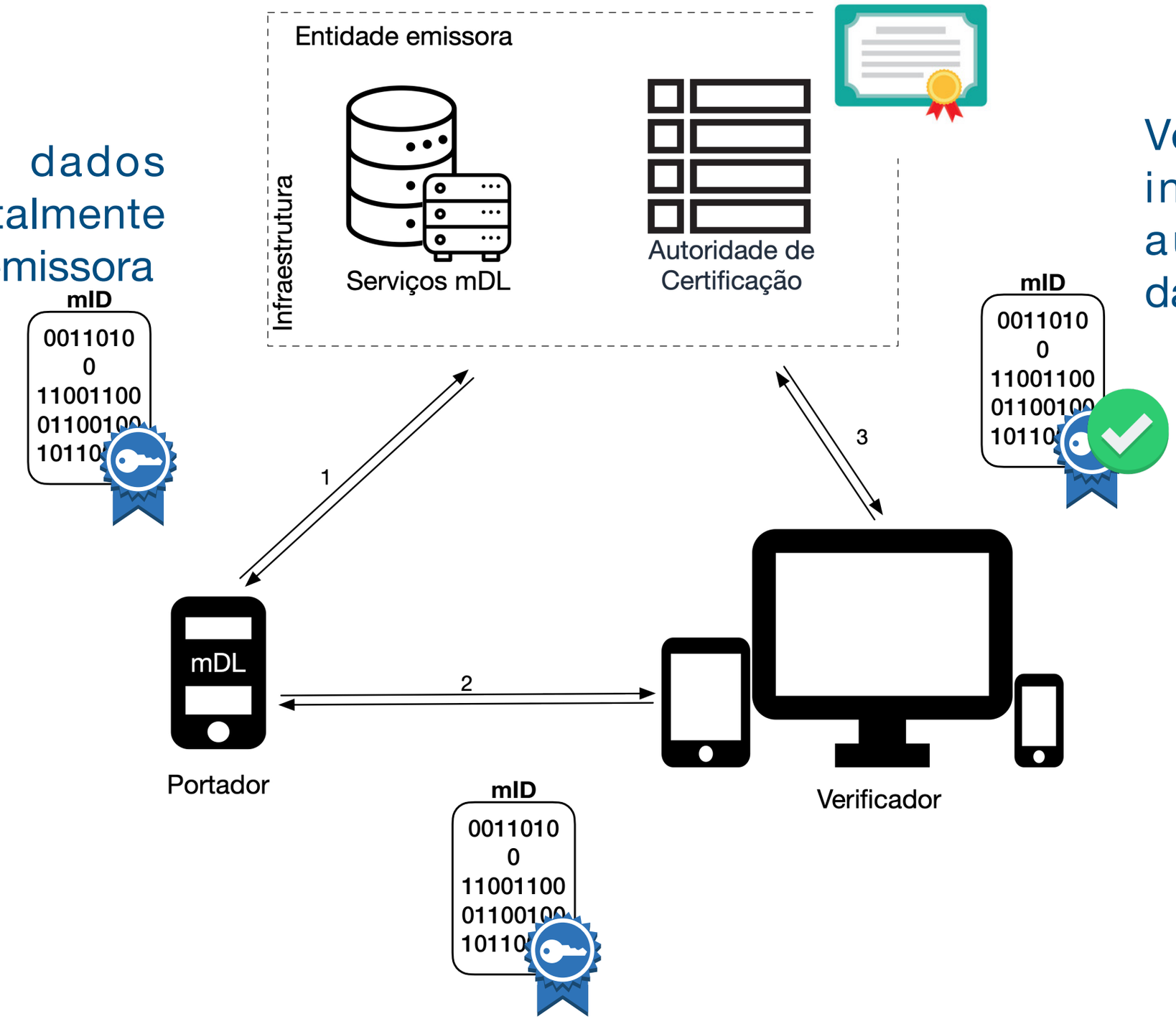
- Transmissão online de atributos

Portador <-> Verificador

- Transmissão de atributos
  - Modo *off-line* (dados)
  - Modo *on-line* (*token*)

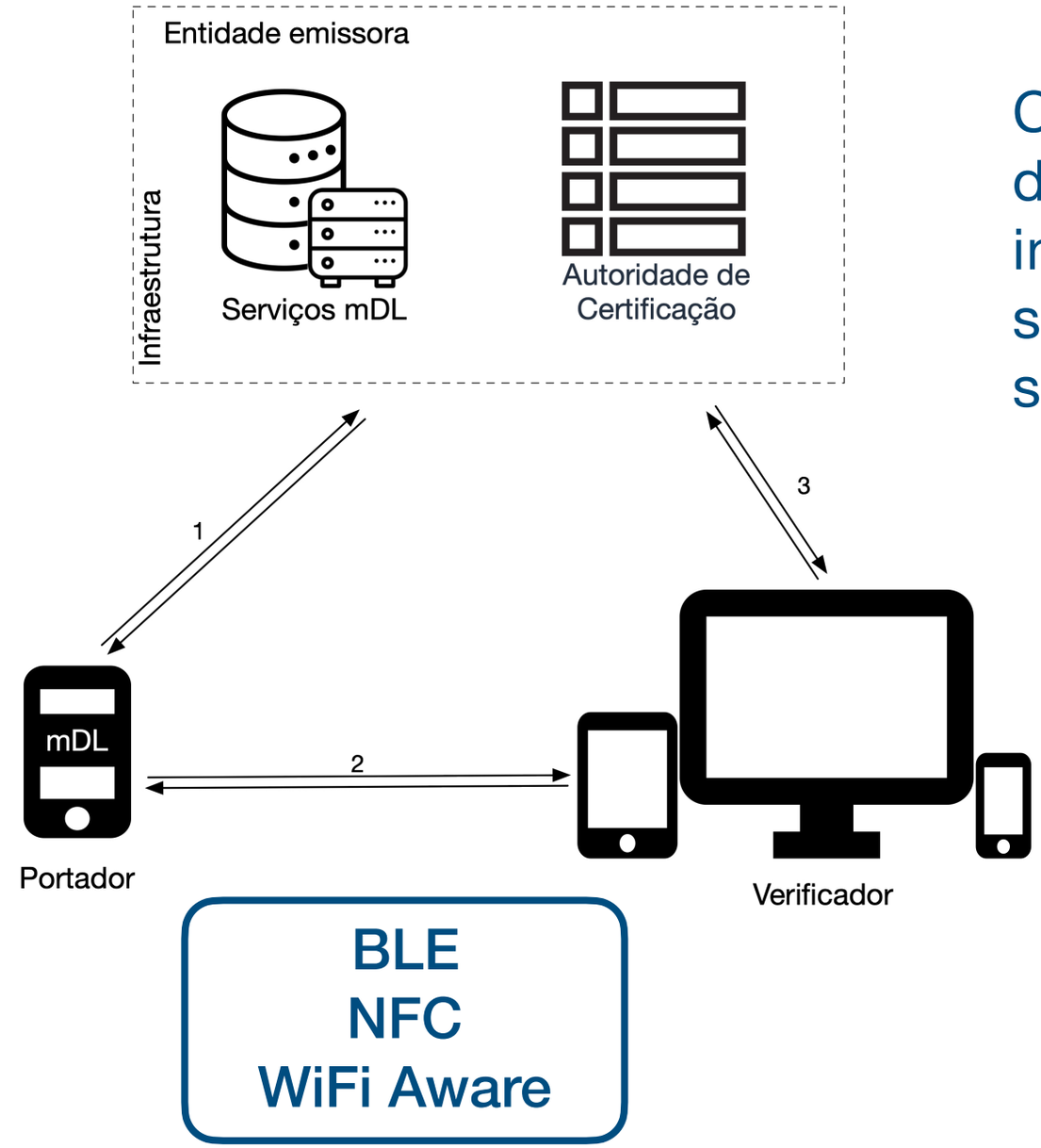
Esquema de confiança

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 usuários

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

Universidade do Minho
Departamento de Informática

Tecnologia de Segurança

João Marco Silva
joaomarco@di.uminho.pt