Universidade do Minho
Escola de Engenharia
Departamento de Informática

Filipa Correia Parente

Mobile ID como um serviço - Generalização da arquitetura do *standard* ISO/IEC DIS 18013-5

June 2022

Universidade do Minho
Escola de Engenharia
Departamento de Informática

Filipa Correia Parente

Mobile ID como um serviço - Generalização da arquitetura do *standard* ISO/IEC DIS 18013-5

Master dissertation
Integrated Master's in Informatics Engineering

Dissertation supervised by
Vítor Francisco Mendes de Freitas Gomes da Fonte
João Marco Cardoso da Silva

June 2022

AGRADECIMENTOS

Gostaria de agradecer às seguintes pessoas, que me ajudaram ao longo deste trabalho.

Em primeiro lugar, agradecer aos meus orientadores, Professor Doutor Vítor Francisco Mendes de Freitas Gomes da Fonte e ao Professor Doutor João Marco Cardoso da Silva, pelos conhecimentos transmitidos, pela paciência e horas despendidas que possibilitaram a realização deste trabalho da melhor forma.

Aos meus pais e ao meu irmão, especialmente à minha mãe por insistir em me manter saudável, durante as várias fases deste trabalho.

Aos meus amigos, pelas palavras de incentivo e pelos bons momentos passados ao longo destes anos.

Por fim, a três amigos que me ajudaram muito não só com palavras, mas com ações. Leonardo e Constança, não me vou esquecer das vezes que vinha a Braga e fazíamos questão de estarmos pessoalmente sempre que fosse possível, seja para conversar sobre a vida, ou sobre a tese. Catarina, já éramos amigas, mas a tese foi um ponto que fortaleceu a nossa amizade. Obrigada pelas sessões de trabalho juntas, e pela paciência que tens para me ouvir. Para além de minha prima és uma excelente amiga.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ouresultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO

O processo de identificação geralmente é usado para facilitar transações comerciais e governamentais. Apesar da existência de formas de identificação, maioritariamente presenciais, estas são pouco úteis para realização de negócios online.

De forma a encarar este problema, vários governos de diferentes países estão a criar sistemas nacionais de identificação eletrónica (eID), isto é, uma coleção de tecnologias e políticas que permitem aos cidadãos provarem eletronicamente a sua identidade, ou um atributo da sua identidade para um sistema de informação. Com o aparecimento da eID, um dos principais problemas que surgiu foi a insuficiente interoperabilidade entre os sistemas de identificação dos diferentes países adotantes, especialmente devido à falta de uma base jurídica comum.

Ao longo dos últimos anos surgiram soluções que, direta ou indiretamente, solucionam o problema de interoperabilidade, como é o caso do eIDAS. No entanto, o eIDAS é um regulamento seguido apenas pela União Europeia, existindo também a necessidade de readaptar o sistema de identificação eletrónica dos diferentes estados membros para criar uma ligação entre os diferentes sistemas.

Como alternativa às soluções já existentes, o comité ISO/IEC JTC 1 estabeleceu uma norma, aplicada especificamente para a Carta (ou licença) de Condução, mas que pode ser adaptada para outros documentos de identificação. Esta norma tem sido bem recebida pela maioria dos países e promete ser uma alternativa bastante viável para a implementação de um sistema de identificação eletrónica.

Assim, o principal foco desta dissertação é a definição de uma arquitetura aplicacional genérica, baseada na norma técnica ISO/IEC DIS 18013-5. Com base na arquitetura definida, como prova de conceito pretende-se criar de um sistema de identificação eletrónica configurável, que permita ao utilizador final implementar o seu sistema de identificação eletrónica, conforme as suas necessidades.

PALAVRAS-CHAVE identificação eletrónica, eIDAS, ISO/IEC DIS 18013-5, sistema de identificação eletrónica configurável, aplicação

ABSTRACT

Identification is commonly used to help facilitate commercial and government transactions. While there are available traditional forms of face-to-face transactions, these forms of identification are less useful for conducting online business.

To face this challenge, many governments are creating national electronic identification (eID) systems, a collection of technologies and policies that enable individuals to electronically prove their identity or an attribute about their identity to an information system. With the emergence of the eID, one of the main problems that came up was the insufficient cross-border interoperability between eID systems from different states/countries, especially due to a lack of common legal basis.

During the last few years, some solutions had been presented that solves these issues. The eIDAS regulation is an example. However, this is a standard adopted by the European Union and there is also a necessity to re-adapt the eID system from the different member states in order to create a link between the different systems.

As an alternative to these solutions, the ISO/IEC JTC 1 committee created a standard, specifically applied to the driving license, but it can also be adapted to other identity documents. It has been welcomed by the majority of countries, and it promises to revolutionize the electronic identity sector.

So, the main goal of this dissertation is to define an application architecture, based on the ISO/IEC DIS 18013-5 standard. As a Proof of Concept (PoC), the architecture will be implemented to create a configurable electronic identification system, allowing the end-user to implement their own electronic identification system and adapt them, according to their requirements.

KEYWORDS electronic identification, eIDAS, ISO/IEC DIS 18013-5, configurable electronic identification system, application

CONTEÚDO

LISTA DE FIGURAS

SIGLAS

AC Autoridade Certificadora. 38
ADSE Instituto Público de Gestão Participada. 11
AE Autoridade Emissora. vi, 20, 21, 23, 24, 25, 26, 27, 28, 29, 30, 32, 34, 35, 36, 37, 38, 39, 40, 41, 42, 45, 46, 47, 48, 49, 50, 55, 56, 57, 58, 61, 62, 63, 64, 66, 67, 68, 70
AMA Agência para a Modernização Administrativa. 8
API Application Programming Interface. 11, 18, 42, 56

BD Base de Dados. vi, 17, 23, 34, 36, 37, 42, 43, 44, 45, 49, 65, 66, 70
BLE Bluetooth Low Energy. 27, 28, 61, 73, 74

CA Autoridade Certificadora. 14
CC Cartão do Cidadão Português. vi, 8, 9
CMD Chave Móvel Digital. vi, 10, 11
COSE CBOR Object Signing and Encryption. 29
CSR Certificate Signing Request. 46, 47

ECDH Elliptic Curve Diffie-Hellman. 27
eID Identificação Eletrónica. 3, 4
eIDAS Electronic Identification, Authentication and Trust Services. 4, 12, 13, 14, 15
EU União Europeia. 12

FA Fornecedor de Autenticação/Authentication Provider. 10, 11, 34, 35
FATF Financial Action Task Force. 3

iAP Interoperabilidade na Administração Pública. 9
ID Identificação, Identidade. 3
ID4D Identification for Development. 3

JWT JSON Web Token. 58, 66

MITM Man In The Middle. 29
MSO Mobile Security Object. 25, 26, 29, 38, 48, 49, 50, 57, 58
MVC Model-View-Controller. 56

NFC Near Field Communication. 27, 28, 61

OCSP Online Certificate Status Protocol. 9, 58, 62

OIDC OpenID Connect. 28

PKI Infraestrutura de Chave Pública. 9, 56, 58, 66

RC Registo Civil. 3, 17, 19

SGBD Sistema de Gestão de Base de Dados. 55, 56, 70
SO Sistema Operativo. 22, 59, 63

TLS Transport Layer Security. 30
TSP Trust Service Provider. vi, 13, 14, 15

URL Uniform Resource Locator. 29, 63, 66

1

INTRODUÇÃO

O termo identidade pode ser definido de várias formas, dependendo da área de estudo. Por exemplo, em álgebra, o termo identidade é utilizado para definir uma equação que é verdadeira para qualquer valor atribuído a uma variável. Já no ramo financeiro e governamental, a *Financial Action Task Force (FATF)* define o termo como a especificação de um indivíduo, baseada nas suas características, chamadas identificadores ou atributos. Estes atributos são reconhecidos pelo estado/governo. Este trabalho terá como base o termo identidade no contexto governamental.

Com o aumento do número de pessoas que utilizam a Internet para aceder a serviços que anteriormente necessitavam de interação física, grande parte delas não consegue completar transações online que necessitam de um processo de identificação. Um dos principais fatores é a falta de uma forma segura, interoperável, fácil de usar e confiável para realizar o processo de identificação eletrónica. Para contornar isso, vários governos estão num esforço de implementação de um mecanismo de identificação que seja amplamente aceite. Nesse sentido, muitos países estão a criar ou já criaram sistemas de Identificação Eletrónica (eID).

Um sistema de identificação eletrónica pode ser definido como um conjunto de tecnologias e políticas que permite a qualquer indivíduo, que possua um documento de identificação, provar a sua identidade, ou um atributo da sua identidade para um sistema de informação (Castro, 2011).

Estes sistemas têm sido desenvolvidos por diversos países, incluindo Portugal, e trouxe bastantes benefícios, não só para a indústria do comércio online, mas também para a gestão governamental (Castro, 2011).

Apesar disso, existem diversos desafios tecnológicos e económicos que impedem as atuais soluções de serem usadas globalmente.

Segundo o conjunto de dados (ou *dataset*) global publicado pelo Identification for Development (ID4D) em 2018, estima-se que, pelo menos 1 bilhão de pessoas em todo o mundo não possuem um documento oficial de identificação (ID4D, 2018). A sua vasta maioria vive na África Subsariana e no sul da Ásia. Os custos diretos e indiretos para obter um documento nacional de identidade ID, bem como a falta de sistemas de Registo Civil (RC) eficientes no registo de nascimentos, mortes, entre outros eventos, são algumas razões que explicam estes números. A falta de um sistema de identificação seguro e confiável também é um problema, pois diminui o potencial valor económico e jurídico (Blogs, 2018).

Implementar sistemas de identificação digital ID apresenta riscos e desafios que necessitam de um planeamento ponderado do desenho do sistema. A existência de recursos técnicos, políticos e financeiros também são essenciais para garantir a implementação de um sistema de identificação seguro e confiável. Isto é particularmente desafiante em países com níveis baixos de literacia, infraestruturas limitadas e com baixo poder

financeiro. Nesse sentido, organizações não-governamentais (ONG) como a ID4Africa[1] tem sido aliados na promoção e acompanhamento no desenvolvimento de sistemas de identificação nos países africanos. Alguns países Europeus, do Médio Oriente e da Ásia tem investido no desenvolvimento de sistemas de identificação, uns com mais sucesso que outros. Alguns países como Portugal e Estónia já implementaram um sistema de identificação eletrónica com sucesso. Contudo, as soluções implementadas não eram interoperáveis o suficiente para serem usadas fora do país (ID4Africa, 2014).

Depois de alguns esforços para resolver o problema de interoperabilidade, em 2014, a Comissão Europeia criou o Regulamento EU n.º 910/2014, mais conhecido como o regulamento eIDAS. Este regulamento pretende estabelecer uma base comum para uma interação eletrónica segura, entre os diferentes estados membros da União Europeia. O eIDAS surgiu como uma solução que assegura "o reconhecimento transfronteiriço da identidade eletrónica"(Comission, 2022). No entanto, esta regulação apenas é adotada pela União Europeia e também existe a necessidade de readaptar os sistemas de eID dos diferentes estados membros de forma a garantir o reconhecimento mútuo entre os diferentes sistemas. Assim, pode-se concluir que, aparte da existência do passaporte como um documento de identificação válido para os diferentes sistemas de identificação, e também do eIDAS, ainda não existe uma norma técnica reconhecida internacionalmente que garanta a interoperabilidade entre diferentes soluções de identidade eletrónica (Thales, 2017).

Para além disso, existe outro desafio inerente à utilização de uma regulação deste tipo. Ela não especifica a arquitetura do sistema, sendo apenas especificado o modo como o reconhecimento mútuo da informação proveniente de sistemas de eID diferentes (ver Secção 2.2). Neste caso, cada estado membro é responsável pelo design da arquitetura do sistema e também pela sua implementação. Isto, por um lado, acaba por ser uma abordagem interessante, principalmente pela sua abertura a diferentes formas de implementação de sistemas de identificação eletrónica. Por outro lado, como referido anteriormente, o planeamento e implementação de um sistema de identificação envolve custos que podem ser reduzidos com a aplicação de uma arquitetura comum.

Nos últimos anos, surgiram algumas iniciativas que, apesar de terem diferentes objetivos, as soluções apresentadas respondem a alguns dos desafios apresentados nos parágrafos anteriores. Um exemplo é o openCRVS, uma iniciativa independente, pensada especificamente para garantir a implementação de um sistema eletrónico de Registo Civil de uma forma mais fácil, rápida e mais barata (openCRVS, 2018). As iniciativas encontradas ao longo deste trabalho são discutidas no Capítulo 2.

1.1 MOTIVAÇÃO E OBJETIVOS

O comité ISO/IEC JTC 1 apresentou uma norma técnica, relativa à Carta de Condução Móvel, que especifica os requisitos técnicos necessários para implementar a licença de condução móvel. Um dos principais aspetos descritos pelo documento é a sua extensibilidade para outros documentos de identificação móvel. Os requisitos técnicos descritos no documento apenas definem os aspetos relacionados com o processo de identificação de

1 Mais informações acerca da organização, consultar https://id4africa.com/about/

um indivíduo perante uma autoridade que pretenda verificar a sua identidade. Nesse sentido, existem aspetos que se encontram em aberto[2], nomeadamente:

- A existência de um desenho específico para a implementação de cada uma das entidades pertencentes a um sistema de identificação, complacente com a norma técnica ISO/IEC DIS 18013-5;
- A definição de algumas fases importantes no ciclo de vida de um documento de identificação móvel.

Tendo em conta estes aspetos, e no contexto desta dissertação, existem os seguintes objetivos:

1. Definição da arquitetura, necessária para a implementação de um sistema de identificação eletrónica que cumpra não só a arquitetura já definida norma técnica ISO/IEC DIS 18013-5, mas também os seus requisitos técnicos. Este esforço de definição implica a modulação de todas as interfaces envolvidas. O processo de definição da arquitetura é essencial para atingir o segundo objetivo;
2. Implementação de um sistema de identificação eletrónica configurável, com base no trabalho de definição da arquitetura abordado no objetivo anterior. O sistema criado permitirá ao utilizador final a implementação de uma solução de identificação eletrónica, de acordo com as suas necessidades, e que respeita a norma técnica ISO/IEC DIS 18013-5.

1.2 ESTRUTURA DO DOCUMENTO

O documento encontra-se organizado nas seguintes secções:

- O Capítulo 2 apresenta uma introdução teórica e histórica dos sistemas de identificação, desde a sua criação, até às soluções utilizadas atualmente. Ainda no mesmo capítulo é explorado o caso de estudo do sistema eletrónico de identificação português, de forma a entender melhor, não só a arquitetura utilizada, mas também o mecanismo de identificação utilizado e os desafios existentes relacionados com a implementação de sistemas de identificação a nível global. Por fim, são analisadas as diferentes soluções que surgiram para mitigar alguns dos problemas referidos ao longo do capítulo;
- No Capítulo 3 encontra-se descrito a norma técnica ISO-IEC DIS 18013-5, nomeadamente os requisitos técnicos definidos pelo documento para a implementação de um sistema de identificação móvel. Este capítulo é importante para atingir os objetivos deste trabalho, pois será a base para a definição da arquitetura do sistema;
- Por sua vez, no Capítulo 4, numa fase inicial, são abordados conceitos que não foram abordados nos capítulos anteriores e que se encontram relacionados com o funcionamento de um sistema de identificação móvel. Assim, com base nos conceitos abordados ao longo do documento é apresentada a arquitetura aplicacional que servirá de base para a implementação da Prova de Conceito de um sistema de identificação eletrónica móvel;

2 A discussão dos aspetos não definidos pela norma técnica ISO/IEC DIS 18013-5 encontra-se na Secção 3.4

- O Capítulo 5 descreve a fase de implementação da Prova de Conceito, nomeadamente as ferramentas utilizadas e a definição dos modelos UML de implementação da arquitetura aplicacional, definida no Capítulo 4. Como forma de demonstração da Prova de Conceito, neste capítulo é também apresentado um exemplo de um mecanismo de configuração de um sistema de identificação móvel a ser gerado, bem como uma descrição demonstrativa do processo de identificação com o sistema já implementado;
- Por último, o Capítulo 6, que engloba as considerações finais, o levantamento dos objetivos alcançados com o trabalho, e a discussão de aspetos que podem ser melhorados no futuro.

Note que o presente trabalho dispõe de uma secção final de Anexos com conteúdo de suporte aos capítulos.

2

TRABALHOS RELACIONADOS

Historicamente, os sistemas de identificação surgiram por necessidade, especialmente em grandes comunidades, onde a tradicional identificação face-a-face se tornou impossível. Assim, como alternativa, uma entidade terceira confiável, geralmente governos ou autoridades religiosas, forneciam à sua população uma prova de identidade (Castro, 2011). Naquela época, algumas nações já tinham sistemas de identidade robustos, baseados em documentação oficial física, como por exemplo certidões de nascimento, certidões de casamento, etc. Note que, atualmente, muitos países ainda possuem um sistema de identidade deste tipo (Castro, 2011).

Contudo, estes sistemas são suscetíveis a fraudes, visto serem sistemas baseados em documentos em papel. Na altura em que esses sistemas de identificação surgiram, os documentos emitidos eram suficientes para os indivíduos provarem quem eram para o estado e para instituições privadas (Castro, 2011).

No sentido de mitigar os problemas de segurança encontrados, foram definidos vários tipos de controlo para garantir a integridade dos documentos de identificação. O uso de propriedades físicas distintas como marcas de água ou texturas de papel diferentes e/ou através a aplicação de medidas condicionantes. Essas medidas condicionantes podem incluir a exigência a menores de idade da presença de um dos pais, ou um tutor responsável, para atestar a sua identidade (Castro, 2011).

Com a descoberta de impressões digitais gravadas em descobertas arqueológicas (ver Figura 1), o conceito de identificação biométrica surgiu como uma potencial solução aos desafios abordados no parágrafo anterior (bio, 2013). Este processo de identificação foi utilizado no início do século 19, e era bastante útil. No entanto, esta abordagem tinha limitações, uma vez que este processo era complexo, demorado e custoso (bio, 2013), pelo que deixou de ser utilizada.

O desenvolvimento da identificação biométrica digital levou a que muitos países começassem a investir na migração dos documentos de identificação em papel para *smartcards*. Estes *smartcards* contém certas propriedades criptográficas que diminuem a probabilidade de haver problemas de falsificação de documentos. Alguns governos estão a fazer a transição dos seus documentos para um formato *machine-readable*, com o objetivo de melhorar a eficiência administrativa (Castro, 2011). Um exemplo de um documento *machine-readable* é o Cartão do Cidadão Português (ver Figura 2).

Para além do governo, o setor privado também pode ser um portador de atributos de identidade, isto é, qualquer empresa que possua informação sobre os seus funcionários, como a sua foto e o nome, pode ser um portador de atributos (Castro, 2011). Esta informação é essencial não só para os novos funcionários entrarem na empresa, mas também para a gestão dos recursos humanos da mesma.

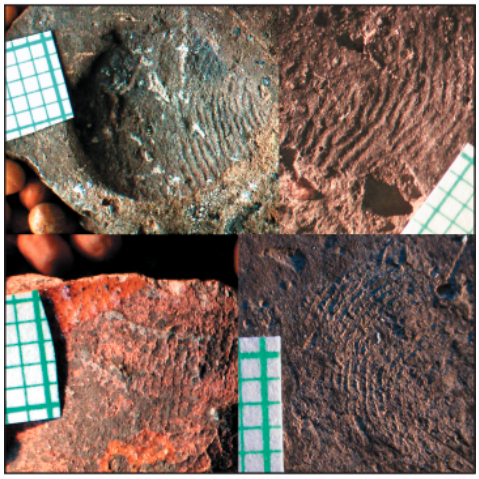

Figura 1: Exemplos de impressões digitais encontrados em vasos cerâmicos de diferentes épocas (descoberto por Martin Hložek) (fin, 2014)

Figura 2: Espécime do Cartão de Cidadão português (AMA, 2008)

2.1 CASO DE ESTUDO DO CARTÃO DO CIDADÃO PORTUGUÊS

Portugal apresentou o seu primeiro sistema de identificação eletrónica em 2008, com o surgimento do Cartão do Cidadão Português (CC) (Thales, 2019). É um documento de identidade fornecido pelo governo português aos seus cidadãos (AMA, 2008). Este cartão foi introduzido com o objetivo de reduzir o número de diferentes documentos necessários para as interações com as várias instituições do Estado (Thales, 2019).

Junto com o Cartão do Cidadão, apareceu um novo serviço chamado Autenticacao.gov[1]. É um serviço de autenticação para o acesso a serviços online[2]. Surgiu da necessidade de um processo de identificação seguro, que permitisse identificar um individuo em diferentes serviços online. É gerido pela Agência para a Modernização Administrativa (AMA), uma instituição pública indiretamente integrada com a administração do Estado português.

A Figura 3 demonstra o processo de autenticação de um utilizador numa entidade pertencente ao serviço, utilizando o Cartão do Cidadão Português (CC):

1 O documento encontra-se disponível para leitura. Para aceder à versão impressa, selecionar este **link**.
2 As entidades aderentes encontram-se disponíveis em https://www.autenticacao.gov.pt/web/guest/entidades-aderentes

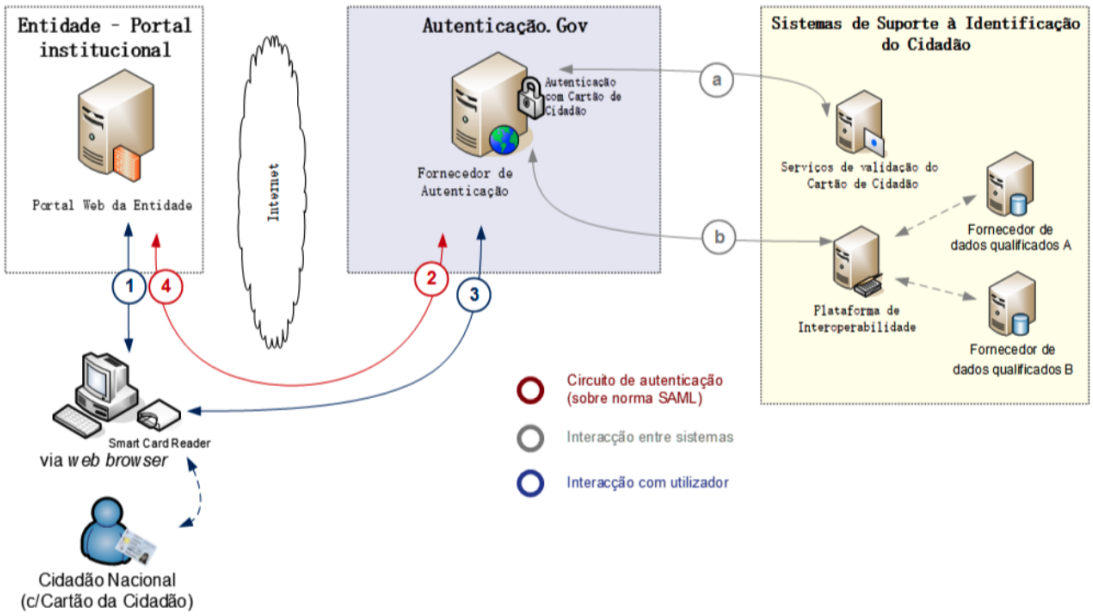

Figura 3: Diagrama exemplo do processo de autenticação de um utilizador através do Autenticacao.gov com o Cartão do Cidadão Português(AMA, 2020)

O diagrama da Figura 3 apresenta as seguintes iterações:

1. O utilizador pretende aceder à área privada de um determinado serviço *web* que necessita de um processo de validação da sua identidade;

2. O utilizador é redirecionado para o serviço Autenticacao.gov com um pedido de autenticação assinado digitalmente;

3. O Autenticacao.gov valida o pedido e pede ao utilizador para se autenticar utilizando o Cartão do Cidadão Português. Este processo de autenticação envolve a inserção de um PIN de autenticação, fornecido ao cidadão no momento em que recebe um novo cartão. Durante este processo, ocorrem as seguintes operações internas:

   a) Validação das credenciais inseridas, através da validação do certificado digital proveniente da Infraestrutura de Chave Pública (PKI). A validação do certificado é feita via Online Certificate Status Protocol (OCSP);

   b) A Plataforma de Interoperabilidade (iAP) obtém os atributos pedidos de diferentes fornecedores de atributos qualificados (ver Definição 2.1), e envia os dados recebidos para o Autenticacao.gov. Este passo ocorre em casos onde alguns atributos não se encontram disponíveis no chip interno do cartão do cidadão ou no certificado público proveniente da PKI.

4. A identificação do utilizador e os atributos pedidos são autenticados e assinados digitalmente pelo Autenticacao.gov, sendo o utilizador posteriormente redirecionado para o serviço *web* que efetuou o pedido.

Esse serviço, assim que recebe a informação, verifica se esta se encontra devidamente autenticada e assinada. Se estiver, o utilizador é redirecionado para a sua área privada.

Fornecedor de atributos: Define-se como um fornecedor de atributos, uma entidade que possua e disponibilize, de acordo com a identificação e autorização (explícita ou implícita) do utilizador, dados autênticos sobre ele (AMA, 2020).

O processo de autenticação também pode ser feito via Chave Móvel Digital (CMD). O diagrama seguinte mostra o processo de autenticação via CMD, bem como a busca dos atributos (Figura 4).

Chave Móvel Digital (CMD): É uma forma alternativa de autenticação, e de utilização assinatura digital, fornecida pelo Estado português. Para a utilização do CMD, o serviço Autenticacao.Gov associa um número de telemóvel ao número de identificação civil para um cidadão português, e o número de passaporte ou título/cartão de residência para um cidadão estrangeiro.

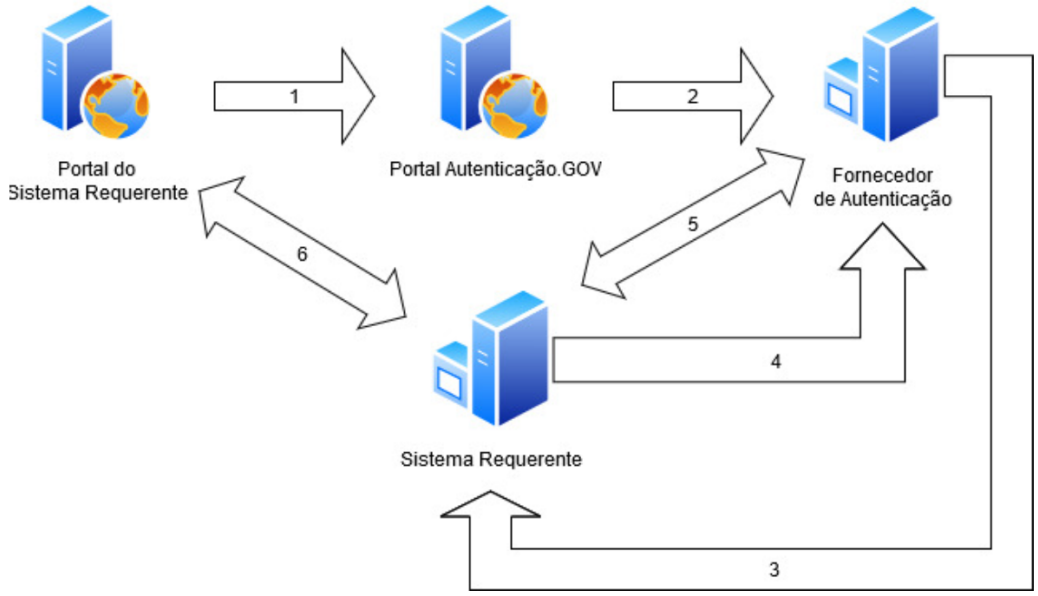

Figura 4: Diagrama exemplo do processo de autenticação de um utilizador através Autenticacao.gov com a CMD (AMA, 2020)

1. O serviço da entidade requerente faz um *GET request* ao Fornecedor de Autenticação (FA)[3], com os parâmetros necessários para obter o *token* de autenticação;

2. O serviço Autenticacao.Gov pede o consentimento do utilizador para o acesso aos dados requeridos pela entidade requerente. Caso consinta, faz a sua autenticação via Chave Móvel Digital CMD, inserindo o número de telemóvel associado e o PIN.

3 Neste contexto, o fornecedor de autenticação é o serviço do Autenticacao.Gov (ver Figura 3)

3. No caso de o processo de autenticação via CMD ser bem sucedido, um token e outros atributos necessários são enviados ao serviço do Sistema Requerente. Com os atributos recebidos, o Sistema Requerente pode usar o token de recebimento para solicitar os atributos necessários.

4. O Sistema Requerente envia um objeto JSON contendo o token de autenticação, nomes de atributos e outras informações necessárias;

5. O Sistema Requerente faz um pedido GET, para obter os atributos pedidos do FA API.

A partir da análise dos diagramas das Figuras 3 e 4 é possível observar que o sistema de identificação eletrónico português utiliza a assinatura digital para o processo de identificação. Uma assinatura digital possui certificados digitais associados que asseguram a identidade de quem assina um documento digital.

As assinaturas digitais geradas pela Autenticacao.Gov seguem um regulamento europeu, o eIDAS (ver Secção 2.2). Através deste regulamento, um cidadão português consegue autenticar-se num portal oficial de outro estado membro, utilizando o seu certificado digital para se identificar.

Um dos exemplos da aplicação do sistema de identificação eletrónica português, nomeadamente da plataforma Autenticacao.gov é o id.gov.pt.

2.1.1 *id.gov.pt*

O id.gov.pt é uma aplicação móvel desenhada pela AMA. Este aplicativo permite que o utilizador final guarde, verifique e compartilhe dados de seus documentos de identificação usando o *smartphone*. Outra funcionalidade é a possibilidade de uma entidade externa verificar qualquer documento disponível na aplicação. Essas entidades podem ser agentes da polícia, funcionários do registo civil e também cidadãos.

Para já a app possui apenas três documentos disponíveis, o cartão do cidadão, a carteira de habilitação e o cartão da Instituto Público de Gestão Participada (ADSE). Esses documentos são válidos apenas dentro do país.

O processo de associação para obter os documentos digitais envolve o uso da Chave Móvel Digital no serviço do Autenticacao.Gov.

Uma vez que não existe nenhuma documentação oficial acerca da app, não foi possível analisar os aspetos técnicos da aplicação, em particular, os mecanismos de segurança utilizados para verificar e validar um documento.

2.1.2 *Desafios existentes com a implementação de um sistema de identificação eletrónico*

Como foi referido no Capítulo 1, existem desafios inerentes ao desenvolvimento de um sistema de identificação eletrónico, e que necessitam de ser ultrapassados. Implementar sistemas de identificação eletrónica apresenta desafios técnicos, políticos, organizacionais e financeiros (Castro, 2011).

É necessário encontrar soluções que sejam fáceis de implementar, e que garantam a segurança e confiabilidade de sistemas de identificação já implementados atualmente.

Com o crescimento das transações eletrónicas a nível internacional, também existe a necessidade da criação de sistemas de identificação que sejam interoperáveis entre si. Por outras palavras, é necessário a definição de uma solução que garanta o reconhecimento de um indivíduo em transações que envolvam o processo de identificação (por exemplo, o reconhecimento da identidade de um cidadão português pela autoridade de segurança espanhola, para entrar em Espanha).

Nesse sentido, as próximas secções (Secções 2.2, 2.3 e 2.4) descrevem as soluções que surgiram para a resolução de alguns dos desafios referidos nesta secção.

2.2 ELECTRONIC IDENTIFICATION, AUTHENTICATION AND TRUST SERVICES (EIDAS)

O eIDAS é um regulamento europeu utilizado para as transações eletrónicas no Mercado Interno Único. Este regulamento foi adotado pelos co-legisladores em 2014 e pelos restantes Estados Membros em 2016. É uma regulação que apresenta um conjunto de regras específicas que permitem interações eletrónicas seguras entre empresas, cidadãos e autoridades públicas (Jonathan Allin, 2017).

Antes do eIDAS, algumas iniciativas foram criadas para encorajar o reconhecimento mútuo de assinaturas eletrónicas em toda a EU. Contudo foram mal sucedidas, uma vez que a falta de um padrão comum levou os países a implementarem diferentes sistemas de assinatura eletrónica, a maioria deles com incompatibilidades entre si (Jonathan Allin, 2017).

Assim, uma das principais diferenças entre o regulamento eIDAS e as diretivas anteriormente propostas é a existência de uma orientação específica, necessária para garantir a interoperabilidade entre os diferentes serviços de confiança em toda a EU (Jonathan Allin, 2017).

Este regulamento coloca requisitos técnicos específicos para a sua correta implementação, através da utilização de formatos de assinatura reconhecidos e do reconhecimento de entidades pan-europeias. Afeta todos os provedores e serviços de confiança que protegem as transações na rede pública. Atividades relacionadas com transações de viagens, contratos jurídicos e de seguro, e serviços comerciais que exigem uma identidade da EU são algumas atividades abrangidas por este regulamento (Jonathan Allin, 2017).

2.2.1 *Especificações do eIDAS*

Antes de entrar nos requisitos, é importante explicar os níveis ou dimensões do domínio em que esses requisitos são especificados (eIDAS, 2014):

- A primeira dimensão é a definição de quais são os requisitos básicos a serem adotados em toda a EU;
- A segunda dimensão é representada pelo conjunto de *standards* disponíveis recomendados por especialistas do setor;
- A terceira dimensão é representada pelos atuais atos de execução da EU, que recomendam ou impõem a utilização de certas normas;

- A quarta e última dimensão é representada pelas regras nacionais, que variam de país para país. Em outras palavras, para atender à perspectiva de uma nação, alguns *standards* que não são obrigatórios podem precisar ser adaptados ou estendidos.

Existem duas entidades que são preponderantes nesta regulação, os Serviços de Identidade e os *Trust Services*.

2.2.2 *Serviços de Identidade*

Os Serviços de Identidade consistem em sistemas eletrónicos que tentam verificar a identidade de alguém eletronicamente. O eIDAS oferece três tipos diferentes de níveis de garantia, dependendo do tipo de transação: Baixo, Substancial e Alto.

Tendo em conta o contexto do tema deste trabalho, estes níveis de garantia podem ser representados por (eIDAS, 2014):

- **Baixo:** É representado por um processo de autenticação simples, usando, por exemplo, um e-mail e uma senha;
- **Substancial:** Envolve autenticação de dois fatores, com verificações extras num telefone previamente registado e verificações de identidade durante o registo;
- **Alto:** Utiliza mecanismos de autenticação sofisticados, com verificações abrangentes de identidade durante o registo. Um exemplo disso é a utilização da assinatura digital como mecanismo de autenticação no sistema de identificação do governo português (ver Secção 2.1).

Cada Estado Membro e respetivas organizações mantém as suas próprias Bases de Dados (BD). Esses serviços de identidade são responsáveis pelo reconhecimento transfronteiriço da identidade de um indivíduo.

2.2.2.1 *eIDAS Trust Services*

De acordo com o regulamento eIDAS, um Trust Service Provider (TSP) é definido como "uma pessoa física ou jurídica que fornece um ou mais serviços de confiança como um provedor de serviços de confiança qualificado ou não qualificado". Os TSPs são responsáveis por garantir a identificação eletrónica dos signatários e serviços por meio de fortes mecanismos de segurança (eIDAS, 2014). Um TSP que respeita o regulamento eIDAS deve abrangir o seguinte:

- Suportar a assinaturas eletrónicas;
- Suportar selos eletrónicos (ver Definição 2.2.2.1);
- Suportar autenticação web;
- Fornecer *e-delivery* registada entre as partes autenticadas.

ASSINATURA ELETRÓNICA: Uma assinatura eletrónica é uma assinatura que identifica um indivíduo, no formato eletrónico. Existem diversos formatos de assinaturas eletrónicas. Um exemplo de um tipo de assinatura eletrónica é o caso da assinatura digital. A assinatura digital é uma assinatura eletrónica que utiliza algoritmos complexos de assinatura, CA's e um TSP's, para autenticar tanto a entidade que assinou, como para garantir a integridade dos dados assinados.

SELO ELETRÓNICO: Um selo eletrónico é um novo conceito jurídico introduzido pelo eIDAS. Pode ser definida como uma assinatura eletrónica criada por um indivíduo ou pessoa, equivalente a uma assinatura manuscrita. Apesar de utilizar os mesmos mecanismos da assinatura eletrónica para assinar, o selo eletrónico é utilizado para autenticar a entidade que assinou o documento.

Do ponto de vista técnico, o selo eletrónico corresponde a uma assinatura eletrónica que associa os dados assinados, à entidade legal que assinou. Para provar a sua autenticidade, para além de efetuar a validação da assinatura, também é necessário o estabelecimento da relação entre a entidade que a assinou e a própria assinatura. O eIDAS também regula não só os elementos presentes na assinatura eletrónica, mas também os elementos presentes num selo eletrónico.

De forma a perceber melhor o papel destas duas entidades, o diagrama da Figura 5 mostra o processo de autenticação de um utilizador numa instituição bancária:

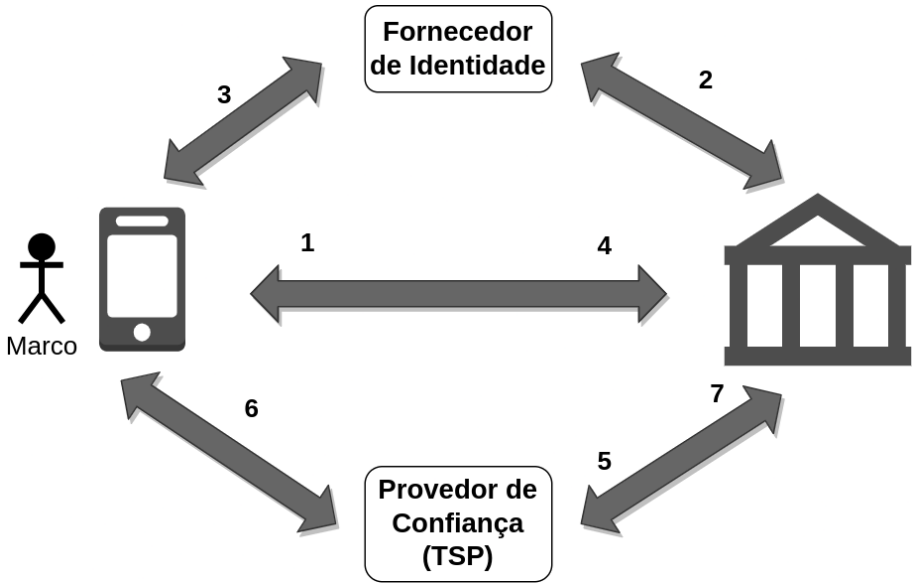

Figura 5: Diagrama exemplificativo da interação entre um Fornecedor de Identidade e um TSP (Jonathan Allin, 2017)

No contexto deste diagrama, um utilizador português (o Marco) pretende consultar o seu extrato bancário na sua conta bancária francesa. Este processo pode ser definido nos seguintes passos:

1. Primeiro, o utilizador efetua o seu processo de login;

2. Assim que a entidade bancária recebe o pedido desse utilizador, a mesma efetua um pedido de confirmação da sua identidade ao Fornecedor de Identidade português (neste caso recorre à plataforma Autenticacao.gov);

3. O utilizador recebe o pedido de verificação da sua identidade do seu Fornecedor de Identidade. Caso consinta, o Fornecedor de Identidade procede à verificação da identidade do utilizador e envia a confirmação para a entidade bancária. Neste momento o utilizador já entrou na sua conta pessoal do banco;

4. Para consultar o seu extrato bancário, o utilizador preenche um formulário, requerindo o acesso ao seu extrato bancário. Note que, neste caso um formulário corresponde a um pedido no formato JSON ou XML;

5. O banco recebe esse formulário, enviando-o para um Provedor de Confiança qualificado (ou *Qualified Trust Service Provider*);

6. O utilizador ativa a sua assinatura, através do seu eID e do PIN;

7. O TSP autentica as credenciais inseridas pelo utilizador. Posteriormente a assinatura resultante é enviada para a entidade bancária. Note que a plataforma Autenticacao.gov também é responsável pela autenticação.

Apesar de a regulação eIDAS já possuir um quadro regulamentar já estabelecido, alguns aspetos ainda não se encontram finalizados. Assim, algumas alterações à regulação são expectáveis, à medida que novas versões forem publicadas.

2.3 FAST HEALTHCARE INTEROPERABILITY RESOURCES (FHIR)

O FHIR é uma norma que define a forma como a informação relativa a instituições de saúde, isto é, dados relativos a pacientes, exames, etc. devem ser trocados entre os diferentes sistemas de saúde, independentemente da implementação adotada. A norma surgiu em 2012, como forma de resposta à necessidade do mercado de soluções de comunicação de dados de saúde mais fáceis e rápidos de implementar, e que permitissem transacionar um grande volume de dados de forma mais rápida e leve(of the National Coordinator for Health Information Technology, 2019).

2.3.1 *Arquitetura*

Um dos objetivos principais desta norma é garantir a interoperabilidade entre sistemas, através da utilização de modelos de dados bem estruturados, e de mecanismos de troca de informação simples e eficientes. Assim, de um ponto de vista arquitetural, a norma FHIR define duas componentes principais (FHIR, 2012):

1. **Recursos:** Conjunto de modelos de informação que definem os elementos de dados utilizados, as constantes, e as relações entre os objetos de negócio relevantes no contexto das instituições de saúde. Do ponto de vista técnico, os recursos encontram-se representados em objetos XML ou JSON[4].
    - Apesar de não existir um conceito universalmente definido, no contexto de instituições de saúde, considera-se como objetos de negócio todos os conceitos relacionados com o funcionamento de um sistema de saúde (ex. paciente, médico, procedimentos cirúrgicos, etc.).
2. **API's:** Interfaces que garantem a interoperabilidade entre duas aplicações distintas. A norma FHIR especifica um conjunto de interfaces *RESTfull* para a implementação da API, contudo a utilização desta especificação não é obrigatória[5].

O FHIR baseia-se em *web standards* bastante utilizados pela indústria fora da área da saúde. Incluem a utilização:

- Formato XML ou JSON para a representação dos Recursos;
- Protocolo de comunicação HTTP para a comunicação entre os diferentes sistemas;
- Abordagem REST para o envio e receção dos Recursos.

2.4 OPENCRVS

O openCRVS é uma solução *open source* de implementação de sistemas eletrónicos de registo civil. Esta solução pretende agilizar o desenvolvimento de um sistema eletrónico de registo civil de forma fácil e acessível, de modo a que qualquer país possa adotar um sistema eletrónico de Registo Civil, independentemente da sua capacidade financeira.

2.4.1 *Funcionalidades*

Existe um conjunto de funcionalidades relacionadas com o funcionamento de um registo civil que são suportadas pelo openCRVS. Note que estas funcionalidades estão divididas em componentes lógicas presentes na arquitetura funcional da solução(openCRVS, 2018).

1. Funcionalidades principais fornecidas pelo openCRVS:
    - **Registo e validação de eventos**. Atualmente, apenas se encontram suportados os eventos de nascimento e morte;
    - **Notificação de eventos**, provenientes de sistemas externos (ex: DHIS2[6]);

4 A lista de recursos atualmente existentes encontra-se disponível em https://www.hl7.org/fhir/resourcelist.html

5 O conjunto das interfaces RESTfull encontra-se definida em https://www.hl7.org/fhir/http.html

6 O DHIS2 é um sistema de gestão de dados associados a instituições de saúde. Este sistema, utilizado em mais de cem países, é gerido pela Organização Mundial da Saúde(OMS). Mais informações consultar https://dhis2.org/about/

- **Declaração de eventos** registados no sistema;
- **Emissão de certificados** correspondentes aos eventos registados e declarados no sistema;
- **Exportação de dados estatísticos** associados ao sistema;
- **Verificação de atributos** específicos **associados a eventos** registados no sistema (ex: verificação da idade, através do certificado de nascimento);
- **Correção de atributos** associados a eventos registados no sistema;

2. Funcionalidades de suporte:
   - **Autenticação** de um utilizador no sistema;
   - **Gestão do desempenho** do sistema. Essa gestão é feita através da monitorização dos indicadores de performance fornecidos por uma *dashboard* (designada por *Operational Dashboard*);
   - **Auditoria** de todas as interações efetuadas por um utilizador, bem como de todas as alterações efetuadas a um evento no sistema;
3. Funcionalidades de gestão administrativa do sistema:
   - **Gestão de utilizadores**;
   - **Gestão de dados**;
   - **Gestão da comunicação** com **provedores de serviços** utilizados pelo sistema (ex. fornecedores externos de dados), bem como com os **utilizadores do sistema**.

2.4.2 *Arquitetura*

A arquitetura do sistema varia conforme as necessidades de cada país que pretenda implementar o seu sistema de Registo Civil eletrónico, através desta solução. Assim, para a arquitetura, o openCRVS usa um conjunto de containers Docker orquestrados através da ferramenta de orquestração Docker Swarm. O sistema pode estar alocado numa *cloud* pública ou privada.

Para cada camada aplicacional o openCRVS atualmente utiliza as seguintes ferramentas(openCRVS, 2018):

- **Camada de Dados**:
  1. Como motor de pesquisa na Base de Dados (BD) do sistema é utilizado o *ElasticSearch*, devido à sua rapidez de pesquisa, mesmo com dados de pesquisa imprecisos;
  2. Para a gestão da BD é utilizado o InfluxData, pela sua rapidez de resposta a *queries* de leitura de grandes volumes de dados feitas à BD do sistema;
  3. Também existe a possibilidade de utilizar um servidor de BD compatível com a especificação FHIR (Hearth). Esta integração pode ser efetuada em países que já utilizem esta especificação nos seus sistemas de saúde e pretendam importar esses dados para o sistema.

- **Camada de Negócio**: As funcionalidadades definidas na Secção 2.4.1 encontram-se definidas nesta camada. Cada funcionalidade está definida em microsserviços que se contatam através de API's seguras. Cada microsserviço está escrito em TypeScript e utiliza a *framework* de desenvolvimento NodeJS.
- **Camada de Interoperabilidade**: Atualmente, o openCRVS apenas apresenta interoperabilidade com sistemas externos baseados na especificação FHIR. Para isso, utiliza um *middleware* designado openHIM. Para efetuar a tradução dos dados enviados/recebidos do openHIM, o openCRVS utiliza a linguagem GraphQL.
- **Camada de Apresentação**: O utilizador pode interagir com o sistema de duas formas:
  - Através de uma aplicação móvel, que permite o registo de eventos;
  - Através de um serviço online. Para o tratamento dos inputs/outputs, bem como a configuração linguística da interface com o utilizador, este serviço utiliza a biblioteca React.

  O sistema encontra-se protegido através da utilização de protocolos e mecanismos de segurança definidos por entidades certificadas.
  - Autenticação a dois fatores, nas aplicações móveis;
  - Utilização do protocolo OAuth durante o processo de autenticação e no acesso aos microsserviços fornecidos pelo sistema;
  - Gestão centralizada dos utilizadores, a sua função no sistema, e as suas permissões;

2.5 DISCUSSÃO DAS SOLUÇÕES ABORDADAS

Tendo em conta o inicio da Secção 2.2, o regulamento eIDAS surgiu a partir de sistemas de identificação já implementados, em Estados Membros europeus. No entanto, os sistemas de identificação existentes são caros e exigem infraestruturas que suportem um mecanismo online de identificação, o que implica uma boa ligação à Internet. Assim, este regulamento não é adequado para ser seguido na implementação de sistemas de identificação eletrónicos em zonas remotas com baixa conexão à Internet.

O FHIR, à semelhança do eIDAS, demonstra ser uma boa abordagem para a comunicação de dados entre sistemas com implementações diferentes, uma vez que estabelece um mecanismo de comunicação comum entre eles e também utiliza protocolos atualmente reconhecidos e bastante utilizados na implementação de sistemas eletrónicos. Contudo, o facto de utilizar normas de comunicação *web based*, implica a existência de uma boa infraestrutura de rede. Por isso, esta abordagem também não é viável em zonas remotas.

O openCRVS, ao contrário das outras soluções, apresenta uma abordagem distinta. Isto, uma vez que o seu principal objetivo não é garantir a interoperabilidade entre sistemas, mas sim permitir a implementação de um sistema eletrónico associado a um registo civil de forma rápida, e com menos custos financeiros associados à implementação.

As ferramentas utilizadas, bem como a componente funcional da aplicação, encontram-se bem definidas o que, por um lado, cumpre com os objetivos da solução. Por outro lado, não existe adaptabilidade necessária

para a implementação de diferentes tipos de sistemas de identificação, pois esta solução apenas está definida para implementar sistemas eletrónicos de Registo Civil. Note que o openCRVS apenas deixa em aberto a arquitetura de microsserviços do sistema pois, dependendo das necessidades de cada país, é utilizado um diferente conjunto de microsserviços. Contudo, esta é uma abordagem a ser considerada na definição da arquitetura de um sistema de identificação interoperável, uma vez que estabelece uma base comum de implementação. Essa base comum, por consequência, garante a interoperabilidade entre sistemas que utilizam a mesma solução.

Nesse sentido, a norma técnica ISO/IEC DIS 18013-5 surge como uma alternativa às soluções apresentadas. Os requisitos definidos pela norma técnica ISO/IEC DIS 18013-5 são discutidos no Capítulo 3.

3

NORMA TÉCNICA ISO/IEC DIS 18013-5

A norma técnica ISO-IEC DIS 18013-5[1] é um documento que define a interface e os requisitos necessários para a implementação de uma licença de condução *ISO-compliant* em dispositivos móveis. Esta norma foi desenvolvida por membros da *International Organization for Standardization* (ISO/IEC TC JTC1/SC 17/WG 10).

Os requisitos presentes na norma técnica ISO/IEC DIS 18013-5 foram definidos de forma a permitir a qualquer entidade, afiliada ou não a uma entidade reconhecida pela Autoridade Emissora, o acesso à informação presente num documento de identificação. Também inclui a verificação da autenticidade do documento.

Um dos conceitos fundamentais introduzidos nesta norma técnica ISO/IEC DIS 18013-5 é o **mdoc**. O termo mdoc pode ser definido como um documento ou aplicação que reside num dispositivo móvel ou que requer um dispositivo móvel como parte do processo para aceder a um documento ou aplicação(British Standards Institution, 2021). Partindo do conceito de mdoc, existem outros conceitos importantes na definição de um sistema de identificação *ISO-compliant*.

- **documento móvel:** documento de identificação eletrónica que reside num dispositivo móvel;
- **aplicação portadora:** aplicação móvel responsável pelo armazenamento do documento móvel e pela sua gestão dos processos relacionados com a sua utilização, principalmente durante o processo de identificação. O utilizador final da aplicação portadora é o indíviduo portador do documento móvel (ou **entidade portadora**);
- **entidade portadora do documento móvel (ou *mdoc holder*):** indivíduo que possui um documento de identificação móvel. Utiliza a aplicação portadora para se identificar perante uma **entidade verificadora**;
- **aplicação leitora (ou *mdoc reader*):** aplicação que obtém dados da aplicação portadora para a sua respetiva verificação. É utilizada pela **entidade verificadora**;
- **entidade verificadora (ou *mdoc verifier*):** entidade (indivíduo/organização), que usa e controla a **aplicação leitora**. Uma entidade verificadora pode pertencer a uma **Organização Verificadora**, que é detentora dos seus dados;

1 O documento da norma técnica está disponível em: https://www.iso.org/standard/69084.html

- **Organização Verificadora:** Organização, pública ou privada, reconhecida pela Infraestrutura da Autoridade Emissora (AE), detentora de uma/várias entidades verificadoras. É responsável pelo registo das entidades verificadoras na Infraestrutura da AE;
- **Autoridade Emissora(AE):** organização, que pode ser patenteada ou não, detentora de um/vários documentos móveis. Note que cada organização possui a sua Infraestrutura (**Infraestrutura da AE**) onde é feita a gestão dos vários documentos móveis. Essa infraestrutura também é responsável pela emissão do documento móvel para a **aplicação portadora**.

De forma a perceber melhor não só os requisitos estabelecidos pela norma técnica ISO/IEC DIS 18013-5, mas também os aspetos que não se encontram definidos, é importante discutir os conceitos relacionados com o ciclo de vida de um documento de identificação móvel.

3.1 CICLO DE VIDA DE UMA IDENTIDADE

De acordo com a iniciativa ID4D, o ciclo de vida de uma identidade corresponde ao conjunto de processos necessários, não só para estabelecer a identidade de um indivíduo, mas também para garantir o seu correto uso em posteriores transações. Desta forma, para o ciclo de vida de uma identidade, existem quatro fases (for Development, ID4D):

1. **Registo**, fase em que o indivíduo faz a reivindicação do seu documento de identificação (i.e. pede o seu documento de identificação), fornecendo os seus dados, tipicamente suportados por documentos que provam a sua identidade. Estes dados são validados e registados numa infraestrutura pertencente à entidade responsável pela gestão e emissão desses dados;
2. **Emissão** do documento de identificação para o indivíduo portador do documento. O documento pode ser emitido em formato físico e/ou eletrónico. Um exemplo de um documento de identificação é o Cartão do Cidadão Português (ver Secção 2.1);
3. A fase de **Uso**, que corresponde ao conjunto dos processos associados à utilização da identidade por parte do indivíduo portador do documento;
4. **Gestão**, fase que envolve todos os processos relativos à gestão das credenciais e da identidade do indivíduo no sistema.

Note que, para um documento de identificação ser considerado um documento eletrónico, todos os processos relativos à gestão dos dados devem ser efetuados eletronicamente. O uso desses dados também deve ser possível da mesma forma.

Tendo em conta o contexto da norma técnica ISO/IEC DIS 18013-5, existem particularidades que advém do desenvolvimento de sistemas de identificação digital móvel, nomeadamente:

- O **ciclo de vida de uma aplicação móvel**. Este aspeto é importante, principalmente para o desenvolvimento das aplicações portadora e leitora. A sua descrição encontra-se na Secção 3.2;

3.2 CICLO DE VIDA DE UMA APLICAÇÃO MÓVEL

Um ciclo de vida de uma aplicação móvel contém um conjunto de fases, definidas na Figura 6:

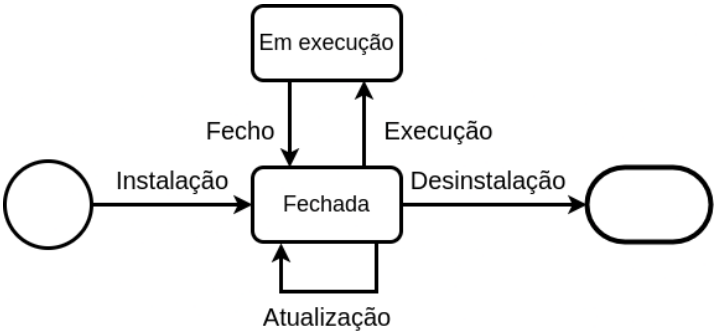

Figura 6: Ciclo de vida de uma aplicação móvel

Numa fase inicial a aplicação é instalada no dispositivo (**Instalação**). O utilizador do dispositivo pode obter a aplicação através da loja de aplicações providenciada pelo Sistema Operativo (SO), por lojas alternativas não oficiais, ou através de outro mecanismo especificado pela entidade fornecedora da aplicação.

Após a instalação, o utilizador do dispositivo pode executar a aplicação e usufruir as funcionalidades fornecidas pela mesma (**Execução**). Durante o estado em que a aplicação está em execução, ela pode estar em primeiro plano, no caso de o utilizador estar a usar a aplicação, ou em segundo plano, no caso de ter outra aplicação aberta.

Caso a aplicação esteja em execução, o utilizador pode fechar a aplicação (**Fecho**). Durante o período em que a aplicação se encontra instalada no dispositivo, ela pode receber novas atualizações (**Atualização**).

Por último, o utilizador pode remover a aplicação do dispositivo, bem como os dados presentes em memória, utilizados pela aplicação (**Desinstalação**).

3.3 CICLO DE VIDA DE UM DOCUMENTO DE IDENTIFICAÇÃO DIGITAL MÓVEL

Tendo em conta os conteúdos abordados nas Secções 3.1 e 3.2, obtém-se a seguinte representação do ciclo de vida de um documento de identificação digital móvel.

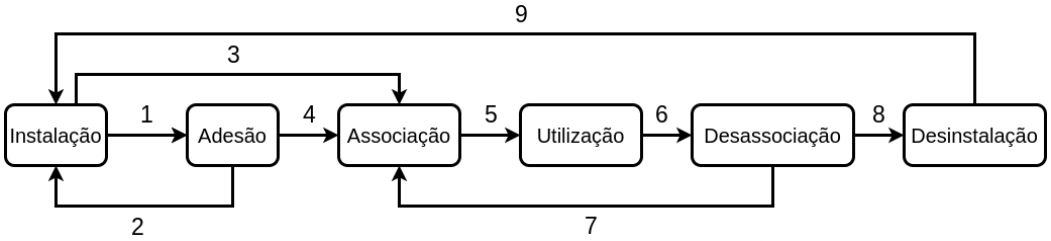

Figura 7: Ciclo de Vida de um documento de identificação digital móvel

Existem seis fases:

1. A fase de **Instalação** inclui todas as etapas para tornar um documento de identificação móvel pronto para a fase de Associação. Nesta fase, o utilizador final escolhe carregar e instalar a aplicação móvel, através das lojas de aplicações móveis disponíveis ou através de um serviço próprio, providenciado pela Autoridade Emissora do documento. Também engloba todos os mecanismos de interação do utilizador com a aplicação móvel, antes do processo de Associação, por exemplo, a definição de um mecanismo de autenticação local (PIN ou autenticação biométrica). A fase de **Instalação** pode ocorrer:
   - Após a fase de **Adesão** (ver seta 2, Figura 7);
   - Depois da fase de **Desinstalação** (ver seta 9, Figura 7).
2. **Adesão** de um novo utilizador na Infraestrutura da AE. Esta fase envolve a recolha dos atributos que, dependendo do esquema de dados definido para o documento móvel (ver Secção 3.3.2), pode ser efetuada a partir de uma ou várias **fontes de atributos**. Também se verifica a ligação do novo utilizador com os atributos recolhidos. Pode ser feita através de meios não eletrónicos, por exemplo, através da inspeção de um documento físico, comparando a foto do utilizador com a presente no documento, por mecanismos de identificação eletrónicos, ou por um sistema de identificação eletrónico. A fase de **Adesão** pode ocorrer antes, ou depois (ver seta 1, Figura 7) da fase de **Instalação**;

   FONTE DE ATRIBUTOS: No contexto deste trabalho, considera-se uma fonte de atributos qualquer entidade ou infraestrutura fornecedora de atributos associados à identidade de um indivíduo. São definidos dois tipos de fontes:
   - **Fonte de atributos local:** Fonte de atributos pertencente à Infraestrutura da AE. Este tipo de fonte não necessita de autenticação para a obtenção dos atributos. Também é possível fazer a gestão dos atributos a partir deste tipo de fonte uma vez que, tipicamente, corresponde à BD da Infraestrutura da AE;
   - **Fonte de atributos externa:** Fonte de atributos pertencente a uma entidade terceira. Note que para obter os atributos requeridos neste tipo de fonte, é exigido o processo de autenticação na Infraestrutura onde se encontra alocada a fonte de atributos.
3. A fase de **Associação** corresponde ao conjunto de processos necessários para a emissão do documento móvel para a aplicação portadora. Pode ocorrer após a fase de **Instalação** (ver seta 3, Figura 7), após a fase de **Desassociação** (ver seta 7, Figura 7), ou após a fase de **Adesão** (ver seta 4, Figura 7). A fase de **Associação** divide-se em duas subfases:
   - A subfase da **Descoberta** dos dados associados ao documento móvel. Esta fase envolve a obtenção dos dados associados ao documento móvel a partir de fontes de atributos locais ou externas. Note que esta fase pode ser suprimida, caso os processos de Adesão e Associação se realizem em conjunto;
   - **Emissão** dos dados do documento móvel, onde os atributos, as estruturas de segurança, e as credenciais da entidade portadora são enviadas para a aplicação portadora.

4. A fase de **Utilização**, que inclui todos os processos relacionados com o uso da aplicação portadora após a fase de Associação, por exemplo, no processo de **identificação de uma entidade portadora perante uma entidade verificadora**. Note que o processo de identificação envolve a **transação de dados**, presentes no documento móvel, para a aplicação leitora. O fluxo de transação de dados difere, dependendo do fornecedor dos dados associados ao documento móvel (aplicação portadora ou Infraestrutura da AE). Os fluxos de transação de dados estabelecidos pela norma técnica ISO/IEC DIS 18013-5 encontram-se definidos na Secção 3.3.4;

5. A fase de **Desassociação**, onde todos os dados emitidos na fase de Associação são removidos da aplicação;

6. A fase de **Desinstalação** corresponde à remoção do dispositivo do software associado à aplicação previamente instalada.

3.3.1 *Interfaces definidas pela norma técnica ISO/IEC DIS 18013-5*

O documento da norma técnica estabelece a existência de três interfaces, ou relações entre as diferentes entidades. Estas relações encontram-se apresentadas no diagrama da Figura 8:

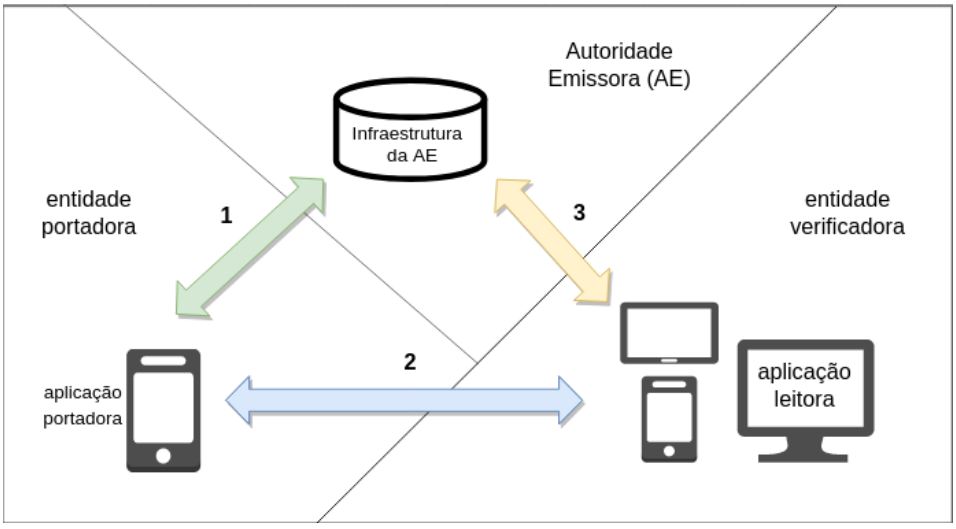

Figura 8: Interfaces definidas pela norma técnica ISO/IEC DIS 18013-5(British Standards Institution, 2021)

- A *interface 1* representa a relação entre a Autoridade Emissora e a aplicação portadora. O fluxo de transação dos dados, existente nesta interface, não está definido pelo documento da norma técnica ISO/IEC DIS 18013-5;
- A *interface 2* representa a relação entre a aplicação portadora e a aplicação leitora;
- A *interface 3* representa a relação entre a aplicação leitora e a Autoridade Emissora.

3.3.2 *Estrutura dos dados presente num documento móvel*

O documento da norma técnica ISO/IEC DIS 18013-5 define uma estrutura de dados extensível para outros documentos móveis, como demonstra a Figura 9:

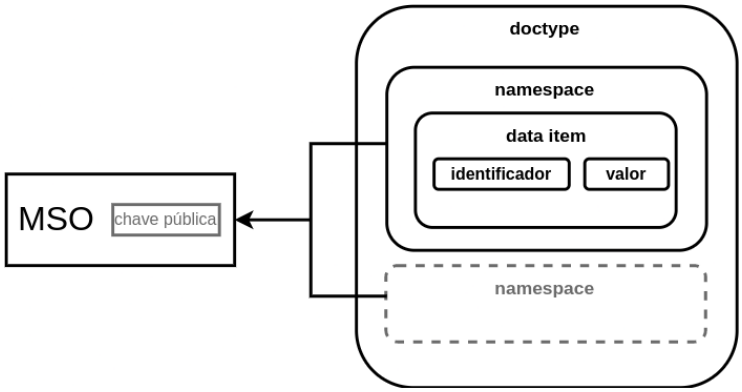

Figura 9: Estrutura de dados definida pela norma técnica ISO/IEC DIS 18013-5 para um documento móvel (British Standards Institution, 2021)

- ***doctype*:** tipo de documento móvel associado à aplicação portadora;
- ***namespace*:** conjunto de **atributos** com um propósito associado a esse *namespace*. Um documento móvel pode conter elementos de dados de vários *namespaces*;
- **atributo (ou *data item*):** elemento de dados, associado a um *namespace*. Cada atributo apresenta um **identificador** único, bem como o seu respetivo **valor**.

Para cada documento móvel, existe uma estrutura de segurança associada, designada na norma técnica ISO/IEC DIS 18013-5 como Mobile Security Object (MSO). A estrutura encontra-se descrita na Secção 3.3.3.

3.3.3 *Mobile Security Object (MSO)*

A norma técnica ISO/IEC DIS 18013-5 define a existência de uma estrutura específica para garantir a segurança do documento móvel emitido pela Infraestrutura da AE, designada como *Mobile Security Object (MSO)*.

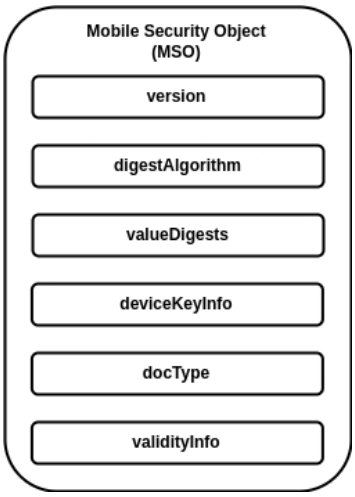

Figura 10: Estrutura do MSO (British Standards Institution, 2021)

Desta forma, o MSO apresenta a estrutura presente na Figura 10:

- **version:** Versão da estrutura criada. No contexto da última versão do documento publicado da norma técnica ISO/IEC DIS 18013-5, a versão definida é "1.0";
- **digestAlgorithm:** Algoritmo utilizado para a geração dos *digests* calculados pela aplicação leitora, durante o mecanismo de autenticação dos dados provenientes da Infraestrutura da AE (ou *Issuer Data Authentication*);
- **valueDigests:** Contém um conjunto de *digests* utilizados no processo de autenticação dos dados da Infraestrutura da AE (ou *Issuer Data Authentication*);
- **deviceKeyInfo:** Estrutura que contém a chave pública utilizada para verificação da assinatura gerada pela aplicação portadora durante o mecanismo de autenticação dos dados gerados da aplicação portadora (ou *mdoc authentication*);
- **docType:** Tipo de documento associado à aplicação portadora, que é assinada pelo MSO;
- **validityInfo:** Estrutura composta por datas associadas à criação, emissão e prazo de validade do documento móvel. Esta estrutura é importante para garantir que o documento móvel não está caducado;

Note que no documento, a nível técnico, apenas são especificados os mecanismos de segurança da informação relacionados com o processo de transação dos dados associados ao documento móvel. Os mecanismos de segurança definidos pela norma técnica ISO/IEC DIS 18013-5 são descritos ao longo da Secção 3.3.4.

3.3.4 *Fluxo de transação dos dados de um documento móvel*

O fluxo de transação de dados é dividido em três fases: a fase de **Inicialização**, onde os dados do documento móvel e as estruturas de segurança são carregadas para memória, o **Estabelecimento da conexão** (ou *De-*

vice Engagement) e a fase da **Obtenção dos dados** (ou *Data Retrieval*). Note que existem diferentes fluxos, dependendo da entidade que fornece os dados para a aplicação leitora (aplicação portadora ou a Infraestrutura da AE).

3.3.4.1 *Estabelecimento da conexão*

O fase de Estabelecimento da conexão corresponde ao conjunto de processos necessários para o estabelecimento de uma conexão entre a aplicação portadora e a aplicação leitora. Envolve os seguintes processos: (British Standards Institution, 2021):

1. A aplicação portadora gera e envia para a aplicação leitora uma estrutura, designada **DeviceEngagement**. A aplicação leitora obtém a estrutura através da leitura de um QR-Code, gerado pela aplicação portadora, ou via NFC, através da utilização de um dos protocolos de *Connection Handover* definidos pela especificação técnica do NFC[2].

   A estrutura DeviceEngagement contém a informação relativa às tecnologias de transporte suportadas pela aplicação portadora para a fase de Obtenção dos dados. É importante referir que a norma técnica ISO/IEC DIS 18013-5 permite apenas a utilização de uma das tecnologias, durante o processo de Obtenção dos dados, pode ser Bluetooth Low Energy (BLE), Near Field Communication (NFC) ou Wi-Fi Aware. Também contém uma chave pública gerada pela aplicação portadora, designada *EDeviceKey.Pub*. É utilizada na geração das chaves de sessão, necessárias para o mecanismo de **Encriptação da Sessão**.

   - **Encriptação da Sessão (ou *Session Encryption*):** Mecanismo de segurança responsável pela criação de uma sessão segura de transferência de dados entre a aplicação portadora e a aplicação leitora, protegendo os dados do documento móvel de possíveis alterações e de ataques de *eavesdropping*. A sessão é estabelecida através da encriptação das mensagens enviadas e da desencriptação das mensagens recebidas. O par de chaves utilizadas para os processos de encriptação/desencriptação, designadas por chaves de sessão[3], resultam da derivação de chaves efémeras, através da utilização do protocolo Elliptic Curve Diffie-Hellman (ECDH). Este protocolo envolve a troca de chaves públicas[4] entre as aplicações portadora e leitora.

2. A aplicação leitora recolhe da estrutura *DeviceEngagement* a chave pública, proveniente da aplicação portadora (*EDeviceKey.Pub*), necessária para a geração do par de chaves de sessão, utilizadas no mecanismo de Encriptação da Sessão. Também recolhe a informação relativa às tecnologias de transporte suportadas pela aplicação portadora. A partir da informação proveniente da estrutura, a aplicação leitora gera as chaves de sessão, e escolhe a tecnologia a ser utilizada durante a fase de Obtenção dos dados.

2 Mais informações consultar: https://nfc-forum.org/our-work/specification-releases/specifications/

3 O documento da norma técnica ISO/IEC DIS 18013-5 define as chaves de sessão por *SKDevice* e *SKReader*. A chave *SKDevice* é responsável pela encriptação das mensagens enviadas pela aplicação portadora e desenpcripação das mesmas pela aplicação leitora, quando as recebe. No caso inverso, utiliza-se a chave *SKReader*.

4 O par de chaves assimétricas utilizadas no processo de derivação e de troca, são designadas no documento da norma técnica ISO/IEC DIS 18013-5 como *EDeviceKey* o par gerado pela aplicação portadora, e *EReaderKey* o par gerado pela aplicação leitora.

3. Geração e envio da estrutura *SessionEstablishment*, através da tecnologia de transporte escolhida no ponto anterior, para a aplicação portadora. Contém a chave pública (*EReaderKey.Pub*) gerada pela aplicação leitora e o pedido de atributos (ou *mdoc request*), encriptado pela chave de sessão *SKReader*. A estrutura do pedido de atributos é composta pelo conjunto de atributos requeridos, e uma estrutura de segurança, responsável por autenticar tanto a entidade verificadora como o pedido de atributos (ver descrição do mecanismo de autenticação da entidade verificadora, Item 1, Secção 3.3.4.2);

4. A aplicação portadora recebe e processa o conteúdo a estrutura *SessionEncryption*, proveniente da aplicação leitora. Posteriormente, gera o par de chaves de sessão (*SKDevice* e *SKReader*). Nesta fase, a conexão entre as duas entidades (aplicação portadora e aplicação leitora) já se encontra estabelecida.

3.3.4.2 *Obtenção dos dados*

Após o estabelecimento da conexão entre a aplicação portadora e a aplicação leitora, a aplicação portadora desencripta com a chave *SKReader* e processa o pedido de atributos (ou *mdoc request*).

O processamento do pedido divide-se em duas fases:

1. Verificação da existência de um pedido de atributos **autenticado por uma entidade verificadora**.
   - **Autenticação da entidade verificadora (ou *mdoc reader authentication*):** Este mecanismo de segurança serve para garantir que tanto a entidade verificadora, como o pedido efetuado à aplicação portadora se encontram autenticados por uma Organização Verificadora reconhecida pela Infraestrutura da AE. Envolve dois processos:
     a) Validação da assinatura presente na estrutura *ReaderAuth*. Esta estrutura contém uma cadeia de certificados emitida por uma Infraestrutura associada à Organização Verificadora, e uma assinatura gerada pela aplicação leitora;
     b) Validação da cadeia de certificados x509v3 presente na estrutura *ReaderAuth*. A validação da cadeia de certificados serve para estabelecer uma relação de confiança entre a entidade verificadora, a Organização Verificadora, e a Infraestrutura da AE.

2. Verificação do tipo de obtenção requerido pela aplicação leitora. O documento da norma técnica ISO/IEC DIS 18013-5 define a existência de dois processos distintos de obtenção dos dados (British Standards Institution, 2021):
   a. **Server Retrieval:** Neste tipo de obtenção, o responsável pelo envio dos dados é a Infraestrutura da AE. Este processo deve ser feito via WebAPI ou através do protocolo OpenID Connect (OIDC);
   b. **Device Retrieval:** Neste caso, o responsável pelo envio dos dados à aplicação leitora é a aplicação portadora. Para este processo apenas podem ser usadas as tecnologias Bluetooth Low Energy (BLE), Near Field Communication (NFC) ou Wi-Fi Aware . Não é obrigatória a existência de uma conexão com a Infraestrutura da AE.

Posteriormente, a aplicação portadora gera a estrutura de resposta ao pedido de atributos. A estrutura é composta por quatro componentes:

1. Conjunto de atributos emitidos pela Infraestrutura da AE (ou *IssuerNameSpaces*);
2. A assinatura do MSO (ou *IssuerAuth*), no formato *CBOR Object Signing and Encryption (COSE)*;
3. Conjunto de atributos gerados pela aplicação portadora (ou *DeviceNameSpaces*);
4. A assinatura dos atributos gerados pela aplicação portadora (ou *DeviceAuth*), no formato COSE.

Note que os atributos inseridos na estrutura de resposta variam não só com a entidade que gera os atributos, mas também de acordo com o tipo de obtenção requerido pela aplicação leitora.

- Caso se utilize o mecanismo de *Server Retrieval*, envia-se uma estrutura composta por um *token* com o pedido de atributos assinado pela aplicação portadora, e o Uniform Resource Locator (URL) onde se efetua o pedido de atributos à Infraestrutura da AE;
- Para o mecanismo de *Device Retrieval*, são enviados os atributos pedidos pela aplicação leitora;

Após a criação da estrutura, esta é enviada para aplicação leitora, que faz o seu processamento. Envolve a verificação dos seguintes mecanismos de segurança da informação:

- **Autenticação dos dados provenientes da AE (ou *Issuer Data Authentication*):** Este mecanismo de segurança serve para garantir que os dados são emitidos pela Autoridade Emissora, e que não foram alterados desde a fase de Associação. Consiste nas seguintes fases:
  1. Validação da cadeia de certificados x509v3, associada à Infraestrutura da AE. Note que para fazer a validação, é necessário obter o certificado proveniente da estrutura de resposta, enviada pela aplicação portadora, bem como do certificado raiz de assinatura da Autoridade Emissora;
  2. Validação da assinatura onde se encontra o MSO;
  3. Validação dos *digests* presentes no campo *valueDigests* do MSO (ver Secção 3.3.3). Consiste na comparação entre o valor do *hash*, gerado pela aplicação leitora, de cada atributo fornecido pela estrutura *IssuerNameSpaces*, com os valores presentes em cada atributo, no campo *valueDigests*;
  4. Validação do parâmetro *doctype* presente no MSO, através da comparação com o valor do *doctype* presente na estrutura de resposta, enviada pela aplicação portadora;
  5. Verificação da caducidade do documento móvel através da estrutura *validityInfo*, presente no MSO (ver Secção 3.3.3).
- **Autenticação da aplicação portadora (ou *mdoc authentication*):** Este tipo de mecanismo de segurança garante que o dispositivo que enviou a mensagem é o mesmo dispositivo para o qual foi emitido o documento móvel na fase de Associação. Isto, uma vez que a chave pública utilizada na verificação da assinatura está incluida no MSO. Também previne o risco de ataques Man In The Middle (MITM), uma vez que se faz a validação da assinatura gerada pela aplicação portadora.

Caso a aplicação leitora opte pela requisição de atributos utilizando o processo de *Server Retrieval*, esta envia o *token* com o pedido de atributos, gerado e assinado pela aplicação portadora, para a Infraestrutura da AE.

Durante este processo, existem dois mecanismos de segurança a considerar:

- **Utilização do protocolo TLS com autenticação do servidor:** Este mecanismo serve para garantir uma comunicação segura entre a aplicação leitora e a Infraestrutura da AE.
- **Utilização de assinaturas digitais** em tokens enviados pela Infraestrutura da AE. As assinaturas servem para autenticar a mensagem proveniente do emissor, neste caso, da Infraestrutura da AE.

Após a obtenção dos atributos, a aplicação leitora faz o processamento dos atributos recebidos, apresentando-os à entidade verificadora.

Note que o fluxo de obtenção dos dados é cíclico, ou seja, para cada pedido de atributos por parte da aplicação leitora é efetuado o mesmo fluxo descrito ao longo desta Secção.

3.3.5 *Mecanismos de Consentimento (entidade portadora de um documento móvel)*

De forma a cumprir com um dos princípios de privacidade, nos quais a norma técnica ISO/IEC DIS 18013-5 se baseia (ver princípio de Consentimento e Escolha, no documento da norma técnica ISO/IEC 29100), o documento da norma técnica ISO/IEC DIS 18013-5 define dois tipos de consentimento:

- **Consentimento prévio:** A entidade portadora pode configurar entidades verificadoras especifícas, em que confia, para partilhar determinados atributos, sem a necessidade de um novo consentimento durante o período de transação;
- **Consentimento durante a transação (ou *Transaction-time consent:*)** O consentimento pode ser feito durante o processo de transação, ou seja, a entidade portadora pode obter o pedido de atributos, consentir o envio, e enviar os atributos requeridos para a aplicação leitora.

As formas de consentimento explicitadas nos pontos anteriores devem respeitar uma máxima, que exige um consentimento informado para todas as transações de dados relativos à carta de condução móvel. Uma vez que é um caso específico de um documento de identificação móvel, e o documento define a sua extensibilidade para outros tipos de documentos de identificação, os mesmos mecanismos devem ser aplicados para qualquer documento móvel.

Considera-se um consentimento informado quando estão preenchidos os seguintes requisitos:

1. A entidade portadora recebe um aviso/notificação, com informação sobre os atributos pedidos, a entidade verificadora requerente, e o motivo do pedido;
2. A entidade portadora deve poder aceitar ou rejeitar o envio dos atributos requeridos.

3.4 ASPETOS NÃO DEFINIDOS PELA NORMA TÉCNICA ISO/IEC DIS 18013-5

Tendo em conta o conteúdo abordado na Secção 3.3, e ao longo do Capítulo 3, é possível observar que a norma técnica ISO/IEC DIS 18013-5 tem como objetivo principal uniformizar o processo de transação e validação de documentos móveis de identificação. Desta forma, não existe uma especificação concreta de fases importantes no ciclo de vida de um documento móvel, nomeadamente as fases de **Instalação**, **Adesão**, **Associação**, **Desassociação** e **Desinstalação**. Consequentemente, também não se encontram definidos para estas fases os **mecanismos de segurança da informação** necessários para cumprir o princípio de Segurança da Informação, no qual o documento norma técnica ISO/IEC DIS 18013-5 se baseia.

1. As fases de **Instalação** e **Desinstalação** não serão definidas a nível técnico na arquitetura proposta no Capítulo 4. Compete a cada organização definir qual o mecanismo de fornecimento das aplicações portadora e leitora e o tipo de autenticação local que pretenda adotar. Pode optar, por exemplo, pela definição de um PIN e/ou pela utilização da biometria como forma de autenticação na aplicação;

2. Para a fase de **Adesão**, tendo em conta a descrição presente no item 2, Secção 3.3, é necessário definir os mecanismos responsáveis pela:

    a) **Recolha dos atributos relativos ao novo utilizador**. Estes atributos podem ser recolhidos através de documentos de identificação físicos ou por fontes de atributos externas;

    b) **Verificação da ligação entre os atributos recolhidos e o novo utilizador**, no caso da adesão de uma nova entidade portadora. Pode ser feita através da inspeção do documento físico, ou através de sistemas de identificação eletrónicos. Este mecanismo encontra-se fora do âmbito deste trabalho.

3. A fase de **Associação** envolve processos que também precisam de ser definidos:

    a) O processo de **Descoberta** dos dados, associados à entidade portadora que esteja a associar um dispositivo móvel no sistema. É necessário estabelecer o fluxo de:

        - **Associação** de um, ou vários **dispositivos móveis** a uma **entidade portadora**;
        - **Obtenção dos atributos** associados à **entidade portadora**.

    b) A **Emissão** dos dados para o dispositivo móvel onde está instalada a aplicação portadora. Esta fase envolve a geração da estrutura do documento móvel, e das estruturas de segurança responsáveis pelos mecanismos de segurança estabelecidos pela norma técnica ISO/IEC DIS 18013-5.

    É importante voltar a referir que as fases de **Adesão** e **Associação** podem ocorrer em conjunto (ver Secção 3.3). Assim, existem algumas fases que são suprimidas, como o caso da obtenção/recolha dos atributos.

4. Por último é necessário também estabelecer um mecanismo de **Desassociação** de um dispositivo móvel do sistema.

Para além da definição das fases associadas ao ciclo de vida de um documento móvel, a norma técnica ISO/IEC DIS 18013-5 também não define nenhuma abordagem para a implementação das funcionalidades necessárias ao funcionamento de cada uma das entidades (Infraestrutura da AE, aplicação portadora e aplicação leitora).

1. **Gestão dos mecanismos de segurança**, descritos ao longo da Secção 3.3.4;
2. **Definição dos mecanismos de segurança** a serem utilizados durante as fases de **Associação** e de **Adesão**, que não se encontram definidos pela norma técnica ISO/IEC DIS 18013-5. A descrição dos mecanismos encontra-se nas Secções 4.1.7.1 e 4.1.11.1;
3. Estabelecimento dos **fluxos de comunicação** entre a **aplicação portadora e a Infraestrutura da AE**, e a **aplicação leitora e a Infraestrutura da AE**;
4. **Gestão dos dados** dentro de cada uma das entidades definidas pela norma técnica ISO/IEC DIS 18013-5 (ver Secção 3.3.1);
5. Implementação dos **mecanismos de consentimento** definidos na Secção 3.3.5

Por fim, considerando o mecanismo de autenticação da entidade verificadora (ou *mdoc reader authentication*), descrita na Secção 3.3.4, a norma técnica ISO/IEC DIS 18013-5 define a possibilidade de uma entidade verificadora estar autenticada numa Infraestrutura associada à Organização Verificadora. Nesse sentido, é importante referir que as fases de Adesão e Associação do ciclo de vida de um documento móvel (ver Secção 3.3) também são aplicáveis para a aplicação leitora. Contudo estas fases diferem, tanto a nível do fluxo de comunicação, como a nível dos dados que são transmitidos.

- No contexto deste trabalho, a fase de **Adesão** é efetuada pela **Organização Verificadora**. Ela é responsável por registar as entidades verificadoras no sistema. Tendo em conta que é a Organização que está a fazer esse registo, não existem atributos a serem recolhidos. Logo, não se efetua o processo de verificação da ligação entre entidade verificadora e atributos recolhidos.
- Na fase de **Associação**, apenas são emitidas para a aplicação leitora a cadeia de certificados de autenticação da entidade verificadora (ver mecanismo de autenticação da entidade verificadora, Item 1, Secção 3.3.4.2). Não existe a fase de Descoberta, uma vez que o certificado raiz já se encontra gerado e o certificado de autenticação é assinado na fase de Emissão.

Assim, a definição de uma arquitetura que também cubra os aspetos não definidos pela norma técnica ISO/IEC DIS 18013-5 vai não só facilitar, como acelerar o processo de desenvolvimento de um sistema de identificação móvel *ISO-compliant*.

3.5 SUMÁRIO DO CAPÍTULO

Ao longo do Capítulo 3 são discutidos aspetos importantes no desenvolvimento da arquitetura de um sistema de identificação baseado na norma técnica ISO/IEC DIS 18013-5.

As primeiras secções apresentam um conjunto de conceitos importantes, não só para perceber os requisitos definidos pela norma técnica ISO/IEC DIS 18013-5, na qual este trabalho se concentra, mas também os aspetos técnicos que não estão definidos. Um dos conceitos vitais no desenvolvimento de um sistema de identificação móvel é o conceito de ciclo de vida de um sistema de identificação móvel. Com base nisso, são apresentados os requisitos definidos pela norma técnica ISO/IEC DIS 18013-5.

Após a análise dos requisitos abordados, verifica-se que a norma técnica ISO/IEC DIS 18013-5 apenas define os requisitos técnicos relacionados com a transação de atributos do documento de identificação e a validação dos atributos recebidos durante esse processo. Tendo em conta esta constatação, existem aspetos que não se encontram definidos pela norma técnica ISO/IEC DIS 18013-5. Note que estes aspetos estão relacionados especialmente com fases importantes associadas ao ciclo de vida de um documento móvel. Existem também algumas fases que não serão definidas a nível técnico na arquitetura do sistema (fase de Instalação e Desinstalação).

Assim, com base nos conceitos discutidos neste capítulo, o Capítulo 4 apresentará a arquitetura definida para a implementação de um sistema de identificação móvel.

4

PROPOSTA DE ARQUITETURA DE UM SISTEMA DE IDENTIFICAÇÃO BASEADO NA NORMA TÉCNICA ISO/IEC DIS 18013-5

4.1 ARQUITETURA GERAL DO SISTEMA

A definição da proposta de arquitetura parte da relação entre as interfaces presentes na Figura 8. Assim, para cada entidade envolvida (Infraestrutura da AE, aplicação portadora, e aplicação leitora), definem-se componentes necessárias para o seu desenvolvimento, descritos nas Secções 4.1.1, 4.1.3 e 4.1.4.

4.1.1 *Infraestrutura da AE*

Para a Infraestrutura da AE, definem-se as seguintes componentes, presentes na Figura 11:

1. **Gestão**, componente responsável pela gestão de todos os processos associados ao ciclo de vida do documento móvel, nos quais Infraestrutura da AE é responsável. Dentro desta componente, existem as seguintes subcomponentes:
    a) **Gestão e Obtenção de Atributos/Credenciais:** Gestão e obtenção dos atributos presentes na BD local. Os atributos podem ser credenciais de autenticação em fontes de atributos externas, credenciais de autenticação na Infraestrutura da AE, atributos associados a um documento móvel, estruturas de segurança, entre outros. Do ponto de vista técnico, é responsável pela comunicação com a BD da Infraestrutura da AE;
    b) **Gestão de atributos de FA's externas:** Obtenção de atributos de FA's externas (ver descrição do fluxo de obtenção de atributos de FA's externas, na Secção 4.1.6.1). Também efetua a gestão da atualização dos dados provenientes dessas fontes (ver definição de fonte de atributos externa, Secção 3.3, item 2);
    c) **Gestão de *nameSpaces*:** Componente responsável pelo povoamento da BD, com base na estrutura do documento móvel. Note que os atributos presentes na estrutura do documento móvel (ver Secção 3.3.2) são definidas pelo utilizador final do sistema. A Secção 5.1.3, mostra um exemplo de uma configuração da estrutura de um documento móvel para um sistema de identificação estudantil;

d) **Gestão de Associações:** Gestão dos dados relativos à fase de Associação de todas as entidades portadoras e entidades verificadoras pertencentes ao sistema. Podem ser relativos ao dispositivo atualmente associado, a chave (ou chaves) de associação (ver Secção 4.1.11.1), entre outros dados necessários durante a fase de Associação, por exemplo credenciais de autenticação na Infraestrutura da AE. Importante referir que, no contexto da arquitetura proposta, a fase de **Associação da entidade verificadora** também se **efetua na Infraestrutura da AE**;

e) **Gestão de entidades verificadoras:** Componente responsável pela gestão dos dados associados a entidades verificadoras que efetuaram, ou que estão a efetuar o processo de Adesão na Infraestrutura da AE.

2. **Adesão**, responsável pela gestão do processo de Adesão de um novo utilizador na Infraestrutura da AE. Dentro desta componente, existem as seguintes subcomponentes:

   a) **Geração do documento móvel:** Geração da estrutura de dados do documento móvel, com base nos atributos obtidos a partir de FA's locais e/ou externas. A descrição dos fluxos de obtenção de dados encontram-se nas Secções 4.1.6 e 4.1.6.1;

   b) **Geração dos dados associados à entidade verificadora:** Geração da estrutura de dados associada a uma entidade verificadora que esteja em processo de Adesão na Infraestrutura da AE.

3. **Associação**, componente responsável pela gestão da fase de Associação na Infraestrutura da AE. Os processos envolvidos na fase de Associação encontram-se descritos na Secções 4.1.10 e 4.1.8;

4. **Transação**, responsável pela gestão do processo de transação dos dados entre a aplicação portadora e a aplicação leitora na Infraestrutura da AE (ver Secção 3.3.4). Dentro desta componente, existem as seguintes subcomponentes:

   a) **Validação do documento móvel (modo *online*):** Componente responsável por todos os subprocessos, executados pela Infraestrutura da AE, e que estão associados ao processo de *Server Retrieval*;

5. **Comunicação com aplicações ISO 18013-5 *compliant***, responsável pelo fluxo de comunicação entre aplicações *compliant* com a norma técnica ISO/IEC DIS 18013-5 (neste caso, a aplicação portadora e a aplicação leitora);

6. **Autenticação**, responsável pela gestão do fluxo de autenticação. Note que o processo de autenticação é realizado em dois casos distintos:

   - Autenticação em fontes de atributos externas (ver item 2, Secção 3.3 a definição de Fonte de Atributos), para a obtenção de atributos e posterior geração da estrutura de dados do documento móvel;
   - Autenticação na Infraestrutura da AE, necessária para a fase de Associação das entidades portadora e leitora (ver Secção 4.1.10 e Anexo 4.1.8);

7. **Segurança da Informação**, responsável pelos mecanismos de segurança necessários para a implementação de uma Autoridade Emissora de dados confiável e *ISO-compliant*;

8. **Desassociação**, responsável pelo fluxo de Desassociação de uma entidade (portadora ou verificadora) da Infraestrutura da AE (ver Secção 3.3).

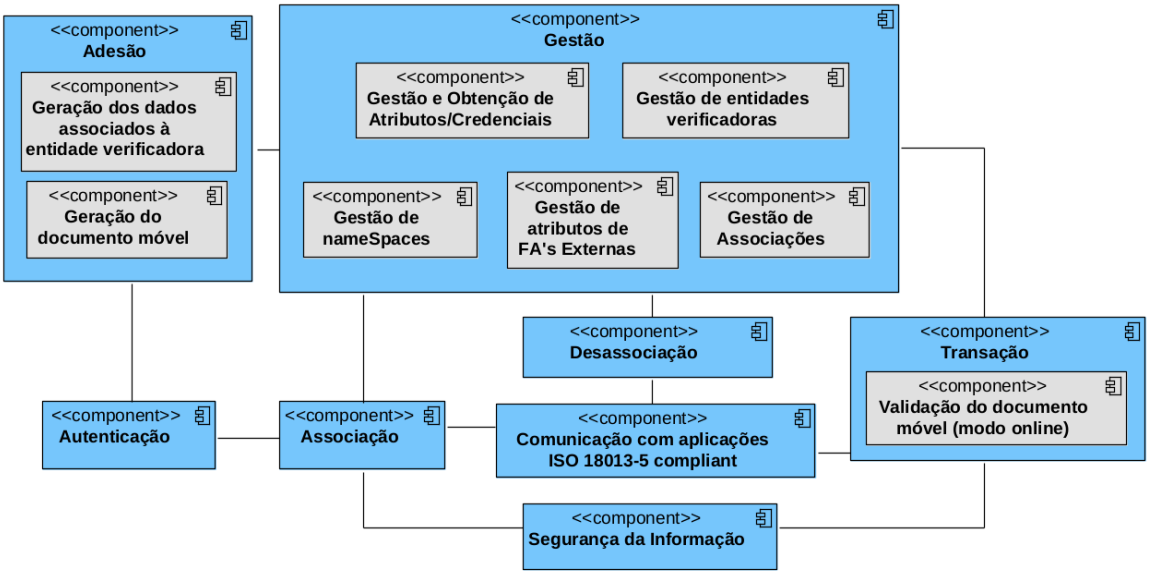

Figura 11: Componentes da Infraestrutura da AE

A modelação da Infraestrutura da AE implica a modelação do esquema lógico da BD, descrita na Secção seguinte.

4.1.2 *Modelação do SGBD da Infraestrutura da IA*

A Figura 12 apresenta o esquema lógico proposto para a BD da Infraestrutura da IA.

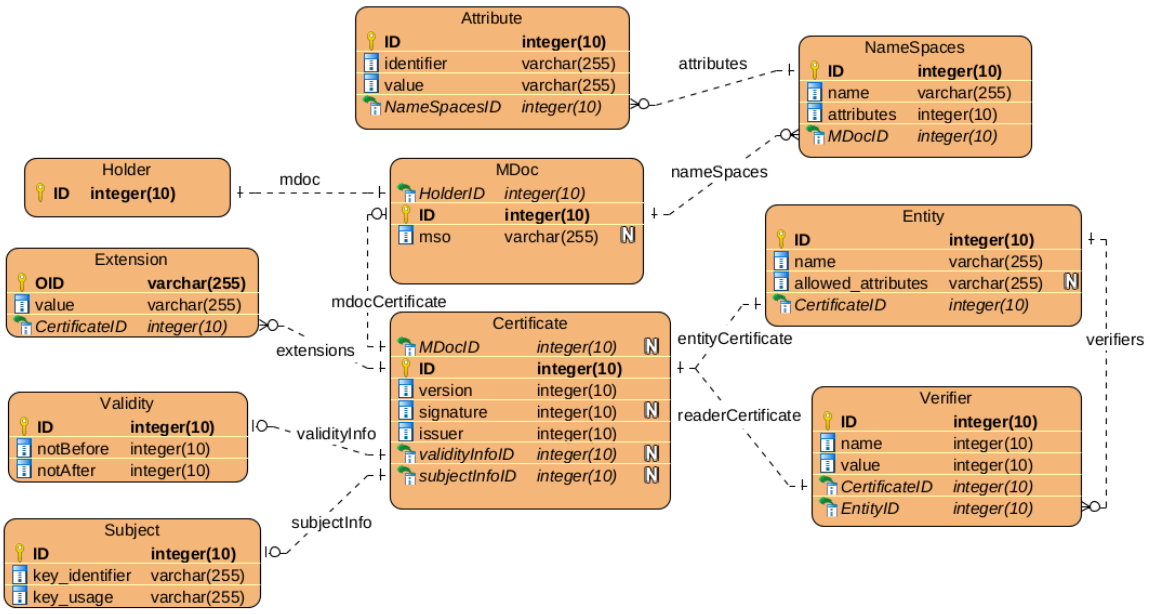

Figura 12: Esquema lógico proposto para a BD da Infraestrutura da AE

Uma solução de identificação móvel genérica deve guardar informação relativa aos individuos que já efetuaram o processo de Adesão na entidade (ou entidades portadoras). Esses indivíduos, representados pela tabela **Holder**, são portadores de um, ou vários, documentos móveis. Cada entrada da tabela Holder contém um conjunto de chaves públicas de associação (ver Secção 4.1.11.1). Note que estas chaves são necessárias para associar um/um conjunto de dispositivo(s) móvel(veis) a um documento móvel, após a Associação.

A tabela **MDoc** guarda todos os documentos móveis existentes na Infraestrutura da AE. Esta tabela apresenta um, ou vários, *nameSpaces* (ver tabela **NameSpace**) que podem ser definidos através da definição da estrutura do documento móvel no ficheiro de configuração do sistema de identificação. Por defeito, serão utilizados os *nameSpaces* definidos pela norma técnica ISO/IEC DIS 18013-5. Para cada *nameSpace*, existe um conjunto de atributos (ver tabela **Attribute**) associados. Os atributos também são definidos através da configuração da estrutura do documento móvel, no ficheiro de configuração do sistema.

Para armazenar os dados associados a uma entidade verificadora, definiu-se a tabela **Verifier**. Relativamente à organização, à qual pertence a entidade verificadora, criou-se a tabela **Entity**.

De forma a modelar os atributos presentes nos certificados associados a cada entidade (portador, entidade verificadora e organização verificadora) criou-se uma tabela (**Certificate**), com atributos relativos a um certificado x509v3 a ser gerado. As tabelas **Extension**, **Validity** e **Subject** representam a componente das extensões ao certificado, a componente de validade do certificado e a componente *Subject*, respetivamente.

4.1.3 *Aplicação portadora*

Para a aplicação portadora, definem-se as seguintes componentes, presentes na Figura 13:

1. Componente de **Gestão**, responsável pela gestão da informação necessária ao funcionamento da aplicação portadora. Esta componente subdivide-se nas seguintes componentes:
    a) **Gestão de atributos:** Componente responsável pela gestão dos atributos relativos ao documento móvel, recebido durante a fase de Associação;
    b) **Gestão de credenciais:** Efetua a gestão das credenciais de autenticação na Infraestrutura da AE;
    c) **Gestão de estruturas de segurança:** Gestão das estruturas necessárias para efetuar os mecanismos de segurança da informação estabelecidos pela norma técnica ISO/IEC DIS 18013-5. As estruturas incluem o MSO e o certificado raiz da Autoridade Certificadora (AC) associada à Infraestrutura da AE;
    d) **Gestão de entidades verificadoras autorizadas:** Gestão das entidades verificadoras que apresentam consentimento prévio. Note que as entidades verificadoras pré-consentidas são definidas pela entidade portadora (ver Secção 3.3.5);
        - **Perfil de entidade verificadora:** Corresponde ao conjunto pré-definido de atributos que a aplicação leitora pode pedir à aplicação portadora, durante a fase de transação dos dados. Após a transação, a entidade portadora pode guardar esse perfil na aplicação portadora, dando consentimento prévio em transações posteriores.

          O conjunto de atributos pode ser pré-definido na Infraestrutura da AE, no caso de uma entidade verificadora estar associada na aplicação leitora, ou pela aplicação leitora, no caso de a entidade verificadora não se encontrar associada na aplicação leitora. Também existe a possibilidade da configuração de subconjuntos de atributos na aplicação leitora a partir do conjunto de atributos pré-definidos.
    e) **Armazenamento de dados:** Componente com métodos responsáveis pelo acesso direto à base de dados segura do dispositivo. De referir que a norma técnica ISO/IEC DIS 18013-5 exige o armazenamento dos dados associados ao documento móvel numa área segura, contudo não define os mecanismos de segurança a serem utilizados;
        - Atualmente, os sistemas operativos móveis existentes já providenciam áreas de armazenamento seguro. Estas áreas são protegidas através de mecanismos criptográficos, que impedem o acesso não autorizado aos dados armazenados (KeyStore e/ou IdentityCredentialStore, no caso do sistema Android e Secure Enclave no caso do sistema iOS).
    f) **Gestão de acesso a atributos do documento móvel:** Gestão dos atributos, presentes na aplicação portadora, nos quais as entidades verificadoras, configuradas pela entidade portadora, apresentam consentimento prévio (ver Secção 3.3.5 e a definição de perfil de entidade verificadora item 1d).

2. Componente de **Associação**, responsável pela gestão do processo de Associação de uma entidade portadora na Infraestrutura da AE (ver Descrição 3, Secção 3.3).

3. **Transação**, responsável pela gestão do processo de transação dos dados estabelecido pela norma técnica ISO/IEC DIS 18013-5. Subdivide-se nas seguintes componentes:

    a) **Inicialização, DeviceEngagement e Data Retrieval:** Componentes responsáveis pelas fases de transação explicitadas na Secção 3.3.4;

4. **Desassociação**, responsável pelo processo de desassociação da Infraestrutura da AE, no caso de a entidade portadora estar associada na aplicação portadora.

    a) **Remoção do documento móvel:** Remoção de todos os dados associados ao documento móvel, incluindo estruturas de segurança (MSO e o certificado de assinatura da MSO), do armazenamento seguro do dispositivo.

5. **Segurança da Informação**, responsável pelos mecanismos de segurança definidos pela norma técnica ISO/IEC DIS 18013-5 durante o processo de transação dos dados do documento móvel. Também é responsável pelos mecanismos de segurança não definidos pela norma técnica, por exemplo, para a fase de Associação (os mecanismos de segurança definidos para a fase de Associação encontram-se descritos na Secção 4.1.11.1);

6. Componente de **Comunicação**, responsável pelos fluxos de comunicação entre as entidades definidas pela norma técnica ISO/IEC DIS 18013-5. Subdivide-se nas seguintes componentes:

    a) **Comunicação com Infraestrutura da AE:** Componente responsável pelo fluxo de comunicação entre a aplicação portadora e a Infraestrutura da AE;

    b) **Comunicação com a aplicação leitora:** Responsável pelo fluxo de comunicação entre a aplicação portadora e a aplicação leitora.

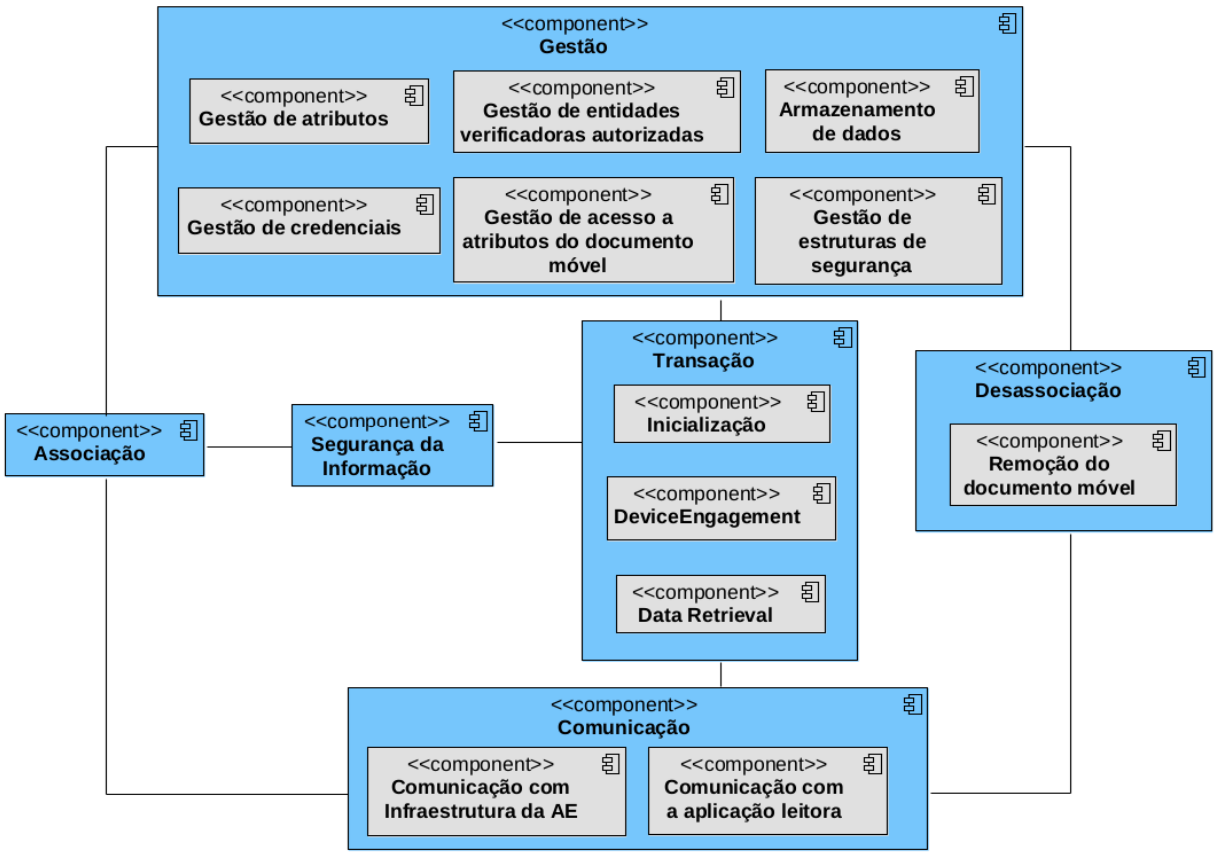

Figura 13: Diagrama de componentes da aplicação portadora

4.1.4 *Aplicação leitora*

Para a definição da aplicação leitora, consideram-se as seguintes componentes, presentes na Figura 14:

1. **Gestão**, componente responsável pela gestão da informação necessária ao funcionamento da aplicação leitora. Subdivide-se nas seguintes componentes:
   a) **Gestão de atributos:** Gestão dos atributos relativos à entidade verificadora que efetuou a Associação na aplicação, por exemplo, nome, idade, Organização Verificadora a que pertence, etc. Esta componente é opcional, uma vez que a norma técnica ISO/IEC DIS 18013-5 apenas define a possibilidade de entidades verificadoras estarem autenticadas na Infraestrutura da AE (ver penúltimo parágrafo da Secção 3.4);
   b) **Gestão de credenciais:** Efetua a gestão das credenciais de autenticação na Infraestrutura da AE. Esta componente é opcional pelo mesmo motivo do ponto anterior;
   c) **Gestão de perfis de entidade verificadora:** Uma componente responsável pela gestão dos perfis de acesso aos atributos da entidade portadora, por parte da aplicação leitora (ver descrição de perfil de entidade verificadora na Secção 4.1.3, Item 1d);

d) **Armazenamento dados:** ver Descrição 1e, na Secção 4.1.3;

2. **Associação**, responsável pela gestão do processo de Associação de uma entidade verificadora na Infraestrutura da AE (ver Descrição 3, Secção 3.3). Esta componente é opcional, pelo motivo explicitado no Item 1a.

3. Componente de **Transação**, ver Descrição 3 e das suas subcomponentes, na Secção 4.1.3;

4. Componente de **Desassociação**, ver Descrição 4, na Secção 4.1.3. Note que os atributos removidos dizem respeito à entidade verificadora associada;

5. Componente de **Segurança da Informação:** ver Descrição Item 5, Secção 4.1.3;

6. Componente de **Comunicação:** ver Descrição 6, Secção 4.1.3. Subdivide-se nas seguintes subcomponentes:

   a) **Comunicação com a aplicação portadora:** Responsável pelo fluxo de comunicação entre a aplicação leitora e a aplicação portadora.

   b) **Comunicação com Infraestrutura da AE:** Componente responsável pelo fluxo de comunicação entre a aplicação leitora e a Infraestrutura da AE;

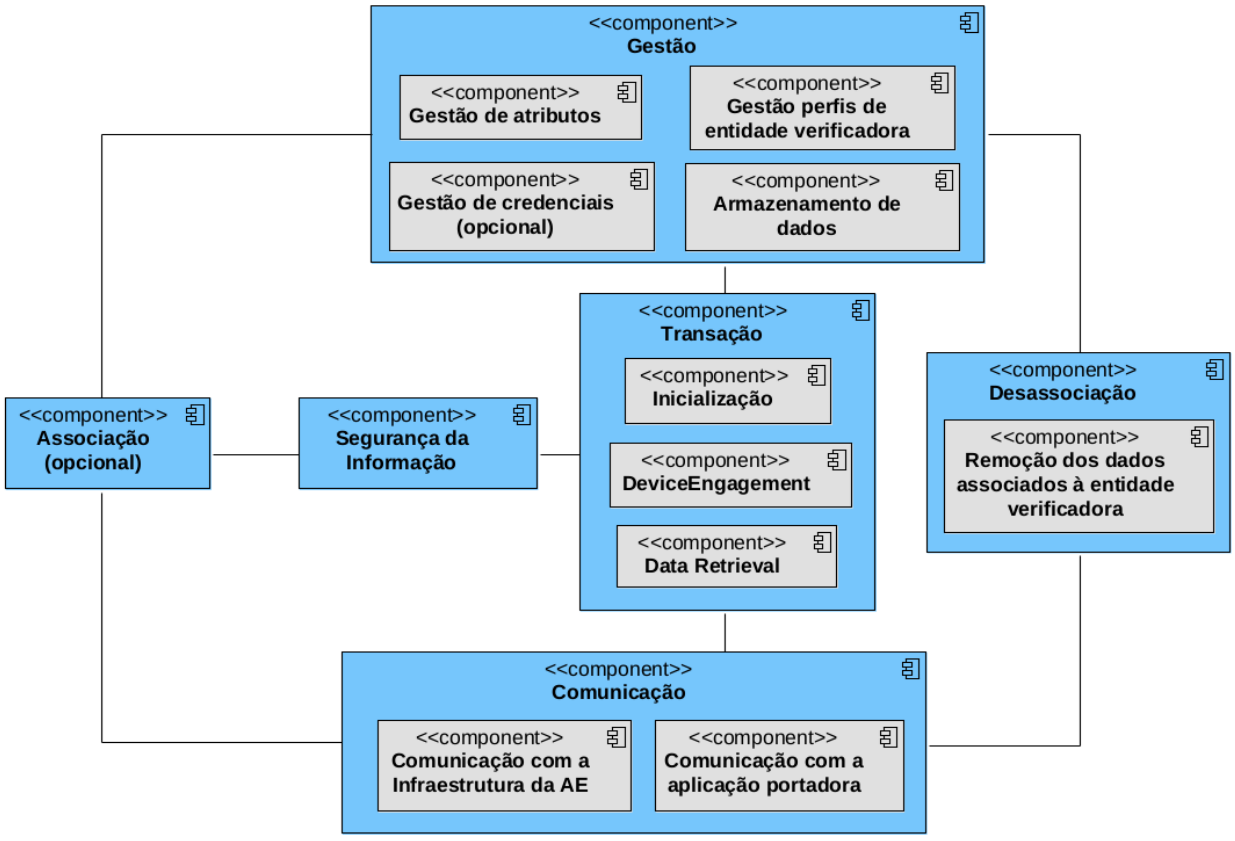

Figura 14: Diagrama de componentes da aplicação leitora

4.1.5 *Adesão de uma entidade portadora (Infraestrutura da AE)*

A fase de **Adesão** de uma entidade portadora pode ser efetuada num espaço físico pertencente à Autoridade Emissora dos dados, numa entidade devidamente reconhecida pela mesma, ou pelo próprio utilizador que pretende aderir[1]. Note que **ambas as abordagens necessitam de acesso a uma API** que permita efetuar a **comunicação com a Infraestrutura** responsável pela emissão dos dados (Infraestrutura da AE). A Figura 15 demonstra o fluxo de processos existentes durante a fase de Adesão.

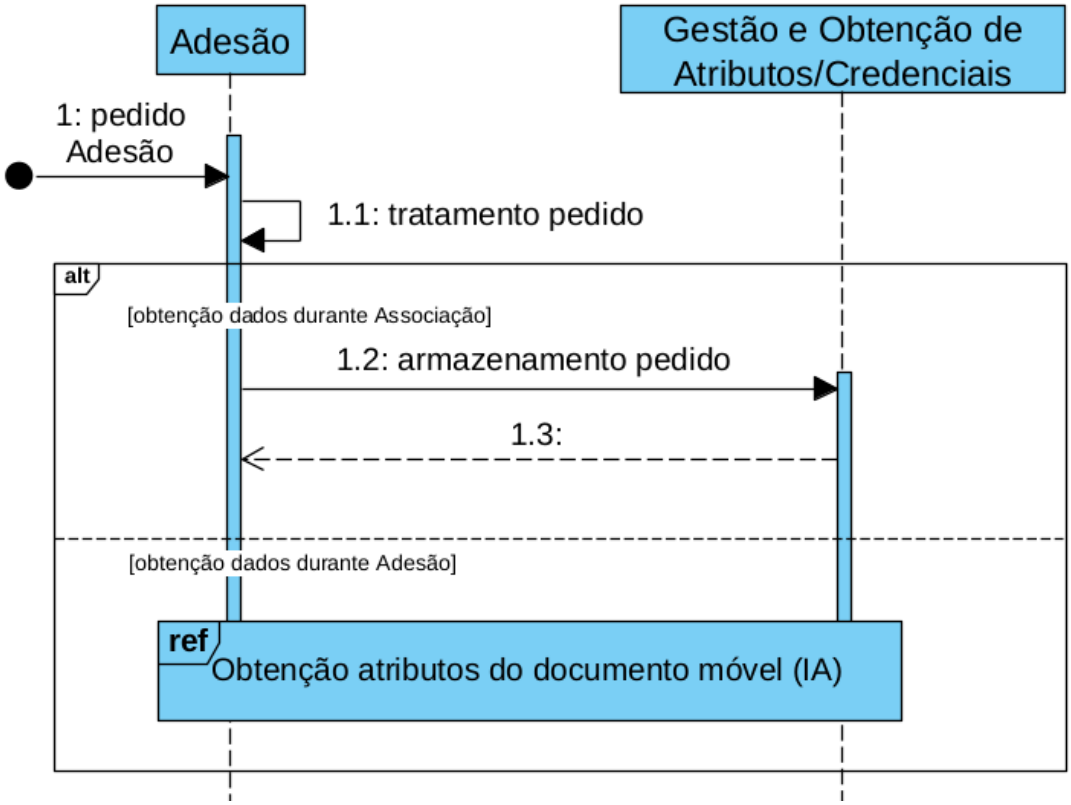

Figura 15: Diagrama de sequência do processo de Adesão de uma nova entidade portadora

Após a **verificação da ligação** entre os **atributos de identidade recolhidos** e o **novo utilizador** (ver Secção 3.3), é efetuado um **pedido de Adesão** à API da Infraestrutura da AE. A **receção e tratamento** do pedido é feito pela componente de **Adesão**.

Dependendo da implementação da Infraestrutura, a fase de **obtenção dos dados**, pode ser realizada:

1. Durante a fase de **Associação**. Neste caso o **pedido de obtenção dos dados** é **guardado na BD** da Infraestrutura da AE;
2. Na fase de **Adesão**. O fluxo de obtenção dos dados de uma nova entidade portadora encontra-se descrito na Secção 4.1.6.

1 No contexto deste trabalho, o processo de Adesão apenas será efetuado por entidades pertencentes à Autoridade Emissora dos dados.

4.1.6 *Obtenção de atributos relativos a um novo utilizador*

A Figura 16 demonstra o fluxo de interação entre as componentes definidas na Secção 4.1.1, durante o processo de obtenção dos atributos associados a uma nova entidade portadora no sistema.

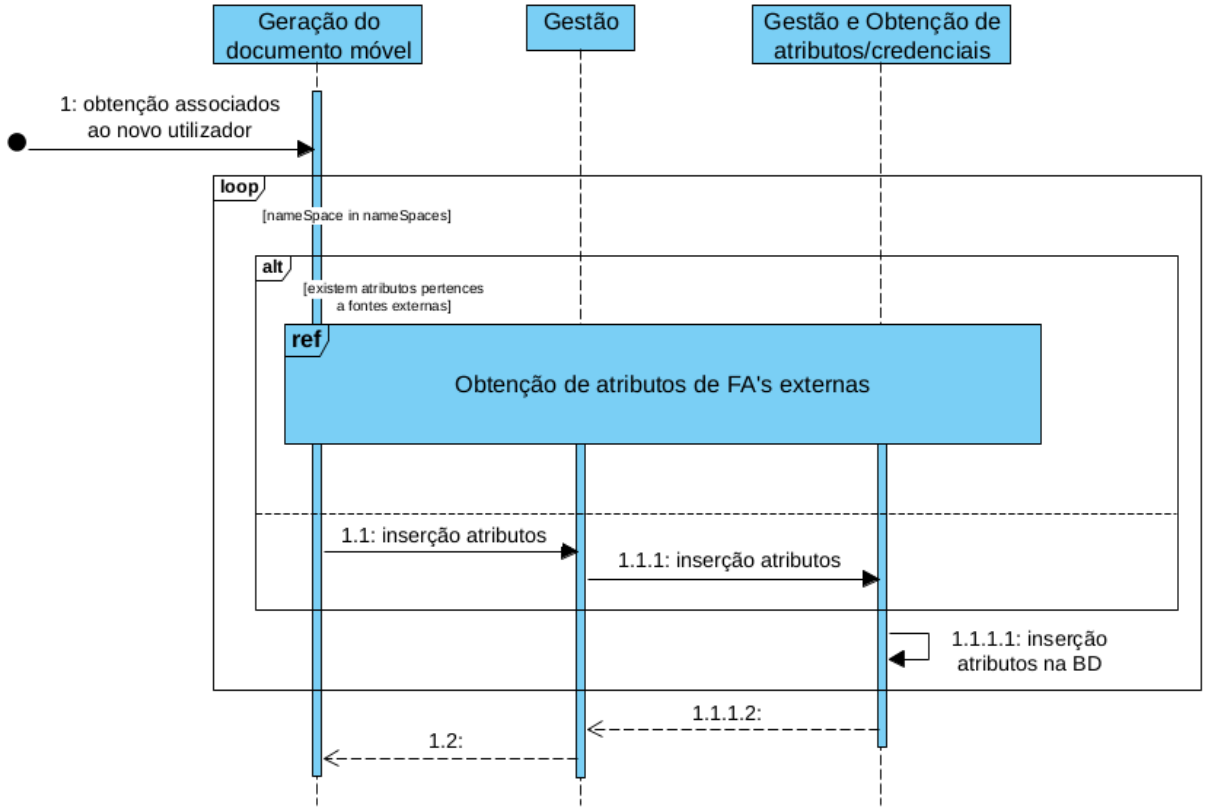

Figura 16: Diagrama de sequência do processo de obtenção dos atributos associados ao novo utilizador

O processo de Obtenção dos dados associados a um nova entidade portadora processa-se da seguinte forma:

1. Numa primeira fase, para cada *nameSpace* presente na estrutura de dados definida pela configuração do sistema, verifica-se a **existência de atributos pertencentes a fontes de atributos externas**. Esta verificação é feita na componente de **Geração do documento móvel**;

2. No caso de existirem, é necessário efetuar sua **obtenção diretamente a essas fontes** (ver Secção 4.1.6.1). Note que, no contexto deste trabalho, **para o *nameSpace*** com atributos pertencentes a fontes de atributos externas, **todo o conjunto pertence à mesma fonte de atributos**;

3. Por fim, na componente de **Gestão e Obtenção de atributos/credenciais**, faz-se a **inserção dos atributos associados a esse nameSpace na BD do sistema**.

4.1.6.1 *Obtenção de atributos de fontes de atributos externas*

Para obter um conjunto de atributos a partir de uma fonte de atributos externa, é necessário efetuar um conjunto de processos definidos no diagrama da Figura 17:

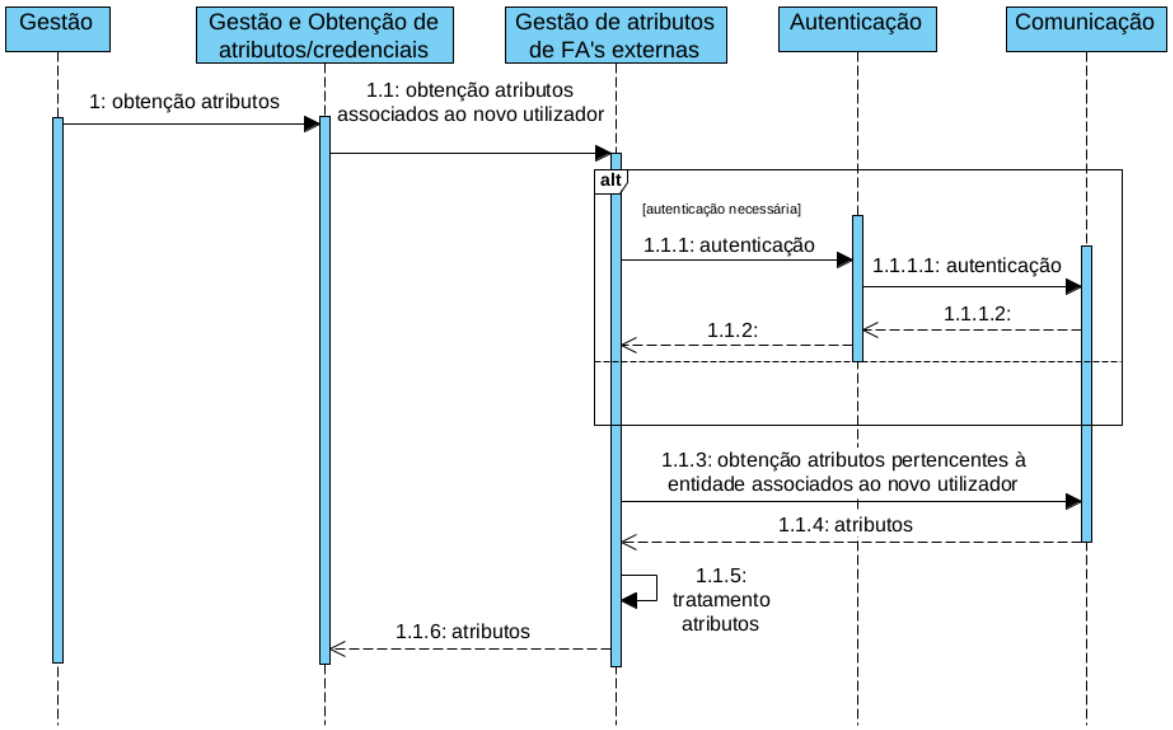

Figura 17: Diagrama de sequência do processo de obtenção dos atributos de fontes de atributos externas

1. Primeiramente, dentro da componente de **Gestão de atributos de FA's externas** verifica-se a **necessidade de obtenção de credenciais de autenticação na fonte de atributos externa**. Caso exista, é feito um **pedido à infraestrutura responsável pela emissão das respetivas credenciais**. Um exemplo desse processo é a obtenção das credenciais de autenticação através do serviço Autenticacao.gov, para a obtenção dos atributos da carta de condução portuguesa, no serviço fornecido pelo Instituto da Mobilidade e dos Transportes (IMT);

2. Posteriormente, **estabelece-se um fluxo de comunicação com a fonte de atributos externa** para a **obtenção dos atributos necessários**. O fluxo de comunicação deve ser adaptado de acordo com a API da infraestrutura onde se encontra a fonte de atributos externa;

3. De forma a existir um **reconhecimento do sistema dos atributos recebidos**, após a **receção dos atributos**, é feito um **tratamento dos mesmos**. Esse tratamento inclui a conversão de tipos dos atributos (ex. datas, números) e/ou a reestruturação da estrutura recebida numa estrutura reconhecida pela componente responsável pela inserção dos dados na BD. Para a inserção dos atributos é utilizada a componente de **Gestão e obtenção de atributos/credenciais**.

4.1.7 *Adesão de uma Entidade Verificadora (Infraestrutura da AE)*

A Figura 18 demonstra o processo de Adesão de uma entidade verificadora, após o envio do pedido de Adesão:

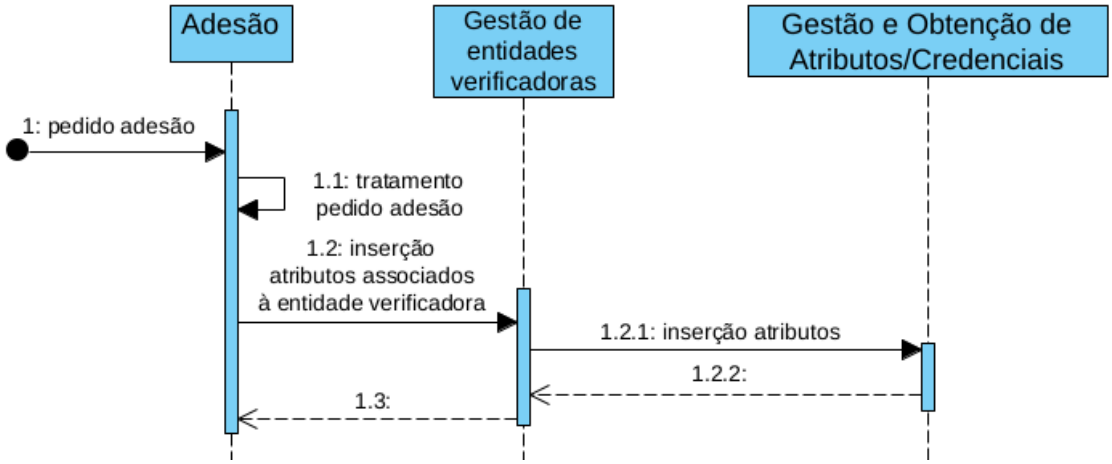

Figura 18: Diagrama de sequência do processo de Adesão de uma nova entidade verificadora

O processo de **Adesão de uma entidade verificadora** consiste no **tratamento** e **inserção dos atributos** associados à mesma na BD da Infraestrutura da AE. Note que, como foi referido no final da Secção 3.4, a fase de **Adesão** é feita pela **Organização Verificadora**. O **tratamento dos dados** recebidos é efetuado na componente de **Gestão de entidades verificadoras**. A mesma recorre à componente de **Gestão e Obtenção de Atributos/Credenciais** para a **inserção na BD** da Infraestrutura da AE.

4.1.7.1 *Mecanismos de Segurança (Adesão)*

Para a definição dos mecanismos de segurança efetuados durante o processo de Adesão é preciso considerar a entidade que efetua o pedido. Tendo em conta que a fase de Adesão é efetuada por entidades pertencentes e/ou reconhecidas pela Autoridade Emissora dos dados, no contexto deste trabalho, o mecanismo de segurança definido para esta fase é a utilização do protocolo TLS com autenticação do servidor, no fluxo de comunicação com a Infraestrutura da AE.

4.1.8 *Associação de uma Entidade Verificadora (Infraestrutura da AE)*

A Figura 19 demonstra o processo de Associação de uma entidade verificadora assim que o pedido de associação é recebido na Infraestrutura da AE:

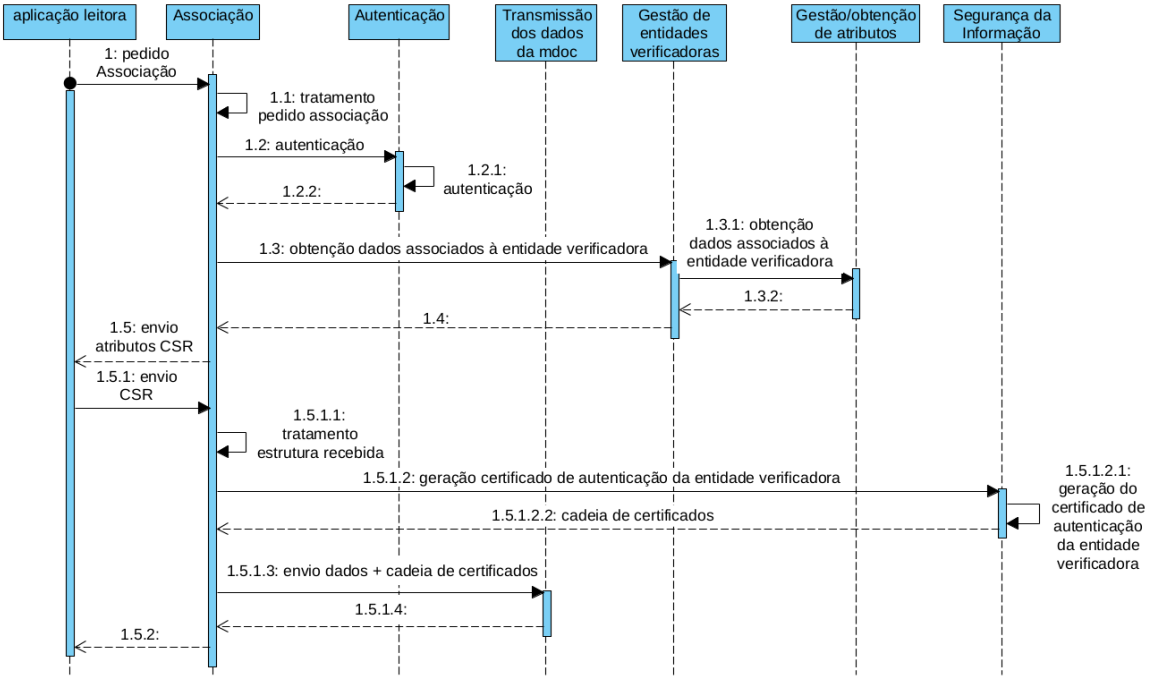

Figura 19: Diagrama de sequência do processo de Associação de uma entidade verificadora

A fase de Associação de uma entidade verificadora apresenta um conjunto de processos semelhantes à fase de Associação de uma entidade portadora, nomeadamente:

1. **Autenticação** da entidade verificadora na **Infraestrutura da AE**;
2. **Obtenção dos atributos** associados à entidade verificadora autenticada. Os atributos recolhidos podem incluir informação acerca da entidade verificadora (ver descrição das tabelas *Entity* e *Verifier* na Secção 4.1.2). Também incluem atributos necessários para a geração do Certificate Signing Request (CSR) (ver descrição das tabela *Certificate* na Secção 4.1.2);
3. A partir dos **atributos recolhidos da tabela *Certificate***, os mesmos são **enviados para a aplicação leitora**, que a utilizará para **gerar o Certificate Signing Request (CSR)**;
4. Após a **receção do CSR**, este é **enviado para a Autoridade Certificadora**, que assina a estrutura, gerando o **certificado de autenticação da entidade verificadora**. Note que a **Autoridade Certificadora retorna a cadeia de certificados** associada à Organização Verificadora, incluindo o certificado de autenticação gerado;
5. **Envio dos atributos e da cadeia de certificados** para a aplicação leitora.

4.1.9 *Associação de uma entidade verificadora (aplicação leitora)*

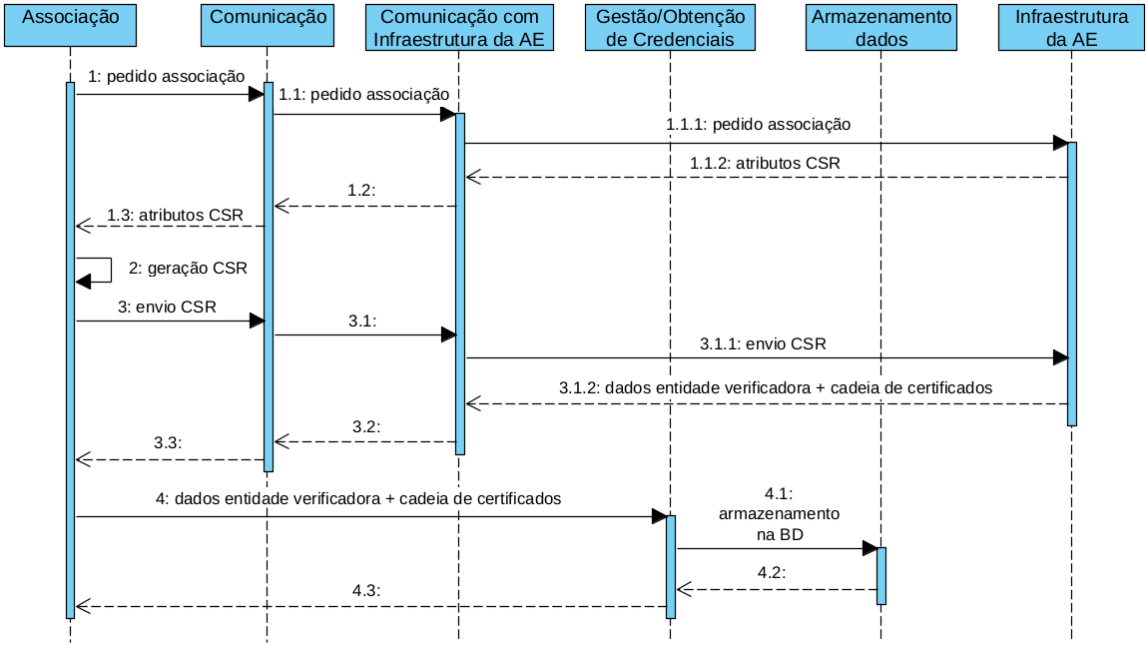

Figura 20: Diagrama de sequência do processo de Associação de uma Entidade Verificadora na aplicação leitora

Na aplicação leitora a fase de Associação apresenta as seguintes sub-fases, presentes na Figura 20:

- **Criação** do **pedido de Associação** com as credenciais de autenticação;
- **Envio** do **pedido de Associação** para a Infraestrutura da AE;
- **Receção e tratamento** da estrutura com os atributos a serem inseridos em cada um dos parâmetros do CSR e um *token* de autenticação no sistema;
- **Geração** e **envio** do CSR para a Intraestrutura da AE;
- **Receção, tratamento da resposta e armazenamento** dos dados associados à entidade verificadora e da respetiva cadeia de certificados.

4.1.10 *Associação de uma entidade portadora (Infraestrutura da AE)*

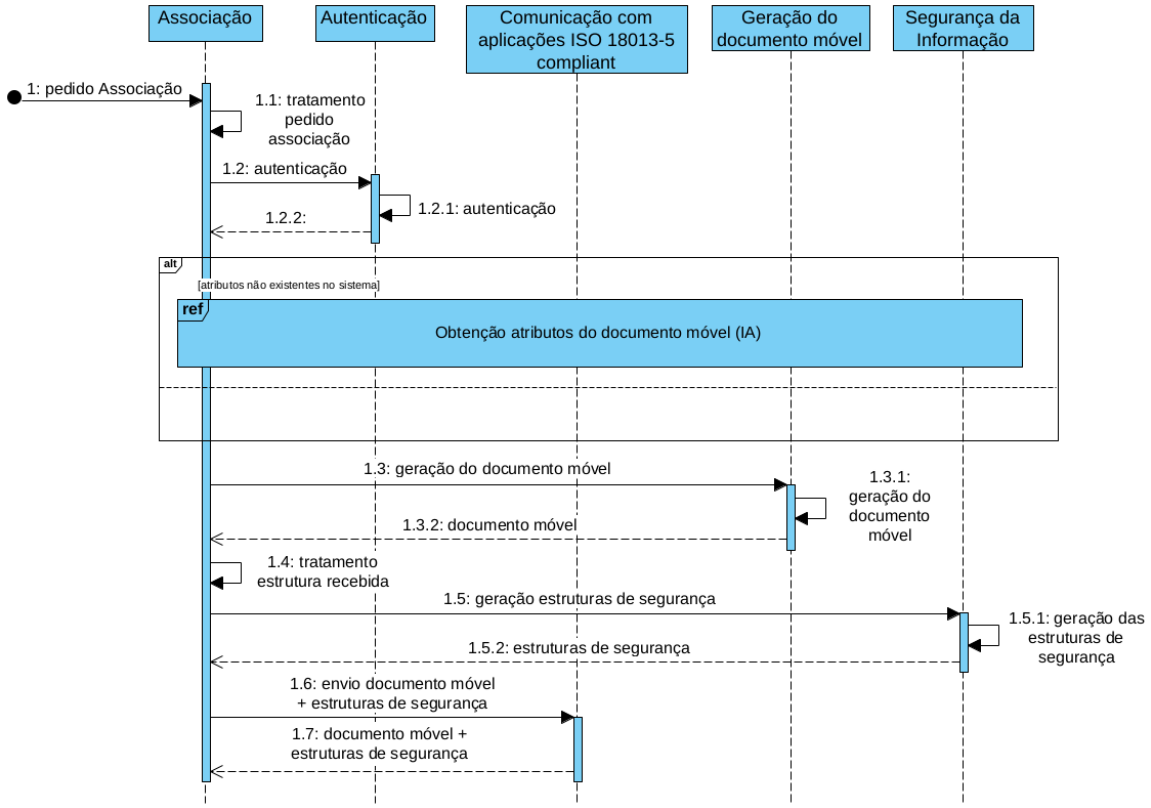

Figura 21: Diagrama de sequência do processo de Associação de uma entidade portadora

Para o processo de Associação de uma entidade portadora, numa fase inicial, dentro da componente de **Autenticação**, efetua-se o processo de **autenticação na Infraestrutura da AE**. Posteriormente, na componente de **Associação**, verifica-se a **existência dos atributos necessários para a geração do documento móvel**.

1. Caso não existam, é feita a **obtenção** e **armazenamento** dos **atributos** localmente (ver Secção 4.1.6);
2. Já no caso de todos os atributos existirem localmente, a **estrutura do documento móvel é gerada**.

Após a sua formação, são **geradas as estruturas de segurança** essenciais para garantir os princípios de segurança da informação definidos ao longo da Secção 3.3.4. No caso da aplicação portadora, as estruturas de segurança geradas são **o MSO e o certificado de assinatura do MSO**.

Posteriormente, as **estruturas geradas** são **enviadas para a aplicação portadora**. As **estruturas recebidas nas aplicações**, são **armazenamenadas** na base de dados local do dispositivo. Preferencialmente, o armazenamento local dos dados deverá ser protegido através da utilização de bases de dados encriptadas, como é o caso da *KeyStore* em dispositivos móveis Android e a *Secure Enclave* para dispositivos móveis iOS (ver Secção 3.3).

4.1.11 *Associação de uma Entidade Portadora (aplicação portadora)*

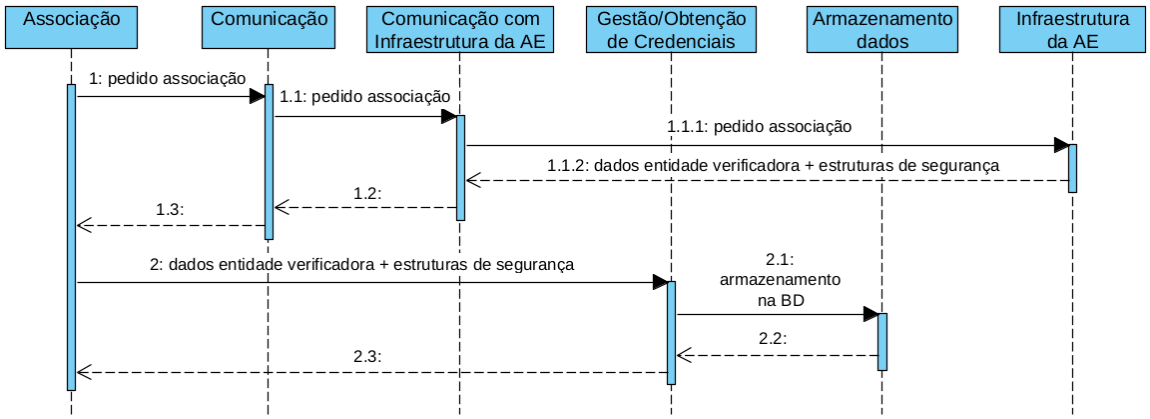

Figura 22: Diagrama de sequência do processo de Associação de uma Entidade Portadora na aplicação portadora

À semelhança do processo efetuado na aplicação leitora, o processo de Associação de uma entidade portadora na aplicação portadora apresenta as mesmas subfases. Apenas difere na resposta ao pedido de Associação, que neste caso corresponde ao documento móvel e às estruturas de segurança definidas pela norma para a entidade portadora (MSO e o certificado de assinatura do MSO).

4.1.11.1 *Mecanismos de Segurança (Associação)*

Para a fase de Associação é necessário definir os seguintes mecanismos de segurança para a aplicação portadora:

1. A utilização de um **protocolo de comunicação entre a aplicação portadora e a Infraestrutura da AE**. Para isso, tendo em conta que a Infraestrutura da AE utiliza o protocolo TLS para a comunicação segura com a aplicação leitora, o mesmo protocolo é utilizado para a comunicação entre a aplicação portadora e a Infraestrutura da AE;

2. Criação de uma **estrutura de segurança** utilizada para **estabelecer a relação entre o dispositivo móvel associado e o documento móvel emitido**, durante a fase de Associação. Nesse sentido, durante a fase de Associação de uma entidade portadora definem-se os seguintes processos:

    a) Geração na aplicação portadora de um **par de chaves de assinatura assimétricas**, designadas por **chaves de associação**. Note que o mesmo par de chaves também é utilizado para autenticar os dados gerados e enviados pela aplicação portadora (ver *mdoc authentication*, Secção 3.3.4);

    b) **Envio da chave pública**, junto com as **credenciais de autenticação** para a Infraestrutura da AE;

    c) **Verificação das credenciais de autenticação**;

    d) **Armazenamento da chave pública de associação** na BD da Infraestrutura da AE;

e) **Obtenção do documento móvel** e **geração das estruturas de segurança** (MSO e certificado de assinatura do documento móvel);

f) **Envio dos dados e das estruturas de segurança** para a aplicação portadora.

No caso da **aplicação leitora**, **não é necessário definir os mecanismos de segurança**, uma vez que o protocolo de comunicação com a Infraestrutura da AE, bem como a estrutura de segurança emitida (certificado de autenticação da entidade verificadora ou *mdoc reader authentication certificate*) já se encontram definidos pela norma técnica ISO/IEC DIS 18013-5. No entanto **é necessário definir o fluxo de comunicação com a Infraestrutura da AE**. A descrição do fluxo de Associação de uma entidade verificadora encontra-se nas Secções 4.1.8 e 4.1.9.

4.1.12 *Transação dos dados*

4.1.12.1 *Inicialização e Estabelecimento da conexão*

Para os fluxos de Inicialização e Estabelecimento da conexão, descritos na Secção 3.3.4, foram definidos os diagramas de sequência presentes nas Figuras 24 e 23:

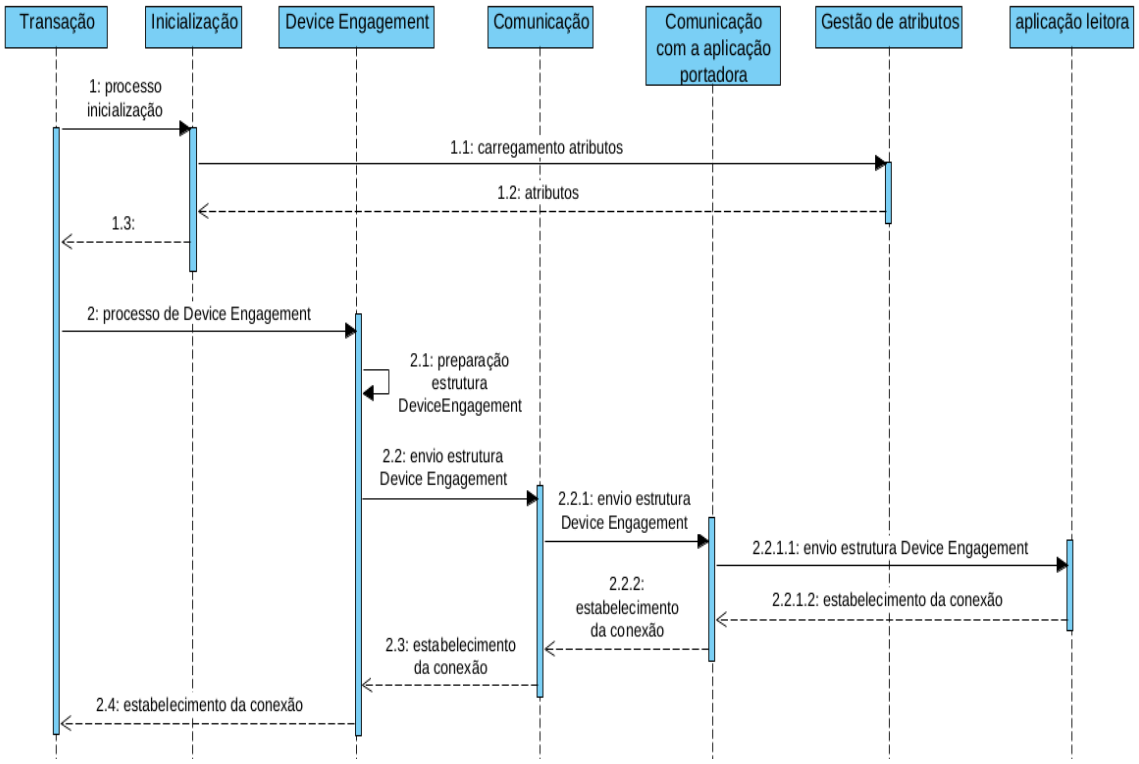

Figura 23: Diagrama de sequência da fase de Estabelecimento da conexão, na aplicação portadora

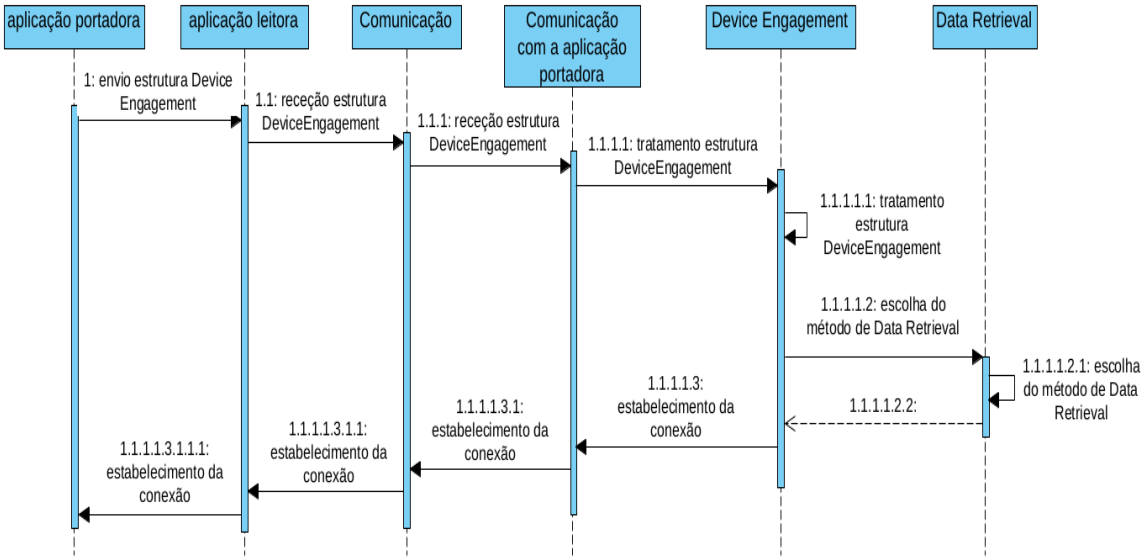

Figura 24: Diagrama de sequência da fase de Estabelecimento da conexão, na aplicação leitora

Existem quatro processos a se destacarem:

1. **Carregamento do documento móvel** e das **estruturas de segurança para memória** na aplicação portadora;
2. **Geração da estrutura DeviceEngagement** na aplicação portadora e **envio** da estrutura para a aplicação leitora;
3. **Receção e tratamento** da estrutura DeviceEngagement na aplicação leitora;
4. **Escolha do método de Obtenção de dados** na aplicação leitora.

4.1.12.2 *Obtenção dos dados*

No que diz respeito ao fluxo de Obtenção dos dados foram definidos os diagramas de sequência presentes nas Figuras 25 e 26:

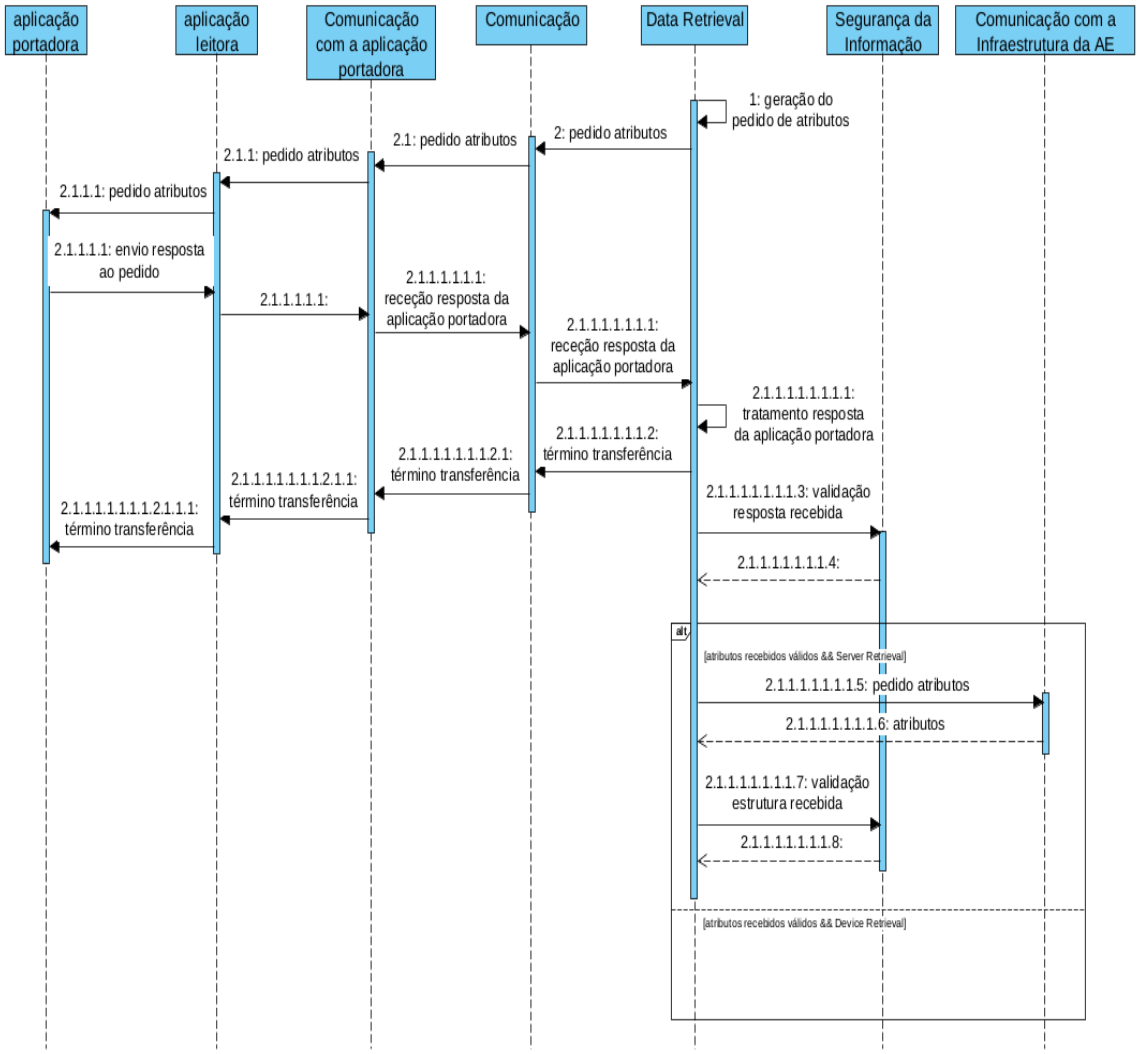

Figura 25: Diagrama de sequência da fase de Obtenção dos dados, na aplicação leitora

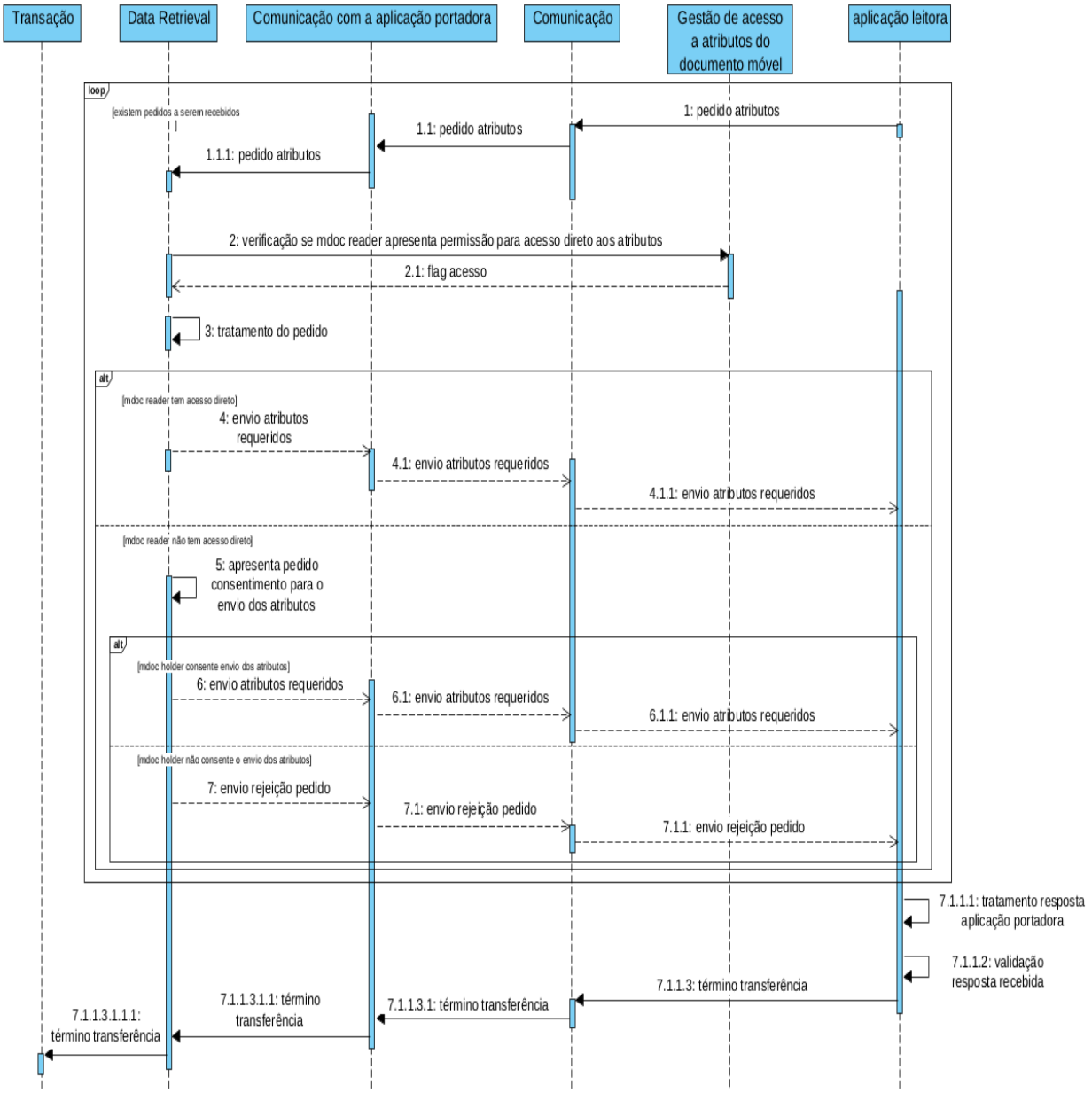

Figura 26: Diagrama de sequência da fase de Obtenção dos dados, na aplicação portadora

Os diagramas encontram-se divididos em três processos:

- **Geração e envio** do **pedido de atributos** (ver fluxos 1 a 2.1.1.1 na Figura 25);
- **Receção e tratamento do pedido de atributos** (ver fluxos 1 a 3 na Figura 26);
- **Geração e envio dos atributos requeridos** e das **estruturas de segurança** descritos ao longo na Secção 3.3.4 (ver fluxos 3 a 7.1.1.3.1.1.1 na Figura 26);
- **Receção, tratamento e validação das estruturas recebidas** (a partir do fluxo 2.1.1.1.1, na Figura 25);

4.2 SUMÁRIO DO CAPÍTULO

O Capítulo 4 apresenta a proposta de arquitetura de um sistema de identificação móvel baseado na norma técnica ISO/IEC DIS 18013-5. A proposta de arquitetura está dividida em diagramas com componentes necessárias à implementação de cada uma das entidades estabelecidas pela norma técnica ISO/IEC DIS 18013-5. Importante referir que as componentes descritas, a nível de implementação, podem corresponder a classes, métodos, a módulos e/ou bibliotecas importadas.

De forma a perceber o fluxo de interação entre as componentes definidas definiram-se diagramas de sequência, descritos na segunda parte deste Capítulo.

5

PROVA DE CONCEITO DO CARTÃO DE ESTUDANTE DA UNIVERSIDADE DO MINHO

No sentido de apresentar uma demonstração de um sistema de identificação móvel, baseado na arquitetura proposta no Capítulo 4, considera-se o exemplo do Cartão de Estudante da Universidade do Minho[1]. Este cartão permite ao seu portador, o acesso a serviços como reserva de espaços, reserva de livros, e a refeições na cantina universitária. Importante referir que o ponto comum entre estes serviços é a necessidade do indivíduo portador (ou entidade portadora) se identificar perante um funcionário da instituição (ou entidade verificadora). O desenvolvimento da Prova de Conceito, numa primeira fase, parte da implementação um sistema de identificação configurável. A descrição do seu desenvolvimento e da configuração do sistema, encontra-se na Secção 5.1.

5.1 DESENVOLVIMENTO E CONFIGURAÇÃO DO SISTEMA

Partindo da arquitetura definida na norma técnica ISO/IEC DIS 18013-5, o desenvolvimento do sistema de identificação configurável divide-se em três fases, correspondentes ao desenvolvimento da Infraestrutura da AE, da aplicação portadora, e da aplicação leitora, respetivamente.

Note que, para cada entidade presente na arquitetura, existe um ficheiro de configuração associado. As Secções 5.1.1 e 5.1.2, apresentam a modelação de cada uma das entidades, com base na arquitetura definida no Capítulo 4, bem como os parâmetros existentes em cada um dos ficheiros de configuração.

5.1.1 *Infraestrutura da AE*

No desenvolvimento da Infraestrutura da AE, para cada camada aplicacional, escolheram-se as seguintes ferramentas:

- Como ferramenta de desenvolvimento da **Camada de Dados** foi utilizado o SGBD *PostgreSQL*. Esta ferramenta foi escolhida principalmente pela sua estabilidade e performance. Outro aspeto determinante

1 Este exemplo surge do projeto realizado na unidade curricular de Projeto de Engenharia Informática. O relatório técnico do projeto encontra-se disponível para visualização em https://docs.google.com/document/d/17zHkmiAqlb2jIl18UqJlOjlQxEkG21ct6Zyo5UCtMQU/edit?usp=sharing

para a escolha do *PostgreSQL* é a grande comunidade de desenvolvimento e suporte existente, pois este SGBD é de código aberto;

- Para a **Camada de Negócio**, é utilizada a framework Django. O Django é uma *framework* Python de desenvolvimento de aplicações *web*. Baseada no padrão arquitetural Model-View-Controller (MVC), esta *framework* destaca-se pela sua simplicidade e rapidez na criação de serviços *web* complexos[2].

- A framework Django contém um conjunto de vistas definidas para a gestão do sistema (mais conhecidas por paineis de administração do Django). Uma vez que se está a implementar uma Prova de Conceito, em que os utilizadores finais (entidade portadora e entidade leitora) não comunicam diretamente com a Infraestrutura da AE, na **Camada de Apresentação**, são utilizadas as vistas já fornecidas pela *framework*;

A Infraestrutura de Chave Pública (PKI) foi desenvolvida através da ferramenta Vault, por permitir a criação de um serviço, em que a gestão da PKI se encontra automatizada. Para a automatização da gestão da PKI é utilizada a ferramenta Terraform.

A Infraestrutura da AE está dividida em três serviços, que comunicam entre si através de API's internas:

- **mdoc_provider:** responsável pela gestão dos atributos associados ao documento móvel. Também é responsável pela fase de Adesão das entidades portadoras;

- **mdoc_readers:** serviço responsável pela gestão das organizações verificadoras e respetivas entidades verificadoras. Também é responsável pela fase de Adesão das entidades verificadoras;

- **mdoc_core:** gestão das fases do ciclo de vida de um documento móvel (exceto a fase de Adesão), em que a Infraestrutura da AE é responsável.

Estes serviços recorrem aos métodos implementados pelo módulo **mdoc_management**. A Figura 27 apresenta o diagrama de classes utilizado pelo módulo *mdoc_management*, definido de acordo com o diagrama de componentes apresentado na Secção 4.1.1:

2 Para mais informações acerca da framework Django, consultar: https://developer.mozilla.org/en-US/docs/Learn/Server-side/Django/Introduction

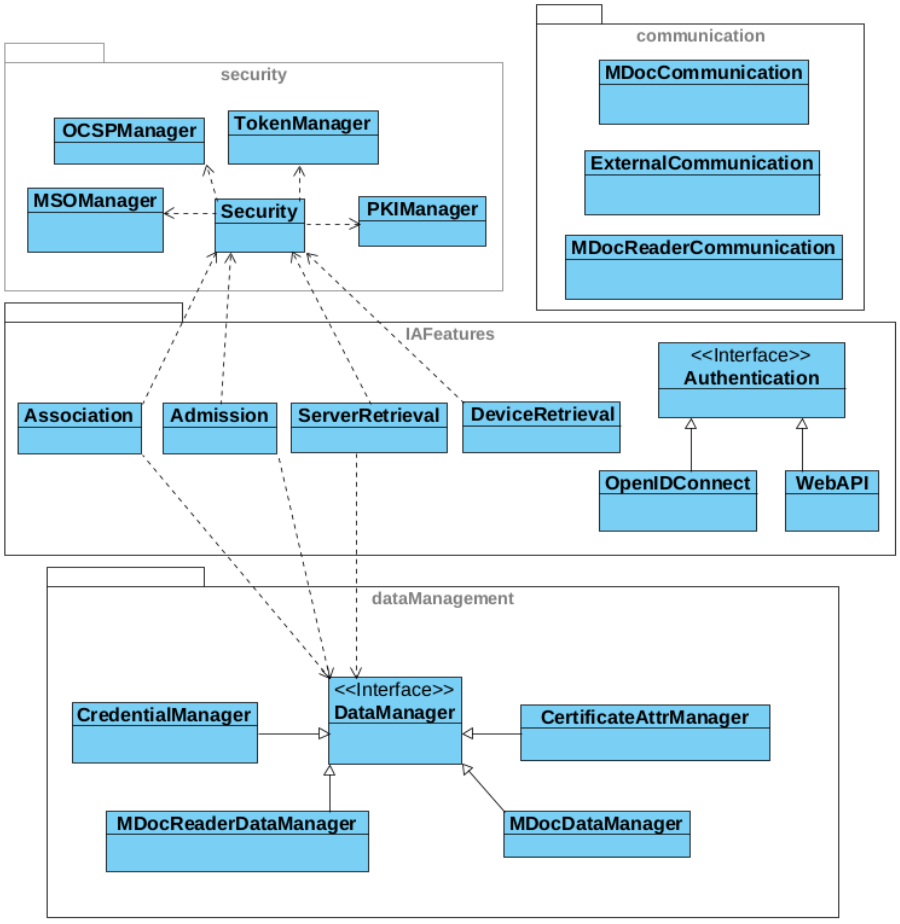

Figura 27: Diagrama de classes utilizado pelo módulo *mdoc_management*

Definiram-se quatro pacotes (ou *packages*), nas quais:

- O pacote **IAFeatures**, contém classes responsáveis pela gestão das fases do ciclo de vida de um documento móvel (ver Secção 3.3):

  SERVERRETRIEVAL: Gestão do processo de obtenção de dados, via *Server Retrieval* (ver Secção 3.3.4.2);

  ASSOCIATION: Gestão do processo de Associação de uma entidade verificadora ou de uma entidade portadora na Infraestrutura da AE;

  ENROLLMENT: Gestão do processo de Adesão de uma nova entidade portadora ou verificadora na Infraestrutura da AE;

  DEVICERETRIEVAL: Gestão do processo de obtenção de dados, via *Device Retrieval* (ver Secção 3.3.4.2), mais especificamente na comunicação com o servidor OCSP, no caso de existir conetividade entre a aplicação leitora e a Infraestrutura da AE. Este processo é utilizado, por parte da aplicação leitora, para a validação do certificado de assinatura do MSO (ver *Issuer Data Authentication*, Secção 3.3.4);

AUTHENTICATION: Interface responsável pelo processo de autenticação na Infraestrutura da AE;

OPENIDCONNECT: Gestão do processo de autenticação, através do protocolo *OpenID Connect*;

WEBAPI: Gestão do processo de autenticação, através da utilização de protocolos tradicionais de autenticação num servidor web;

- O pacote **security**, com classes responsáveis pelos mecanismos de segurança definidos nas Secções 3.3.4, 4.1.7.1 e 4.1.11.1:

SECURITY: Classe intermédia, responsável pela invocação dos métodos de verificação, validação e obtenção de estruturas de segurança, necessários no contexto da Infraestrutura da AE;

MSOMANAGER: Geração da estrutura do Mobile Security Object (MSO) (ver Secção 3.3.3);

PKIMANAGER: Comunicação com a PKI;

TOKENMANAGER: Geração e validação de *tokens* do tipo JWT;

OCSPMANAGER: Comunicação com o servidor OCSP.

- O pacote **dataManagement**, que contém classes responsáveis pela gestão dos dados associados a uma Infraestrutura de gestão de documentos móveis de identificação:

DATAMANAGER: Interface com métodos responsáveis pela gestão dos atributos presentes na base de dados da Infraestrutura da AE;

MDOCREADERDATAMANAGER: Gestão dos atributos associados à entidade verificadora;

MDOCDATAMANAGER: Gestão dos atributos associados ao documento móvel;

CERTIFICATEATTRMANAGER: Gestão dos atributos presentes nos certificados definidos pela norma técnica ISO/IEC DIS 18013-5 (ver descrição da tabela *Certificate* na Secção 4.1.2);

CREDENTIALMANAGER: Gestão das credenciais de autenticação no sistema;

- Por fim, o pacote **communication**, responsável pela comunicação com entidades remotas:

MDOCREADERCOMMUNICATION/MDOCCOMMUNICATION: Gestão do fluxo de comunicação com a aplicação leitora e portadora, respetivamente. Estas classes são necessárias para o processo de Associação e de Desassociação de cada uma das entidades (ver diagramas de sequência da fase de Associação, nas Secções 4.1.10 e 4.1.8);

EXTERNALCOMMUNICATION: Gestão do fluxo de comunicação com entidades terceiras. Note que esta classe não se encontra implementada, uma vez que, no contexto da Prova de Conceito, não existe comunicação com entidades terceiras.

5.1.2 *Aplicações portadora e leitora*

Para o desenvolvimento das aplicações móveis, existem duas formas de desenvolvimento, através de uma *framework* híbrida de desenvolvimento de aplicações móveis, ou através da utilização de ferramentas de desenvolvimento nativo de aplicações móveis. Note que a utilização de ferramentas híbridas é aconselhável, especialmente para a implementação de um Produto Mínimo Viável (MVP) e/ou de uma Prova de Conceito. Isto, uma vez que o desenvolvimento das aplicações parte apenas de um código fonte, o que permite uma gestão mais simples de alterações no código, na testagem das funcionalidades, etc. Assim, no contexto desta Prova de Conceito, foi utilizada uma *framework* híbrida de desenvolvimento.

Para a escolha da *framework* híbrida, existem pontos a considerar:

1. Existência de uma grande comunidade de suporte à *framework*;
2. Existência de bibliotecas/*plugins* que suportem as especificações técnicas definidas nos Capítulos 3 e 4, para o desenvolvimento das aplicações portadora e leitora.

Considerando o ponto 1, existem quatro *frameworks* híbridas de desenvolvimento a considerar, Ionic, React Native, Xamarin, e o Flutter.

Por sua vez, tendo em conta o ponto 2, após a análise das bibliotecas disponibilizadas por cada *framework*, é possível concluir que não existe uma ferramenta de desenvolvimento híbrida que disponibilize todos os *plugins* de suporte necessários. Nesse sentido, tendo em conta as bibliotecas disponibilizadas por cada *framework*, o Ionic é a ferramenta que apresenta um conjunto de bibliotecas que satisfazem a maioria dos requisitos técnicos, especialmente a nível das tecnologias de transporte utilizadas durante a fase de transação de dados (ver Secção 3.3.4).

O Ionic é uma *framework* de desenvolvimento híbrido de aplicações móveis baseado em tecnologias de desenvolvimento *web* bem conhecidas, como o Vue, React, e Angular[3]. Para a Prova de Conceito, as aplicações portadora e leitora foram desenvolvidas através do Ionic Angular.

Tendo em conta os diagramas de componentes definidos nas Secções 4.1.3 e 4.1.4, definiu-se o diagrama de classes presente na Figura 28. Note que existem classes que se encontram definidas para satisfazer os requisitos específicos do SO no qual se está a desenvolver a aplicação móvel (por exemplo, a classe DozeMode é necessária para desativar o modo "poupança de bateria" no Android). Assim, dependendo do SO em que se estiver a desenvolver a aplicação, esta classe não é necessária.

3 Para mais informações acerca da framework Ionic, consultar: `https://ionicframework.com/`

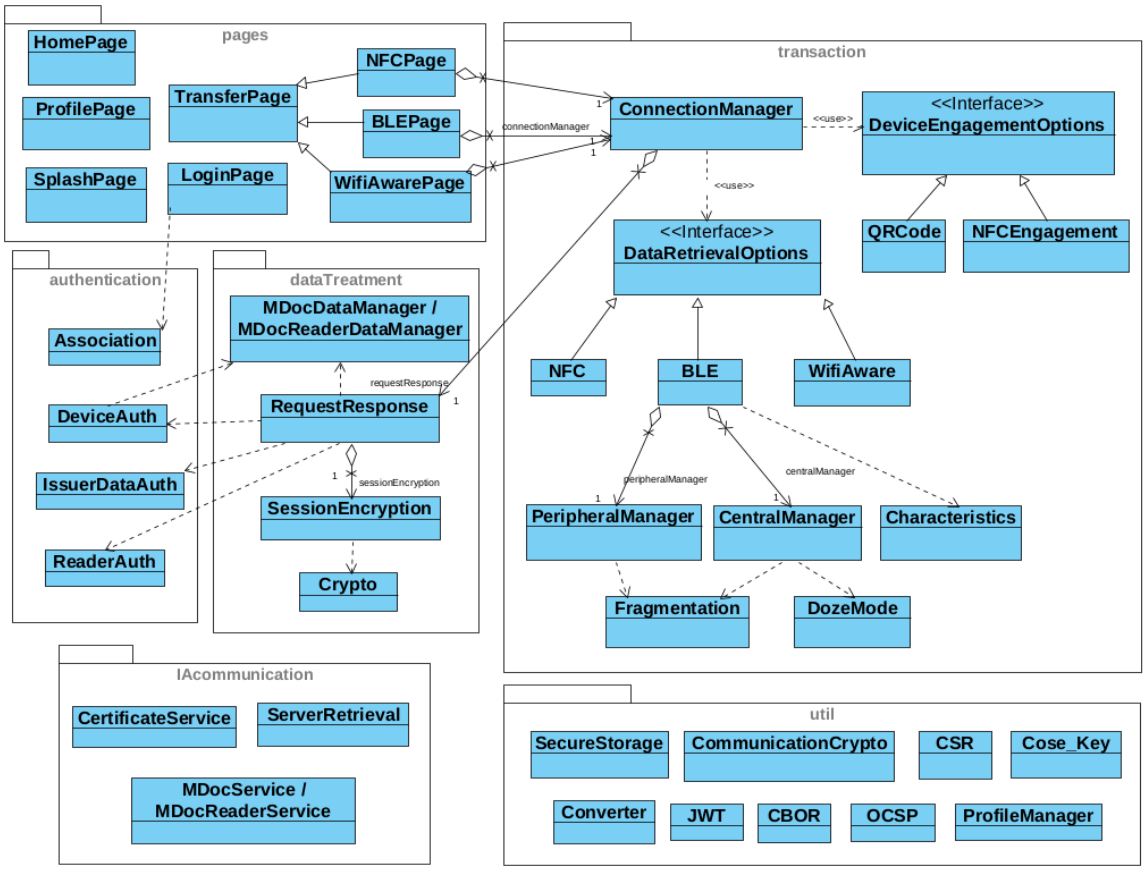

Figura 28: Diagrama de classes definido para as aplicações móveis

Existem seis pacotes (ou *packages*), entre os quais:

- Um pacote com todas as classes, responsáveis pela gestão da camada de apresentação das aplicações móveis (**pages**). De referir que na camada de apresentação, o *Ionic Angular* utiliza páginas para apresentar uma vista na aplicação. Uma página é uma componente *Angular* definida pelo *Ionic* para representar uma vista na aplicação (Team, 2022). Uma página pode conter um conjunto de componentes *Angular*, que podem ser reutilizados por páginas *Ionic* diferentes. Do ponto de vista da modulação do diagrama de classes, tanto as páginas como as componentes correspondem a classes UML. Nesse sentido, dentro do pacote pages, existem as seguintes classes:

  SPLASHPAGE: página de abertura das aplicações;

  LOGINPAGE: página de visualização do processo de Associação na aplicação;

  HOMEPAGE: página principal das aplicações;

  PROFILEPAGE: página de gestão dos perfis de entidade verificadora (ver definição de perfil de entidade verificadora, Item 1d Secção 4.1.1). Classe pertencente à aplicação leitora;

  TRANSFERPAGE: página de visualização do processo de transação dos dados (ver Secção 3.3.4). Dependendo do tipo de tecnologia de comunicação ponto-a-ponto utilizada para efetuar a gestão

do processo de *Data Retrieval* (ver Secção 3.3.4.2), esta classe recorre a três subclasses, correspondentes a componentes Angular.

BLEPAGE: Obtenção dos dados, via Bluetooth Low Energy (BLE);

NFCPAGE: Obtenção dos dados, via Near Field Communication (NFC);

WIFIAWAREPAGE: Obtenção dos dados, via WiFi Aware.

- Um pacote composto pelas classes responsáveis pela componente funcional do processo de transação dos dados entre a aplicação portadora e a aplicação leitora, como descrito na Secção 3.3.4 (**transaction**).

CONNECTIONMANAGER: Classe responsável pela gestão do fluxo de transação de dados entre a aplicação portadora e a aplicação leitora (ver Secção 3.3.4);

DEVICEENGAGEMENTOPTIONS: Interface responsável pela gestão do processo de *Device Engagement*;

QRCODE: Estabelecimento da conexão, via QR Code;

NFCENGAGEMENT: Estabelecimento da conexão, via NFC;

DATARETRIEVALOPTIONS: Interface responsável pela gestão do fluxo de Data Retrieval;

NFC: Obtenção dos dados, via NFC;

WIFIAWARE: Obtenção dos dados, via WiFi Aware;

BLE: Obtenção dos dados, via BLE. Esta classe recorre a classes específicas necessárias para a fase de Obtenção dos dados, via BLE (ver Anexo A.1):

PERIPHERALMANAGER: Gestão do fluxo de Obtenção dos dados, no caso de o dispositivo local atuar no modo periférico (ver Anexo A.1).

CENTRALMANAGER: Gestão do fluxo de Obtenção dos dados, no caso de o dispositivo local atuar no modo central;

CHARACTERISTICS: Classe auxiliar, que contém as características determinadas pela norma técnica ISO/IEC DIS 18013-5, onde o dispositivo local deve ler a informação recebida ou escrever informação para o dispositivo remoto. Estas características apenas são válidas para a transferência via BLE (ver Anexo A.1).

- O pacote **IAcommunication** contém um conjunto de classes responsáveis pelo fluxo de comunicação com a Infraestrutura da AE, em diferentes fases do ciclo de vida de um documento móvel:

CERTIFICATESERVICE: Obtenção dos certificados x509v3, necessários para a verificação dos mecanismos de segurança definidos pela norma técnica ISO/IEC DIS 18013-5;

SERVERRETRIEVAL: Obtenção dos atributos requeridos e das estruturas de segurança, via *Server Retrieval* (ver Secção 3.3.4);

MDOCSERVICE/MDOCREADERSERVICE: Obtenção dos dados associados à entidade portadora e a entidade verificadora da Infraestrutura da AE. Esta obtenção pode ser efetuada na fase de Associação, ou durante a atualização dos dados da entidade (portadora ou verificadora).

- Um conjunto de classes relacionadas com os mecanismos de autenticação dos dados, previstos pela norma técnica ISO/IEC DIS 18013-5, bem como pelo processo de Associação na Infraestrutura da AE (**authentication**):

  ASSOCIATION: Classe responsável pelo fluxo de Associação na Infraestrutura da AE;

  DEVICEAUTH: Autenticação dos dados gerados na aplicação portadora (ver *mdoc authentication*, Secção 3.3.4);

  ISSUERDATAAUTH: Autenticação dos dados emitidos pela Infraestrutura da AE (ver *Issuer Data Authentication*, Secção 3.3.4);

  READERAUTH: Autenticação dos dados gerados pela aplicação leitora (ver *mdoc reader authentication*, Secção 3.3.4);

- O pacote **util**, abrange todas as classes que contenham métodos auxiliares regularmente utilizados na aplicação:

  SECURESTORAGE: Classe composta por métodos necessários para o acesso à base de dados local do dispositivo;

  JWT: Classe pertencente à aplicação portadora. É responsável pela geração do *token* necessário para a obtenção dos dados via Server Retrieval;

  CBORCONVERTER: Codificação e descodificação de dados em formato CBOR;

  COSE_KEY: Conversão de chaves no formato JWK em formato Cose_Key e vice-versa;

  PROFILEMANAGER: Classe pertencente à aplicação leitora. Contém métodos auxiliares na construção de perfis de entidades verificadoras diferentes, de acordo com os atributos que são acessíveis por esse perfil (ver definição de perfil de entidade verificadora, Item 1d Secção 4.1.1);

  COMMUNICATIONCRYPTO: Classe com métodos auxiliares, utilizados na implementação dos vários mecanismos de segurança, definidos pela norma técnica ISO/IEC DIS 18013-5;

  CSR: Classe pertencente à aplicação leitora. É responsável pela criação de um Certificate Signing Request (CSR) a ser enviado para a Infraestrutura da AE;

  CERTIFICATEVALIDATOR: Verificação da validade de certificados x509v3, via protocolo OCSP.

- Por último, o pacote **dataTreatment** contém classes responsáveis pelo tratamento dos dados trocados entre a aplicação portadora e a aplicação leitora:

  REQUESTRESPONSE: Classe responsável pelo tratamento dos dados provenientes do dispositivo externo conectado, bem como pela geração da resposta a ser enviada. Note que o tratamento dos dados difere, dependendo da aplicação que se está a implementar. No caso da aplicação portadora esta classe é responsável pela:

  1. Receção e tratamento do pedido de atributos proveniente da aplicação leitora (ver estrutura *"DeviceRequest"* no documento da norma técnica ISO/IEC DIS 18013-5);
  2. Criação da estrutura de resposta ao pedido da aplicação leitora, de acordo com consentimento da entidade portadora (ver estrutura *"DeviceResponse"* no documento da norma técnica ISO/IEC DIS 18013-5).

  Já no caso da aplicação leitora, é responsável pela:

  1. Criação da estrutura, com o respetivo pedido de atributos, a ser enviada para a aplicação portadora (ver estrutura *"DeviceRequest"* no documento da norma técnica ISO/IEC DIS 18013-5);
  2. Receção e tratamento da resposta da aplicação portadora ao pedido de atributos (ver estrutura *"DeviceResponse"* no documento da norma técnica ISO/IEC DIS 18013-5).

  A classe RequestResponse recorre às seguintes classes:

MDOCREADERDATAMANAGER/MDOCDATAMANAGER:	Gestão dos dados e estruturas de segurança associadas à entidade verificadora ou à entidade portadora, respetivamente;
SESSIONENCRYPTION:	Classe composta por métodos responsáveis pelo estabelecimento de uma sessão segura de transferência ponto a ponto entre a aplicação leitora e a aplicação portadora (ver *Session Encryption*, Secção 3.3.4);
CRYPTO:	Contém métodos auxiliares criptográficos, utilizados pela classe SessionEncryption.

5.1.3 *Configuração do Sistema de Identificação de estudantes da Universidade do Minho*

Numa fase inicial, a configuração do sistema de identificação de estudantes envolve a instalação da *framework* Ionic[4], para o *deployment* das aplicações portadora e leitora, e da ferramenta Docker[5] para o *deployment* da Infraestrutura da AE. Posteriormente, é necessário obter o código fonte de cada uma das entidades dos respetivos repositórios. A obtenção pode ser feita via terminal, utilizando o comando "git clone + URL do repositório", ou através da interface do serviço de gestão de repositórios.

4 Para mais informações sobre o processo de instalação do Ionic em diferentes SO's, consultar: https://ionicframework.com/docs/intro/cli

5 Para mais informações sobre o processo de instalação do Docker em diferentes SO's, consultar: https://docs.docker.com/engine/install/

- **Infraestrutura da AE:** `https://github.com/filipap/backend.git` (Nota: utilizar a *branch* "main".)
- **Aplicação portadora:** `https://gitlab.inesctec.pt/mid-incm/equipa/mdoc-holder.git` (Nota: utilizar a *branch* "2-perfis".)
- **Aplicação leitora:** `https://gitlab.inesctec.pt/mid-incm/equipa/mdoc-reader.git` (Nota: utilizar a *branch* "2-perfis".)

Após a obtenção do código fonte, é necessário fazer a configuração de cada uma das entidades, nomeadamente a configuração dos parâmetros presentes em cada um dos ficheiros de configuração associados a cada entidade. Note que os ficheiros já apresentam parâmetros pré-configurados. O ficheiro de configuração da Infraestrutura da AE (*mdoc.json*) apresenta a seguinte estrutura:

```
{
    "mdoc": {
        "iso.iec.18013.5.PT.UM.Card": {
            "iso.iec.18013.5.PT.UM.CE": {
                "userType": "str", // "str" tipo de atributo - string
                "username": "str",
                "fullName": "str",
                "birthdate": "date", // "date" tipo de atributo - data
                "picture": "str",
                "number": "int", // "int" tipo de atributo - inteiro
                "year": "int",
                "academicYear": "int"
            },
            "iso.iec.18013.5.PT.UM.Course": {
                "designation": "str",
                "teachingResearchUnits": "str"
            }
        }
    },
    "organizations": [{
        "name": "UMinho",
        "country": "PT",
        "state": "Braga"
    }]
}
```

Existem dois parâmetros a se destacar:

- O parâmetro **mdoc**, representa o **esquema de dados do documento móvel**, no qual se está a desenvolver o sistema de identificação. Tendo em conta que a Prova de Conceito se centra na implementação de um sistema de identificação estudantil, a estrutura de dados, está dividida nos seguintes parâmetros:
  - **"iso.iec.18013.5.PT.UM.Card"**: tipo de documento (ou *docType*) associado ao cartão de estudante da Universidade do Minho. Para cada *docType*, está associado um conjunto de *namespaces*, re-

presentados pelos parâmetros **"iso.iec.18013.5.PT.UM.CE"** e **"iso.iec.18013.5.PT.UM.Course"**. Dentro de cada *namespace* existe um conjunto de atributos. Note que cada atributo representado pelo identificador do atributo, e pelo tipo de dados que deve ser representado, por exemplo, "str" corresponde a um atributo do tipo *string*, "date" a um atributo do tipo *datetime*, "int" a um atributo do tipo inteiro, entre outros.

Para o *namespace* **"iso.iec.18013.5.PT.UM.CE"**:

* **userType:** tipo de utilizador;
* **username:** nome do utilizador;
* **fullName:** nome completo do estudante;
* **birthdate:** data de nascimento;
* **picture:** fotografia de identificação;
* **number:** número de identificação do aluno;
* **year:** ano letivo;
* **academicYear:** ano curricular;

Para o *namespace* **"iso.iec.18013.5.PT.UM.Course"**:

* **designation:** designação do curso;
* **teachingResearchUnits:** departamento a que o curso pertence. Por exemplo, o curso de Engenharia Informática pertence à Escola de Engenharia (que em sigla se representa por EE).

O parâmetro **mdoc** é utilizado pelo sistema, como estrutura de base para:

1. A criação do documento móvel, durante a fase de Adesão de uma entidade portadora;
2. Definição da lista de atributos necessária para a definição dos perfis de entidade verificadora.

- O parâmetro **organizations**, com atributos associados à(s) Organização(ões) Verificadora(s). Do ponto de vista técnico, este parâmetro é necessário para o povoamento da tabela *Entity*, definida no esquema lógico da BD (ver Secção 4.1.2).

O ficheiro de configuração da aplicação portadora (*environment.ts*) apresenta a seguinte estrutura. Note que o ficheiro de configuração da aplicação leitora (*environment.ts*) também apresenta a mesma estrutura:

```
{
    LOCAL_IP = '192.168.1.11';
    SERVER_URL = 'http://' + LOCAL_IP + ':8000';
    PKI_URL = 'http://' + LOCAL_IP + ':8200';

    SESSION_ENCRYPTION = true;
    MDOC_MAC_AUTH = false;
    MDOC_DOCTYPE = 'iso.iec.18013.5.PT.UM.Card';
```

```
    READER_AUTH = true;

    COSE_Sign1_Alg = 'ES384';
    COSE_Sign1_crv = 'p384';
    COSE_Sign1_hash = 'sha384';
    COSE_MAC0_Alg = 'ES384';
    COSE_MAC0_crv = 'P-384';
    JWT_Alg = 'ES384';
    JWT_hash = 'SHA-384';
    JWT_crv = 'P-384';
}
```

Os parâmetros presentes nesta estrutura dividem-se em três grupos:

1. **Uniform Resource Locator** da Infraestrutura da AE (parâmetro **SERVER_URL**) e da Infraestrutura de Chave Pública (parâmetro **PKI_URL**). O parâmetro **LOCAL_IP** corresponde ao endereço IP onde se encontra alocada a Infraestrutura da AE. No caso de existir um domínio atribuido, o parâmetro corresponde ao nome do domínio;

2. Sinalizadores que especificam o contexto em que as aplicações operam.
   - **SESSION_ENCRYPTION**: determina se o processo de Obtenção dos dados envolve a encriptação do canal de comunicação entre a aplicação portadora e a aplicação leitora;
   - **MDOC_MAC_AUTH**: define se o mecanismo de autenticação da aplicação portadora (ver *mdoc authentication*, Secção 3.3.4), é feito através da utilização de uma assinatura MAC. Caso este parâmetro esteja falso utiliza-se uma assinatura digital;
   - **READER_AUTH**: autenticação da entidade verificadora na aplicação leitora.

3. Parâmetros utilizados na definição das estruturas de segurança utilizadas durante a fase de Obtenção dos dados. Note que os seguintes parâmetros correspondem a identificadores requeridos pela biblioteca criptográfica, utilizada nas aplicações móveis, para a geração de:
   - **COSE_Sign1_Alg**, **COSE_Sign1_crv** e **COSE_Sign1_hash**: assinaturas do tipo COSE_Sign1;
   - **COSE_MAC0_Alg** e **COSE_MAC0_crv**: mensagens autenticadas no formato COSE_MAC0;
   - **JWT_Alg**, **JWT_crv** e **JWT_hash**: *tokens* no formato JWT.

Após a configuração dos ficheiros faz-se o *deployment* do sistema.

O deployment da Infraestrutura da AE consiste na instanciação e execução de um conjunto de containers correspondentes à BD, à PKI e à Infraestrutura da AE. Assim:

```
$ docker-compose build
$ docker-compose up -d
```

Por sua vez, para as aplicações portadora e leitora, o *deployment* consiste na construção e instalação da aplicação nos dispositivos móveis destino (Nota: O *device ID* corresponde ao identificador do dispositivo móvel onde se pretende instalar a aplicação):

- Android

```
$ ionic cordova prepare android
$ ionic cordova build android --device="device ID"
```

- iOS

```
$ ionic cordova prepare ios
$ ionic cordova build ios --device="device ID"
```

5.2 ASPETO GERAL DAS APLICAÇÕES MÓVEIS

O diagrama da Figura 29 demonstra o fluxo de vistas definidas para as aplicações portadora e leitora. O fluxo da aplicação baseia-se no pacote *pages* do diagrama de classes da Figura 28. Note que ambas as aplicações apresentam um fluxo idêntico.

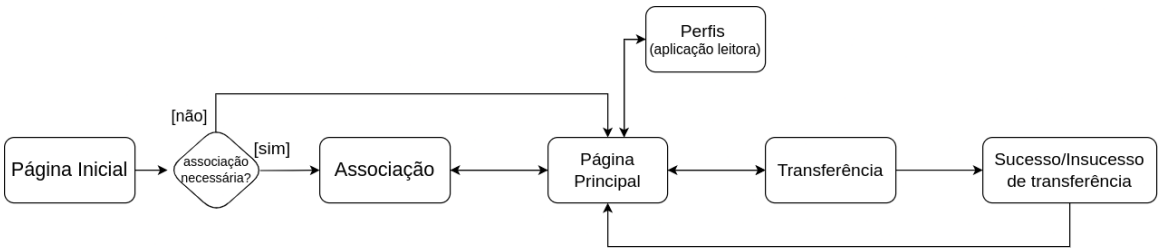

Figura 29: Fluxo das vistas definidas para as aplicações leitora e portadora

A aplicação está dividida nas seguintes páginas:

- **Página Inicial**, representada no diagrama de classes das aplicações móveis pela classe **SplashPage**. Corresponde à página de abertura da aplicação;
- A página de **Associação** de uma entidade portadora ou leitora na Infraestrutura da AE. No diagrama de classes das aplicações móveis pela é representada pela classe **LoginPage**;
- **Página Principal** da aplicação, representada pela classe **HomePage** (ver Figuras 43 e 44, no Anexo A.5);
- A página de **Perfis** de entidade verificadora, representada pela classe **ProfilePage**;
- Por fim, as páginas de **Transferência** e **Sucesso/Insucesso de transferência**. Estas páginas apresentam para o utilizador final o fluxo de transação dos dados. Para cada tecnologia utilizada na fase de

Obtenção dos dados (ver Secção 3.3.4), a página de **Transferência** usa uma classe diferente (BLEPage, WifiAwarePage e NFCPage) para demonstrar a fase de transação. Assim que o processo de transação termina o utilizador final é redirecionado para a página de **Sucesso/Insucesso de transferência**.

Nos Anexos A.2, A.3 e A.4 encontram-se as imagens da interface gráfica tanto das aplicações quanto do sistema de gestão da Infraestrutura da AE para as fases de **Adesão**, **Associação** e **Transação dos dados**, respetivamente.

5.3 SUMÁRIO DO CAPÍTULO

O Capítulo 5, resumidamente, discute todos os aspetos relativos à implementação do sistema de identificação configurável, um dos objetivos definidos por este trabalho. Importante referir que a Prova de Conceito é o resultado da configuração do sistema. O processo de configuração está descrito na Secção 5.1.3. Ao longo deste capítulo também são discutidos aspetos como a definição das ferramentas de desenvolvimento utilizadas, a modelação das aplicações portadora, leitora, e da Infraestrutura da AE.

A última secção deste capítulo apresenta a demonstração da camada de apresentação da Prova de Conceito, nomeadamente o fluxo de vistas definidas para as fases de Adesão, Associação e Transação dos dados.

6

CONCLUSÕES E TRABALHO FUTURO

A realização deste trabalho permitiu implementar, de forma bem sucedida, um sistema de identificação móvel configurável, baseado na norma técnica ISO/IEC DIS 18013-5. O sistema de identificação foi implementado com base na proposta de arquitetura, apresentada no Capítulo 4.

A definição da proposta de arquitetura seguiu uma abordagem de implementação genérica, isto é, independente a nível de ferramentas de desenvolvimento e da linguagem utilizada. Assim, definiram-se diagramas com componentes necessárias para a definição de cada uma das entidades definidas pela norma técnica.

O Capítulo 5 representa a materialização da proposta de arquitetura num sistema de identificação configurável. A Prova de Conceito apresentada nesse Capítulo demonstra um exemplo de configuração desse sistema, aplicado ao cartão de estudante. É importante referir que, uma vez que o sistema de identificação é configurável, é possível aplicar o mesmo sistema para diferentes tipos de documento móvel. Note que a norma técnica ISO/IEC DIS 18013-5, garante a sua extensibilidade para outros documentos de identificação (ver Secção 3.3.2).

Durante o desenvolvimento deste trabalho, surgiram desafios relacionados com o desenvolvimento da proposta de arquitetura. Em primeiro lugar, a norma técnica apenas define um conjunto restrito de requisitos, na sua maioria funcionais, para a implementação do sistema de identificação móvel. Também é importante referir que os requisitos apenas foram estabelecidos para a fase de Transação dos dados do documento móvel (presente na Secção 3.3.4). Tendo isso em conta, fases importantes no ciclo de vida de um documento móvel, como a Adesão e a Associação, não estão definidas. A definição da proposta de arquitetura envolveu também a definição do fluxo de processos existentes em cada uma das fases não definidas pelo documento da norma técnica, e os mecanismos de segurança inerentes a cada uma delas. A implementação do sistema de identificação também teve alguns desafios, especialmente relacionados com a escolha das ferramentas de desenvolvimento a serem utilizadas no desenvolvimento das aplicações portadora e leitora.

Tendo em conta os objetivos definidos na Secção 1.1:

1. O primeiro objetivo consistia na definição da arquitetura de um sistema de identificação, com base na norma técnica ISO/IEC DIS 18013-5. Para atingir este objetivo, no Capítulo 4 definiram-se um conjunto de diagramas com componentes e subcomponentes necessárias para a definição de cada uma das entidades envolvidas (Infraestrutura de AE, aplicação portadora e aplicação leitora). Note que no contexto de implementação, as componentes podem estar representadas em métodos, classes, ou através de módulos;

2. O segundo e último objetivo deste trabalho era a implementação de um sistema de identificação eletrónica configurável, com base na arquitetura definida no primeiro ponto. Assim, para atingir este objetivo, inicialmente foi necessário fazer a modelação de cada entidade, com base nas componentes definidas no Capítulo 4, e nas ferramentas de desenvolvimento escolhidas. Posteriormente, definiu-se o modelo de configuraração do sistema, que consiste na definição de ficheiros de configuração para cada entidade definida na arquitetura inicial, estabelecida pela norma técnica ISO/IEC DIS 18013-5 (Infraestrutura de AE, aplicação portadora e aplicação leitora, ver Secção 3.3.1). Como Prova de Conceito, foi implementado um sistema de identificação estudantil. A descrição do processo de configuração do sistema encontra-se na Secção 5.1.

Em suma, é possível concluir que, apesar dos desafios encontrados, os objetivos definidos para este trabalho foram atingidos com sucesso.

6.1 TRABALHO FUTURO

No âmbito deste trabalho, existe uma multiplicidade de trabalhos futuros que poderão ser realizados. Note que, apesar de os objetivos desta dissertação estarem concluídos, existem aspetos que podem ser melhorados, nomeadamente:

- A definição de uma plataforma de Interoperabilidade entre a Infraestrutura da AE e as Infraestruturas pertencentes a entidades externas. A plataforma tem como objetivo facilitar, por exemplo, a implementação de fases como a Obtenção de dados de Fontes de atributos externas e/ou a Adesão de entidades verificadoras. Contudo, exige uma adaptação, tanto da Infraestrutura da AE, quanto da Infraestrutura da entidade que pretenda aderir e/ou comunicar com a Infraestrutura da AE;

- Suporte a diferentes documentos móveis na mesma Infraestrutura da AE. Atualmente uma instância da Infraestrutura implementada está desenhada para suportar a gestão de apenas um tipo de documento móvel. Isto implica um esforço de remodularização da Prova de Conceito implementada;

- Implementação de funcionalidades nas aplicações móveis, como:
  - Criação de uma página de gestão de perfis de entidade verificadora pré-consentidos, na aplicação portadora;
  - Utilização da tecnologia NFC para o processo de Estabelecimento da conexão e para a fase de Obtenção dos dados e da tecnologia Wi-Fi Aware para a fase de Obtenção dos dados.

- A adição de novas formas de autenticação na Infraestrutura da AE, por exemplo a utilização de autenticação a dois fatores;

- Definição de mecanismos de segurança adicionais para o SGBD do fornecedor de atributos local, por exemplo a utilização de mecanismos mais complexos de encriptação dos dados na BD.

BIBLIOGRAFIA

[1] Identification for development: The biometrics revolution. *SSRN Electronic Journal*, page 1, 2013. ISSN 1556-5068. doi: 10.2139/ssrn.2226594. URL http://www.ssrn.com/abstract=2226594.

[2] Fingerprints on artifacts and historical items: Examples and comments. *Journal of Ancient Fingerprints*, 2: 7, 2014. URL https://www.researchgate.net/publication/268811220.

[3] AMA. Cartão de cidadão: O novo documento de identificação dos cidadãos portugueses. page 14, 2008.

[4] AMA. Autenticacao.gov - fornecedor de autenticação da administração pública portuguesa. Technical report, Agência para a Modernização Administrativa, 2020.

[5] WorldBank Blogs. The global identification challenge: Who are the 1 billion people without proof of identity?, 2018. URL https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity.

[6] British Standards Institution. Personal identification – ISO-Compliant driving licence — part 5: Mobile driving licence (mDL) application. Standard, International Organization for Standardization, London, EN, 2021. URL https://www.iso.org/standard/69084.html.

[7] Daniel Castro. Explaining International Leadership: Electronic Identification Systems. Publication, ITIF, September 2011.

[8] European Comission. e-identification | shaping europe's digital future — european commission, 2022. URL https://ec.europa.eu/digital-single-market/en/e-identification.

[9] eIDAS. eidas - the ecossystem, 2014. URL https://www.eid.as/#regulation.

[10] FHIR. Overview-arch - fhir v4.0.1, 2012. URL https://www.hl7.org/fhir/overview-arch.html#framework.

[11] World Bank Group's Identification for Development(ID4D). Technology Landscape for Digital Identification. 2018.

[12] ID4Africa. About — id4africa, 2014. URL https://id4africa.com/about/.

[13] ID4D. Data | identification for development, 2018. URL https://id4d.worldbank.org/global-dataset.

[14] Nick Pope Jonathan Allin. *The eIDAS Regulation for Dummies*. Thales, 2017.

[15] Office of the National Coordinator for Health Information Technology. What is fhir? *ONC Fact Sheet*, 2019.

[16] openCRVS. Functional architecture, 2018. URL https://documentation.opencrvs.org/opencrvs-core/docs/system_overview/functionalArchitecture.

[17] openCRVS. Our solution, 2018. URL https://www.opencrvs.org/our-solution.

[18] Ionic Team. Angular unit and end-to-end testing for ionic app components, 2022. URL https://ionicframework.com/docs/angular/testing#pages-and-components.

[19] Thales. The eidas regulation in 2017 – a pivotal year for digital services in the eu, 2017. URL https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/eidas-regulation-in-2017.

[20] Thales. 11 years of eid: Portugal's citizen card, 2019. URL https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/portugal-id.

A

ANEXOS

A.1 OBTENÇÃO DOS DADOS, VIA BLUETOOTH LOW ENERGY (BLE)

Este tópico surge com o objetivo de explicitar algumas das opções tomadas na descrição do diagrama de classes na Secção 5.1.2. Os diagramas das Figuras 30 e 31 demonstram as duas abordagens que se são adotar no processo de *Data Retrieval*, via BLE. Estas abordagens são designadas pela norma técnica ISO/IEC DIS 18013-5 como modo *mdoc central client* e o modo *mdoc peripheral server*, respetivamente. Note que a abordagem a ser utilizada durante a fase de obtenção dos dados é negociada na fase de estabelecimento da conexão.

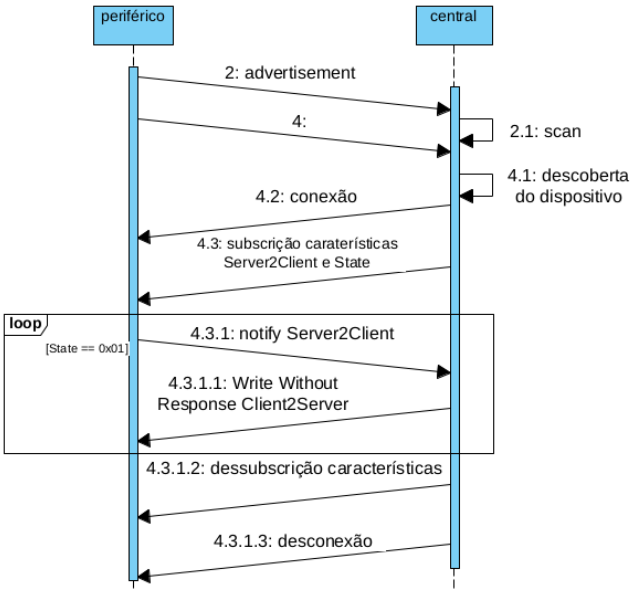

Figura 30: Diagrama de sequência do modo *mdoc central client*

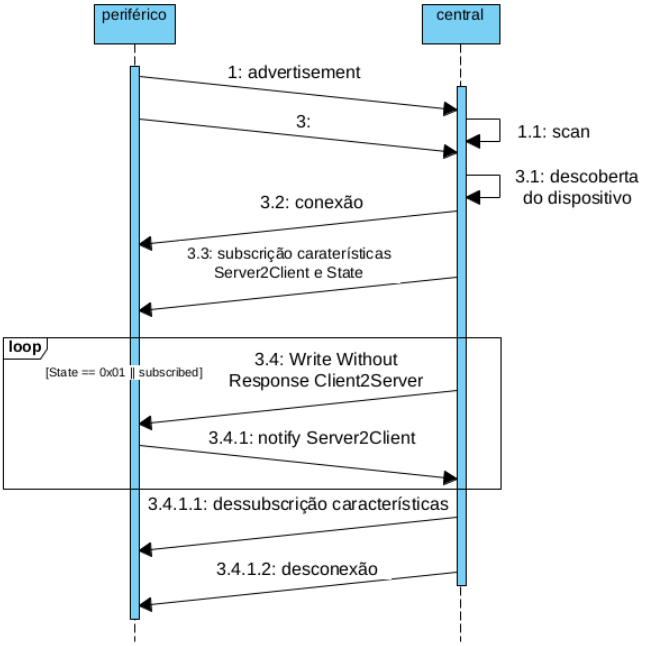

Figura 31: Diagrama de sequência do modo *mdoc peripheral server*

Existem quatro fases comuns às duas abordagens:

1. Publicitação (ou *advertisement*) do dispositivo que se encontra no modo periférico. Nesta fase, o dispositivo periférico faz um conjunto de notificações a anunciar a sua presença. O dispositivo central, por sua vez, efetua o scaneamento dos dispositivos periféricos existentes na sua proximidade, com um identificador único (denominado **puuid**);

2. Deteção do dispositivo periférico, conexão, subscrição nas características anunciadas pelo dispositivo periférico, e estabelecimento de um canal seguro (ver *Session Encryption*, Secção 3.3.4);

3. Troca de dados entre os dois dispositivos. É nesta fase onde ocorre a transação dos dados entre a aplicação portadora e a aplicação leitora;

4. Término da conexão. Do ponto de vista técnico, esta fase corresponde à dessubscrição das características e à desconexão do dispositivo central do dispositivo periférico.

É importante referir que existem algumas diferenças, nomeadamente:

- O modo, definido pela especificação do BLE, em que a aplicação portadora e a aplicação leitora atuam. No caso de se utilizar a abordagem *mdoc central client* a aplicação portadora atua no modo central e a aplicação leitora no modo periférico. O inverso ocorre no caso de se utilizar a abordagem *mdoc peripheral server*.

- Os valores das características Client2Server e Server2Client. Cada aplicação apresenta um conjunto de características, cada uma com um **uuid** diferente.

A.2 ADESÃO

A.2.1 *Adesão de uma entidade portadora*

A Adesão de uma entidade portadora divide-se nas seguintes fases:

1. Criação de um Curso;

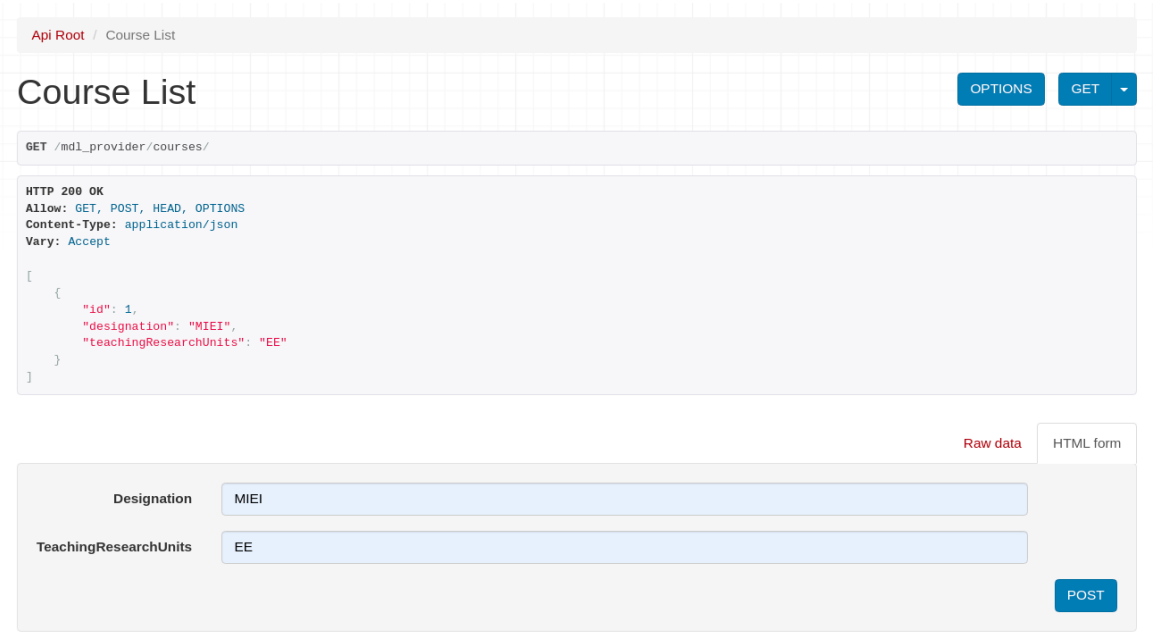

Figura 32: Criação curso

2. Criação de um utilizador do tipo "STUDENT".

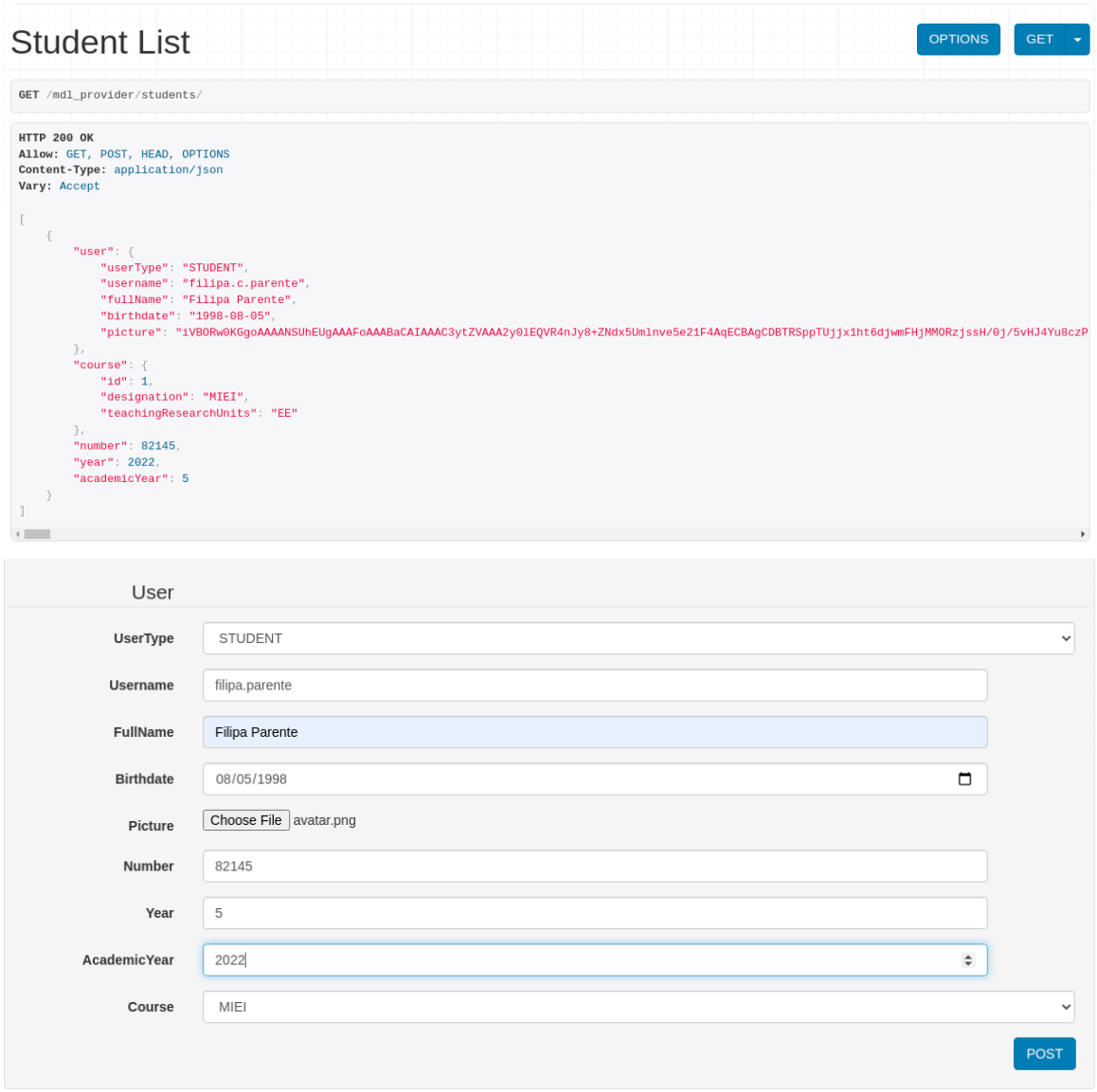

Figura 33: Adesão de um estudante (entidade portadora)

A.2.2 *Adesão de uma entidade verificadora*

A Adesão de uma entidade verificadora divide-se nas seguintes fases:

1. Criação de um Reader.

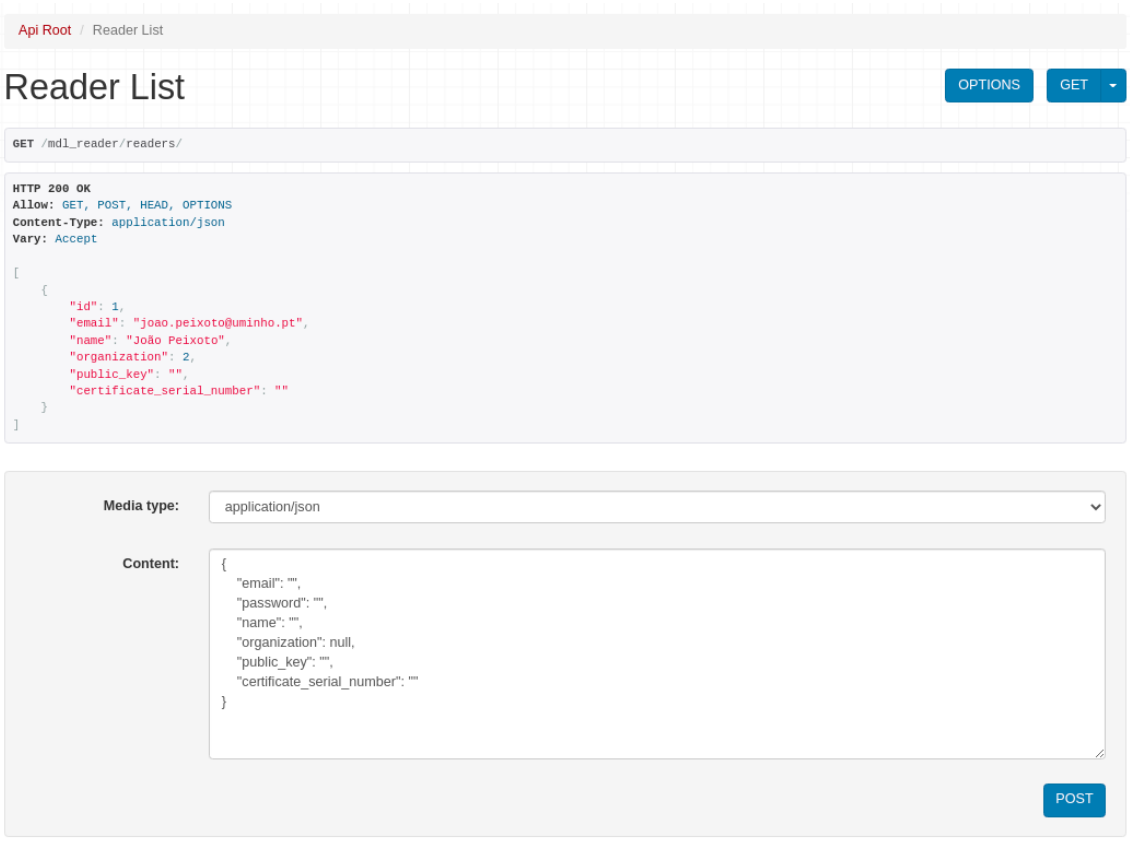

Figura 34: Adesão de uma entidade verificadora

A.3 ASSOCIAÇÃO

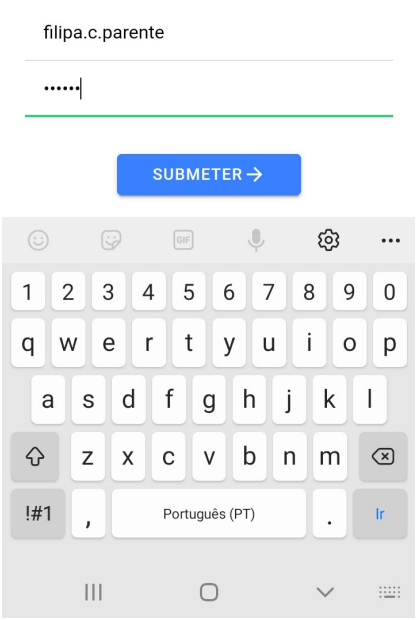

Figura 35: Página de Associação (aplicação portadora)

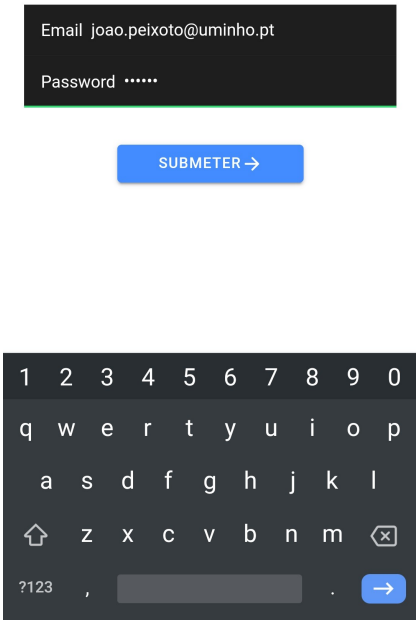

Figura 36: Página de Associação (aplicação leitora)

A.4 TRANSAÇÃO DOS DADOS

A.4.1 *Aplicação portadora*

Figura 37: Página de transferência durante a fase de Estabelecimento da Conexão

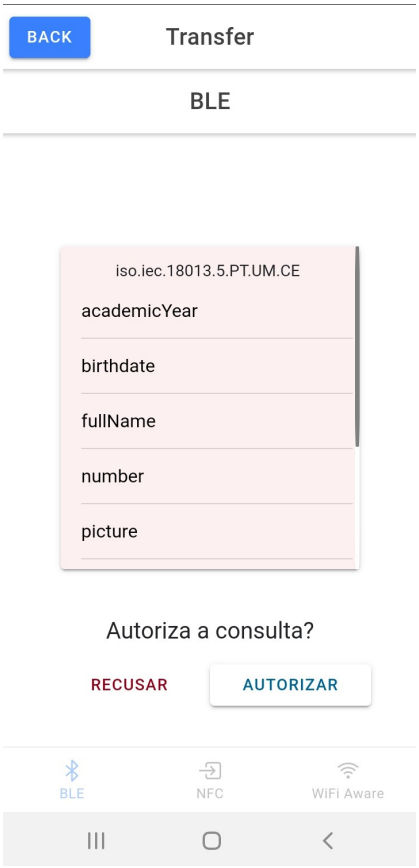

Figura 38: Página de consentimento durante a fase de transação

Figura 39: Página de sucesso/insucesso da transferência

A.4.2 *Aplicação leitora*

Figura 40: Página de transferência durante a fase de Estabelecimento da Conexão

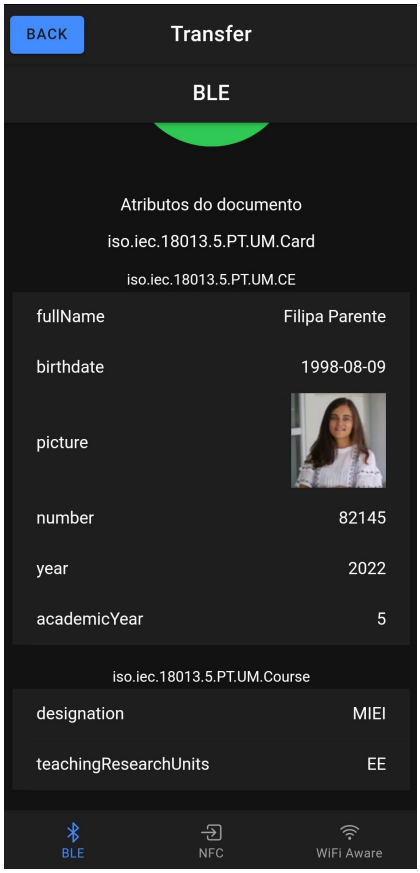

Figura 41: Página de sucesso/insucesso da transferência

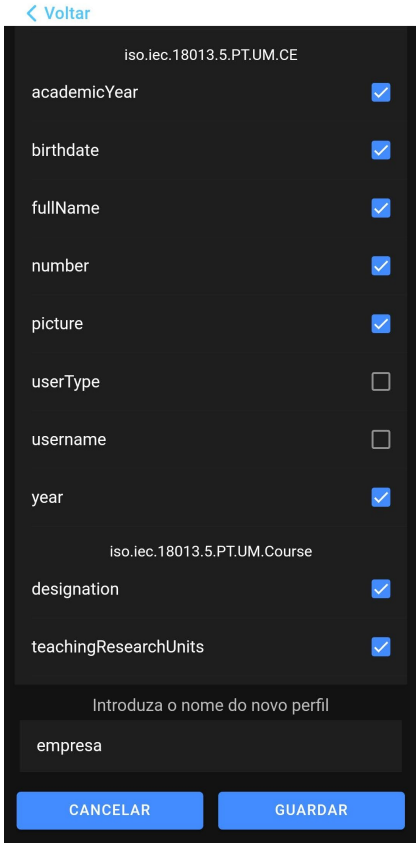

Figura 42: Página de criação dos perfis de entidade verificadora

A.5 PÁGINA PRINCIPAL

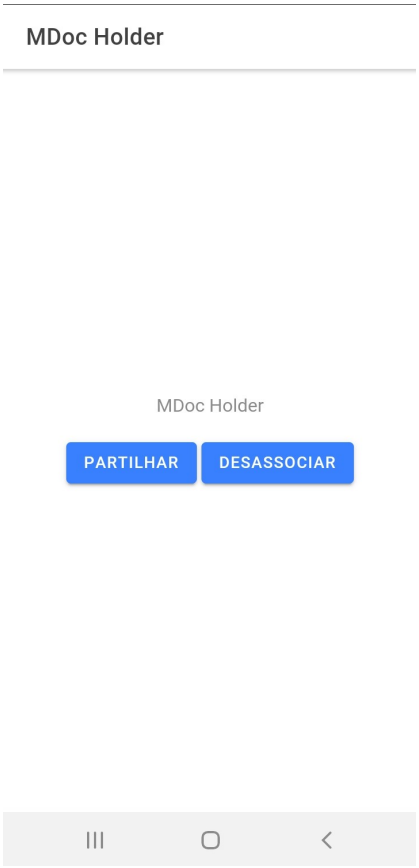

Figura 43: Página principal da aplicação portadora

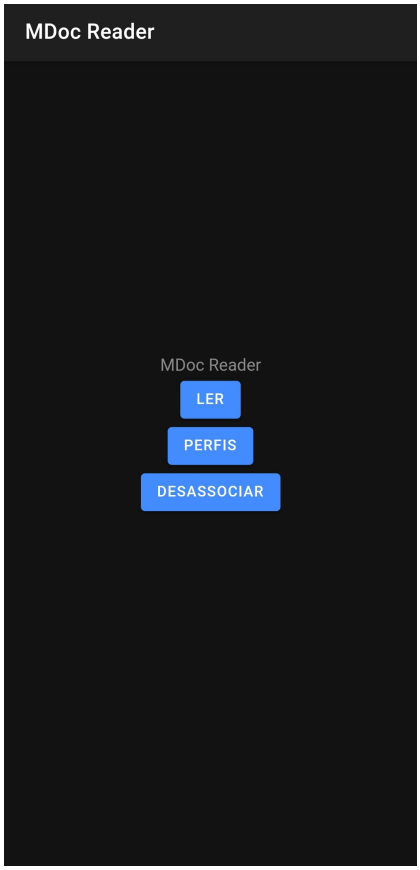

Figura 44: Página principal da aplicação leitora