Engenharia de Segurança

Universidade do Minho

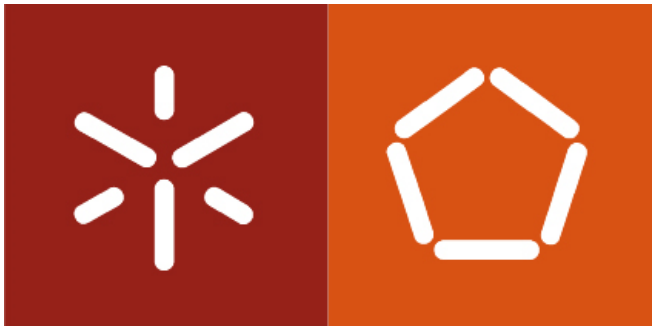
Mestrado Integrado em Engenharia Informática

Projeto em Identificação *mobile*

mDL (*mobile Driving License*)

Autores:
A77531 - Daniel Maia
A78034 - Diogo Costa
A77364 - Mafalda Nunes

3 de Abril de 2019



Resumo

Conteúdo

1 Introdução

Este projeto é desenvolvido no âmbito da unidade curricular de Engenharia de Segurança, do Mestrado Integrado em Engenharia Informática, da Universidade do Minho.

Um dos principais objetivos deste trabalho é a investigação e análise do *standard* ISO de desmaterialização da Carta de Condução, mais especificamente o "`ISO/IEC CD 18013-5 Information technology – Personal identification – ISO compliant driving licence – Part 5: Mobile driving licence application (mDL)`". Pretende-se dar especial atenção à estrutura de dados requerida e aos vários algoritmos, primitivas criptográficas e *workflows* que garantem a segurança da mDL. Por fim, deverá apresentar-se uma implementação da mDL, de acordo com o ISO, através da utilização de bibliotecas *open-source*.

De facto, esta desmaterialização de documentos, que se baseia em técnicas e algoritmos criptográficos, torna possível o acesso aos mesmos através de dispositivos móveis, que são comummente utilizados na atualidade. Assim, começa a surgir a tendência de substituir os documentos de identificação, como hoje os conhecemos (em papel ou *smartcard*), por documentos desmaterializados.

2 Contextualização

O *standard* ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*) 18013 é caracterizado pelo título geral `Personal Identification – ISO Compliant Driving Licence` e é constituído pelas seguintes partes:

- **Parte 1** – `Physical Characteristics and Basic Data Set`: descreve as características físicas, o conjunto básico de elementos de dados, o *layout* visual e as capacidades de segurança física (recursos legíveis pelo ser humano) de uma *ISO-compliant driving licence* (IDL);
- **Parte 2** – `Machine-Readable Technologies`: descreve as tecnologias, legíveis por máquina, que podem ser utilizadas por este *standard*, incluindo a estrutura de dados lógica e o mapeamento de dados por cada tecnologia;
- **Parte 3** – `Access Control, Authentication and Integrity Validation`: descreve as capacidades de segurança eletrónica que podem incorporar este *standard*, incluindo mecanismos para controlo de acesso aos dados, verificação da origem de uma IDL e confirmação da integridade dos dados;
- **Parte 4** – `Test Methods`: descreve métodos de teste que podem ser utilizados para determinar se uma IDL está de acordo com os requisitos das tecnologias legíveis por máquinas especificadas na parte 2 e com as capacidades de segurança eletrónica especificadas na parte 3.

Este *standard* cria uma base comum para a utilização internacional e reconhecimento mútuo da IDL, sem impedir que países ou estados apliquem as suas regras de privacidade e que autoridades nacionais/comunitárias/regionais de trânsito tratem das suas necessidades específicas.

A **Parte 5** do ISO/IEC 18013 – `Mobile Driving Licence` – pretende estabelecer um *standard* de especificações de interface para a implementação de cartas de condução associadas a dispositivos móveis (*Mobile Driving License* - mDL). Assim, esta parte descreve a interface e requisitos físicos e funcionais associados, que possibilitam a utilização de dispositivos móveis pelo titular da carta de condução, para a fornecer a um verificador, facilitando o acesso do mesmo a informação da carta de condução.

Neste contexto, considera-se que dispositivos móveis são os dispositivos eletrónicos com interface de utilizador e a capacidade de armazenar informação da mDL e de a partilhar com um leitor, após instrução do titular – *smartphones*, *wearables*, entre outros. Um leitor mDL é um dispositivo portátil ou computador, que pode trocar dados com uma mDL, enquanto que o titular da mDL é o indivíduo para quem a mDL é emitida, isto é, o titular legítimo dos privilégios de condução refletidos na mDL.

O objetivo do ISO/IEC 18013-5 é permitir que verificadores não associados à autoridade de emissão da mDL, como outras autoridades de emissão ou entidades verificadoras de outros países, ganhem acesso à informação para a qual o titular da mDL providenciar consentimento, conseguindo autenticá-la. Para o conjunto de informações disponibilizado pelo titular da mDL, estas entidades deverão poder:

1. Utilizar uma máquina para obter a informação da mDL;
2. Estabelecer a conexão entre a mDL e o seu titular, com um grau aceitável de confiança;
3. Autenticar a origem da informação da mDL;
4. Verificar a integridade da informação da mDL.

Salienta-se a utilidade do titular poder aceder e facultar dados da sua carta de condução através de um dispositivo móvel, sendo este tipo de dispositivos muito utilizado atualmente. Outra vantagem das mDL em relação às cartas de condução físicas é a capacidade de atualizar informação com mais frequência e autenticá-la com um nível de confiança superior.

Existem três interfaces fulcrais para esta parte do *standard*, que são explicadas de seguida:

1. Interface entre a mDL e a autoridade emissora, que permite controlar, entre outros, como a mDL é fornecida e como são efetuadas atualizações. Esta interface não é o foco desta parte do ISO/IEC 18013, uma vez que a interoperabilidade entre autoridades emissoras não é requerida para as funcionalidades pretendidas.
2. Interface entre a mDL e o leitor, que tem de funcionar em tempo real e é descrita na parte 5 do ISO/IEC 18013.
3. Interface entre a autoridade emissora e a entidade de verificação, que facilita a troca de informação requerida para permitir a um leitor confirmar a autenticidade da informação da mDL e, em alguns casos, ler alguma informação da mesma. Esta interface é estabelecida preferencialmente entre a entidade verificadora e a autoridade emissora (diretamente ou através de intermediários), em vez de diretamente entre o leitor e a autoridade de emissão. Para além disso, não precisa de funcionar em tempo real e pode ser usada pela própria autoridade emissora, em leitores sob o seu controlo. Esta interface é descrita nesta parte do ISO/IEC 18013.

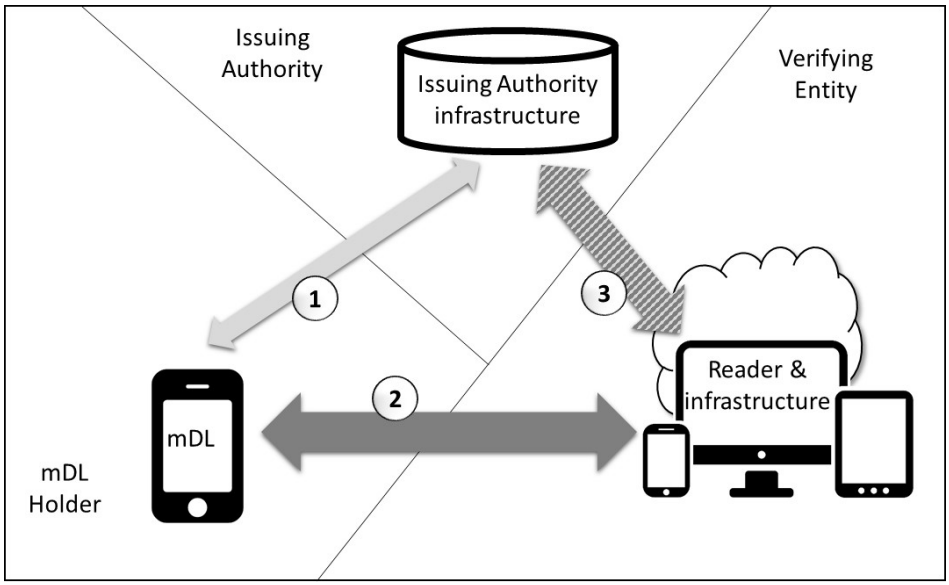


Figura 1: Ecossistema mDL, incluindo as interfaces associadas

3 Requisitos

Os requisitos funcionais abrangidos por esta parte do *standard* para a solução do mDL incluem:

- Capaz de funcionar durante verificação num ambiente *offline* (leitor mDL *offline* e mDL *offline*).
- Capaz de funcionar durante verificação num ambiente *online* (leitor mDL *online* e mDL *online*).
- Inclui mecanismos ou envolve uma arquitetura que permite a partes interessadas na mDL (titular, aplicador da lei ou entidade privada) estabelecer confiança na informação providenciada pela mDL, isto é, ter garantias de que a mDL foi emitida pela alegada autoridade de emissão e que informação não foi alterada.
- Confirmar a ligação entre uma mDL e um titular de mDL.
- Transmitir privilégios de condução.
- Permitir a leitura de informação entre autoridades emissoras.
- Permitir que um titular de mDL autorize a libertação de alguma informação selecionada da mDL para um leitor de mDL.

Para além destes requisitos, existem ainda alguns problemas que as autoridades de emissão deverão resolver, mas que não são abrangidos por esta versão do ISO/IEC 18013-5:

- Mecanismos e tecnologias de armazenamento dos dados da mDL.
- Suporte a aplicações de gestão remota da mDL, pelo titular.

- Referência ao consentimento do utilizador para um titular de mDL controlar interações online com os sistemas da autoridade de emissão.

Existem ainda requisitos técnicos relativos à interface entre uma mDL e um leitor de mDL, que são especificados nesta parte do ISO/IEC 18013:

- Estrutura de dados lógicos com as informações da mDL, quando transferidas entre uma mDL e um leitor mDL, deve respeitar os seguintes aspetos:
  - Elementos de dados considerados no ISO/IEC 18013-2:
    - TODO: ISO/IEC 18013-2
  - Elementos de dados adicionais:
    - Inclusão obrigatória da imagem facial do titular.
    - Elementos de dados adicionais para "Informação Atualizada".
    - Identificador adicional que indica o fator de forma.
    - Grupos de dados mDL, utilizados para transferência de informação seletiva (inclui novos elementos de dados).
- Protocolo de comunicação para troca de dados mDL entre uma mDL e um leitor:
  - Camada de transmissão:
    - ISO/IEC 14443 e/ou ISO/IEC 18092 (NFC)
    - Interface visual (câmara)
    - Wi-Fi *Aware*
    - Internet
    - *Bluetooth Low Energy* (BLE)
  - Camada de apresentação:
    - Comandos ISO/IEC 7816-4 e ISO/IEC 7816-8 (TODO: Part 2 and Part 3 of this standard) para o equivalente a *Standard Encoding* para mDL
    - Códigos de barras 2D (para estabelecimento de conexão entre dispositivos e o equivalente a *Compact Encoding* para mDL, na transferência de dados da mDL)
- Mecanismos de proteção de dados para serem aplicados, tendo em conta o ISO/IEC 18013-3 - preservar confidencialidade, integridade e autenticação de dados mDL.

Especificam-se ainda alguns requisitos funcionais relativos a uma aplicação de leitores de mDL, para assegurar a verificação fiável de uma mDL:

- Disponibilidade de verificação de dados (com certificados digitais, por exemplo) de autoridades emissoras, incluindo a definição do modelo de confiança utilizado para uma mDL.
- Sequência de leitura para dados de uma mDL.
- Sequência de verificação para dados de uma mDL.

4 Estrutura de Dados Lógica

A estrutura de dados mDL é codificada como um conjunto de objetos de dados BER-TLV e pode ser apresentada em dois formatos: *standard encoding* e *compact encoding*.

4.1 *Standard encoding*

4.1.1 Estrutura de ficheiros

A estrutura de dados lógica do mDL é constituída por um conjunto de ficheiros elementares, cada um deles contendo um ou mais grupos de dados. Cada um destes pode ser classificado como obrigatório, opcional ou condicional (dependendo do suporte providenciado) na implementação do mDL. Relativamente à permissão de acesso a um dado ficheiro é necessário indicar se o consentimento explícito é requirido do titular mDL.

Ficheiro Elementar	Presença	Consentimento
Data group 1	Obrigatória	Explícito
Data group 2-4	Opcional	Explícito
Data group 5	Opcional (Não recomendado)	Explícito
Data group 6	Obrigatória	
Data group 7-9	Opcional	Explícito
Data group 10	Obrigatória	
Data group 11	Opcional	Explícito
Data group 13	Condicional (Obrigatória se Active Authentication é suportada)	
Data group 14	Condicional (Obrigatória se autenticação PACE e/ou Chip é suportada)	
Data group 32-127	Opcional	Explícito
EF.COM	Obrigatória	
EF.SOD	Obrigatória	
EF.CardAccess	Condicional (Obrigatória se PACE é suportada)	
EF.GroupAccess	Obrigatória	

4.1.2 Comandos

Os comandos de uma aplicação mDL cumprem a norma ISO/IEC 18013-2. Cada comando toma a forma de uma mensagem que será transmitida a um recipiente, sendo constituída por um cabeçalho e um corpo.

O cabeçalho é constituído por quatro *bytes*, cada um dos quais indicando um de campos, presentes na seguinte ordem:

- O byte Class (CLA) que, como o nome indica, especifica a classe, interindustria ou proprietária, do comando a executar. Indica também, caso se trate de um comando de

classe interindústria, se se pretende executar *chaining* de comandos e respostas (e.g. transmissão de uma *string* demasiado longa para um único comando). Adicionalmente, indica se se pretende utilizar um canal seguro para a transmissão de dados e o respetivo formato. Por fim, é indicado o canal lógico sobre o qual a transmissão será efetuada.

- O byte Instruction (INS), que especifica exatamente qual comando será processado. Existe uma variedade de comandos providenciados pela norma ISO/IEC 18013-2. Para além dos comandos especificados na norma, é especificado um comando adicional UPDATE BINARY, que atualiza o ficheiro EF.GroupAccess.
- Os bytes Parameter 1 e 2 (P1 e P2), que indicam controlos e opções para o processamento do comando.

4.1.3 Grupos de dados

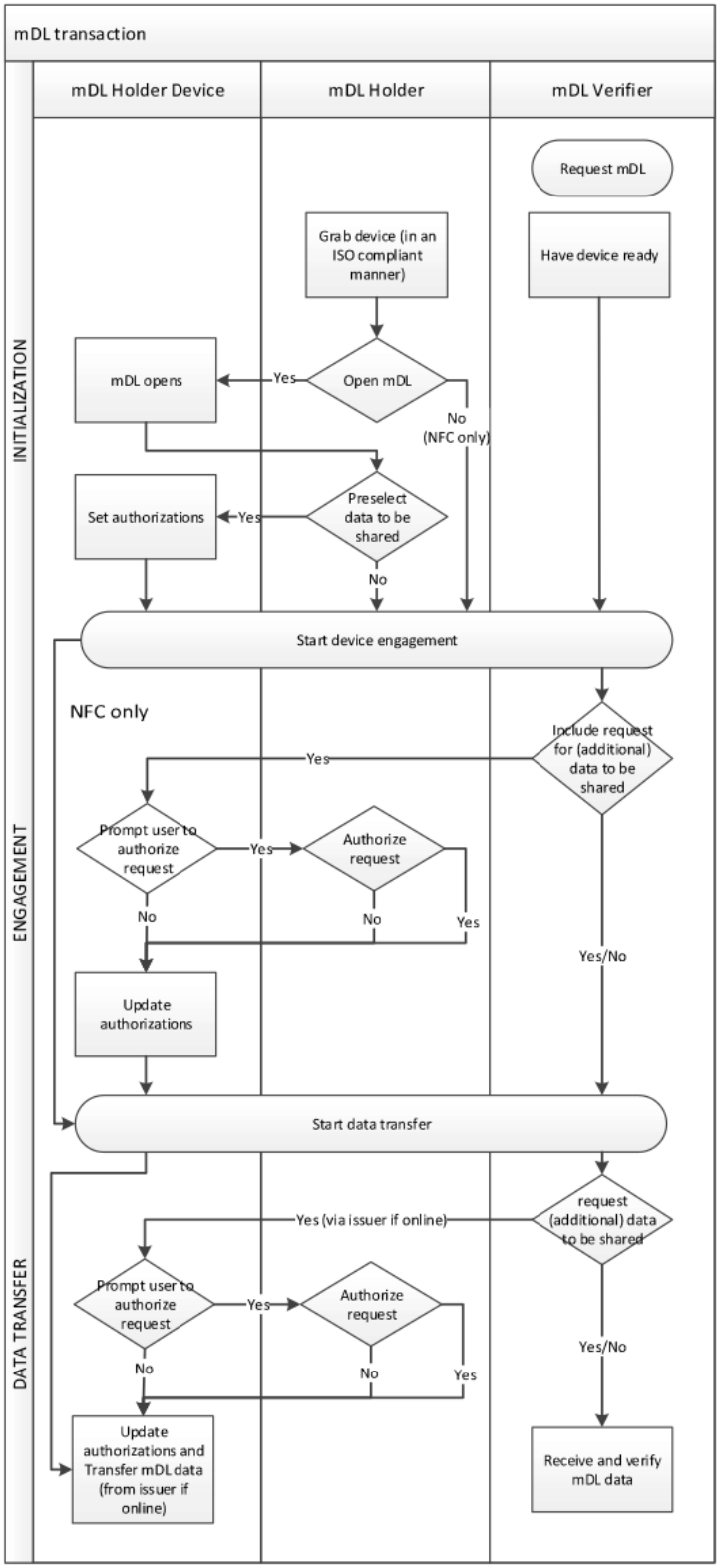
Os dados mDL são organizado em 11 grupos de dados de acordo com a norma ISO/IEC 18013-2, com algumas alterações. O primeiro grupo de dados (DG 1) é responsável por guardar o conjunto mínimo de dados essenciais para identificação internacional, com a exceção da assinatura e foto do indivíduo. Os grupos de dados 6 e 10, são feitos obrigatórios na implementação do mDL.

Ficheiro Elementar	Conteúdo
Data group 1	Elementos obrigatórios
Data group 2	Detalhes do titular
Data group 3	Detalhes da autoridade emissora
Data group 4	Foto do titular
Data group 5	Assinatura
Data group 6	Biométrica da face
Data group 7	Biométrica do dedo
Data group 8	Biométrica da íris
Data group 9	Outras biométricas
Data group 10	Dados mDL obrigatórios
Data group 11	Dados domésticos

Para além destes, são introduzidos os grupos de dados opcionais 32 a 127, que permitirão a autorização seletiva da informação mDL ao leitor. Quaisquer destes grupos que contenha dados é introduzido no elemento EF.SOD. É introduzido também o elemento EF.GroupAccess, que contem a informação sobre quais grupos de dados são disponibilizados ao leitor mDL. **4.2 *Compact encoding***

O *Compact encoding* é o esquema de dados utilizado na transferência de informação por meio de uma interface ótica, tais como códigos de barras ou tiras magnéticas. Estes requerem um espaço de armazenamento entre 300 B e 5 kB. Devido a esta limitação, o número de grupos de dados é restrito, bem como o espaço permitido para cada um. O esquema do *compact encoding* providencia espaço para os grupos de dados 1, 6 e 10 obrigatoriamente, bem como a possibilidade da utilização dos grupos 2, 3, 4, 7 e 11, caso necessário. **5 Transferência de Dados da mDL**

Uma transação mDL consiste em três fases, sendo estas a inicialização, a conexão entre dispositivos e a transferência de dados. Estas fases são bem expressas no diagrama que se segue:



Inicialização

Durante a inicialização, uma mDL é aberta pelo utilizador ou, potencialmente, ativada pelo NFC. O utilizador pode, opcionalmente, pré-autorizar a partilha de certos elementos de dados.

Conexão entre Dispositivos

Durante o estabelecimento da conexão entre dispositivos, é utilizado NFC ou um código QR (*Quick Response*) para transferir a estrutura de conexão de dispositivos, de forma a configurar o passo seguinte de transferência de dados. Os leitores mDL devem suportar tanto a interface ótica (código QR) como as tecnologias NFC. Quando é utilizado NFC, é possível a comunicação nos dois sentidos, possibilitando que o leitor mDL solicite acesso a elementos adicionais para partilha.

Transferência de Dados

A transferência de dados pode utilizar um método *offline* ou *online*. Em qualquer caso, a conexão pode ser utilizada para solicitar acesso a elementos de dados (adicionais) ao leitor mDL. Uma mDL deverá suportar qualquer um dos seguintes métodos de transferência de dados *offline*: NFC, *Bluetooth Low Energy* (BLE) ou código de barras 2D. Os leitores mDL deverão suportar, obrigatoriamente, essas três tecnologias, bem como, opcionalmente, a *Wi-Fi Aware*.

Figura 2: Processo de transferência de dados de uma mDL

6 Mecanismos de Proteção de Dados da mDL

7 Implementação da mDL (ISO *compliant*)

8 Conclusões