

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

5 de Maio de 2019



Resumo

Conteúdo

1	Introdução	2
2	Contextualização	2
3	Requisitos	4
4	Estrutura de Dados Lógica	6
4.1	<i>Standard encoding</i>	6
4.1.1	Estrutura de ficheiros	6
4.1.2	Comandos	7
4.1.3	Grupos de dados	8
4.1.4	Data group 1	8
4.1.5	Data group 6	9
4.1.6	Data group 10	10
4.1.7	EF.COM	10
4.1.8	EF.SOD	10
4.1.9	EF.GroupAccess	10
4.2	<i>Compact encoding</i>	10
5	Transferência de Dados da mDL	11
6	Mecanismos de Proteção de Dados da mDL	13
6.1	Controlos de segurança	13
6.1.1	Autenticação Passiva (ISO/IEC 18013-3)	13
6.1.2	Outros mecanismos	15
6.2	Controlos de privacidade	16
6.2.1	Consentimento do utilizador	16
7	Implementação da mDL (ISO <i>compliant</i>)	16
8	Conclusões	17

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 comumente 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.

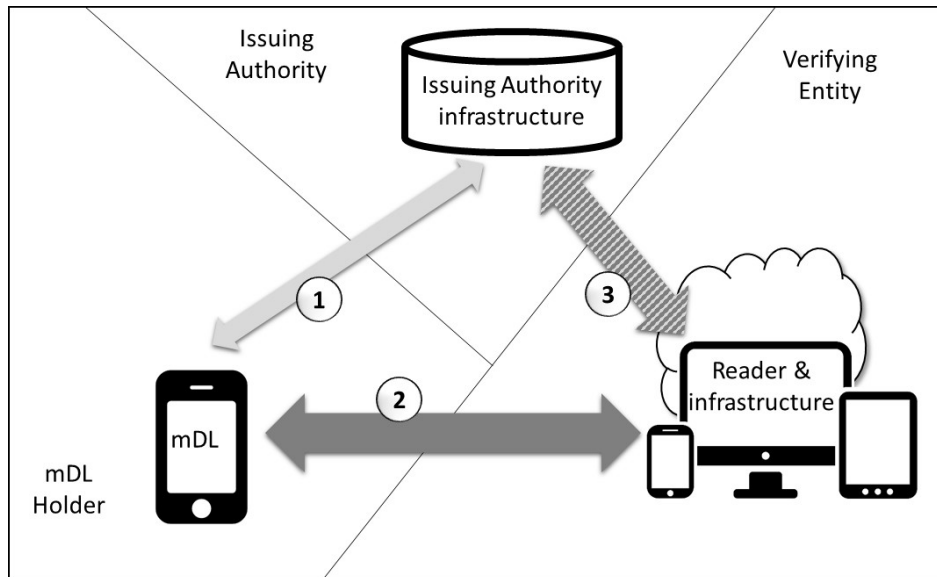


Figura 1: Ecossistema mDL, incluindo as interfaces associadas

3 Requisitos

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

- Capacidade de funcionar durante verificação num ambiente *offline* (leitor mDL *offline* e mDL *offline*).
- Capacidade de funcionar durante verificação num ambiente *online* (leitor mDL *online* e mDL *online*).
- Mecanismos ou 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 informação especificamente seleccionada da mDL para um leitor mDL.

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

- 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:
 - * DG1: elementos de texto (obrigatório).
 - * DG2: detalhes do titular da licença (opcional).
 - * DG3: detalhes da autoridade de emissora (opcional).
 - * DG4: imagem do retrato do titular da licença (opcional).
 - * DG5: assinatura / imagem de marca habitual (opcional).
 - * DG6: modelo biométrico facial (opcional).
 - * DG7: modelo biométrica do dedo (opcional).
 - * DG8: modelo biométrico da íris (opcional).
 - * DG9: outro modelo biométrico (opcional).
 - * DG10: reservado para uso futuro.
 - * DG11: dados domésticos (opcional).
- Elementos de dados adicionais:
 - * Inclusão obrigatória da imagem facial do titular.
 - * Elementos de dados adicionais para “Up to Date info”.
 - * **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 (Parte 2 e 3) 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 (e.g. certificados digitais) de autoridades emisoras, 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.

Assim sendo, todos estes requisitos são necessários para assegurar a competência do sistema.

4 Estrutura de Dados Lógica

A estrutura de dados mDL é codificada como um conjunto de objetos de dados BER-TLV.

As *Basic Encoding Rules* (BER) especificam o formato da estrutura de dados, recorrendo a um método de *encoding type-length-value* (TLV). A codificação de dados consiste em quatro elementos que se apresentam na seguinte ordem:

1. O octeto *Type*, que distingue os dados de outros membros.
2. O octeto *Length*, que define o número de bytes que constituem o objeto.
3. O octeto *Value*, que contém o conteúdo do elemento de dados.

Deste modo, a estrutura mDL pode ser apresentada em dois formatos: *standard encoding* e *compact encoding*.

4.1 *Standard encoding*

O *standard encoding* do mDL é constituído por três componentes primários: A estrutura de ficheiros, o conjunto de comandos e os grupos de dados que o constituem.

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 requerido do titular mDL.

Na tabela 1 são identificados os vários conjuntos de ficheiros elementares que constituem a estrutura de dados lógica do mDL.

Tabela 1: Conjunto de ficheiros elementares.

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 campo, presentes na seguinte ordem:

- O *byte Class* (CLA) que, como o nome indica, especifica a classe, interindústria 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 detalhados 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, tornam-se obrigatórios na implementação do mDL.

Tabela 2: Grupos de dados 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 de informação mDL para ser fornecida ao leitor. Quaisquer destes grupos que contenha dados é introduzido no elemento EF.SOD. É incluído também o elemento EF.GroupAccess, que contém informação sobre que grupos de dados são disponibilizados ao leitor mDL.

Por motivos de simplicidade, e tendo em conta que se pretende implementar apenas os campos obrigatórios do mDL, serão apenas aprofundadas as constituições dos elementos DG1, DG6, DG10, EF.COM, EF.SOD e EF.GroupAccess.

4.1.4 Data group 1

Este ficheiro elementar contém os dados demográficos do titular, bem como as categorias de veículo para os quais este tem qualificações e é identificado pela *tag* '61' e o identificador '01', seguido pelo comprimento total deste grupo. Como a totalidade da informação contida neste é obrigatória e encontra-se numa ordem fixa, a informação demográfica encontra-se concatenada num único objeto com a *tag* '5F1F' seguida do comprimento da mesma.

De tal modo, sabendo que cada campo de tamanho variável é precedido pelo respetivo valor de comprimento, os dados demográficos seguem a seguinte estrutura:

Nome	Tamanho Variável/ Fixo	Formato	Exemplo
Nome Próprio	Variável	Até 36 letras e/ou símbolos	Smithe-William
Apelidos	Variável	Até 36 letras e/ou símbolos	Alexander George TH
Data de nascimento (yyyymmdd)	Fixo	8 números	19700301
Data de emissão (yyyymmdd)	Fixo	8 números	20020915
Data de expiração (yyyymmdd)	Fixo	8 números	20070930
País emissor	Fixo	3 letras	JPN
Autoridade emissora	Variável	Até 65 letras, números e/ou símbolos	HOKKAIDO PREFEC POLICE ASAHIKAWA PUBLIC SAFETY COM
Número de licença	Variável	Até 65 letras e/ou números	A29065439516427

Por sua vez, cada uma das qualificações de veículo é codificada com a *tag* '7F63', seguida pelo comprimento total da lista e pelo número de entradas da mesma, codificado com a *tag* '02'. Cada elemento da lista é codificado com a *tag* '87' seguida pelo comprimento do elemento.

4.1.5 Data group 6

Este grupo é responsável pelo armazenamento de uma variedade de identificadores biométricos do titular. No entanto, por motivos de simplicidade, assume-se que apenas a foto estará presente. Este ficheiro é identificado pela *tag* '75' e o identificador '06', seguido pelo comprimento total do grupo. A seguir segue a seguinte formatação:

Tag	Comprimento	Valor
'7461'	Variável	Informação dos subgrupos biométricos
'02'	Variável	Número de subgrupos biométricos do grupo (no contexto do Projeto, 1)
'7F60'	Variável	Subgrupo biométrico
'A1'	Variável	Header do subgrupo biométrico (BHT)
'80'	02	Versão da header
'86'	02	BDB product owner, product type (2 números positivos concatenados)
'87'	02	BDB format owner (1 número positivo)
'88'	02	BDB format type (1 número positivo)
'5F2E'	Variável	Bloco de dados biométrico (formato definido pelos dois anteriores)

4.1.6 Data group 10

Este grupo é responsável por guardar os dados obrigatórios mDL, sendo identificado pela *tag* '62' e o identificador '0A', seguido pelo comprimento total do grupo. Seguem-se então os seguintes parâmetros:

Tag	Comprimento	Valor
02	01	Versão do mDL
'5F28'	07	Data do último update. Timestamp em UTC, no formato YYYYMMDDhhmmss
'5F2B'	07	Data de expiração do mDL. Timestamp em UTC, no formato YYYYMMDDhhmmss
'5F38'	07	Data do próximo update. Timestamp em UTC, no formato YYYYMMDDhhmmss
'5F39'	Variável	Informação de gestão mDL para autoridades, string de octetos

4.1.7 EF.COM

Este grupo de dados é responsável pelo armazenamento da versão da estrutura de dados lógica e a lista de *tags* correspondentes aos grupos de dados presentes na implementação do mDL. O EF.COM é identificado pela *tag* '60' e o identificador '1E', seguido pelo comprimento total do grupo. Seguem-se então os seguintes parâmetros:

Tag	Comprimento	Valor
'5F01'	Variável	Número da versão em formato 'aabb', no qual 'aa' define o maior nível de revisão e 'bb' define o nível de lançamento. Ambos são numéricos e codificados como 2 bytes em formato BCD.
'5C'	Variável	A lista de tags de grupos de dados.

4.1.8 EF.SOD

O elemento EF.SOD é um documento de segurança identificado pela *tag* '77' e o identificador '1D'. Trata-se de uma assinatura digital gerada através da concatenação das assinaturas de todos os restantes elementos presentes, em formato DER.

4.1.9 EF.GroupAccess

O grupo EF.GroupAccess contém a informação de quais dados estão disponíveis a um leitor mDL, sendo identificado pelo identificador '18'. Este contém apenas a *tag* '04', o comprimento dos dados e uma *string* de octetos correspondentes aos grupos de dados a que o leitor tem acesso, bem como as respetivas *tags*. Como este elemento é dinâmico, a sua *hash* não está presente no ficheiro EF.SOD.

4.2 Compact encoding

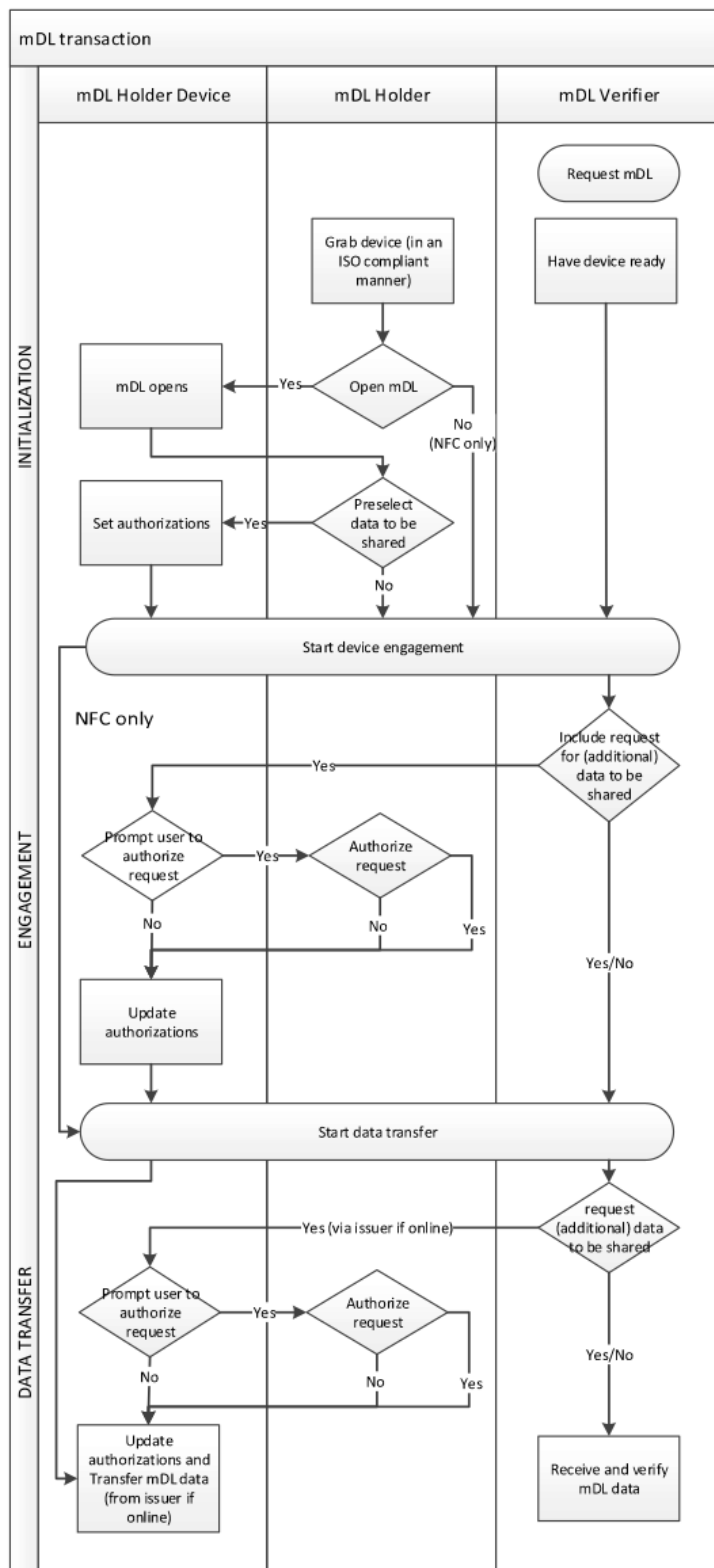
O *Compact encoding* é o esquema de dados utilizado na transferência de informação por meio de uma interface ótica, tais como códigos de barras ou fitas magnéticas. Estes requerem

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

6.1 Controlos de segurança

6.1.1 Autenticação Passiva (ISO/IEC 18013-3)

A autenticação passiva tem como objetivo confirmar que a *machine-readable data* não foi alterada desde que a IDL (ISO-compliant driving license) foi emitida.

Na prática, este mecanismo é implementado usando criptografia de chave pública (assimétrica) para produzir assinaturas digitais sobre *machine-readable data*.

De facto, se for usado *standard encoding*, a *machine-readable data* deve incluir:

- uma *message digest* de cada grupo de dados presente na IDL;
- uma assinatura digital relativa à coleção de todas as *message digest*. Esta assinatura deve usar a chave privada da autoridade emissora (IA).

Posteriormente, quando uma autoridade de leitura (RA) tentar aceder ao conteúdo da IDL, esta deve realizar os seguintes passos:

- verificar a assinatura digital utilizando a chave pública da IA;
- computar o *message digest* para cada um dos grupos de dados que sejam de interesse e comparar o seu resultado com os respetivos *message digest* guardados no *machine-readable data* do IDL.

Desta forma, após os passos anteriores estarem concluídos, a RA pode considerar que os grupos de dados que quer ler são autênticos se:

- a assinatura digital verifica;
- os *message digest* calculados correspondem aos armazenados na *machine-readable data*;
- a RA está confiante que a chave pública, usada para verificar a assinatura, pertence efetivamente à IA que emitiu a IDL.

No entanto, caso algum dos passos anteriores não seja válido, então significa que pelo menos um dos seguintes aspetos aconteceu:

- a assinatura digital não foi verificada com sucesso;
- a chave pública usada não era a correta;
- os dados na IDL foram alterados.

Funções de Hash - Codificação *standard*

Para *standard encoding* a IA deve utilizar funções de hash presentes na seguinte lista:

- SHA-1 (apenas por compatibilidade)
- SHA-224

- SHA-256 (recomendada)
- SHA-384
- SHA-512

Um *message digest* é calculado para cada grupo de dados presente na IDL e armazenado na *machine-readable data*.

A mesma função de hash deve ser usada para todos os grupos de dados.

O cálculo do *message digest* deve ser aplicado à concatenação de todos os elementos de dados, presentes num dado grupo de dados, pela ordem especificada no ISO/IEC 18013-2.

Funções de Hash - Codificação compacta

Neste tipo de codificação não é realizado o cálculo do valor de hash para cada grupo de dados em particular. Desta forma, não é necessário o uso de funções de hash.

Método de assinatura - Codificação *standard*

A assinatura digital do IDL deve ser gerada sobre a concatenação dos *message digest* dos grupos de dados presentes. Para tal, a IA pode utilizar dois métodos de assinatura diferentes:

- ECDSA
- RSA

Por um lado, caso a IA opte pelo uso do ECDSA, então deve:

- usar ANSI X9.62
- incluir, de forma explícita, na chave pública os parâmetros de domínio da curva elíptica usados para gerar o par de chaves ECDSA. Assim, esta informação deve ser do tipo **ECParameters** (sem nomes de curvas e sem parâmetros implícitos) e deve incluir o *cofactor* opcional.
- garantir que os **ECPoints** estão no formato descompactado.
- garantir que o tamanho mínimo da ordem do ponto base seja 160 bits.

Por outro lado, caso a IA opte pelo uso do RSA, então deve:

- seguir o RFC 4055, ou seja, escolher o mecanismo RSASSA-PSS (recomendado) ou o RSASSA-PKCS1-v1_5.
- garantir que o tamanho mínimo do *modulus* (*n*) é 1024 bits.

Assim sendo, a IA, além do **EF.COM** e dos grupos de dados mencionados no ISO/IEC 18013-2 (DG1 até ao DG11), deve adicionar um SOD para incluir as hashes individuais de cada grupo de dados e a assinatura digital no IDL. O SOD deve ser do tipo **SignedData** (RFC 3369) e deve ser produzido no formato DER.

Método de assinatura - Codificação compacta

Neste tipo de codificação, a assinatura digital é gerada sobre a totalidade dos dados, ou seja, desde o DG1 até ao DG12 sem contar com o DG.SOD e o cabeçalho. O valor é depois armazenado no DG.SOD.

O método usado para assinar deve ser o ECDSA com uma ordem de tamanho mínimo de 224 bits. Além disso, de forma a reduzir o armazenamento necessário para os parâmetros de domínio deve ser usada uma das seguintes curvas:

- P-224
- P-256
- P-384
- P-521
- brainpoolP224r1
- brainpoolP224t1
- brainpoolP256r1
- brainpoolP256t1
- brainpoolP320r1
- brainpoolP320t1
- brainpoolP384r1
- brainpoolP384t1
- brainpoolP512r1
- brainpoolP512t1

Na prática, o elemento DG.SOD deve ser composto pelos seguintes campos:

- DG.SOD.1: assinatura digital (codificada em DER)

SEQUENCE ::= { r INTEGER, s INTEGER }

- DG.SOD.2: chave pública
- DG.SOD.3: identificador da curva

Posteriormente, este campo deve ser adicionado aos restantes na seguinte ordem:

```
[header] x [Data Group 1] x [Data Group 2] x [Data Group 3] x
[Data Group 4] x [Data Group 7] x [Data Group 11] x
[Data Group 12] x [DG.SOD.1 length] [digital signature] x
[DG.SOD.2 length] [public key] x [DG.SOD.3: named curve]
```

6.1.2 Outros mecanismos

Além dos mecanismos de segurança anteriormente mencionados, existem ainda outros, como:

- **Autenticação ativa.** Tem como objetivo confirmar que o *secure integrated chip* (SIC) foi emitido juntamente com a *machine-readable data*.
- **Proteção de acesso básico (BAP).** Tem como objetivo verificar que o IS tem acesso ao *proximity integrated circuit card* (PICC) antes de aceder aos dados guardados no seu interior. Adicionalmente, o BAP assegura que a comunicação entre o IS e o PICC é protegida.

- **Proteção de acesso estendido (EAP).** Tem como objetivo permitir o acesso condicional autenticado a certos grupos de dados.

Apesar destes mecanismos se encontrarem no documento ISO, utilizam dispositivos físicos em algum momento do seu processo. Dado que o objetivo é focar num sistema completamente digital optou-se por não aborda-los.

6.2 Controlos de privacidade

6.2.1 Consentimento do utilizador

O acesso, por parte de um dispositivo de leitura, aos dados guardados numa mDL, apenas deve ser permitido depois do consentimento (implícito ou explícito) do titular do mDL.

Os métodos para o consentimento do utilizador não fazem parte dos temas abrangidos neste documento.

Com o objetivo de proteger a privacidade do titular do mDL, aplicações do governo não devem rastrear os movimentos de indivíduos através de *geo tagging*.

7 Implementação da mDL (ISO *compliant*)

8 Conclusões

Referências