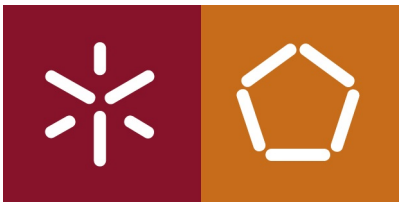

Universidade do Minho

Mestrado Integrado em Engenharia Informática

Engenharia de Segurança

Mobile Driving License (mDL)

Autores

João Sousa (A77768)

Francisco Araújo (A79281)

19 de Junho de 2019

Conteúdo

Resumo

Este documento diz respeito ao projeto proposto na unidade curricular de Engenharia de Segurança da Universidade do Minho, cujo objetivo consiste em analisar os documentos associados ao mobile driving license(mDL), bem como identificar os vários algoritmos, primitivas criptográficas e workflows que garantem segurança dessa mesma mDL. Por fim é nos proposto implementar um verificador da mDL, que valida se a mesma se encontra bem construída e se é válida.

Ao longo do presente relatório iremos começar por fazer um pequeno resumo sobre a análise feita por nós aos documentos disponibilizados sobre o mDL. Posteriormente iremos identificar os diferentes algoritmos, primitivas criptográficas e workflows usados na segurança do mesmo, e por fim iremos falar sobre a nossa abordagem na implementação do verificador mDL.

1 Introdução

Este projeto tem como tema principal o aprofundar de conhecimento sobre o tema das mobile driving license(mDL). Para isto, será necessário recorrer à leitura dos vários documentos fornecidos pelo professor de modo a poder extrair o máximo de informação. Posteriormente este trabalho tem também como objetivo a implementação de um verificador da mDL.

2 Análise aos documentos sobre o mobile driving license (mDL)

O projeto do mDL surge devido ao desaparecimento dos documentos de identificação, como hoje os conhecemos, isto é, em formato físico. Com o avanço recente da parte tecnológica esses mesmos documentos de identificação irão ser desmaterializados, podendo as pessoas recorrem ao mesmo a partir de um dispositivo móvel. A construção deste tipo de documentos segue diversas regras específicas bem como é necessário diversos algoritmos e primitivas criptográficas.

2.1 Introdução

O documento **ISO/IEC 18013**, que por sua vez possui vários documentos, e que foi por nós analisado, tem como propósito a emissão de um documento(IDL) que tem como finalidade servir de licença de condução, abrangendo a licença de condução tanto a nível nacional como a nível internacional, seguindo certas diretrizes definidas pela entidade *ISO*.

O intuito de guardar esses dados neste tipo de *standard*, prende se com o facto de aumentar assim a produtividade, facilitar a troca eletrónica dos dados e ajudar na validação da autenticidade e integridade dos mesmos.

O documento por nós analisado de forma mais aprofundado e que vai ser abordado maioritariamente foi o **ISO/IEC18103-5**, apesar de haver no entanto certas informações retiradas dos outros documentos, tem como objetivo a definição de certos padrões de forma a construir uma aplicação de mDL, isto é, criar um exemplo de uma cartão de condução digital.

2.2 *ISO/IEC 18013-5*

Este documento, tal como em cima já foi mencionado, standardiza um conjunto de especificações de forma a poder implementar a cartão de condução num dispositivo móvel(mDL) de modo a que outras entidades que não a entidade emissora possam para um determinado conjunto de informações que o titular dá o respetivo consentimento possam:

- Obter informações do mDL;
- Verificar a integridade da informação mDL;
- Autenticar a origem das informações mDL, entre outras;

Antes de entrar numa parte mais técnica é necessário ter presentes algumas definições que vão ser usados, e que serão importantes de modo a entender melhor todo o processo.

- **IDL** - licença de condução emitida em conformidade com o *ISO/IEC 18013*

- **dispositivo eletrónico** - dispositivo eletrónico com uma interface de utilizador, que permite armazenar informação/dados mDL, e permite partilhar essa mesma informação com um leitor, com consentimento por parte do titular.
- **mDL** - tipo eletrónico de um mDL conforme os requisitos presentes no documento.
- **mDL Reader** - dispositivo portátil ou *desktop* que permite trocar dados com um mDL.
- **mDL Holder** - indivíduo a quem é emitido um mDL. É o titular legítimo dos privilégios de condução presentes no mDL.
- **cartão** - documento com dimensões nominais de acordo com o *ISO/IEC 7810 ID-1*.
- **elementos de dados** - dados que podem aparecer na carta de condução de um humano ou legível numa máquina.
- **dados legíveis por máquinas** - dados ou informações que estão codificados dentro de uma máquina legível, como uma fita magnética, código de barras, circuitos integrados.

2.2.1 Visão Global

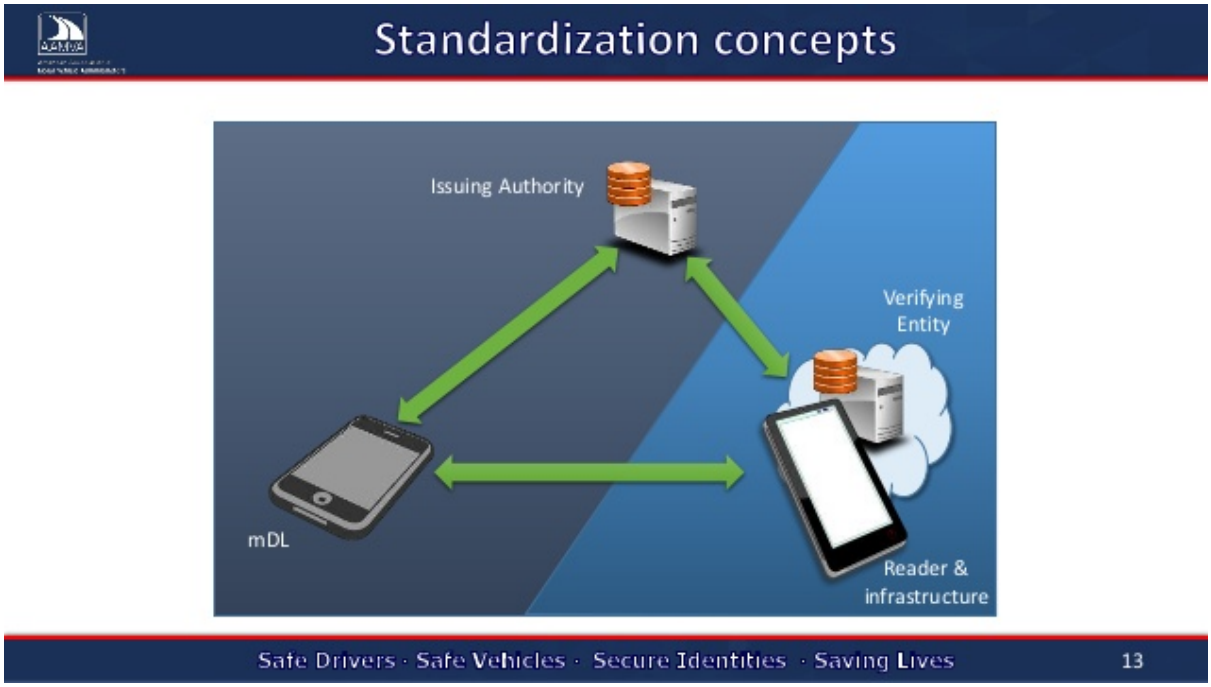

Figura 1: Digarama global do mDL

2.2.2 Requisitos funcionais

Na imagem acima apresentada, podemos ter uma noção concreta do ecossistema relativo ao à construção de um mDL, onde a solução tem de ser capaz de cumprir determinados requisitos, tais como:

- Tem de ser capaz de funcionar durante a verificação num ambiente offline.
- Tem de ser capaz de funcionar durante a verificação num ambiente online.
- Inclui mecanismos ou abrange uma arquitetura que permite aos *stakeholders* do mDL estabelecer confiança na informação fornecida pelo mDL.
- Confirmar a ligação entre um mDL e o titular do mesmo.
- Permitir a leitura de informações entre as autoridades de emissão.
- Permitir que o titular do mDL autorize seletivamente a libertação de informações a partir de um mDL para um mDL Reader.

Existem ainda requisitos devem ser tratados por parte da entidade emissora, mas que não serão abordados com mais profundidade:

- Mecanismos e tecnologias de armazenamento de dados mDL.
- Suporte remoto para o titular do mDL para gestão da aplicação.
- Endereço de consentimento do utilizador para o titular do mDL controlar a interação online com um sistema de entidades emissoras

Por fim, é importante salientar a existência de mais alguns requisitos funcionais, neste caso relativos ao mDL Reader, que permitem a este garantir a verificação confiável de um mDL:

- Disponibilidade dos dados de verificação(ex: certificados digitais) de autoridades emissoras.
- Ler sequência de dados mDL.
- Verificar sequência de dados mDL.

2.2.3 Requisitos técnicos

Nesta secção, iremos abordar mais profundamente os requisitos técnicos que devem ser levados em conta, para uma correta construção do mDL, na interface existente entre o mDL e o mDL Reader, sendo estes requisitos divididos em três pontos essenciais que são a estrutura de dados lógica dos dados transferidos entre o mDL e o mDL Reader, o protocolo de comunicação para transferência desses mesmos dados e por fim os mecanismos de proteção a serem aplicados de modo a preservarem a integridade, confidencialidade e autenticidade dos dados mDL.

Estrutura de dados lógica:

- Inclusão obrigatória de uma imagem do dono.
- Elementos de dados adicionais sempre atualizados.
- Identificador adicional indicando o factor "forma".
- Grupos de dados adicionais, usados para transferência de informação seletiva. Estes inclui novos elementos de dados.

Protocolo de comunicação:

Camada de transmissão Visual Interface, Wi-Fi Aware, Internet, Bluetooth Low Energy(BLE).

Camada de aplicação Codificação standard para o mDL e Código de barras 2D, para "device engagement"e o equivalente para codificação compacta do mDL.

2.2.4 Estrutura de dados lógica

As estruturas de dados mDL são organizadas e definidas de acordo com o documento *ISO/IEC 18013-2*. Existem onze grupos de dados. Apenas um grupo de dados é obrigatório enquanto todos os outros são opcionais, um destes grupos é reservado para futuro uso do mDL. Em cada grupo de dados existem elementos desse grupo que podem ser obrigatórios ou não, podendo ainda cada elemento de dados ser indicado como tendo consentimento explicito para acesso do mesmo.

Iremos apresentar de seguida um exemplo de um dos grupos de dados que podem estar presentes no mDL. O grupo de dados 1 (DG1) é constituído por nove elementos obrigatórios e contém a seguinte informação:

Name	Fixed or Variable	Field Format/length/type	Example
Family Name	V	36AS	Smith-Williams
Given Names	V	36AS	Alexander Geroge Thomas
Date of Birth(yyyymmdd)	F	8N	19700301
Date of issue	F	8N	20020915
Date of expiry	F	8N	20070930
Issuing country(per ISO 3166-1)	F	3A	JPN
Issuing authority	V	65ANS	HOKKAIDO PREFECTURAL POLICE ASAHIKAWA AREA PUBLIC SAFETY COMMISSION
Licence number	V	25AN	A290654395164273X
Categories of vehicles/restrictions/conditions	V	ADNS	C1;20000315;20100314;93;<=;8000

Tabela 1: Tabela dos elementos presentes no DG1

Posto isto, todos os grupos de dados seguem o exemplo do acima apresentando para os elementos que os constituem.

2.2.5 Protocolos de comunicação

Para a comunicação entre o mDL e o mDL Reader existem duas opções para a transferência de dados mDL: o primeiro com a codificação *standard*, o segundo consiste na transferência da estrutura de dados através de codificação compacta.

2.2.6 Transações mDL

Uma transação mDL consiste em três fases: inicialização, dispositivo de emparelhamento e transferência de dados.

Durante a inicialização um mDL é aberto (pelo utilizador, ou pela tecnologia NFC). O utilizador durante este processo pode, opcionalmente, autorizar certos elementos de dados a serem partilhados.

Posteriormente, durante o emparelhamento de dispositivos, através de um QR Code ou NFC são usados para a transferência da estrutura de emparelhamento, de forma a configurar os dados de transferência para a próxima transferência. Os mDL Reader devem suportar as duas interfaces (QR Code e NFC).

Por fim encontra-se a etapa de transferência de dados onde a conexão entre os dois dispositivos para a transferência é efetuada. Nesta transferência pode ser efetuado através de um método offline ou através de um método online. Em qualquer um dos métodos usados, a conexão deve ser usada para solicitar o acesso aos elementos de dados através do mDL Reader. Aós o consentimento por parte do mDL Holder podem ser transferidos os elementos dos dados. Para este tipo de transferência, existem diversas tecnologias disponíveis tais como: *Bluetooth Low Energy(BLE)*, *Near Field Communication(NFC)*, *Wi-Fi Aware* e *Optical Interface*.

2.2.7 Mecanismos de proteção de dados mDL

A segurança dos dados mDL trocados entre entre um mDL e um mDL Reader deve preservar a integridade, confidencialidade e autenticidade dos mesmos. Estes mecanismos de proteção para implementação estão especificados no *ISO/IEC 18013-3* e que serão apresentados com mais pormenor mais à frente neste relatório, juntamente com as primitivas e algoritmos criptográficos em que se baseiam.

Os controlos de privacidade também devem salvaguardar a identidade e os direitos do mDL Holder assim como enquadrar as obrigações legais do mesmo.

Para concluir esta secção é importante referir que aceder aos dados guardados de um mDL através de um dispositivo que lê essa informação só deve ser autorizada após o consentimento por parte do mDL Holder. Estes métodos para o consentimento do utilizador são da responsabilidade da entidade emissora.

3 Mecanismos, primitivas criptográficas, algoritmos e workflows que garantem a segurança da mDL

Antes de aprofundar sobre quais os algoritmos, primitivas criptográficas que são usadas nos mecanismos de segurança de modo a garantir a integridade, confidencialidade e autenticidade dos dados usados a quando da construção do mDL, achamos por bem, de forma a compreender melhor o enquadramento do mesmo, alguns termos e definições que serão usados posteriormente.

- **active authentication** - mecanismo que usa informação guardada numa área segura dos circuitos integrados seguros (SIC).
- **basic access protection (BAC)** - mecanismo que confirma que um sistema de inspeção tem acesso físico a um cartão de circuito integrado próximo.
- **chip authentication** - protocolo de acordo de chaves que fornece autenticação a um circuito integrado seguro e a mensagens seguras.
- **clone** - cópia não autorizada exata de um ficheiro que tem as mesmas características de segurança das do documento original e não pode ser distinguido do legítimo.
- **compact enconding** - método de codificação usado quando a capacidade de memória disponível da aplicação do IDL não excede os 5Kb, aplica-se geralmente a tecnologias códigos de barra
- **DG** - coleção de elementos de dados relacionados.

3.1 Mecanismo de autenticação passiva

O propósito da autenticação passiva é confirmar que os dados legíveis pela máquina não sofreram alterações desde que a IDL foi emitida. Este tipo de mecanismo é implementado tendo por meio uma assinatura digital sobre os dados legíveis pela máquina, usando um par de chaves assimétrico.

Existindo duas formas de codificação, no caso da codificação *standard* um resumo da mensagem é calculado separadamente para grupo de dados e incluído nos dados legíveis pela máquina. Todos os resumos das mensagens são depois assinados digitalmente e essa mesma assinatura é adicionada aos dados. No caso da codificação compacta os resumos das mensagens não são calculadas separadamente, pelo contrário, o conteúdo dos dados presentes nos grupos de dados são diretamente assinados e essa mesma assinatura é adicionada aos dados legíveis pela máquina.

Quando a IDL é apresentada à autoridade de leitura, esta autoridade usa a chave pública da entidade emissora para verificar a assinatura digital. A autoridade de leitura gera o resumo das mensagens de cada grupo de dados e compara com as que se encontram armazenadas nos dados legíveis pela máquina.

A autoridade de leitura pode considerar o grupo de dados autêntico caso:

- A assinatura digital verifica.
- Se o resumo da mensagem é o mesmo que está armazenado nos dados legíveis pela máquina.
- Se a autoridade de leitura está confiante que a chave pública usada para verificar a assinatura pertence realmente àquela e autoridade emissora.

3.1.1 Funções de hash

Para a codificação *standard* deve-se escolher entre as seguintes funções de hash: SHA-1, SHA-224, SHA-256, SHA-384 ou SHA-512. No caso do da codificação compacta como não são calculadas os resumos da mensagens, não há necessidade de escolher uma função de hash excepto no mecanismo de assinatura digital.

3.1.2 Método de assinatura

A assinatura digital é realizada sobre a concatenação dos resumos das mensagens dos grupos de dados. Para o tipo de codificação *standard* devem se usar assinaturas baseadas em curvas elípticas(ECDSA) ou baseadas em RSA.

Para o tipo de codificação compacta a assinatura é realizada sobre todos os grupos de dados, desde do DG1 até ao DG12. Neste tipo de codificação deve se usar ECDSA, baseado em curvas elípticas, de maneira a reduzir o tamanho.

3.2 Mecanismo de autenticação ativa

O propósito da autenticação ativa é usar informação guardada na área segura de um circuito integrado seguro (SIC) de modo a confirmar que o SIC e os outros dados legíveis pela máquina foram emitidos conjuntamente, é de salientar que este tipo de mecanismos apenas se aplicam a circuitos integrados seguros.

Um dos protocolos existentes neste tipo de mecanismos, consiste num par de chaves SIC, a pública e a privada. A chave privada é armazenada na memória segura do SIC e não pode ser copiada, enquanto que a chave pública é armazenada na parte dos dados assinados sobre o SIC.

Neste tipo de mecanismo o SIC assina digitalmente um desafio arbitrário escolhido pelo sistema de inspeção, esse mesmo sistema fica convencido que o SIC é autêntico se e só se retornar a assinatura corretamente. Os algoritmos e as primitivas criptográficas usadas neste tipo de mecanismo são idênticas às usadas no tipo de mecanismo já acima mencionada.

3.3 Considerações

Existem diversos outros mecanismos de segurança que garantem a segurança do mDL, no entanto não serão aqui abordados, uma vez que em quase todos eles a maior parte são baseadas nos algoritmos/primitivas criptográficas dos mesmos que já foram em cima apresentados.

4 Implementação de um verificador da mDL

Nesta secção iremos abordar a implementação por nós desenvolvida de um verificador da mDL. Começamos por abordar a constituição do *verify.py*, neste ficheiro começamos por verificar se todos os elementos de dados presentes nos grupos de dados existentes na mDL se encontram construídos de forma correta, isto é, de acordo com o *standard* definido nos documentos analisados, esta verificação foi feita com base nos ficheiros que estão na pasta *data_ groups* e configurados de forma com o que está presente na pasta *configs*. Dentro desse mesmo ficheiro, por fim, verificamos se o certificado que assina a mDL emitida ainda se encontra dentro da validade e posteriormente é verificado se a datas presentes na mDL se encontram dentro dos limites, isto é, se a sua data de emissão está entre a data de validade do certificado.

Por fim verificamos se as *hash disgests* de cada grupo de dados e verificamos com a *hash disgest* do certificado de modo a verificar a autenticidade e a integridade, por meio da assiantura digital.

Relativamente ao *verify_ cert.py*, aqui verificamos se a data do certificado que assina a respetiva mDL se encontra expirada e se as datas presentes na mDL se encontram entre os limites das datas do certificado. Por fim é verificado a assinatura do certificado, verificando se a chave pública está associada aquela mesma entidade.

De modo a testar o verificador por nós desenvolvido é necessário, é necessário apenas correr o ficheiro *verify.py*.

Por fim, enviamos também um *script* qu se encontra na pasta *Certs* denominado *expriment_ v1.py*.

5 Conclusão e Trabalho Futuro

Durante a realização deste trabalho fomos adquirindo conhecimento sobre um tema sensível, tendo em conta que os dados presentes neste tipo de documentos são bastante sensíveis, podendo comprometer a identidade do titular da mesma e foi posto em prática, também conhecimentos adquiridos em unidades curriculares anteriormente lecionas.

No entanto nem tudo foi positivo, uma vez que a quando da análise dos documentos fornecidos pelo professor não foi possível ter uma ideia clara do tipo de standard usado, estando a informação um pouco confusa na nossa opinião.

Como trabalho futuro gostaríamos de poder implementar uma *trusted list* e uma *revogated list* de modo a quando da verificação da mDL verificar se os certificado que assinou a mesma é de confiança ou não.