Authenticating Taxicab Services[1]

Authors
Cesar Augusto Bonilla, MSc (Royal Holloway, 2014)
Keith Mayes, ISG, Royal Holloway

OVERVIEW

The taxicab service industry is undergoing a lot of changes with, for example, the introduction of booking technology and in some cases looser regulation of service providers. Unfortunately some of these changes may actually have decreased the safety of taxicab passengers, with serious incidents including sexual assaults, armed robbery and even kidnapping. Moreover, current taxicab booking applications do not provide sufficient security functionality in a usable form for the protection of taxi users. Here we propose the TAXI authentication scheme as a fast and convenient mechanism for users to authenticate taxicabs in the street, and thereby travel in safety.

Public transportation is one of the vital services in every modern city. A number of changes have been have introduced in this service over the past few years in order to improve efficiency. The provision of effective transportation for the increasing population living in urban areas is a major concern for local and national authorities. Taxicab services are an important part of the solution and in some countries they are an absolutely crucial means of transportation.

Some of these changes have decreased the safety of taxicab passengers. A classical example is the adoption of more deregulated schemes by local authorities to provide an additional supply of taxicabs and a reduction of taxi fares. These measures are well meaning, but cause a relaxation of the licence requirements for companies, drivers and vehicles, which may contribute in part to an increase in cases of sexual assaults robbery, kidnapping, illegal taxi service 'touting' and general decline in service quality.

Instead of enhancing the safety of taxicab passengers, the response from the market is the proliferation of applications in smart phones that are controlled by commercial companies aiming to increase profits. This aim is assisted by setting explicit lower requirements, below legal regulations, in order to enrol more taxicabs. This is one of the reasons why there is a need for an independent centralised system to protect passengers by authenticating the legitimacy of taxicabs and their drivers.

[1] This article is to be published online by Computer Weekly as part of the 2015 Royal Holloway info security thesis series. The full MSc thesis is published on the ISG's website.

In order to provide essential controls to ensure a consistent level of security in the provision of service, every taxicab should possess a device which can prove its identity. These devices should be hard to tamper with, in order to prevent any unauthorised attempt to access, modify or delete the data stored in them. The advantage of using conventional smart cards is that they are already considered tamper-resistant devices with a sufficient level of protection for use in other environments in which security is an essential requirement, such as banking and mobile communications.

The solution of providing an identity by means of smart cards would be useless, if passengers did not possess a mobile device to interact with them. Fortunately, there is an increasingly adopted technology called Near Field Communication (NFC). This supports communication with contactless smart cards, and it is implemented on a great number of smart phones, tablets and other mobile devices which passengers could use to validate the licences of taxicabs.

THE SOLUTION:

Using contactless smart cards and NFC-enabled devices as terminals, the TAXI mobile application can execute an off-line asymmetric authentication protocol.

The scheme's objectives

Based on the use of contactless smart cards and NFC-capable devices, the requirements for the proposed scheme started with the analysis of common characteristics of taxicab service around the world. As a starting point, the solution took into account different taxicab regulation schemes and the issues concerning their passengers. Firstly, three groups of security related requirements were defined: user safety, quality of service and system efficiency.

- User safety goals guarantee every user can verify the legality of taxicabs when they hire a taxicab in the street.
- Quality of service goals ensure a fair mechanism of evaluation of taxicab services which promotes the offer of a better service by taxicab companies and their drivers.
- System efficiency goals ensure the system will be scalable and operationally reliable, in spite of the fact that the number of customers and taxicabs will be increasing over time.

The TAXI Authentication scheme

The scheme is a hierarchical model where the local transportation authority certify the licence operator centres and, in turn, they issue licences to the taxicabs. The model guarantees the scalability of the scheme allowing the decentralisation of operational activities: issuing, renewing and revoking taxicab licences.

The model is based on digital signatures: the local authority holds a master key used to sign digital certificates of licence operators. After that, the operators sign the certificates of taxicabs. Therefore, passengers only have to possess the certificate of a local authority to authenticate legal taxicabs. A similar process is widely used by the banking card sector in cash and card machines, so that a public key/certificate is sufficient to authenticate a vast number of cards.

The authentication protocol is conducted between the NFC-capable device (e.g. user phone) and the smart card located on the taxicab door. The device retrieves two certificates from the smart card: the licence operator certificate and the smart card/taxicab certificate. As soon as it gets the certificates, the public master key (of the local authority) is used to verify the licence operator certificate, and then, it gets the public key from this digital certificate to check the legality of the taxicab certificate.

The TAXI Authentication protocol was designed as a modified asymmetric authentication protocol so that it could be used reliably off-line. As we did not wish to store sensitive secret keys in mobile apps a symmetric authentication protocol would have needed to be on-line; creating major issues around reliability, efficiency, scalability, network bandwidth and processing at authentication servers.

The System Architecture

Behind the authentication protocol there are seven processes that fulfil the system's objectives:

1. Administration of the Licence Operators. The Local Authority has the role of issuing, renewing and revoking licences to the Licence Operators.

2. Administration of the licences for taxicabs by Licence Operators. Licence Operators can be responsible for both issuing and withdrawing licences to taxi vehicles according to legal requirements. Vehicles should not be registered by more than one Licence Operator.

3. Up-to-date taxicab licences. Licence operators have the responsibility of communicating in real time which vehicle licences they have issued or revoked.

4. Control of users. The Local Authority manages the user enrolment process and the status of updating revoked vehicle licences and valid licence operators in order to guarantee the trustworthiness of the authentication protocol.

5. The TAXI Authentication protocol. The user can check the Operator licence is valid and that the taxicab vehicle licence is not associated with revoked licences issued. It also notifies the Local Authority of the authentication event in order to track the user should any issue arise.

6. Quality of service evaluation. The process allows users to assess the quality of service provided by the taxicab preserving data confidentiality at all times.

7. Quality of service statistics. The Local Authority can evaluate the Licence Operator using the information extracted from the Quality of Service feedback left by users. Furthermore, it can send quality assessments to Licence Operators for every taxicab under their supervision.

Figure 01. The TAXI authentication protocol

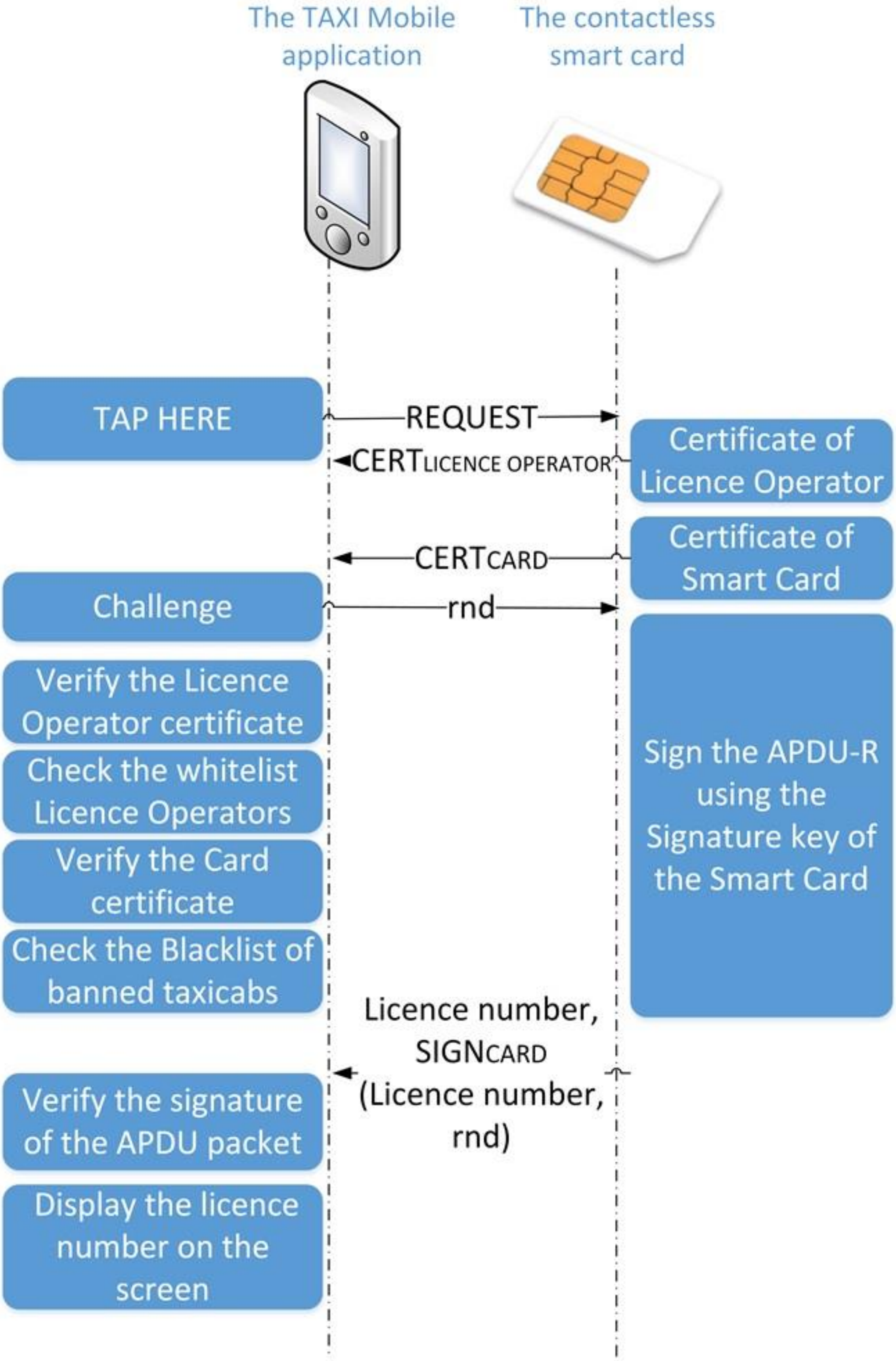
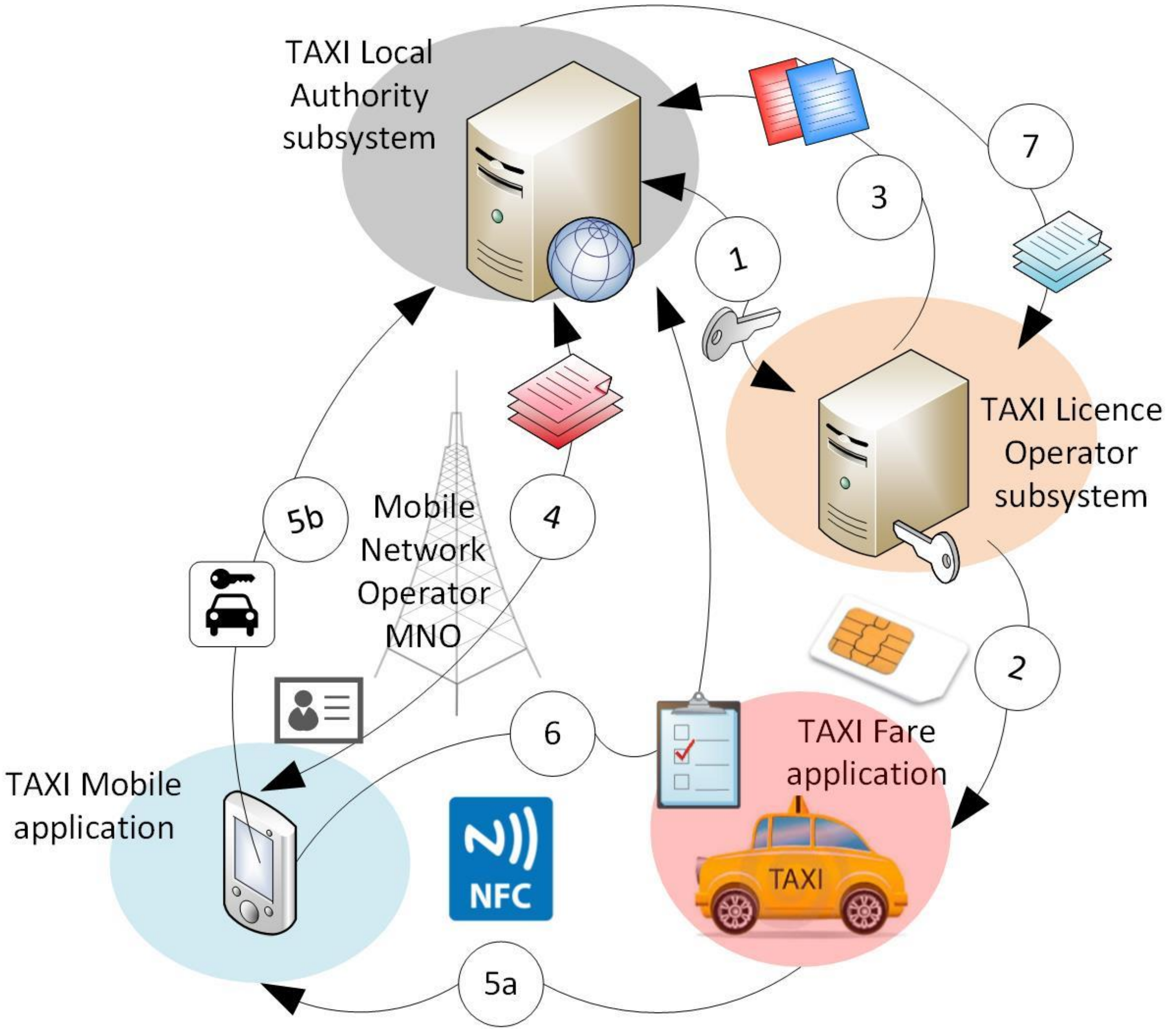

The TAXI Mobile application
The contactless smart card
TAP HERE
REQUEST
CERTLICENCE OPERATOR
Certificate of Licence Operator
CERTCARD
Certificate of Smart Card
Challenge
rnd
Verify the Licence Operator certificate
Check the whitelist Licence Operators
Verify the Card certificate
Check the Blacklist of banned taxicabs
Sign the APDU-R using the Signature key of the Smart Card
Licence number, SIGNCARD (Licence number, rnd)
Verify the signature of the APDU packet
Display the licence number on the screen

Figure 02. The TAXI Authentication scheme.


TAXI Local Authority subsystem
TAXI Licence Operator subsystem
Mobile Network Operator MNO
TAXI Mobile application
TAXI Fare application
TAXI
NFC
1
2
3
4
5a
5b
6
7

Conclusions

The ultimate goal of the TAXI Authentication scheme is to make taxi travel safer, more reliable and convenient for passengers. It can help to achieve this by detecting illegal taxicabs or forged taxicabs' identities; storing records of events to help police investigations; keeping up-to-date with revoked or expired licences; managing the quality of service evaluations of taxicabs and licence operators; controlling the issue of licences for vehicles supplying the taxicab service.

The implementation of the scheme is based on the increasingly accepted NFC technology and tamper-resistant contactless smart cards. Users wishing to benefit from TAXI protection would carry an NFC-enabled mobile device ready to communicate with the smart card placed on taxicabs. The application on the device would be kept up-to-date with public keys and revoked licences in order to correctly evaluate the authenticity of taxicab licences.

The authentication is carried out by an asymmetric authentication protocol, which means it works reliably off-line and supports scalability using digital certificates. The certificates establish the chain of trust where the validation of taxicabs is made upon licence operators' certificates, and these are validated by the local authority key.

Final thoughts

The taxicab service is changing rapidly incorporating new technologies to enhance its performance. This work contributes the design of a system architecture that would allow local authorities to control the safety and quality of taxicab services. The system is flexible to include other technologies such as Global Position System (GPS), which would help to establish where the nearest taxi is, where it was authenticated and that a particular user was present. The NFC phone could also be used as the payment device, linking to a stored electronic wallet or on-line account; removing some potential frauds and crimes relating to cash transactions.

Biographies

Cesar Augusto Bonilla received a B.Eng. in Information Technology Engineering from the National University of Colombia in 2006. He started work as an IT Engineer for an important Call Centre company providing telecommunication services to multinational corporations such as ING Finance Corporation. In 2009, he joined a multinational telecommunication company to develop security strategies to reduce fraud. In 2013, he joined the Information Security team at Bank of Bogota as a content developer and he won the Colfuturo scholarship award the same year. A year later, he received his M.Sc. in Information Security from Royal Holloway, and was an exhibitor at the Smart Card Centre Open Day. Currently he is working as a Network Engineer for F5 Networks EMEA.

Keith Mayes B.Sc. Ph.D. CEng FIET A.Inst.ISP, has spent much of his life working in/with industry, yet is also an active researcher/author with 100+ publications. He is Director of the ISG Smart Card Centre at Royal Holloway University of London and of Crisp Telecom Limited. He has worked in hardware/software development, DSP and sensors, standardisation, mobile communications, smart cards/RFIDs, embedded systems, systems modelling plus diverse aspects of information security. Current interests include (but are not restricted to) mobile comms and trusted execution technologies, NFC, Smart cards/RFIDs, transport ticketing systems, automotive security, m-commerce, attacks and attack resistant system implementations.