



Concept Note DVLA

A Concept Note of Using PKI to Mitigate Fraud in Licensing & Registration

Introduction

DVLA is the Vehicle Registration and Driver licensing authority in Ghana responsible for issuance of driver's licenses, issuance and renewal of vehicle registration certificates, and managing various functions around the same including but not limited to facilitation of verification of licenses, registration certificates, active insurance policies, etc for each applicable citizen or resident of Ghana.

In the current technological ecosystem, users with mal-intentions are able to get away with issuance and usage of fake driver's licenses, fake registration certificates, and non-insured vehicle (or drivers) thus causing a lot of harm to society, exposing risk (in terms of usage of such fake identification), and financial loss arising from money that is not paid but should be paid to the authorities and insurance companies.

Requirement Summary

Given the current gaps in the system, DVLA has an agenda to specifically address below points:

- Eliminate or significantly mitigate the probability of issuance of fake driver licenses
- Eliminate or significantly mitigate the probability of issuance of fake registration certificates
- Provide for an easy method of verification of driver's licenses and registration certificates using devices that are either connected to the internet, NOT connected to the internet, or enabled with SMS capability
- Track insurance policy issuance against a given driver or vehicle to ensure that at any given time, an active insurance policy provided by any insurance vendor or broker, exists
- Provide for a simple methodology to verify that a given vehicle or driver has an active insurance policy using a device that is either connected to the internet, not connected to the internet, or enabled with SMS capability
- Trigger various alerts to the driver/citizens informing them of registration due dates, insurance expiry dates, etc to ensure that they do not violate the law
- Provision of a mechanism that allows DVLA to hold perpetrators of system (within DVLA) legally accountable for improper and unethical actions

It is also understood that DVLA already has systems in place currently for issuance of driver license cards which are chip-based and registration certificates which are printed on normal or security paper. Further, it is also understood that DVLA systems at this moment, does not have any connectivity with the systems of any or all of the insurance providers in Ghana.

The Proposed Solution

The proposed solution is a multi-pronged solution, some of which involve PKI and others which do not.

Broadly, there are four elements to this solution which will be addressed at a high level in this concept note:

- Ensuring Insurance Policy exists against each vehicle (or driver) as per Ghana DVLA norms
- Ensuring authenticity of drivers licenses which are issued
- Ensuring authenticity of Registration Certificates and Insurance Policies which are issued using bar code (online/offline) and/or SMS
- Triggerring of Alerts to drivers on insurance policy renewal due dates, registration renewal due dates, etc.
- Legal accountability of improper user actions within DVLA

The above 4 points would be the 4 major items which the proposed solution would need to address to ensure that the requirements of DVLA are adequately met.

Ensuring Existence of Insurance Policy

Note: We assume in this concept note that insurance is issued against the vehicle but conceptually, same would be applicable if it is issued to a driver.

There are multiple insurance companies in Ghana and various brokers who issue through an insurance company, various types of policies to Vehicles on the roads in Ghana. For the purpose of this initiative, the key stakeholders involved would be the underwriting insurance companies and DVLA.

An (Open) API would be built by eMudhra to which would allow multiple insurance companies to push data into the DVLA systems. Specifically, the API would capture at minimum, below parameters:

- Vehicle License Plate Number
- Vehicle Registration Number
- Primary Driver Name
- Driver License Number
- Insurance Policy Type (Code)
- Insurance Issuance Company
- Issuance Date
- Expiry Date

The above information would be stored in a separate table in a relational DB. The logic layer would do the calculation around whether a given vehicle has an active insurance policy at any given moment or not. Further, the logic layer will also be able to deny registration if insurance renewal is due within a short amount of time of registration renewal of vehicle.

An SMS channel can be initiated to the server with incoming requests in the format SMS: XXXX (phone number) X12345 (Vehicle number) OR 1234 5668 9012 (Driver License Number) to check whether Insurance Policy currently exists or not. Upon receiving this SMS based input, the logic layer will pull up the insurance records for a given vehicle or driver and then do a simple calculation to provide a Y/N output on whether insurance exists for that particular query.

API can be RESTful API.

Ensuring Authenticity of Insurance Policies (and Registration Certificates)

Insurance Policies

The first layer of security is to ensure whether a given vehicle or driver actually has an Insurance Policy or not. A simple SMS message can query the server and return to the police with a simple and easy Yes/No response to this question. However, let us think of a scenario where a driver has forged his friend's License Plate and Insurance Policy! In this case, a SMS based approach may not be sufficient in identifying him as a culprit. In this case, since all the variables check out, the person may escape despite having provided fraudulent documents and forging a license plate.

That is where eMudhra's Hybrid Secure QR comes into the picture. eMudhra's Hybrid Secure QR (HBQR) is a simple module which can be built into the insurance provider's systems. HBQR will digitally sign all the key data points in each Insurance Policy issued by a specific insurance company and subsequently generate a unique QR code for each policy. HBQR uses simple PKI to eliminate the chance of document forgery whereby a Police officer can scan the QR in any Insurance Policy and identify whether it was forged or whether it was actually generated by the insurance company. Further, they can even check the key values like the expiry date, issuance date, etc against what is on the document to ensure authenticity of each data point.

Using HBQR, there is zero chance of document fraud. HBQR works online and offline through a dedicated app which can be whitelabeled. In the HBQR instance, if a person happens to forge the license plate and the insurance policy, the fake insurance policy will be immediately evident to policy officer upon scanning the QR code because the officer would be able to verify whether the policy was issued by an authorized system.

Note: The SMS based solution may not address a scenario where an individual has forged someone else's license plate and insurance policy/registration certificate unless the car make, model, and color is the same. We have thought about this scenario and the same is covered in 'Ensuring authenticity of registration certificates and insurance policies' section of the document.

Registration Certificate

The registration certificate scenario would broadly follow the same principle as the insurance policy scenario but would be much simple as it is fully in control of DVLA systems. DVLA would have emCA installed on their premise which is capable of issuing Digital Signature Certificates. A single Digital Signature Certificate would be issued to the server (to the organization). This certificate would be used to sign all the key data in the registration certificate. The data points would at minimum be:

- Vehicle Number
- Driver License Number
- Issuance Date
- Expiry Date
- Vehicle Make
- Vehicle Model
- Vehicle Color
- Vehicle License Plate Number
- Driver Name

It can include other details that are critical. A unique QR code will be issued against each registration certificate which is printed. The same can be verified online/offline using a generic QR reader or a white labelled app (offline verification). A SMS channel will also be facilitated where a simple SMS can be sent as per X12345 (Vehicle no.) or 1234 5678 9012 (Driver license number) to ensure that an active registration certificate exists. The response will be in a Yes/No fashion or any alternate fashion as desired by DVLA.

Note: The SMS based solution may not address a scenario where an individual has forged someone else's license plate and insurance policy/registration certificate unless the car make, model, and color is the same. We have thought about this scenario and the same is covered in 'Ensuring authenticity of registration certificates and insurance policies' section of the document.

Ensuring Authenticity of Driver Licenses

The driver license authenticity is usually a pressing issue in many developing markets. Given the importance of the driver license as a form of authorized identification for many purposes, it is imperative that it is foolproof. eMudhra's emCA is ideally positioned to address this issue for DVLA. eMudhra's emCA is a Certificate Lifecycle Management Solution which can integrate with your existing CMS. eMudhra is also partnering with global leaders in CMS solutions and bring you a full-fledged solution with an integrated CMS as required by DVLA.

emCA will integrate with the CMS to issue a unique Digital Signature Certificate to each license which is issued. The certificate would have the details of the driver to whom it is being issued in addition to having the flexibility to determine the duration of validity of this certificate and ability to revoke the certificate at any given moment (on suspicion of terrorist activities, etc.).

Each license would hold the certificate in its chip which can be read by specific card readers to determine whether a given license is truly authentic and if so, to whom it has been issued. Each certificate is given a unique ID (and its corresponding user) and the solution gives immense flexibility in ensuring whether a license card is issued by a trusted system, is valid in the current date, and more.

Alerts

Perhaps a key aspect in putting in place a foolproof solution is to ensure that people do not cheat the system in the first place. To do so, it is imperative to ensure that alerts are going at the right time (and sometimes, multiple times) to the key stakeholders in the system. While this does not involve any PKI, eMudhra uses alerts in its own solutions extensively to enable preventive solutions rather than corrective solutions.

Based on the parameters defined by DVLA, eMudhra can enable relevant alerts in DVLA systems to ensure that people are aware of expiry of various documents/license well ahead of time and are aware of the steps they need to take ensure they act on a timely manner.

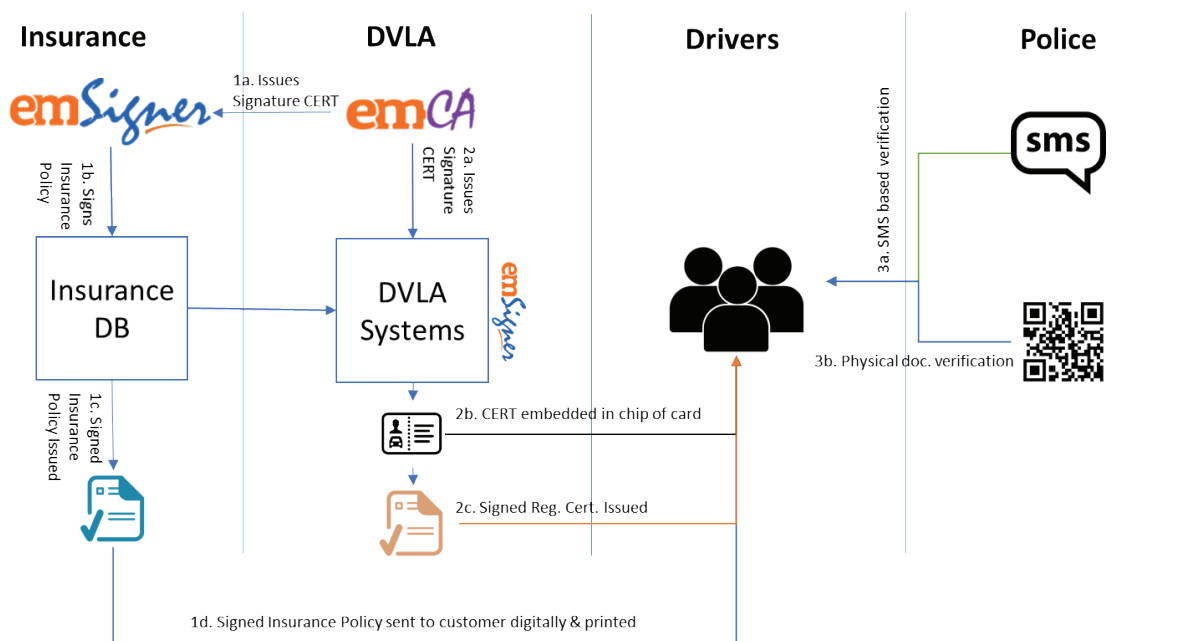
Managing Internal Fraud within DVLA

eMudhra's systems are planned not only to mitigate external threats but also internal threats. Admin folks sometimes, can be persuaded to perform the wrong deeds which could cost DVLA. To ensure that we are bringing legal admissibility for admin actions, eMudhra can enable digital signature based authentication and 'm out of n' access control to eMudhra's systems to ensure following:

- Anybody who performs a wrong deed can be held legally liable
- No single person has full control over the system

Authentication has an important role in any such solution and eMudhra enables multiple standard authentication scenarios which help our customers to put in place, adequate access level control. In case there is a higher and more sensitive requirement, eMudhra's emAS can cater to any complex and bespoke authentication scenario.

Flow Chart



Summary

In conclusion, PKI is crucial element in enabling the highest levels of accountability, preventive security, and mitigation of fraud in the current DVLA ecosystem. With the global Digital Transformation wave taking effect, having a PKI based architecture inside DVLA could lead a tremendous long term benefits. PKI is seen as a foundation for driving effective digital transformation due to its ability to preserve confidentiality, data integrity, identity, and due to the preceding three factors, legal accountability. It is also the most cost effective and scalable solution in the market today which is proven time and again to facilitate Digital Transformation.

eMudhra's emCA can form a foundation over which many applications can be brought by DVLA over time and offered to citizens in a Digital manner so as to improve user convenience. Further, as required, the CA system installed in DVLA could also at a later date, be signed by the National Ghana Root CA to bring full legal accountability in the system.

We see tremendous value to DVLA in using PKI and look forward to helping DVLA achieve their goals.

About eMudhra

Much like the name, which is an embodiment of the seal of authenticity in the electronic or digital world, eMudhra is a cyber security solutions company and a trust service provider that is focused on accelerating the world's transition to a secure integrated digital society. With presence in 5 continents and a global delivery center in Bengaluru, India, eMudhra is empowering secure digital transformation of over 45 global banks, several Fortune 100 customers and thousands of SMEs.

