emudhra
Trust Delivered

Concept Note
NIC

A concept note on Insurance Verification

fido ALLIANCE MEMBER
CAB CA/BROWSER FORUM
Webtrust Accredited
AATL
CLOUD SIGNATURE CONSORTIUM
Asia PKI Consortium
India PKI Forum

Introduction

The Office of the Commissioner of Insurance, Ghana is planning to engage in Digital Transformation measures to facilitate easier workflows, ensure authenticity of insurance documents, and provide for a multi-channel system for verification of whether a given driver has an insurance policy in place at any given point in time. The purpose of putting this system in place is to bring forth a standard of practice amongst all insurance companies and providers which allows for more transparency across the insurance and licensing ecosystem.

The greater levels of transparency between relevant systems in real-time is an important factor in ensuring that the right data points flow through the entire system from issuance of insurance policies to verification of whether insurance policies exist. Having such systems in place ensures adequate protection to all citizens, improves revenue of insurance companies, and enables greater level of enforceability of law in Ghana pertaining to non-existence of policies and fraudulent policies.

Requirement Summary

The Office of the Commissioner of Insurance has an agenda to specifically address below points:

1) Issuance of insurance policies with unique QR codes embedded with the insurance company's digital signature to ensure authenticity of printed documents

a. Note: This is important since the SMS based systems would not be able to identify perpetrators of the system (easily) who have forged the license plate and the policy certificate.

2) Provide for an easy method of verification of insurance policy authenticity and existence using devices that are either connected to the internet, NOT connected to the internet, or enabled with SMS capability

3) Triggering of various alerts to the driver/citizens informing them of insurance policy expiry dates, and other relevant updates

The Proposed Solution

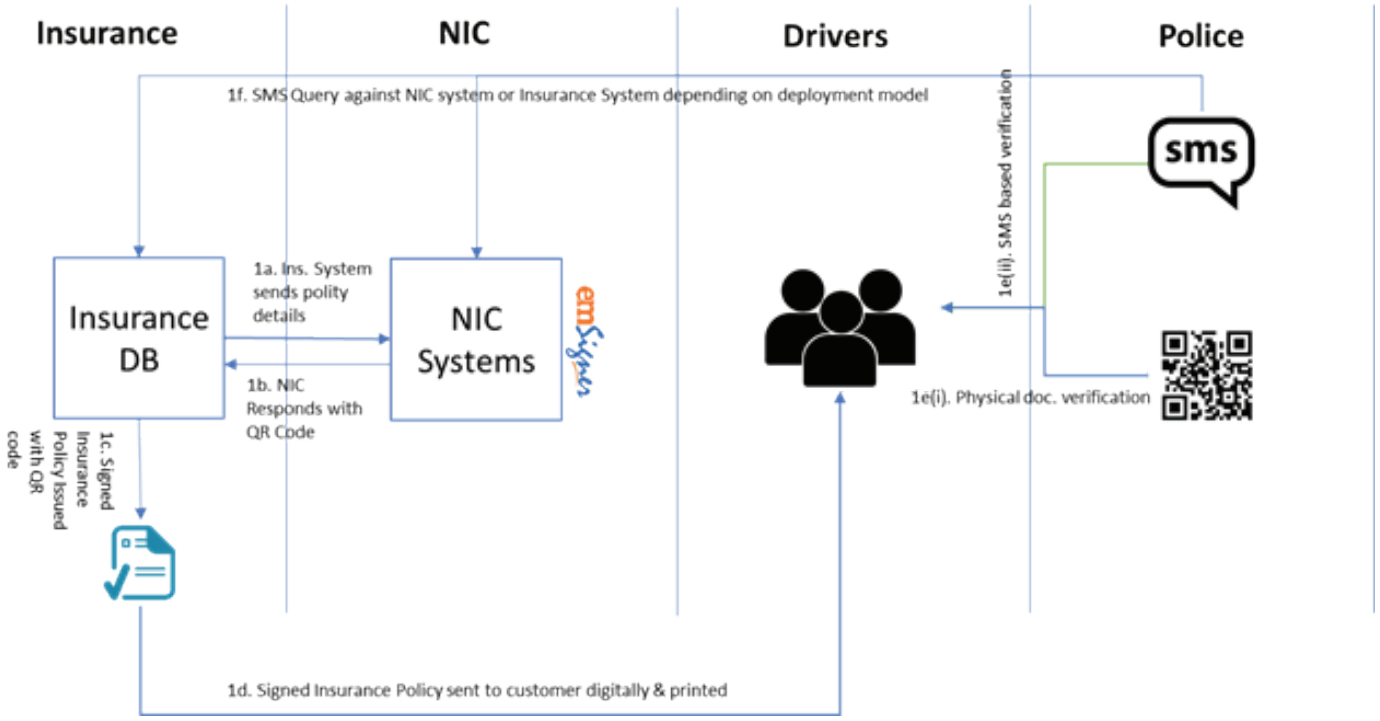
Issuance of Insurance Policies

A system will be deployed on the premise of the insurance companies (or alternatively, can be hosted by the National Insurance Commission and provided to Insurance Companies) whereby, a Digital Signature Certificate will reside in this system and sign all the insurance documents issued by all insurance companies. The Digital Signature Certificate used will be an ESS 256 bit signature, will be unique to each organization, changed periodically for each organization, and will be used to encrypt key data points in the insurance policy. The utility can be installed and integrated with the systems of the insurance company or can be hosted by NIC and provided as a service (or free utility) by NIC to the insurance companies. The relevant API's, connectors, etc will be provided by eMudhra.

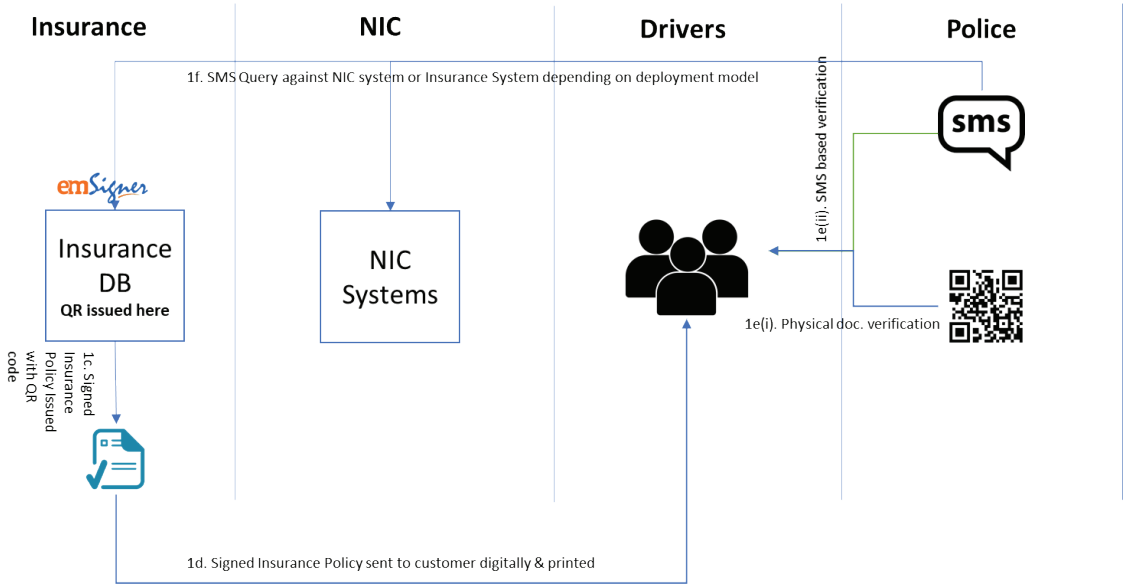
A digitally signed QR Code (Secure Hybrid QR Technology) will be printed on the insurance document. The QR code will be unique to each individual insurance policy issued.

The diagrams below would help in clarifying how the framework would operate on a hosted model (hosted by NIC) and on a non-hosted model where the utility is directly deployed at each insurance company. For those entities that have a manual approach to policy issuance, the utility can be extended to facilitate electronic issuance.

Hosted Model (hosted at NIC and integrated with third party systems)



On premise Model (Deployed directly into third party systems)



Verification of existence and authenticity of Insurance Policies using QR code

The QR code based approach is relatively, an easier way of verification of existence and authenticity of insurance documents. There is minimal interfacing and integration between systems required in this approach. Insurance companies can install their own version of the utility or push data to the NIC which can respond with the bar code to be printed on the document. There is also full legal accountability in the process and no possibility of fraud as the bar codes will be issued against each document (so values will not match if bar code is issued to wrong person or for wrong value), and authentication to the system (if hosted by NIC) can be managed through strong authentication.

Quite simply, for any officer willing to verify whether an insurance document exists and whether it is valid, he/she would have to request the driver to provide the insurance policy. Once the policy is in hand (in printed form or on mobile), the verifying officer can simply scan this code doing one of the following:

- Scan code using a generic QR Code reader – Internet connection would be required to verify document authenticity and authenticity of values in the document.
- Scan code using NIC App – This will work offline and will be able to verify document authenticity and authenticity of values in the document.

The response time in less than 2 seconds for online methodology and immediate for offline verification.

Verification of existence of Insurance Policies using SMS

There are two components to this solution. In order to verify the existence of an insurance policy and corresponding details of the policy, we need to facilitate the use of short SMS and query mechanism on the client side. More importantly, we need to define the back-end architecture in terms of the way the data will flow, where it will reside, and HOW it will be queried. Further, the volume can affect the type of DB we must use to ensure the best response times.

Client Side

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. The response format can be customized within the boundaries of the allowed number of characters by the SMS service provider (Usually approximately 180 characters)

Back End Structure

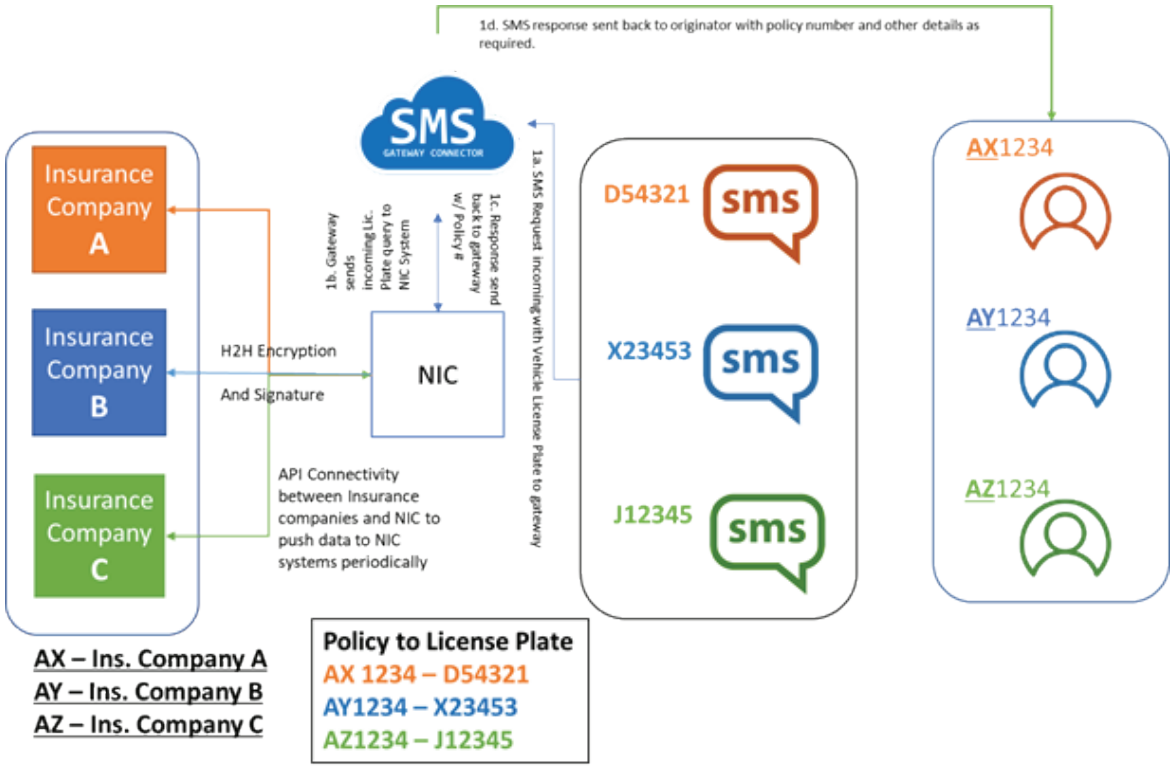
This is where further thought needs to be given to how the ecosystem will intercommunicate to enable quick querying. Broadly, the approach would be as described below.

Verification requestor sends SMS to NIC. NIC has all the insurance data which is updated on a daily basis from all insurance companies. Based on the license plate number, NIC queries its own DB to respond to the SMS query with specific details on insurance policies.

- In this instance, an API or data feed is required between insurance company's systems and NIC's systems to facilitate data sharing between systems
- It is preferred that all communication be digitally signed and encrypted for highest level of data protection and ensuring compliance with global data protection regulations
- Since the data volume will be high, back end DB architecture may use Mongo DB, complimented with an application layer to facilitate easy and quick querying and search

Please see the diagram below for a detailed flow of activities. Kindly note that the diagram is intended to provide an overview of the process. The actual framework used from a technical capacity would depend on the volume of data and estimated number of requests that the authority is planning to receive.

Though it is not captured in the diagram, for high volume use cases, we would recommend the usage of multiple instances of Mongo DB for distributed storage and easy querying. Further, we would also recommend multiple instances on the application layer to facilitate incoming requests, and re-direct such requests to the appropriate instance of the Database so as to enable to highest levels of performance and speed.



API Connectivity between NIC and Insurance Companies

An (Open) API would be built by eMudhra to allow multiple insurance companies to push data into the NIC 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 or in a distributed DB instance. The logic layer would do the calculation around whether a given vehicle has an active insurance policy at any given moment or not.

API can be RESTful API to keep with highest industry standards. The communication will be digitally signed and encrypted to protect the flow of personal data from third party attacks

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 the Office of the Commissioner, eMudhra can enable relevant alerts in the process on an SMS or email channel to ensure that people are aware of expiry of policies well ahead of time and are aware of the steps they need to take to ensure they act on a timely manner.

Summary

In conclusion, having such a system in place to complement the existing methodologies of insurance issuance and verification today would be a great value addition to the entire insurance industry and to the society financially, and otherwise. It is imperative to ensure that systems provide citizens and businesses with peace of mind and protection against threats, fraudulent activities, and other such elements which would deter promotion of business activities in the Insurance Industry and erode the value of insurance with regards to the public.

In line with eMudhra's core values, eMudhra sees this initiative as a key initiative aimed at betterment of society and is glad to be able to share its experiences in this domain to enable such betterment. The goal is already established by the Office of the Commissioner of Insurance, Ghana. However, this document serves to address the methodologies through which this goal can be achieved.

For any further clarifications, please reach out to your relationship manager for the quickest response from eMudhra.

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 isfocused 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.