1. **Understanding the Q-CERGEN**
   1. Overview of Features in Q-CERGEN

This is a software developed to generate E-Certificates in large numbers with security and online verification systems.

1. 1000 certificates can be generated in 5 minutes optimally.

2. Online verification system is embedded in each certificate, 3rd party can scan and verify online about the authenticity & details of the certificate.

3. The verification links are SHA-3 encrypted preventing any forgery.

4. Authorized login with surveillance, to keep track of who generated which certificate number. This helps in the accountability and tracing of lawbreakers.

5. Steganographic encryption as a second layer of security is hidden in the inner layer of the certificate. Decodable only by the institutional head.

6. Easy UI, certificate development from a template.

7. Place candidate images on the certificate, multiple dignitary's signatures, and QR code.

8. Application to access the data and rectify erroneous certificates.

9. Certificate data can be fed in XLSX, CSV, and Text file formats, containing thousands of rows and columns of data required.

10. The template, font, and style formats are reusable once created on any other computer where it's installed.

11. The data, font, style, and template formats are mapped and stored. The certificates can be generated when required instead of wasting storage space for certificate images.

* 1. Working of Q-CERGEN

The key feature of the invention is:

**CREATING ENCRYPTED LINKS**

* To begin with, user is asked to login if he/she already has an account
* If user is not registered, option is given to register the account
* Once the user is registered, he/she can login through the credentials
* User tokens are generated for every user at registration time.
* File upload option asks user to upload .csv/.xlsx file.
* Next alphanumeric codes will be generated (Datagram) which are further used for creating SHA-3 encrypted 256-Bit tokens.
* Finally append the static URL to the generated encrypted link and return the file to cloud server for further processing.

**VERIFICATION**

* After successful generation of certificate with QR code, scan the QR-Code for verification.
* Decoding of encrypted link happens at backend
* If decoding is successful query the database for the data, retrieve the data and display the same along with a header saying “VERIFIED”.
* If no data is found in the database, display “NOT VERIFIED” on the web page.

**CERTIFICATE GENERATION**

* Secured Login interface.
* Certificate template in format of .jpg / .png is chosen for generation
* Steganography security is embedded into the image, by hiding data inside the certificate generated. This is achieved by sophisticated image processing.
* This hidden code can also be used to verify the authenticity of the certificate issued.
* The encrypted links form the large data files of .xlsx / .csv are placed as QR codes on the certificate. These are scanned to verify the certificate issued.
* Values of the .xlsx file are formatted. Selection of location of the data on the certificate image, and also adjusting colour, size, and font type of the data.
* Images of recipients can be embedded with path of image pointing in the .xlsx file. The dignitary signatures can also be added in the generation time, instead of appending on the certificate template image.
* The complete process is logged, can be reused elsewhere to generate the same format certificates with new set of data.

**DATABASE**

* Access to verify and edit data.
* Erroneous data can be rectified.
* Keep a track of certificates generated, purpose and number.