Tech Stack

- Frontend: React.js
- Backend: Node.js, Express
- Database: MongoDB
- Version Control: Git/GitHub
- API Documentation: Swagger

Authentication

- Create a list of predefined emails in the database which can register on the platform.
- Users can only sign up with the predefined emails.
- Use HTTP Cookies for storing auth tokens on the frontend.
- Encrypt user passwords before saving them in the database with bcrypt.
- Create log out and log out from all devices functionality.

Admin

- Admins can read, create, update and delete certificates in the database.
- When admins upload a new certificate, a specific QR Code will be added to the first page of the certificate, which will lead to the certificate verification page.
- Save the uploaded and processed certificate PDFs in an amazon S3 bucket.
- Save the link of each PDF inside the database corresponding to each certificate.
- Admins can mark a certificate and update it as valid or invalid, by default a certificate will be valid.
- When a certificate's details are changed, the corresponding admin's user ID will be saved as history with it.

End User

- End user will land on a verification page by physically scanning the QR code on a certificate.
- On the verification page, a soft copy of the certificate will be displayed with the current status (valid/invalid) of the certificate.
- End user does not need any authentication.