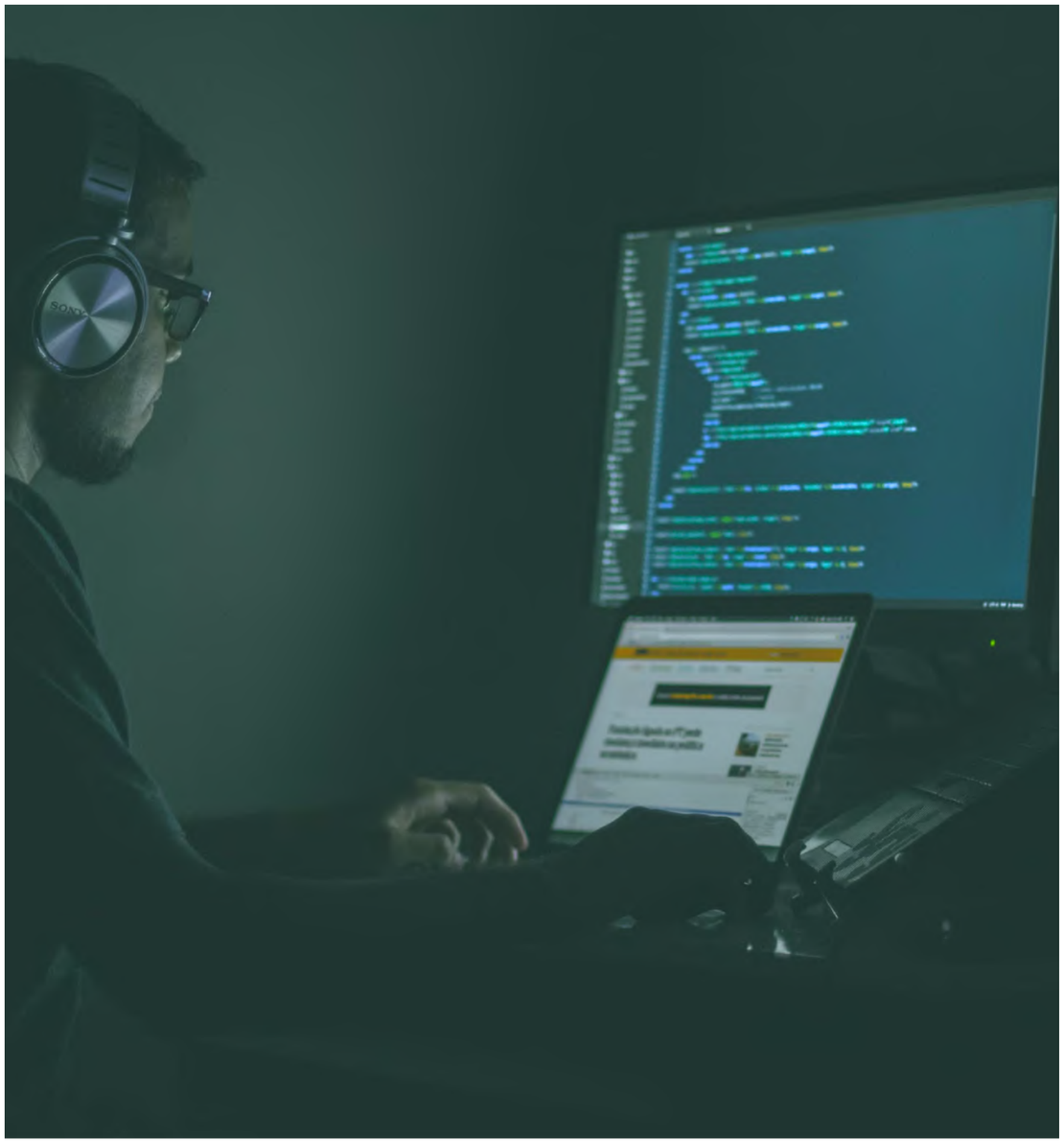
Dutch National Cyber Security Center

DEFENSE IN DEPTH



Secure system for managing cases of suspected internet crime in accordance with the national counterterrorism and cybersecurity policy

TABLE OF CONTENTS

Problem & Solution

What?

NCSC Netherlands coordinates enhancing the cyber resilience of the Netherlands in the digital domain. Our goal is to realize a safe, open and stable application by sharing knowledge in terms of current cyber threats and current IT solutions with local and federal governments.

AUGUST 2022

Why?

"Digital threat continues to grow" *1*

More powers for public authorities. A bill currently proceeding through parliament will authorize the police and prosecutors to:

- Arrest persons suspected of selling stolen digital data;
- investigate or hack into suspects' computers remotely, for instance, by installing software to detect severe forms of cybercrime;
- intercept data or make it inaccessible by blocking child pornography or intercepting email messages containing information about offences.

1

https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands

How?

NCSC App was built first and foremost by teamwork.

Our group carefully analysed the problem and developed a technical implementation using an array of Firebase products to support our front-end interface, which can be used by the NCSC Cyber Specialists.

Features

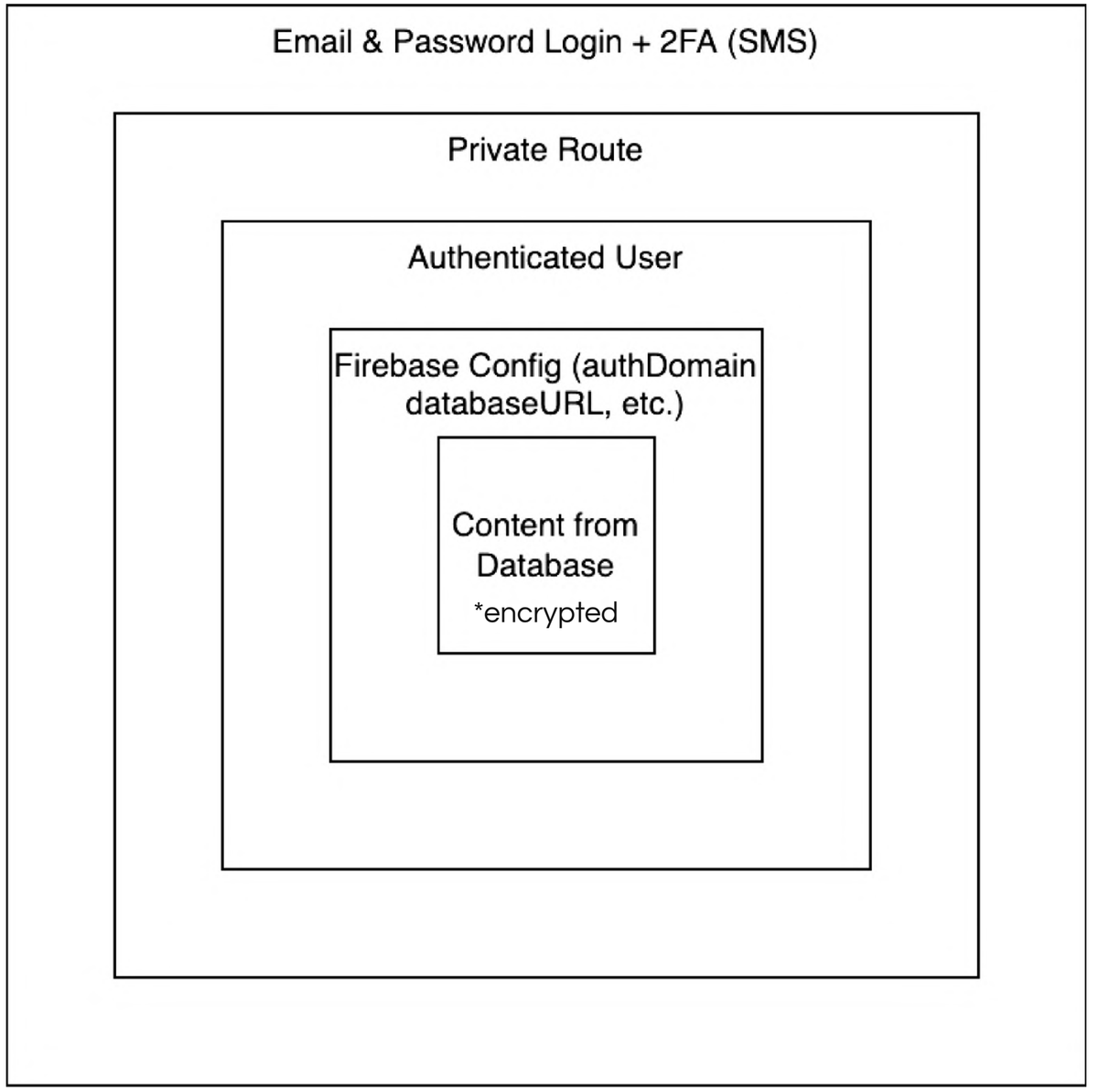
FEATURES

- User creation (Google Identity Platform - an extension of Firebase)
  - Setup for 2FA
- Login + 2FA
- Public & Private Reporting
  - CRUD
  - Private reports allow for more details during the creation
  - Report Lifecycle (To do, In Progress, Done, Declined)

FEATURES

- Authorities (can be assigned to reports)
  - CRUD
- IT Updates
  - Create
  - Read
  - Delete
  - There is no update option for IT Updates, as they are considered to be a form of a newsletter

Security Layers



SECURITY LAYERS

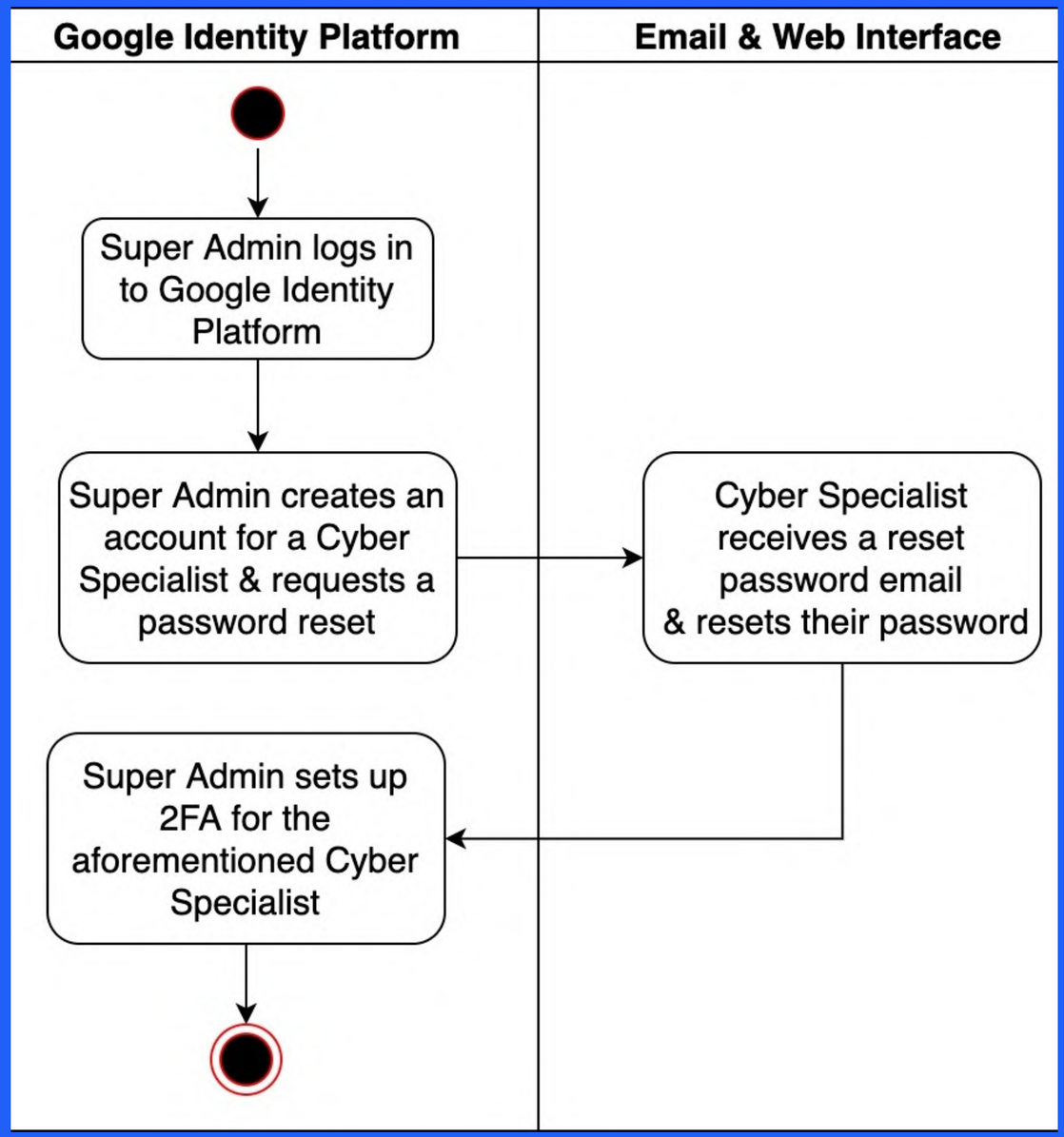
To protect the data in the NCSC app, we decided to implement multiple layers of security, which can be seen on the image on the left side.

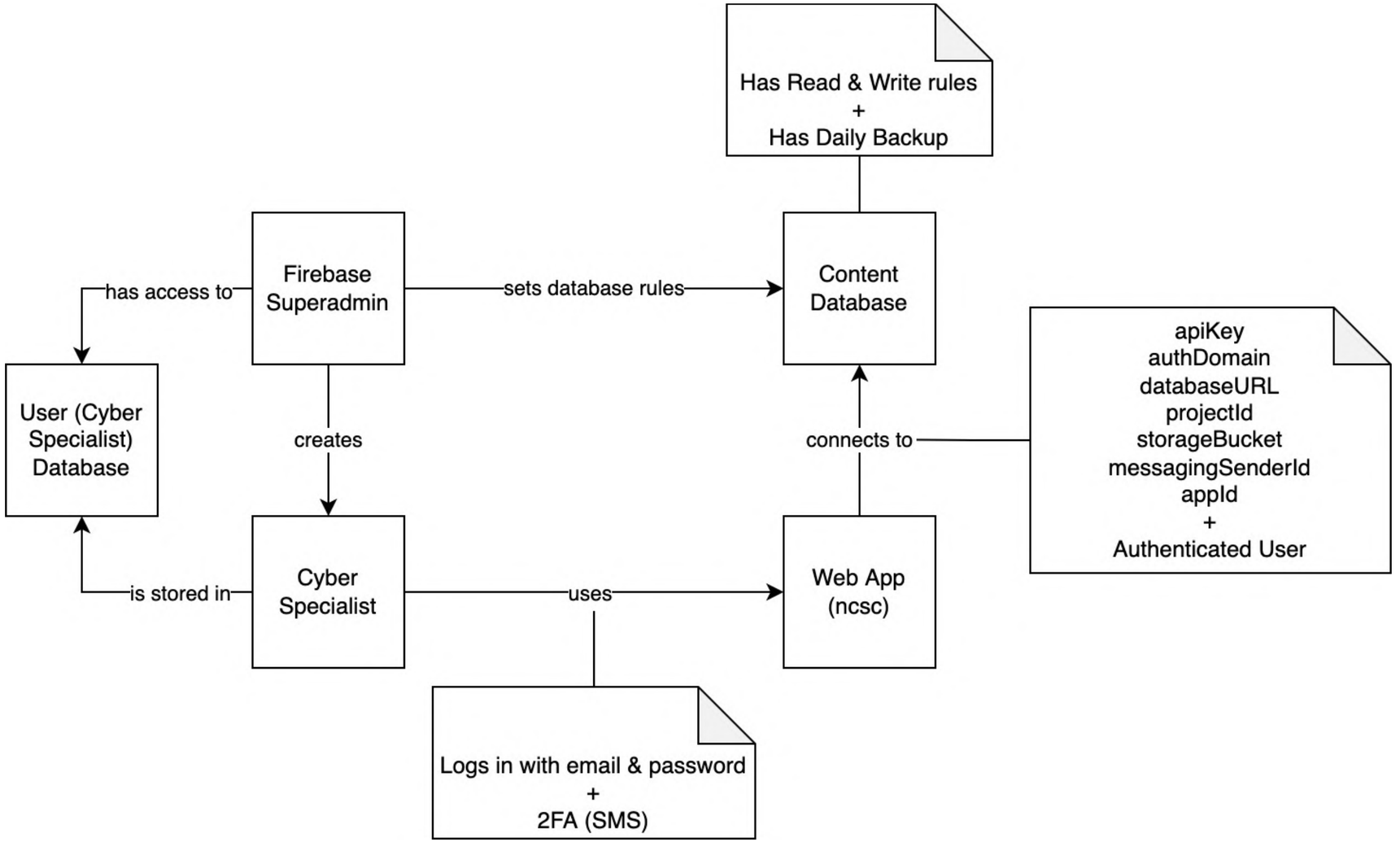
To reach the content, the following terms have to be fulfilled:

- Firebase config holds secret information like API key, database URL, etc.
- Check whether there's an authenticated user before making the call to the DB
- Protected route to the page, which allows only authenticated users to reach the page
- Users have to log in with email and password and confirm their login with 2-factor authentication in the form of an OTP sent in an SMS message.
- The web app has an SSL certificate, which transfers the data in a secure and encrypted way

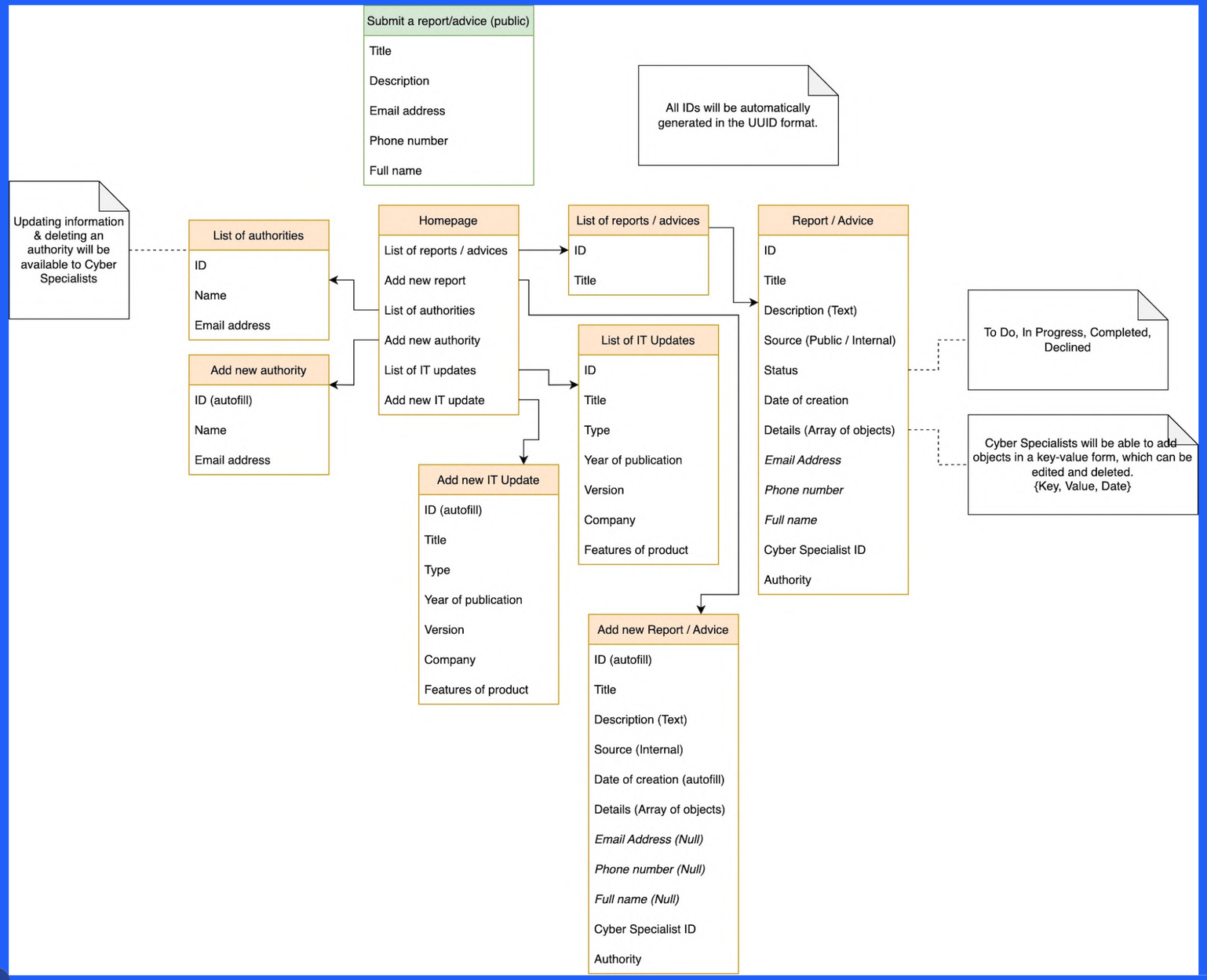
Process of creating a user with access to the NCSC dashboard

- This process includes both Super Admin and the Cyber Specialist
- Super Admin creates the account and requests a password reset
- Cyber Specialist resets the password
- Super Admin sets up the 2-factor authentication





This is a diagram explaining how the whole NCSC system is connected.



This is a sitemap for the NCSC web application.

It depicts the views/pages and their properties used in the app.

Q&A

Thank you