netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

Components & Encryption

COMPASS NUM-APP

19.04.2021

Objectives

After this session, you should be able to:

- differentiate between the different components of the NUM-App and their functionality
- explain how data protection is ensured in the NUM-App

netzwerk universitätsmedizin

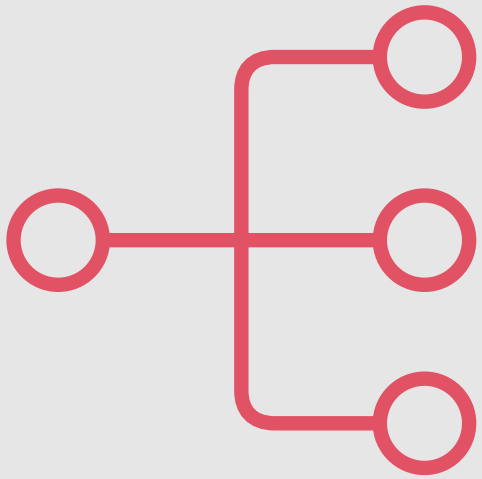
GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

Agenda

- Component
- Encryption – What? Why? How?
- Encryption in the NUM-App
  - Frontend
  - Backend
  - Downloader
- Q&A



netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

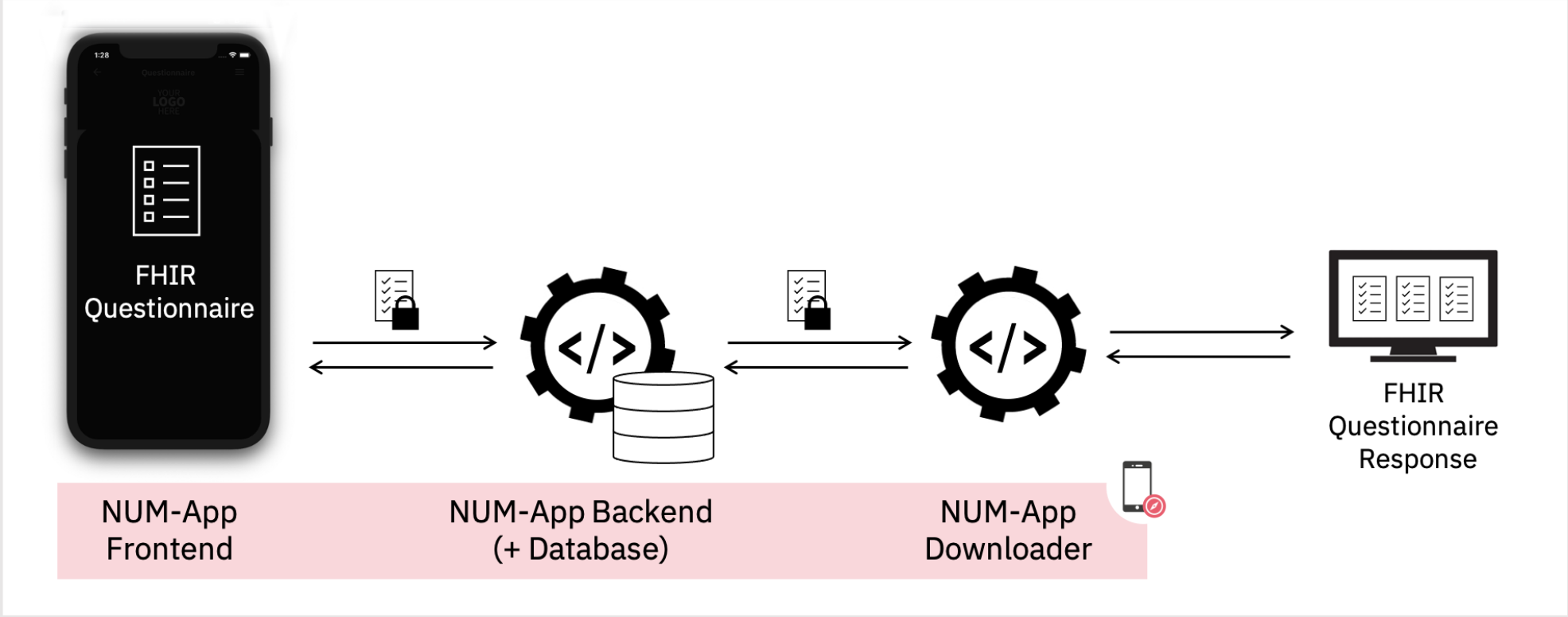
netzwerk universitäts medizin

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

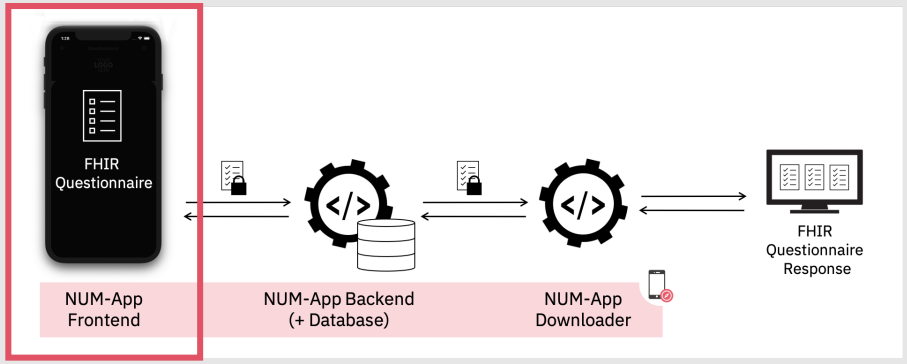
IBM

Components

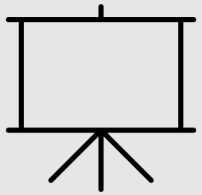
NUM-App Components



NUM-App Frontend

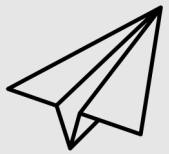


Login

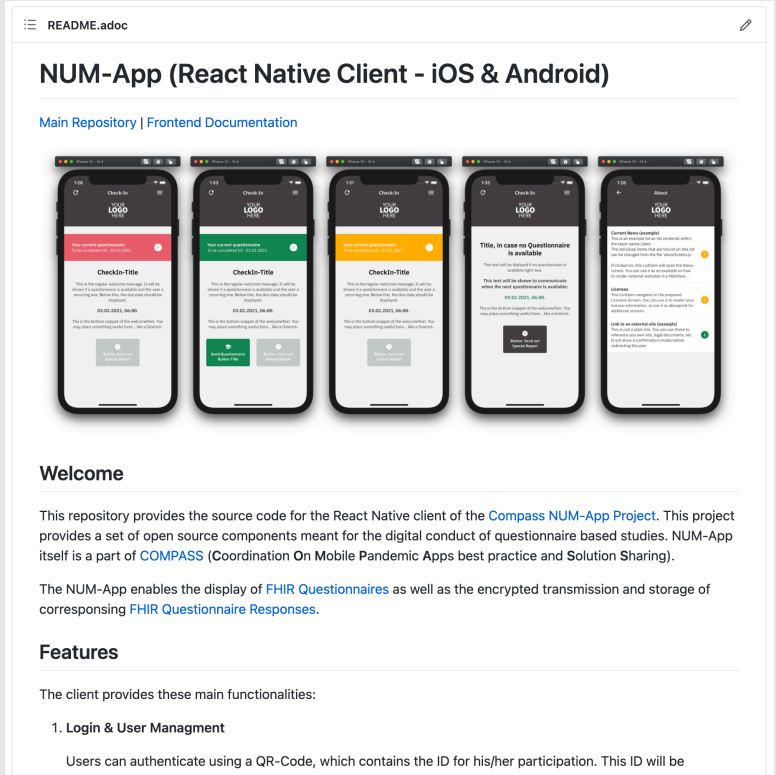


Display
FHIR questionnaire

Encrypt FHIR
questionnaire response



Submit FHIR
questionnaire response


README.adoc

NUM-App (React Native Client - iOS & Android)

Main Repository | Frontend Documentation

Welcome

This repository provides the source code for the React Native client of the Compass NUM-App Project. This project provides a set of open source components meant for the digital conduct of questionnaire based studies. NUM-App itself is a part of COMPASS (**C**oordination **O**n **M**obile **P**andemic **A**pps best practice and **S**olution **S**haring).

The NUM-App enables the display of FHIR Questionnaires as well as the encrypted transmission and storage of corresponsing FHIR Questionnaire Responses.

Features

The client provides these main functionalities:

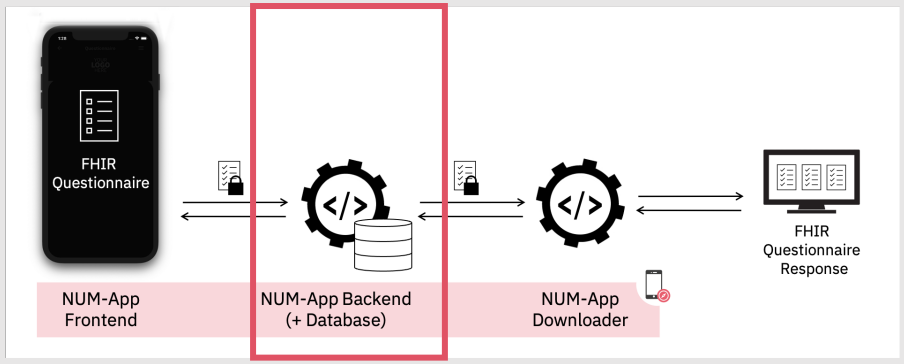
1. **Login & User Managment**

   Users can authenticate using a QR-Code, which contains the ID for his/her participation. This ID will be

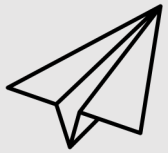
netzwerk universitätsmedizin

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

NUM-App Backend

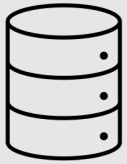


Login



Provisioning of
FHIR questionnaire

Signing of FHIR
questionnaire response



Storage of FHIR
questionnaire response

README.adoc

NUM-App Mobile Back End

Main Repository | Back End Documentation

Welcome

This repository provides the source code for the mobile back end of the Compass NUM-App Project. This project provides a set of open source components meant for the digital conduct of questionnaire based studies. The mobile back end itself is a part of COMPASS (**C**oordination **O**n **M**obile **P**andemic **A**pps best practice and **S**olution **S**haring).

The mobile back end provides study data for the NUM-App in form of FHIR Questionnaires. It also stores the study data that is uploaded from the mobile app. Additionally it makes the collected data accessible for other parties.

Development

Local Setup

- Make sure you have a recent version (LTS recommended) of Node.js installed and run the following commands to download and prepare this repository:

```
git clone https://github.com/NUMde/compass-numapp-backend.git
npm install
```

- In case you use VSCode as your editor, install the recommended extensions

Run the back end locally

Create .env file

Some configuration values need to be present as environment variables during runtime. The application loads a file with the name `.env` during startup, if it is present.

To get started copy the file `.env.sample` to `.env` and add your values.

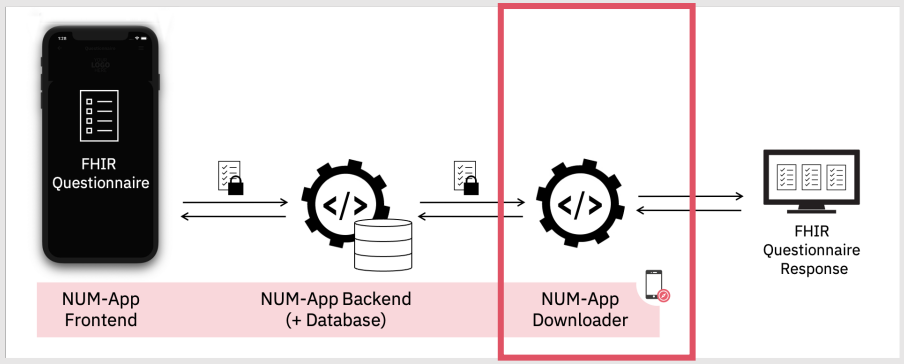
Generating RSA key pair

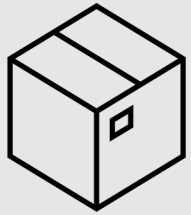
netzwerk universitäts medizin

GEFÖRDERT VOM

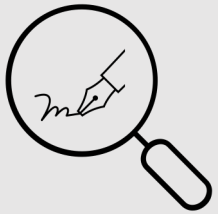
Bundesministerium für Bildung und Forschung

NUM-App Downloader





Retrieve latest FHIR questionnaire responses



Verify signature

Decrypt FHIR questionnaire responses

Delete retrieved FHIR questionnaire responses

README.adoc

COMPASS Questionnaire Response Downloader

Main Repository | Downloader Documentation

This Python project allows for an authenticated download of latest questionnaire response objects via the mobile backend. The retrieved objects are validated and decrypted.

Refer to the docs for detailed information on configuration and usage of the script as well as the download api.

Functionality

The script provides the following functions which are executed in the given order:

1. **Request of authentication token for requests to the mobile backend**: The authentication credentials are AES encrypted and the random key used for the latter is RSA encrypted. Both ciphers are submitted in request payload together with the random initialization vector used for the AES encryption.
2. **Using pagination, all current data is retrieved from the queue**: This action is performed via a request to the download api of the mobile backend. The responses are written to a file as the intermediate result. The response for every page contains a JWS token which is verified. If the RSA SHA 256 signature is valid, then the contained payload is extracted and used for further processing.
3. **Decryption of validated questionnaire responses**: The questionnaire responses which were validated in the previous step are decrypted (RSA PKCS#7) with the private key and certificate. The results are written to a file.
4. **Delete retrieved questionnaire responses from queue**: All elements that have been decrypted in step 3 are deleted via the mobile backend based on their UUID identifiers.

```
(base) ➜  compass-numapp-downloader git:(main) ✗ make docker-run
echo 'Logging to directory /Users/alenaschmickl/bin/COMPASS/compass-numapp-downloader/logs'
Logging to directory /Users/alenaschmickl/bin/COMPASS/compass-numapp-downloader/logs
docker run -v /Users/alenaschmickl/bin/COMPASS/compass-numapp-downloader/logs:/logs --name compass-downloader compass-numapp-downloader

########## (1/5) Getting authentication token

########## (2/5) Getting pages from queue

########## (3/5) Decrypting verified questionnaire response objects

########## (4/5) Writing dencrypted response objects to: logs/decrypted_questionnaire_responses.txt

########## (5/5) Deleting all decrypted questionnaire response objects
Deleted 1 objects
docker rm compass-downloader
compass-downloader
(base) ➜  compass-numapp-downloader git:(main) ✗ ls logs/
```


netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

netzwerk universitäts medizin

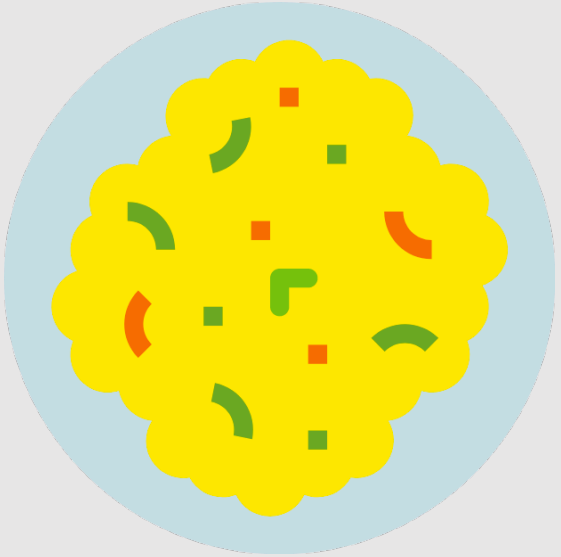
GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

Encryption
What? Why? How?

Encryption – What?

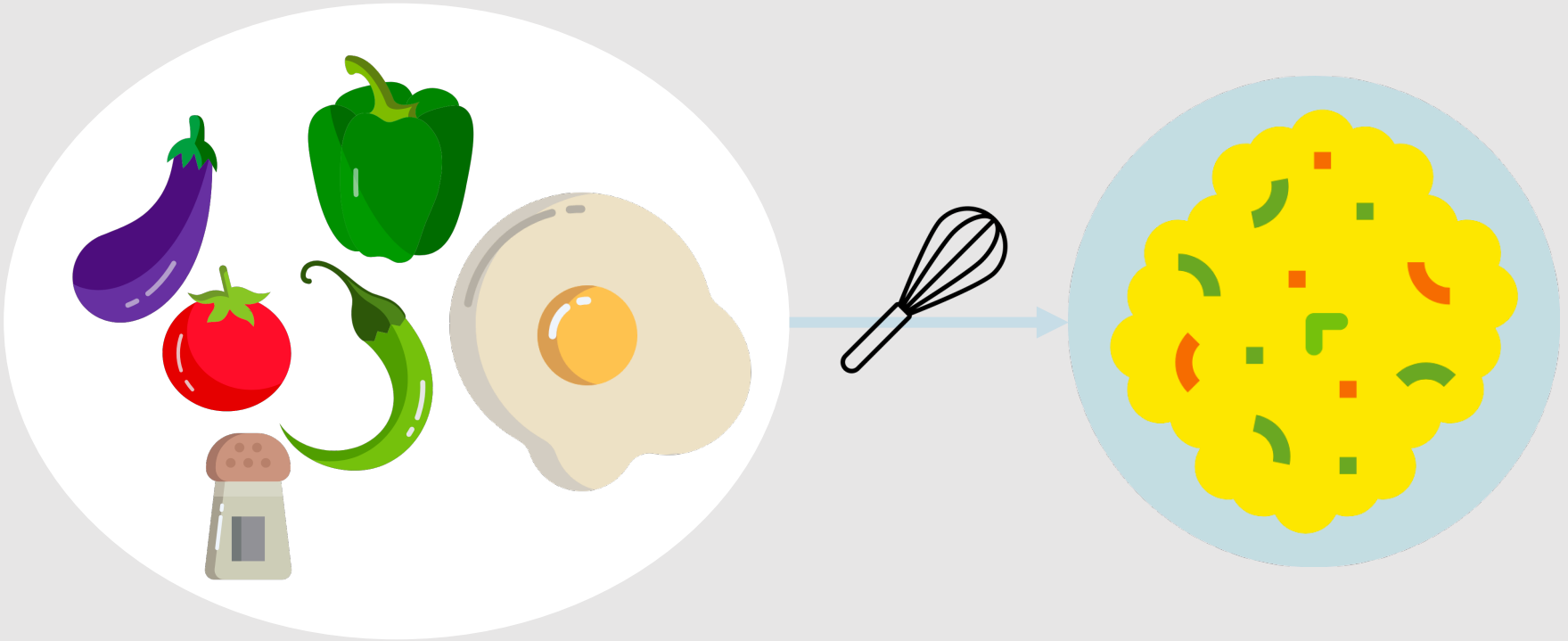


What is the recipe for this scrambled egg?

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Icons made by Nhor Phai from www.flaticon.com

Encryption – What?



netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Icons made by Nhor Phai + Icongeek26 from www.flaticon.com

Encryption – Why?

- Keep **privacy** of sensitive information
- Preserve **integrity** of message
- Ensure **authentication** before accessing data

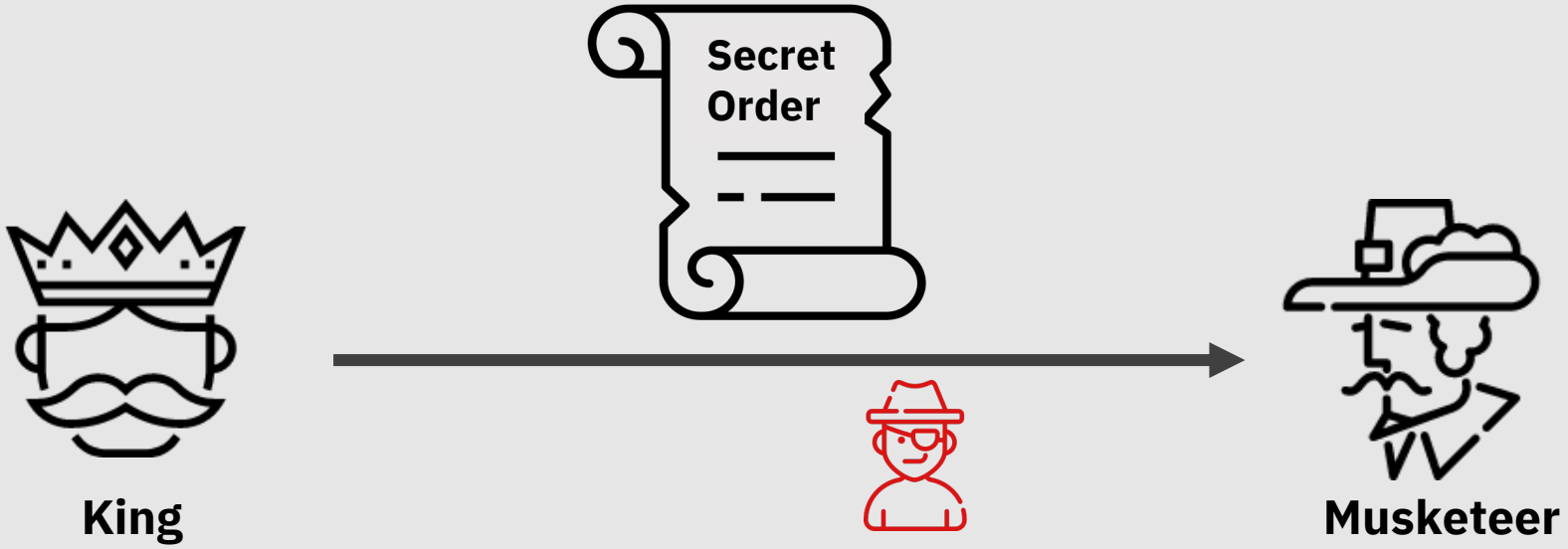
netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

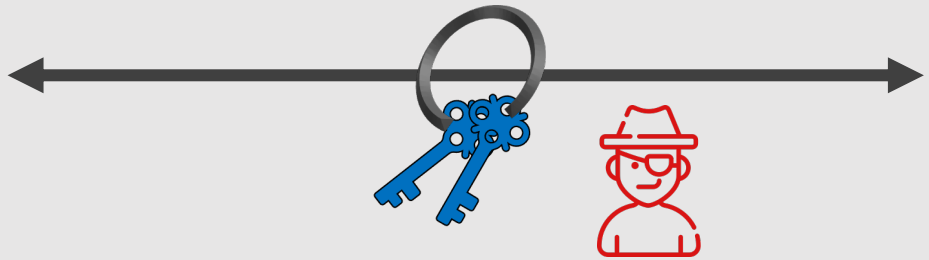
No Encryption

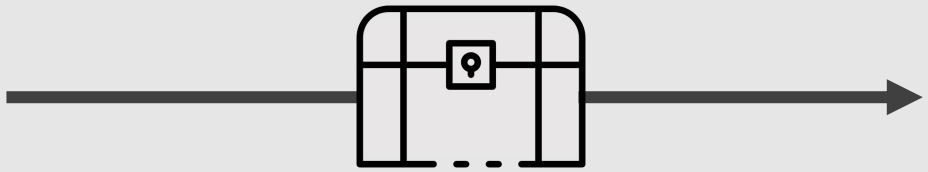


GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

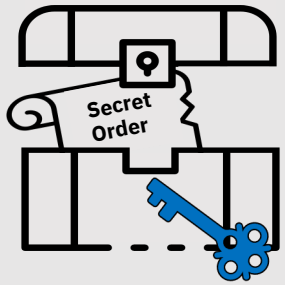
Icons made by Freepic & Eucalyp & DinosoftLabs from www.flaticon.com

Symmetric Encryption

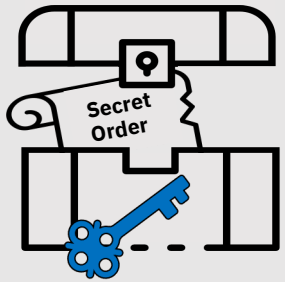




Encryption



Decryption



King

Musketeer

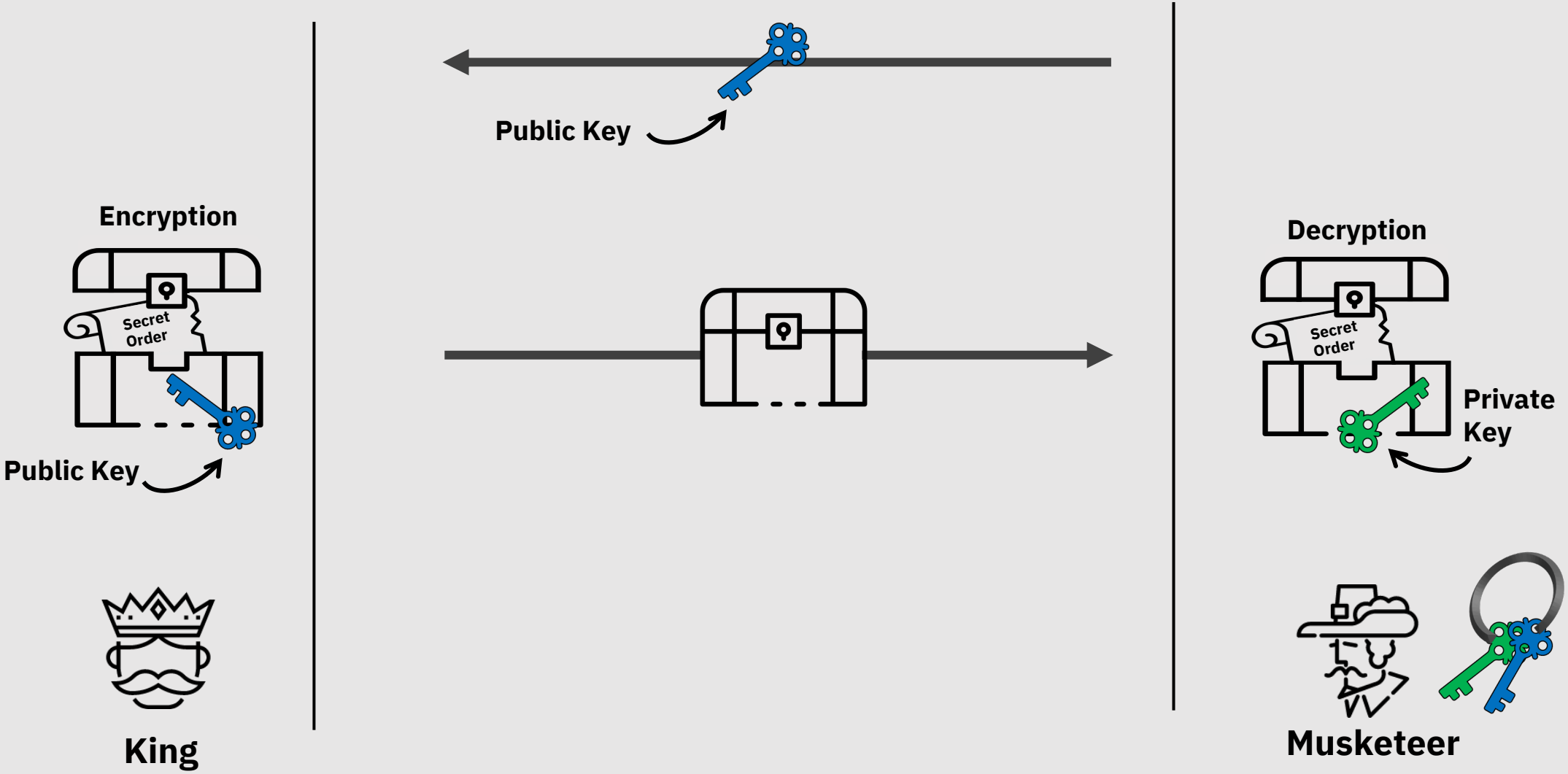
Icons made by Freepic & Eucalyp & DinosoftLabs from www.flaticon.com

netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

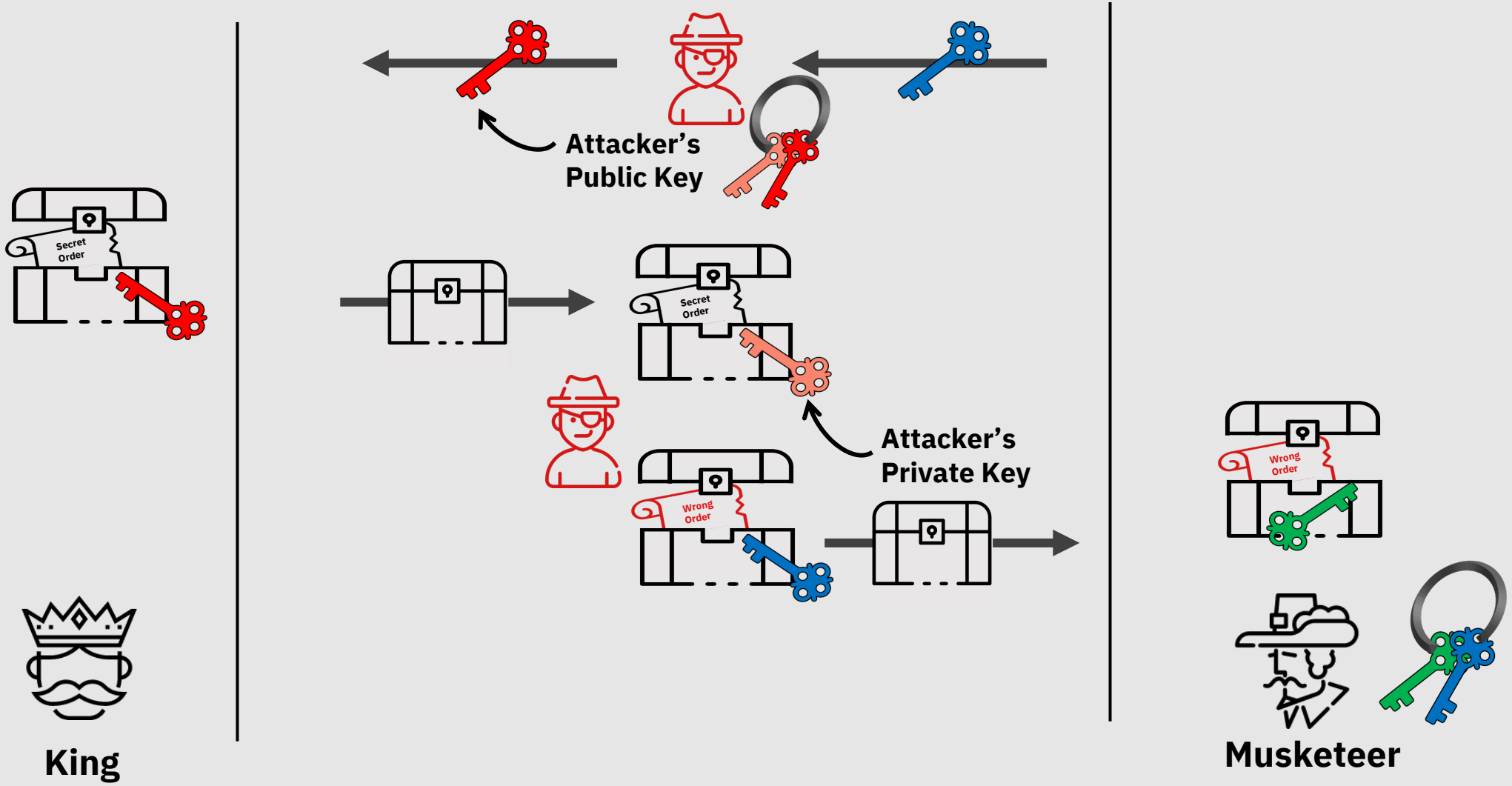
Asymmetric Encryption



netzwerk universitäts medizin
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

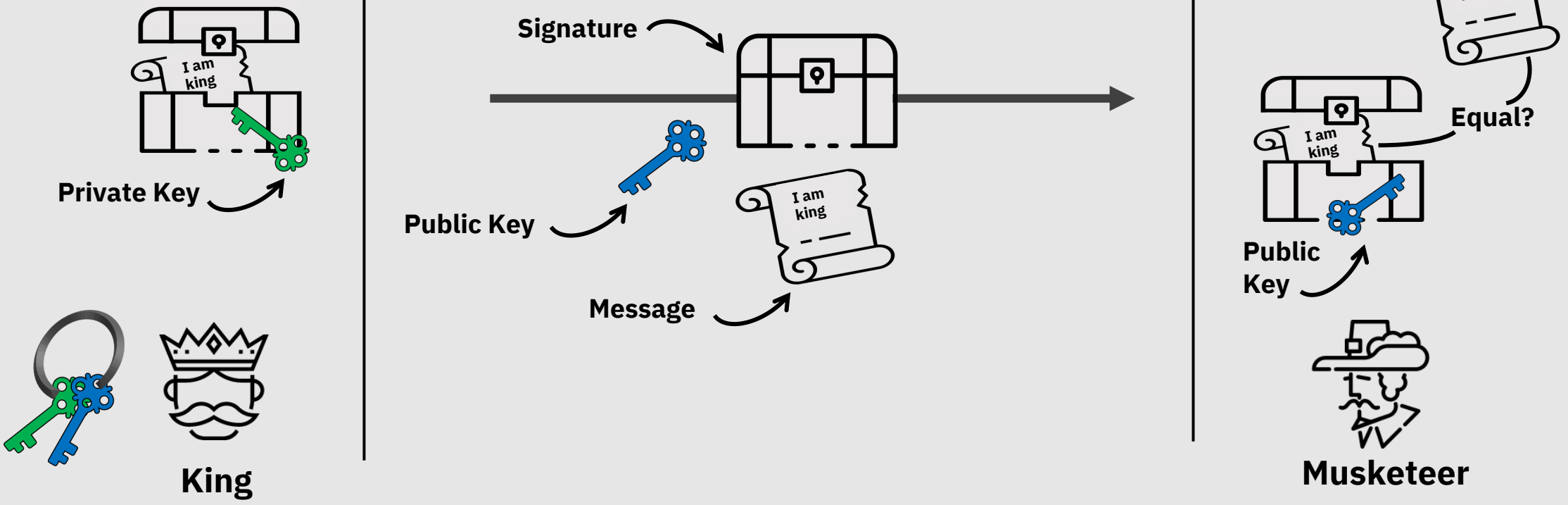
Icons made by Freepic & Eucalyp & DinosoftLabs from www.flaticon.com

Man in the Middle Attack



netzwerk universitäts medizin
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Digital Signature



netzwerk universitäts medizin
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Icons made by Freepic & Eucalyp & DinosoftLabs from www.flaticon.com

netzwerk universitäts medizin

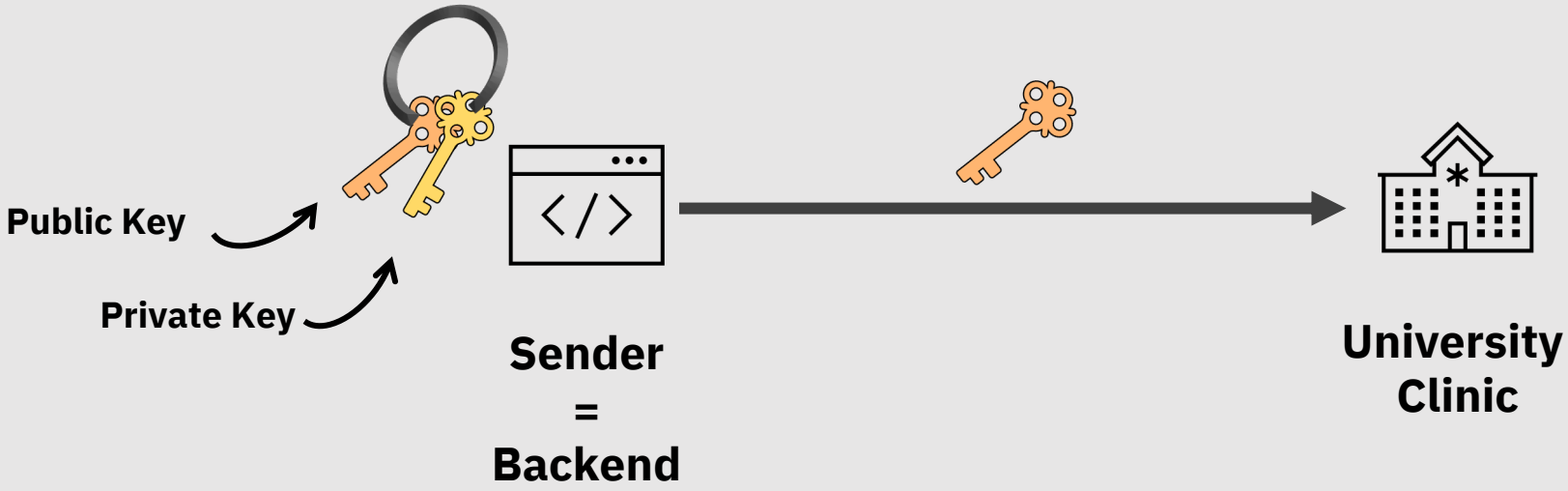
GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

Encryption in the NUM-App

Keys - Sender

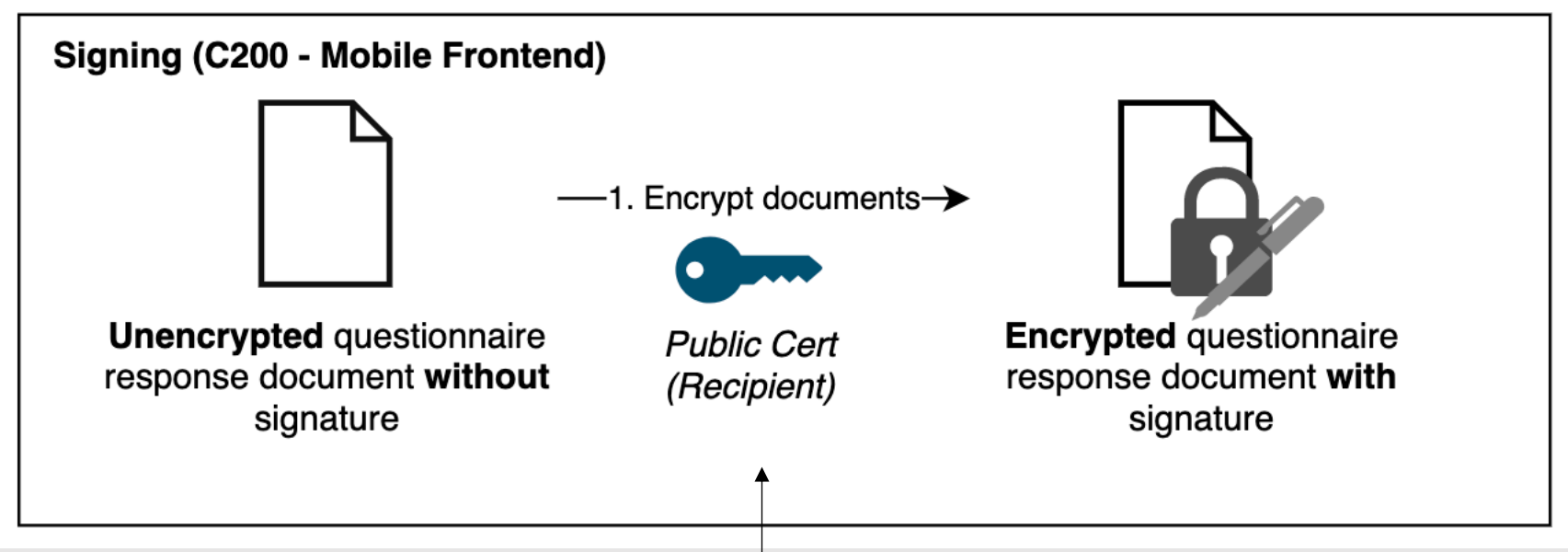


netzwerk universitätsmedizin
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Keys - Recipient

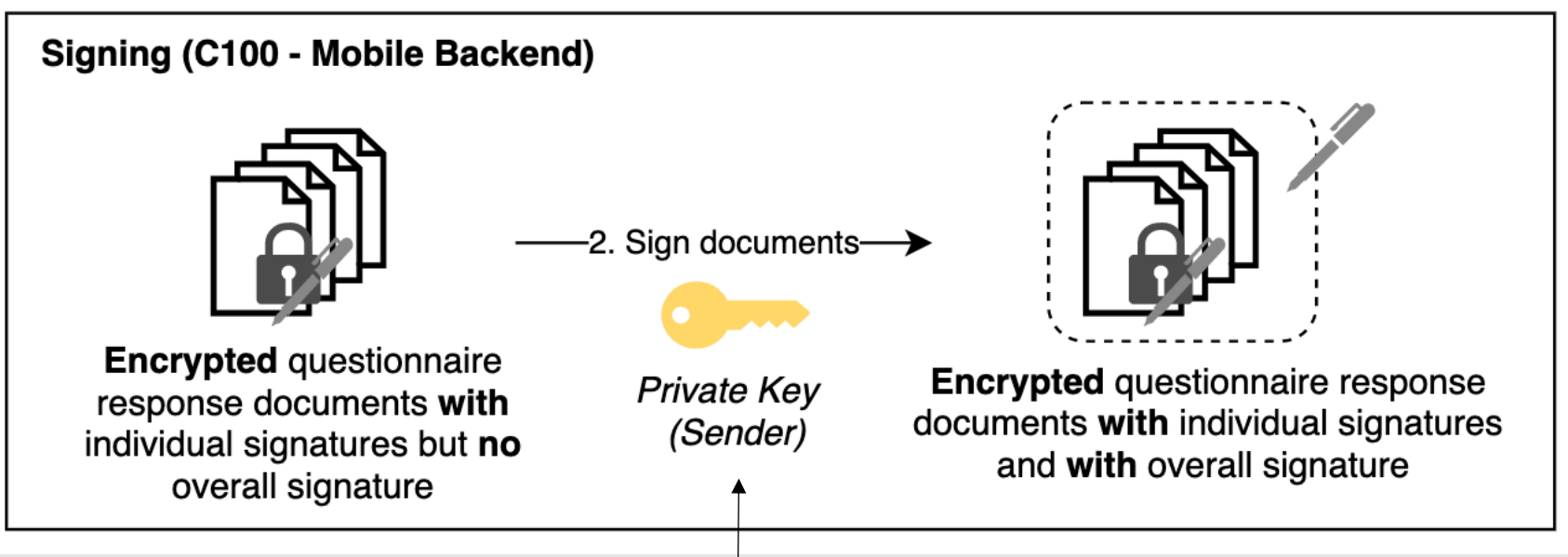
netzwerk universitätsmedizin
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Encryption Frontend



RSA PKCS #7: Cryptographic Message Syntax"

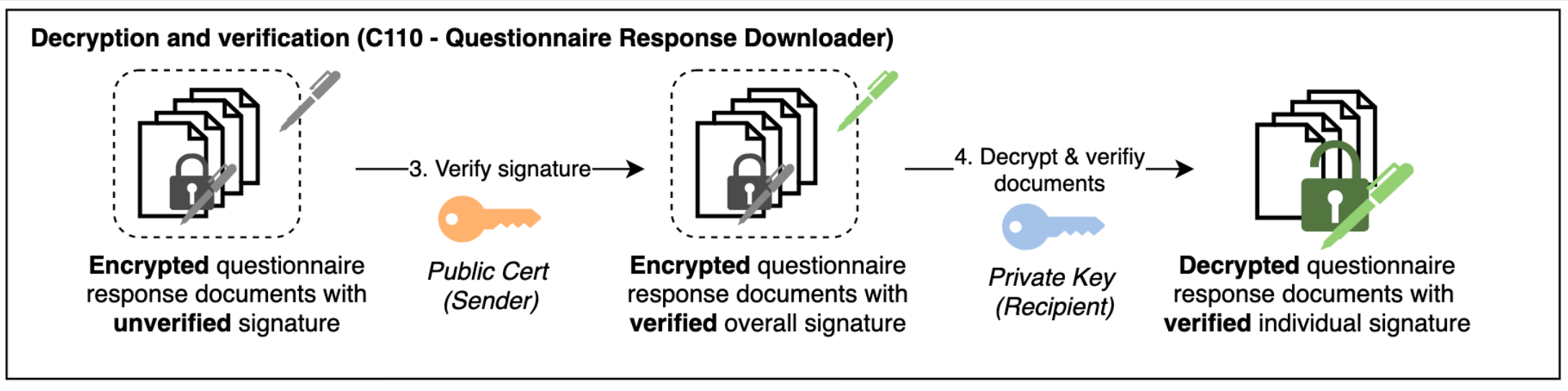
Encryption Backend



JSON Web Signature (RSA SHA 256)

Header	Payload	Signature

Encryption Downloader



netzwerk universitäts medizin
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

Links

Links

Encryption - General

- https://howhttps.works/the-keys/
- https://medium.com/@isuruj/introduction-to-encryption-4b810996a871

JWS

- https://medium.facilelogin.com/jwt-jws-and-jwe-for-not-so-dummies-b63310d201a3

Encryption Documentation

- https://github.com/NUMde/compass-numapp/tree/main/docs/encryption

netzwerk universitätsmedizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

netzwerk universitätsmedizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

IBM

Q&A

Q&A

What questions do you have?

netzwerk universitäts medizin

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

