



GO.DATA ANONYMIZATION

Krunal Badsiwal
EETAC - UPC

01

ANONYMIZATION

Private and sensitive data are not visible in Go.Data service.

02

PROTECTION

Private and sensitive data owned by an institution cannot be seen by other institutions, only by itself.

03

SEAMLESS MERGE

Although cases are anonymized, if the same patient are added later by the same or other institution, the system knows that these cases correspond to the same patient and can be seamlessly merged.

04

DECODE

The right to visualize sensitive data owned by an institution, can be transferred to other institutions keeping all the security mechanisms.

05

SECURITY

Although Go.Data server is compromised no sensitive data can be seen, as licenses are unique for each institution and stored in a different server.

HASH ID

Each patient or case has a HashID that:
Identifies the patient inside the system
The HashID is generated from unambiguous data from the user, typically birth date and some unique ID for the user, i.e driver license, national security number or CIP in Catalonia.
From the hashID, it is NOT possible to recover original data, that it is both sensible and not anonymous.



ARCHITECTURE I

01

License server based on Digital Rights Management (DRM) techniques.

- Protected Licenses
- Secure sharing

02

Using Public/Private Key cryptography for license creation.

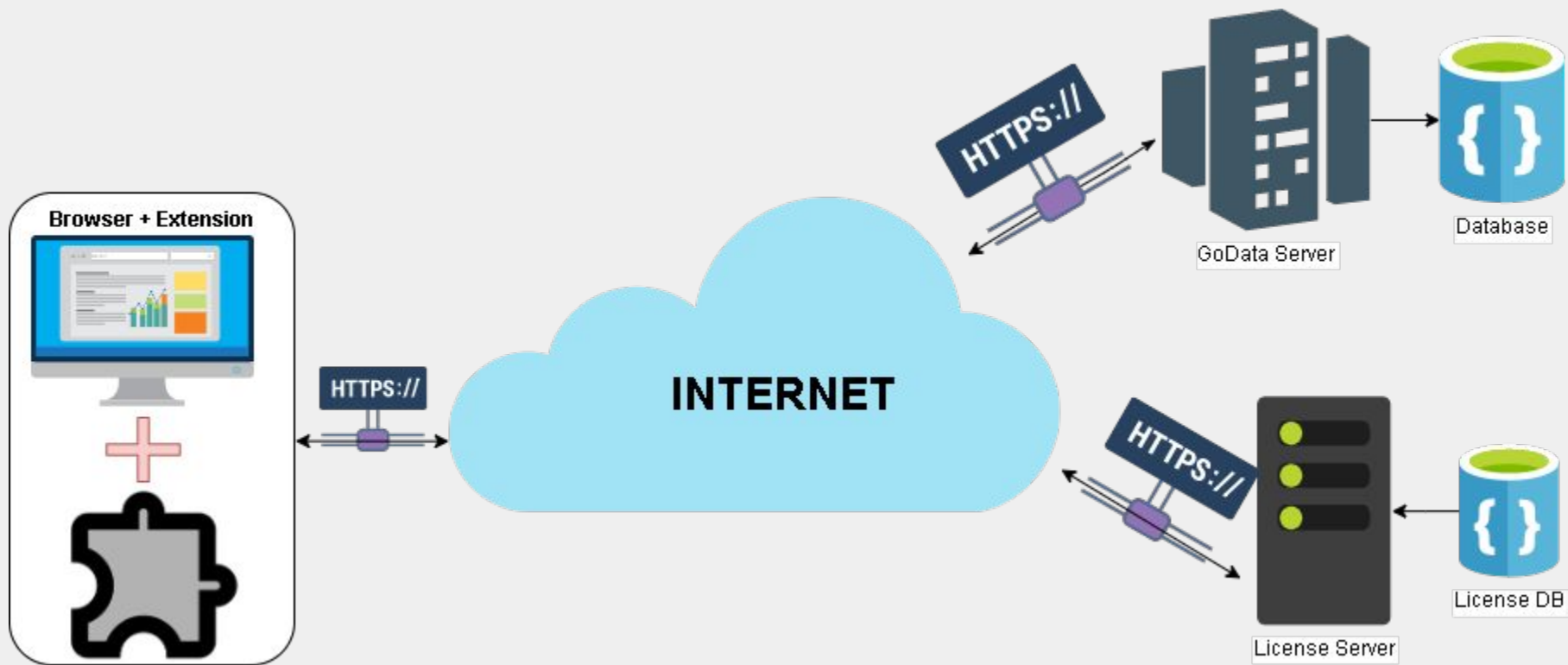
- Digital signatures
- No key exchange required
- Strong security provided

03

Using symmetric cryptography for case encryption.

- Secret key Encryption/Decryption
- Fastest cryptography

ARCHITECTURE II



ARCHITECTURE III

1. The **user** edits and views cases and contacts through the **browser**.
2. This data is stored inside the Go.Data Server.
3. The **License Server** is connected to the Go.Data API and encrypts all sensitive data as cases are added. Licenses are generated for the institution that owns this sensible data.
 - a. This license is unique to each case and institution pair.
 - b. Licenses are stored out of GoData in the license server minimizing risks.
 - c. Specific license for each case is needed to be able to decrypt sensible data.
 - d. Licenses for an institution cannot be used by other institutions because they require private key of the owner institution.
 - e. Original institution can generate additional licenses to other institutions for their owned cases.
4. Go.Data extension installed in the browser, decrypts the case and shows the sensitive data.

The license server provides 2 functions:

- Generates, stores and manages licenses.
- Auto Encrypts new added cases when they are added.

This second function can be separated for increased security.

USE CASES

1. User level:

- a. What the user see in the browser...

2. Technical level:

- a. What is happening between browser, godata, license server and extension.
- b. i.e communications
- c. what happens with the keys inside license, how are encrypted, what public/private keys are used.

USE CASE 0. AUTHENTICATION IN THE LICENSE SERVER

Login

Register

Email GoData

Password GoData

Register

Login

Login

Email

Password

Private Key

Login

Register

- User/Hospital email address
- Password
- Private Key
- Login Button

USE CASE I. MANUAL DATA ENTRY IN GODATA

Cases > Create case

[Active] Covid 19

English

1 Personal 2 Address 3 Epidemiology 4 Done

First name * Middle name ? Last name ? Gender
Pregnancy Status Occupation Age Date of birth Years ? Years / Months
Case ID 999999999 ? Date of reporting * Date of reporting approximate ?

Risk level
Risk reason

Vaccines received



Escola d'Enginyeria de Telecomunicació i
Aeroespacial de Castelldefels

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

USE CASE 2. BULK DATA ENTRY IN GODATA

Cases > Import case data

Selected outbreak
[Active] Covid 19

Language
English

Drag & drop a file of the following types here: .csv, .xls, .xlsx, .xml, .ods, .json

or, click

Import case data

Choose file

Browse

Decrypt password

?

Upload file

USE CASE 3. DECRYPTION OF PRIVATE DATA

Personal

Address

Epidemiology

First name

Middle name

Last name

Gender

/ENC/GENERIC/

/ENC/GENERIC/

/ENC/GENERIC/

Female

Pregnancy Status

Occupation

Age

Date of birth

No - Not Pregnant

Child

2021-03-

C...

Date of reporting

Date of reporting approximate

?

2021-03-12

Risk level

1 - Low

Risk reason

accines received

o vaccines

documents

Document type

Document number

CIP

/ENC/GENERIC/

Document type

Document number

National ID card

/ENC/GENERIC/

Decryption

Personal

Address

Epidemiology

First name

Middle name

Last name

Gender

test2

testMiddle

testLast3

Fema

Pregnancy Status

Occupation

Age

No - Not Pregnant

Child

C...

Date of reporting

Date of reporting approximate

?

2021-03-12

Risk level

1 - Low

Risk reason

accines received

o vaccines

documents

Document type

Document number

CIP

111222333

Document type

Document number

National ID card

123455sas

Document type

Document number

HASHID

\$2b\$10\$Ox

Home

Logout

Personal

Information

CIP

111222333

NATIONALIDCARD

123455sas

firstName

test2

lastName

testLast3

middleName

testMiddle

phoneNumber

11122333

edf15df1-b89d-474c-b5

Decrypt

Target Email

Transfer License

USE CASE 4. TRANSFER OF PRIVATE DATA TO OTHER INSTITUTION

Cases > View /ENC/GENERIC/MuqZ1LpKxGpII3uESZqNsQ==:MI0cHRc= /ENC/GENERIC/MuqZ1LpKxGpII3uESZqNsQ==:MI0cHWh2fNnx9A== /ENC/GENERIC/MuqZ1LpKxGpII3uESZqNsQ==:MI0cHWh2fNnx9A==

Personal

Address

Epidemiology

First name

test2

Middle name

testMiddle

Last name

testLast3

Gender

Female

Pregnancy Status

No - Not Pregnant

Occupation

Child

Age

Date of birth

Date of birth

2021-03-01

Case ID

0000000001

Date of reporting

2021-03-12

Date of reporting approximate

Risk level

1 - Low

Risk reason

Vaccines received

No vaccines

Documents

Document type

CIP

Document number

111222333

Document type

National ID card

Document number

123455sas

Login

Personal

Information

CIP

111222333

NATIONALIDCARD

123455sas

firstName

test2

lastName

testLast3

middleName

testMiddle

phoneNumber

11122333

edf15df1-b89d-474c-b5

Decrypt

test3@test3.com

Transfer License

USE CASE 5. MERGE OF TWO CASES OF THE SAME PATIENT

First name /ENC/GENERIC/MuqZ1LpKxG	Middle name /ENC/GENERIC/MuqZ1LpK?	Last name /ENC/GENERIC/MuqZ1LpK?	Gender Female
Pregnancy Status No - Not Pregnant	Occupation Child	Age	Date of birth 2021-03-01
Case ID 0000000001	Date of reporting 2021-03-12	Date of reporting approximate	

Risk level 1 - Low
Risk reason Maybe

accines received
o vaccines
ocuments

Document type CIP	Document number /ENC/GENERIC/MuqZ1LpK?
----------------------	-------------------------------------------

Document type National ID card	Document number /ENC/GENERIC/MuqZ1LpK?
-----------------------------------	-------------------------------------------

Document type HASHID	Document number \$2b\$10\$OxgMdxg7TAI49dhI
-------------------------	-----------------------------------------------

First name /ENC/GENERIC/N7mSVv7Xw1	Middle name /ENC/GENERIC/N7mSVv7?	Last name /ENC/GENERIC/N7mSVv7?	Gender Female
Pregnancy Status	Occupation	Age	Date of birth 2021-03-01
Case ID 0000000002	Date of reporting 2021-03-15	Date of reporting approximate	

Risk level 1 - Low
Risk reason Maybe

accines received
o vaccines
ocuments

Document type CIP	Document number /ENC/GENERIC/N7mSVv7X?
----------------------	-------------------------------------------

Document type National ID card	Document number /ENC/GENERIC/N7mSVv7X?
-----------------------------------	-------------------------------------------

Document type HASHID	Document number \$2b\$10\$QiaTh7Hgiivjhr2Jdl
-------------------------	-------------------------------------------------

NEXT STEPS



1. Integration of the extension directly into godata except the DRM License Server?
2. Do it have sense to maintain the licenses out of Go.Data in other physical server?



THANKS

Does anyone have any questions?
EETAC

- Krunal Badsiwal

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik** and illustrations by **Stories**

Please keep this slide for attribution.