eHealth Network

European Interoperability Certificate Governance

A Security Architecture for contact tracing and warning apps

The onboarding of several member states to the European Federation Gateway Service needs an appropriate level of trust and a high attention on the security, integrity and authenticity of a further data exchange. This document describes how this trust can be established.

The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent authorities dealing with digital health. The Joint Action supporting the eHealth Network (eHAction) provides scientific and technical support to the Network.

Adopted by consensus by the eHealth Network, Brussels, 02/09/2020

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1 Introduction

1.1 Context

The secure and trusted exchange of diagnosis keys[1] between European Countries is realized by the European Federation Gateway Service (EFGS) which distributes the data between the member states. This exchange of diagnosis keys is secured by cryptographic signatures which are transparent to all countries that take part in the system. The following figure presents an overview of the EFGS data distribution flow.

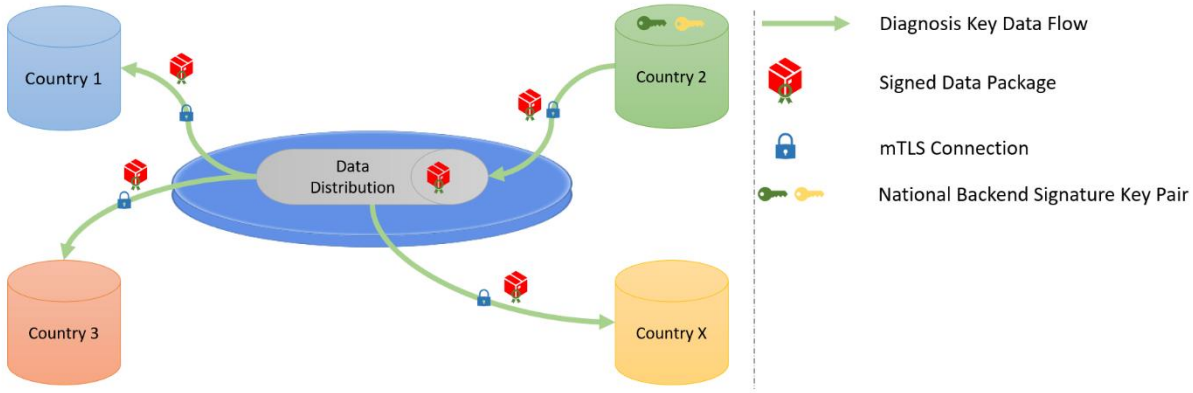

Figure 1: Data Distribution with the European Federation Gateway Service

1.2 Scope of Document

Digital signatures can be used to achieve data integrity and authenticity. A well-defined trust model is necessary to bind the public key of an entity to its identity in order to allow other participants to verify the data origin or the identity of the communication partner. In the context of the EFGS this means that the public keys of the European Member States as well as the public key of the EFGS must be bound to their identities in order to establish trust between the participants. By this means, Member States are enabled to verify the integrity and authenticity of the signed diagnosis keys provided by the EFGS. This document will present how the trust and security services that build upon it will be established in the EFGS

[1] Diagnosis keys are temporary exposure keys for individuals who have had a positive diagnosis of COVID-19. (source: https://developer.apple.com/documentation/exposurenotification/setting_up_an_exposure_notification_server)

system. The document also contains the design rationales that led to this design. Legal and lawful procedures are not in the scope of this document, they must be defined separately.

1.3 Terminology

The following table contains abbreviations and terminology used throughout this document.

Term	Definition
Certificate	Or public key certificate. An X.509 v3 certificate that contains the public key of an entity
Diagnosis Key Batch	A batch of diagnosis keys submitted by a National Backend. Diagnosis keys are temporary exposure keys for individuals who have had a positive diagnosis of COVID-19.
EC-DSA	Elliptic Curve Digital Signature Algorithm. A cryptographic signature algorithm based on elliptic curves
EFGS	European Federation Gateway Service
$EFGS_{TLS}$	Abbreviation for the TLS certificate that the EFGS uses to establish the mutual TLS connection. This certificate shall be issued by a publicly trusted CA (following the CA Browser Forum Baseline Requirements)
$EFGS_{TA}$	Abbreviation for the Trust Anchor certificate that the EFGS uses to sign the trust list and the NB_{BS} certificate
mTLS	Mutual TLS. The Transport Layer Security Protocol with mutual authentication
NB	National Backend of a Member State
NB_{BS}	The National Backend diagnosis key batch signature (NB_{BS}) certificate. The National Backend uses the corresponding private key to sign the diagnosis key batches it sends to the EFGS
NB_{TLS}	The National Backend TLS authentication certificate used to authenticate during the mutual TLS authentication with the EFGS. This shall be a certificate issued by a public CA (following the CA Browser Forum Baseline Requirements)
RSA	Asymmetric cryptographic algorithm based on integer factorization used for digital signatures or asymmetric encryption
Trust list	A signed list maintained by the EFGS that contains the National Backend diagnosis key batch signature (NB_{BS}) certificates and the (NB_{TLS}) certificates used for internal validation on the EFGS
White list	A list maintained by the EFGS that contains the authorized National Backend TLS authentication certificates (NB_{TLS}). The EFGS TLS endpoint (e.g.

	load balancer) only accepts connections to whitelisted National Backends.

Table 2: Terminology

2 EFGS communication flows and security services

This section gives an overview of the communication flows and security services in the EFGS system. It also defines which keys and certificates are used to protect the communication, the diagnosis key batches and the trust list. The following figure gives a high-level overview of the EFGS trust model and security services. The following sub-sections will explain the design in more detail.

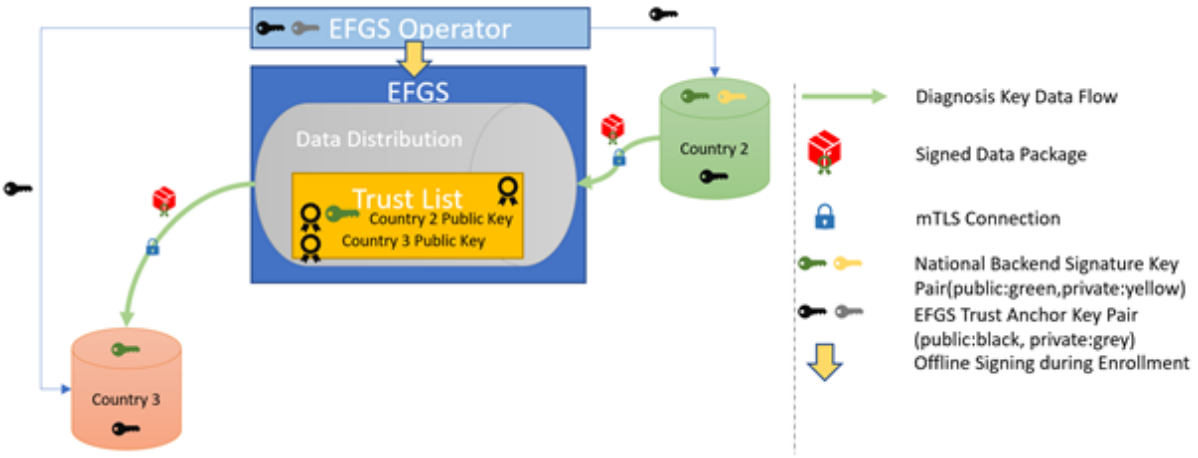

Figure 2: EFGS communication and security services (high-level overview)

2.1 General

The EFGS works as a data hub that allows the exchange of diagnosis keys for registered EU Member States. The EFGS uses mutual TLS (mTLS) to establish a secure connection with the National Backends (see Section 2.2).

Diagnosis keys are provided by the EFGS “as is”, meaning that the EFGS does not add or delete diagnosis keys from the batches it receives. The national backend (NB) of the Member States shall be enabled to verify the end-to-end integrity and authenticity of the diagnosis key batches uploaded by other Member States (see Section 2.3).

2.2 Authentication and connection establishment

The EFGS uses Transport Layer Security (TLS) with mutual authentication to establish an authenticated encrypted channel between the Member State’s national backend (NB) and the Federation Gateway environment. Therefore, the EFGS and the NB hold a TLS

certificate (see Section 4 for certificate templates) abbreviated $EFGS_{TLS}$ resp. NB_{TLS} certificate.

Since there is no central Public Key Infrastructure (PKI) for the EFGS stakeholders in place, it was jointly decided that every national backend can provide their own TLS certificate. In order to establish consistent certificate verification processes, these certificates shall be issued by publicly trusted certificate authorities (CAs) that are included in all major browsers (i.e. the CA adheres to the CA Browser Forum Baseline Requirements[2]).

Every Member State is responsible for their national data and the protection of the private key used to establish the connection to the EFGS. Clearly, the "bring your own certificate" approach requires a well-defined registration and identification process as well as revocation and renewal procedures that are described in Section 3.

The EFGS uses a whitelist where the TLS certificates of NBs are explicitly added after their successful registration. Only NBs that authenticate themselves with a private key that corresponds to a certificate from the whitelist can establish a secure connection to the EFGS.

The EFGS will also use a TLS certificate that allows the NBs to verify that they are indeed establishing a connection to the "real" EFGS and not some malevolent entity posing as EFGS. The certificate of the EFGS will be provided to the NBs after successful registration. The $EFGS_{TLS}$ certificate must be issued by a publicly trusted CA (included in all major browsers).

2.3 Integrity and authenticity of diagnosis key batches

National backends can use the EFGS to upload and download digitally signed diagnosis key batches after successful mutual authentication. The key pair that is used by the national backend for the digital signature of diagnosis key batches in the EFGS system is called National Backend (diagnosis key) ***b***atch ***s***ignature key pair and the corresponding public key certificate is abbreviated by NB_{BS} certificate. Each Member State brings its own NB_{BS} certificate, which might be signed by a publicly trusted CA, a private CA, or the owner of the corresponding private key (self-signed). The requirements on this certificate are defined in Section 4.

National backends shall use a new asymmetric key pair to sign the diagnosis key batches. They shall not use the same key pair that is used for their national exposure notification services and they shall not reuse the TLS authentication key pair. Every Member State is responsible for their national data and the protection of the private key that is used for the diagnosis key batch signatures.

[2] https://cabforum.org/about-the-baseline-requirements/

The EFGS will maintain a signed trust list that contains the NB_{BS} certificates of the registered Member States for its internal verifications. More precisely, the EFGS verifies that the connection is established from a trusted NB (through the NB_{TLS} certificate) and the EFGS will verify the integrity and authenticity of the signed diagnosis key batch. The signed trust list will be created/updated after the successful identification and registration process (see Section 3.1). The EFGS operator will use a dedicated asymmetric key pair to sign the trust list and the certificates in an offline environment. The private key will not be stored on the online EFGS system, such that a compromise of the online EFGS system does not enable an attacker to compromise the trust list. The corresponding **t**rust **a**nchor certificate, $EFGS_{TA}$, will be provided to the National Backends during the onboarding process.

The EFGS will not manipulate the content of diagnosis key batches. In order to ensure end-to-end integrity of the diagnosis key batches, the EFGS will provide the original digital signature of the origin Member State over the auditing functions. Moreover, the EFGS will add the NB_{BS} certificate, signed with the $EFGS_{TA}$ private key, directly in the audit reply in order to minimize operational overhead when certificates are renewed or new Member States are onboarded. Stated differently, the EFGS does not need to inform the NBs centrally when the trust list is updated since the NB_{BS} certificates will be sent along with the diagnosis key batch.

Member States that retrieve digitally signed diagnosis key batches must verify the signed NB_{BS} certificate and the batch signature and they shall link the batch to the Member State of the NB that uploaded it to the EFGS. This can be achieved by verifying that the NB_{BS} certificate contains the NBs country code in the subject name (C = Member State).

2.4 Requirements on the technical EFGS architecture

The requirements on the technical EFGS architecture can be summarized as follows:

- The EFGS uses mutual TLS authentication to establish an authenticated encrypted connection with the NBs. Therefore, the EFGS maintains a whitelist of registered NB_{TLS} certificates
- The EFGS uses two digital certificates ($EFGS_{TLS}$ and $EFGS_{TA}$) with two distinct key pairs. The private key of the $EFGS_{TA}$ key pair is maintained offline (not on the online components of the EFGS)
- The EFGS maintains a trust list of the NB_{BS} certificates that is signed with the $EFGS_{TA}$ private key. The EFGS will send the unchanged diagnosis key batches together with the signed NB_{BS} certificate to the requesting NB.

3 Certificate Lifecycle Management

3.1 Public certificate authorities and self-signed certificates

Public certificate authorities (i.e. certificate authorities that adhere to the baseline requirements of the CA browser forum[3]) will verify the identity of subjects during the registration process. Typical verification methods are Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV). Hence, using a certificate under a public CA ensures that an additional identification was performed. Moreover, these certificate authorities have policies in place that ensure strong cryptographic algorithms (see Section 4.1) and other best practices. The verification of public TLS certificates shall include the verification of the CA chain, validity information and revocation status of the certificates as security best practice.

The diagnosis key batch signature certificates used in the EFGS system might be self-signed certificates. Hence, the EFGS trust list will ensure that only registered NB_{BS} can upload signed diagnosis key batches. Other NBs can verify the integrity and authenticity of the signed diagnosis key batches when they trust the $EFGS_{TA}$ certificate without the need to establish a connection to another NB.

Because of the “bring your own certificate” approach, the EFGS operator shall verify that the Member States follow the requirements from Section 4. Due to the explicit whitelisting of TLS certificates, the trust list of signature keys and the limited number of Member States, the “bring your own certificate” approach combined with the registration procedure allows flexibility, security, and minimal operational overhead in the given setup and timeframe.

3.2 Registration of National Backends

Member States must register with the EFGS operator to take part in the EFGS system. This section describes the technical and operational procedure that must be followed to register a national backend. Legal and lawful procedures are not in the scope of this document, they must be defined separately.

The EFGS operator and the Member State must exchange technical contact persons for the onboarding process. It is assumed that the technical contact persons are legitimated by their Member States and identification/authentication is performed over other channels. For example, the authentication can be achieved when the Member States technical contact provides the certificates as password-encrypted files via E-Mail and shares the corresponding password with the EFGS operator via telephone.

[3] https://cabforum.org/baseline-requirements/

The Member State must provide *two* digital certificates during the registration and identification process:

- The Member States TLS certificate NB_{TLS} that follows the requirements from Section 4.3 and that adheres to the requirements on cryptographic algorithms defined in Section 4.1
- The Member States diagnosis key batch signature certificate NB_{BS} that follows the certificate templates from Section 4.4 and that adheres to the requirements on cryptographic algorithms defined in Section 4.1

The EFGS operator must verify that the provided certificate adheres to the requirements of Section 4. Besides this, the EFGS operator must verify that the certificate content corresponds to the requesting member state (e.g. that C = Member State).

After the identification and registration, the EFGS operator

- signs the NB_{BS} certificate with the private key that corresponds to the $EFGS_{TA}$ public key certificate and adds the signed certificates to the database of the EFGS online system.
- adds the NB_{BS} certificate to the trust list and signs the trust list with the private key that corresponds to the $EFGS_{TA}$ public key certificate.
- adds the NB_{TLS} certificate to the whitelist of the EFGS TLS endpoint
- provides the $EFGS_{TA}$ and $EFGS_{TLS}$ public key certificate to the Member State.

3.3 Revocation of certificates

In general, digital certificates can be revoked by their issuing CA using certificate revocation lists or online certificate status responder. In the EFGS trust model, manual revocation processes are used in addition.

Member States must inform the EFGS operator when they must revoke a digital certificate, for example due to compromise of a system. The EFGS operator can then remove the trust for the affected certificate by removing it from the TLS whitelist and by issuing a new trust list where the affected certificate is not contained anymore. The EFGS operator can revoke the NB_{BS} and NB_{TLS} certificates in the EFGS database, or it can be deleted from the database.

Since the EFGS will provide the signed NB_{BS} certificates together with the batch diagnosis keys, the NBs do not need to update the trust list regularly. In case of a necessary revocation, the EFGS operator should inform the Member States' technical contact person that the trust list was updated.

In case that the $EFGS_{TLS}$ certificate or the $EFGS_{TA}$ certificate must be revoked, the EFGS operator and the Member States must work together to establish a new trusted TLS connection and trust list.

3.4 Renewal of certificates

Digital certificates contain a validity period that enforces certificate renewal. Renewal is necessary to use fresh cryptographic keys and to adapt the key sizes when new improvements in computation or new attacks threaten the security of the cryptographic algorithm that is used.

In the EFGS trust model, certificates shall not be used longer than *two years*. The technical contact persons of the Member States and the EFGS operator shall work together to update the whitelist and trust list during a maintenance window. Certificates shall be renewed at least one month prior to their expiration to have enough time for the necessary operational changes. The renewal process can be similar to the original enrollment process, at least from a technical viewpoint. Expired certificates shall be removed from the whitelist and trust list.

Member states and the EFGS operator must keep track of the validity of *their own* certificates. There is no central entity that keeps record of the certificate validity and informs the participants.

4 Certificate templates

The following sections contain cryptographic requirements and recommended certificate templates. The required fields in the certificate templates are marked **bold**. For absent fields, no requirements are defined.

4.1 Cryptographic requirements

Cryptographic algorithms and TLS cipher suites shall be chosen based on the recommendation from the German Federal Office for Information Security (BSI) or SOG-IS. These recommendations and the recommendations of other institutions and standardization organization are quite similar[4]. The recommendations can be found in the technical guidelines[5] TR 02102-1 and TR 023102-2 or SOG-IS Agreed Cryptographic Mechanisms[6].

For digital certificates and cryptographic signatures in the EFGS context, the major requirements on cryptographic algorithms and key length are summarized in the following table (as of 2020):

Signature Algorithm	**Key size**	**Hash function**
EC-DSA	Min. 250 Bit	SHA-2 with an output length ≥ 256 Bit or better
RSA-PSS (recommended) RSA-PKCS#1 v1.5 (legacy)	Min. 3000 Bit RSA Modulus (n) with a public exponent e > 2^16	SHA-2 with an output length ≥ 256 Bit or better
DSA	Min. 3000 Bit prime p 250 Bit key q	SHA-2 with an output length ≥ 256 Bit or better

Named curves shall be used for EC-DSA (e.g. NIST-p-256).

4.2 Validity periods

The certificates used in the EFGS system shall have a validity between one and two years (Min= 1 year, Max= 2 years).

---

[4] See https://www.keylength.com/en for a comparison

[5] See https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html

[6] See https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

4.3 Public TLS certificates (*EFGS$_{TLS}$*, *NB$_{TLS}$*)

The following table contains a recommended certificate template for the TLS certificates used in the EFGS system. Since certificates from publicly trusted CAs must be used, the applicable certificate template will be enforced by the issuing CA.

Subject	**cn=<NB_Server_CommonName>,** ou=<Organizational Unit of Country>**, o=<Provider> ,c=<your country>,** e= <your contact email>
SubjectAltName	**dnsName: <DNSName_NB>**
Key Usage	**Digital Signature**, (optional) Key Encipherment
Extended Key Usage	**Client Authentication (1.3.6.1.5.5.7.3.2),** **Server Authentication (1.3.6.1.5.5.7.3.1)**

4.4 Diagnosis key batch signature certificate (*NB$_{BS}$*)

Subject	**cn=<NB_BS Common Name >,** ou = <Organizational Unit of Country>, **o=<Provider> ,c=<your country>,** e= <your contact email>, L= <locality>
Key Usage	**Digital Signature**

4.5 Trust list signature certificate (*EFGS$_{TA}$*)

Subject	**cn= EU Federation Gateway Service, o=<Provider> , c=BE**
Key Usage	**Digital Signature**

REFERENCES

[1] European Interoperability Architecture – Federation Gateway Service (July 7, 2020)