Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRIME MINISTER

Subject: notification of the electronic identification scheme of France

The French Republic has the honour to notify the European Commission of an electronic identification scheme to be published on the list referred to in Article 9(3) of Regulation (EU) No 910/2014 and confirms the following:

- The information provided in this notification is consistent with the information provided to the cooperation network in accordance with Article 7(g) of Regulation (EU) No 910/2014,
- The electronic identification scheme can be used to access at least one service provided by a public sector body in the French Republic.

Mr Nadi BOU HANNA

Interministerial Digital Director

1. General information

Title of the scheme (if any)	Level(s) of Assurance (low, substantial or high)
French eID scheme "FranceConnect+ /The Digital Identity La Poste"	Substantial

2. Authority(s) responsible for the scheme

Name(s) of authority(ies)	Postal address(es)	Email address(es)	Telephone No
DINUM (Interministerial Digital Direction)	20 avenue de Ségur 75007 PARIS	christine.balian@modernisation.gouv.fr	+33 6 48 83 90 29

DINUM is a service of the Prime Minister under the authority of the Minister of Transformation and Public Service. It is in charge of the digital transformation of the French State to the benefit of both citizens and agents, in all its aspects: modernisation of the French state information system, quality of digital public services, creation of innovative services for citizens, digital tools for collaborative work for agents.

3. Information on relevant parties, entities and bodies (where there are multiple parties, entities or bodies, please list them all, in accordance with Article 3(2) and (3)

3.1. Entity which manages the registration process of the unique person identification data

Name of the entity that manages the process of recording unique personal identification data
La Poste La Poste, a public limited company owned by the French State, is both the operator of postal services (mail, parcel and express), bank, insurance, mobile telephony operator, provider of digital services and business solutions, online commerce (marketing, logistics) and data collection and sale. In particular, it operates the digital service "Digital Identity" (LIN), a digital identity service that allows an individual to acquire a verified digital identity free of charge, with a "substantial" assurance level, and thus to prove who he is. For more details, refer to *G1_General_Information, §2*.

3.2. Party issuing the means of electronic identification

Name of the party issuing the means of electronic identification. Specify whether the part is referred to in Article 7(1a)(i), (ii) or (iii) of Regulation (EU) No 910/2014		
La Poste For more details, refer to *G1_General_Information, §2*.		
Article 7(a)(i) ☐	Article 7(a)(ii) ☐	Article 7(a)(iii) ☒

3.3. Party operating the authentication procedure

Name of the party that manages the authentication procedure
La Poste (Identity Provider) **DINUM** (FranceConnect+) For more details, refer to *G1_General_Information, §2*.

3.4. Supervisory body

Name of the supervisory body [indicate name(s), if applicable]
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) – *French National Cyber Security Agency* For more details, refer to *G1_General_Information, §2*.

4. Description of the electronic identification scheme

One or more documents may be attached for each of the following descriptions:

a) Briefly describe the scheme including the context within which it operates and its scope
FranceConnect + is a federator of digital identity providers which aims to be recognized by all administrations and certain regulated actors in the private sector. It allows a French or European user to be recognized for carrying out their procedures online. La Poste is the leading identity provider offering identities with a substantial level of security. Service Providers and the French eIDAS Bridge must be OpenID Connect customers (also known as relaying parties), and French Identity Providers and Bridge eIDAS must be OpenID Connect providers (also known as providers). For more details, refer to *G1_General_Information, §3*.
b) Where applicable, list the additional attributes which may be provided for natural persons under the scheme if requested by a relying party
The document *T1_Table_of_attributes* provides the table of attributes of the electronic identification scheme "FranceConnect+/L'identité Numérique La Poste".

[1]Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions within the internal market and repealing Directive 1999/93/EC
Article 7(a) means of electronic identification covered by the electronic identification scheme shall be issued:
by the notifying Member State
II) within the framework of a mandate of the notifying Member State
III) independently of the notifying Member State and recognised by that Member State

c) Where applicable, list the additional attributes which may be provided for legal persons under the scheme if requested by a relying party
Not applicable

4.1. Applicable supervisory, liability and management regime

4.1.1 Applicable supervisory regime

a) Supervisory regime applicable to the party issuing the electronic identification means
The supervisory body (ANSSI) is responsible for assessing the compliance with the requirements of the regulation. This compliance is attested by a formal administrative decision issued by the Director General of ANSSI. This decision relies on several sub-processes: - "Qualification" according to national regulation of the components handling sensitive cryptographic material. - Conformity assessment of the identity provider and all associates and subcontractors with regards to the production, delivery and management of the electronic identification means. - Specific assessment of solutions relates to remote identity verification when appropriate, according to national requirements. The certification decision is valid for a maximum of two years from the date of its delivery. Checks may be requested or carried out by ANSSI during this period in order to verify compliance of the means of electronic identification with the applicable requirements. In the event of non-compliance detected or recognized after the decision, the Director General of ANSSI may revoke or impose restrictive conditions on the decision. For more details, refer to *G4_Supervision*
b) Supervisory regime applicable to the party operating the authentication procedure
Cf a) supervisory regime applicable to the party issuing the electronic identification means

4.1.2 Applicable liability regime

Describe briefly the applicable national liability regime for the following scenarios:

a) liability of the Member State under Article 11(1) of Regulation (EU) No 910/2014 5.11.2015 L 289/22 Official Journal of the European Union EN
For the State (DINUM/ANSSI): administrative liability for fault. It will be necessary to prove the intention or negligence of the damage, the breach of the obligations under article 7 (d) and (f) for transnational transactions, the causal link between the fault and the injury suffered. The courts of the administrative order shall have sole jurisdiction to hear it.
b) liability of the party issuing the electronic identification means under Article 11(2) of Regulation (EU) No 910/2014
If the party issuing the means of electronic identification is an administration within the meaning of Article L.100-3 of the Code of Relations between the Public and Administration (public Identity provider), the regime of its responsibility is governed by administrative law. Administrative liability for fault. It will be necessary to prove the intention or negligence at the origin of the damage, the breach of the obligations laid down in Article 7(e) for transnational transactions, the link between the fault and the injury suffered (causal link).

The courts of the administrative order shall be competent to hear it. In other cases (private Identity provider), the liability regime is that of common law (civil law). It will be necessary to prove the intention or negligence at the origin of the damage, the breach of the obligations laid down in Article 7(e) for transnational transactions, the link between the fault and the injury suffered (causal link). Jurisdiction of courts to hear them.
c) liability of the party operating the authentication procedure under Article 11(3) of Regulation (EU) No 910/2014
If the party managing the authentication procedure is an administration within the meaning of Article L.100-3 of the Code of Relations between the Public and Administration (public Identity provider), the regime of its responsibility is governed by administrative law. Administrative liability for fault. It will be necessary to prove the intention or negligence at the origin of the damage, the incorrect management of the authentication referred to in Article 7(f) in the case of a transnational transaction, the link between the fault and the damage suffered (causal link). The courts of the administrative order shall be competent to hear it. In other cases (private Identity provider), the liability regime is that of common law (civil law). The intention or negligence of the intention or negligence causing the damage, the incorrect management of the authentication referred to in Article 7(f) in the case of a transnational transaction, the link between the fault and the damage suffered (causal link) must be proved. Jurisdiction of courts to hear them.

4.1.3 Applicable management arrangements

Describe the arrangements for suspending or revoking of either the entire identification scheme or authentication, or their compromised parts

DINUM has the capacity to temporarily suspend or permanently terminate the use of an eID means or of an eID means issuer, both at national level and in the cross-border context, on the grounds that an issuer does not have respect contractual obligations

For more details, refer to *G4_Supervision, §9*.

4.2. Description of the components of the scheme

Describe how the following elements of Commission Implementing Regulation (EU) 2015/1502 ([2]) have been met in order to reach a level of assurance of an electronic identification means under the scheme the Commission is being notified of:
(include any standards adopted)

The following documents provide a detailed analysis of the compliance of the French trust framework with the eIDAS implementing regulation (EU) 2015/1502:

- *N2_FranceConnect+_LOA_Mapping*;
- *N3_LIN_LOA_Mapping*.

4.2.1 **Enrolment**

a) Application and registration
The different steps and processes are detailed in the *N3_LIN_LOA_Mapping* document.

[2] 5.11.2015 L 289/23 Official Journal of the European Union EN (1)Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 7).

b) Identity proofing and verification (natural person)
The different steps and processes are detailed in the *N3_LIN_LOA_Mapping* document.
b) Identity proofing and verification (legal person)
Not applicable
d) Binding between the electronic identification means of natural and legal persons
Not applicable

4.2.2 **Electronic identification means management**

a) Electronic identification means characteristics and design (including, where appropriate, information on security certification)
The different steps and processes are detailed in the *N3_LIN_LOA_Mapping* document.
b) Issuance, delivery and activation
The different steps and processes are detailed in the *N3_LIN_LOA_Mapping* document, section 2.2.2.
c) Suspension, revocation and reactivation
The different steps and processes are detailed in the *N3_LIN_LOA_Mapping* document, section 2.2.3.
d) Renewal and replacement
The different steps and processes are detailed in the *N3_LIN_LOA_Mapping* document, section 2.2.4.

4.2.3 Authentication

Describe the authentication mechanism including terms of access to authentication by relying parties other than public sector bodies

See documents:

- *N2_FranceConnect+_LOA_Mapping*;
- *N3_LIN_LOA_Mapping*.

Describe the management and organisation of the following aspects:

a) General provisions concerning management and organisation
The different steps and processes are detailed in the following documents: • *G4_Supervision;* • *G5_Obligations.*
b) Published notices and user information
The different steps and processes are detailed in the following documents: • *G4_Supervision;* • *General conditions of use of the FranceConnect service for Users (use the browser translation option to have the English version);* • *General conditions of use of the L'Identité Numérique La Poste service for Users (use the browser translation option to have the English version);* • *FranceConnect+ User Portal (use the browser translation option to have the English version of the site);* • *L'Identité Numérique La Poste User Portal (use the browser translation option to have the English version of the site).*

c) Information Security Management
The different steps and processes are detailed in the *G4_Supervision* document, *§5, 6, 7, 8, 10*.
d) Retention of information
The different steps and processes are detailed in the following documents: • *N2_FranceConnect+_LOA_Mapping, section 2.4.4*; • *N3_LIN_LOA_Mapping, section 2.4.4;* • *N4_French_eID_LOA_Mapping*.
e) Facilities and personnel
The different steps and processes are detailed in the *G4_Supervision* document.
f) Technical checks
The different steps and processes are detailed in the following documents: • *N2_FranceConnect+_LOA_Mapping, section 2.4.6*; • *N3_LIN_LOA_Mapping, section 2.4.6.*
g) Compliance and audit
The different steps and processes are detailed in the following documents: • *N2_FranceConnect+_LOA_Mapping, section 2.4.7*; • *N3_LIN_LOA_Mapping, section 2.4.7;* • *N4_French_eID_LOA_Mapping, article 10.*

4.3. Interoperability requirements

Describe how the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501 ([3]) are met. List and attach any document that may give further information on compliance, such as the opinion of the Cooperation Network, external audits, etc.

The French eID scheme is based on custom development and is fully compliant with the eIDAS technical specifications, including crypto and operational security aspects.

- The French eIDAS Bridge Service is able to connect with other Member States in both the test environment and in production and are fully integrated and operational.
- The French eIDAS Bridge Service is developed according to approved eIDAS technical requirements and does not impose costs or additional issues for other Member States.
- The French eIDAS Bridge Service does not store any personal data, except for the purposes specified in Article 9(3).

The French eID scheme is used exclusively for the identification of natural persons.

For more details, refer to *N4_French_eID_LOA_Mapping.*

The following documents provide additional information on compliance:

- *A1_FranceConnect+_ISO27001_Attestation_FR*: ISO 27001:2013 certificate issued by LSTI to FranceConnect+;
- *A2_FranceConnect+_ANSSI_Formal_Decision_FR*: FranceConnect+ eIDAS certificate of conformity with substantial and high levels of guarantee issued by ANSSI;

[3] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 1).

- *A3_LIN_ANSSI_Formal_Decision*: L'identité Numérique La Poste eIDAS certificate of conformity with substantial level of guarantee issued by ANSSI;
- *A4_AR24_ANSSI_Formal_Qualification_Decision*: ANSSI qualification decision for the AR24 service.

4.4. Supporting documents

List here all supporting documentation submitted and state to which of the elements above they relate. Include any domestic legislation which relates to the electronic identification provision relevant to this notification. Submit an English version or English translation whenever available.

All supporting documents for scheme notification are mentioned in the *G0_Index_Documentation* document.