

ReFineID – déclaration d'un moyen de cryptologie

Déclaration de fourniture et de transfert depuis un État membre de l'Union européenne d'un moyen de cryptologie, au titre de l'article 30 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et du chapitre II du décret n° 2007-663 du 2 mai 2007.

ReFineID est un intergiciel qui permet aux titulaires d'une carte nationale d'identité finlandaise résidant en France de l'utiliser comme identité numérique sur les plateformes Apple.

Le déclarant demande la délivrance de l'attestation de déclaration.

A. Déclarant (personne physique)

Nom et prénoms	Koistinen, Petri
Nationalité	finlandaise
Adresse	Niittaajankatu 8a A 21, 00810 Helsinki, Finlande
Numéro de téléphone	+358 44 956 4098
Adresse de courrier électronique	petri.koistinen@iki.fi

B. Moyen de cryptologie auquel s'applique la déclaration

B.1. Informations générales sur le moyen

Nom	ReFineID
Désignation générique	Intergiciel pour carte nationale d'identité
Référence commerciale	Aucune
Version	26
Date prévue de mise sur le marché	1er novembre 2026
Plateformes	iOS, iPadOS, macOS

B.2. Description fonctionnelle du moyen

B.2.1. Classez le moyen dans la ou les catégorie(s) correspondante(s)

Logiciel.

B.2.2. Description générale du moyen

Le moyen lit la carte via l'antenne NFC du téléphone ou un lecteur de carte à contact, publie le certificat d'authentification et la clé publique de la carte dans le trousseau du système par CryptoTokenKit, et transmet les demandes de signature à la carte. Safari et les autres applications du système s'authentifient ensuite avec la carte comme avec tout autre certificat client.

B.2.3. Indiquez à quelle catégorie se rapporte la fonction principale du moyen

Sécurité de l'information (bibliothèque et intergiciel cryptographiques).

B.3. Description technique des services de cryptologie fournis

B.3.1. Description des fonctionnalités cryptographiques du moyen

Messagerie sécurisée avec la carte, signatures d'authentification client et signatures de documents PAdES.

B.3.2. Indiquez à quelle(s) catégorie(s) se rapporte(nt) la ou les fonctions cryptographiques du moyen

Authentification, intégrité, confidentialité et signature.

B.3.3. Indiquez le(s) protocole(s) sécurisé(s) utilisés par le moyen

PACE et messagerie sécurisée ISO/IEC 7816-4.

B.3.4. Précisez les algorithmes cryptographiques utilisés et leurs longueurs maximales de clés

Algorithme	Mode	Taille de clé	Fonction
ECDH sur brainpoolP384r1	PACE	384 bits	Accord de clés
AES	CBC	256 bits	Chiffrement
AES	CMAC	256 bits	Intégrité
SHA-256	s.o.	s.o.	Dérivation de clés
SHA-224, SHA-256, SHA-384, SHA-512	s.o.	s.o.	Condensats de signature
ECDSA sur NIST P-384	s.o.	384 bits	Signature
RSA	PKCS#1 v1.5	3072 bits	Signature
RSA	PSS	3072 bits	Signature

Gestion des clés

- Les clés privées sont générées dans la carte par l'autorité émettrice et n'en sortent jamais.

C. Cas d'un moyen de cryptologie relevant de la catégorie 3 de l'annexe 2 du décret n° 2007-663 du 2 mai 2007

Le déclarant déclare que le moyen relève de la catégorie 3.

Présentez le mode de commercialisation du moyen de cryptologie et le marché auquel il s'adresse

Le moyen sera mis à disposition du public sur l'App Store d'Apple.

Expliquez pourquoi la fonctionnalité cryptographique du moyen ne peut pas être modifiée facilement par l'utilisateur

La suite cryptographique de la carte à puce finlandaise délivrée par l'État ne peut pas être modifiée par l'utilisateur.

Expliquez en quoi les modalités d'installation du moyen ne nécessitent pas d'assistance importante ultérieure de la part du fournisseur

L'utilisateur installe l'application, simple d'utilisation, sans intervention du fournisseur.

D. Renouvellement d'autorisation de transfert ou d'exportation

Aucune autorisation antérieure.

E. Pièces à joindre

ReFineID est un logiciel libre. Le code source et la documentation sont disponibles ici :

<https://github.com/ReFineID/ReFineID-Apple>

F. Attestation

Je soussigné, Koistinen Petri, agissant en qualité de fournisseur et pour mon propre compte, certifie que les renseignements figurant dans le présent dossier sont exacts et ont été établis de bonne foi, et m'engage à porter à la connaissance de l'Agence nationale de la sécurité des systèmes d'information, sans délai, tout élément nouveau de fait ou de droit de nature à modifier la présente déclaration.

Fait à Helsinki, le 7 août 2026.

Ce document est signé électroniquement. La signature est une signature électronique qualifiée : en vertu de l'article 25, paragraphe 2, du règlement (UE) n° 910/2014, elle a un effet juridique équivalent à celui d'une signature manuscrite. Validation en ligne et gratuite à l'adresse <https://dvv.fineid.fi/en/validation>, entre autres services.