Rédacteur : Timothée Rusch — Ingénieur cybersécurité, DSI CHU de Nantes **Date :** 25/08/2026 **Version :** 1.0	Intitulé **Annexe technique — Exigences applicables aux solutions SaaS émettant des messages électroniques au nom du CHU de Nantes**

1. Objet

Cette annexe technique définit les exigences applicables à toute solution SaaS amenée à émettre des messages électroniques au nom du CHU de Nantes (notification, transactionnel, campagne, portail patient, etc.). Elle a pour objectif de garantir la traçabilité, l'authentification et la protection de la réputation des domaines de messagerie du CHU, dans le cadre de la politique DMARC en p=reject déployée sur l'ensemble du parc GHT 44.

2. Périmètre

Ces exigences s'appliquent à tout éditeur ou prestataire SaaS émettant des courriels affichant une adresse d'expédition sous le domaine chu-nantes.fr ou l'un de ses sous-domaines, quel que soit le canal (API, SMTP relais, plateforme marketing, outil RH, module métier tiers…).

3. Exigences techniques obligatoires

Toute solution SaaS candidate à l'émission de messages au nom du CHU doit répondre aux quatre exigences suivantes, détaillées ci-dessous.

Exigence	Description
Sous-domaine dédié	L'éditeur doit être en capacité d'émettre les messages depuis une adresse rattachée à un sous-domaine applicatif dédié, de la forme expediteur@nomapplication.chu-nantes.fr, jamais depuis le domaine racine chu-nantes.fr.
Signature DKIM	L'éditeur signe chaque message avec une clé DKIM (RSA 2048 bits minimum) propre au sous-domaine et fournit la clé publique correspondante (sélecteur + valeur TXT) à intégrer dans la zone DNS du CHU.
Enregistrement SPF	L'éditeur communique les hôtes/IP autorisés à émettre pour le sous-domaine, sous une forme exploitable dans un enregistrement SPF (include, ip4/ip6) respectant la limite de 10 lookups DNS.
Alignement DMARC	Le sous-domaine doit passer l'authentification DMARC (SPF et/ou DKIM alignés) afin de rester compatible avec la politique p=reject appliquée par le CHU sur l'ensemble de ses domaines et sous-domaines.

3.1 Sous-domaine applicatif dédié

Chaque solution SaaS se voit attribuer un sous-domaine dédié de la forme nomapplication.chu-nantes.fr. Cette isolation permet :

- de circonscrire l'impact d'une éventuelle compromission ou d'un mauvais paramétrage à ce seul sous-domaine ;
- d'appliquer une politique DMARC et des règles de filtrage propres à chaque usage, sans affecter le domaine racine ni les autres applicatifs ;
- de tracer précisément, dans les rapports agrégés DMARC, l'origine de chaque flux applicatif.

L'éditeur ne doit en aucun cas émettre depuis chu-nantes.fr directement ni depuis un sous-domaine non validé par le CHU.

3.2 Signature DKIM

L'éditeur doit signer l'intégralité des messages sortants avec une clé DKIM dédiée au sous-domaine concerné (RSA 2048 bits minimum, rotation recommandée tous les 12 mois). L'éditeur fournit au CHU :

- le nom du sélecteur DKIM ;
- la clé publique correspondante, au format à publier en enregistrement TXT ;
- la confirmation que l'en-tête DKIM-Signature couvre a minima les champs From, To, Subject, Date et le corps du message (body hash).

Le CHU publie l'enregistrement DNS correspondant et confirme sa propagation avant activation des envois en production.

3.3 Enregistrement SPF

L'éditeur communique la liste exhaustive des hôtes et adresses IP autorisés à émettre pour le compte du sous-domaine (mécanismes include, ip4, ip6). Le CHU intègre ces éléments dans un enregistrement SPF propre au sous-domaine, en veillant à :

- respecter la limite de 10 lookups DNS imposée par la RFC 7208 ;
- privilégier un qualifieur strict (-all) une fois la solution validée en production ;
- documenter toute évolution des plages d'émission communiquée ultérieurement par l'éditeur.

3.4 Alignement DMARC — politique p=reject

Le domaine chu-nantes.fr et l'ensemble de ses sous-domaines applicatifs sont couverts par une politique DMARC p=reject. En conséquence, chaque solution SaaS doit :

- obtenir un alignement DMARC (SPF et/ou DKIM aligné avec le domaine From) sur 100 % des flux avant bascule en production ;
- accepter une phase probatoire en p=none, puis p=quarantine, pilotée par le CHU sur la base des rapports agrégés (rua) et, si besoin, des rapports d'échec (ruf) ;
- signaler sans délai tout changement d'infrastructure d'envoi (nouvelle IP, nouveau relais, nouveau prestataire technique) susceptible de casser l'alignement SPF/DKIM.

Tout flux non aligné à l'issue de la phase probatoire sera rejeté par les serveurs de messagerie destinataires appliquant la politique DMARC du CHU.

4. Processus de mise en œuvre

N°	Étape	Responsable
1	Recensement du besoin et validation du nom de sous-domaine applicatif (nomapplication.chu-nantes.fr).	CHU (RSSI / DSI)
2	Transmission par l'éditeur du sélecteur et de la clé publique DKIM, de la politique SPF souhaitée (hôtes/IP émetteurs) et de l'adresse d'expédition.	Éditeur SaaS
3	Création des enregistrements DNS (SPF, DKIM, DMARC en mode p=none puis p=quarantine) dans la zone chu-nantes.fr.	CHU (équipe cybersécurité)
4	Phase d'observation : contrôle des rapports agrégés DMARC (rua) et vérification de l'alignement SPF/DKIM sur les envois réels.	CHU / Éditeur
5	Bascule du sous-domaine en p=reject une fois l'alignement confirmé sans faux positif.	CHU (équipe cybersécurité)

5. Modèle d'enregistrements DNS attendus

Le tableau suivant synthétise, à titre d'exemple, les enregistrements DNS à faire compléter par l'éditeur puis à publier par le CHU pour un sous-domaine nomapplication.chu-nantes.fr :

Type	Nom	Valeur (exemple à faire compléter par l'éditeur)	Porteur
TXT	nomapplication.chu-nantes.fr	v=spf1 include:_spf.<editeur>.com -all	Éditeur → CHU
TXT	<sélecteur>._domainkey.nomapplication.chu-nantes.fr	v=DKIM1; k=rsa; p=<clé publique fournie par l'éditeur>	Éditeur → CHU
TXT	_dmarc.nomapplication.chu-nantes.fr	v=DMARC1; p=reject; rua=mailto:<adresse de reporting CHU>; ruf=mailto:<adresse de reporting CHU>; fo=1	CHU

6. Contact

Toute demande d'ouverture de sous-domaine applicatif ou toute question relative à la présente annexe est à adresser à l'équipe Cybersécurité de la DSI du CHU de Nantes.