Constat technique personnel — masquage de l’adresse dans le certificat de scolarité

Date du constat : 14 septembre 2026
Fichier examiné : `certificat-scolarite [ l'enfant en danger ].pdf` **Courriel source examiné :** `Re_ Réponse à votre e-mail du 04_09_2026 - 'EEPU--ST-GERMAIN-SUR-AY .' (ce.0501780n@ac-normandie.fr) - 2026-09-07 1346.eml`

---

1. Origine du fichier analysé et établissement de sa provenance

1.1. Le courriel original comme point de départ du constat

Je prends comme point de départ de mon analyse le **courriel original au format EML** dans lequel le certificat de scolarité m’a été transmis en pièce jointe.

Fichier EML examiné :

```
Re_ Réponse à votre e-mail du 04_09_2026 - 'EEPU--ST-GERMAIN-SUR-AY .' (ce.0501780n@ac-normandie.
```

Taille constatée :

```
8 783 291 octets
```

Empreintes calculées sur le fichier EML brut :

```
SHA-256 : 93f8f0fccaef929be8f3763d608746cd8e5dd19e3fd91853af11c9692908b13c
SHA-512 : e5c8dd4392f17d9ec1a9a5973bf3311a98624d25012dace6700b2e33bc3b418b728caa15ef182fc3b16c5df
```

Ces empreintes permettent de figer l’exemplaire du courriel utilisé pour le présent constat.

1.2. Identité déclarée de l’expéditeur et contexte du message

Les en-têtes du courriel indiquent :

```
Date: Mon, 07 Sep 2026 13:46:23 +0200
From: "EEPU--ST-GERMAIN-SUR-AY ." <ce.0501780n@ac-normandie.fr>
To: [ mère défendante ]
Cc: "DSDEN50-CIRCONSCRIPTION-1ER-DEGRE-IEN-CARENTAN ." <dsden50-ien-carentan@ac-normandie.fr>
Subject: Re: Réponse à votre e-mail du 04/09/2026
Message-ID: <900341911.19650753.1788781582960.JavaMail.zimbra@msg.education.gouv.fr>
Return-Path: <ce.0501780n@ac-normandie.fr>
X-Mailer: Zimbra 10.1.18_GA_4890 (ZCS/10.1.18_GA_4890)
```

Le corps du message indique expressément que des documents sollicités sont joints au courriel et cite en premier lieu :

```
- le certificat de scolarité de [ l'enfant en danger ] pour l'année scolaire 2026-2027
```

Le message se termine par :

```
Cordialement,

Florian CONSUL
Directeur de l'école de Saint Germain sur Ay
```

Je constate donc que le courriel se présente comme un message émis depuis la boîte institutionnelle de l'école `ce.0501780n@ac-normandie.fr`, que son contenu annonce explicitement l'envoi du certificat, et que ce contenu est signé au nom de **Florian CONSUL, directeur de l'école de Saint-Germain-sur-Ay**.

1.3. Traçabilité par les serveurs de messagerie

Les en-têtes `Received` permettent de reconstituer la progression du message dans l'infrastructure de messagerie.

Je constate notamment la chronologie suivante, toutes les heures étant ramenées à l'heure française CEST (`+02:00`) :

```
07/09/2026 13:46:23  pr-store28.msg.in.phm.education.gouv.fr
                         -> pr-mta-mailstore-out02.localdomain

07/09/2026 13:46:23  pr-mta-mailstore-out02.msg.in.phm.education.gouv.fr
                         -> pr-antivirus-externe-out05.msg.in.phm.education.gouv.fr

07/09/2026 13:46:29  pr-antivirus-externe-out05.msg.in.phm.education.gouv.fr
                         -> pr-mta-externe-out08.localdomain

07/09/2026 13:46:30  messagerie.education.gouv.fr [193.54.151.84]
                         -> mx.google.com
                         connexion ESMTPS TLS 1.3
                         TLS_AES_256_GCM_SHA384

07/09/2026 13:46:32  remise dans l'infrastructure Google du destinataire
```

Je constate ainsi une continuité temporelle de quelques secondes entre les serveurs internes de l'Éducation nationale, le serveur de sortie public `messagerie.education.gouv.fr`, puis les serveurs Google du destinataire.

1.4. Authentification SPF, DKIM et DMARC constatée par Google

Le serveur de réception Google a enregistré les résultats d'authentification suivants :

```
Authentication-Results: mx.google.com;
    dkim=pass header.i=@ac-normandie.fr header.s=msg-nat header.b=ITwv4QFg;
    spf=pass (...) smtp.mailfrom=ce.0501780n@ac-normandie.fr;
    dmarc=pass (...) header.from=ac-normandie.fr
```

Le contrôle SPF précise en outre :

```
Received-SPF: pass
client-ip=193.54.151.84
```

et indique que l'adresse IP publique `193.54.151.84` était autorisée à émettre pour l'adresse d'enveloppe :

```
ce.0501780n@ac-normandie.fr
```

Je constate donc que, lors de la réception du message, **Google a validé SPF, DKIM et DMARC** pour le domaine institutionnel `ac-normandie.fr`.

Cette concordance est importante : il ne s'agit pas seulement d'une adresse `From:` affichée dans un logiciel de messagerie. Le serveur destinataire a vérifié que le message provenait d'une infrastructure autorisée pour ce domaine et que la signature DKIM du domaine était valide.

1.5. Signature DKIM et protection du corps MIME contenant la pièce jointe

Le courriel contient la signature DKIM suivante :

```
DKIM-Signature: v=1;
 a=rsa-sha256;
 c=relaxed/relaxed;
 d=ac-normandie.fr;
 s=msg-nat;
 t=1788781589;
 bh=licq1Nw1nppdYYhWYNojxwaJEhfQ2087d0iqebzioYE=;
 h=Date:From:To:Message-ID:Subject:Content-Type;
 ...
```

Le timestamp DKIM :

```
t=1788781589
```

correspond à :

```
07 septembre 2026 à 13:46:29 CEST (+02:00)
```

La liste :

```
h=Date:From:To:Message-ID:Subject:Content-Type
```

indique notamment les en-têtes couverts par la signature DKIM.

La valeur :

```
bh=licq1Nw1nppdYYhWYNojxwaJEhfQ2087d0iqebzioYE=
```

est l'empreinte SHA-256, encodée en Base64, du corps du message après canonisation DKIM `relaxed`.

J'ai recalculé cette empreinte à partir du **corps MIME brut du fichier EML examiné**, en appliquant la canonisation `relaxed` indiquée par la signature.

Résultat obtenu :

```
licq1Nw1nppdYYhWYNojxwaJEhfQ2087d0iqebzioYE=
```

Cette valeur est **strictement identique** au champ `bh=` de la signature DKIM.

Je constate donc que le corps MIME présent dans l'EML est exactement celui auquel se rapporte l'empreinte de corps de la signature DKIM.

La pièce jointe PDF est située à l'intérieur de ce corps MIME, sous la forme :

```
Content-Type: application/pdf; name="certificat-scolarite [ l'enfant en danger ].pdf"
Content-Disposition: attachment;
 filename="certificat-scolarite [ l'enfant en danger ].pdf"
Content-Transfer-Encoding: base64
```

puis commence par les données Base64 :

```
JVBERi0xLjcKJeLjz9MKNSAwIG9iago8PC9GaWx0ZXIvRmxhdGVEZWNvZGUvR...
```

Ainsi, les données Base64 de la pièce jointe font partie du corps du message dont Google a constaté la validité DKIM (`dkim=pass`).

1.6. Scellement ARC ajouté par Google

Le courriel comporte également des en-têtes ARC ajoutés par Google, notamment :

```
ARC-Seal: i=1; a=rsa-sha256; ... d=google.com; s=arc-20260327; ...
ARC-Message-Signature: i=1; a=rsa-sha256; ... d=google.com; ...
ARC-Authentication-Results: i=1; mx.google.com;
    dkim=pass ...;
    spf=pass ...;
    dmarc=pass ...
```

Je constate donc que Google a non seulement enregistré les résultats d'authentification, mais a également intégré ces résultats dans une chaîne ARC lors de la réception du message.

1.7. Extraction de la pièce jointe Base64 et identité exacte avec le PDF analysé

J'ai extrait la pièce jointe directement du fichier EML en décodant le contenu MIME Base64, sans passer par un réenregistrement dans un lecteur PDF.

La pièce jointe extraite est :

```
certificat-scolarite [ l'enfant en danger ].pdf
```

Sa taille après décodage Base64 est :

```
38 492 octets
```

Empreintes du PDF extrait directement de l'EML :

```
SHA-256 : 7bf1068a69f04789fb345bef80a21163be9813e3e66d1164f031dbeb0547af3d
SHA-512 : 4391b8f32ab7fc07be1b1ba926f8b2f54834685904e4ed1c3a9e68f3f2b9f44a6eaf8a5d8e7931791dda67e
```

L'empreinte SHA-512 est exactement celle du PDF faisant l'objet de mon analyse :

```
4391b8f32ab7fc07be1b1ba926f8b2f54834685904e4ed1c3a9e68f3f2b9f44a6eaf8a5d8e7931791dda67efb0c225eca
```

J'ai également effectué une comparaison binaire entre :

1. le PDF extrait directement du MIME Base64 du courriel ;
2. le fichier `certificat-scolarite [ l'enfant en danger ].pdf` examiné dans la suite du présent constat.

Résultat :

```
IDENTIQUE OCTET PAR OCTET
```

Je constate donc qu'il ne s'agit pas simplement de deux documents portant le même nom : **le fichier analysé est exactement, bit pour bit, le fichier PDF contenu en pièce jointe dans le courriel institutionnel du 7 septembre 2026**.

1.8. Chaîne technique de provenance que je peux établir

Au regard des éléments précédents, j'établis la chaîne technique suivante :

```
Boîte / infrastructure Éducation nationale

          From: ce.0501780n@ac-normandie.fr
          corps signé : Florian CONSUL, Directeur

Serveurs internes education.gouv.fr


Serveur de sortie public
messagerie.education.gouv.fr
193.54.151.84

          DKIM ac-normandie.fr
          SPF = PASS
          DMARC = PASS

Google / Gmail
07/09/2026 vers 13:46:30 CEST

          DKIM = PASS
          ARC Google

Corps MIME authentifié

          texte du courriel signé « Florian CONSUL »

          pièce jointe Base64
             certificat-scolarite [ l'enfant en danger ].pdf

                       décodage Base64

                PDF de 38 492 octets

                       SHA-512

4391b8f32ab7fc07be1b1ba926f8b2f54834685904e4ed1c3a9e68f3f2b9f44a6eaf8a5d8e7931791dda67efb0c225eca


             PDF analysé ci-après
```

1.9. Attribution de l'envoi à Florian CONSUL

Je distingue ici ce qui résulte directement des éléments techniques de ce que je connais personnellement du contexte de l'école.

Sur le plan technique, la provenance du fichier est établie de manière cohérente et concordante : le PDF analysé est exactement la pièce jointe du message reçu par Gmail

; le message a été émis par l'infrastructure institutionnelle et les contrôles Google indiquent `SPF=pass`, `DKIM=pass` et `DMARC=pass` pour `ac-normandie.fr` ; le corps authentifié du message annonce l'envoi du certificat et est signé « Florian CONSUL, Directeur de l'école de Saint Germain sur Ay ».

Je constate donc que **ce PDF précis a été transmis dans un courriel authentifié provenant de la boîte institutionnelle `ce.0501780n@ac-normandie.fr`, avec un contenu rédigé à la première personne et signé par Florian CONSUL en sa qualité de directeur**.

À cela s'ajoute le contexte concret que je connais personnellement : il s'agit d'une **petite école**, avec un fonctionnement local direct, et ce courriel s'inscrit dans mes échanges avec son directeur. Au regard de cette concordance entre l'adresse institutionnelle, l'infrastructure de l'Éducation nationale, le contenu du message, sa signature nominative et le contexte réel de l'établissement, **je considère certain que ce courriel et le PDF qui y est joint ont été envoyés par Florian CONSUL**.

Cette conclusion d'attribution ne repose donc pas sur le seul champ `From:` ni sur la seule signature DKIM : elle résulte de la **concordance de plusieurs éléments techniques et contextuels indépendants**.

Les mécanismes SPF, DKIM, DMARC et ARC, pris isolément, n'identifient pas physiquement la personne assise devant un poste informatique. Cette limite théorique doit être rappelée. Toutefois, dans le présent cas, **je ne constate dans le message examiné aucun élément technique contradictoire avec l'attribution à Florian CONSUL**, tandis que l'ensemble des éléments disponibles converge vers lui comme émetteur du courriel et de la pièce jointe.

Je distingue enfin cette question de celle de l'auteur matériel de l'annotation blanche : **l'analyse du courriel permet d'attribuer l'envoi du PDF à Florian CONSUL ; elle ne suffit pas, à elle seule, à démontrer qu'il a personnellement réalisé le tracé blanc dans le PDF.**

1.10. Concordance temporelle avec la modification du PDF

Le PDF transmis dans ce courriel contient, comme détaillé plus loin, les métadonnées suivantes :

```
Annotation blanche : 07/09/2026 11:06:42 +02:00
ModDate du PDF     : 07/09/2026 11:06:44 +02:00
```

Le message est ensuite pris en charge par l'infrastructure de messagerie à :

`07/09/2026 13:46:23 +02:00`

La signature DKIM est horodatée à :

`07/09/2026 13:46:29 +02:00`

Le fichier PDF envoyé par courriel étant **identique octet par octet** au fichier contenant l'annotation, je constate que la version comportant ce masquage était déjà intégrée à la pièce jointe au moment de l'envoi institutionnel.

Les heures internes du PDF restent des métadonnées techniquement modifiables et doivent être appréciées avec cette réserve. En revanche, l'envoi du **fichier exact identifié par son empreinte** est, lui, rattaché au courriel reçu le 7 septembre 2026 vers 13:46 par la chaîne de messagerie décrite ci-dessus.

---

2. Objet du constat

Je souhaite consigner de manière factuelle ce que je constate dans le fichier PDF intitulé :

`certificat-scolarite [ l'enfant en danger ].pdf`

Mon objectif est de vérifier si l'adresse de domicile figurant dans le document a réellement été supprimée du fichier, ou si elle est toujours présente dans le contenu du PDF mais simplement masquée visuellement par un élément graphique ajouté par-dessus.

Le présent document constitue un **constat technique personnel** fondé sur l'examen du fichier numérique lui-même. Il ne constitue pas, à lui seul, une expertise judiciaire et ne permet pas d'identifier avec certitude l'auteur matériel d'une modification.

---

3. Identification et empreinte du fichier examiné

Afin de figer précisément le fichier sur lequel porte mon constat, j'en calcule l'empreinte SHA-512.

Commande utilisée :

```
sha512sum "certificat-scolarite [ l'enfant en danger ].pdf"
```

Résultat :

```
4391b8f32ab7fc07be1b1ba926f8b2f54834685904e4ed1c3a9e68f3f2b9f44a6eaf8a5d8e7931791dda67efb0c225eca
```

Cette empreinte SHA-512 est celle du fichier examiné dans le présent constat.

Taille du fichier constatée :

```
38 492 octets
```

---

4. Premier constat : l'adresse est toujours présente dans le contenu textuel du PDF

J'extrais le texte du PDF avec l'outil `pdftotext` :

```
pdftotext -layout "certificat-scolarite [ l'enfant en danger ].pdf" -
```

L'extraction fait apparaître notamment :

```
Domiciliée : 22 RUE ERMICE
             50430 SAINT-GERMAIN-SUR-AY
```

Je constate donc que l'adresse n'a pas été supprimée du contenu numérique du PDF.

Elle reste présente sous forme de texte exploitable et extractible, même si elle est masquée visuellement lors de l'affichage normal du document.

---

5. Constat dans le flux de contenu de la page

Après décompression du flux de contenu de la page PDF, je retrouve les instructions de dessin du texte suivantes :

```
q
BT
/F1 10.5 Tf
45 600.56 Td
(Domiciliée : )Tj
ET
Q

q
BT
/F1 10.5 Tf
99.83 600.56 Td
(22 RUE ERMICE)Tj
ET
Q

q
BT
/F1 10.5 Tf
99.83 587.96 Td
(50430 SAINT-GERMAIN-SUR-AY)Tj
ET
Q
```

Les opérateurs PDF utilisés ont une signification précise :

- `BT` / `ET` délimitent une séquence de texte ;
- `Tf` sélectionne la police et sa taille ;
- `Td` positionne le texte sur la page ;
- `Tj` affiche effectivement la chaîne de caractères dans la page.

Je constate ainsi que le PDF contient explicitement les chaînes :

```
Domiciliée :
22 RUE ERMICE
50430 SAINT-GERMAIN-SUR-AY
```

Le texte fait donc toujours partie du contenu de la page.

---

6. Présence d’une annotation ajoutée sur la page

L’examen de la structure PDF montre que la page comporte une référence à des annotations :

```
/Annots 9 0 R
```

L’objet référencé contient notamment :

```
9 0 obj
[ 10 0 R 11 0 R]
endobj
```

L'objet `10 0` est une annotation de type `Ink` :

```
10 0 obj
<<
/Type/Annot
/Subtype/Ink
/P 4 0 R
/F 4
/M(D:20260907110642+02'00')
/NM(2b17500f-e464-4c38-a051-b1ea68aea5a3)
/Rect[ 26.305645 580.210205 275.053528 620]
/C[ 1 1 1]
/CA 1
/CreationDate(D:20260907110642+02'00')
/BS<</Type/Border/W 18/S/S>>
/InkList[
...
]
/AP<</N 12 0 R>>
>>
```

Je constate plusieurs éléments techniques importants.

6.1. Type de l'annotation

```
/Subtype/Ink
```

Il s'agit d'une annotation graphique de type « encre », c'est-à-dire d'un tracé ajouté sur la page.

6.2. Couleur de l'annotation

```
/C[ 1 1 1]
```

En espace RGB PDF, les valeurs `[1 1 1]` correspondent au **blanc pur**.

6.3. Opacité

```
/CA 1
```

La valeur `1` correspond à une opacité de 100 %.

Le tracé est donc complètement opaque.

6.4. Épaisseur du tracé

```
/BS<</Type/Border/W 18/S/S>>
```

La largeur du trait est de **18 points**, ce qui correspond à un trait particulièrement épais destiné à recouvrir une zone importante.

---

7. L'apparence graphique confirme un tracé blanc épais

L'objet d'apparence associé à l'annotation contient notamment :

```
1.000 1.000 1.000 RG
18.00 w
1 J
1 j
...
```

Je constate que :

```
1.000 1.000 1.000 RG
```

fixe la couleur du contour à blanc pur, tandis que :

```
18.00 w
```

fixe la largeur du trait à 18 points.

Ces instructions confirment directement que l'annotation est rendue sous la forme d'un **trait blanc très épais**.

---

8. Concordance entre la zone du texte et la zone de l'annotation

Le texte de l'adresse est positionné dans le flux de la page aux coordonnées suivantes :

```
« Domiciliée : »                  y = 600.56
« 22 RUE ERMICE »                 y = 600.56
« 50430 SAINT-GERMAIN-SUR-AY »    y = 587.96
```

L'annotation blanche possède le rectangle englobant suivant :

```
/Rect[ 26.305645 580.210205 275.053528 620]
```

Soit approximativement :

```
x : 26,31 à 275,05
y : 580,21 à 620,00
```

Je constate que les deux lignes constituant l'adresse, situées aux ordonnées `600.56` et `587.96`, se trouvent à l'intérieur de cette zone.

La position horizontale du texte est également comprise dans le rectangle de l'annotation.

Il existe donc une concordance directe entre :

1. la position du texte contenant l'adresse ;
2. la position du tracé blanc ajouté à la page.

Je constate que l'annotation blanche recouvre précisément la zone dans laquelle l'adresse est dessinée.

---

9. Constat d’une modification incrémentale du PDF

Je constate également que le fichier contient une première fin de structure PDF :

```
startxref
16479
%%EOF
```

Puis, après cette première marque de fin de fichier, de nouveaux objets sont ajoutés, notamment :

```
4 0 obj
...
/Annots 9 0 R
...
endobj

9 0 obj
[ 10 0 R 11 0 R]
endobj

10 0 obj
<</Type/Annot/Subtype/Ink ... >>
```

Le fichier possède ensuite un nouveau `trailer` comprenant :

```
/Prev 16479
```

puis une seconde fin :

```
startxref
38114
%%EOF
```

Je constate donc que le PDF contient **deux états successifs enregistrés dans le même fichier**.

La présence de `/Prev 16479` indique que la dernière structure PDF renvoie vers la table de références de la version précédente.

Cela correspond au mécanisme PDF appelé **mise à jour incrémentale** : le logiciel n’écrase pas nécessairement l’intégralité du document d’origine, mais ajoute à la fin du fichier les objets nouveaux ou modifiés.

Dans le présent fichier, la révision ajoutée contient notamment la référence aux annotations ainsi que l’annotation blanche de type `Ink`.

---

10. Dates internes constatées

Les métadonnées générales du PDF indiquent :

```
CreationDate : D:20260904175312+02'00'
ModDate      : D:20260907110644+02'00'
```

L’annotation blanche contient quant à elle :

```
/M            : D:20260907110642+02'00'
/CreationDate : D:20260907110642+02'00'
```

Je constate donc, selon les métadonnées internes du fichier :

- une date de création du document au **4 septembre 2026 à 17:53:12 +02:00** ;
- une date associée à la création/modification de l'annotation au **7 septembre 2026 à 11:06:42 +02:00** ;
- une date de modification générale du PDF au **7 septembre 2026 à 11:06:44 +02:00**.

La différence entre l'heure de l'annotation et celle de la modification générale du document est donc d'environ deux secondes.

Je précise toutefois que les dates contenues dans les métadonnées d'un fichier PDF peuvent techniquement être modifiées. Elles constituent donc un élément technique à conserver, mais ne suffisent pas, isolément, à identifier une personne ou à établir avec certitude le moment réel d'une action.

---

11. Vérifications reproductibles en ligne de commande

11.1. Vérifier le courriel source et extraire la pièce jointe sans modification

Empreinte du fichier EML :

```
sha512sum "Re_ Réponse à votre e-mail du 04_09_2026 - 'EEPU--ST-GERMAIN-SUR-AY .' (ce.0501780n@ac
```

Résultat attendu :

```
e5c8dd4392f17d9ec1a9a5973bf3311a98624d25012dace6700b2e33bc3b418b728caa15ef182fc3b16c5df5dae2831b3
```

Exemple d'extraction du PDF avec la bibliothèque standard Python :

```
python3 - <<'PYEXTRACT'
from email import policy
from email.parser import BytesParser
from pathlib import Path

eml = Path("Re_ Réponse à votre e-mail du 04_09_2026 - 'EEPU--ST-GERMAIN-SUR-AY .' (ce.0501780n@a
msg = BytesParser(policy=policy.default).parsebytes(eml.read_bytes())

for part in msg.iter_attachments():
    if part.get_filename() == "certificat-scolarite [ l'enfant en danger ].pdf":
        Path("certificat-extrait-de-eml.pdf").write_bytes(part.get_payload(decode=True))
        break
PYEXTRACT

sha512sum "certificat-extrait-de-eml.pdf" \
          "certificat-scolarite [ l'enfant en danger ].pdf"

cmp -s "certificat-extrait-de-eml.pdf" \
       "certificat-scolarite [ l'enfant en danger ].pdf" \
  && echo "IDENTIQUE OCTET PAR OCTET"
```

Les deux SHA-512 doivent être identiques et `cmp` doit afficher :

IDENTIQUE OCTET PAR OCTET

11.2. Vérifier l'empreinte du fichier

```
sha512sum "certificat-scolarite [ l'enfant en danger ].pdf"
```

Résultat attendu :

```
4391b8f32ab7fc07be1b1ba926f8b2f54834685904e4ed1c3a9e68f3f2b9f44a6eaf8a5d8e7931791dda67efb0c225eca
```

11.3. Vérifier que l'adresse reste extractible

```
pdftotext -layout "certificat-scolarite [ l'enfant en danger ].pdf" -
```

On doit notamment retrouver :

```
Domiciliée : 22 RUE ERMICE
             50430 SAINT-GERMAIN-SUR-AY
```

11.4. Rechercher l'annotation dans le fichier brut

```
grep -aobF '/Annots 9 0 R' "certificat-scolarite [ l'enfant en danger ].pdf"
grep -aobF '/Subtype/Ink' "certificat-scolarite [ l'enfant en danger ].pdf"
grep -aobF '/C[ 1 1 1]' "certificat-scolarite [ l'enfant en danger ].pdf"
grep -aobF '/CA 1' "certificat-scolarite [ l'enfant en danger ].pdf"
grep -aobF '/W 18' "certificat-scolarite [ l'enfant en danger ].pdf"
grep -aobF '/Prev 16479' "certificat-scolarite [ l'enfant en danger ].pdf"
```

Sur le fichier examiné, je constate notamment les positions suivantes :

```
17172:/Annots 9 0 R
17249:/Subtype/Ink
17384:/C[ 1 1 1]
17407:/CA 1
17467:/W 18
38456:/Prev 16479
```

11.5. Rechercher les deux fins de structure PDF

```
grep -aobE 'startxref|%%EOF' "certificat-scolarite [ l'enfant en danger ].pdf"
```

Sur le fichier examiné :

```
16994:startxref
17010:%%EOF
38470:startxref
38486:%%EOF
```

La présence de deux séquences `startxref` / `%%EOF` est cohérente avec l'enregistrement d'une mise à jour incrémentale.

---

12. Synthèse de mes constatations

À l'issue de cet examen, je constate les éléments suivants :

1. Le point de départ de l'analyse est le courriel original au format EML, lui-même figé par une empreinte SHA-512.
2. Ce courriel est déclaré comme provenant de :

   `"EEPU--ST-GERMAIN-SUR-AY ." <ce.0501780n@ac-normandie.fr>`
3. Le message est daté du **7 septembre 2026 à 13:46:23 +02:00**, possède un `Message-ID` Zimbra de l'infrastructure `msg.education.gouv.fr`, et son corps est signé :

   ```
   Florian CONSUL
   Directeur de l'école de Saint Germain sur Ay
   ```
4. Les traces `Received` montrent le passage du message par plusieurs serveurs internes de l'Éducation nationale puis par le serveur public `messagerie.education.gouv.fr [193.54.151.84]` avant sa réception par Google.
5. Google a enregistré les résultats :

   ```
   SPF   = pass
   DKIM  = pass
   DMARC = pass
   ```

   pour le domaine institutionnel `ac-normandie.fr`.
6. Le corps MIME contient la pièce jointe :

   ```
   certificat-scolarite [ l'enfant en danger ].pdf
   Content-Transfer-Encoding: base64
   ```
7. L'empreinte de corps DKIM `bh=` présente dans la signature est identique à l'empreinte que je recalcule sur le corps MIME brut selon la canonisation `relaxed` annoncée dans la signature.
8. Le PDF extrait directement du Base64 de l'EML possède une taille de **38 492 octets** et l'empreinte SHA-512 :

   `4391b8f32ab7fc07be1b1ba926f8b2f54834685904e4ed1c3a9e68f3f2b9f44a6eaf8a5d8e7931791dda67efb0c2`
9. Le PDF extrait de l'EML et le PDF analysé sont **identiques octet par octet**.
10. Le fichier analysé est donc exactement la pièce jointe du courriel institutionnel authentifié reçu le 7 septembre 2026.
11. Le message est signé nominativement par **Florian CONSUL, Directeur de l'école de Saint Germain sur Ay**. Compte tenu de la taille réduite de l'établissement, du contexte concret de mes échanges et de la concordance de l'ensemble des éléments techniques et contextuels, **je considère certain que le courriel et le PDF joint ont été envoyés par Florian CONSUL**.
12. Le texte de l'adresse est toujours présent dans le contenu interne du PDF et peut être extrait directement avec `pdftotext`.
13. Le flux de contenu de la page contient explicitement :

```
Domiciliée : 22 RUE ERMICE
50430 SAINT-GERMAIN-SUR-AY
```

14. Une annotation PDF de type `Ink` a été ajoutée à la page.
15. Cette annotation est blanche, entièrement opaque et possède un trait de 18 points :

```
/C[ 1 1 1]
/CA 1
/W 18
```

16. Le rectangle occupé par cette annotation recouvre les coordonnées correspondant aux deux lignes de l'adresse.
17. L'apparence graphique de l'annotation confirme l'utilisation d'un trait blanc de 18 points :

```
1.000 1.000 1.000 RG
18.00 w
```

18. Le PDF contient une révision incrémentale postérieure à sa première fin de fichier et cette révision contient les objets correspondant aux annotations.
19. Les métadonnées internes associent l'annotation au **7 septembre 2026 à 11:06:42 +02:00** et la modification générale du document au **7 septembre 2026 à 11:06:44 +02:00**.
20. Le même fichier, avec cette annotation déjà intégrée, est ensuite transmis dans le courriel institutionnel pris en charge à **13:46:23 +02:00** et authentifié par DKIM à **13:46:29 +02:00**.

---

13. Conclusion factuelle

Avant même l'analyse interne du PDF, je constate que le fichier examiné est **strictement identique, octet par octet, à la pièce jointe Base64 du courriel institutionnel reçu le 7 septembre 2026**. Ce courriel a été reçu avec les résultats `SPF=pass`, `DKIM=pass` et `DMARC=pass` pour `ac-normandie.fr`, et son corps authentifié annonce l'envoi du certificat tout en étant signé « Florian CONSUL, Directeur de l'école de Saint Germain sur Ay ».

Compte tenu de cette chaîne technique, du contenu nominatif du message, de la taille réduite de l'école et du contexte concret de mes échanges avec son directeur, **je considère certain que ce courriel et le PDF joint ont été envoyés par Florian CONSUL**. Je ne fonde pas cette attribution sur un élément isolé, mais sur la concordance de l'ensemble des éléments techniques et contextuels disponibles.

Au regard de la structure numérique du fichier, **je constate que l'adresse n'a pas été supprimée du contenu du certificat de scolarité**.

Le texte :

```
Domiciliée : 22 RUE ERMICE
50430 SAINT-GERMAIN-SUR-AY
```

reste présent dans le flux de contenu de la page et demeure extractible.

Je constate parallèlement la présence d'une **annotation graphique blanche, opaque et particulièrement épaisse**, ajoutée dans une révision du PDF et positionnée sur la même zone que l'adresse.

Techniquement, le résultat visible correspond donc à un masquage graphique de l'adresse par superposition d'une annotation blanche, et non à la suppression du texte d'origine dans le PDF.

Je ne déduis pas du seul fichier l'identité de la personne ayant réalisé cette annotation. En revanche, les éléments internes du PDF permettent de constater objectivement la coexistence du texte d'origine et de l'élément graphique qui le recouvre.

---

14. Conservation de la preuve numérique

Pour préserver la valeur technique de ce constat, je conserve le fichier original **sans le réenregistrer ni le modifier**, sous son nom d'origine, avec son empreinte SHA-512.

Il est recommandé de conserver ensemble :

```
Re_ Réponse à votre e-mail du 04_09_2026 - 'EEPU--ST-GERMAIN-SUR-AY .' (ce.0501780n@ac-normandie.
certificat-scolarite [ l'enfant en danger ].pdf
constat-technique-masquage-adresse-certificat-scolarite-[ l'enfant en danger ]-....md
```

ainsi qu'un fichier d'empreinte, par exemple :

```
sha512sum "certificat-scolarite [ l'enfant en danger ].pdf" > certificat-scolarite-[ l'enfant en
```

Toute copie destinée à une analyse complémentaire devrait être réalisée à partir du fichier original, sans modification de celui-ci.

Je conserve également le fichier EML d'origine et son empreinte SHA-512 :

```
e5c8dd4392f17d9ec1a9a5973bf3311a98624d25012dace6700b2e33bc3b418b728caa15ef182fc3b16c5df5dae2831b3
```

La conservation conjointe du `.eml` et du PDF permet de conserver la relation probatoire entre le message authentifié et la pièce jointe analysée.