CERTIFICATS : IDENTITY ATTRIBUTES : LES ATTRIBUTS ET LEURS RÔLES

PRÉFACE

Les **Identity Attributes** sont des éléments permettant l'identification de certaines informations comme la chaîne de certification, le nom des machines, leurs types et parfois même leurs numéros de série.

LA NOMENCLATURE DCI

Chaque certificat a des champs **Issuer** et **Subject** formatés avec une certaine nomenclature.

```
# openssl x509 -in certificate.pem -text | grep "Issuer:\|Subject:"

Issuer: O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DC.DMS.DC2.SMPTE, dnQualifier = "+LLvuYNO4YBJSp9Jjmlv8o
Subject: O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = CS.DMSJP2K-80119.DC.DC2.SMPTE, dnQualifier = SQFYSSqWwj
```

Si nous prenons quelques certificats publics provenant d'autres appareils DCI, vous trouverez une certaine récurrence :

```
# KODAK
CN = MDI MDA MDS FMI FMA SPB LE SM.Kodak.KSM3000.000.04146, OU = KodakDevice, O = DC.CA.Kodak.Com, dnQualifier = RDowxMeC7Ws5
CN = SM.Kodak.KSM3000.000.04153, OU = KodakDevice, O = DC.CA.Kodak.Com, dnQualifier = "51pl1/pMAelK4y4xLfo+fmtLbgw="

# Sony
CN = SM.Sony.SSP-27-K.452ZK9B3-0027, OU = PRO, O = DC.CA.Sony.Com, dnQualifier = "nf8+WpTqshbU0Kli7HBv6EJ7ing="
CN = SM.Sony.XCT-M10.2400590, OU = PRO, O = DC.CA.Sony.Com, dnQualifier = Zk3vtTcrDeiozAlBl/VuKiSN6u4=

# Clipster
CN = SPB MDA MDI SM.ClipsterDCI.28100291, O = .DC.CA.DVS, OU = .Software.DvsAG.DC.CA.DVS, dnQualifier = aGt3jThUDviP1GFdWrj22

# CineCert
O = .ca.cinecert.com, OU = .ca.cinecert.com, CN = .s430-2, dnQualifier = 8O8W8oYHlf97Y8n0kdAgMU7/jUU=
O = .ca.cinecert.com, OU = .cc-ra-1a.s430-2.ca.cinecert.com, CN = SM.default, dnQualifier = s4afO4dGcdPFz3mSoE7fNSOMnc8=

# Doremi
O = CA.DOREMILABS.COM, OU = DOREMILABS.INC, CN = LE SPB MD SM.DCP2000-200022.DC.DOLPHIN.CA.DOREMILABS.COM, dnQualifier = "2rM
O = CA.DOREMILABS.COM, OU = DOREMILABS.INC, CN = .DC.ORCA.CA.DOREMILABS.COM, dnQualifier = rlpve6MSncWouNIpFcTSIhk6w2A=
O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = CS.DMSJP2K-80119.DC.DC2.SMPTE, dnQualifier = SQFYSSqWwjefppqasMJmf
O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = LD.IMBLD-197169.DC.DOLPHIN.DC2.SMPTE, dnQualifier = 0LDWrkGpgLkjg4
O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = LE SPB MD FM SM.Clarus-002023.DC.DOLPHIN.DC2.SMPTE, dnQualifier =

# CST
O = CA.CST.FR, OU = CST FRANCE, CN = SM.KMS.CST.FR, dnQualifier = zGFTluRuudYVrzFH1cB9VRb2yVU=

# OpenCube
O = DC.OPENCUBETECH.COM, OU = CS.DC.OPENCUBETECH.COM, CN = CS.DC.OPENCUBETECH.COM, dnQualifier = "xLDr7zpeNB/i5+NBpvVJ+LDfO4w

# Deluxe
O = bydeluxe.com, OU = dc, CN = CS.dlx-1.leaf, dnQualifier = "YxqCYce87+wo3F0/B1JUnolgoq8="
O = ca.christiedigital.com, OU = Christie Digital Systems, CN = SM.Christie.IMB-S2.0000001C0D1C, dnQualifier = OIapC/dNdnGpmR

# ROPA Media
O = SE.CA.ropaMedia, OU = ropa Media GmbH, CN = MD SM SPB TMS.CS-09-007-0301, dnQualifier = 8Fcg4MMYKhZq/OdpGVMiDP/gaZs=

# Dolby
OU = DOLBY.DCINEMA, O = DC256.Cinea.Com, CN = LS.Dolby-IMS3000_CID1002_SIGN-375148, dnQualifier = EmHtaAYYb5inb5QdJDR/JdGg43M
OU = DOLBY.DCINEMA, O = DC256.Cinea.Com, CN = SMS.Dolby-IMS3000_CID1002_SMS-375148, dnQualifier = "2PpT+O+Jby1bPUI/WsaCkjPeNz
OU = DOLBY.DCINEMA, O = DC256.Cinea.Com, CN = SPB MD FM SM.Dolby-IMS3000_CID1002_MPEG-375148, dnQualifier = "2PpT+O+Jby1bPUI/
OU = DolbyMediaBlock, O = DC256.Cinea.Com, CN = SM.Dolby256-CAT862-0007a158, dnQualifier = nLa5ihsEpY/AjcucGXdRUbCrw2U=
OU = DolbyShowPlayer, O = DC.Cinea.Com, CN = SM.Dolby-DSP100-0000029f, dnQualifier = "eycIbOhtIOvTKdw4j0SmGEAqe+4="
OU = DolbyShowPlayer, O = DC256.Cinea.Com, CN = SM.Dolby256-DSP100-000001ca, dnQualifier = IUHR8vIQeA4P3N7tl4EVLuffgQU=

# XDC
dnQualifier = "+G2JkUl/9A9GatSqmrsT0uJQ0o4=", O = xdcinema.com, OU = csc.xdcinema.com, CN = SPB SM MDI MDA FMI FMA LE.XDC.SOL
dnQualifier = "+JEIQ85V3nJgpfNVJmGbR9Vwojs=", OU = CA.GDC-TECH.COM, O = CA.GDC-TECH.COM, CN = LE MD FM SM SPB.A09013.SA2100.S
dnQualifier = "+Om8oDCqXZRRNbS/T2R51c0cpeg=", OU = CA.GDC-TECH.COM, O = CA.GDC-TECH.COM, CN = SMS.A32767.CONTROL.SERVERS.PROD

# Qube
dnQualifier = H3pcY1qFQCC/247pkJqRkLFOuKA=, O = CA256.QUBE.IN, OU = CA256.QUBE.IN, CN = SM SPB MDI MDA LE.QCPD-01743-07-11.XP
dnQualifier = fBfXMgDPI04a5WJUKXaCalLaM1U=, O = CA256.QUBE.IN, OU = CA256.QUBE.IN, CN = SM SPB MDI MDA LE.AUWEDIGITAL-MASTER1
```

Vous retrouverez une liste avec quelques exemples ici

Comme nous le constatons, nous n'aurons qu'une suite de **O**, **OU**, **CN** et **dnQualifier**, peu importe l'ordre. Ces attributs respectent la norme définie dans la RFC 2253 - String Representation of Distinguished Names [1]

Pour la simplicité, les normes SMPTE utilisent le nommage existant x509v3 sous un autre nommage orienté D-Cinéma :

Code x509	Nommage x509	Nommage D-Cinéma
`O`	OrganizationName	**Root Name**
`OU`	OrganizationUnitName	**Organization Name**
`CN`	CommonName	**Entity Name**
`dnQualifier`	dnQualifier	**Public Key Thumbprint**

Voyons maintenant chaque attribut pour comprendre leurs rôles.

ROOT NAME - ORGANIZATIONNAME - O

C'est le nom de l'organisation qui détient et gère la racine de la chaine de certificats.

Quelques exemples :

```
O = CA.CST.FR                    - CST
O = .DCINEMA.FRAUNHOFER.DE       - Franhofer
O = CA.DOREMILABS.COM            - Doremi
O = CA.GDC-TECH.COM              - GDC
O = CA.QUBE.IN                   - Qube
O = DC.CA.Kodak.Com              - Kodak
O = DC.CA.Sony.Com               - Sony
O = DC.Cinea.Com                 - Cinea
O = bydeluxe.com                 - Deluxe
O = ca.christiedigital.com       - Christie
O = xdcinema.com                 - XDC
```

L'OrganizationName (O) utilisé dans le champ **Subject** doit correspondre à celui utilisé dans le champ **Issuer**. Cela sous-entend également que l'OrganizationName doit être le même sur toute la chaîne de certificats.

Constatons ceci avec la chaîne de certificat pour un certificat d'un Doremi :

```
Subject (leaf)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = CS.DMSJP2K-80119.DC.DC2.SMPTE, dnQualif
Issuer  (leaf)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DC.DMS.DC2.SMPTE, dnQualifier = "+LLvu
Subject (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DC.DMS.DC2.SMPTE, dnQualifier = "+LLvu
Issuer  (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DMS.DC2.SMPTE, dnQualifier = RQ/53RmuL
Subject (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DMS.DC2.SMPTE, dnQualifier = RQ/53RmuL
Issuer  (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .PRODUCTS.DC2.SMPTE, dnQualifier = pkCB
Subject (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .PRODUCTS.DC2.SMPTE, dnQualifier = pkCB
Issuer  (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .ROOT.DC2.SMPTE, dnQualifier = a/wUIHLu
Subject (root)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .ROOT.DC2.SMPTE, dnQualifier = a/wUIHLu
Issuer  (root)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .ROOT.DC2.SMPTE, dnQualifier = a/wUIHLu
```

ou avec une chaîne CineCert (Issuer seulement) :

```
Subject (leaf)         : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = CS.K-DCINEMA, dnQualifier = "Nc+RplQGOuiylg6
Issuer (leaf)          : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-wm-2337-001013, dnQualifier = VxtZZD2q0H
Subject (intermediate) : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-wm-2337-001013, dnQualifier = VxtZZD2q0H
Issuer  (intermediate) : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-ra-5c, dnQualifier = k9Dgt7rESDa6ArkMYkx
Subject (intermediate) : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-ra-5c, dnQualifier = k9Dgt7rESDa6ArkMYkx
Issuer  (intermediate) : O = .ca-2.cinecert.com, OU = .ca-2.cinecert.com, CN = .s430-2, dnQualifier = "ri+G4dXNEhTc9BT4546O
Subject (root)         : O = .ca-2.cinecert.com, OU = .ca-2.cinecert.com, CN = .s430-2, dnQualifier = "ri+G4dXNEhTc9BT4546O
Issuer  (root)         : O = .ca-2.cinecert.com, OU = .ca-2.cinecert.com, CN = .s430-2, dnQualifier = "ri+G4dXNEhTc9BT4546O
```

ORGANIZATION NAME - ORGANIZATIONUNITNAME - OU

C'est le nom de l'organisation qui a généré le certificat. En général, c'est le nom du fabricant de l'appareil (mais pas forcément).

Quelques exemples :

```
OU = CST FRANCE                  - CST
OU = .DCINEMA.FRAUNHOFER.DE      - Fraunhofer
OU = DC.DOREMILABS.COM           - Doremi
OU = DOREMILABS.INC              - Doremi
OU = DOLBY.DCINEMA               - Dolby
OU = PRO                         - Sony
OU = Christie Digital Systems    - Christie
OU = CA.GDC-TECH.COM             - GDC
OU = Cinea CEKM                  - Cinea
OU = DolbyMediaBlock             - Cinea & Dolby
OU = DolbyShowPlayer             - Cinea & Dolby
OU = csc.xdcinema.com            - XDC
```

Constatons de nouveau avec la chaîne de certificat du même Doremi :

```
Subject (leaf)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = CS.DMSJP2K-80119.DC.DC2.SMPTE, dnQualif
Issuer  (leaf)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DC.DMS.DC2.SMPTE, dnQualifier = "+LLvu
Subject (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DC.DMS.DC2.SMPTE, dnQualifier = "+LLvu
Issuer  (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DMS.DC2.SMPTE, dnQualifier = RQ/53RmuL
Subject (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DMS.DC2.SMPTE, dnQualifier = RQ/53RmuL
Issuer  (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .PRODUCTS.DC2.SMPTE, dnQualifier = pkCB
Subject (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .PRODUCTS.DC2.SMPTE, dnQualifier = pkCB
Issuer  (intermediate) : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .ROOT.DC2.SMPTE, dnQualifier = a/wUIHLu
Subject (root)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .ROOT.DC2.SMPTE, dnQualifier = a/wUIHLu
Issuer  (root)         : O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .ROOT.DC2.SMPTE, dnQualifier = a/wUIHLu
```

ou avec le même CineCert (Issuer seulement) :

```
Subject (leaf)         : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = CS.K-DCINEMA, dnQualifier = "Nc+RplQGOuiylg6
Issuer  (leaf)         : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-wm-2337-001013, dnQualifier = VxtZZD2q0H
Subject (intermediate) : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-wm-2337-001013, dnQualifier = VxtZZD2q0H
Issuer  (intermediate) : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-ra-5c, dnQualifier = k9Dgt7rESDa6ArkMYkx
Subject (intermediate) : O = .ca-2.cinecert.com, OU = CineCert RA,        CN = .cc-ra-5c, dnQualifier = k9Dgt7rESDa6ArkMYkx
Issuer  (intermediate) : O = .ca-2.cinecert.com, OU = .ca-2.cinecert.com, CN = .s430-2, dnQualifier = "ri+G4dXNEhTc9BT45460
Subject (root)         : O = .ca-2.cinecert.com, OU = .ca-2.cinecert.com, CN = .s430-2, dnQualifier = "ri+G4dXNEhTc9BT45460
Issuer  (root)         : O = .ca-2.cinecert.com, OU = .ca-2.cinecert.com, CN = .s430-2, dnQualifier = "ri+G4dXNEhTc9BT45460
```

On constate que nous n'avons aucune obligation d'être sur la même OrganizationUnitName dans la chaine de certificat, en dehors du lien Issuer et Subject du parent.

Enfin, la norme indique clairement que les règles de sécurité et de validation ne doivent être affectées, ce champ doit être ignoré par les règles de validation et de certifications : autrement dit, vous pouvez (presque) mettre ce que vous voulez :-D

> La norme est très ambigüe à ce niveau, elle indique que des règles de sécurité et de validation ne doivent être assurées sur cet attribut mais en même temps elle impose certaines règles comme le lien Subject/Issuer de cet attribut.

ENTITY NAME - COMMONNAME - CN

C'est le nom de l'entité - récepteur/player/encodeur (comme le fabricant, le modèle et le numéro de série), ou même de l'entité du certificat intermédiaire.

Elle permet également d'exprimer les rôles autorisés et une brève description de l'appareil :

```
CN = LE SPB MD FM SM.DCP2000-218697.DC.DOLPHIN.DC2.SMPTE          - Player Doremi
CN = SM.Sony.XCT-M10.2400590                                      - Player Sony
CN = SM.Kodak.KSM3000.000.04153                                   - Player Kodak
CN = SM SPB MDI MDA MDS FMI FMA.Dolby-CAT745-00000245             - Player Dolby
CN = ME CS SM.DMSJP2K-80032.DC.DC2.SMPTE                          - Encodeur Doremi
CN = .signer_dcine_christie                                       - Encodeur Christie
CN = .DC.DMS.DC2.SMPTE                                            - Certificat Intermediaire
```

Elle respecte une nomenclature permettant d'obtenir des informations sur le récepteur : le **CommonName** (CN) identifie rapidement l'identité et le rôle d'un device via des petits codes.

Sa nomenclature devrait respecter une certaine codification. "Devrait" car quelques constructeurs respectent et d'autres ne le font pas du tout. Ceci dit, la norme ne l'impose pas, elle indique même que si un code n'est pas reconnu, il peut être ignoré par les différents devices traitant le KDM.

Un **CommonName** est séparé en deux par un point :

- **Rôles** : Première partie indique le rôle via des codes séparés par des espaces limités de 52 caractères. Si aucun rôle n'est défini, on commence directement par un point et la seconde partie. Obligatoire pour des certificats pour des appareils comme des players.
- **Label** : La seconde partie est un simple label pour cette entité.

Voici quatre exemples pour comprendre la séparation entre la partie **Rôles** et la partie **Label**

CommonName (CN)	Rôles	Label
LE SPB MD FM SM.IMB-239697.DC.DOLPHIN.DC2.SMPTE	LE SPB MD FM SM	IMB-239697.DC.DOLPHIN.DC2.SMPTE
SPB MDA MDI SM.ClipsterDCI.21070082	SPB MDA MDI SM	ClipsterDCI.21070082
.Secure Server.Production.DC.CA.Kodak.Com.v4-8	(aucun rôle particulier)	Secure Server.Production.DC.CA.Kodak.Com.v4-8
.EASYDCP-PLAYER.DCINEMA.FRAUNHOFER.DE	(aucun rôle particulier)	EASYDCP-PLAYER.DCINEMA.FRAUNHOFER.DE

Voyons maintenant les codes des Rôles.

RÔLES

Quelques règles à propos des rôles :

- Les rôles ne sont utiles que pour les certificats qui ne font pas partie de l'autorité de certification (vous pouvez l'identifier en analysant le champ BasicConstraint ayant un `CA=True`) [2]
- Les rôles ne seront utiles que pour les certificates leaf (players, encodeurs, ...).
- Les rôles peuvent être ignorés par les mesures de sécurité.

Voici un listing et un descriptif de certains codes de rôles :

Code	Description
TMS	Theater Management System (**TMS**) ou Screen Management System (**SMS**)
SM	Security Manager
SPB	Secure Processing Block fournissant une protection physique
MD	Media Decryptor - Tous canaux
MDI	Media Decryptor – Image/Picture
MDA	Media Decryptor – Audio/Sound
MDS	Media Decryptor - SubtitIte s
PR	Projecteur
LE	Link Encryptor - Picture
LD	Link Decryptor - Picture
FM	Forensic Marker - Tous canaux
FMI	Forensic Marker – Image/Picture (appareil pour le watermark ou le fingerprint)
FMA	Forensic Marker – Audio / Sound
CS	Content Signer (ou le créateur du contenu)

Etudions plus en détail maintenant deux cas en interprétant leurs codes de rôles :

```
CN = LE SPB MD FM SM.IMB-239697.DC.DOLPHIN.DC2.SMPTE
```

Ce **CommonName** nous indique que ce device possède ces caractéristiques suivantes :

- **Link Encryptor** (LE)
- **Secure Processing Block** (SPB)
- **Media Decryptor** (MD)
- **Forensic Marker** (FM)
- **Security Manager** (SM)

Son label est donc `IMB-239697.DC.DOLPHIN.DC2.SMPTE` .

IMB étant l'acronyme de **Integrated Media Block**, il nous indique que c'est un device intégré directement à l'intérieur du projecteur, c'est donc une carte de lecture DCI enfichée dans un projecteur d'une cabine de projection.

```
CN = CN=ME CS SM.DMSJP2K-80032.DC.DC2.SMPTE
```

Ce **CommonName** nous indique que ce device possède ces caractéristiques suivantes :

- **Content Signer** (CS)
- **Security Manager** (SM)
- **Media Encoder** (ME)

Le code **"Content Signer" (CS)** indique très clairement un device pouvant signer du contenu, des médias, des clefs, etc... : ce device est donc un **encodeur DCP**.

PUBLIC KEY THUMBPRINT - DNQUALIFIER

Élément très important car le dnQualifier n'est pas qu'un code aléatoire, il a été calculé.

Le **dnQualifier** est simplement l'encodage en Base64 de la **Public Key Thumbprint**, reportez-vous au chapitre Certificat - Public Key Thumbprint (dnQualifier) pour connaître la méthode de création de cette empreinte.

A ne pas confondre avec le Certificate Thumbprint qui sera utilisé pour d'autres éléments.

CONCLUSION

Ces identifiants de certificats sont l'une des parties importantes de la chaîne de certifications, elles serviront à chacune des étapes cryptographiques que ce soit dans les PKL, les CPL et bien évidemment les KDM (et même au-delà).

CHAPITRES ANNEXES

- Certificats - Les bases
- Certificats - Les champs (fields) d'un certificat x509 DCI
- Certificats - Identity Attributes - les attributs et leurs rôles ⬅ vous êtes ici
- Certificats - La chaîne de certification
- Certificats - Certificate Thumbprint - l'empreinte du certificat
- Certificats - Public Key Thumbprint (dnQualifier) - l'empreinte de la clef public
- Certificats - Création : Nos propres certificats
- RSA - La cryptographie asymétrique pour le chiffrement et les signatures.

NOTES

1. *« 5.3.1 Recipient - The X509SubjectName element shall contain the X.509 suject distinguished name found in the certificate. The X.509 distinguished name values in X509IssuerName and X509SubjectName elements shall be compliant with RFC2253 »* -- SMPTE 430 - KDM ↩
2. La norme SMPTE n'est pas très claire et se contredit d'une phrase à l'autre. En gros, les certificats d'autorité (CA certificates) ne doivent pas contenir de rôle. Mais juste après, ils précisent que c'est possible si ce rôle a été validé comme pouvant faire partie d'un certificat d'autorité : *« CA certificates do not contain any role information. An entity that is acting as a certificate issuing authority (a CA), as indicated in its BasicConstraint field, should only include a role in the CommonName if that role is permitted for CAs according to Table 4, which currently disallows such roles. -- SMPTE 430-2 Digital Certificates »*. Il faudra donc suivre les évolutions de la norme pour savoir si le tableau listing les codes intègre de nouveaux codes pour les certificats d'autorité. ↩