INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC 1/SC 29/WG 8
MPEG GENOMIC CODING

ISO/IEC JTC 1/SC 29/WG 8 M59991
Online – July 2022

Title: Proposal of corrections to ISO/IEC IS 23092-3 Edition 2

Authors: Silvia Llorente, Jaime Delgado, Ferran Mateu (DMAG/IMP-UPC)

1. Introduction

This document proposes two changes to solve some issues detected in document ISO/IEC 23092-3 Edition 2.

2. Changes proposed

In section 7.2.2.1.1.2 URI refmeta/id, line 3, the reference to subclause 6.5.1.4 should be changed to 6.5.2.4 to properly reference the ReferenceMetadata subclause in document ISO/IEC 23092-1.

In Annex D (informative) Example of key transport, the “testRSAPublic” rsa private key is not able to unwrap nor produce the output key specified in D.4 Asymmetric key wrap.

The problem with “testRSAPublic” key is that, if protection parameters defined in Annex D.4 are applied, it gives a “decryption error” as it is not able to decipher the wrapped key specified in D.4.

2.1. Alternate set of keys

To solve the identified issue, we propose an alternate set of keys (encoded in base64):

testRSAPublic

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEA8kGmB18UeHfVih6MfLjIXqPTqYnHCDXEpp/rn7QSxhULemUp
GivHJQf6Ilp8+pBQYAHcr3hwOoc5lz7ZAW4P1bmFIxznPQzKNM8P5EVYTvgXepi1
HzDdY4RxIf0MTAPo+XWdYtaCTIcwTKKMu93X64xh40+hFjoLaEfYWbjfXjf+2Si0
Bbt7zsGkUsBKb5XERAH2UYCzGmHDt4ANqx6bKNUBlm2gTKgxfnvfUZqcYAoboZHL
```

```
zhtOjTKi+ElZrC3X0paK7UG7qIwpSHHL3uX2tZpm7DQQSfvwx09RbWYr5XUn88eG
StMi43Wy3rf8/guoSUHxmm4c3Kb5Bw2tRcM9qYi9AzOTkTA945BltfgTdsDfpP3p
b6awhRvf0pKK9VBQ39L+n60s9PRwxI6Ig0rLZ+47WcbgC7Egd+oHgeohMs3ZZMFc
ao4LHQIPVSQaGVaeuBCo6V7IllUQaHoNY/2xio/xN7tI+cTIlC8fYQEZGeNmxZjt
uo8Nl7tZgKngx6u6ZjzZhLvTTFiLoOWD0Q7deP4qF0HmsJQd7INgQxSTQZ9erl0O
R2ROkhWo98/xSkAmQ6XYM0daYVMGrJJJ6y9k/HFib+ttKmKwrJoOmM6AhCQ8RoQQ
A2olLvLhmum6uKMzdXL6EozzJVrBXsUfDswn6qJUBPeLVROq3G8LHowTxF0CAwEA
AQKCAgAW3zrZLFFm9E1tbmfuKJYGVWpY8eCgNk9cOfIJkHtLR1Zflmh0h5iUNvYX
QzrUf0aPYe2fhXv3EqhNzsm3OFh3Yb4frA1q9qeqp7gE4cUuI383/G3xRXBJgooZ
3uXH0YCv+LpEyCLiLctSGPC3lgDaRNVDHFQFoLJOBKZ5BhrUru25O/4PIn3UbfTh
OTVt5pJyp0rFtCR0w7EyRH1F4CxfBQlS1gPR6PlPS0uwzSuhZ6LnNLgsu+hFLXg0
f9xfBK8BO2RfdRrOFXmaVOAeKdEKoUrBV0MIcShw8Nyruv8++Tot6nMT4m5DUmvy
WiWhKKGZVQgGAApqjLsrPs/Sq9XI2k8du+XJMMB1/95DnU1aNIv1M7jGo3un1Lac
BfPxWkPPr65Ao27P3kSiAS1uHZZLK5Jv0yAGgT1mtcRCbOZaWjGmrrQh59KNPmzp
jXH5fbtAiA9u2uNbJoSLJahrcRtlbTLzFXDEmOI756/DxIZ6eYqN5aMRmgM2EkJI
/yEDEMwjX1zv6Ah44xP+osmYopHUJ0Rzj4nTRMV5TcNZINsSelcfMJK3ClxQSxL6
ZcPMfmec7dG+WOSF0VxeAPpxRNfWEmdtHQy8umYe9UOz6BGpIgi8/K4zs2fkJ0Dl
KJBdpu8CsRADXy4XChVntbgvt/llEbKHTnH7zcFn7mvLll2fgwKCAQEA9EQiYN3U
Odl6/2jTDP+lRQcl liRVoBWswk063sxWAndh3nl5Sd2l+KD/o2DDBrPM2eAByoFq
/mGkdBEMjtwjHrSKmbQYmpalzCI91WTSH+8orcq6P0eIneOOxbyUogG9NKvRa/q4
wlqLeFsENgFUVw4TC63Xm1Gv/0N7ei/sdXlEZwBmwPzGV9l4wrdNAt/tuguwiKE5
JThQTexT2xYfaDywuWc8EPpqcNs3RxtXtgRcD7n6sTWvWGz0YmAMH5dwJ62urdbb
RiPBhmpxjka43Fx+zF5c2XW/rs1KSrp4A3gXjuvoBhWelVFZC5M+tBo73ZGpZaYX
NBkX97mobLLxKwKCAQEA/eTMwZneiSN7kGCD2/+A5FQM0DgF4wLjF4BQ+JzT9trB
hNBFfkmbcGHOpjVpth86hM5jPKZildQ9LzcDolvo6j8GsyLSv9KBY7hsVhzmvgJb
16BFk2Iau5ga4V5wQm9Mk6sq1u9XTbysbt+Gtq937icdFMqVBXMgFkQZm5fbx0LM
/5oimCARjeOBvWHbhlWEGr2dURjVDtZ22/SHTlU3AmCL76j2orCJOnZEu/cuNnhn
P3QgcHUOFOgQ9f4XxfeWVPBqQNdWSMO5RHnsojzDviAoJHUqyorrfA5XDnCtN7Yr
TvTjtSoEdRzepGNE5/OoJR1WoHe8XRaxi3U1PeyMlwKCAQEAjOqBqsBOntEIVDB1
ERqqjZgB5wwvGZtnfvBu9fmL5QBaRa5uel6UUUsQL4CzAjrYAxln7xuaTgamiQ8M
352/5QbirqlnSEeAfrOCWIlBb4rZPOmnaLor5mpRA2I3nP7D2I8G0fRigj0aGOTp
GP7LWS2VbzdrGv+VOP4FTgg3sc2z2Hgyz0MEacncEPkORIpK6vmzbh8UiJRkP5AH
EG1C0S+yBEO6M1FD9reAvFTZ1PfO5IO2TGVcMvcoRViDpfYHjdx02XUKKvyVuKXP
vPSv0PDLdbs6dXmoi3+DTHkmo1m0vY763Ae85Qd5B2R62AwKXVibETkwSa3wVcmV
kJ/q4QKCAQEAr1H6Tkn5UEuvPKBZDWae04xymKnG7t6EgCr8PuDUwaaHcTX8dttP
OchgUYeaqsdfumtmPXBLrVi0s1DS8p9y86Z38uU+EHXFIV4teT1V3Kl2UCx9PuvE
t/utvChhbo66m1HcMDVv3N9HVvyFYstCDrL1svC8/Nlls9pssHOpsSwgsPP3pYKn
fIo4gdT8KQQOSATdiC2Umj1gMDzn3iCb7slKeED9ppQu/q7CgeWLBNQZv8hpyh4a
jjc91xARzINOTPMC/Cl2jKKS4YUr8U/yfuxnq904okpRmAWy+ea2xjzGJSyXvPb5
wwEfgPaHk4A+gPqEYiSsbr+H9FwIWu1omwKCAQANQSNMBi/3wXSnZoo1Cl80741D
Z6cM+neS1g6lMX/8hPmdW80xinMSapN+/FYwvWncDpmPjlRP37iBJ8F21eu/f89F
D+By6EON1o014KaoiNIv4JJ5DDB5Iif2lsshg+d5Urh232UcyPsfP2YkUC9Yn7eR
5SKdesR+bCLqFn38bo4jJsShQbPE/LBht64WSNdOZNCjbYso//A/uZ5mYvOGRSVY
cAMAMTKKfggB9oIRu2U1z5NUR3eqVgeMNjj8QWtkb0E2N5DdUa6vaS1GcAcdODQs
CaufvyKSSLJFwzlCWeV6D51QkOY6IXOvzHG2GHhxS9uNaPFrDuvivmeBinql
-----END RSA PRIVATE KEY-----
```

Key

```
ICEiIyQlJicwMTIzNDU2Nw==
```

WrappedKey


```
PfzCxkMjJd8MjtT8OCupEKmf0cFExjj1xVKC+S7cBS6ZqoqLNF1AwqgbKYng3Id/QxVLp/ZxZP
7YJuNKJ1fR4lO4g8jCDPBpKl8nITt56wxwKpSGPed/f+umyLsEG20sFfjWhK6l0lY33tsKUmgW
SYioZzbvNkfuiRsSdhmSKc/6M2ezCO6fJDFXH7L7UW/67pQHy64WrwUISkHuDkWO9OYKWiAf+K
niIGWG2prXjF8gLEkedecBIfFfk4nt3SBOAXgcL62KhIxjo+buNqUi5N5w/bMWI1j7xHmGvyQo
lKRor+SrXhDwxn0DNlJ5F89KotcoevghG66jCiPdg4KzwlTGZOs0hHtzA+0y1ud462IA41JLzc
JHPLF1qvDbK0TnzL3GPj0FYF/RJXB98OAh9NMhqnjXwj6qsJsAzssva6i8B2kAX3/t4NLznAVS
yu7kRngPTZzrWqhyt1i2nV616GOb7+1xuV6ND/EZQsFp0jPw92F6Lzd7mas3QRy2ObbxbYKpGt
mo6vx07QZJxxxvx0N19i4jTwvT0rSvl5RSHobA4hZcHSNjOfm+AnRCeJhGO7Mjha97/EX6vKQO
LupYiACKma8cEUTCVgTZ6A+oEk9t+tzzHGAD6qCOJRRw65/yvsSf8u5mCBpi4EFOADQu3vg75f
mfKkmAiiPeOZrRNUM=
```


KeyTransport in Annex D.4, including the proposed wrappedKey


```
<?xml version="1.0" encoding="UTF-8" ?>
<KeyTransport xmlns="urn:mpeg:mpeg-g:protection:dataset-group:2019">
<keyName>wrapped2</keyName>
<KeyAsymmetricWrap>
<hashFunction>urn:mpeg:mpeg-g:protection:sha384</hashFunction>
<maskGenerationHashFunction>urn:mpeg:mpeg-
g:protection:sha1</maskGenerationHashFunction>
<publicKeyName>testRSAPublic</publicKeyName>
<wrappedKey>PfzCxkMjJd8MjtT8OCupEKmf0cFExjj1xVKC+S7cBS6ZqoqLNF1AwqgbKYng3I
d/QxVLp/ZxZP7YJuNKJ1fR4lO4g8jCDPBpKl8nITt56wxwKpSGPed/f+umyLsEG20sFfjWhK6l
0lY33tsKUmgWSYioZzbvNkfuiRsSdhmSKc/6M2ezCO6fJDFXH7L7UW/67pQHy64WrwUISkHuDk
WO9OYKWiAf+KniIGWG2prXjF8gLEkedecBIfFfk4nt3SBOAXgcL62KhIxjo+buNqUi5N5w/bMW
I1j7xHmGvyQolKRor+SrXhDwxn0DNlJ5F89KotcoevghG66jCiPdg4KzwlTGZOs0hHtzA+0y1u
d462IA41JLzcJHPLF1qvDbK0TnzL3GPj0FYF/RJXB98OAh9NMhqnjXwj6qsJsAzssva6i8B2kA
X3/t4NLznAVSyu7kRngPTZzrWqhyt1i2nV616GOb7+1xuV6ND/EZQsFp0jPw92F6Lzd7mas3QR
y2ObbxbYKpGtmo6vx07QZJxxxvx0N19i4jTwvT0rSvl5RSHobA4hZcHSNjOfm+AnRCeJhGO7Mj
ha97/EX6vKQOLupYiACKma8cEUTCVgTZ6A+oEk9t+tzzHGAD6qCOJRRw65/yvsSf8u5mCBpi4E
FOADQu3vg75fmfKkmAiiPeOZrRNUM=</wrappedKey>
</KeyAsymmetricWrap>
</KeyTransport>
```