



Content hand-over Use-cases

1 Contents

2	Use-cases for content hand-over	2
3	Terms	2
4	Format of use cases	2
5	Opening a URI by scheme	3
6	Geolocation handover	3
7	No immediate side-effect from plain URIs	3
8	Specifying an action	4
9	Requiring a variant-specific scheme handler	5
10	Disallowing certain scheme handlers	5
11	Interesting URI schemes	5
12	Opening a file by type	6
13	Activating a built-in content-type handler	6
14	Activating a third-party content-type handler	6
15	Choosing one of several content-type handlers	6
16	Requiring a certain content-type handler	7
17	Ensuring that the relevant file is accessible	7
18	Interesting media types	7
19	Registering new media types	8
20	Non-default actions on files	8
21	Possible future additions	9
22	Handling a subset of a scheme	9

23 Use-cases for content hand-over

24 This page collects the use-cases for “one-shot” content handover, as currently
25 mediated by the Didcot service.

26 Some related use-cases which have been associated with the Didcot content-
27 handover service during discussion of its API, but which we believe are suffi-
28 ciently distinct that they should be examined separately, are collected on [Con-
29 tent hand-over/Related](#)¹.

30 Where use-cases describe a requirement for a particular UI/UX behaviour, this
31 is intended to be shorthand for a requirement that the platform provides enough
32 control and enough information that the behaviour described is implementable.

33 Terms

34 A *content-type* (sometimes also called a MIME type or Internet media type) is
35 as defined in [RFC:2046](#)², for example `text/plain`. It is made up of a *top-level*
36 *media type* such as `text`, and a *subtype* such as `plain`.

¹https://sjoerd.pages.apertis.org/apertis-website/concepts/content_hand-over_related/

²<http://www.rfc-editor.org/rfc/rfc2046.txt>

37 A *URI scheme* is the part of a URI before the :, as defined in RFC:3986³. For
38 example, `http`, `tel`, `mailto` and `skype` are URI schemes.

39 An *xyz: URI* is a URI whose scheme is *xyz*.

40 In use-cases, *the platform* refers to the components in the platform layer that
41 provide the required functionality. We anticipate that the implementation for
42 most or all of the functionality required here will be Didcot, a *user service* (as
43 defined in the Multi-User concept document) which is trusted as part of the
44 security boundary between app-bundles, but not trusted as part of the security
45 boundary between users. However, the use cases have been written without this
46 assumption, and in particular, parts of the implementation that do not need
47 to cross a security boundary should be implemented as library code.

48 **Format of use cases**

49 Prerequisites and assumptions

- 50 • Requirement
- 51 • Requirement
- 52 – *Implementation notes*

53 **Opening a URI by scheme**

54 **Geolocation handover**

55 The user activates a geographic location in an application, for example a “show
56 on map” option in a list of hotels.

- 57 • The hotel application asks the platform to resolve a URI representing the
58 location, for example a `geo:` URI with latitude and longitude.
- 59 • The platform may launch an appropriate mapping or navigation applica-
60 tion and direct it to the appropriate point.
- 61 • The platform may instead offer a menu of applications or actions appli-
62 cable to a location. If so, it must be possible for third-party application
63 bundles to add their own actions to this menu.
- 64 – *Open question: do we need to support more than one action per*
65 *application?*

66 **No immediate side-effect from plain URIs**

67 The user activates a `mailto:` URI in a web page.

- 68 • The platform may start an email application in a “compose a message”
69 state, with the `TO` address, subject, body etc. already filled in according
70 to the URI.
- 71 • The email application must not send the resulting email until the user
72 chooses to do so. The user must have the opportunity to cancel.

³<http://www.rfc-editor.org/rfc/rfc3986.txt>

- 73 • The platform may instead choose to offer a menu of reasonable things
74 that can be done with an email address, such as composing a message or
75 providing the email address to a system address book, either as a starting
76 point for a new contact or to be attached to an existing contact.

77 The user activates a `tel:` URI in a web page.

- 78 • The platform should not start an audio call to the the number without
79 giving the user the opportunity to proceed or cancel.
80 • The platform may instead choose to offer a menu of reasonable things
81 that can be done with a telephone number, such as making an audio call,
82 composing a SMS or providing the email address to a system address book,
83 either as a starting point for a new contact or to be attached to an existing
84 contact.
85 • The platform may offer actions from more than one application, such as
86 making a conventional or Skype call.

87 The user activates a `geo:` URI in a web page. Suppose that, in this particular
88 Apertis system, `geo:` URIs are associated with the navigation application.

- 89 • The navigation application may offer a menu of things to do with that loca-
90 tion, such as zooming the map to that point or setting it as a navigation
91 destination or waypoint.
92 • The navigation application may take one of those actions immediately; but
93 if it does, it should offer a way to undo, to avoid malicious applications
94 being able to interfere with navigation, for instance by overwriting the
95 currently-set destination. ()

96 Specifying an action

97 The user activates a telephone number in an address book application. Suppose
98 the application's user interface presents phone numbers in the same way as
99 Android, where activating the number itself is expected to initiate a call, and a
100 keyboard icon alongside the number is expected to initiate a SMS conversation.

- 101 • On activating the number itself, the address book application communi-
102 cates to the platform that an audio call is the desired action.
103 – *One possible implementation would be to avoid Didcot altogether for*
104 *this use-case, and have the address book communicate directly with*
105 *Telepathy Mission Control or with the in-call UI to initiate the call.*
106 *We recommend this implementation.*
107 – *Another possible implementation would be to pass a (URI, action)*
108 *tuple to the platform, such as ("tel:+443457484950", "call").*
109 • Similar to **No immediate side-effect from plain URIs**, if an unprivileged
110 application attempted to do the same thing as the address book, it should
111 not be allowed to initiate the call without user confirmation, to avoid
112 untrusted applications imposing a financial cost on the user.
113 – *Using Telepathy would naturally provide this: only applications whose*

- 114 *AppArmor profiles allowed communication with Telepathy Mission*
 115 *Control would be able to initiate calls.*
- 116 – *Using a (URI, action) tuple would require that this access-control was*
 117 *implemented separately in the API provider, for example Didcot.*
 - 118 • *On activating the SMS icon, the address book application communicates*
 119 *to the platform that composing a SMS is the desired action.*
 - 120 – *As for calls, one possible implementation would be to avoid Didcot*
 121 *altogether for this use-case, and have the address book communicate*
 122 *directly with Telepathy Mission Control or with the SMS composition*
 123 *UI to initiate the SMS conversation.*
 - 124 – *Another possible implementation would be to use a different (URI,*
 125 *action) tuple here, such as ("tel:+443457484950", "sms").*
 - 126 – *A third possible implementation would be to interpret tel: URIs as*
 127 *unambiguously meaning “initiate a call”, and introduce parallel sms:*
 128 *URIs, as has been done in Apple’s iOS. However, this is contrary*
 129 *to the principle that URIs are noun phrases, not verb phrases⁴, and*
 130 *should probably be avoided or deprecated.*

131 *Are there any other use-cases for specifying a non-default action when handling*
 132 *a URI (link), other than telephony and instant messaging?*

133 **Requiring a variant-specific scheme handler**

134 The user activates a `geo:` URI ([RFC:5870](http://www.rfc-editor.org/rfc/rfc5870.txt)⁵) representing a geographic location.
 135 The designer of this particular Apertis variant has chosen to disallow any appli-
 136 cation other than the built-in navigation app from handling `geo:` URIs. ()

- 137 • The platform should launch the navigation app and carry out some default
 138 action, perhaps setting the navigation destination to the specified point,
 139 zooming the map to the specified point, or presenting a menu of applicable
 140 actions.
- 141 • The platform must not launch a third-party app, even if that app is also
 142 able to handle `geo:` URIs (for instance a Wikipedia app might handle `geo:`
 143 URIs by looking up nearby points of interest).

144 **Disallowing certain scheme handlers**

145 All URI scheme handlers in a manifest file should be examined for relevance
 146 to the app during the app-store approval process. Inappropriate URI-scheme
 147 handling should be disallowed.

148 Suppose a third-party application attempts to register itself as the handler for
 149 `file:` URIs, thus hijacking all file operations.

- 150 • This should not be possible. Either the platform or the app-store approval
 151 process should prevent it.

⁴<http://www.w3.org/DesignIssues/Architecture.html#Specific>

⁵<http://www.rfc-editor.org/rfc/rfc5870.txt>

152 Suppose a third-party application attempts to register itself as the handler for
153 `http:` and/or `https:` URIs.

- 154 • This should be allowed by the platform, but should be a “red flag” for
155 app-store curators: only general-purpose web browsers such as Firefox
156 and Chrome should be allowed to do this.

157 **Interesting URI schemes**

- 158 • [IANA registry](#)⁶
- 159 • `file:` is a special case and is described below ([Opening a file by type](#)). It
160 should never have a registered handler.
- 161 • `http:` and `https:` could be handled by general-purpose web browsers,
162 although we anticipate that OEMs would often want to restrict this.
- 163 • Particular namespaces within `http:` and `https:` could be handled by more
164 specific applications ([Handling a subset of a scheme](#)).
- 165 • Telephony and messaging: `tel:`, `skype:`, `sip:`, etc.
- 166 • Geolocation and navigation: `geo:`, `maps:`

167 **Opening a file by type**

168 We anticipate that in practice this mechanism will be used for all `file:` URIs,
169 and for no other schemes.

170 Suppose a USB drive contains some files, which are displayed as icons or list
171 entries in some built-in file manager or search application.

172 **Activating a built-in content-type handler**

173 Suppose the Apertis system has a built-in video player application. The user
174 activates a MPEG video, for instance by tapping on its icon.

- 175 • The file manager should communicate to the platform that this particular
176 file has been activated.
- 177 • The platform should discover that its content-type is `video/mpeg`, discover
178 that the video player app can play videos in that format, launch the video
179 player and instruct it to play the video.

180 **Activating a third-party content-type handler**

181 Suppose the Apertis system does not have anything built-in that can open
182 Word documents, but the user has installed a third-party LibreOffice app-bundle
183 which can. The user activates a Word document.

- 184 • The file manager should communicate to the platform that this particular
185 file has been activated.

⁶<https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml>

- 186 • The platform should discover that its content-type is `application/msword`,
187 launch LibreOffice and instruct it to open the document.

188 **Choosing one of several content-type handlers**

189 Suppose the Apertis system has a built-in image viewer supporting (among
190 others) JPEG images, and additionally, a third-party image viewer also supports
191 JPEG images. The user activates a JPEG image.

- 192 • The file manager should communicate to the platform that this particular
193 file has been activated.
- 194 • The platform should either:
- 195 – launch the built-in image viewer, or
 - 196 – launch the third-party image viewer, or
 - 197 – present the user with a menu from which they can choose one or the
198 other.
- 199 • The platform must provide enough configurability that if the user is
200 prompted with a menu, there can be a “remember this in future” option.
- 201 • It should be possible for the platform to provide a configuration option,
202 for instance in a Settings app, with which the user can select a preferred
203 handler for JPEG images.

204 **Requiring a certain content-type handler**

205 Suppose instead that this particular Apertis system is an OEM variant, which
206 has a built-in image viewer supporting JPEG and PNG images, and that the
207 OEM does not ever want third-party image viewers to be used for these formats
208 (). The user activates a JPEG image.

- 209 • The file manager should communicate to the platform that this particular
210 file has been activated.
- 211 • The platform should identify the image’s format, discover that the built-in
212 image viewer has been configured as preferred, and launch it.
- 213 • It must not launch a third-party viewer or offer a menu.

214 **Ensuring that the relevant file is accessible**

215 The user activates an attachment in an email application; suppose it is a PDF.
216 We assume that the email application must write the attachment into a file, if
217 it is not already represented as a separate file, and pass its `file:` URI to the
218 platform, so that a suitable application (e.g. a PDF viewer) can be launched.

- 219 • The file must be writeable by the initiating app-bundle (in this case email).
220 • The file must be made readable by the receiving app-bundle (in this case
221 the PDF viewer).
222 • The original file must not be writeable by the receiving app-bundle, but
223 if a new copy is made, that copy may be writeable by the receiving app-
224 bundle.

- 225 • The file is potentially confidential, so it must not be made readable to
- 226 unrelated app-bundles (so writing it to our equivalent of Android’s /sdcard
- 227 is not a valid solution).
- 228 • *Possible implementations:*
 - 229 – *One possible implementation would be for a privileged component to*
 - 230 *copy the file content into a directory accessible only by the receiving*
 - 231 *app-bundle, for instance using a btrfs “reflink” to avoid duplicating*
 - 232 *the content.*
 - 233 – *Another possible implementation would be to pass an open file descrip-*
 - 234 *tor across D-Bus from the initiator, through the platform component*
 - 235 *that chooses the recipient, to the recipient.*
 - 236 – *Writing into a directory that is common to all applications is probably*
 - 237 *not a viable implementation in Apertis, because we use AppArmor*
 - 238 *profiles to provide the security boundary between app-bundles, and*
 - 239 *Unix filesystem permissions can discriminate between uids but not*
 - 240 *between AppArmor profiles.*

241 Interesting media types

- 242 • [IANA registry](#)⁷
- 243 • `text/vcard`: contact information
- 244 • `audio/*, video/*`: media
- 245 • We can define a media type for Apertis packages
- 246 • `application/vnd.apple.mpegurl`: playlist or reference to a media stream
- 247 • *Does TPEG have one or more registered media types? If not, can we*
- 248 *register an `application/vnd.xyz` type for it with IANA?*

249 Registering new media types

250 The platform discovers files’ content types via a combination of file extensions
 251 and “magic numbers”. The current implementation of this is the [the freedesk-](#)
 252 [top.org Shared MIME Info specification](#)⁸.

- 253 • (Possible requirement) Apps should be able to register new content types
- 254 with extension and/or “magic number” matches in their app-bundle
- 255 manifest files. For example, a reader for a new document format “mydoc”
- 256 could associate `*.mydoc` files with the `application/vnd.example.mydoc`
- 257 content-type.
 - 258 – *Is this required?*
 - 259 – *This could be implemented by including freedesktop.org MIME regis-*
 - 260 *trations in the package’s content, or by taking input in a simplified*
 - 261 *format as part of the manifest, and generating corresponding files in*
 - 262 *`/var/lib/apertis_extensions/mime`, either prior to upload to the app*
 - 263 *store or during installation.*

⁷<https://www.iana.org/assignments/media-types/media-types.xhtml>

⁸<http://standards.freedesktop.org/shared-mime-info-spec/shared-mime-info-spec-latest.html>

- 264 – Declining to support this use-case would mean that files on disk are
265 never automatically detected as having a content type not described by
266 the platform, but custom media type handlers could potentially still be
267 used for files announced as having that media type by a Web server.
- 268 • If apps can do this, to avoid type handler hijacking, the app review process
269 should include inspecting the desired content types (if any). The app store
270 curator should normally reject anything that would override a standard
271 content-type defined by the platform, and should resolve conflicts between
272 store apps.
273 – This process could be made easier via tools.

274 **Non-default actions on files**

275 *Do we need actions other than the implied “open” for files, or does that only*
276 *make sense for URIs?*

277 **Possible future additions**

278 **Handling a subset of a scheme**

279 A preinstalled or third-party YouTube app-bundle has been installed. The user
280 activates a web link to a YouTube video, such as [https://www.youtube.com/
281 watch?v=dQw4w9WgXcQ](https://www.youtube.com/watch?v=dQw4w9WgXcQ).

- 282 • It should be possible for a YouTube application to “take over” this subset
283 of the `https:` URI namespace and play the desired video within that
284 application.
- 285 • It should be possible for the user to prevent this from happening, and view
286 the web page in an ordinary web browser.
- 287 • This should be a “red flag” for app-store curators: an app-bundle should
288 not be able to take over URIs within the www.youtube.com⁹ origin unless
289 it was published or approved by YouTube.

290 *Is this functionality required?*

291 *Is there any scheme other than `http(s)` where this would make sense?*

⁹<http://www.youtube.com>