

MHP Specification Version 1.1.2 Errata #1

1 Introduction

This document lists solutions for those errors in the MHP 1.1.2 specification (DVB Blue Book A068R1) which DVB has considered and where agreement has been reached on a solution. Changes are identified by their issue number from the DVB project MHP specification issues database which is accessible to members of the DVB project and contains the original problem report which motivated each change. These agreed solutions will be included in version 1.1.3 of the MHP specification unless new input results in a change to the agreed solution in the intervening period. The schedule for publishing version 1.1.3 of the MHP specification is not yet agreed. Where this document quotes text from the MHP specification, that text will have been copied from the PDF version of the MHP specification into the MHP specification issues database and then exported from that into this document. This process is known to some errors in quoted text, e.g. the “fi” character pair being lost from words like file or certificate. Where these are omitted in the quoted text, they may also be omitted in the agreed solution. This does not mean they are removed from the specification. There may also be errors introduced due to translation between differing character sets.

The document also records those requested changes which have so far been rejected and includes some explanation of the reason for the rejection.

2 MHP 1.0.3 errata 3

All changes in errata 3 to MHP 1.0.3 not already included in MHP 1.1.2 are included in this document.

3 Agreed Changes

3.1 Clause 2

3.1.1 Issue #4407

Reference 120 shall be updated as follows;

[120]	OCAP 1.0 OC-SP-OCAP1.0- I16- 050803	"OpenCable Application Platform Specification OCAP 1.0 Profile"
-------	-------------------------------------	---

3.1.2 Issue #4425

In reference 3, replace

<http://www.davic.org>

with

<http://portal.etsi.org/docbox/Reference/DAVIC/>

3.1.3 Issue #4436

Add the note below against the following references;

[33] Java Media Player Specification

[51] Java TV

[74] JMF const

NOTE: This reference is included in JSR-927 with the errata defined in the present document applied.

3.2 Clause 9

3.2.1 Issue #4351 DVB-appmodel.BroadcastApps-511

Remove the first paragraph of 9.1.9.1 and replace it with the following at the end of 9.1.9.1.

When running a cached application where multiple versions of that application are cached, the terminal shall only return files from the cache that were stored in response to an application description file signalled with the same organisation ID, application ID, and version number as the version of the application that is being run.

3.2.2 Issue #4352 DVB-appmodel.BroadcastApps-512

1) In 9.1.9.1, replace

“If the terminal does not have the signalled version of the application stored (when requested), the MHP terminal shall start the broadcast version.”

with

“If the application has not_launchable_from_broadcast set to '0' then the broadcast version shall be used regardless of the value of is_launchable_with_older_version.”

(Subsequent parts of the solution for this issue can be found under clause 10).

3.2.3 Issue #4353 DVB-appmodel.BroadcastApps-512

a) See entry under clause 10.

b) In 9.1.9.1 extend ;

“Terminals should allow different versions of an application to be cached/stored simultaneously. (For example, if two broadcasters use the same application, they may not upgrade to the latest version at the same time.)”

with

“Where multiple versions of an application are stored and one of them is to be started, the one started shall be the one whose version number is less than the version number of the transmitted application by the smallest amount.”

3.2.4 Issue #4354 DVB-appmodel.BroadcastApps-515

Move the following sentence from 9.1.9.1 to 9.1.9.2.

"Terminals are responsible for handling version updates to applications that were proactively cached."

3.2.5 Issue #4355 DVB-appmodel.BroadcastApps-516

In 9.1.9.1, change

Terminals should allow different versions of an application to be cached/stored

simultaneously.

To

Terminals shall allow different versions of an application to be cached/stored simultaneously.

i.e. change should to shall.

3.2.6 Issue #4379 DVB-security.storedapps-140

In 9.7.2, change the bullet point

Sufficient information to be able to construct the set of permissions to be granted to the application (this behaviour is equivalent to evaluating the permission request le at the time of launching the application).

To

Sufficient information to be able to construct the set of permissions to be granted to the application including the certificate files needed for any credentials

See issue#4381 for a check that credential certificates are not expired or revoked.

3.3 Clause 10

3.3.1 Issue #4349 DVB-appsig.ApplicationSignalling-905

In Section 10.14.2, the description of the "launchable_completely_from_cache" field has been inserted in the wrong position in the text. It should immediately precede the "is_launchable_with_older_version" field rather than preceding Table 111.

3.3.2 Issue #4352 DVB-appmodel.BroadcastApps-512

1) See entry under changes to clause 9.

2) In 10.14.2, add to launchable_completely_from_cache:

This flag shall only be set to "1" when not_launchable_from_broadcast is also set to "1".

NOTE: This flag should be set to 1 only for applications where the object carousel is not present at all.

3) Insert the following table at the end of 10.14.2.

<i>not_launchable_from_broadcast</i>	<i>launchable_completely_from_cache</i>	<i>is_launchable_with_older_version</i>	<i>Description</i>
0	0	0	Normal case. MHP 1.0 equivalent.
0	0	1	Shall not be signalled
0	1	0	Shall not be signalled
0	1	1	Shall not be signalled
1	0	0	Runs if signalled version is stored.
1	0	1	Runs if signalled or older version is stored.

<i>not_launchable_from_broadcast</i>	<i>launchable_completely_from_cache</i>	<i>is_launchable_with_older_version</i>	<i>Description</i>
1	1	0	Runs completely from cache if signalled version is stored. The application cannot be stored due to unavailability of DSM-CC for the current service.
1	1	1	Runs if signalled or older version is stored. The application cannot be stored due to unavailability of DSM-CC for the current service.
When set, flag indicates that files are present but bitrate is too low.	When set, flag indicates that files are not present in current broadcast at all.		

3.3.3 Issue #4353 DVB-appmodel.BroadcastApps-512

a) In 10.14.2 Application storage descriptor, in the definition of “is_launchable_with_older_version”, change;

When set to "1", the STB shall start the cached application, regardless of its version number.

To

When set to "1", the STB shall start the cached application where the version number of the cached application is lower than the version number of the broadcast application. If the version number of the cached application is higher than the version number of the broadcast application, the cached application shall not be started.

b) See entry under clause 9.

3.3.4 Issue #4374 DVB-appsig.ApplicationSignalling-970

In 10.14.3.4, change:

Must match the version number signalled in the AIT otherwise the application description file is invalid.

To

Must match the version number signalled in the version field of the application storage descriptor in the AIT entry of this application otherwise the application description file is invalid.

3.4 Clause 11

3.4.1 Issue 4295 Inconsistent specification of granting of IxcPermission

The contents of 11.10.1.12 “javax.microedition.xlet.ixc.IxcPermission” shall be replaced with the contents of 12.6.2.14.1 “Unsigned applications”.

The contents of 11.10.2.14 “javax.microedition.xlet.ixc.IxcPermission” shall be replaced with the contents of 12.6.2.14.2 “Signed applications”.

3.4.2 Issue #4361 DVB-DVBJPlatform.serviceinformation-210

In section 11.6.2, in the bulleted list introduced by “This API shall support the following features on those MHP terminals which support the feature concerned.”, split the last two items in the bulleted list into a bulleted list of their own. (i.e. “Services whose locator is” ... and “Service instances representing PSI-only services”. Prefix this list with the following;

“This API shall support the following features.”

3.4.3 Issue #4362 DVB-DVBJPlatform.serviceinformation-270

In section 11.6.2, the reference to ServiceManager.filterServices should be SIManager.filterServices

3.4.4 Issue #4363 DVB-DVBJPlatform.presentation-890

In 11.4.2.8.5, change

JMF implementations shall tolerate this behaviour when it happens.

to

MHP terminals shall continue to present video on a best effort basis within the constraints imposed by the new video configuration.

3.4.5 Issue #4364 Assertions for DVBJPlatform.permissions

In section 11.10.2.11, change StoredApplicationPermission to ApplicationStoragePermission.

3.5 Clause 12

3.5.1 Issue 4295 Inconsistent specification of granting of IxcPermission

Clause 12.6.2.14 “Inter-application communication policy” shall be reverted to the MHP 1.0.3 text with the following sentence;

"However, an unsigned application is not allowed to communicate with a signed application through the inter-application communication API."

changed to

"However, unsigned and signed applications shall only be able to communicate with each-other using the inter-application communication API in the "dvb:/ixc/" namespace."

3.5.2 Issue 4381 Assertions-for-security.storedapps

Replace section 12.15 with the following;

12.15 Stored and cached applications

At time of execution of an application, all files in stored applications must have been fully authenticated as defined by <xref>clause 12.4.4</xref>. The extent to which this authentication is performed at time of storage and time of execution differs as described below. In all cases, the certificates used must be valid at the time of execution - (e.g. they have not been expired or revoked, and the root certificates they use have not been removed). The normal constraints on authentication, including clause 11.2.3, shall be respected when executing an application. (This applies even if some class files are stored but others are not.)

This may lead to some stored class files failing authentication even if all certificates are still valid.

Files that fail authentication shall be treated in the same manner as files that fail authentication from a carousel. If a stored file fails authentication the implementation shall not fall back to loading that file from carousel.

12.15.1 Stand-alone stored applications

At time of application storage the stored files must be authenticated as if they were being loaded by the application. At this stage the terminal shall not treat class files specially.

In the case that a certificate that was validated during the store process has been revoked or has expired, any additional certificate chains that were not validated at storage time shall now be fully validated using the same rules as would apply to such a file from broadcast - i.e. clause 12.4.3.6.

If stand-alone stored applications access broadcast files (e.g. using the org.dvb.dsmcc API), the full requirements of [clause 12.4.4](#) shall apply to those files.

At time of execution, it shall be checked that any certificates used to authenticate credentials have neither expired nor been revoked.

12.15.2 Cached applications

It is implementation dependent how much authentication is performed at the time of storage.

NOTE: As an optimisation, implementations may calculate hash values of files at the time they are stored.

NOTE: Cached applications which will run without access to an object carousel for the stored files (e.g. not_launchable_from_broadcast set to '1') may be authenticated as described for stand-alone stored applications. The time at which the various steps of the authentication process are performed is not visible to applications.

3.6 Annex A

3.6.1 Issue #4407

The entire contents of clause A.11 shall be replaced with the following;

No errata against the referenced clauses of OCAP [120] have been identified.

3.7 Annex C

3.7.1 Issue #4436

Add the following informative reference;

Reference	Edition	Description
JSR-927	1.1	JavaTV 1.1

3.8 Annex N

3.8.1 Issue #4323 DVB-org.dvb.media.DVBMediaSelectControl-150

In DVBMediaSelectControl - select(Locator[], StreamType[]); add a @throws IllegalArgumentException if the two arrays are not the same size.

3.9 Annex S

3.9.1 Issue #4324 DVB-org.dvb.application.AppProxy-700

In `org.dvb.application.AppProxy.start(String[])`; the reference to "DvbJProxy" should be "DVBJProxy".

3.10 Annex U

3.10.1 Issue #4380 DVB-textpres.TextRendering-320

In the description of the method `DVBTextLayoutManager.render`, change;

“The `HTextLayoutManager` should not modify the clipping rectangle of the `Graphics` object.”

to

“The `HTextLayoutManager` shall not modify the clipping rectangle of the `Graphics` object.”

i.e. change should to shall.

3.10.2 Issue #4409

In the class description of `org.dvb.ui.DVBGraphics`, the middle 2 bullet points from the bulleted list (i.e. those listed below) shall be removed.

- Calling `setXORMode` on an instance of this class shall be equivalent to calling `setDVBComposite` with a special and implementation dependent `DVBAlphaComposite` object which implements the semantics specified for this method in the parent class.
- Calling `getDVBComposite` when `setXORMode` is the last `DVBComposite` set shall return this implementation dependent object. Conformant MHP applications shall not do anything with or to this object including calling any methods on it.

3.11 Annex Y

3.11.1 Issue #4422

In the method `public static void bind(javax.tv.xlet.XletContext xc, java.lang.String name, java.rmi.Remote obj)`, the following sentence

The object shall be made visible to other applications.

shall be replaced with

The object shall be made visible to other applications running in the same service context.

In the method `public static void rebind(javax.tv.xlet.XletContext xc, java.lang.String name, java.rmi.Remote obj)`, the following sentence;

The object shall be made visible to other applications.

shall be replaced with

The object shall be made visible to other applications running in the same service context.

3.11.2 Issue #4423

The following shall be added to the method *rebind(javax.tv.xlet.XletContext, String, Remote, int)*;

Narrowing the scope of the binding (e.g. from GLOBAL to SERVICE) shall have the same effect as a call to unbind for any applications which had references to that object and which were in scope but which are now out of scope.

3.12 Annex AG

3.12.1 Issue #4326 DVB- org.dvb.application.storage.StoredApplicationService-92

In Annex AG, org.dvb.application.storage.StoredApplicationService: change

"If there are any applications installed in the stored application service, then applications should be prepared for the platform consulting the end user of the MHP terminal for permission to remove the stored service. "

to

"If there are any applications installed in the stored application service, then the application calling this method should be prepared for the platform consulting the end user of the MHP terminal for permission to remove the stored service."

i.e. change "then applications" to "then the application calling this method"

3.12.2 Issue #4327 DVB- org.dvb.application.storage.StoredApplicationService-92

In org.dvb.application.storage.StoredApplicationService.removeService, add the following to the method description.

"If the end user is asked and does not give permission to remove the service, none of the applications in the service shall be removed."

3.12.3 Issue #4328 DVB- org.dvb.application.storage.StoredApplicationService-95

In org.dvb.application.storage.StoredApplicationService.removeService(), change the @throws clause for UserRejectedInstallApplication from "remove the application" to "remove the applications in the service."

3.12.4 Issue #4329 DVB- org.dvb.application.storage.StoredApplicationService-210

In org.dvb.application.storage.StoredApplicationService, in the description of the method remove(AppID[]), include the following description

" UserRejectedInstallException - If the user chose not to remove the application. "

3.12.5 Issue #4330 DVB- org.dvb.application.storage.StoredApplicationService-240

In 9.10.5, change

An AppsDatabaseEvent with event id APP_CHANGED shall be sent for that application.

To

An AppsDatabaseEvent with event id APP_ADDED shall be sent for that application.

3.12.6 Issue #4331 DVB- org.dvb.application.storage.ApplicationCache-80

In org.dvb.application.storage.ApplicationCache.remove(), change;

"initiates the removal of an application stored in the MHP terminal from this service"

to

"initiates the removal of an application stored in the MHP terminal from this cache"

i.e. this service to this cache

3.12.7 Issue #4332 DVB- org.dvb.application.storage.ApplicationCache-80

In org.dvb.application.storage.ApplicationCache.remove(..), in the @throws clause for SecurityException, add the following to the end of that clause

and an ApplicationStoragePermission with action "manageCache"

3.12.8 Issue #4333 DVB- org.dvb.application.storage.ApplicationCache-90

In org.dvb.application.storage.ApplicationCache.remove(..), in the following;

"If the application identified by the AppID passed in as a parameter is not installed in this service, the method shall fail silently."

change "this service" to "this cache"

3.12.9 Issue #4334 DVB- org.dvb.application.storage.ApplicationCache-130

In the class description of "ApplicationCache"

- a) Add the following to the end of the paragraph starting "Each instance of an ApplicationCache"
Successfully storing a different version of a cached application than the current one in an ApplicationCache shall result in the current one being removed from that ApplicationCache instance. If the call to store fails then the current version shall not be removed.
- b) Add the following to the end of the paragraph starting "A single MHP terminal"
The underlying application store shall manage the removal of versions of stored applications which are not used in any stored services or application caches.

3.12.10 Issue #4335 DVB- org.dvb.application.storage.ApplicationCache-200

In org.dvb.application.storage.ApplicationCache.store, change the @throws clause for InvalidDescriptionFileException to read

thrown if the application description file is missing, invalid or otherwise not conformant to the specification

3.12.11 Issue #4336 DVB-

org.dvb.application.storage.ApplicationCache-230

In org.dvb.application.storage.ApplicationCache.store;

- a) Replace the sentence before the bulleted list with
MHP terminals may prompt the user for permission to free up resources if and only if all of the following conditions hold:
- b) Replace the paragraph after the bulleted list with
Prompting the end-user for permission is not required however applications setting canPrompt to true should be prepared for the possibility of it happening. Note that if the user decides not to allow the terminal to free up resources, the NotEnoughResourcesException will be thrown (as if the terminal had not asked the user at all).

3.12.12 Issue #4357 DVB-security.storedapps-49

- 1) In StoredApplicationService.store (both signatures), change the @throws clause for ApplicationDownloadException to include "or if the application failed authentication while being downloaded"
- 2) In the class description of org.dvb.application.storage.ApplicationDownloadException, extend the e.g. list with "the application was being authenticated as part of downloading and this failed"

3.12.13 Issue #4372 Assertions-for-org.dvb.application.storage.InvalidApplicationException

In the description of org.dvb.application.storage.InvalidApplicationException, change;
Thrown if an application is not valid for installing into a particular service. There are two reasons why an application may not be valid for installing into a particular service:

- * The application does not include an application_storage_descriptor.
- * The application is not identified as able to run stand-alone in it's application_storage_descriptor.

to

When an application is being installed into a service, this is thrown when:

- * The application does not include an application_storage_descriptor.
- * The application is not identified as able to run stand-alone in it's application_storage_descriptor.

When an application is being stored in a cache this is thrown when:

- * The application does not include an application_storage_descriptor.
- * The application is not signalled as part of the same service as the calling application

3.13 Annex A1

3.13.1 Issue #4317 DVB-org.dvb.auth.callback.PasswordCallback-20

In org.dvb.auth.callback.PasswordCallback clearPassword; the word "retrieved" in the method description should be spelt "retrieve"

3.13.2 Issue #4318 DVB- org.dvb.auth.callback.PasswordCallback-30

1) Add the following o the class description of org.dvb.auth.PasswordCallback

The CallbackHandler uses this to communicate to the security services a password obtained from the end-user.

2) Add an @return clause to org.dvb.auth.PasswordCallback.getPassword as follows;

@return the last password previously set by setPassword or null if none has been set

3.13.3 Issue #4319 DVB- org.dvb.auth.callback.PasswordCallback-30

In org.dvb.auth.callback.PasswordCallback getPassword; the word "retrieved" in the method description should be spelt "retrieve"

3.13.4 Issue #4320 DVB- org.dvb.auth.callback.PasswordCallback-60

In org.dvb.auth.callback.PasswordCallback setPassword; the word "retrieved" in the method description should be spelt "retrieved"

3.13.5 Issue #4321 DVB- org.dvb.auth.callback.UnsupportedCallbackException-40

In org.dvb.auth.callback.UnsupportedCallbackException, add text to the getCallback() method saying that it returns the Callback passed in to the constructor.

3.13.6 Issue #4322 Assertions for org.dvb.auth.callback.CallbackHandler

Add the following to the org.dvb.auth.callback.CallbackHandler.handle method;

@exception IOException if an input or output error occurs when retrieving the password

@exception UnsupportedCallbackException if one of the callbacks in the array is not supported by the handler

3.13.7 Issue #4337 DVB-org.dvb.security.KeyStoreBuilder-20

Add the following to the method org.dvb.security.KeyStoreBuilder.newInstance;

@throws IllegalArgumentException if protection is an application defined class

@throws NullPointerException if type, provider or protection are null

3.13.8 Issue #4338 DVB-org.dvb.security.KeyStoreBuilder-20

Add the following to description of the type parameter in org.dvb.security.KeyStoreBuilder.newInstance

The type parameter is concatenated with the string "KeyStore." and then passed to the get

method of the specified Provider in order to obtain the fully qualified name of the KeyStoreSpi implementation.

For more details, see “How to Implement a Provider for the JavaTM Cryptography Architecture”

3.13.9 Issue #4339 DVB-org.dvb.security.KeyStoreBuilder-20

Add the following to description of the method `org.dvb.security.KeyStoreBuilder.newInstance`
`@throws NullPointerException` if any of the parameters are null

3.13.10 Issue #4340 DVB-org.dvb.security.KeyStoreBuilder-30

In the method `org.dvb.security.KeyStoreBuilder.getKeyStore`, make the following changes;

a) Add the following

`@throws NullPointerException` if any of the parameters are null

b) Add the following to the `@throws` clause for `KeyStoreException`

if an error occurred, e.g. if an error occurred in the constructor or the load method of the `KeyStore`

3.13.11 Issue #4341 DVB-org.dvb.security.KeyStoreBuilder-30

1) Add the following to the description of the method
`org.dvb.security.KeyStoreBuilder.newInstance`

Each call to the `getKeyStore()` method on the returned builder will return a new `org.dvb.security.DVBKeyStore` object of type `type`. Its `load()` method is invoked with the protection parameter used to construct this `KeyStoreBuilder`.

2) Add a new `org.dvb.security.DVBKeyStore` class which extends `java.security.KeyStore` with the following extra method;

```
/**
 * Loads this keystore using the given protection parameters
 * @param p protection parameters to use
 * @throws IllegalArgumentException if the parameter p is not recognized
 * @throws IOException if there is an I/O or format problem with the
 * keystore data
 * @throws NoSuchAlgorithmException if the algorithm used to check the
 * integrity of the keystore cannot be found
 * @throws CertificateException if any of the certificates in the keystore
 * could not be loaded
 */
```

```
public final void load(KeyStoreProtectionParameters p) throws IOException,
    NoSuchAlgorithmException, CertificateException
```

3.13.12 Issue #4343 DVB-org.dvb.security.pkcs11.DVBPkcs11Provider-70

Make the following changes in `org.dvb.security.pkcs11.DVBPkcs11Provider`;

a) Add the following to the class description

Providers have a slot identifier associated with them identifying each smart card reader slot. These are numbered starting from zero. For details, see the PKCS 11 specification.

b) Add the following to the method `getTokenInfo(int)`;

@throws `IllegalArgumentException` if the slot does not exist or there is no token in the slot

c) Add the following to the method `setSlotId(int)`

@throws `IllegalArgumentException` if the slot does not exist

3.13.13 Issue #4344 DVB- org.dvb.security.pkcs11.DVBPkcs11Provider-90

Add the following to the method `org.dvb.security.pkcs11.DVBPkcs11Provider.login`

@throws `NullPointerException` if the `CallbackHandler` parameter is null and either no previous call to `setCallbackHandler` has occurred or the last call to that method set the handler to null.

3.13.14 Issue #4345 DVB- org.dvb.security.pkcs11.DVBPkcs11Provider-90

In `org.dvb.security.pkcs11.DVBPkcs11Provider.login(Principal, CallbackHandler)`, in the description of the handler parameter the method "`setCallbackHandler`" should read "`setCallbackHandler`"

3.13.15 Issue #4346 DVB- org.dvb.security.pkcs11.DVBPkcs11Provider-160

In `org.dvb.security.pkcs11.DVBPkcs11Provider.setSlotId(slotId)`, in the description of the `java.io.IOException` the word "metho" should read "method".

3.13.16 Issue #4347 DVB- org.dvb.security.pkcs11.DVBPkcs11Provider-320

In the class description of `DVBPkcs11Provider`, change the second entry in the bulleted list from
In `javax.security (JCE)` for encryption and decryption.

To

In `javax.crypto (JCE)` for encryption and decryption.

3.13.17 Issue #4359 DVB-security.permfile-860

In 12.6.2.21.3, replace

"`providerPermission (providerName)*`"

with

"`providerPermission (providerName)+`"

3.13.18 Issue #4366 Assertions-for-org.dvb.net.ssl.DVBKeyManagerFactorySpi

In org.dvb.net.ssl.DVBKeyManagerFactorySpi, in the description of the engineInit method, change “KeyStore builders” to “KeyStoreBuilders”.

3.13.19 Issue #4367 Assertions-for-org.dvb.net.ssl.DVBTrustManagerFactorySpi

In org.dvb.net.ssl.DVBTrustManagerFactorySpi, in the description of the engineInit method, change the term “KeyStore builders” to “KeyStoreBuilders”.

3.13.20 Issue #4368 Assertions-for-org.dvb.net.ssl.DVBTrustManagerFactory

In org.dvb.net.ssl.DVBTrustManagerFactory, in the description of the init method, change the term “KeyStore builders” to “KeyStoreBuilders”

3.13.21 Issue #4369 DVB-org.dvb.net.ssl.DVBTrustManagerFactory-20

In DVBTrustManagerFactory.getInstance, add

This method shall return an instance of DVBTrustManagerFactory when provider is an instance of DVBPkcs11Provider.

3.13.22 Issue #4370 Assertions-for-org.dvb.net.ssl.DVBKeyManagerFactory

In org.dvb.net.ssl.DVBKeyManagerFactory, in the description of the init method, change the term “KeyStore builders” to “KeyStoreBuilders”

3.13.23 Issue #4371 DVB-org.dvb.net.ssl.DVBKeyManagerFactory-20

In DVBKeyManagerFactory.getInstance, add

This method shall return an instance of DVBKeyManagerFactory where provider is an instance of DVBPkcs11Provider.

3.14 Annex AK

3.14.1 Issue #4315

The method setDefaultVideoTransformation shall be renamed setDefaultVideoTransformation.

4 Rejected Changes

The following table shows the issues and proposed changes that have been rejected. DVB members can find detailed descriptions of these in the MHP specification issues database.

Issue Number	Issue Title	Reason for rejection
4325	Assertions for org.dvb.application.storage.StoredApplicationService	It's very unclear how to ask a typical end-user such a question in a way that they might understand. Hence consultation is absolutely optional and if any change was to be made, the change would be to remove the possibility of consultation.
4342	DVB-org.dvb.security.KeyStoreBuilder-30	Addressed by solution to 4341
4348	DVB-org.dvb.security.pkcs11.DVBPKCS11Provider-320	The possible set of Spis is listed in the introduction to annex AJ under "a) Implement the subclasses of the needed SPI classes". Which Spis are implemented is upto the provider.
4350	Assertions for objectcarousel.objectcarousel	Withdrawn by proposer.
4356	Assertions for security.storedapps	Addressed by solution to 4381.
4358	DVB-security.storedapps-50	Replaced by 4377 which is more detailed.
4365	Assertions for DVBJPlatform.security	In J2SE, a KeyManagerFactor can be initialised with a class implementing the ManagerFactoryParameters interface. The class KeyStoreBuilderParameters implements this interface and contains a list of KeyStoreBuilders.
4373	DVB-appsig.ApplicationSignalling-905	Duplicate of 4349
4375	DVB-appmodel.BroadcastApps-521	Addressed by solution to 4352 - the table showing which combinations of flags are valid to signal
4376	DVB-security.storedapps-30	Duplicate of 4357.
4377	DVB-security.storedapps-50	Proposal accepted but issue rejected since solution integrated in 4381.
4378	DVB-security.storedapps-50	Agreed in principle - included in solution for #4381.

5 Annex AJ

5.1 Introduction

MHP 1.1.2 annex AJ includes a warning that;

NOTE: This annex and in consequence the lifecycle and management of installed PKCS11 providers are not fully completed. They are liable to change in subsequent releases of the present document.

While there is not yet a complete solution for the issues with this annex, conclusions have been reached on the basic principles of how to address those issues. Those conclusions are described below. A number of details remain, "TBD".

5.2 Principles of Proposed Solution

Each MHP application using a provider has its own separate copy of that provider which runs in the context of that application. The organisations that transmit providers are responsible for ensuring at least one of the following;

- That the applications using the providers co-ordinate to ensure that only one application is using any provider at one time (unless the provider supports simultaneous access by multiple applications).
- That the provider detect when the smart card is busy (e.g. due to another instance of the provider) and re-try later if appropriate.
- That the provider use IXC to detect any other instances of itself running and to co-ordinate between such instances. In order to enable this, applications signalled as containing a provider will get IxcPermission ("dvb:/ixc/provider/provider_name", "bind") where provider_name is the signalled name of the provider.

Providers will be packaged in MHP applications. MHP applications which contain a provider will include in their AIT a (TBD) descriptor identifying the provider including a name and version number. The name must have the current syntax including the MHP org_id which must match the org_id of the certificate used to sign the application containing the Provider. Providers will be stored by storing the application containing them using the MHP 1.1 stored applications API. (TBD whether they are stand-alone stored applications or cached applications).

MHP applications using a provider will indicate this in a (TBD) AIT descriptor. When starting such an application, the implementation attempt to match the signalled provider(s) with the stored applications that contain providers. The process of matching will include comparing the version number of the provider with the version number to be used (TBD whether this is a simpler greater than or something more complex). (TBD should there be a provider type so that we can use the same signalling for other providers e.g. the MHP-IPTV ones?) If there is a match then the stored provider classes are available to the application. If there is no match then if an application signalled as containing a matching provider is stored while this application instance is running, that provider then immediately becomes available to the application. (TBD what about providers which aren't stored but are just signalled in the AIT? Are we assuming Providers are effectively "not launchable from broadcast"?)

The providers available to an application via this mechanism can be listed using the ProviderManager class (TBD update needed). Providers available via this mechanism shall not be registered as providers with the java.security.Security class. They can only be used in API calls where the provider to be used is specified using the Provider master class as an input parameter. They shall not be found by applications which specify providers by name or do not specify a provider at all. Applications may only obtain instances of the Provider master class via ProviderManager (TBD update needed). Attempts by applications to construct instances of DVBPkcs11Provider using the constructor shall fail with a SecurityException following the same model as org.dvb.DVBClassLoader. (TBD whether we specify which Permission controls this but if we do, it shall never be granted to MHP applications).

Providers may control which applications can use them by checking the `organisation_id` and `application_id` passed into the constructor of the provider master class. (TBD update needed). (Since the constructor of a provider can only be called by `ProviderManager`, this `organisation_id` and `application_id` can be relied upon as being accurate).

Providers are only removed when the stored application containing them is removed. If removal of such a stored application is requested while the provider is in use, the removal shall be reported as having succeeded but shall only take place when the provider is no longer in use. (This is the same as with normal stored applications).

5.3 Summary of Expected Specification Edits

- Replace APIs in current Annex AJ with a new much simpler `ProviderManager` class with perhaps two instance methods, `Provider[] listProviders()` and `Provider getProvider(String)`.
- Modify `DVBPKCS11Provider` to add `organisation_id` / `application_id` to the constructor and to require the constructor to throw `SecurityException` when called by any MHP application.
- Add definitions of the two new TBD AIT descriptors to the application signalling chapter
- Extend 11.10.2.14 “Inter-application communication policy” to grant `IxcPermission(“dvb:/ixc/provider/provider_name”, “bind”)` where `provider_name` is each signalled provider name.
- From 12.6.2.21 Cryptographic Service Provider Management, move the syntax of the provider name to where the two new AIT descriptors are defined and remove the rest.
- Replace the text part of the current Annex AJ with an expanded and completed version of the above text.