International Telecommunication Union

# ITU-T J.1020

(10/2017)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Conditional access and protection – Downloadable system for multi-CA/DRM service of mobile broadcasting

## Service model and architecture of downloadable mobile multi-CA/DRM solutions for delivering CA/DRM client software to secondary devices

Recommendation ITU-T J.1020

# Recommendation ITU-T J.1020

## Service model and architecture of downloadable mobile multi-CA/DRM solutions for delivering CA/DRM client software to secondary devices


### Summary

The purpose of Recommendation ITU-T J.1020 is to provide the reference service model, the architecture and the service operation protocols which are needed for multi-CA/DRM service based on a downloadable scheme. The downloadable scheme in this Recommendation means downloading CA/DRM client software images from the multichannel video programming distributor (MVPD) or broadcaster to a secondary device such as smart phone, tablet or laptop PC connected to a primary customer premises equipment (CPE) such as a set-top box. Service providers can change CA/DRM solutions for the secondary device from one to the other using on-line methods as well as operate multiple CA/DRM solutions at the same time.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T J.1020 | 2017-10-22 | 9 | 11.1002/1000/13286 |

### Keywords

Customer premises equipment, CPE, conditional access, digital rights management, DM, downloadable CA/DRM, downloadable mobile multi-CA/DRM, multi-CA/DRM, secondary device.


---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## Table of Contents

# Recommendation ITU-T J.1020

## Service model and architecture of downloadable mobile multi-CA/DRM solutions for delivering CA/DRM client software to secondary devices

### 1 Scope

The objective of this Recommendation is to specify a service model and architecture for downloadable mobile multi-CA/DRM (DM) solutions for delivering CA/DRM client software to a secondary device [ITU-T J.1010], [ITU-T J.1011] such as a smart phone, tablet or laptop PC connected to a primary CPE [ITU-T J.1011] such as a set-top box for cable television services. Note that the terminology of "secondary CPE" is used in [ITU-T J.1011] instead of "secondary device" with the same meaning. The use cases, requirements and architecture of a downloadable multi-CA/DRM service are specified through [ITU-T J.1010] and [ITU-T J.1011] under the name of "exchangeable CA/DRM solutions". The downloadable multi-CA/DRM service is part of a bigger family of services named the renewable CA system (RCAS), which are described in the Recommendations [b-ITU-T J.1001], [b-ITU-T J.1002], [b-ITU-T J.1003] and [b-ITU-T J.1004]. Note that the use case related to this Recommendation is described in Annex A of [ITU-T J.1010].

A reference service model and architecture will include entities such as MVPD, a third-party authorization centre and secondary devices which are necessary for providing downloadable service of CA/DRM client software. This Recommendation also specifies the service operation protocol among the entities that are part of the reference service model and architecture.

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T J.1010] Recommendation ITU-T J.1010 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements*.

[ITU-T J.1011] Recommendation ITU-T J.1011 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

**3.1.1 conditional access (CA)** [b-ITU-T J.193]: The conditional granting of access to cable services and content based upon what service suite has been purchased by the customer.

#### 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 DM_ISS**: One of the roles of a downloadable mobile (DM) system that consists in the personalization of a DM agent installed in a user secondary device.

**3.2.2 DM_MSS**: One of roles of a downloadable mobile (DM) system that consists in the management of on-line or off-line download.

**3.2.3 CDCS_ISS**: One of the roles of a downloadable mobile (DM) system that consists in the personalization of CA/DRM client software (CDCS) installed in a user secondary device.

**3.2.4 CDCS_MSS**: One of the roles of a downloadable mobile (DM) system that consists in the establishment of a secure channel between CDCS_MSS and a DM agent and management of CA/DRM client software (CDCS) download.

**3.2.5 CDCS_PSS**: One of the roles of a downloadable mobile (DM) system that consists in the management of content access entitlement policy, based on access rights, which differ according to the entitlement levels and hardware capability of the secondary device considered.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA Conditional Access

CDCS CA/DRM Client Software

CPE Customer Premises Equipment

DM Downloadable Mobile multi-CA/DRM

DRM Digital Rights Management

ISS Initialization Personalization Sub-System

MSS Management Sub-System

MVPD Multichannel Video Programming Distributor

PSS Policy Sub-System

RCAS Renewable Conditional Access System

SD Secondary Device

## 5 Conventions

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its annexes, the words "shall", "shall not", "should" and "may" sometimes appear, in which case they are to be interpreted, respectively, as "is required to", "is prohibited from", "is recommended" and "can optionally". The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

## 6 Reference model for a DM system

A reference model for DM service for secondary devices is shown in Figure 1. It consists of three parts, a third party authorization centre, a multichannel video programming distributor (MVPD) and the secondary device. The third party authorization centre is called a downloadable mobile multi-CA/DRM (DM) centre and it includes an entitlement control server and entitlement information. The MVPD is connected with a secondary device. CA/DRM client software (CDCS) images are supposed to be delivered in these networks and users can watch pay-television contents using a secondary device.

To securely download CDCS image, a secondary device should be equipped with a DM agent in advance. The DM agent is located inside the secondary device and provides initialization and download functions of CDCS. The DM agent can be loaded into a secondary device using online or offline methods. If the online method is used, the DM centre and the secondary device must use a pre-defined secure communication protocol such as RCAS network protocol [b-ITU-T J.1003]. On the other hand, if the offline method is used, a user who has a secondary device should visit a third party commissioned from the MVPD.

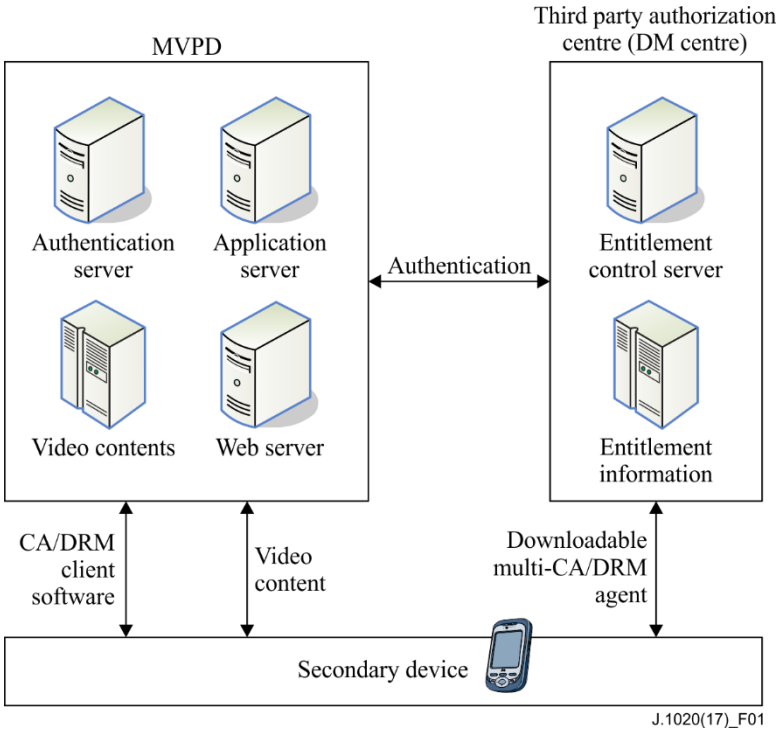


**Figure 1 – Reference model for downloadable mobile multi-CA/DRM system**

## 7 Actors and roles

A system for DM service has actors and roles which are shown in Figure 2. The detailed descriptions for major roles are as follows: DM_MSS is for managing on-line or off-line downloads. DM_ISS is for DM agent personalization. Application is for playing video contents and providing a user interface. A HTML5 web application or an android application could be examples. CDCS_ISS is for CDCS personalization. CDCS_MSS is for establishment of a secure channel between CDCS_MSS and the DM agent and for managing CDCS download. CDCS_PSS is for managing content access entitlement policy based on access rights which differ according to entitlement levels and the hardware capability of the secondary device. It should be noted that CP in Figure 2 means that the content provider is directly operated by MVPD. Finally, the SD I/F agent has a role of not only relaying messages between head-end and a secondary device, but also of establishing a secure link between a primary CPE and a secondary device.

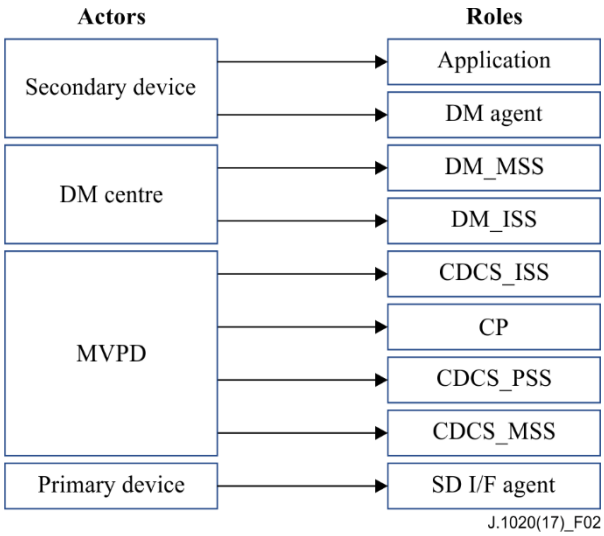


**Figure 2 – Relationship between actors and roles**

## 8 System architecture

A system architecture for DM service is shown in Figure 3. The basic operation flows are as follows: Firstly, a secondary device deploys a DM agent through DM_MSS in the DM centre via an SD I/F agent. At this moment, on-line or off-line methods can be used for downloading the DM agent. Secondly, the application performs as a DM agent when a user wants to access mobile pay TV cable television services. If the DM agent is not personalized at this time, it must be personalized prior to being run by the application. Thirdly, the application downloads the CDCS via the SD I/F agent and installs it to a secondary device. In this step, the types of downloaded CDCS are variously based on access entitlement or hardware capabilities. MVPD has to perform the CDCS download process via the SD I/F agent only after the DM centre has authorized the secondary device. The CDCS should be personalized after downloading. Finally, a user watches pay TV contents through the downloaded CDCS.

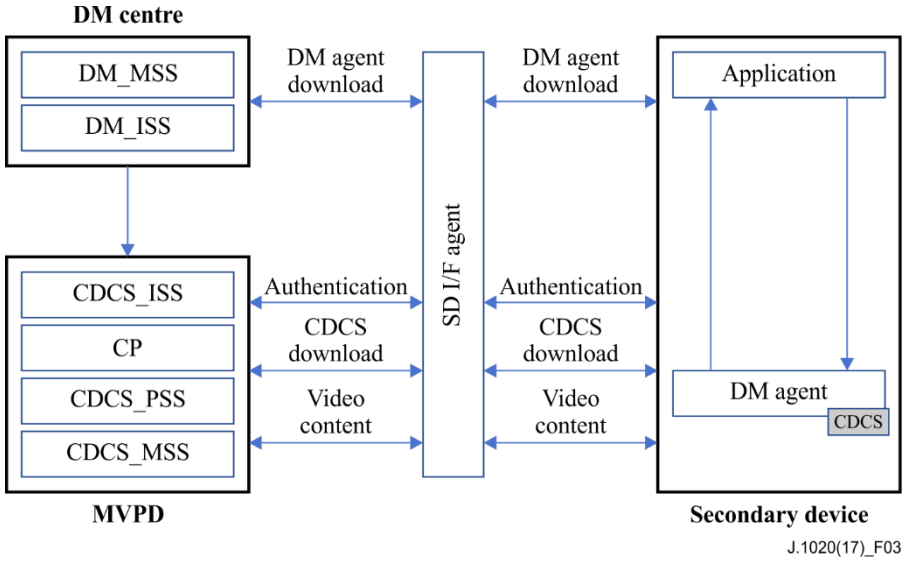


**Figure 3 – Architecture for a DM system**

## 9 DM agent download and installation operation

The DM agent download and installation operation is shown in Figure 4. A detailed description for each step is provided as follows:

In step 1, the application recognizes that the DM agent is not loaded in a secondary device and requests the DM agent download request message from the DM_MSS. The access information for the DM_MSS could be found in the application. The request message should include authentication and secondary device information.

In step 2, the DM_MSS performs secondary device authentication based on the authentication and the secondary device information delivered via a request message from the application.

In step 3, the DM_MSS sets up a secure channel for the DM agent download. The secure channel should provide the DM agent, the application authentication and the message authentication with confidentiality and integrity.

In step 4, the DM_MSS downloads the DM agent through a secure channel which was established in the previous step.

In step 5, the application installs the downloaded DM agent in a secondary device.

In step 6, the application requests DM agent personalization from the DM agent.

In step 7, the DM agent requests DM agent personalization data to the DM_ISS. The access information for DM_ISS could be provided when DM agent is downloaded or found in the DM agent itself. The secondary device hardware capability and identifier/key information for authentication from an application will be delivered along with the DM agent information.

In step 8, the DM_ISS performs the secondary device authentication based on the identifier/key information for authentication, which was delivered in the previous step.

In step 9, the DM_ISS establishes a secure channel between the DM_ISS and the application for secure transmission of personalization data. The secure channel should provide the DM_ISS and the application authentication as well as the message authentication with confidentiality and integrity.

In step 10, the DM_ISS delivers the DM agent personalization data such as the DM identifier and certificates.

In step 11, the DM agent performs its personalization process by utilizing the relevant data, received in the previous step.

In step 12, the DM agent informs the application about the results of its personalization process.

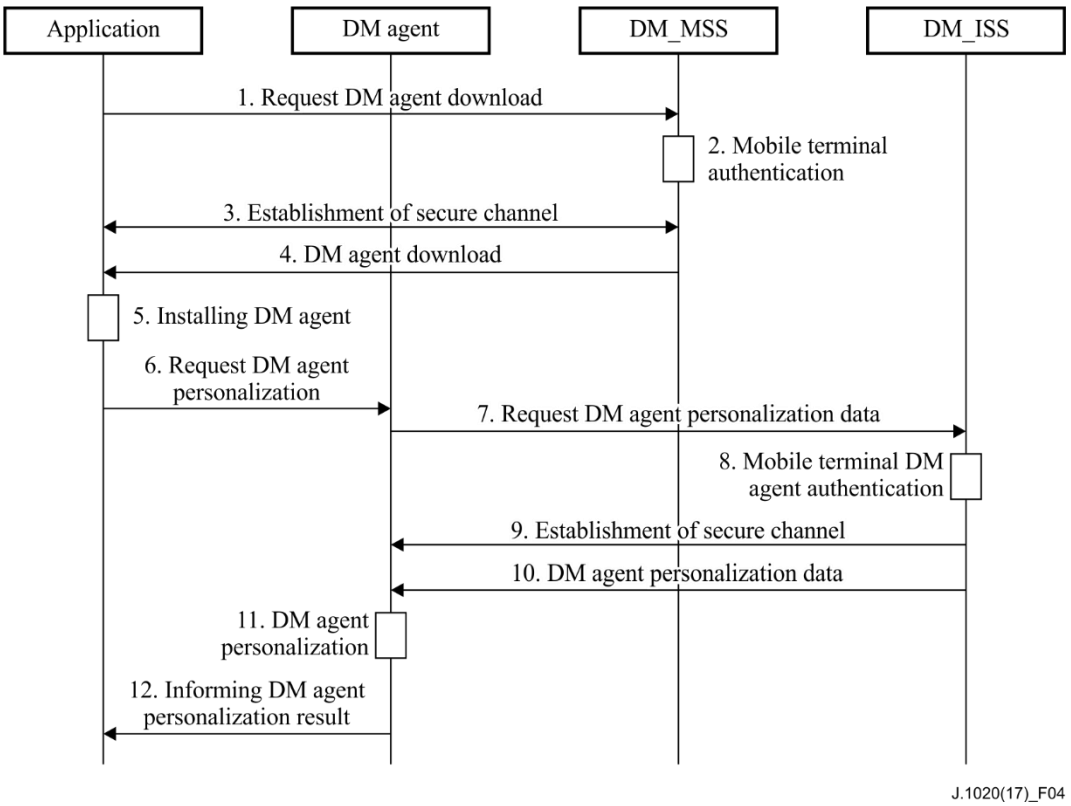


**Figure 4 – A flow of DM agent download and installation operation**

## 10 CA/DRM client software download and installation operation

The CA/DRM client software download and installation operation is shown in Figure 5. A detailed description for each step is provided as follows:

In step 1, the DM agent sends a request message for a secondary device authentication as well as for the authentication of the DM agent itself to the CDCS_PSS.

In step 2, the CDCS_PSS performs the authentication process based on the information from the request message. At this time, personalization and secondary device information is used for the authentication.

In step 3, the CDCS_PSS sets up a secure channel between the CDCS_PSS and the DM agent.

In step 4, the CDCS_PSS requests the CDCS which is to be used by the secondary device from the CDCS_MSS.

In step 5, the CDCS_MSS responds with the CDCS and the CDCS_MSS authentication information.

In step 6, the CDCS_PSS downloads the CDCS and the CDCS_MSS authentication information.

In step 7, the DM agent checks whether a secondary device has already downloaded the CDCS based on the CDCS information.

In step 8, the DM agent requests the CDCS download from the CDCS_MSS.

In step 9, the CDCS_MSS authenticates the CDCS download request message based on the CDCS_MSS authentication information which was delivered in Step 5 and 6.

In step 10, the CDCS_MSS establishes a secure channel between the CDCS_MSS and the DM agent for secure download of the CDCS.

In step 11, the CDCS_MSS requests the CDCS_ISS authentication information for the DM agent from the CDCS_ISS.

In step 12, the CDCS_ISS delivers the CDCS_ISS authentication information, which will be used for authenticating the CDCS personalization information request, to the CDCS_PSS.

In step 13, the CDCS_MSS delivers the CDCS and the CDCS_ISS authentication information for the DM agent through the secure channel.

In step 14, the DM agent installs the CDCS and runs it.

In step 15, the CDCS delivers a request message for personalization of the CDCS.

In step 16, the CDCS_ISS performs the CDCS authentication based on the CDCS_MSS authentication information which is included in the personalization request message.

In step 17, the CDCS_ISS establishes a secure channel to download the CDCS personalization data.

In step 18, the CDCS_ISS delivers the CDCS personalization data through the secure channel.

In step 19, the CDCS performs the personalization process based on the CDCS personalization data which was acquired in the previous step.

In step 20, the CDCS_ISS informs the CDCS_PSS of the results of the personalization.

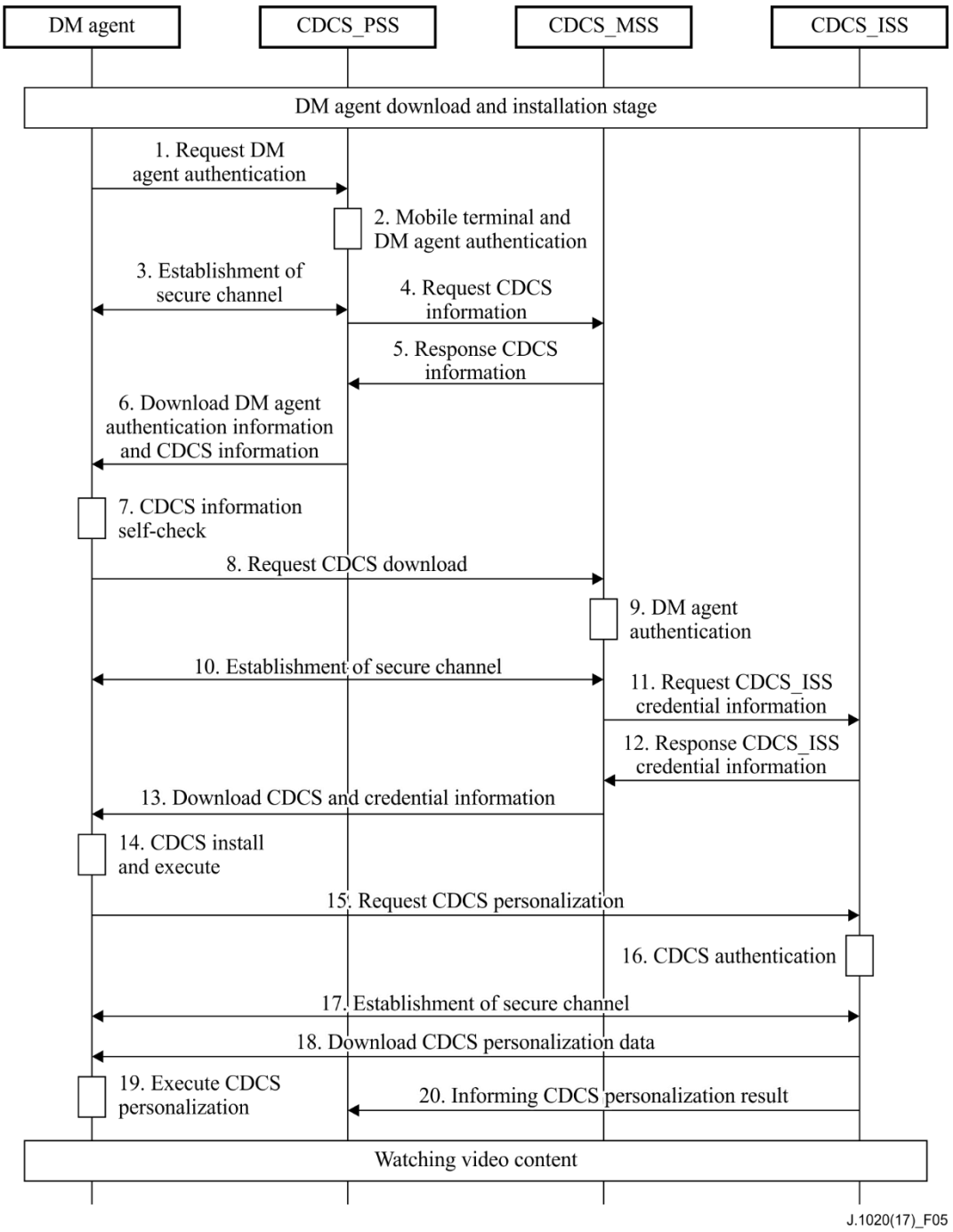


**Figure 5 – A flow of CA/DRM client software download and installation operation**

# Bibliography


[b-ITU-T J.193] Recommendation ITU-T J.193 (2004), *Requirements for the next generation of set-top-boxes*.

[b-ITU-T J.1001] Recommendation ITU-T J.1001 (2012), *Requirements for renewable conditional access system.*

[b-ITU-T J.1002] Recommendation ITU-T J.1002 (2013), *Pairing protocol specification for renewable conditional access system.*

[b-ITU-T J.1003] Recommendation ITU-T J.1003 (2014), *Specifications of network protocol for renewable conditional access system.*

[b-ITU-T J.1004] Recommendation ITU-T J.1004 (2015), *Specifications of authorization centre interfaces for renewable conditional access system*.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | Tariff and accounting principles and international telecommunication/ICT economic and policy issues |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| **Series J** | **Cable networks and transmission of television, sound programme and other multimedia signals** |
| Series K | Protection against interference |
| Series L | Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling, and associated measurements and tests |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks, open system communications and security |
| Series Y | Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2017