**“적자생존: 적는 자만이 살아 남는다”**

**DRM 기능 구현**

**상세설계서**

Version 1.0

**㈜ 마크애니**

문서정보

|  |  |
| --- | --- |
| 버 전 | 1.0 |
| 작성일 | 2019년 05월 30일 |
| 작성자 | 김홍구 |
| 검토자 | 이래욱, 이주용, 하홍준 |
| 승인자 | 신동환 |

개정 이력

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 버전 | 개정일자 | 개정 내역 | 작성자 | 승인자 |
| 1.0 | 2019.05.30 | 초안 작성 | 김홍구 | 신동환 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Copyright © 2019 MarkAny**

이 문서의 내용을 임의로 전재 및 복사할 수 없으며, 이 문서의 내용을 부분적으로라도 이용 또는 전재할 경우, 반드시 저자인 ㈜마크애니의 서면 허락을 취득하여야 한다.

**문서 확인**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 구분 | 성명 | 기여부분 | 소속 | 날짜 | 확인  결과 |
| 작성자 | 김홍구 |  | 마크애니 |  | OK |
| 검토자 | 이래욱 | 상세설계 검토 | 마크애니 |  | OK |
| 이주용 | 마크애니 |  | OK |
| 하홍준 | 마크애니 |  | OK |
| 품질보증 | 김현규 | 상세설계 내용 품질 검토 | 마크애니 |  | OK |
| 사업책임자 | 신동환 | 상세설계 검토 내용 확인 | 마크애니 |  | OK |

목차

[1 개요 6](#_Toc530937129)

[1.1 문서의 목적 6](#_Toc530937130)

[1.2 용어 정의 및 약어 6](#_Toc530937131)

[1.3 참고문헌 7](#_Toc530937132)

[2 고속 CID 삽입 및 검출 기술 8](#_Toc530937133)

[2.1 고속 CID 삽입 및 검출기술의 필요성 8](#_Toc530937134)

[2.1.1 콘텐츠용 CID 삽입 연동기술이 필요한 이유 8](#_Toc530937135)

[2.2 고속 CID 삽입 및 검출기술의 필요성 10](#_Toc530937136)

[2.2.1 고속 CID 삽입기술의 요구사항 10](#_Toc530937137)

[2.2.2 오디오 CID삽입 기술 11](#_Toc530937138)

[2.2.3 오디오 CID삽입 기술 API 정의 11](#_Toc530937139)

[2.2.4 비디오 CID삽입 기술 12](#_Toc530937140)

[2.2.5 비디오 CID삽입기 API 정의 12](#_Toc530937141)

[2.3 고속 CID 검출기술 13](#_Toc530937142)

[2.3.1 고속 CID 검출기술의 필요성 13](#_Toc530937143)

[2.3.2 오디오용 고속 CID 검출기술 13](#_Toc530937144)

[2.3.3 오디오용 고속 CID 검출기 API정의 14](#_Toc530937145)

[2.3.4 비디오용 고속 CID 검출기술 15](#_Toc530937146)

[2.3.5 비디오용 고속 CID 검출기 API정의 15](#_Toc530937147)

**그림 목차**

[그림 2‑1. DRM 패키징시스템 구성도 8](file:///D:\MyDocuments\2.연구과제\2.블럭체인_대용량DRM%20연구과제\5.2차년도%20자료\19MA-DDD-DRM-1.0_DRM%20기능%20구현_상세설계서.docx#_Toc14426768)

[그림 2‑2 DRM 패키징시스템 구성도 9](file:///D:\MyDocuments\2.연구과제\2.블럭체인_대용량DRM%20연구과제\5.2차년도%20자료\19MA-DDD-DRM-1.0_DRM%20기능%20구현_상세설계서.docx#_Toc14426769)

[그림 2‑3. 오디오용 CID삽입기 동작 흐름도 11](file:///D:\MyDocuments\2.연구과제\2.블럭체인_대용량DRM%20연구과제\5.2차년도%20자료\19MA-DDD-DRM-1.0_DRM%20기능%20구현_상세설계서.docx#_Toc14426770)

[그림 2‑4. 비디오용 CID삽입기 동작 흐름도 12](file:///D:\MyDocuments\2.연구과제\2.블럭체인_대용량DRM%20연구과제\5.2차년도%20자료\19MA-DDD-DRM-1.0_DRM%20기능%20구현_상세설계서.docx#_Toc14426771)

[그림 2‑5. 블록체인에서 CID 검출 시스템의 사용 예 14](file:///D:\MyDocuments\2.연구과제\2.블럭체인_대용량DRM%20연구과제\5.2차년도%20자료\19MA-DDD-DRM-1.0_DRM%20기능%20구현_상세설계서.docx#_Toc14426772)

[그림 2‑6. 오디오용 CID 추출기 동작 흐름도 15](file:///D:\MyDocuments\2.연구과제\2.블럭체인_대용량DRM%20연구과제\5.2차년도%20자료\19MA-DDD-DRM-1.0_DRM%20기능%20구현_상세설계서.docx#_Toc14426773)

[그림 2‑7. 비디오용 CID추출기 동작 흐름도 16](file:///D:\MyDocuments\2.연구과제\2.블럭체인_대용량DRM%20연구과제\5.2차년도%20자료\19MA-DDD-DRM-1.0_DRM%20기능%20구현_상세설계서.docx#_Toc14426774)

# 개요

‘고속 CID 삽입 및 검출 기술’은 대용량 콘텐츠를 유통은 기존의 다양한 환경을 지원하고자 한다. CDN, Adaptive 스트리밍, 트랜스코딩 등과 같은 환경을 거치면서 같은 콘텐츠 임에도 다양한 변형이 생기게 되는데 기존의 해쉬값을 이용한 콘텐츠 추적은 더 이상 사용할 수 없다. 콘텐츠 내부에 워터마크를 이용하여 CID를 삽입, 추출하여 콘텐츠를 인식하고 이를 바탕으로 정상적인 사용이 가능한 구조를 개발하고자 한다.

## 문서의 목적

본 문서는 ‘실시간 대용량 데이터 유통을 위한 온-오프체인 하이브리드 블록체인 기술 개발’ 과제 수행의 일환으로 시스템을 통하여 유통될 디지털콘텐츠에 대하여 콘텐츠 내부에 워터마크 기술을 이용하여 CID를 삽입하고 DRM 기술을 이용하여 암호화처리하여, 콘텐츠의 위변조 방지 및 불법 복제를 방지하는데 그 목적이 있다.

## 용어 정의 및 약어

* **PID:** Producer Identifier
* **SID**: Supplier Identifier
* **DID:** Distributor Identifier
* **CID**: Content Identifier
* **UID**: User Identifier
* **UCI** : Universal Content Identifier
* **PInfo**: Payment Information
* **IPFS**: Inter Planetary File System
* **SP**: Service Provider
* **CEK**: Content Encryption Key
* **KIDS** : Keyless Infra Digital Signature

## 참고문헌

1. 마크애니, ‘실시간 대용량 데이터 유통을 위한 온-오프 하이브리드 블록체인 기술 개발’ 과제 사업계획서, 2018.03.
2. 마크애니, ‘실시간 대용량 데이터 유통을 위한 온-오프 하이브리드 블록체인 기술 개발’ 시스템 요구사항 정의서v1.0, 2018.05
3. 마크애니, ‘온-오프 하이브리드 블록체인 기술 개발’ 구조기능 설계서 v1.0, 2018.07
4. 마크애니, ‘온-오프 하이브리드 블록체인 기술 개발’ 상세설계서 v1.0, 2018.09

# DRM 패키징 시스템

## 시스템 구성

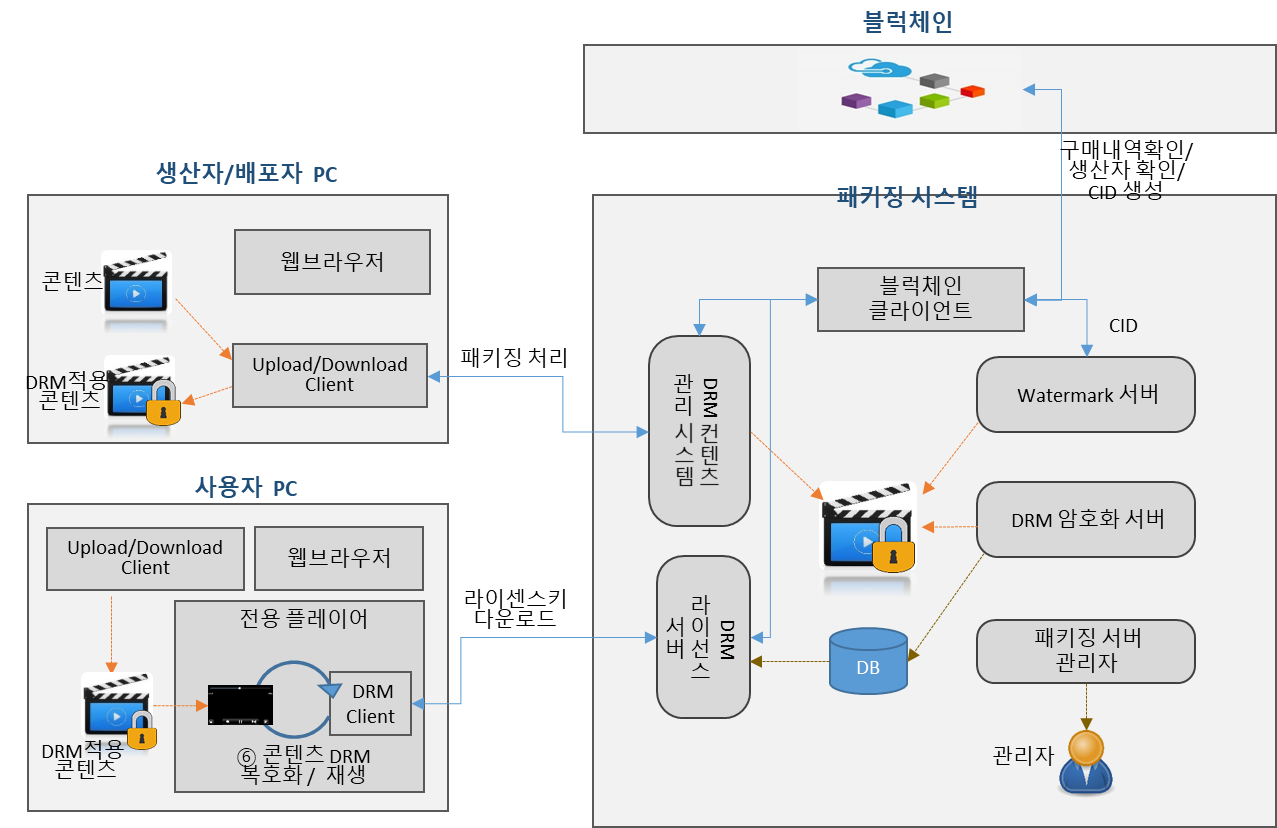


그림 2‑1. DRM 패키징시스템 구성도

DRM패키징시스템은 생산자로부터 패키징요청 및 패키징이 완료된 파일을 다운로드처리하는 DRM 컨텐츠 관리시스템, 워터마크를 처리하는 워터마크 서버, DRM암호화를 처리하는 서버, DRM라이선스 서버, 패키징 서버 관리자로 구성된다.

* **DRM 컨텐츠 관리시스템**: 생산자가 제작한 콘텐츠를 보호하기 위하여 배포 전에 워터마크 및 DRM 처리를 요청하거나, 처리가 완료된 콘텐츠를 다운로드 하는 시스템
* **DRM 라이선스 서버**: DRM이 적용된 콘텐츠를 재생하기 위한 라이선스키를 배포하는 시스템
* **Watermakr 서버**: 디지털콘텐츠 내에 콘텐츠식별자(CID)를 삽입하는 시스템
* **DRM 암호화 서버 :** 디지털콘텐츠를 암호화처리 하는 시스템
* **패키징서버 관리자 :** 패키징처리 과정을 관리하고, 처리로그를 조회할 수 있는 관리자용 시스템

## DB table 구조

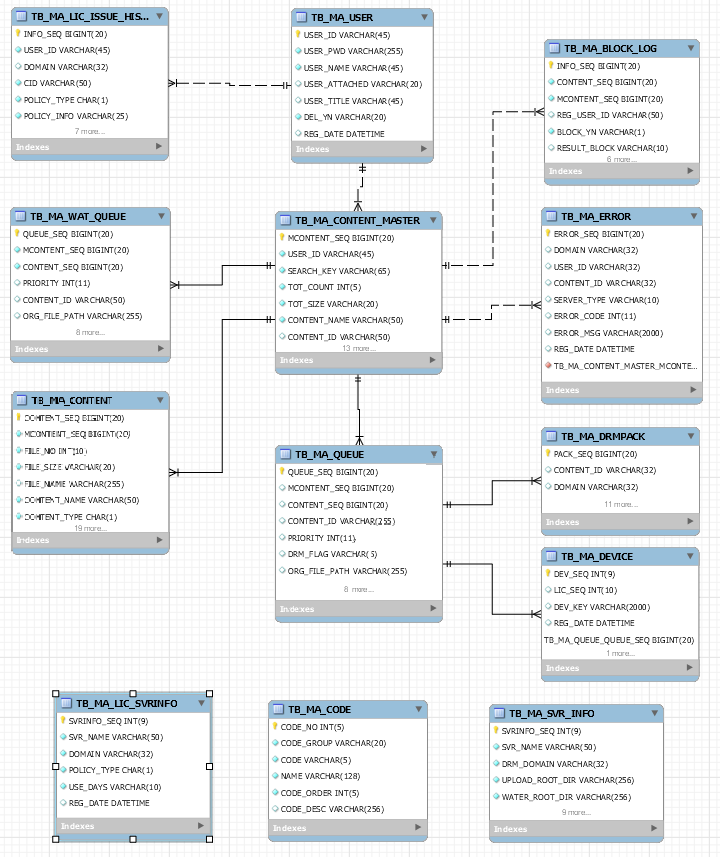
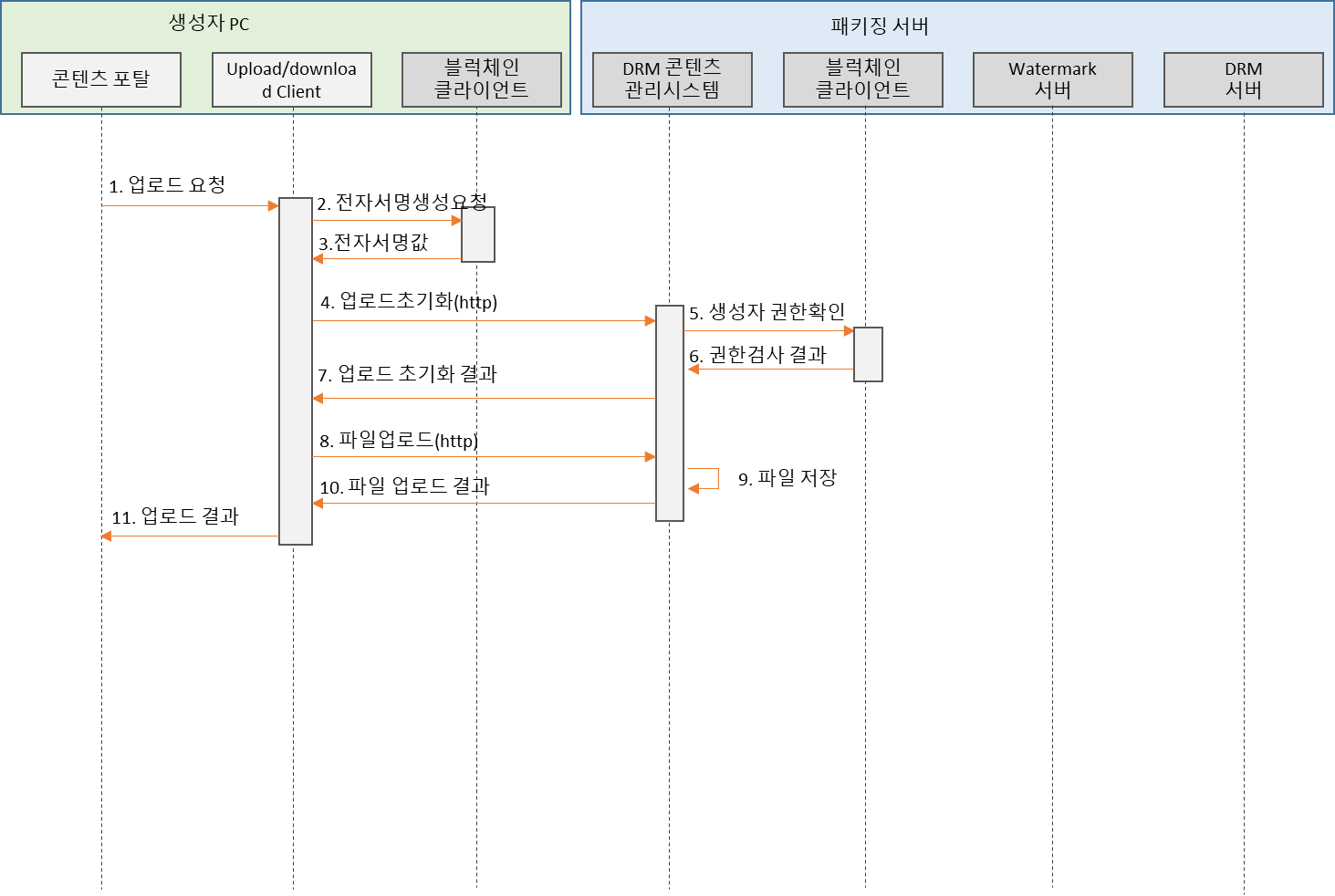


그림 2‑2 DRM 패키징시스템 ERD

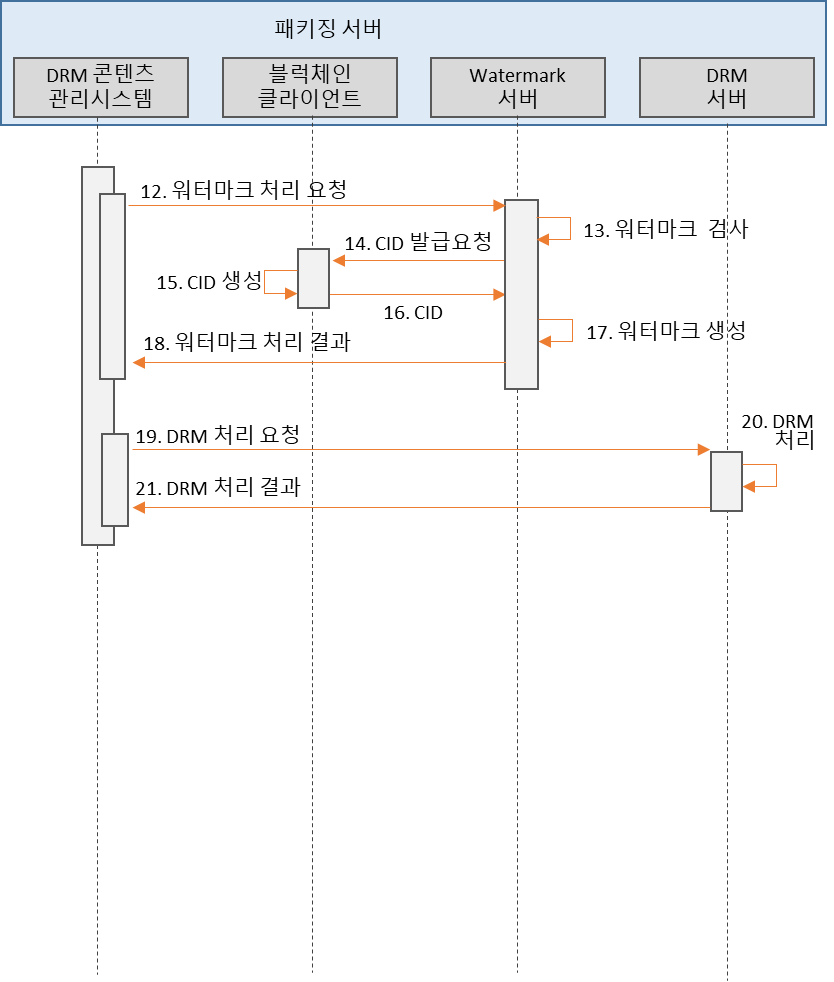
## 서비스 흐름

### 디지털콘텐츠 DRM 처리 요청



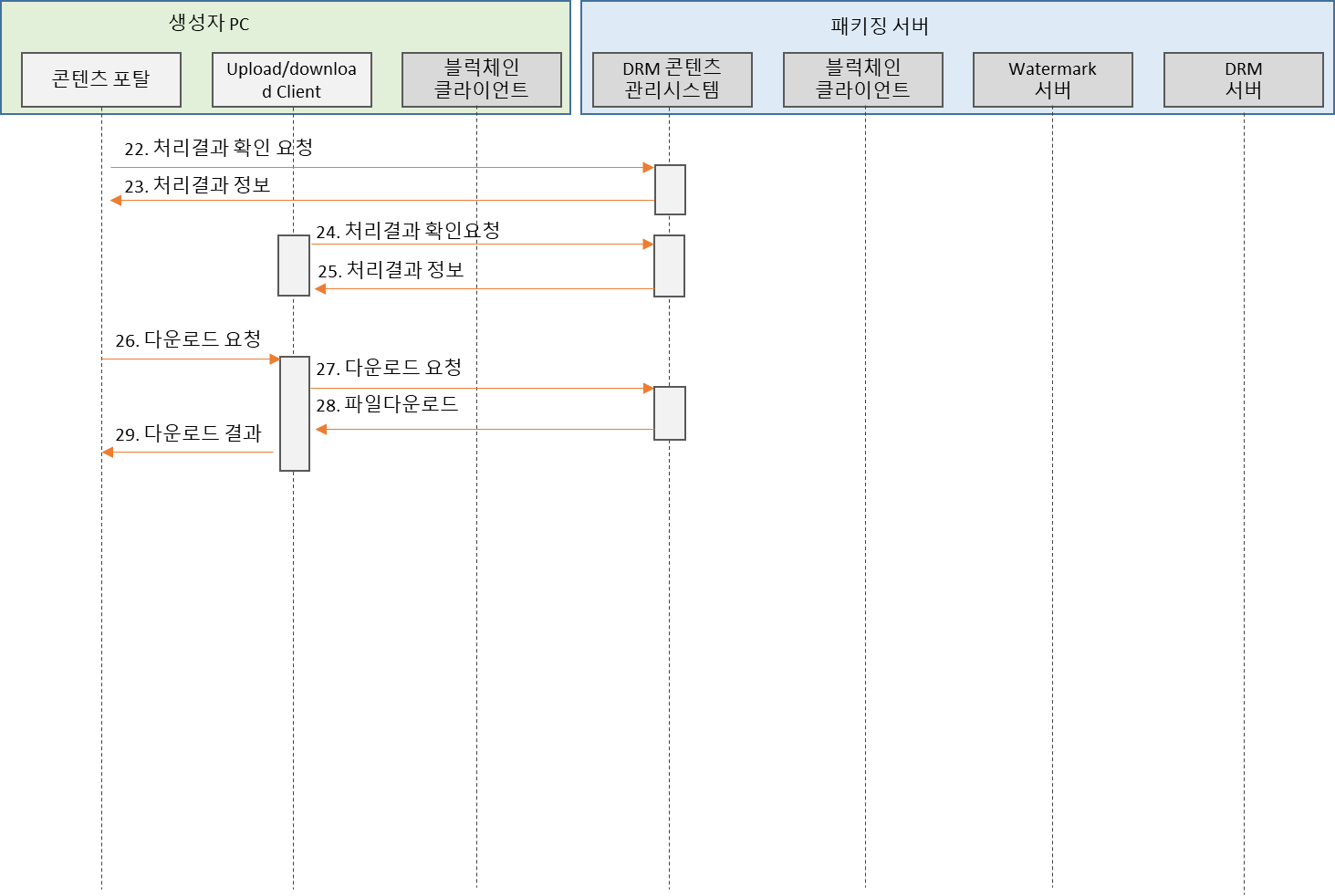
* 생산자는 본인이 생성한 디지털 콘텐츠를 배포하기전에 불법유통 차단, 권한이 없는 사용자의 이용 차단 등의 콘텐츠 보호를 위하여 DRM 패키징을 수행한다.
* 생산자는 패키징서버에 업로드 요청을 위하여 디지털 콘텐츠와 사용자 ID를 이용하여 전자서명서명을 생성하고, 업로드할 콘텐츠정보를 패키징서버로 전송한다.
* 패키징서버에서는 업로드한 사용자가 ‘생산자’ ROLE이 부여되었는지 확인하고, 파일을 업로드할 수 있는 ‘업로드초기화정보’를 생산자에게 전송한다.
* 생산자는 업로드초기화정보를 이용하여 콘텐츠를 업로드처리한다.

### DRM 처리 흐름



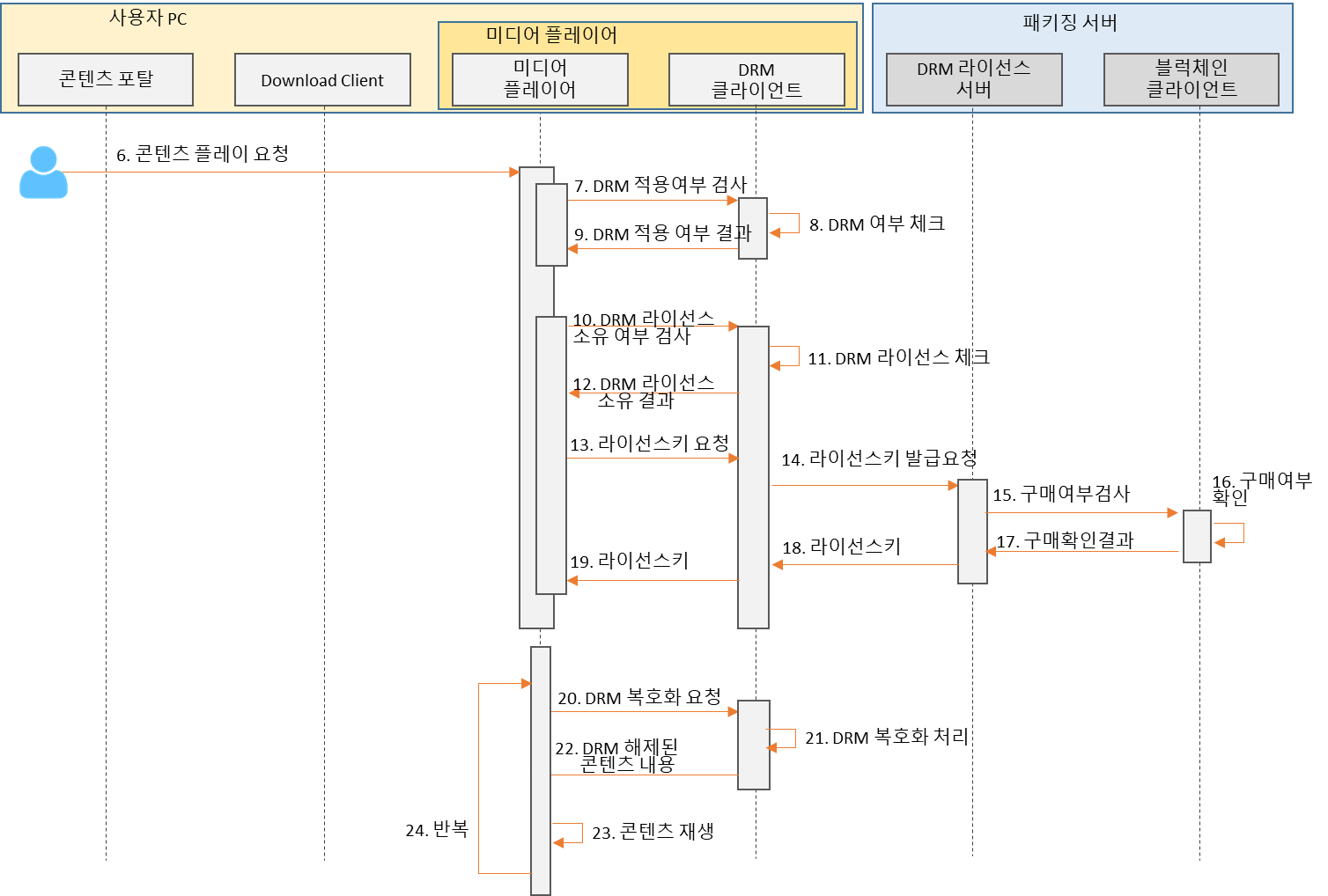
* DRM콘텐츠 관리시스템에서 생산자의 파일업로드가 완료되면 업로드된 파일 정보를 Watermark 서버로 전달한다.
* Watermark 서버에서는 전달되어온 업로드 파일에 대하여 워터마크가 존재하는지 여부를 판단하고, 블록체인 클라이언트를 이용하여 CID를 발급한다.
* CID 발급이 완료되면 콘텐츠에 CID워터마크를 생성한다.
* DRM콘텐츠 관리시스템에서 Watermark 서버에서 처리가 완료되었는지 모니터링 후 처리가 완료되면 파일의 정보를 DRM 서버로 전달한다.
* DRM서버에서는 전달되어온 파일에 대하여 DRM 암호화를 수행한다.
* DRM콘텐츠 관리시스템에서 DRM 서버에서 처리가 완료되었는지 모니터링을 진행한 후 처리 과정이 완료되면 생산자가 다운로드 가능하도록 상태정보를 변경한다.

### 다운로드 처리 흐름



* 생산자는 업로드한 파일이 DRM처리 상태를 확인하기 위하여 DRM콘텐츠관리시스템에 접속하여 진행상태를 체크한다.
* DRM처리상태가 완료상태인 경우 DRM처리완료 파일을 다운로드 처리한다.
* DRM콘텐츠관리시스템에서 생산자가 요청한 파일에 대하여 상태를 확인하고, 다운로드에 필요한 정보(파일크기, 상태, CID등)을 반환한다.

### 콘텐츠 재생 흐름



* 디지털콘텐츠를 구매한 사용자가 파일다운로드 환경을 통하여 다운로드한 파일에 대하여 요청하면 미디어플레이어에서 DRM클라이언트를 이용하여 DRM이 적용되었는지 확인한다.
* DRM이 적용되어 있는 경우 기존에 라이선스를 가지고 있는지 체크하고, 라이선스가 없는 경우 DRM라이센스 서버에 접속하여 라이선스를 다운로드 한다.
* 라이선스 서버에서는 블록체인에 접속하여 해당 사용자가 콘텐츠를 구매하였는지 검사 후 사용자에게 라이선스를 전송한다.
* 사용자는 다운로드한 라이선스를 이용하여 콘텐츠를 재생처리한다.