

Securitatea Conținutului Multimedia

Conf. dr. ing. Radu Ovidiu Preda

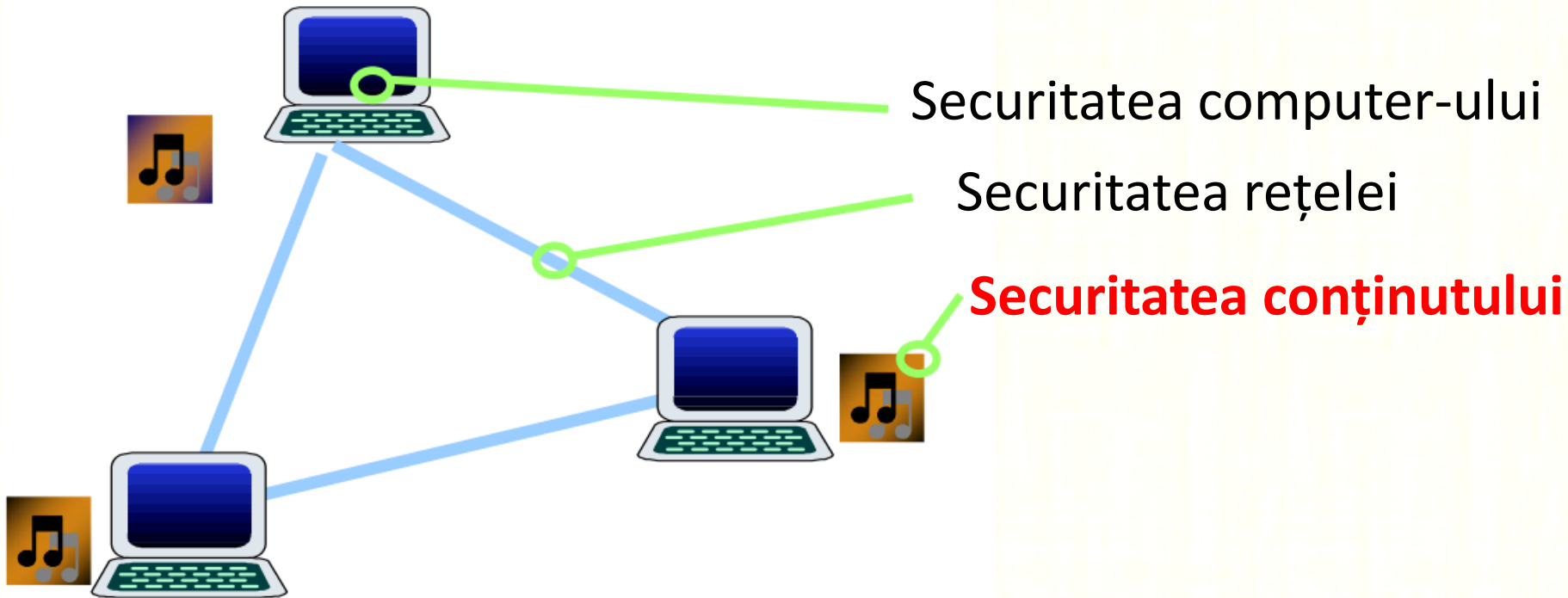
www.comm.pub.ro/preda/scm

Structura cursului

- Cap. 1 – Introducere în domeniul securității conținutului multimedia
- Cap. 2 – Sisteme de protecție și securizare a conținutului multimedia
- Cap. 3 – Tehnici de watermarking pentru semnale audio
- Cap. 4 – Tehnici de watermarking pentru imagini
- Cap. 5 – Tehnici de watermarking pentru video
- Cap. 6 – Atacuri asupra sistemelor de watermarking
- Cap. 7 – Autentificarea conținutului multimedia
- Cap. 8 – Tehnici criptografice

Introducere în domeniul securității conținutului multimedia

Tipuri de securitate



Tipuri de securitate

- Securitatea computerului
 - antivirus, firewall, criptare
- Securitatea rețelei
 - Autentificare sigură
 - Router cu ACL
 - Protocoale de rețea:
 - Secure File Transfer Protocol (SFTP),
 - Secure Hypertext Transfer Protocol (HTTPS)
 - Secure Socket Layer (SSL).
- Securitatea conținutului
 - tematica cursului

Tipuri de securitate

- Securitatea conținutului
 - Protecția la copiere;
 - Protecția proprietății intelectuale (watermarking, criptare, DRM);
 - Identificarea conținutului (fingerprinting);
 - Confidențialitatea datelor (criptare);
 - Autentificarea conținutului (activă sau pasivă);
 - Restaurarea conținutului (watermarking).



???



???

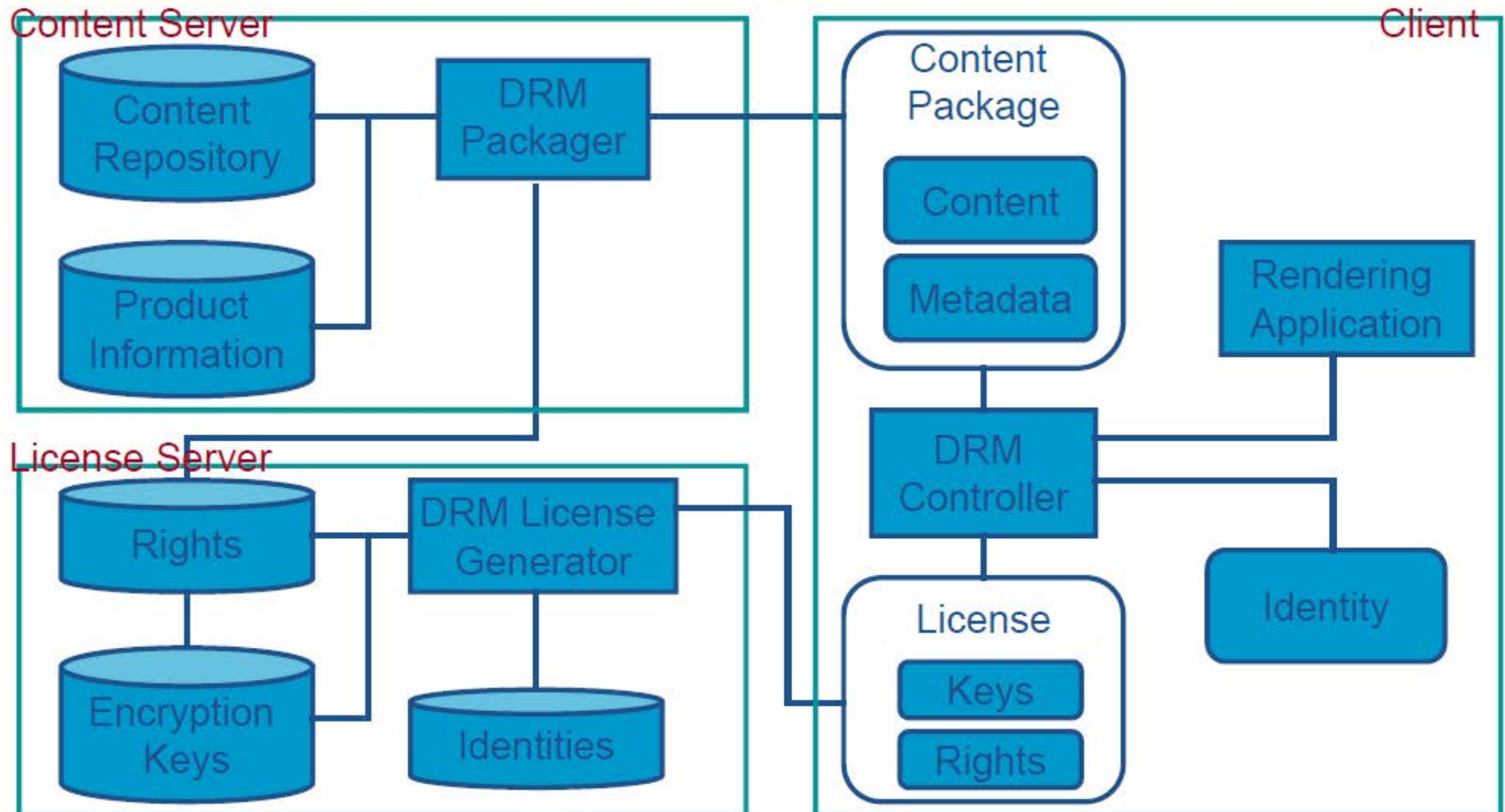
distribuitor de
conținut

beneficiar de
conținut

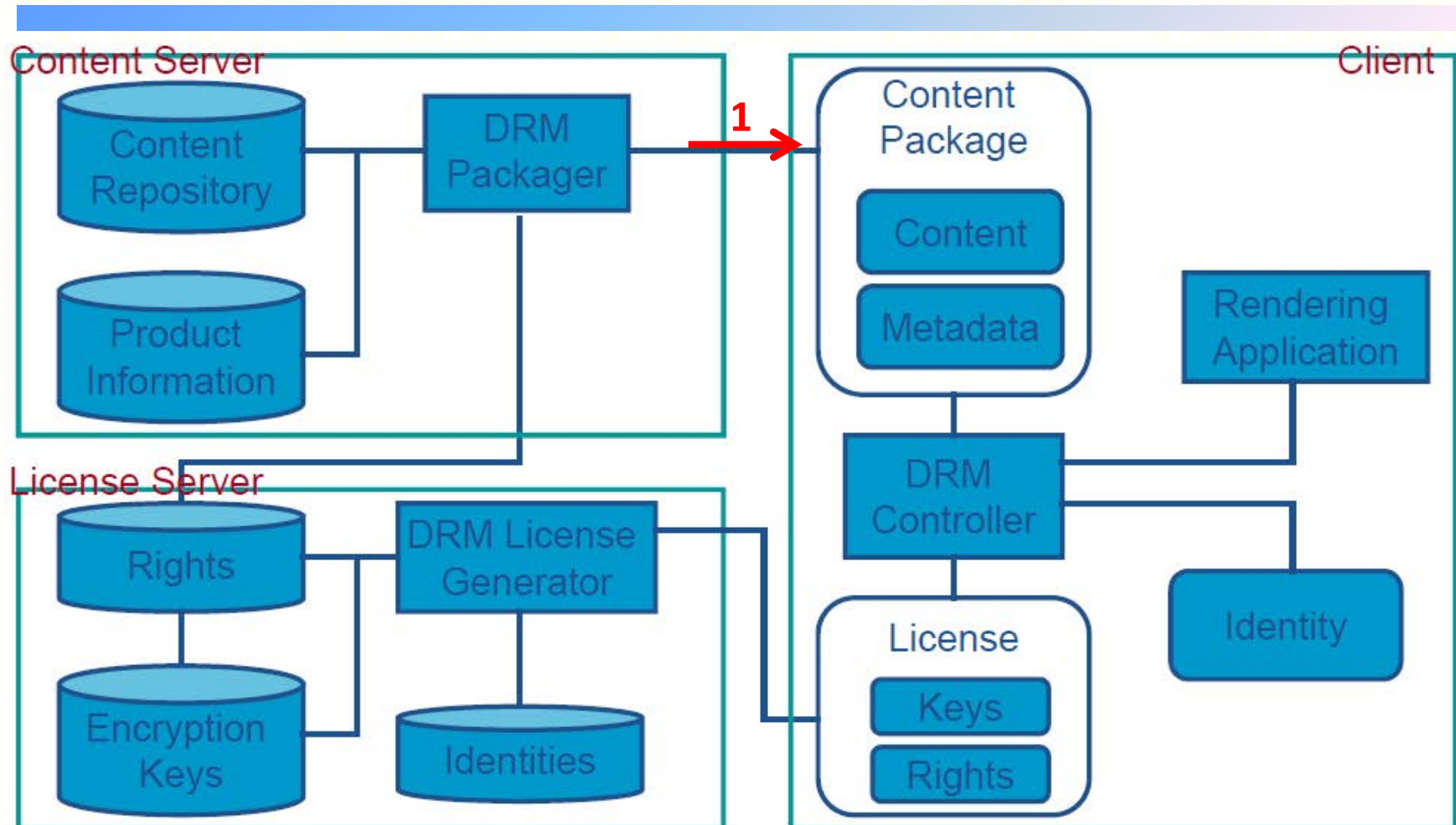
Sisteme DRM (Digital Rights Management)

- Sistem DRM = sistem de management al drepturilor de utilizare și distribuire a informațiilor multimedia;
- O clasă de tehnologii utilizate de producători de echipamente hardware, proprietari și distribuitori de conținut multimedia
- cu scopul de a controla utilizarea de conținut pe dispozitive digitale după vânzare
- Leagă anumite drepturi de utilizator de conținut pentru a controla accesul, duplicarea și partajarea datelor.

Arhitectura unui sistem DRM

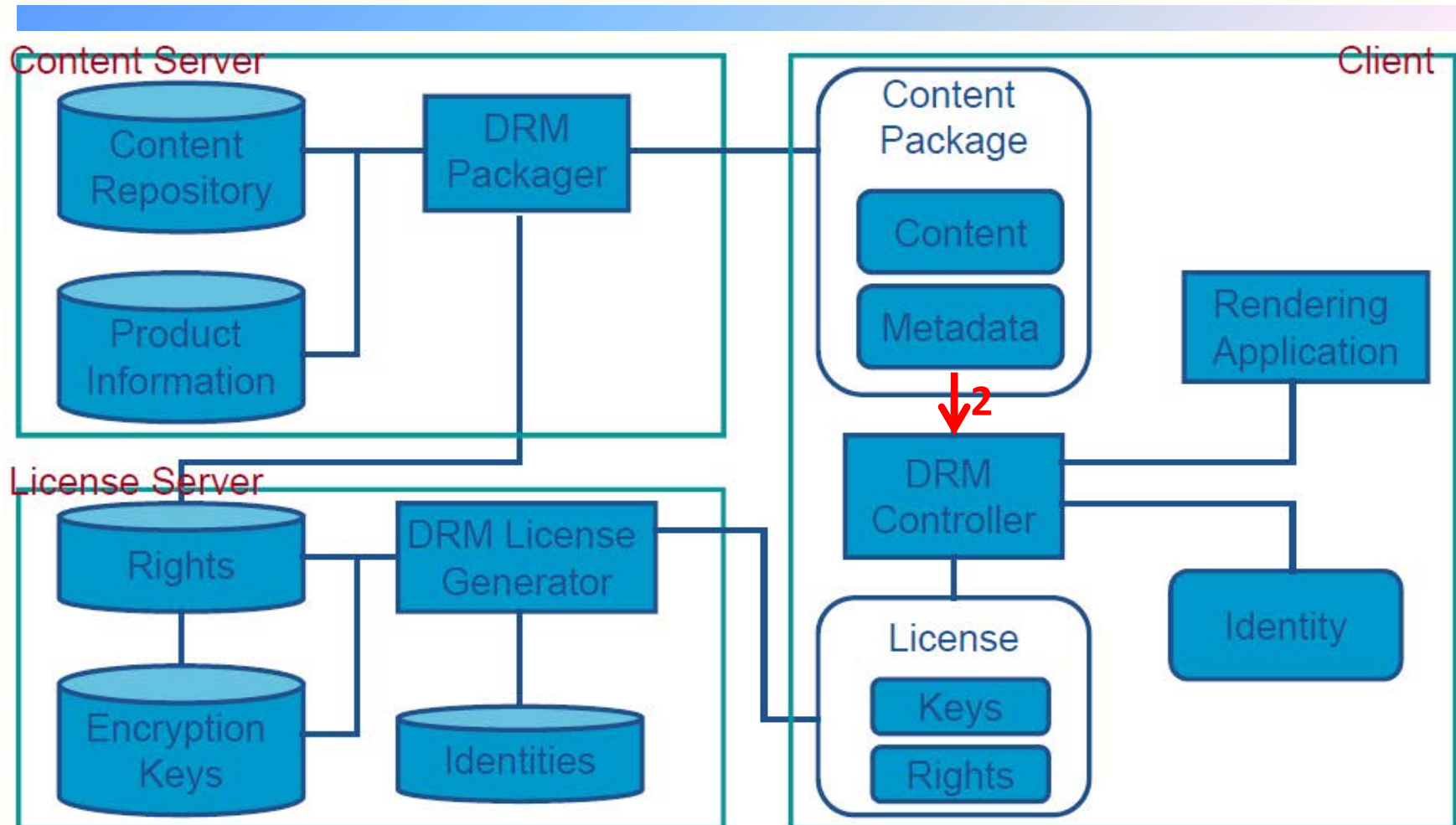


Arhitectura unui sistem DRM



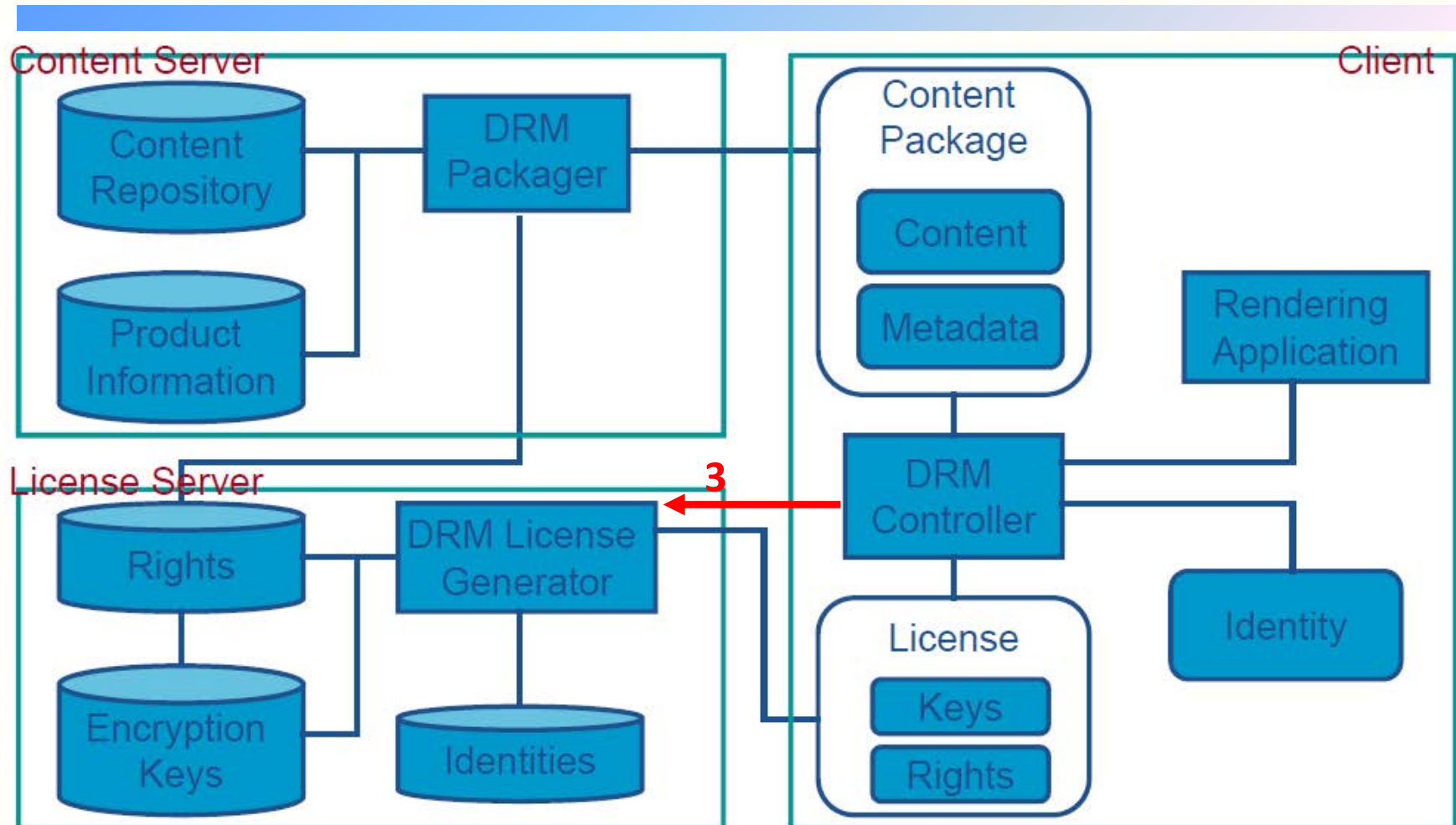
(1) obținerea pachetului de date

Arhitectura unui sistem DRM



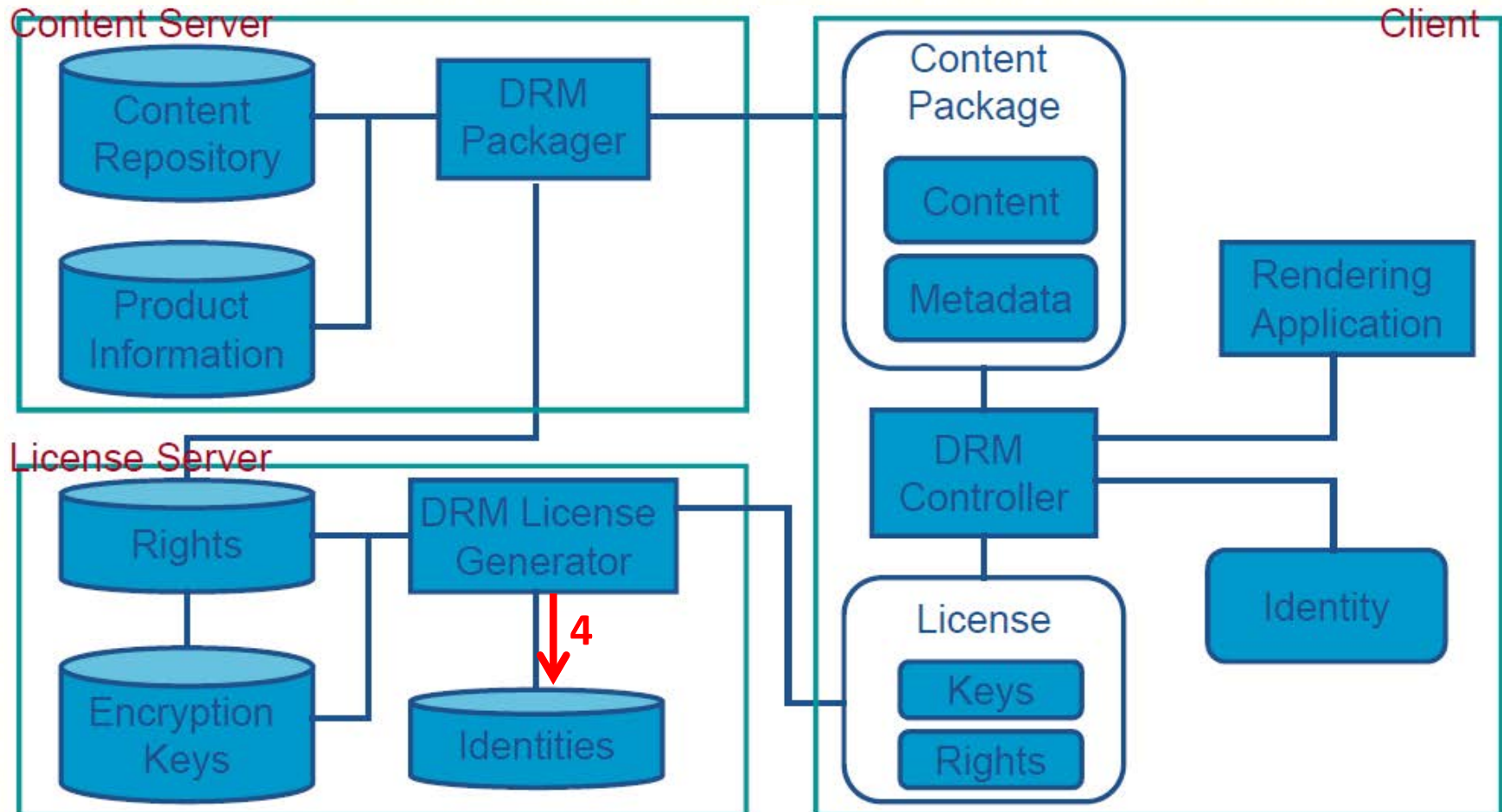
(2) Activarea controller-ului DRM

Arhitectura unui sistem DRM



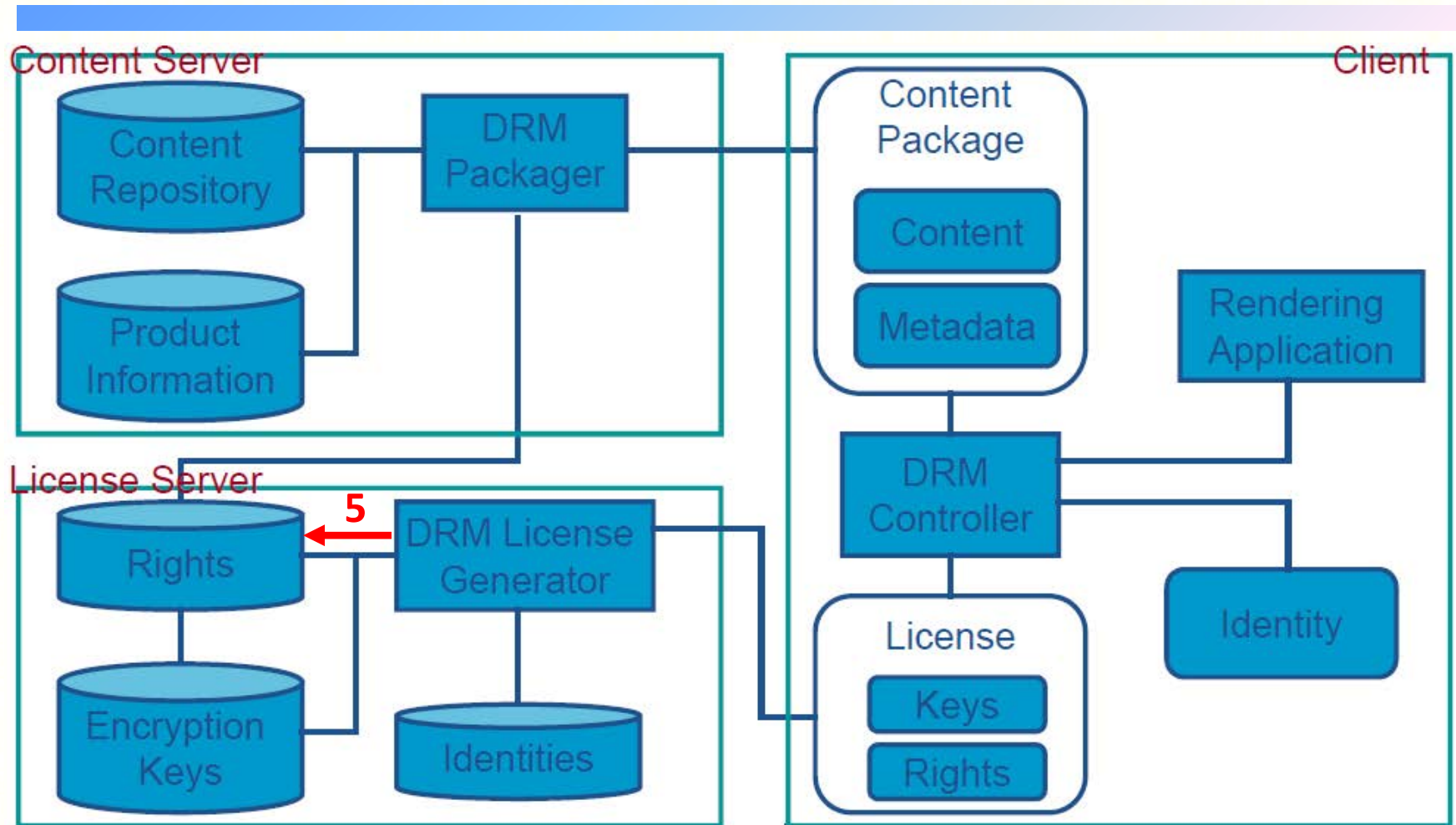
(3) Trimiterea informației către serverul de licențe

Arhitectura unui sistem DRM



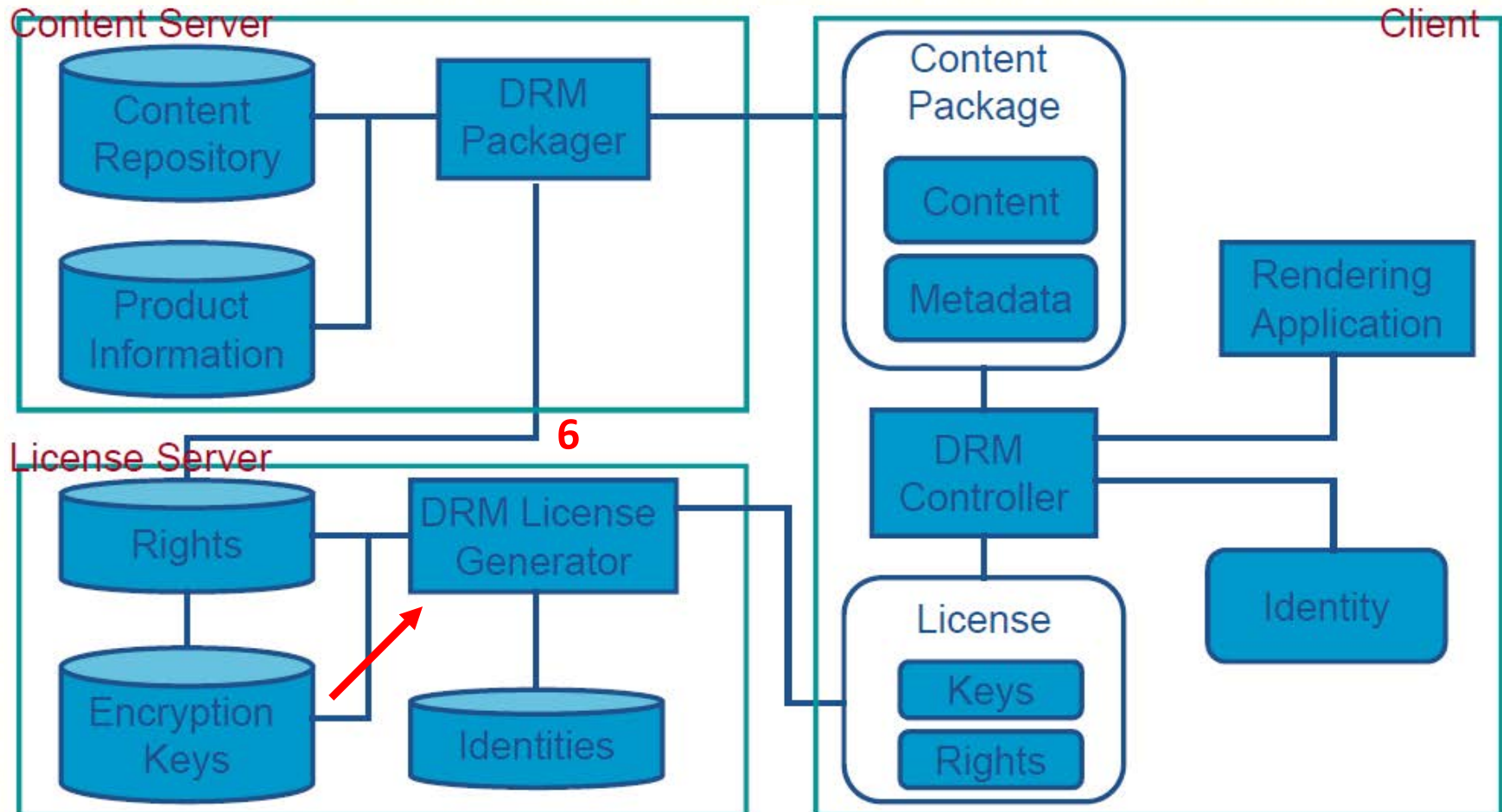
(4) Autentificarea identității clientului

Arhitectura unui sistem DRM



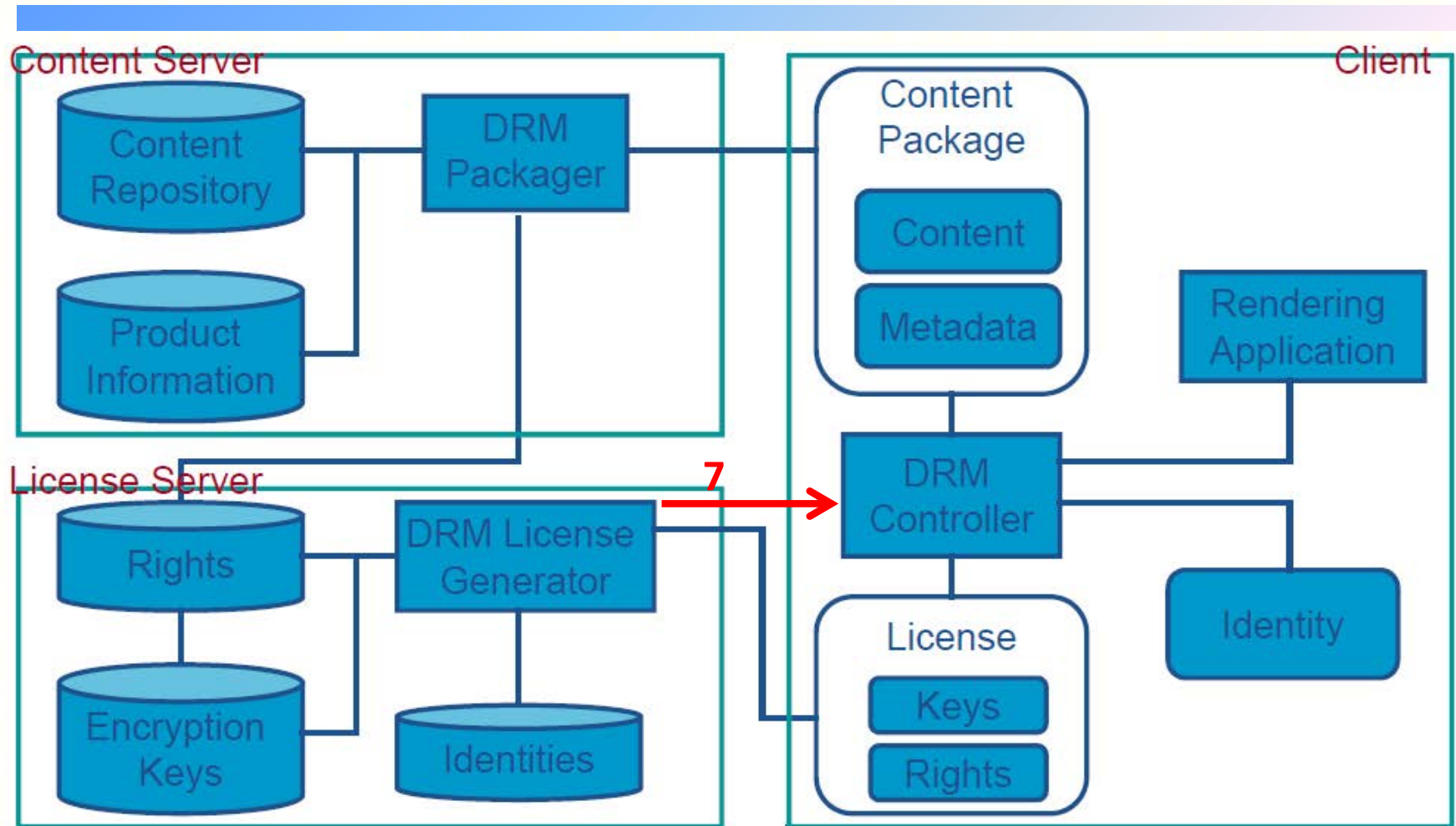
(5) Căutare informații de drepturi de utilizator

Arhitectura unui sistem DRM



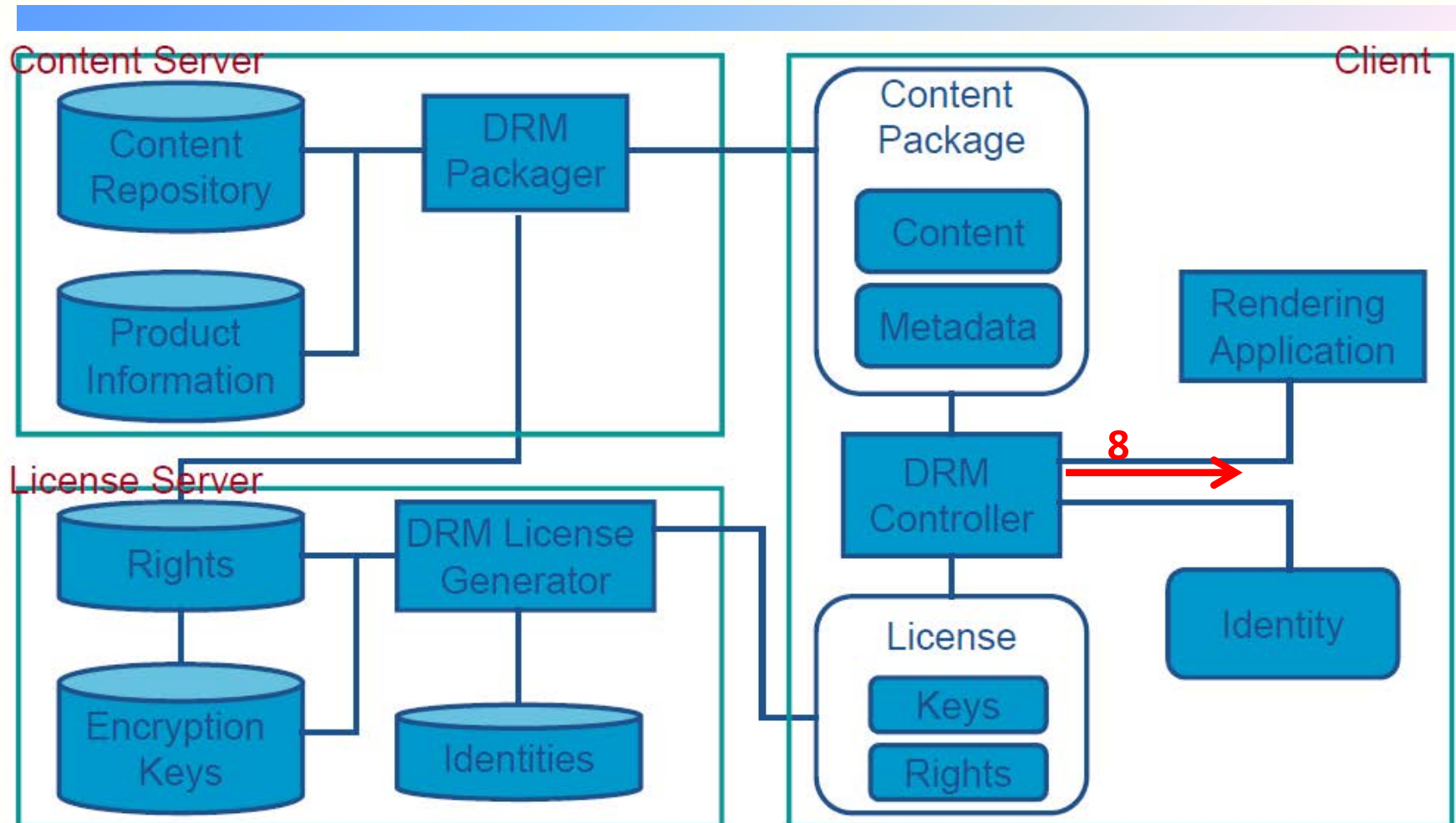
(6) Generarea licenței

Arhitectura unui sistem DRM



(7) Trimiterea licenței către controllerul DRM al clientului

Arhitectura unui sistem DRM



(8) Decriptarea conținutului și transmiterea către aplicația de redare

Sisteme DRM (Digital Rights Management)

Cărți electronice

- Amazon DRM pentru Mobipocket, KF8 și Topaz
- Adobe Adept DRM pentru ePub și PDF
- Apple Fairplay DRM pentru ePub; poate fi citit de aplicația iBooks pentru iOS.
- Marlin DRM pentru ePub

Sisteme DRM (Digital Rights Management)

Film

- Content Scrambling System (CSS) pentru DVD
- Advanced Access Content System (AACS) pentru HD DVD și Blu-ray Discs
- Marlin DRM pentru IPTV

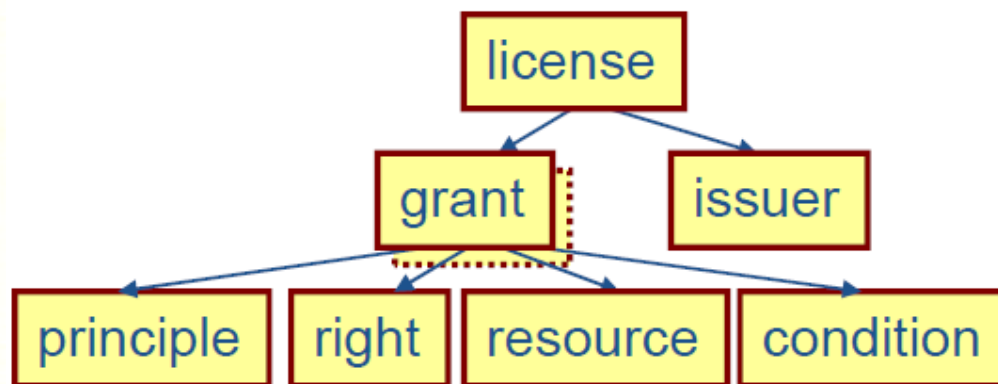
Tehnologii utilizate la sistemele DRM

Criptare	Watermarking	Multimedia Forensics	Metadata	Limbaje DRM
Protocoale criptografice	Watermark vizibil/invizibil	Identificarea sursei	Autor	XrML (eXtensible Rights Markup Language)
Cifruri simetrice	Watermark robust	Verificarea integrității	Distribuitoare	ODRL (Open Digital Rights Language)
Cifruri asimetrice	Watermark semi-fragil	Tehnici pasive	Cumpărător	MPEG REL (MPEG-21 Rights Expression Language)
Semnături digitale	Watermark fragil	Tehnici oarbe	Data achiziției	
Funcții Hash				

MPEG REL (MPEG-21 Rights Expression Language)

Structura unei licențe simple

- licență caracterizată prin emitent și conținut licență
- Conținut:
 - principle = persoana căreia îi este emisă licența;
 - right = drepturile pe care le specifică licența;
 - resource = resursele asupra cărora se aplică licența
 - condition = condiția care trebuie îndeplinită pentru ca drepturile să poată fi exercitate



MPEG REL

Exemplu:

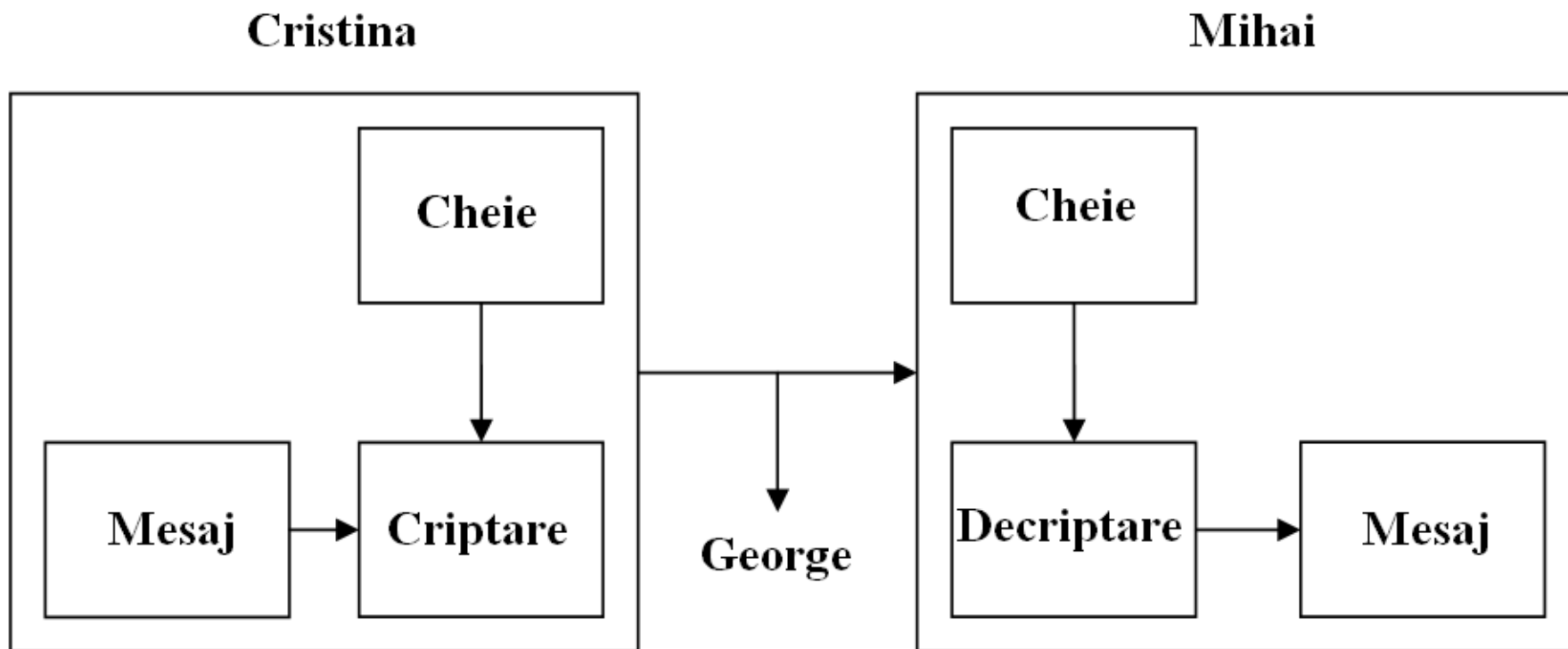
- Un student poate să vizioneze filmul XYZ de la adresa www.videoserver.com timp de șase luni, dacă se loghează de pe un computer cu o adresă IP 186.125.14.X
- **issuer** = www.videoserver.com
- **principle** = student
- **right** = să vizioneze
- **resource** = filmul XYZ
- **condition1** (validityInterval) = șase luni
- **condition2** = dacă se loghează de pe un computer cu o adresă IP 186.125.14.X

Sisteme de protecție și securizare a conținutului multimedia

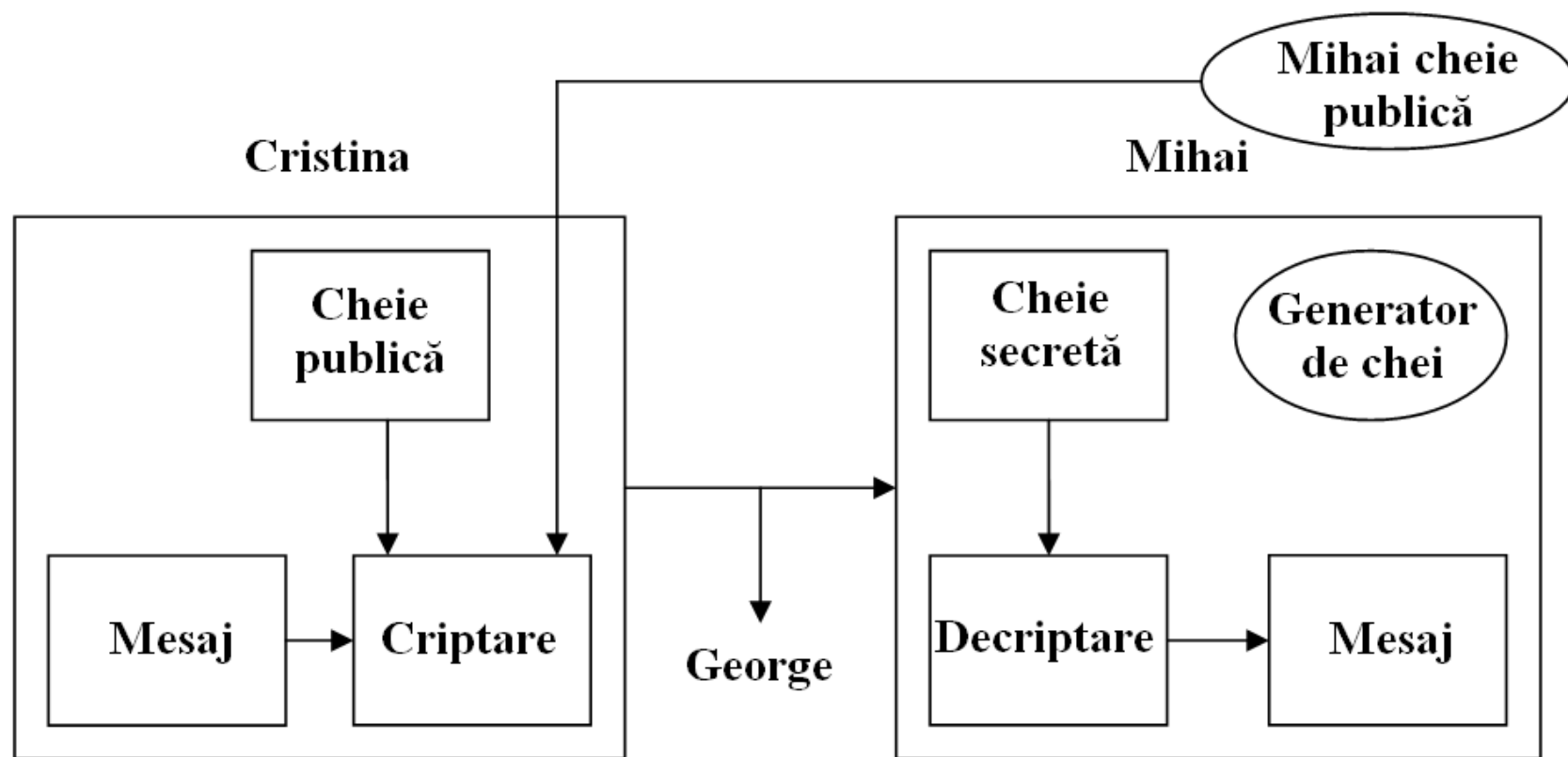
Criptarea

- fișierul este criptat
- cheia de decriptare distribuită persoanelor autorizate
- fișierul criptat → Internet
- inutil pentru un pirat fără cheie
- după criptare mesaj fără înțeles și neinteligibil
- două tipuri de sisteme de criptare: simetrice și asimetrice
 - simetrice: aceeași cheie pentru criptare și decriptare
 - asimetrice: chei diferite pentru criptare și decriptare

Sistem de criptare simetric



Sistem de criptare asimetric



Criptarea

Exemplu simplu de criptare și decriptare a unui mesaj binar

Criptare		Decriptare	
Mesaj:	0 1 0 1 1 0 0 1	Mesaj:	1 1 0 0 1 1 1 0
Cheie:	1 0 0 1 0 1 1 1	Cheie:	1 0 0 1 0 1 1 1
Mesaj criptat:	1 1 0 0 1 1 1 0	Mesaj decriptat:	0 1 0 1 1 0 0 1
Mesaj $\oplus$ cheie		Mesaj $\oplus$ cheie	

Criptarea

Exemplu de criptare a unei imagini



Imagine necriptată



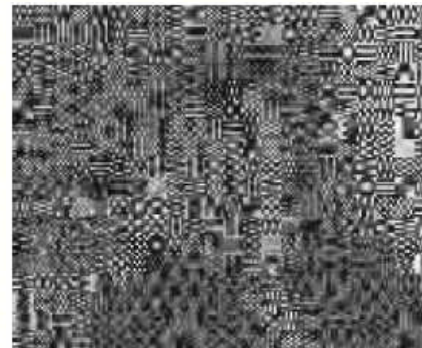
Imagine criptată
(imagine originală
neidentificabilă)

Criptarea

Exemple de criptare a unui cadru video



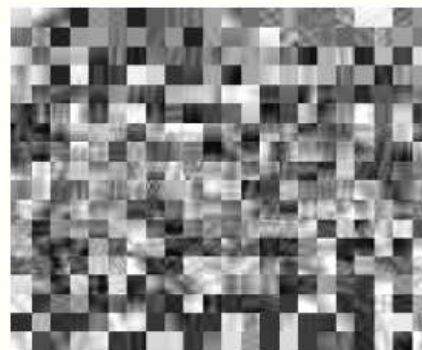
cadru original



Permutare coeficienți
DCT



Criptarea semnului



Permutare blocuri +
rotire blocuri +
permutare coef. DCT

Watermarking Digital

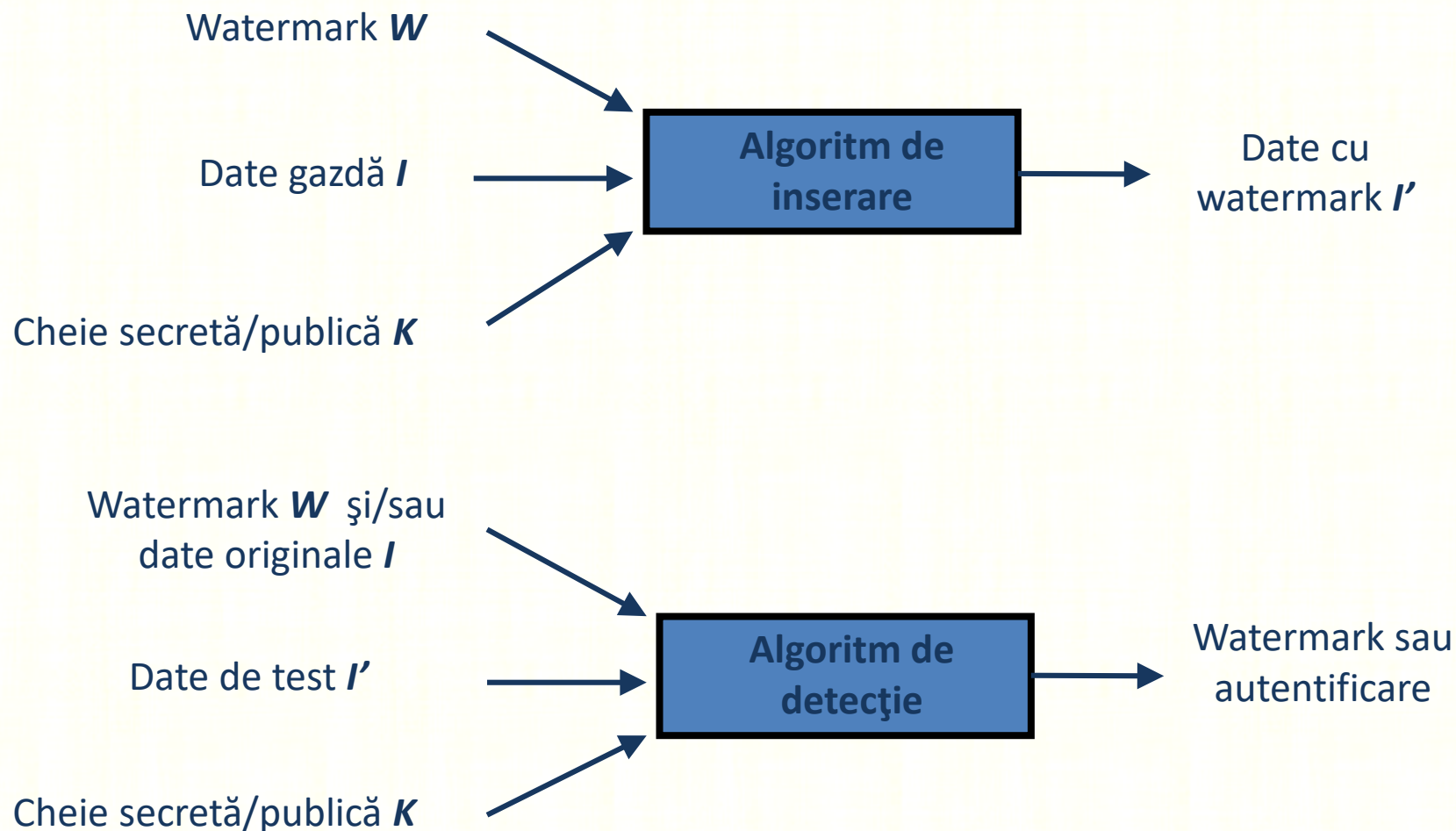
- informație ascunsă în text, imagini, date audio sau video
- modificare perceptibilă / imperceptibilă a acestora
- în secolul al XIII-lea în Fabriano, Italia, pentru marcarea și identificarea hârtiei
- „watermarking” deoarece urmele formate de marcajele prin fire erau percepute ca suprafețe de apă pe articolele marcate

Watermarking Digital

Domenii de aplicabilitate:

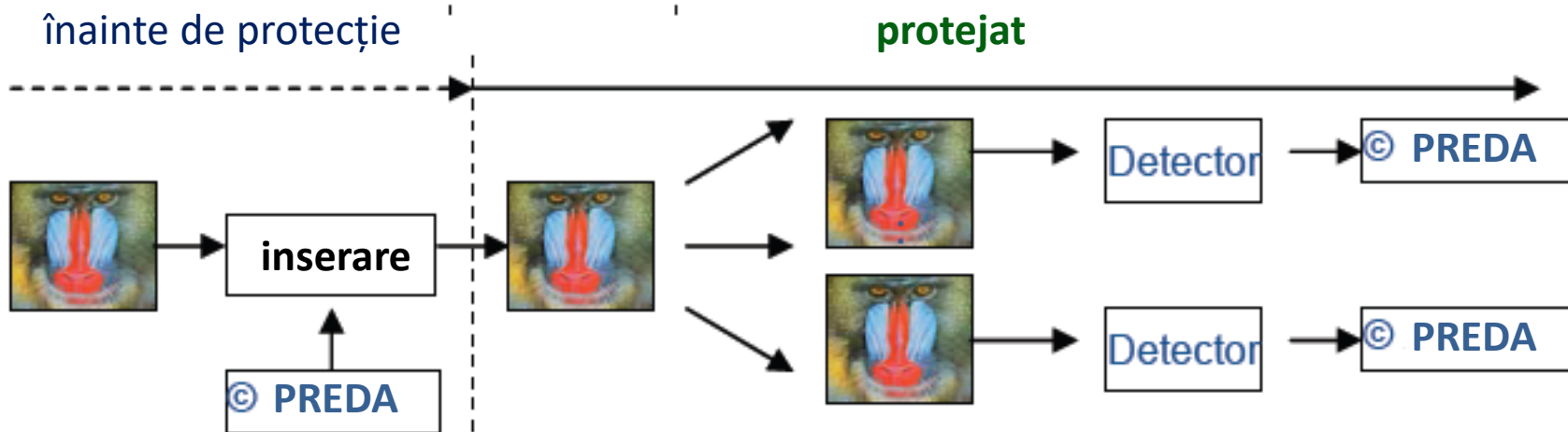
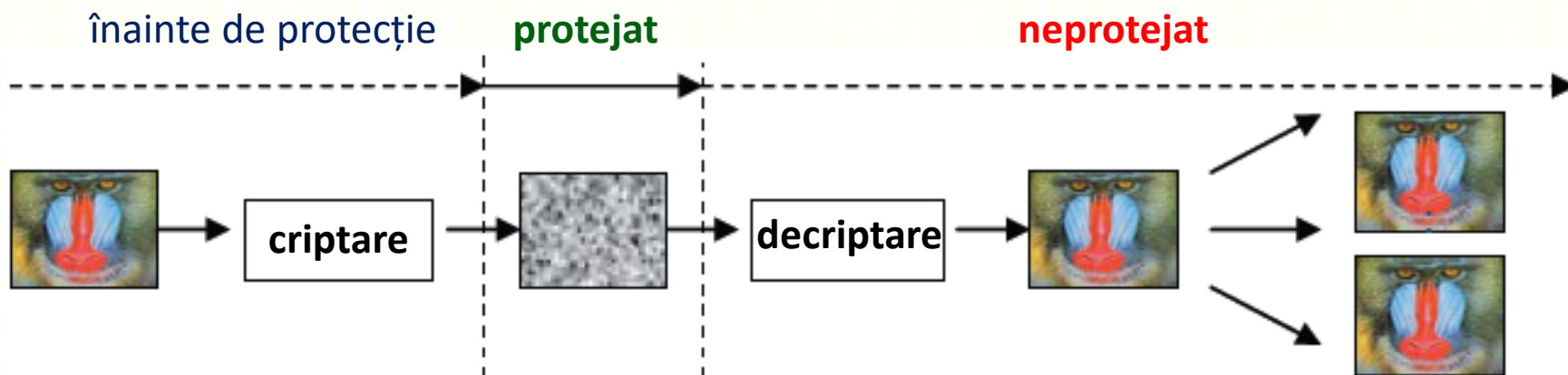
- Protecția drepturilor de autor
- Amprentarea
- Protecția la copiere
- Monitorizarea emisiei
- Autentificarea datelor
- Indexarea
- Siguranța medicală
- Ascunderea datelor

Schema unui sistem de watermarking



Criptare vs. watermarking

Criptare



watermarking

Multimedia Forensics

- Oferă soluții pentru:
 - Identificarea sursei materialului multimedia
 - Identificarea producătorului (CFA, metadata EXIF)
 - Identificarea modelului (cuantizare JPEG, metadata EXIF)
 - Identificarea dispozitivului (analiza zgomotului senzorului)
 - Verificarea integrității (autentificarea) conținutului multimedia



Multimedia Forensics

Verificarea integrității conținutului multimedia

- Verificarea dacă materialul media a fost prelucrat într-un fel
 - Editare neagresivă
 - Editare agresivă (falsificare)
- Modalități de falsificare:
 - Copiere-mutare
 - Ștergere
 - Inserare conținut nou

Multimedia Forensics

Copiere-mutare



Inserare conținut nou



Ștergere

