

Alternative Distribution Models Based On P2P

Martin Schmucker
Peter Ebinger

<http://www.igd.fhg.de/igd-a8>

martin.schmucker@igd.fraunhofer.de
peter.ebinger@igd.fraunhofer.de

Supreme Court Rules Against P2P Companies

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Monday 27th June 2005: “Supremes down P2P software makers in unanimous decision.”

„The ruling means that developers of P2P software can be held liable for their users' actions and that the software makers must work to prevent the distribution of copyrighted material.“

source: http://www.theregister.co.uk/2005/06/27/p2p_goes_down/

Requirement: Legal and Trusted P2P

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- To protect content owners
- To protect technology developers and service providers
- To protect users

Problems of Existing Technologies

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ DRM

- „Secure Container“ → Usability
- Security → Hackz, Crackz, „analog hole“

■ Internet

- “DarkNets”, “Groupers” → content distribution cannot be controlled

➔ To create a framework for legal content exchange

Specific Requirements

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

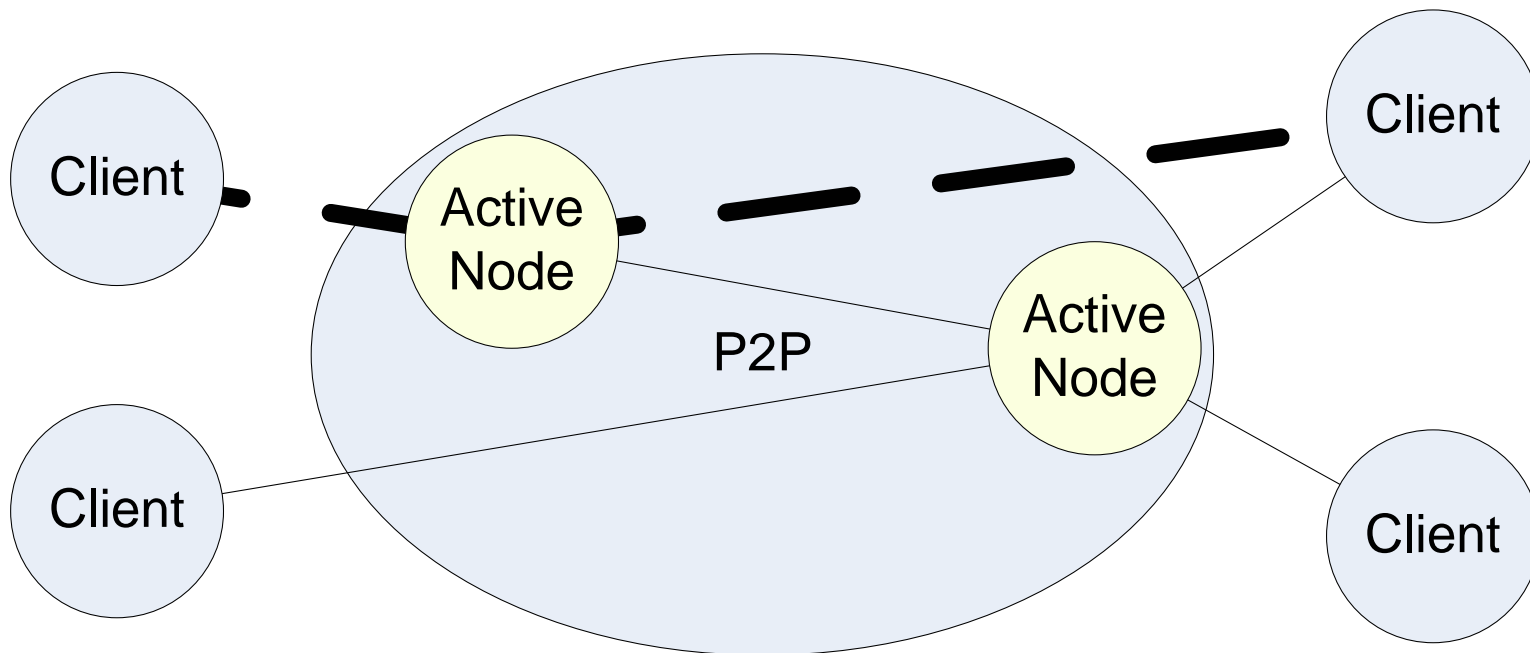
- Only legal exchange must be possible!
- Audio visual content requires a P2P based framework
- Users are responsible for their actions
- Users are aware of their actions' legal status

©2005, Fraunhofer IGD

First problem: Legal exchange on P2P

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

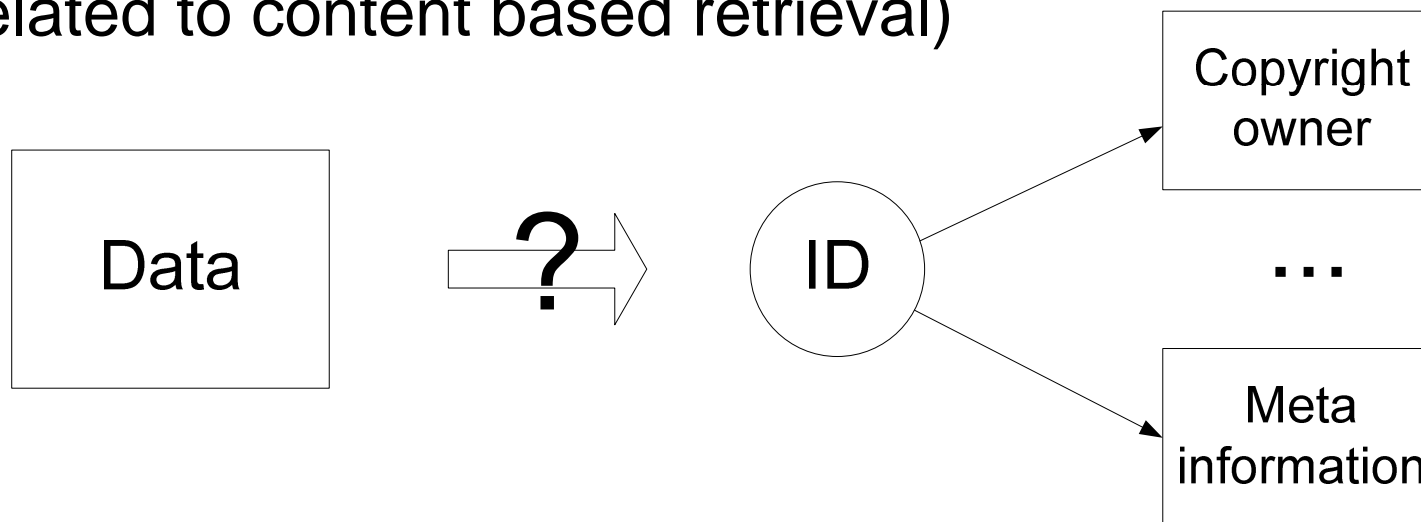
- First solution: active „filter nodes“:



Perceptual hashing/fingerprinting

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Meta data: problems of “spelling mistakes”
- Content identification based on content characteristics (related to content based retrieval)

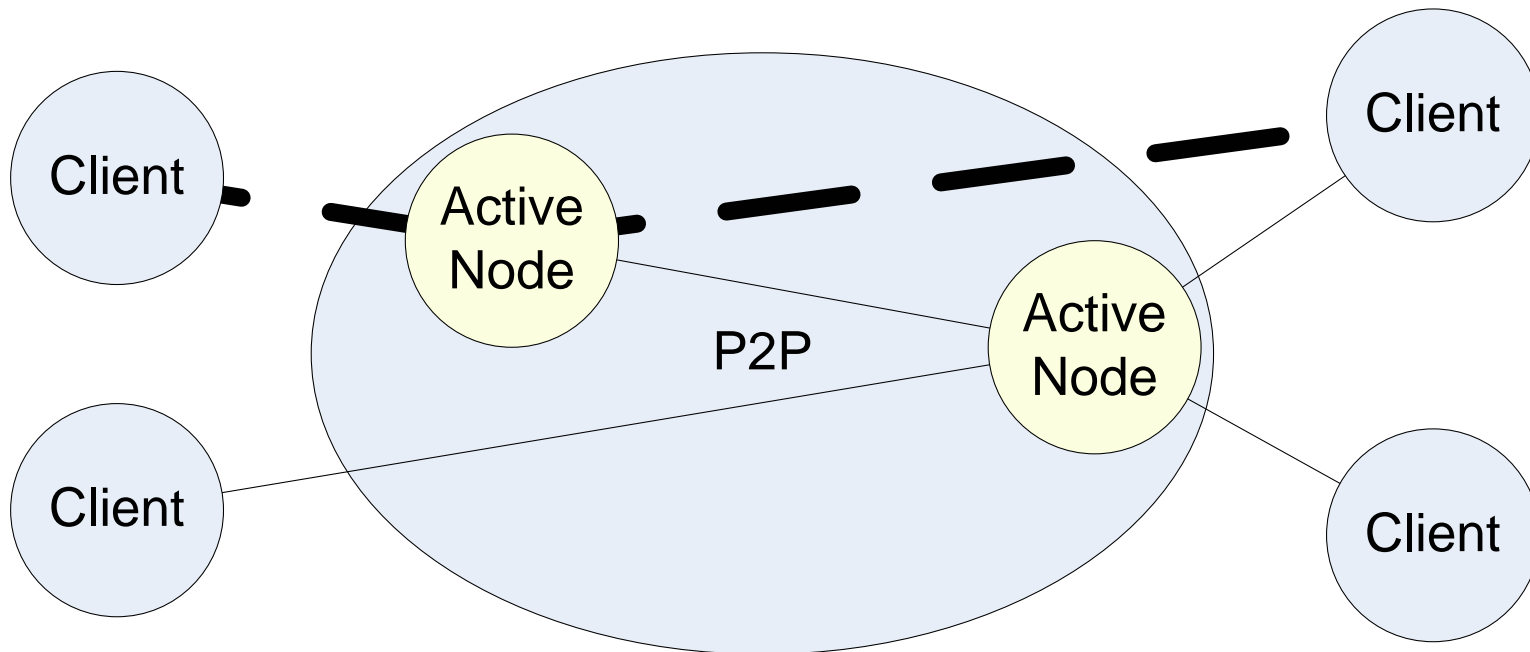


©2005, Fraunhofer IGD

First problem: Legal exchange on P2P

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

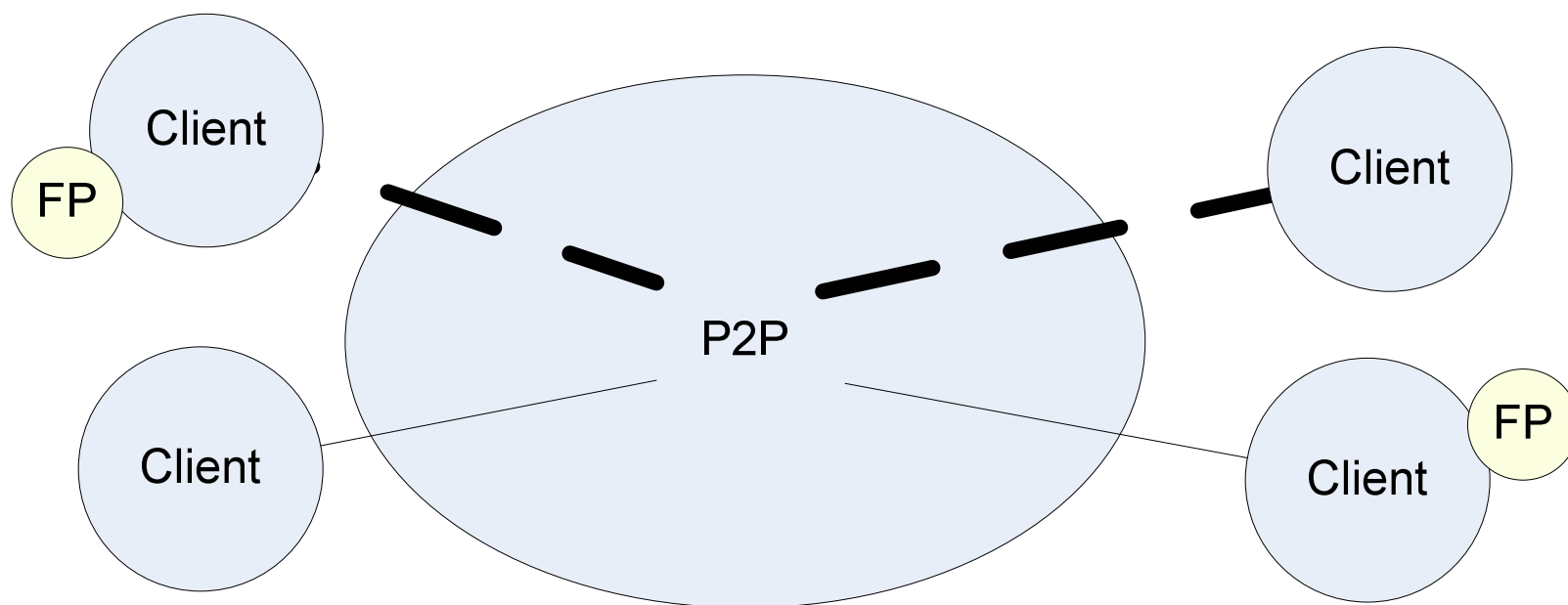
- First solution: active „filter nodes“:



Filtering technology „with“ the peers

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

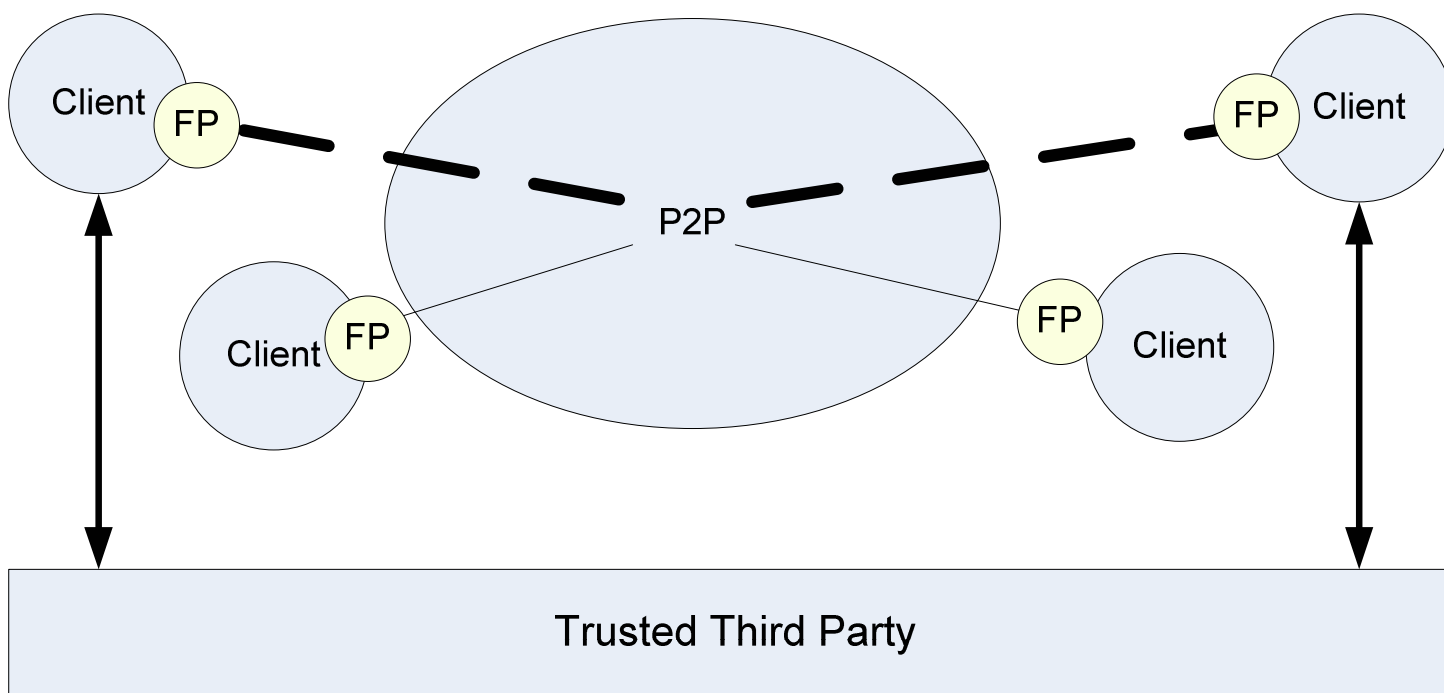
- Encrypted or scrambled content → FP „with“ Peers



Design: Mutual observing peers

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ report of illegal behaviour



©2005, Fraunhofer IGD

10

Mutual observing peers

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Problem: “customers are unaware”
 - Fingerprinting technology identifies content

- Problem: “the police is always needed”
 - each peer observes the peers it is exchanging content with

- Misuse
 - Public keys for provable identification of misuse

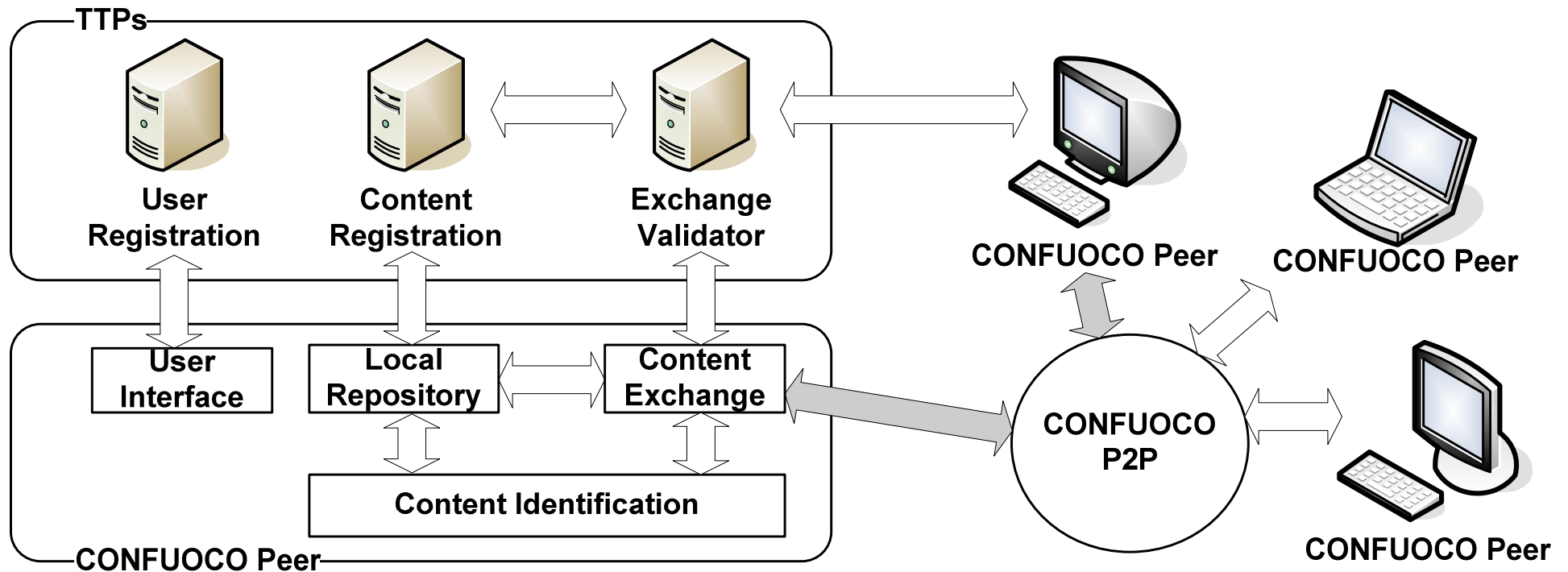
User awareness

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



Overall Architecture

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••



©2005, Fraunhofer IGD

13

Summary

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- A P2P framework for legal exchange is possible
 - Risk of detecting illegal exchange is very high
 - Other networks will be used for illegal exchange

- Ideally suited for promotional distribution of content
 - Costs are transferred to participants
 - Content must not be protected/encrypted → Usability

- Can be extended to support various business models
 - Support of rights collecting societies
 - Support of “flat rate” models

Promotional and Commercial Content Distribution based on a Legal and Trusted P2P Framework

Martin Schmucker
Peter Ebinger

<http://www.igd.fhg.de/igd-a8>

martin.schmucker@igd.fraunhofer.de
peter.ebinger@igd.fraunhofer.de

References

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- DarkNet, <http://crypto.stanford.edu/DRM2002/darknet5.doc>
- DirectShare, <http://www.laplink.com>
- PeerImpact, <http://www.peerimpact.com>
- Audible Magic, <http://www.audiblemagic.com>
- Gracenote, <http://www.gracenote.com/>
- M2any, <http://www.m2any.com/>
- CONFUO©O, <http://www.igd.fhg.de/igd-a8/en/projects/watermarks/confuoco/index.html>